MS-W11-22H2-I-003

Microsoft Windows, Microsoft Windows Server and Azure version 22H2 Assurance Activity Report

Version 1.0

2023-08

01-09-2023

Product:
Microsoft Windows 11 (version 22H2), Microsoft Windows 10 (version 22H2), Microsoft Windows Server 2022, Microsoft Windows Server Datacenter: Azure edition Edition, Microsoft Azure Stack HCIv2 version 22H2, Microsoft Azure Stack Hub and Microsoft Azure Stack Edge

Developer:	Microsoft Corporation
Sponsor:	Microsoft Corporation
Security Target:	Microsoft Windows, Windows Server and Azure version 22H2 Security Target, version 0.04, July 3 2023
Certification body:	Centro Criptólogico Nacional - CCN
ITSEF:	DEKRA Testing and Certification S.A.U.

Prepared by:

DEKRA Testing and Certification S.A.U.
NIF A29507456

Avenida de los Pirineos, 7
Nave 9A
28703, San Sebastián de los Reyes (Madrid)

Telephone: +34 916588314
+34 916238772

Document approved, revised and signed by the Project Manager: Álvaro Ortega Chamorro

Contents

1 Version History **25**

2 Introduction **26**
2.1 Background 26
2.2 Scope 27

3 Samples Identification **32**

4 Evaluation basis **33**

5 References **34**

6 Competences, guarantees and general conditions **36**

7 TOE Configuration **37**

8 Test environment definition **38**
8.1 Evaluation approach 38
8.1.1 Testing strategy 39

9 FAU_GEN.1.1 **41**
9.1 Documentation Review Activity 41
9.1.1 Findings 41
9.1.2 Verdict 47
9.2 Test Activity 47
9.2.1 Test 1 - Startup, Shutdown and Authentication events 47
9.2.2 Test 2 - Privileges or role escalation and audit and log data access events 49
9.2.3 Test 3 - User and group management events 51
9.2.4 Test 4 - Use of privileged rights and file and object events 53
9.2.5 Test 5 - Cryptographic verification of software events 54
9.2.6 Test 6 - Program initiation events 57
9.2.7 Test 7 - Kernel module loading events 59
9.2.8 Test 8 - Lock and unlock user accounts 60
9.3 Final Verdict 62

10 FAU_GEN.1.2 **63**
10.1 Documentation Review Activity 63
10.1.1 Findings 63
10.1.2 Verdict 64
10.2 Test Activity 64
10.2.1 Test 64
10.3 Final Verdict 65

11 FCS_CKM.1.1(1) 66
11.1 Documentation Review Activity . . . 68
11.1.1 Findings . . . 68
11.1.2 Verdict . . . 82
11.2 Test Activity . . . 82
11.2.1 Test (Key Generation for FIPS PUB 186-4 RSA Schemes) . . . 84
11.2.2 Test (Key Generation for Elliptic Curve Cryptography (ECC)) . . . 84
11.2.3 Test (Key Generation for Finite-Field Cryptography (FFC)) . . . 85
11.3 Final Verdict . . . 86

12 FCS_CKM.2.1(1) 87
12.1 Documentation Review Activity . . . 90
12.1.1 Findings . . . 90
12.1.2 Verdict . . . 125
12.2 Test Activity . . . 126
12.2.1 Test 1 (KAS-ECC) . . . 127
12.2.2 Test 2 (KAS-FFC) . . . 128
12.2.3 Test 3 (KAS-RSA) . . . 129
12.3 Final Verdict . . . 134

13 FCS_CKM_EXT.4 135
13.1 Documentation Review Activity . . . 138
13.1.1 Findings . . . 138
13.1.2 Verdict . . . 140
13.2 Test Activity . . . 140
13.2.1 Test 1 . . . 140
13.3 Final Verdict . . . 141

14 FCS_COP.1.1(1) 142
14.1 Documentation Review Activity . . . 147
14.1.1 Findings . . . 147
14.1.2 Verdict . . . 157
14.2 Test Activity . . . 157
14.2.1 Test 1 . . . 159
14.3 Final Verdict . . . 159

15 FCS_COP.1.1(2) 160
15.1 Documentation Review Activity . . . 161
15.1.1 Findings . . . 161
15.1.2 Verdict . . . 175
15.2 Test Activity . . . 175
15.2.1 Test 1 . . . 176
15.3 Final Verdict . . . 177

16 FCS_COP.1.1(3) 178
16.1 Documentation Review Activity . . . 179
16.1.1 Findings . . . 179
16.1.2 Verdict . . . 189
16.2 Test Activity . . . 189
16.2.1 Test 1 Signature generation . . . 190
16.2.2 Test 2 Signature verification . . . 191
16.3 Final Verdict . . . 192

17 FCS_COP.1.1(4) 193
17.1 Documentation Review Activity . . . 193
17.1.1 Findings . . . 193
17.1.2 Verdict . . . 206
17.2 Test Activity . . . 206
17.2.1 Test 1 . . . 207
17.3 Final Verdict . . . 208

18 FCS_DTLS_EXT.1.1 209
18.1 Documentation Review activity . . . 209
18.1.1 Findings . . . 209
18.1.2 Verdict . . . 209
18.2 Test Activity . . . 209
18.2.1 Test 1 . . . 213
18.3 Final Verdict . . . 214

19 FCS_DTLS_EXT.1.2 215
19.1 Documentation Review activity . . . 215
19.1.1 Findings . . . 215
19.1.2 Verdict . . . 215
19.2 Test Activity . . . 215
19.2.1 Test 1 - FCS_TLSC_EXT.1.1 for DTLS . . . 215
19.2.2 Test 2 - FCS_TLSC_EXT.1.1 for DTLS . . . 217
19.2.3 Test 3 - FCS_TLSC_EXT.1.1 for DTLS . . . 217
19.2.4 Test 4 - FCS_TLSC_EXT.1.1 for DTLS . . . 218
19.2.5 Test 5.1 - FCS_TLSC_EXT.1.1 for DTLS . . . 218
19.2.6 Test 5.2 - FCS_TLSC_EXT.1.1 for DTLS . . . 219
19.2.7 Test 5.3 - FCS_TLSC_EXT.1.1 for DTLS . . . 220
19.2.8 Test 5.4 - FCS_TLSC_EXT.1.1 for DTLS . . . 220
19.2.9 Test 5.5 - FCS_TLSC_EXT.1.1 for DTLS . . . 221
19.2.10 Test 5.6 - FCS_TLSC_EXT.1.1 for DTLS . . . 221
19.2.11 Test 1 - FCS_TLSC_EXT.1.2 for DTLS . . . 222
19.2.12 Test 2 - FCS_TLSC_EXT.1.2 for DTLS . . . 223
19.2.13 Test 3 - FCS_TLSC_EXT.1.2 for DTLS . . . 224
19.2.14 Test 4 - FCS_TLSC_EXT.1.2 for DTLS . . . 224

19.2.15 Test 5.1 - FCS_TLSC_EXT.1.2 for DTLS . . . 225
19.2.16 Test 5.2 - FCS_TLSC_EXT.1.2 for DTLS . . . 226
19.2.17 Test 5.3 - FCS_TLSC_EXT.1.2 for DTLS . . . 226
19.2.18 Test 1 - FCS_TLSC_EXT.1.3 for DTLS . . . 227
19.2.19 Test 2 - FCS_TLSC_EXT.1.3 for DTLS . . . 228
19.2.20 Test 3 - FCS_TLSC_EXT.1.3 for DTLS . . . 229
19.2.21 Test 4 - FCS_TLSC_EXT.1.3 for DTLS . . . 230
19.3 Final Verdict . . . 230

20 FCS_RBG_EXT.1.1 231
20.1 Documentation Review Activity . . . 232
20.1.1 Findings . . . 232
20.1.2 Verdict . . . 251
20.2 Test Activity . . . 251
20.2.1 Test 1 . . . 252
20.2.2 Results . . . 253
20.3 Final Verdict . . . 253

21 FCS_RBG_EXT.1.2 254
21.1 Documentation Review Activity . . . 254
21.1.1 Findings . . . 254
21.1.2 Verdict . . . 255
21.2 Test Activity . . . 255
21.3 Final Verdict . . . 255

22 FCS_STO_EXT.1.1 256
22.1 Documentation Review Activity . . . 256
22.1.1 Findings . . . 256
22.1.2 Verdict . . . 258
22.2 Test Activity . . . 259
22.2.1 Test 1 . . . 259
22.3 Final Verdict . . . 260

23 FCS_TLSC_EXT.1.1 261
23.1 Documentation Review activity . . . 262
23.1.1 Findings . . . 262
23.1.2 Verdict . . . 263
23.2 Test Activity . . . 263
23.2.1 Test 1 . . . 266
23.2.2 Test 2 . . . 267
23.2.3 Test 3 . . . 268
23.2.4 Test 4 . . . 269
23.2.5 Test 5.1 . . . 269
23.2.6 Test 5.2 . . . 270

23.2.7 Test 5.3 . . . 270
23.2.8 Test 5.4 . . . 271
23.2.9 Test 5.5 . . . 272
23.2.10 Test 5.6 . . . 272
23.3 Final Verdict . . . 273

24 FCS_TLSC_EXT.1.2 274
24.1 Documentation Review activity . . . 275
24.1.1 Findings . . . 275
24.1.2 Verdict . . . 276
24.2 Test Activity . . . 276
24.2.1 Test 1 . . . 276
24.2.2 Test 2 . . . 278
24.2.3 Test 3 . . . 278
24.2.4 Test 4 . . . 279
24.2.5 Test 5.1 . . . 280
24.2.6 Test 5.2 . . . 280
24.2.7 Test 5.3 . . . 281
24.2.8 Test 6 . . . 282
24.2.9 Test 7 . . . 282
24.3 Final Verdict . . . 283

25 FCS_TLSC_EXT.1.3 284
25.1 Documentation Review activity . . . 284
25.1.1 Findings . . . 284
25.1.2 Verdict . . . 284
25.2 Test Activity . . . 284
25.2.1 Test 1 . . . 285
25.2.2 Test 2 . . . 286
25.2.3 Test 3 . . . 287
25.2.4 Test 4 . . . 288
25.3 Final Verdict . . . 289

26 FCS_TLSC_EXT.2.1 290
26.1 Documentation Review activity . . . 290
26.1.1 Findings . . . 290
26.1.2 Verdict . . . 290
26.2 Test Activity . . . 290
26.2.1 Test 1 . . . 291
26.3 Final Verdict . . . 292

27 FCS_TLSC_EXT.3.1 293
27.1 Documentation Review activity . . . 293
27.1.1 Findings . . . 293

27.1.2 Verdict 293
27.2 Test Activity 294
27.2.1 Test 1 294
27.3 Final Verdict 295

28 FCS_TLSC_EXT.4.1 296
28.1 Documentation Review activity 296
28.1.1 Findings 296
28.1.2 Verdict 296
28.2 Test Activity 297
28.2.1 Test 1 297
28.2.2 Test 2 298
28.3 Final Verdict 300

29 FDP_ACF_EXT.1.1 301
29.1 Documentation Review Activity 302
29.1.1 Findings 302
29.1.2 Verdict 302
29.2 Test Activity 303
29.2.1 Test 1, Test 2, Test 3, Test 4, Test 5 and Test 6 303
29.3 Final Verdict 304

30 FIA_AFL.1.1 305
30.1 Documentation Review Activity 305
30.1.1 Findings 305
30.1.2 Verdict 305
30.2 Test Activity 305
30.2.1 Test 305
30.3 Final Verdict 306

31 FIA_AFL.1.2 307
31.1 Documentation Review Activity 307
31.1.1 Findings 307
31.1.2 Verdict 307
31.2 Test Activity 307
31.2.1 Test 1 308
31.2.2 Test 2 & Test 3 309
31.3 Final Verdict 310

32 FIA_UAU.5.1 311
32.1 Documentation Review Activity 312
32.1.1 Findings 312
32.1.2 Verdict 312

32.2 Test Activity 313
32.2.1 Test 1 & Test 2 - Username and password 313
32.2.2 Test 1 & Test 2 - Username and a PIN that releases an asymmetric key stored in OE-protected storage (TPM) 314
32.2.3 Test 1 & Test 2 - Username and a PIN that releases an asymmetric key stored in OE-protected storage (Smart Card) 316
32.2.4 Test 1 & Test 2 - X.509 Certificates 323
32.3 Final Verdict 324

33 FIA_UAU.5.2 325
33.1 Documentation Review Activity 325
33.1.1 Findings 325
33.1.2 Verdict 326
33.2 Test Activity 326
33.2.1 Test 1 326
33.2.2 Test 2 327
33.3 Final Verdict 328

34 FIA_X509_EXT.1.1 329
34.1 Documentation Review activity 330
34.1.1 Findings 330
34.1.2 Verdict 330
34.2 Test Activity 330
34.2.1 Test 1 331
34.2.2 Test 2 332
34.2.3 Test 3 333
34.2.4 Test 4 337
34.2.5 Test 5 339
34.2.6 Test 6 340
34.2.7 Test 7 341
34.3 Final Verdict 341

35 FIA_X509_EXT.1.2 342
35.1 Documentation Review activity 342
35.1.1 Findings 342
35.1.2 Verdict 342
35.2 Test Activity 342
35.2.1 Test 1 343
35.2.2 Test 2 344
35.2.3 Test 3 345
35.3 Final Verdict 346

36 FIA_X509_EXT.2.1 347
36.1 Documentation Review activity 347
36.1.1 Findings 347
36.1.2 Verdict 347
36.2 Test Activity 347
36.2.1 Test 1 348
36.3 Final Verdict 349

37 FMT_MOF_EXT.1.1 & FMT_SMF_EXT.1.1 350
37.1 Documentation Review Activity 350
37.1.1 Findings 350
37.1.2 Verdict 353
37.2 Test Activity 354
37.2.1 Test 1 - Enable/Disable Screen Lock 354
37.2.2 Test 2 - Configure Screen Lock Inactivity Timeout 355
37.2.3 Test 3 - Configure Local Audit Storage Capacity 362
37.2.4 Test 4 - Configure Minimum Password Length 364
37.2.5 Test 9 - Configure Lockout Policy for Unsuccessful Authentication Attempts through Timeouts between Attempts, Limiting Number of Attempts During a Time Period 365
37.2.6 Test 10 - Configure Host-based Firewall 367
37.2.7 Test 11 - Configure Name/Address of Directory Server to Bind with . . 368
37.2.8 Test 12 - Configure Name/Address of Remote Management Server from Which to Receive Management Settings 370
37.2.9 Test 14 - Configure Audit Rules 371
37.2.10Test 15 - Configure Name/Address of Network Time Server 373
37.2.11Test 16 - Enable/Disable Automatic Software Update 374
37.2.12Test 17 - Configure Wi-Fi interface 375
37.2.13Test 18 - Enable/Disable Bluetooth interface 377
37.2.14Test 19 - Enable/Disable Local Area Network interface 378
37.2.15Test 19 (2) - Configure USB interfaces 379
37.2.16Test 20 - Manage Windows Diagnostics settings 381
37.2.17Test 20 (2) - Configure Remote Connection Inactivity Timeout 382
37.3 Final Verdict 383

38 FPT_ACF_EXT.1.1 384
38.1 Documentation Review Activity 384
38.1.1 Findings 384
38.1.2 Verdict 385
38.2 Test Activity 385
38.2.1 Test 1 385
38.2.2 Test 2 386
38.2.3 Test 3 388
38.2.4 Test 4 389

38.2.5 Test 5 . . . 390
38.2.6 Test 6 . . . 391
38.3 Final Verdict . . . 392

39 FPT_ACF_EXT.1.2 **393**
39.1 Documentation Review Activity . . . 393
39.1.1 Findings . . . 393
39.1.2 Verdict . . . 393
39.2 Test Activity . . . 393
39.2.1 Test 1 . . . 393
39.2.2 Test 2 . . . 395
39.2.3 Test 3 . . . 396
39.3 Final Verdict . . . 397

40 FPT_ASLR_EXT.1.1 **398**
40.1 Documentation Review Activity . . . 398
40.1.1 Findings . . . 398
40.1.2 Verdict . . . 398
40.2 Test Activity . . . 398
40.2.1 Test 1 . . . 398
40.3 Final Verdict . . . 399

41 FPT_SBOP_EXT.1.1 **400**
41.1 Documentation Review Activity . . . 400
41.1.1 Findings . . . 400
41.1.2 Verdict . . . 401
41.2 Test Activity . . . 401
41.2.1 Test 1 . . . 401
41.3 Final Verdict . . . 402

42 FPT_SRP_EXT.1.1 **403**
42.1 Documentation Review Activity . . . 404
42.1.1 Findings . . . 404
42.1.2 Verdict . . . 404
42.2 Test Activity . . . 404
42.2.1 Test 1 & Test 2 . . . 408
42.2.2 Test 3 & Test 4 . . . 416
42.2.3 Test 5 & Test 6 . . . 422
42.2.4 Test 7 & Test 8 . . . 434
42.3 Final Verdict . . . 440

43 FPT_TST_EXT.1.1 **441**
43.1 Documentation Review Activity . . . 442
43.1.1 Findings . . . 442

43.1.2 Verdict 443
43.2 Test Activity 443
43.2.1 Test 1 443
43.2.2 Test 2 444
43.2.3 Test 3 445
43.3 Final Verdict 448

44 FPT_TUD_EXT.1.1 449
44.1 Documentation Review Activity 449
44.1.1 Findings 449
44.1.2 Verdict 451
44.2 Test Activity 452
44.2.1 Test 1 452
44.3 Final Verdict 453

45 FPT_TUD_EXT.1.2 454
45.1 Documentation Review Activity 454
45.1.1 Findings 454
45.1.2 Verdict 455
45.2 Test Activity 455
45.2.1 Test 1 455
45.2.2 Test 2 456
45.3 Final Verdict 457

46 FPT_TUD_EXT.2.1 458
46.1 Documentation Review Activity 458
46.1.1 Findings 458
46.1.2 Verdict 460
46.2 Test Activity 460
46.2.1 Test 1 460
46.3 Final Verdict 461

47 FPT_TUD_EXT.2.2 462
47.1 Documentation Review Activity 462
47.1.1 Findings 462
47.1.2 Verdict 463
47.2 Test Activity 463
47.2.1 Test 1 463
47.2.2 Test 2 466
47.3 Final Verdict 467

48 FTA_TAB.1.1 468
48.1 Documentation Review Activity 468
48.1.1 Findings 468

48.1.2 Verdict . . . 470
48.2 Test Activity . . . 471
48.2.1 Test 1 . . . 471
48.3 Final Verdict . . . 472

49 FTP_ITC_EXT.1.1 (DTLS) 473
49.1 Documentation Review activity . . . 473
49.1.1 Findings . . . 473
49.1.2 Verdict . . . 473
49.2 Test Activity . . . 473
49.2.1 Test 1 . . . 473
49.3 Final Verdict . . . 474

50 FTP_ITC_EXT.1.1 (TLS) 475
50.1 Documentation Review activity . . . 475
50.1.1 Findings . . . 475
50.1.2 Verdict . . . 475
50.2 Test Activity . . . 475
50.2.1 Test 1 . . . 475
50.3 Final Verdict . . . 492

51 FTP_TRP.1.1 493
51.1 Documentation Review Activity . . . 493
51.1.1 Findings . . . 493
51.1.2 Verdict . . . 494
51.2 Test Activity . . . 494
51.2.1 Test 1 & Test 3 . . . 494
51.2.2 Test 2 . . . 500
51.2.3 Test 4 . . . 501
51.3 Final Verdict . . . 503

52 FAU_GEN.1/WLAN 504
52.1 Documentation Review activity . . . 505
52.1.1 Findings . . . 505
52.1.2 Verdict . . . 506
52.2 Test Activity . . . 506
52.2.1 Test 1 . . . 506
52.3 Final Verdict . . . 507

53 FCS_CKM.1/WPA & FCS_CKM.2/WLAN 508
53.1 Documentation Review activity . . . 509
53.1.1 Findings . . . 509
53.1.2 Verdict . . . 510

53.2 Test Activity 510
53.2.1 Test 1 510
53.2.2 Test 2 511
53.3 Final Verdict 512

54 FCS_TLSC_EXT.1/WLAN 513
54.1 Documentation Review activity 514
54.1.1 Findings 514
54.1.2 Verdict 515
54.2 Test Activity 515
54.2.1 Test 1 515
54.2.2 Test 2 517
54.2.3 Test 3 518
54.2.4 Test 4 519
54.2.5 Test 5 520
54.3 Final Verdict 522

55 FCS_TLSC_EXT.2/WLAN 523
55.1 Documentation Review activity 523
55.1.1 Findings 523
55.1.2 Verdict 523
55.2 Test Activity 524
55.2.1 Test 1 524
55.3 Final Verdict 525

56 FCS_WPA_EXT.1/WLAN 526
56.1 Documentation Review activity 526
56.1.1 Findings 526
56.1.2 Verdict 526
56.2 Test Activity 526
56.2.1 Test 1 526
56.3 Final Verdict 528

57 FIA_PAE_EXT.1/WLAN 529
57.1 Documentation Review activity 529
57.1.1 Findings 529
57.1.2 Verdict 529
57.2 Test Activity 529
57.2.1 Test 1 529
57.2.2 Test 2 530
57.2.3 Test 3 531
57.3 Final Verdict 533

58 FIA_X509_EXT.1/WLAN 534
58.1 Documentation Review activity . . . 534
58.1.1 Findings . . . 534
58.1.2 Verdict . . . 535
58.2 Test Activity . . . 535
58.2.1 Test 1 . . . 535
58.2.2 Test 2 . . . 536
58.2.3 Test 3 . . . 538
58.2.4 Test 4 . . . 539
58.2.5 Test 5 . . . 540
58.2.6 Test 6 . . . 541
58.3 Final Verdict . . . 542

59 FIA_X509_EXT.2/WLAN 543
59.1 Documentation Review activity . . . 543
59.1.1 Findings . . . 543
59.1.2 Verdict . . . 544
59.2 Test Activity . . . 544
59.2.1 Test 1 . . . 544
59.3 Final Verdict . . . 545

60 FIA_X509_EXT.6/X.509 546
60.1 Documentation Review activity . . . 546
60.1.1 Findings . . . 546
60.1.2 Verdict . . . 546
60.2 Test Activity . . . 546
60.2.1 Test 1 . . . 546
60.2.2 Test 2 . . . 547
60.3 Final Verdict . . . 548

61 FMT_SMF.1/WLAN 549
61.1 Documentation Review activity . . . 549
61.1.1 Findings . . . 549
61.1.2 Verdict . . . 549
61.2 Test Activity . . . 549
61.2.1 Test 1 . . . 549
61.3 Final Verdict . . . 561

62 FPT_TST_EXT.3/WLAN 562
62.1 Documentation Review activity . . . 562
62.1.1 Findings . . . 562
62.1.2 Verdict . . . 564
62.2 Test Activity . . . 564
62.2.1 Test 1 . . . 564

62.2.2 Test 2 . . . 565
62.3 Final Verdict . . . 566

63 FTA_WSE_EXT.1/WLAN 567
63.1 Documentation Review activity . . . 567
63.1.1 Findings . . . 567
63.1.2 Verdict . . . 567
63.2 Test Activity . . . 568
63.2.1 Test 1 . . . 568
63.3 Final Verdict . . . 569

64 FTP_ITC.1/WLAN 570
64.1 Documentation Review activity . . . 570
64.1.1 Findings . . . 570
64.1.2 Verdict . . . 571
64.2 Test Activity . . . 571
64.2.1 Test 1 . . . 571
64.2.2 Test 2 . . . 572
64.2.3 Test 3 . . . 573
64.2.4 Test 4 . . . 574
64.3 Final Verdict . . . 575

65 FAU_GEN.1(VPN) 576
65.1 Documentation Review activity . . . 577
65.1.1 Findings . . . 577
65.1.2 Verdict . . . 580
65.2 Test Activity . . . 581
65.2.1 Test 1 . . . 581
65.3 Final Verdict . . . 583

66 FAU_SEL.1 584
66.1 Documentation Review activity . . . 584
66.1.1 Findings . . . 584
66.1.2 Verdict . . . 584
66.2 Test Activity . . . 585
66.2.1 Test 1 and Test2 . . . 585
66.3 Final Verdict . . . 586

67 FCS_CKM.1.1 (VPN) 587
67.1 Documentation Review activity . . . 587
67.1.1 Findings . . . 587
67.1.2 Verdict . . . 600
67.2 Test Activity . . . 600
67.3 Final Verdict . . . 600

68 FCS_CKM.2.1 601
68.1 Documentation Review activity . . . 601
68.1.1 Findings . . . 601
68.1.2 Verdict . . . 606
68.2 Test Activity . . . 606
68.3 Final Verdict . . . 606

69 FCS_EAP_EXT.1 607
69.1 Documentation Review activity . . . 608
69.1.1 Findings . . . 608
69.1.2 Verdict . . . 608
69.2 Test Activity . . . 608
69.2.1 Test 1, Test 2, Test 3 and Test 4 . . . 608
69.3 Final Verdict . . . 610

70 FCS_IPSEC_EXT.1.1 611
70.1 Documentation Review activity . . . 613
70.1.1 Findings . . . 613
70.1.2 Verdict . . . 616
70.2 Test Activity . . . 616
70.2.1 Test 1, Test 2 and Test 4 (FCS_IPSEC_EXT.1.2) . . . 616
70.3 Final Verdict . . . 619

71 FCS_IPSEC_EXT.1.2 620
71.1 Documentation Review activity . . . 620
71.1.1 Findings . . . 620
71.1.2 Verdict . . . 621
71.2 Test Activity . . . 621
71.2.1 Test 1, Test 2 & Test 3 . . . 621
71.2.2 Test 4 . . . 623
71.3 Final Verdict . . . 623

72 FCS_IPSEC_EXT.1.3 624
72.1 Documentation Review activity . . . 624
72.1.1 Findings . . . 624
72.1.2 Verdict . . . 625
72.2 Test Activity . . . 626
72.2.1 Test 1 . . . 626
72.3 Final Verdict . . . 627

73 FCS_IPSEC_EXT.1.4 628
73.1 Documentation Review activity . . . 628
73.1.1 Findings . . . 628
73.1.2 Verdict . . . 629

73.2 Test Activity . . . 629
73.2.1 Test 1 . . . 629
73.3 Final Verdict . . . 630

74 FCS_IPSEC_EXT.1.5 631
74.1 Documentation Review activity . . . 631
74.1.1 Findings . . . 631
74.1.2 Verdict . . . 632
74.2 Test Activity . . . 632
74.2.1 Test 1 . . . 632
74.2.2 Test 2 . . . 634
74.3 Final Verdict . . . 635

75 FCS_IPSEC_EXT.1.6 636
75.1 Documentation Review activity . . . 636
75.1.1 Findings . . . 636
75.1.2 Verdict . . . 637
75.2 Test Activity . . . 637
75.2.1 Test 1 . . . 637
75.3 Final Verdict . . . 638

76 FCS_IPSEC_EXT.1.7 639
76.1 Documentation Review activity . . . 640
76.1.1 Findings . . . 640
76.1.2 Verdict . . . 641
76.2 Test Activity . . . 641
76.2.1 Test 1, Test 2 and Test 3 . . . 641
76.2.2 Test 4 . . . 642
76.3 Final Verdict . . . 643

77 FCS_IPSEC_EXT.1.8 644
77.1 Documentation Review activity . . . 644
77.1.1 Findings . . . 644
77.1.2 Verdict . . . 644
77.2 Test Activity . . . 645
77.2.1 Test 1 . . . 645
77.3 Final Verdict . . . 646

78 FCS_IPSEC_EXT.1.9 647
78.1 Documentation Review activity . . . 647
78.1.1 Findings . . . 647
78.1.2 Verdict . . . 648
78.2 Test Activity . . . 648
78.3 Final Verdict . . . 648

79 FCS_IPSEC_EXT.1.10 649
79.1 Documentation Review activity . . . 649
79.2 Test Activity . . . 649
79.3 Final Verdict . . . 649

80 FCS_IPSEC_EXT.1.11 650
80.1 Documentation Review activity . . . 652
80.1.1 Findings . . . 652
80.1.2 Verdict . . . 653
80.2 Test Activity . . . 653
80.2.1 Test 1 . . . 653
80.2.2 Test 2 . . . 654
80.2.3 Test 3 . . . 655
80.2.4 Test 4, 5, 6, 8, 10 . . . 656
80.2.5 Test 7 and Test 9 . . . 658
80.3 Final Verdict . . . 658

81 FCS_IPSEC_EXT.1.12 659
81.1 Documentation Review activity . . . 659
81.2 Test Activity . . . 659
81.3 Final Verdict . . . 659

82 FCS_IPSEC_EXT.1.13 660
82.1 Documentation Review activity . . . 660
82.2 Test Activity . . . 660
82.3 Final Verdict . . . 660

83 FCS_IPSEC_EXT.1.14 661
83.1 Documentation Review activity . . . 661
83.1.1 Findings . . . 661
83.1.2 Verdict . . . 663
83.2 Test Activity . . . 663
83.2.1 Test 1, Test 2, Test 3 and Test 4 . . . 663
83.3 Final Verdict . . . 664

84 FDP_IFC_EXT.1(VPN) 665
84.1 Documentation Review activity . . . 665
84.1.1 Findings . . . 665
84.1.2 Verdict . . . 666
84.2 Test Activity . . . 666
84.2.1 Test 1 . . . 667
84.3 Final Verdict . . . 668

85 FDP_RIP.2 **669**
85.1 Documentation Review activity . . . 669
85.1.1 Findings . . . 669
85.1.2 Verdict . . . 670
85.2 Test Activity . . . 670
85.3 Final Verdict . . . 671

86 FDP_VPN_EXT.1/VPN **672**
86.1 Documentation Review activity . . . 672
86.1.1 Findings . . . 672
86.1.2 Verdict . . . 673
86.2 Test Activity . . . 673
86.2.1 Test 1 . . . 674
86.3 Final Verdict . . . 675

87 FIA_PSK_EXT.1 **676**
87.1 Documentation Review activity . . . 676
87.1.1 Findings . . . 676
87.1.2 Verdict . . . 677
87.2 Test Activity . . . 677
87.2.1 Test 1 . . . 677
87.3 Final Verdict . . . 678

88 FIA_PSK_EXT.2 **679**
88.1 Documentation Review activity . . . 679
88.1.1 Findings . . . 679
88.1.2 Verdict . . . 680
88.2 Test Activity . . . 680
88.3 Final Verdict . . . 680

89 FIA_X509_EXT.3 **681**
89.1 Documentation Review activity . . . 681
89.1.1 Findings . . . 681
89.1.2 Verdict . . . 682
89.2 Test Activity . . . 682
89.2.1 Test 1 . . . 682
89.3 Final Verdict . . . 684

90 FMT_SMF_EXT.1/VPN **685**
90.1 Documentation Review activity . . . 685
90.1.1 Findings . . . 685
90.1.2 Verdict . . . 685
90.2 Test Activity . . . 686
90.2.1 Test 1 . . . 686

90.3 Final Verdict 687

91 FPT_TST_EXT.1(VPN) 688
91.1 Documentation Review activity 689
91.1.1 Findings 689
91.1.2 Verdict 690
91.2 Test Activity 690
91.2.1 Test 1 690
91.2.2 Test 2 692
91.3 Final Verdict 693

92 FPT_ITC.1(VPN) 694
92.1 Documentation Review activity 695
92.1.1 Findings 695
92.1.2 Verdict 696
92.2 Test Activity 696
92.2.1 Test 1 696
92.2.2 Test 2 698
92.2.3 Test 3 699
92.2.4 Test 4 700
92.3 Final Verdict 701

93 FAU_GEN.1(BT) 702
93.1 Documentation Review activity 702
93.1.1 Findings 702
93.1.2 Verdict 710
93.2 Test Activity 710
93.2.1 Test 1 710
93.3 Final Verdict 712

94 FCS_CKM.8 (BT) 713
94.1 Documentation Review activity 713
94.1.1 Findings 713
94.1.2 Verdict 714
94.2 Test Activity 714
94.2.1 Test 1 714
94.3 Final Verdict 715

95 FIA_BLT_EXT.1 716
95.1 Documentation Review activity 716
95.1.1 Findings 716
95.1.2 Verdict 717
95.2 Test Activity 717
95.2.1 Test 1 717

95.3 Final Verdict 719

96 FIA_BLT_EXT.2 720
96.1 Documentation Review activity 720
96.1.1 Findings 720
96.1.2 Verdict 720
96.2 Test Activity 721
96.2.1 Test 1 721
96.3 Final Verdict 722

97 FIA_BLT_EXT.3 723
97.1 Documentation Review activity 723
97.1.1 Findings 723
97.1.2 Verdict 723
97.2 Test Activity 724
97.2.1 Test 1 724
97.3 Final Verdict 725

98 FIA_BLT_EXT.4 726
98.1 Documentation Review activity 726
98.1.1 Findings 726
98.1.2 Verdict 726
98.2 Test Activity 727
98.2.1 Test 1 727
98.3 Final Verdict 728

99 FIA_BLT_EXT.6 729
99.1 Documentation Review activity 729
99.1.1 Findings 729
99.1.2 Verdict 730
99.2 Test Activity 730
99.2.1 Test 1 and Test 2 730
99.3 Final Verdict 731

100FIA_BLT_EXT.7 732
100.1Documentation Review activity 733
100.1.1Findings 733
100.1.2Verdict 733
100.2Test Activity 733
100.3Final Verdict 733

101FMT_MOF_EXT.1/BT 734
101.1Documentation Review activity 734
101.1.1Findings 734

101.1.2 Verdict 734
101.2 Test Activity 735
101.2.1 Test 1 735
101.3 Final Verdict 736

102 FMT_SMF_EXT.1/BT **737**
102.1 Documentation Review activity 739
102.1.1 Findings 739
102.1.2 Verdict 739
102.2 Test Activity 740
102.2.1 Test 1, Test 6 and Test 8 740
102.3 Final Verdict 741

103 FTP_BLT_EXT.1 **742**
103.1 Documentation Review activity 742
103.2 Test Activity 742
103.3 Final Verdict 742

104 FPT_BLT_EXT.2 **743**
104.1 Documentation Review activity 743
104.1.1 Findings 743
104.1.2 Verdict 744
104.2 Test Activity 744
104.2.1 Test 1 744
104.3 Final Verdict 745

105 FPT_BLT_EXT.3/BR **746**
105.1 Documentation Review activity 747
105.1.1 Findings 747
105.1.2 Verdict 747
105.2 Test Activity 748
105.2.1 Test 1 748
105.2.2 Test 2 749
105.2.3 Test 3 750
105.3 Final Verdict 751

106 FPT_BLT_EXT.3/LE **752**
106.1 Documentation Review activity 753
106.1.1 Findings 753
106.1.2 Verdict 753
106.2 Test Activity 754
106.2.1 Test 1 754
106.2.2 Test 2 755
106.2.3 Test 3 756

106.3 Final Verdict 757

107 Final results 758

108 Evidence List 762

109 Evaluation Tools 763

110 Acronyms 764

111 Glossary 765

111.1 Common Criteria Terms 765

111.2 Technology Terms 765

1 Version History

Version	Date	Approved by	Changes	Application Notes
1.0	September 1, 2023	AOC	Initial version	First version of the report

2 Introduction

2.1 Background

Evaluation information:

Document identifier	MS-W11-I-003 Version 1.0 Microsoft Windows, Microsoft Windows Server and Azure version 22H2 Assurance Activity Report
Date of issue	2023-09-01
Evaluation period	2023-02-03 // 2023-09-01
Reception of the TOE	2023-04-24
Product - TOE	Windows Operating Systems (OS): • Microsoft Windows 11 Enterprise Edition • Microsoft Windows 11 version 22H2 Pro edition • Microsoft Windows 11 version 22H2 Education edition • Microsoft Windows 11 version 22H2 IoT Enterprise edition • Microsoft Windows 10 Pro edition • Microsoft Windows 10 Enterprise edition (64-bit version) • Microsoft Windows Server 2022 Standard Edition • Microsoft Windows Server 2022 Datacenter Edition • Microsoft Windows Server Datacenter: Azure Edition • Microsoft Azure Stack HCIv2 version 22H2 • Microsoft Azure Stack Hub (Microsoft Windows Server Core Datacenter) • Microsoft Azure Stack Edge (Microsoft Windows Server Core Datacenter) TOE Builds: • Microsoft Windows 11 build 10.0.22621.1 (also known as version 22H2) • Microsoft Windows 10 build 10.0.19045.2006 (also known as version 22H2) • Microsoft Windows Server 2022 10.0.20348.587 • Microsoft Windows Server Datacenter: Azure Edition build 10.0.20348.1006 • Microsoft Azure Stack HCIv2 version 10.0.20349.1129 • Microsoft Azure Stack Hub and Edge build 10.0.17784.1068 TOE Updates: Windows 11, Windows 10, Windows Server, and Azure Stack: all critical updates as of June 1, 2023

Offer number	74445
Package number	2023-08
Testing procedure	PECS002_03 & PECS018_01
Certification Body	Centro Criptológico Nacional - CCN
Developer	Microsoft Corporation Microsoft Way, Redmond, WA 98052, United States of America
Sponsor	Microsoft Corporration Microsoft Way, Redmond, WA 98052, United States of America
Laboratory	DEKRA Testing and Certification S.A.U Avenida de los Pirineos, 7 Nave 9A 28703, San Sebastián de los Reyes (Madrid)
Author or authors	Santiago Gómez Muñoz - SGM Manuel Mancera Jiménez - MMJ Javier Vázquez Moreno - JVM
Evaluation Level	In conformance with [GPOSPP421]
Laboratory equipment	Nº8287 Nº8185 CTC-1847-W
Security Target	Microsoft Windows, Windows Server and Azure Stack Security Target, version 0.04, July 3, 2023
Report template	FCS210_00 GPOSPP_CC-AAR

2.2 Scope

This document includes the results of the evaluation activities performed by DEKRA Testing and Certification in the Common Criteria evaluation of the following operating systems:

- Microsoft Windows 11 version 22H2 Enterprise edition
- Microsoft Windows 11 version 22H2 Pro edition
- Microsoft Windows 11 version 22H2 Education edition
- Microsoft Windows 11 version 22H2 IoT Enterprise edition
- Microsoft Windows 10 version 22H2 Pro edition
- Microsoft Windows 10 version 22H2 Enterprise edition
- Microsoft Windows Server 2022 Standard edition (With December 13, 2022 cumulative update)
- Microsoft Windows Server 2022 Datacenter edition (With December 13, 2022 cumulative update)
- Microsoft Windows Server Datacenter: Azure Edition (December 2022 virtual machine image from Azure Marketplace)

- Microsoft Azure Stack HCIv2 version 22H2
- Microsoft Azure Stack Hub
- Microsoft Azure Stack Edge

The TOE build tested are the following:

- Microsoft Windows 11 build 10.0.22621.1 (also known as version 22H2)
- Microsoft Windows 10 build 10.0.19045.2006 (also known as version 22H2)
- Microsoft Windows Server 2022 10.0.20348.587
- Microsoft Windows Server Datacenter: Azure Edition build 10.0.20348.1006
- Microsoft Azure Stack HCIv2 version 10.0.20349.1129
- Microsoft Azure Stack Hub and Edge build 10.0.17784.1068

The hardware platforms used during the evaluation are listed below:

- Microsoft Surface Laptop 5
- Microsoft Surface Pro 9
- Microsoft Surface Pro 9 5G (Qualcomm)
- Surface Studio 2+
- Microsoft Surface Laptop Go 2
- Microsoft Surface Go 3
- Microsoft Surface Laptop Studio
- Microsoft Surface Laptop 4 (AMD)
- Microsoft Surface Laptop 4 (Intel)
- Dell Latitude 7420
- Dell Latitude 9520
- HP EliteBook 840 G10
- Lenovo ThinkPad Z13 (AMD)
- Panasonic CF-33
- Panasonic FZ-55 Toughbook
- Zebra L10ax / RTL 10C1
- Zebra ET80Z Tablet
- Microsoft Windows Server 2022 Hyper-V
- Microsoft Windows Server 2019 Hyper-V
- Dell PowerEdge R640
- Dell PowerEdge R6625
- Dell PowerEdge R760xp
- Dell PowerEdge R840
- HPE Edgeline EL8000 / ProLiant e910 Server Blade
- Voyager Klaas Telecom

Note: For the sake of a better readability the following platforms:

- Microsoft Windows Server 2019 Hyper-V
- Microsoft Windows Server 2022 Hyper-V

has been referenced to:

- Microsoft Windows Hyper-V Server 2019
- Microsoft Windows Hyper-V Server 2022

This naming convention has been used hereinafter.

The [SERIES] methodology has been applied for this evaluation, the Reference TOEs have been selected according to the information included in section **6. Selection of the References TOEs** of [DAR&TRR] document.

The following list summarizes the combination between hardware platforms and operating system editions used for the testing:

- **Reference TOEs:**
  - Microsoft Surface Laptop 5 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
  - Microsoft Surface Pro 9 with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
  - Dell PowerEdge R6625 with Windows Server 2022 Datacenter edition (21H2, build 10.0.20348.587)
  - Microsoft Windows Server 2022 Hyper-V with Windows Server Azure Datacenter edition (21H2, build 10.0.20348.1006)
  - Dell PowerEdge R6625 with Windows Server Datacenter edition (21H2, build 10.0.20348.1006)
  - Dell PowerEdge R6625 with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
  - Dell PowerEdge R6625 with Azure Stack Hub (build 10.0.17784.1068)
  - Dell PowerEdge R6625 with Azure Stack Edge (build 10.0.17784.1068)
- **Supplementary TOEs:**
  - Panasonic CF-33 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
  - Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
  - Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
  - Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
  - Dell PowerEdge R640 with Windows Server 2022 Standard edition (21H2, build 10.0.20348.587)
  - Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
  - Dell PowerEdge R840 with Azure Stack Edge (build 10.0.17784.1068)
  - HPE Edgeline EL8000 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
  - Voyager Klaas Telecom with Azure Stack Hub (build 10.0.17784.1068)
  - Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)

- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (21H2, build 10.0.20348.587
- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)

As described in section **7. Testing Reuse Rational (TRR)** of [DAR&TRR], the following testing strategy has been followed:

- The reference TOEs cover all the build versions (at least one platform per each build has been selected).
- The reference TOEs cover the most complete edition (Enterprise and Datacenter editions have been selected).

As it is concluded in the DAR analysis included in section **5. Differential analysis report (DAR)** of [DAR&TRR] document, the security functionalities offered by the TOE and intended to be evaluated are the same independently of the type of edition.

Therefore, and due to this selecion, it can be guarantee that the testing results obtained for the reference TOEs can be resued for the rest of the additional platforms.

As to the hardware platform where the TOE is installed, for most of the evaluated functionalities (e.g. security audit, access control rules) it is not relevant. Hence, this implies it is not expected to have different results between different hardware platforms.

However, there are some requirements in which the architecture of the hardware components used may be relevant (for instance, memory randomization requirement or binaries compiled with buffer overflow protection). Due to this, additional platforms will be used to expand the testing coverage and provide and individual analysis of the obtained results (it is detailed in this documnt when applicable)

The following information is included for each SFR:

1. Description of the assurance activity, considering any modification issued by NIAP Technical Decisions.
2. Documentation review activity for both TSS and guidance including the corresponding verdict if applicable.
3. Testing activity. Composed of setup, procedure for its execution, obtained results (expected results are specified in the assurance activity description) and verdict. All this information is provided for all test cases.

3 Samples Identification

Since the TOE is an operating system, which is purely software, there is no physical samples identified and tracked into the DEKRA internal system.

Control number	Description	Model	Serial Number	Reception date
NA	NA	NA	NA	NA

4 Evaluation basis

The basis for this evaluation effort is as follows:

CC Version	Common Criteria for Information Technology Security Evaluation. Version: 3.1 Release 5 Date: April 2017 Part 1: Introduction and general model CC ref: CCMB-2017-04-001 Part 2: Security functional requirements CC ref: CCMB-2017-04-002 Part3: Security assurance requirements CC ref: CCMB-2017-04-003
Methodology version	Common Criteria for Information Technology Security Evaluation. Version: 3.1 Release 5 Date: April 2017 CC ref: CCMB-2017-04-004
Evaluation level	In conformance with [GPOSPP421]
Protection profile	NIAP - Protection Profile for General Purpose Operating Systems, Version: 4.2.1, April 22, 2019 and NIAP Technical Decisions (TDs). NIAP - PP Module for Wireless Local Area Network (WLAN) Clients, Version 1.0, March 31, 2022. NIAP - PP Module for Virtual Private Network (VPN) Clients, Version 2.4, March 31, 2022 NIAP - PP Module for Bluetooth Version 1.0, April 15, 2023
CCRA Supporting documents	None
JIL interpretations	[JIL10] Joint Interpretation Library. Evaluation methodology for product series Version 1.0. April 2017
Additional interpretations	None
Other regulations	None

5 References

[CC31p1] Common Criteria for Information Technology Security Evaluation.
Part 1: Introduction and general model.
Version 3.1, Revision 5

[CC31p2] Common Criteria for Information Technology Security Evaluation.
Part 2: Security Functional Components.
Version 3.1, Revision 5

[CC31p3] Common Criteria for Information Technology Security Evaluation.
Part 3: Security Assurance Components.
Version 3.1, Revision 5

[CEM31] Common Criteria for Information Technology Security Evaluation.
Evaluation Methodology.
Version 3.1, Revision 5

[SERIES] Evaluation methodology for product series, version 1.0, April 2017

[MS-W11-22H2-I-000] Evidences list

[GPOSPP421] NIAP - Protection Profile for General Purpose Operating Systems, Versions: 4.2.1, April 22, 2019 [GPOSPP421] and NIAP Technical Decisions (TDs)

[GPOSPP-VR10] National Information Assurance Partnership Common Criteria Evaluation and Validation Scheme (CCEVS-VR-PP-0047), 01 May 2019 Version 1.0

[GPOSPP42-ANER] Extended Component Definitions for GPOSPP v.4.2

[PPMWLAN10] NIAP - General Purpose Operating Systems Protection Profile/Mobile Device Fundamentals Protection Profile Extended Package Wireless Local Area Network (WLAN) Clients, Version 1.0, February 08, 2016

[PPMWLAN10-VR10] National Information Assurance Partnership Common Criteria Evaluation and validation Scheme (CCEVS-VR-PP-0036), 17 August 2017 Version 1.0.

[PPMVPN24] NIAP - PP Module for Virtual Private Network (VPN) Clients, Version 2.4, March 31, 2022

[PPMVPN24SD] Supporting Document Mandatory Technical Document PP-Module for Virtual Private Network (VPN) Clients, Version 2.4, March 31, 2022

[VPN-PPCONF13] PP-Configuration for General Purpose Operating Systems and Virtual Private Network (VPN) Clients, March 21, 2022, version 1.3

[PPMBT10]	NIAP - PP Module for Bluetooth, Version 1.0, April 15, 2021
[PPMBT10SD]	Supporting Document Mandatory Technical Document PP-Module for Bluetooth, Version 1.0, April 15, 2021
[PECS002_03]	Procedimiento de Proteccion
[PECS018_01]	Procedimiento de Evaluacion Common Criteria

The evaluation evidences are listed in section **108 Evidence List**.

6 Competences, guarantees and general conditions

DEKRA Testing and Certification S.A.U. is a testing laboratory accredited by the National Accreditation Body (ENAC - Entidad Nacional de Acreditación), to perform the tests indicated in the Certificate No. 51/LE 1399.

In order to assure the traceability to other national and international laboratories, DEKRA Testing and Certification S.A.U. has a calibration and maintenance program for its measurement equipment.

DEKRA Testing and Certification S.A.U. guarantees the reliability of the data presented in this report, which is the result of the measurements and the tests performed to the item under test on the date and under the conditions stated on the report and, it is based on the knowledge and technical facilities available at DEKRA Testing and Certification at the time of performance of the test.

DEKRA Testing and Certification S.A.U. is liable to the client for the maintenance of the confidentiality of all information related to the item under test and the results of the test.

The results presented in this Test Report apply only to the particular item under test established in this document.

IMPORTANT: No parts of this report may be reproduced or quoted out of context, in any form or by any means, except in full, without the previous written permission of DEKRA Testing and Certification S.A.U.

1) This report is only referred to the item that has undergone the test.
2) This report does not constitute or imply on its own an approval of the product by the Certification Bodies or competent Authorities.
3) This document is only valid if complete; no partial reproduction can be made without previous written permission of DEKRA Testing and Certification S.A.U.
4) This test report cannot be used partially or in full for publicity and/or promotional purposes without previous written permission of DEKRA Testing and Certification S.A.U. and the Accreditation Bodies.

7 TOE Configuration

The operational guidance [OPE_230714] gives proper steps to carry out the installation and configuration of the TOE and its environment that is consistent with [ST004].

The evaluator has installed and configured the TOE and its environment according to the [OPE_230714] documentation.

The TOE configuration is consistent with the information provided in the security target [ST004].

Therefore, the TOE configuration used to execute the independent test plan is consistent with the evaluated configuration according to the security target [ST004].

8 Test environment definition

8.1 Evaluation approach

The evaluation approach performed is as follows:

- Canonical platforms: Canonical platforms are the reference TOEs. They were selected by applying the following criteria: One canonical platform will be set for each build version of the TOEs (i.e 10.0.22621.1, 10.0.19045.2006 , 10.0.20348.587, 10.0.20348.1006...) and it covers the most complete edition (Enterprise and Datacenter editions have been selected). Therefore, eight canonical platforms were configured. The complete testing coverage was performed over these platforms. The selected canonical platforms were the following:
  - Microsoft Surface Laptop 5 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
  - Microsoft Surface Pro 9 with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
  - Dell PowerEdge R6625 with Windows Server 2022 Datacenter edition (21H2, build 10.0.20348.587)
  - Microsoft Windows Server 2022 Hyper-V with Windows Server Azure Datacenter edition (21H2, build 10.0.20348.1006)
  - Dell PowerEdge R6625 with Windows Server Datacenter edition (21H2, build 10.0.20348.1006)
  - Dell PowerEdge R6625 with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
  - Dell PowerEdge R6625 with Azure Stack Hub (build 10.0.17784.1068)
  - Dell PowerEdge R6625 with Azure Stack Edge (build 10.0.17784.1068)
- Supplementary platforms: These supplementary platforms had been tested to expand the testing coverage of the previous platforms.
  - Panasonic CF-33 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
  - Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
  - Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
  - Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
  - Dell PowerEdge R640 with Windows Server 2022 Standard edition (21H2, build 10.0.20348.587)
  - Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
  - Dell PowerEdge R840 with Azure Stack Edge (build 10.0.17784.1068)
  - HPE Edgeline EL8000 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
  - Voyager Klaas Telecom with Azure Stack Hub (build 10.0.17784.1068)

- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (21H2, build 10.0.20348.587
- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)

8.1.1 Testing strategy

Not all the activities included in this report have been carried out at DEKRA Testing and Certification laboratory facilities. Some of the tests included in this report have been performed at the vendor facilities, since access to internal tools and private debug symbols are required.

The following SFRs have been tested by the evaluator at the vendor premises: FCS_CKM_EXT.4, FCS_RBG_EXT.1, FIA_UAU.5 (smart card authentication), FPT_ASLR_EXT.1, FPT_SBOP_EXT.1 and FPT_TST_EXT.1.

The on-site testing has allowed the access to critical parts of the source code, access to debugging capabilities and to vendor certificates and propietary test tools for the functional testing of the above mentioned SFRs. These capabilities could only be available for the evaluator on the vendor's premises.

The canonical platforms were fully tested, therefore, the evaluator had a complete coverage for each version of the TOE.

A sampling strategy was used for the supplementary platforms to gain confidence about the results obtained for the canonical platforms and to widen the testing coverage.

As detailed in the above section, the selection of the reference TOEs meets the following criteria:

- The reference TOEs cover all the build versions (at least one platform per each build has been selected).
- The reference TOEs cover the most complete edition (Enterprise and Datacenter editions have been selected).

The security functionalities offered by the TOE and intended to be evaluated are the same independently of the type of edition.

Therefore, and due to this selection, it can be guarantee that the testing results obtained for the reference TOEs can be reused for the rest of the additional platforms.

As to the hardware platform where the TOE is installed, for most of the evaluated functionalities (e.g. security audit, access control rules), the hardware platform in which the TOE was installed was not relevant. Hence, this implies that it is not expected to have different results between different hardware platforms.

However, there are some requirements in which the architecture or the hardware components used may be relevant (for instance memory randomization requirement or binaries compiled with buffer overflow protection). Due to this, additional platforms will be used to expand the testing coverage and provides an individual analysis of obtained results.

Summarizing, the testing strategy followed was:

- Canonical platforms: Complete testing.
- Supplementary platforms: Complete testing for hardware-relevant requirements and sampling for the rest of requirements.

Using the above approach, the testing had a complete coverage since at least one platform was completely tested for each combination of operating system edition and all the hardware-relevant requirements were tested in all platforms.

> NOTE: WLAN Extended package is not applicable for Windows Server/Azure operating system editions.

9 FAU_GEN.1.1

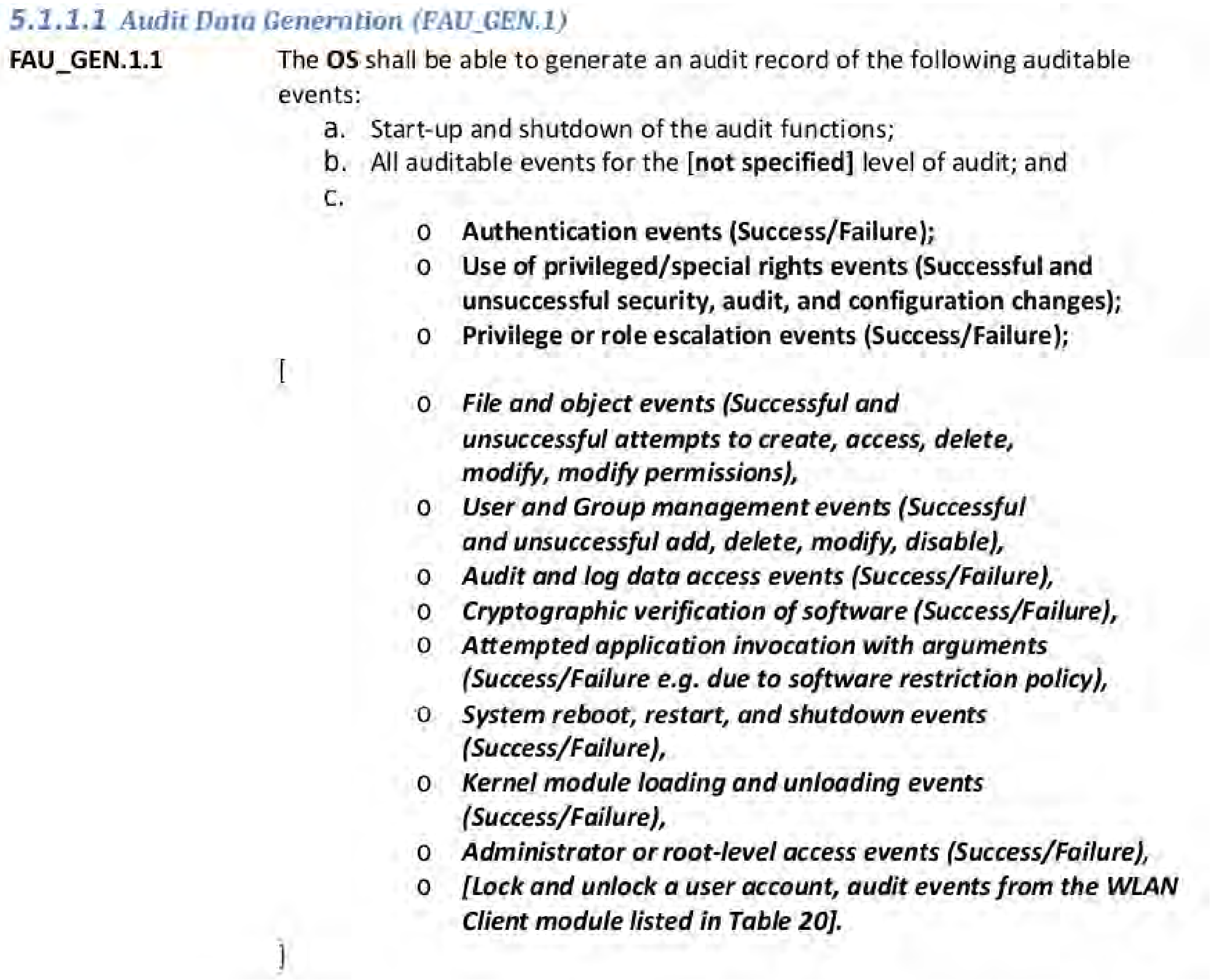
The assurance activity for the **FAU_GEN.1.1** requirement is stated as follows:

> The evaluator will check the administrative guide and ensure that it lists all of the auditable events. The evaluator will check to make sure that every audit event type selected in the ST is included.
>
> The evaluator will test the OS's ability to correctly generate audit records by having the TOE generate audit records for the events listed in the ST. This should include all instance types of an event specified. When verifying the test results, the evaluator will ensure the audit records generated during testing match the format specified in the administrative guide, and that the fields in each audit record have the proper entries.

9.1 Documentation Review Activity

9.1.1 Findings

The ***Security Target*** document, defines in its section **5.1.1.1 Audit Data Generation(FAU_GEN.1)**, the following auditable events:



5.1.1.1 *Audit Data Generation (FAU_GEN.1)*

FAU_GEN.1.1 The **OS** shall be able to generate an audit record of the following auditable events:

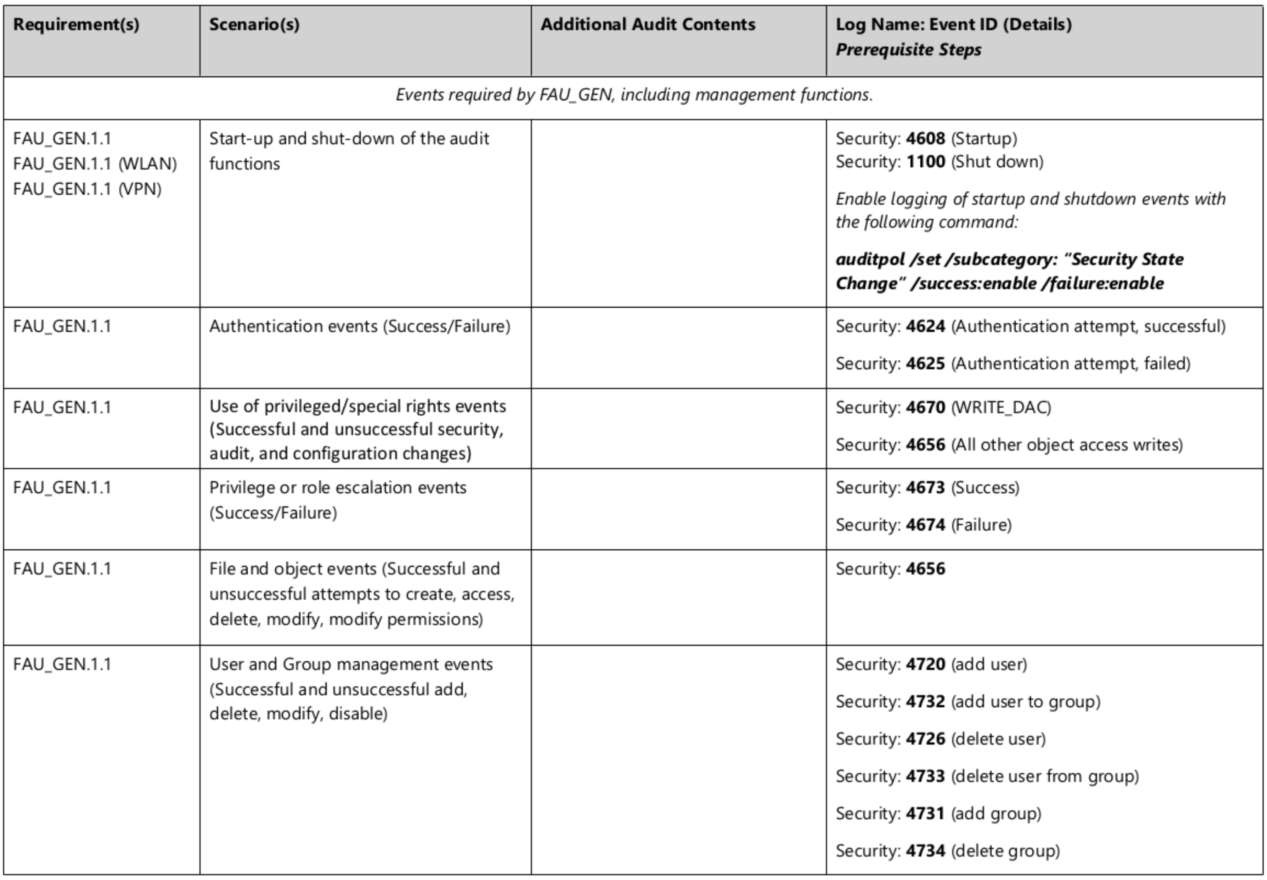
a. Start-up and shutdown of the audit functions;
b. All auditable events for the [**not specified**] level of audit; and
c.
- **Authentication events (Success/Failure);**
- **Use of privileged/special rights events (Successful and unsuccessful security, audit, and configuration changes);**
- **Privilege or role escalation events (Success/Failure);**

[

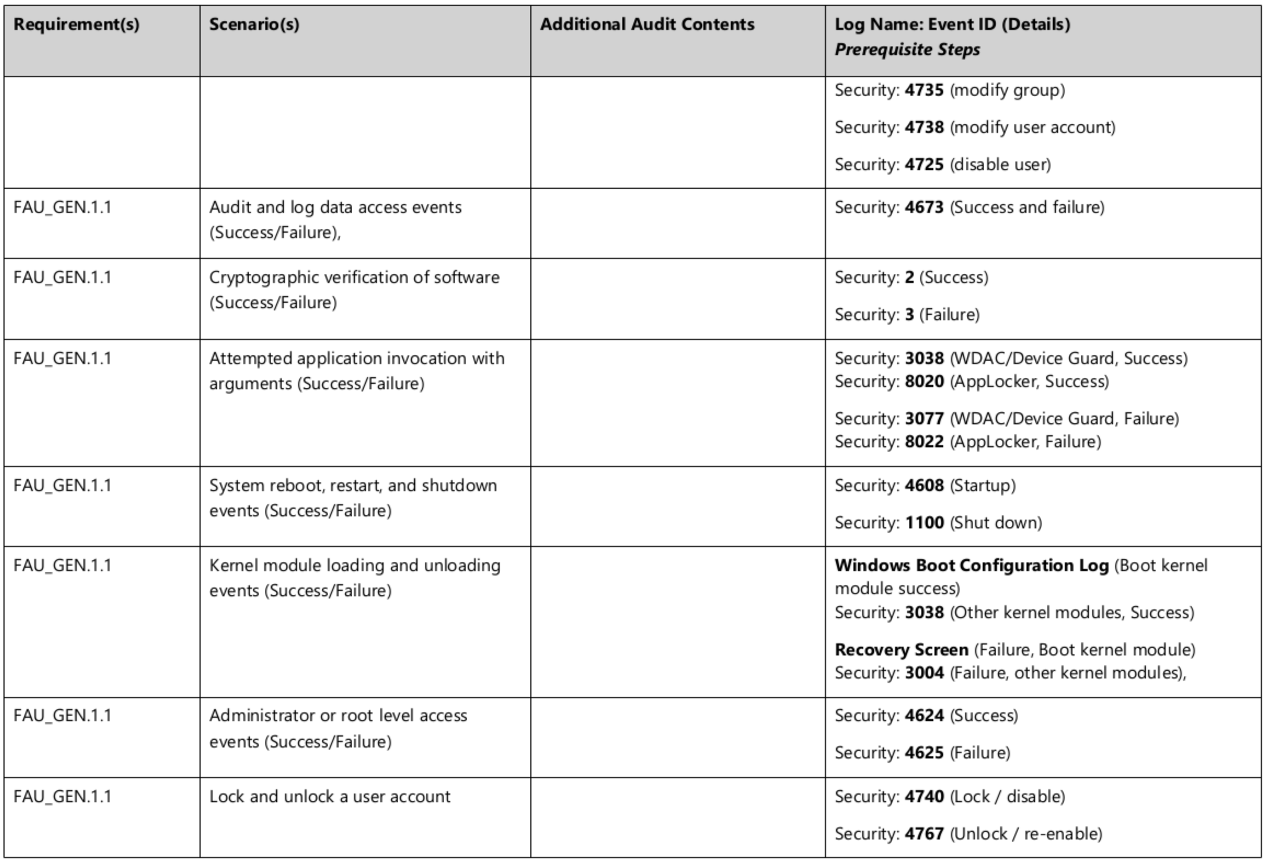
- ***File and object events (Successful and unsuccessful attempts to create, access, delete, modify, modify permissions),***
- ***User and Group management events (Successful and unsuccessful add, delete, modify, disable),***
- ***Audit and log data access events (Success/Failure),***
- ***Cryptographic verification of software (Success/Failure),***
- ***Attempted application invocation with arguments (Success/Failure e.g. due to software restriction policy),***
- ***System reboot, restart, and shutdown events (Success/Failure),***
- ***Kernel module loading and unloading events (Success/Failure),***
- ***Administrator or root-level access events (Success/Failure),***
- ***[Lock and unlock a user account, audit events from the WLAN Client module listed in Table 20].***

]

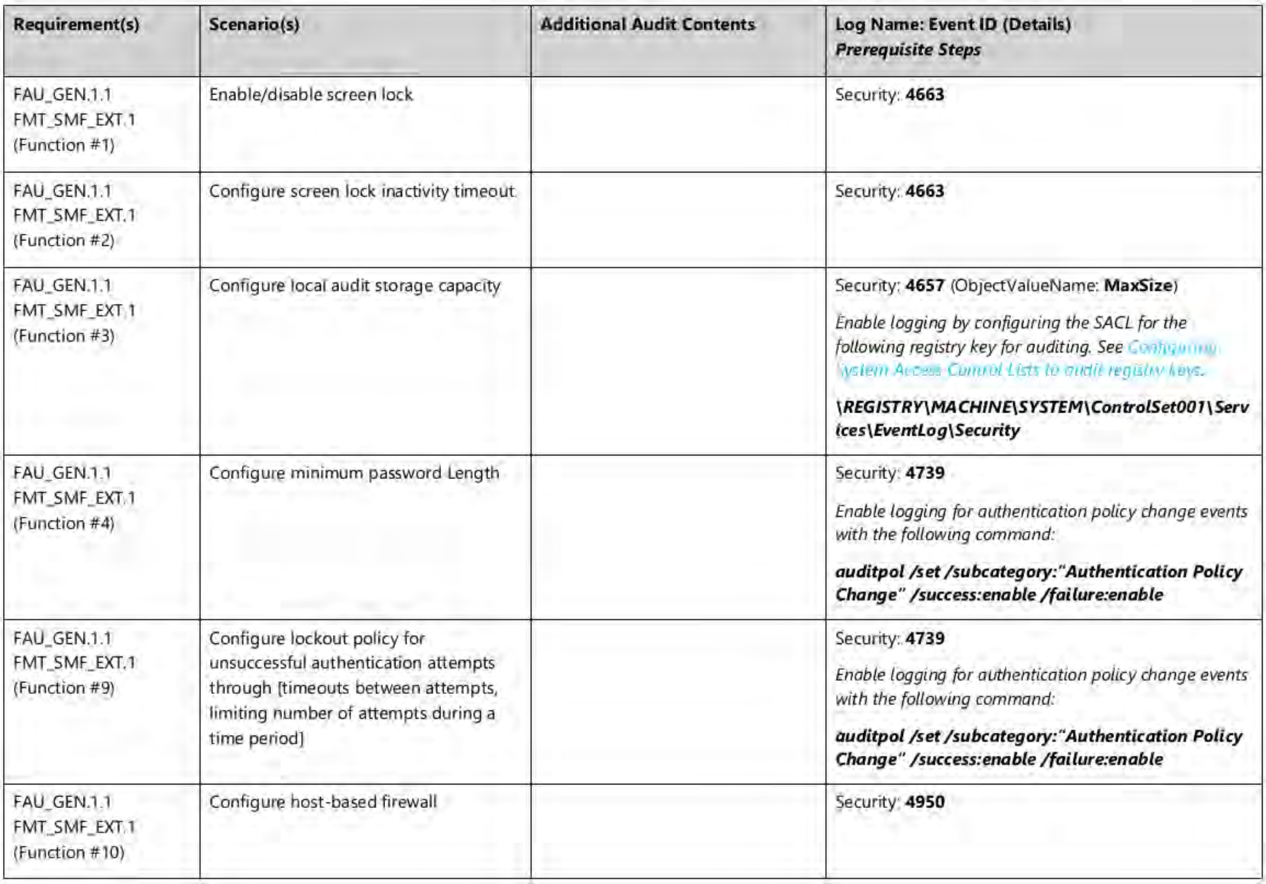
In addition, the ***Operational Guidance*** document, includes in its section **5.1 Audit Events by scenario** a table with all the auditable events generated by the TOE.



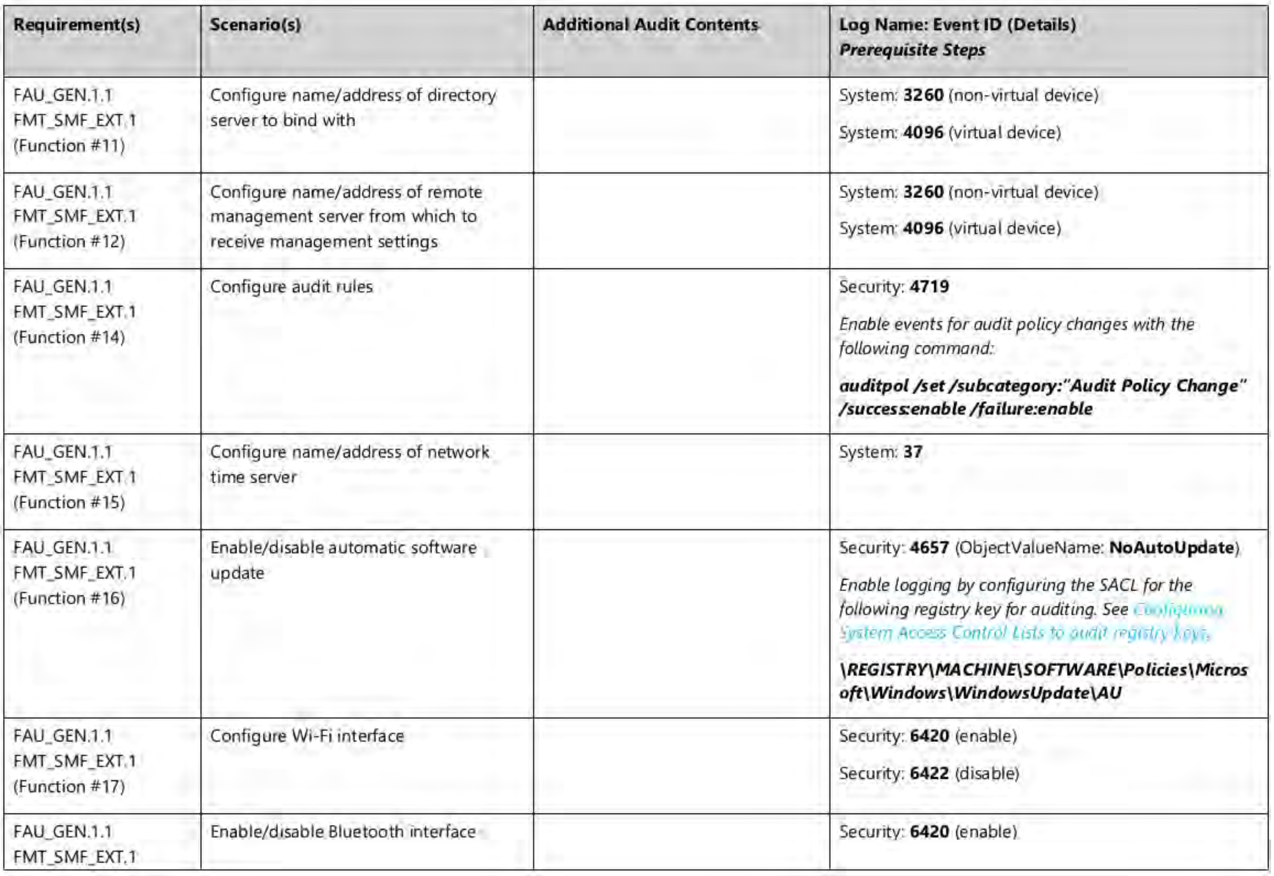
Requirement(s)	**Scenario(s)**	**Additional Audit Contents**	**Log Name: Event ID (Details)** ***Prerequisite Steps***
Events required by FAU_GEN, including management functions.			
FAU_GEN.1.1 FAU_GEN.1.1 (WLAN) FAU_GEN.1.1 (VPN)	Start-up and shut-down of the audit functions		Security: **4608** (Startup) Security: **1100** (Shut down) *Enable logging of startup and shutdown events with the following command:* ***auditpol /set /subcategory: "Security State Change" /success:enable /failure:enable***
FAU_GEN.1.1	Authentication events (Success/Failure)		Security: **4624** (Authentication attempt, successful) Security: **4625** (Authentication attempt, failed)
FAU_GEN.1.1	Use of privileged/special rights events (Successful and unsuccessful security, audit, and configuration changes)		Security: **4670** (WRITE_DAC) Security: **4656** (All other object access writes)
FAU_GEN.1.1	Privilege or role escalation events (Success/Failure)		Security: **4673** (Success) Security: **4674** (Failure)
FAU_GEN.1.1	File and object events (Successful and unsuccessful attempts to create, access, delete, modify, modify permissions)		Security: **4656**
FAU_GEN.1.1	User and Group management events (Successful and unsuccessful add, delete, modify, disable)		Security: **4720** (add user) Security: **4732** (add user to group) Security: **4726** (delete user) Security: **4733** (delete user from group) Security: **4731** (add group) Security: **4734** (delete group)



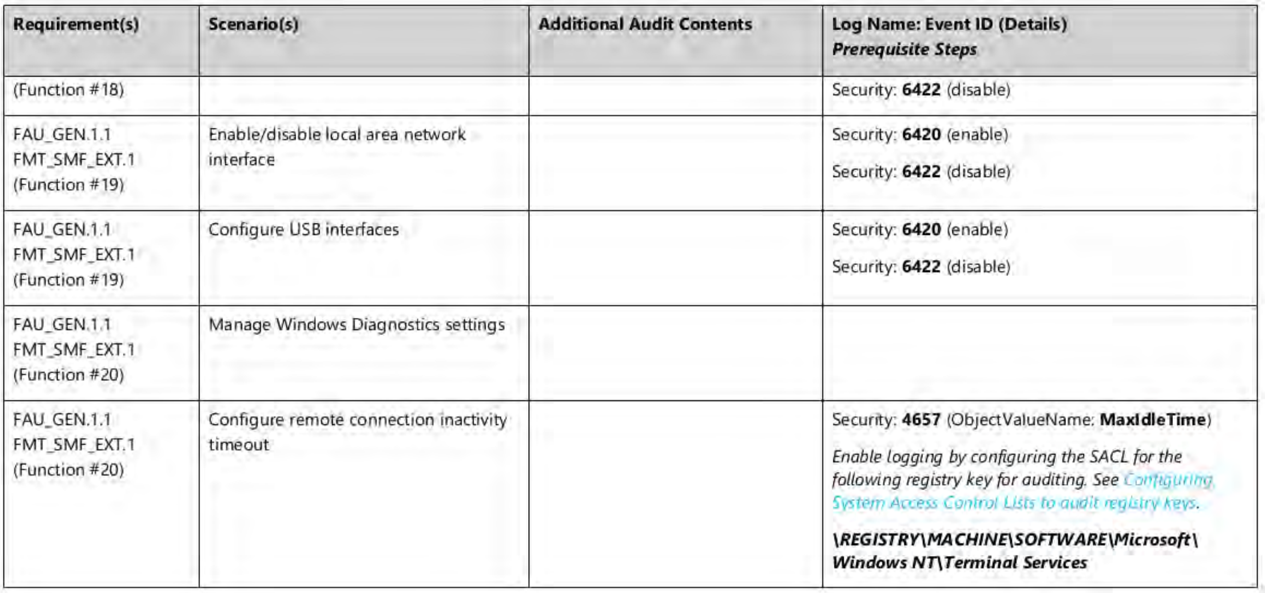
Requirement(s)	**Scenario(s)**	**Additional Audit Contents**	**Log Name: Event ID (Details)** ***Prerequisite Steps***
			Security: **4735** (modify group) Security: **4738** (modify user account) Security: **4725** (disable user)
FAU_GEN.1.1	Audit and log data access events (Success/Failure),		Security: **4673** (Success and failure)
FAU_GEN.1.1	Cryptographic verification of software (Success/Failure)		Security: **2** (Success) Security: **3** (Failure)
FAU_GEN.1.1	Attempted application invocation with arguments (Success/Failure)		Security: **3038** (WDAC/Device Guard, Success) Security: **8020** (AppLocker, Success) Security: **3077** (WDAC/Device Guard, Failure) Security: **8022** (AppLocker, Failure)
FAU_GEN.1.1	System reboot, restart, and shutdown events (Success/Failure)		Security: **4608** (Startup) Security: **1100** (Shut down)
FAU_GEN.1.1	Kernel module loading and unloading events (Success/Failure)		**Windows Boot Configuration Log** (Boot kernel module success) Security: **3038** (Other kernel modules, Success) **Recovery Screen** (Failure, Boot kernel module) Security: **3004** (Failure, other kernel modules),
FAU_GEN.1.1	Administrator or root level access events (Success/Failure)		Security: **4624** (Success) Security: **4625** (Failure)
FAU_GEN.1.1	Lock and unlock a user account		Security: **4740** (Lock / disable) Security: **4767** (Unlock / re-enable)



Requirement(s)	**Scenario(s)**	**Additional Audit Contents**	**Log Name: Event ID (Details)** ***Prerequisite Steps***
FAU_GEN.1.1 FMT_SMF_EXT.1 (Function #1)	Enable/disable screen lock		Security: **4663**
FAU_GEN.1.1 FMT_SMF_EXT.1 (Function #2)	Configure screen lock inactivity timeout		Security: **4663**
FAU_GEN.1.1 FMT_SMF_EXT.1 (Function #3)	Configure local audit storage capacity		Security: **4657** (ObjectValueName: **MaxSize**) *Enable logging by configuring the SACL for the following registry key for auditing. See Configuring System Access Control Lists to audit registry keys.* ***\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\EventLog\Security***
FAU_GEN.1.1 FMT_SMF_EXT.1 (Function #4)	Configure minimum password Length		Security: **4739** *Enable logging for authentication policy change events with the following command:* ***auditpol /set /subcategory:"Authentication Policy Change" /success:enable /failure:enable***
FAU_GEN.1.1 FMT_SMF_EXT.1 (Function #9)	Configure lockout policy for unsuccessful authentication attempts through [timeouts between attempts, limiting number of attempts during a time period]		Security: **4739** *Enable logging for authentication policy change events with the following command:* ***auditpol /set /subcategory:"Authentication Policy Change" /success:enable /failure:enable***
FAU_GEN.1.1 FMT_SMF_EXT.1 (Function #10)	Configure host-based firewall		Security: **4950**



Requirement(s)	Scenario(s)	Additional Audit Contents	Log Name: Event ID (Details) ***Prerequisite Steps***
FAU_GEN.1.1 FMT_SMF_EXT.1 (Function #11)	Configure name/address of directory server to bind with		System: **3260** (non-virtual device) System: **4096** (virtual device)
FAU_GEN.1.1 FMT_SMF_EXT.1 (Function #12)	Configure name/address of remote management server from which to receive management settings		System: **3260** (non-virtual device) System: **4096** (virtual device)
FAU_GEN.1.1 FMT_SMF_EXT.1 (Function #14)	Configure audit rules		Security: **4719** *Enable events for audit policy changes with the following command:* ***auditpol /set /subcategory:"Audit Policy Change" /success:enable /failure:enable***
FAU_GEN.1.1 FMT_SMF_EXT.1 (Function #15)	Configure name/address of network time server		System: **37**
FAU_GEN.1.1 FMT_SMF_EXT.1 (Function #16)	Enable/disable automatic software update		Security: **4657** (ObjectValueName: **NoAutoUpdate**) *Enable logging by configuring the SACL for the following registry key for auditing. See Configuring System Access Control Lists to audit registry keys.* ***\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU***
FAU_GEN.1.1 FMT_SMF_EXT.1 (Function #17)	Configure Wi-Fi interface		Security: **6420** (enable) Security: **6422** (disable)
FAU_GEN.1.1 FMT_SMF_EXT.1	Enable/disable Bluetooth interface		Security: **6420** (enable)



Requirement(s)	Scenario(s)	Additional Audit Contents	Log Name: Event ID (Details) ***Prerequisite Steps***
(Function #18)			Security: **6422** (disable)
FAU_GEN.1.1 FMT_SMF_EXT.1 (Function #19)	Enable/disable local area network interface		Security: **6420** (enable) Security: **6422** (disable)
FAU_GEN.1.1 FMT_SMF_EXT.1 (Function #19)	Configure USB interfaces		Security: **6420** (enable) Security: **6422** (disable)
FAU_GEN.1.1 FMT_SMF_EXT.1 (Function #20)	Manage Windows Diagnostics settings		
FAU_GEN.1.1 FMT_SMF_EXT.1 (Function #20)	Configure remote connection inactivity timeout		Security: **4657** (ObjectValueName: **MaxIdleTime**) *Enable logging by configuring the SACL for the following registry key for auditing. See Configuring System Access Control Lists to audit registry keys.* ***\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\Terminal Services***

The content of this table matches with the selection performed by the vendor in the ***Security Target*** document, as it can be seen in the image above.

9.1.2 Verdict

The evaluator has reviewed the ***Security Target*** document and has ensured that every auditable event type selected in the ***Security Target*** document is included in the ***Operational Guidance*** document.

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfilment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to this activity.

9.2 Test Activity

There are quite a few auditable events. To make a better coverage, the evaluator has divided this test activity into different subtests. For each of these subtests, the evaluator has developed a script to obtain the selected audit events.

The auditable events defined in the ***Security Target*** document are the following, including the *eventID* defined in the ***Operational Guidance*** document:

1. Start-up and shutdown of the audit functions (4608, 1100)
2. Authentication events (4624, 4625)
3. Use of privileged/special rights events (4656, 4670)
4. Privilege or role escalation events (4673, 4674)
5. File and object events (4656)
6. User and Group management events (4720, 4725, 4726, 4731, 4732, 4733, 4734, 4735, 4738)
7. Audit and log data access events (4673)
8. Cryptographic verification of software (2, 3)
9. Attempted application invocation with arguments (3077, 3038, 8020, 8022)
10. System reboot, restart and shutdown events (1100, 4608)
11. Kernel module loading and unloading events (3004, 3038)
12. Administrator or root-level access events (4624, 4625)
13. Lock and unlock a user account (4740,4767)
14. Audit events from the WLAN Client EP (**covered in FAU_GEN.1/WLAN requirement**)

The table below, shows the coverage between the auditable events and the subtests division performed by the evaluator. All the auditable events selected in the ***Security Target*** document are covered:

9.2.1 Test 1 - Startup, Shutdown and Authentication events

The correct generation of the startup and shutdown of the audit functions, system reboot, restart and shutdown, authentication and administrator access events will be tested in this test case.

Scripts/Events	1	2	3	4	5	6	7	8	9	10	11	12	13
Test 1 - Startup, shutdown and authentication events	✓	✓								✓		✓	
Test 2 - Privileges or role escalation and audit and log data access events				✓			✓						
Test 3 - User and Group management events						✓							
Test 4 - Use of privileged rights and File and object events			✓		✓								
Test 5 - Cryptographic verification of software events								✓					
Test 6 - Attempted application invocation events									✓				
Test 7 - Kernel module loading events											✓		
Test 8 - Lock and unlock a user account													✓

9.2.1.1 Setup

Before the test execution, the following setup condition must be fulfilled:

- A user account with administrator rights shall exist.
- The *PowerShell* execution policy shall be configured to allow the execution of *PowerShell* scripts. To do it, execute in a *Powershell* terminal with administrator rights the command:

```
Set-ExecutionPolicy Unrestricted -Force
```

- Scripts *Test1_Setup.ps1* and *Test1_Startup&Shutdown&Logon.ps1* shall be available.

9.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

9.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R840 with Azure Stack Edge (build 10.0.17784.1068)

- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

9.2.1.4 Verdict

As the result above states, the audit events related to the startup and shutdown of the audit functions, system events like reboot, restart and shutdown and successful and failed authentication events have been correctly generated and they include all the information defined in the ***Security Target*** document.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

9.2.2 Test 2 - Privileges or role escalation and audit and log data access events

Generation of audit and log data access and privileges elevation events will be tested in this test case.

9.2.2.1 Setup

The applicable setup for this test is the same as the one defined in the previous test case.

9.2.2.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

9.2.2.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R840 with Azure Stack Edge (build 10.0.17784.1068)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

9.2.2.4 Verdict

As the result above states, the audit events related to the privileged events and audit data access events have been correctly generated and they include all the information defined in the ***Security Target*** document.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 2** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 2.**

9.2.3 Test 3 - User and group management events

Generation of user and group management audit events will be tested in this test case.

9.2.3.1 Setup

Before the test execution, the following setup conditions must be fulfilled:

- A user account with user name *userFAU* shall not exist.
- A local group with name *groupFAU* shall not exist.
- The *PowerShell* execution policy shall be configured to allow the execution of *PowerShell* scripts. To do it, execute in a *Powershell* terminal with administrator rights the command:

  ```
  Set-ExecutionPolicy Unrestricted -Force
  ```

- Script *Test3_Users&Groups.ps1* shall be available.

9.2.3.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

9.2.3.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R840 with Azure Stack Edge (build 10.0.17784.1068)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE’s behavior is as expected and detailed in the security target [ST004].

9.2.3.4 Verdict

As the result above states, the audit events related to user and group management events have been correctly generated and they include all the information defined in the ***Security Target*** document.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 3** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 3.**

9.2.4 Test 4 - Use of privileged rights and file and object events

Generation of privileged rights and file and object audit events will be tested in this test case.

9.2.4.1 Setup

Before the test execution, the following setup conditions must be fulfilled:

- A user account with user name *userFAU* shall exist. This user shall belong to the default *Users* group.
- A file in path *C:\TEMP\file.txt* shall not exist.
- The *PowerShell* execution policy shall be configured to allow the execution of *PowerShell* scripts. To do it, execute in a *Powershell* terminal with administrator rights the command:

  ```
  Set-ExecutionPolicy Unrestricted -Force
  ```

- Script *Test4_Fileobject&AdminRoot.ps1* shall be available.

9.2.4.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

9.2.4.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)

- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R840 with Azure Stack Edge (build 10.0.17784.1068)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

9.2.4.4 Verdict

As the result above states, the audit events related to file and object events have been correctly generated and they include all the information defined in the ***Security Target*** document.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 4** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 4.**

9.2.5 Test 5 - Cryptographic verification of software events

Generation of audit events related to cryptographic verification of software will be tested in this test case.

9.2.5.1 Setup

Before the test execution, the following setup conditions must be fulfilled:

- *SignTool*, a command line tool that provides the ability to sign files and verify signatures in files. It is distributed with the *Windows 10 Software Development Kit (SDK)*.
- A hexadecimal editor (e.g. *HxD*).
- A valid update file must be downloaded in the tested platform. To do this, the evaluator shall carry out the following steps:
  - Open *Microsoft Edge* and go to the following URL: Windows Update Catalog
- In the search box type *'Windows 10 22H2'*, *'Windows 11 22H2'*, *'Windows Server 21H2'*, *'Azure Stack HCI'*, *'Azure Stack Hub'* and *'Azure Stack Edge'* a list of available updates will be shown.
  - Choose one update from the list, and ensure that the selected update is valid to the architecture of the platform which is being tested.
- Finally, click the *Download* button. Choose the folder where the update will be stored and wait until the download has finished. The downloaded file shall have the *.msu* extension (*Microsoft Update Standalone Package*).
- The *PowerShell* execution policy shall be configured to allow the execution of *PowerShell* scripts. To do it, execute in a *Powershell* terminal with administrator rights the command:

  ```
  Set-ExecutionPolicy Unrestricted -Force
  ```
- Scripts *Test5_Setup.ps1* and *Test5_CryptographicVerificationEvents.ps1* shall be available.

9.2.5.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

9.2.5.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)

- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R840 with Azure Stack Edge (build 10.0.17784.1068)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE’s behavior is as expected and detailed in the security target [ST004].

9.2.5.4 Verdict

As the result above states, the audit events related to the cryptographic verification of software have been correctly generated and they include all the information defined in the ***Security Target*** document.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 5** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 5.**

9.2.6 Test 6 - Program initiation events

Generation of audit events related to the success or failure initiation programs due to software restriction policies will be tested in this test case.

9.2.6.1 Setup

The applicable setup is different depending on the operating system and the edition installed in the evaluated platform.

The evaluator shall configure *Applocker*. The following conditions must be fulfilled to perform this part of the test:

- The *PowerShell* execution policy shall be configured to allow the execution of *PowerShell* scripts. To do it, execute in a *Powershell* terminal with administrator rights the command:

  ```
  Set-ExecutionPolicy Unrestricted -Force
  ```

- *Application Identity Service* must be running. The evaluator has developed a script to automate the start of the service and set it to start on Windows boot. The content of the script is the following:
- *AppLocker* shall not have any defined rules in section *Packaged app Rules*.
- For Windows Server, *TestConsolev10.exe* and *TestConsolev11.exe* and *Test6_ProgramInitiationEvents_AppLocker_GetLog_Server.ps1* shall be available.
- Scripts *Test6_ProgramInitiationEvents_AppLocker_Setup.ps1* and *Test6_Program InitiationEvents_AppLocker_GetLog.ps1* shall be available.

9.2.6.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

9.2.6.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)

- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R840 with Azure Stack Edge (build 10.0.17784.1068)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

9.2.6.4 Verdict

As the result above states, the audit events related to the program initiation events have been correctly generated and they include all the information defined in the ***Security Target*** document.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 6** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 6.**

9.2.7 Test 7 - Kernel module loading events

Generation of kernel module loading events will be tested in this test case.

9.2.7.1 Setup

Before the test execution, the following setup conditions must be fulfilled:

- A hexadecimal editor (e.g. *HxD*)
- A *WinPE* USB for all the architectures must be available.
- The *PowerShell* execution policy shall be configured to allow the execution of *PowerShell* scripts. To do it, execute in a *Powershell* terminal with administrator rights the command:

  ```
  Set-ExecutionPolicy Unrestricted -Force
  ```

- Scripts *Test7_KernelModuleLoading events_Step1.ps1* and \ *Test7_KernelModule LoadingEvents_Step2.ps1* shall be available.

9.2.7.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

9.2.7.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R840 with Azure Stack Edge (build 10.0.17784.1068)

- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

9.2.7.4 Verdict

As the result above states, the audit events related to the kernel module loading and unloading events have been correctly generated and they include all the information defined in the ***Security Target*** document.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 7** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 7.**

9.2.8 Test 8 - Lock and unlock user accounts

Generation of events related to lock and unlock user account will be tested in this test case.

9.2.8.1 Setup

The applicable setup for this test is the same as the one defined for *FIA_AFL.1*.

9.2.8.2 Procedure

This test is done at the same time as *FIA_AFL.1*.

9.2.8.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Panasonic CF-33 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R840 with Azure Stack Edge (build 10.0.17784.1068)
- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- HPE Edgeline EL8000 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE’s behavior is as expected and detailed in the security target [ST004].

9.2.8.4 Verdict

As the result above states, the audit events related to the lock and unlock user account events have been correctly generated and they include all the information defined in the ***Security Target*** document.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 8** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 8.**

9.3 Final Verdict

Due to documentation review activity and all subtests have assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FAU_GEN.1.1.

10 FAU_GEN.1.2

The assurance activity for the **FAU_GEN.1.2** requirement is stated as follows:

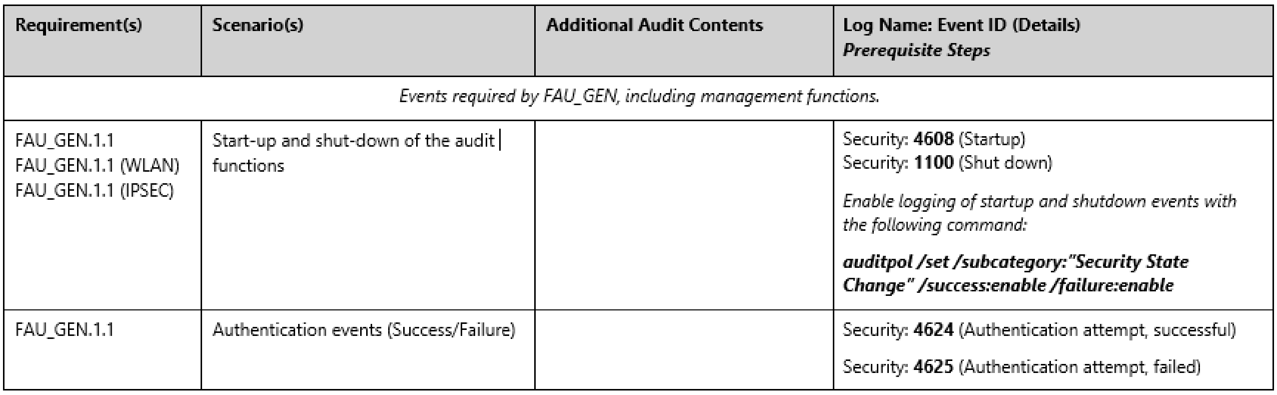
> The evaluator will check the administrative guide and ensure that it provides a format for audit records. Each audit record format type must be covered, along with a brief description of each field. The evaluator will ensure that the fields contains the information required.
>
> The evaluator shall test the OS's ability to correctly generate audit records by having the TOE generate audit records for the events listed in the ST. The evaluator will ensure the audit records generated during testing match the format specified in the administrative guide, and that the fields in each audit record provide the required information.

10.1 Documentation Review Activity

10.1.1 Findings

The evaluator has reviewed the ***Operational Guidance*** document. This document includes in its section **5.1 Audit Events by scenario** a table with all the auditable events. The content of this table matches with the selection performed by the vendor in the ***Security Target*** document.

For example, the following image shows some of the auditable events defined in the ***Operational Guidance*** document:



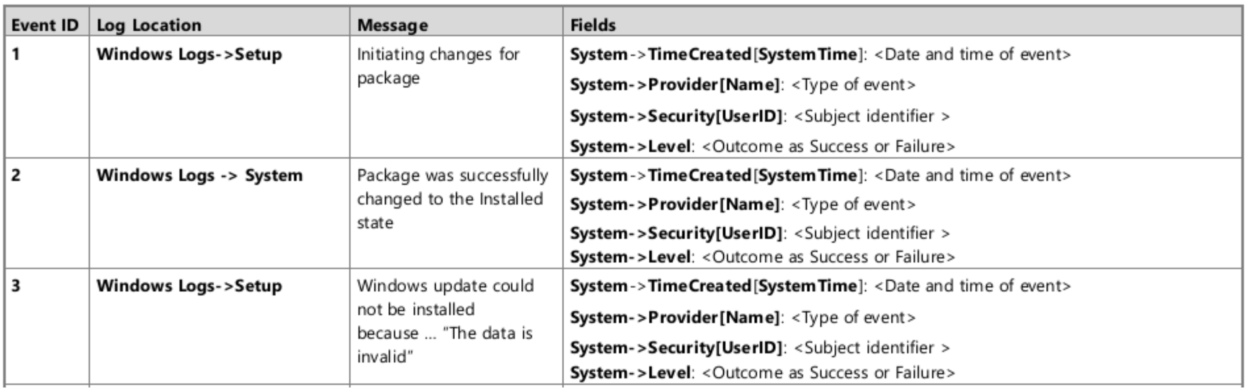
Requirement(s)	Scenario(s)	Additional Audit Contents	Log Name: Event ID (Details) ***Prerequisite Steps***
Events required by FAU_GEN, including management functions.			
FAU_GEN.1.1 FAU_GEN.1.1 (WLAN) FAU_GEN.1.1 (IPSEC)	Start-up and shut-down of the audit functions		Security: **4608** (Startup) Security: **1100** (Shut down) *Enable logging of startup and shutdown events with the following command:* ***auditpol /set /subcategory:"Security State Change" /success:enable /failure:enable***
FAU_GEN.1.1	Authentication events (Success/Failure)		Security: **4624** (Authentication attempt, successful) Security: **4625** (Authentication attempt, failed)

The ***Security Target*** document also states the minimum information that each audit record should include. These fields are the following:

- Date and time of the event.
- Type of the event.
- Subject identity.

- Outcome (success or failure) of the event.

In addition, the ***Operational Guidance*** document also provides information related the main fields for each auditable event. This information includes the name of these fields and a brief description for each one. For example, the following image shows the main required fields for the auditable event 2 (*Package was successfully changed to the Installed state*).



Event ID	Log Location	Message	Fields
1	**Windows Logs->Setup**	Initiating changes for package	**System**->**TimeCreated[SystemTime]**: <Date and time of event> **System->Provider[Name]**: <Type of event> **System->Security[UserID]**: <Subject identifier > **System->Level**: <Outcome as Success or Failure>
2	**Windows Logs -> System**	Package was successfully changed to the Installed state	**System**->**TimeCreated[SystemTime]**: <Date and time of event> **System->Provider[Name]**: <Type of event> **System->Security[UserID]**: <Subject identifier > **System->Level**: <Outcome as Success or Failure>
3	**Windows Logs->Setup**	Windows update could not be installed because ... "The data is invalid"	**System**->**TimeCreated[SystemTime]**: <Date and time of event> **System->Provider[Name]**: <Type of event> **System->Security[UserID]**: <Subject identifier > **System->Level**: <Outcome as Success or Failure>

10.1.2 Verdict

The evaluator has reviewed the ***Security Target*** document and has ensured that the format of every auditable event is described, including at least the fields defined in the ***Security Target*** document (*date and time, type of the event, subject identity and outcome*).

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfilment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

10.2 Test Activity

This test is done at the same time as *FAU_GEN.1.1*.

10.2.1 Test

10.2.1.1 Setup

The applicable setup for this test is the same as the one defined for *FAU_GEN.1.1*.

10.2.1.2 Procedure

This test is done at the same time as *FAU_GEN.1.1*.

10.2.1.3 Results

Results for this test are included in *FAU_GEN.1.1*.

10.2.1.4 Verdict

As it is can be appreciated in the obtained results section of *FAU_GEN.1.1* requirement, all the audit events generated by the TOE match with the format described in the operational guidance and include, at least, the fields listed in the ***Security Target*** document.

Therefore, the **PASS** verdict is assigned to the test activity.

10.3 Final Verdict

Since this requirement has been tested alongside the *FAU_GEN.1.1* requirement, where all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to this FAU_GEN.1.2 requirement.

11 FCS_CKM.1.1(1)

The assurance activity for the **FCS_CKM.1.1(1)** requirement is stated as follows:

> The evaluator will ensure that the TSS identifies the key sizes supported by the OS. If the ST specifies more than one scheme, the evaluator will examine the TSS to verify that it identifies the usage for each scheme.
>
> The evaluator will verify that the AGD guidance instructs the administrator how to configure the OS to use the selected key generation scheme(s) and key size(s) for all uses defined in this PP.
>
> Evaluation Activity Note: The following tests may require the vendor to furnish a developer environment and developer tools that are typically not available to end-users of the OS.
>
> **Key Generation for FIPS PUB 186-4 RSA Schemes**
>
> The evaluator will verify the implementation of RSA Key Generation by the OS using the Key Generation test. This test verifies the ability of the TSF to correctly produce values for the key components including the public verification exponent e, the private prime factors p and q, the public modulus n and the calculation of the private signature exponent d. Key Pair generation specifies 5 ways (or methods) to generate the primes p and q. These include:
>
> 1. Random Primes:
>   - Provable primes
>   - Probable primes
> 2. Primes with Conditions:
>   - Primes p1, p2, q1,q2, p and q shall all be provable primes
>   - Primes p1, p2, q1, and q2 shall be provable primes and p and q shall be probable primes
>   - Primes p1, p2, q1,q2, p and q shall all be probable primes
>
> To test the key generation method for the Random Provable primes method and for all the Primes with Conditions methods, the evaluator must seed the TSF key generation routine with sufficient data to deterministically generate the RSA key pair. This includes the random seed(s), the public exponent of the RSA key, and the desired key length. For each key length supported, the evaluator shall have the TSF generate 25 key pairs. The evaluator will verify the correctness of the TSF's implementation by comparing values generated by the TSF with those generated from a known good implementation.
>
> If possible, the Random Probable primes method should also be verified against a known good implementation as described above. Otherwise, the evaluator will have the TSF generate 10 keys pairs for each supported key length nlen and verify:

- $n = p \cdot q$,
- p and q are probably prime according to Miller-Rabin tests,
- GCD(p-1,e) = 1,
- GCD(q-1,e) = 1,
- $2^{16} \leq e \leq 2^{256}$ and e is an odd integer,
- $|p-q| > 2^{nlen/2-100}$,
- $p \geq 2^{nlen/2-1/2}$,
- $q \geq 2^{nlen/2-1/2}$,
- $2^{(nlen/2)} < d < LCM(p-1,q-1)$,
- e*d = 1 mod LCM(p-1,q-1).

Key Generation for Elliptic Curve Cryptography (ECC)

FIPS 186-4 ECC Key Generation Test

For each supported NIST curve, i.e., P-256, P-384 and P-521, the evaluator will require the implementation under test (IUT) to generate 10 private/public key pairs. The private key shall be generated using an approved random bit generator (RBG). To determine correctness, the evaluator will submit the generated key pairs to the public key verification (PKV) function of a known good implementation.

FIPS 186-4 Public Key Verification (PKV) Test

For each supported NIST curve, i.e., P-256, P-384 and P-521, the evaluator will generate 10 private/public key pairs using the key generation function of a known good implementation and modify five of the public key values so that they are incorrect, leaving five values unchanged (i.e., correct). The evaluator will obtain in response a set of 10 PASS/FAIL values.

Key Generation for Finite-Field Cryptography (FFC)

The evaluator will verify the implementation of the Parameters Generation and the Key Generation for FFC by the TOE using the Parameter Generation and Key Generation test. This test verifies the ability of the TSF to correctly produce values for the field prime p, the cryptographic prime q (dividing p-1), the cryptographic group generator g, and the calculation of the private key x and public key y.

The Parameter generation specifies 2 ways (or methods) to generate the cryptographic prime q and the field prime p:

- Cryptographic and Field Primes:
  - Primes q and p shall both be provable primes
  - Primes q and field prime p shall both be probable primes

and two ways to generate the cryptographic group generator g:

- Cryptographic Group Generator:
  - Generator g constructed through a verifiable process

  - Generator g constructed through an unverifiable process

The Key generation specifies 2 ways to generate the private key x:

- Private Key:
  - len(q) bit output of RBG where $1 \leq x \leq$ q-1
  - len(q) + 64 bit output of RBG, followed by a mod q-1 operation where $1 \leq x \leq$ q-1

The security strength of the RBG must be at least that of the security offered by the FFC parameter set. To test the cryptographic and field prime generation method for the provable primes method and/or the group generator g for a verifiable process, the evaluator must seed the TSF parameter generation routine with sufficient data to deterministically generate the parameter set. For each key length supported, the evaluator shall have the TSF generate 25 parameter sets and key pairs. The evaluator shall verify the correctness of the TSF's implementation by comparing values generated by the TSF with those generated from a known good implementation. Verification must also confirm:

- g != 0,1
- q divides p-1
- g^q mod p = 1
- g^x mod p = y

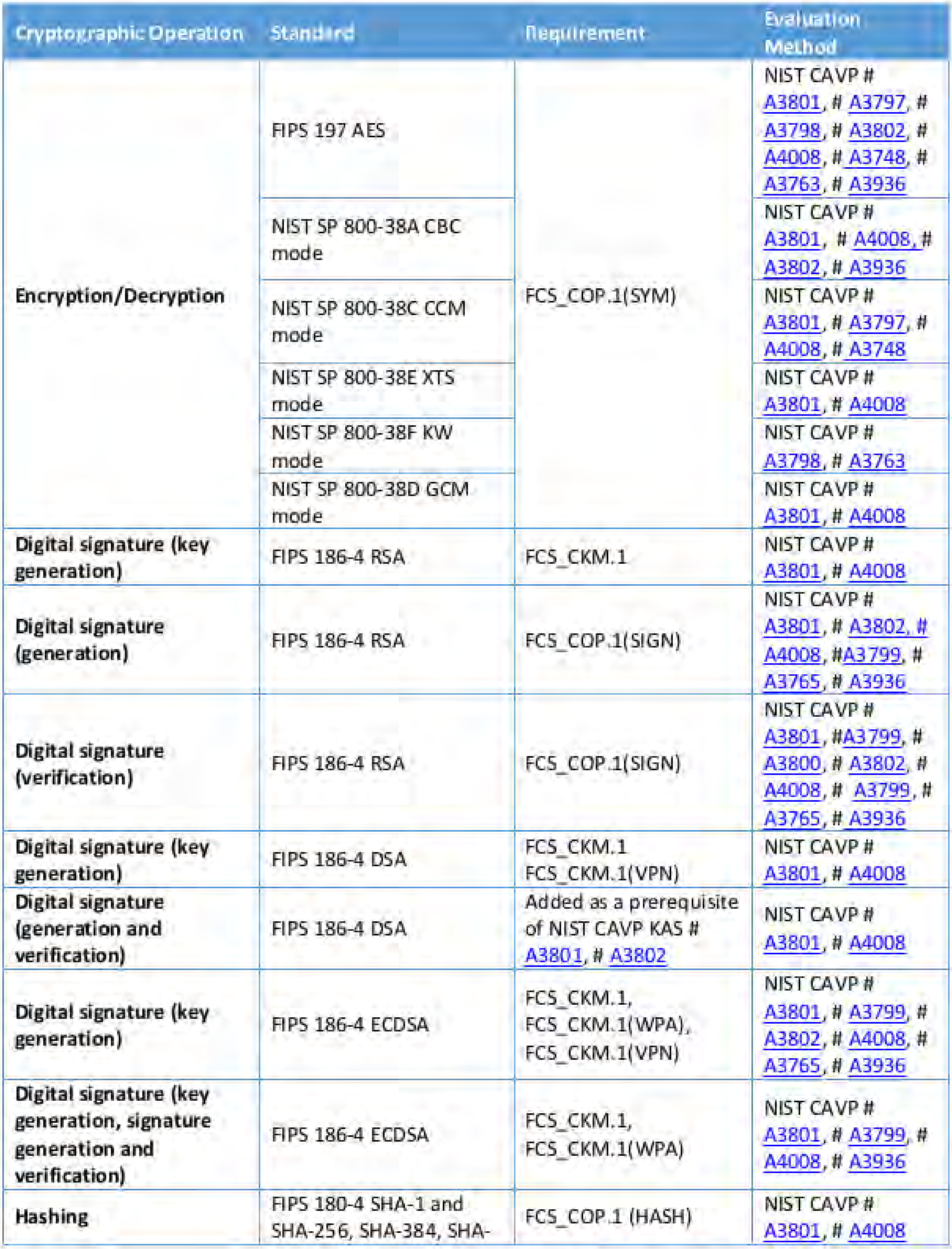
for each FFC parameter set and key pair.

11.1 Documentation Review Activity

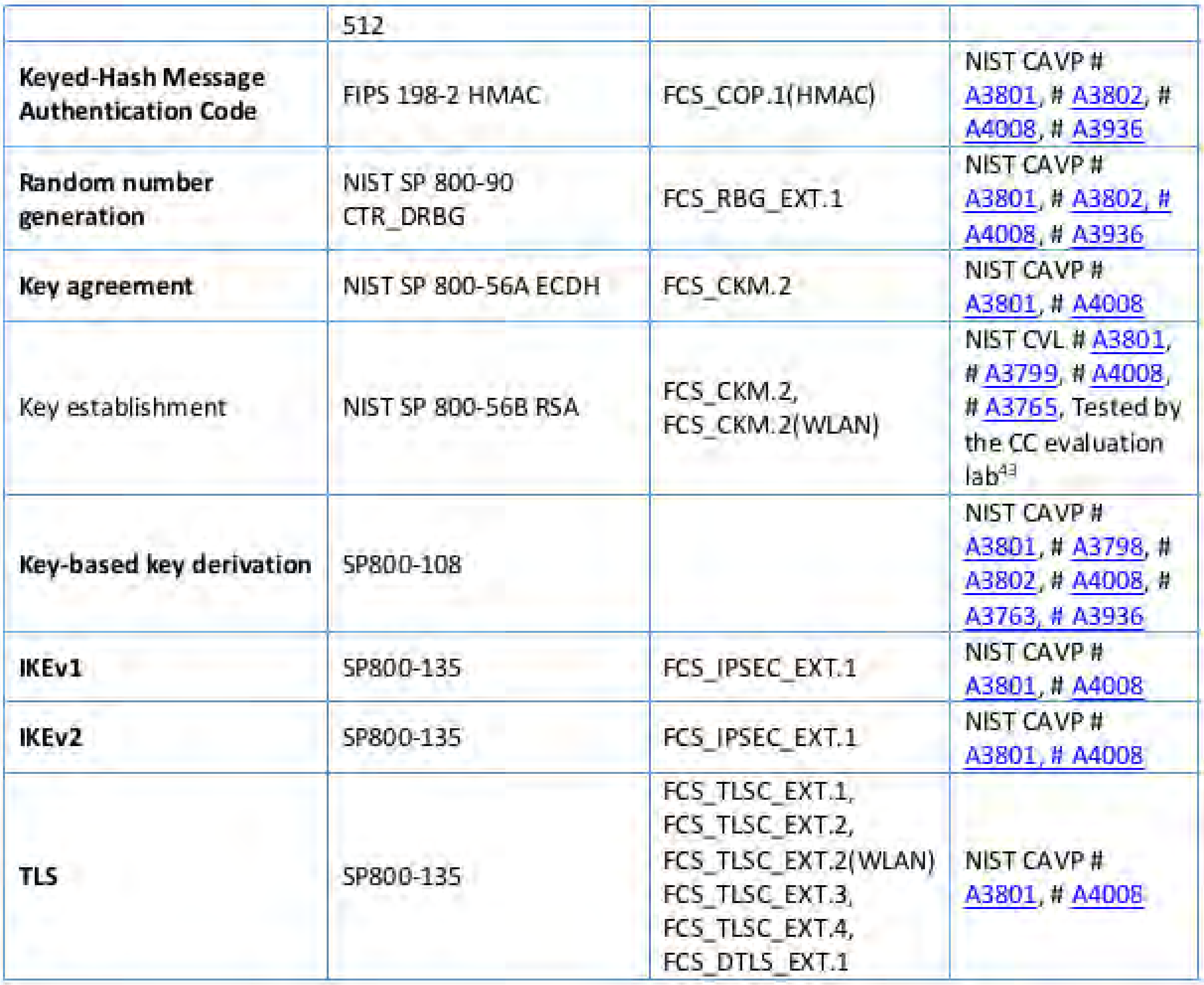
11.1.1 Findings

The evaluator has reviewed the ***Security Target*** document and the information provided in the TSS, section **6.2.2 Cryptographic Algorithm Validation**.

11.1.1.1 Cryptographic Algorithm Standards and Evaluation Methods for Windows 11 (version 22H2)

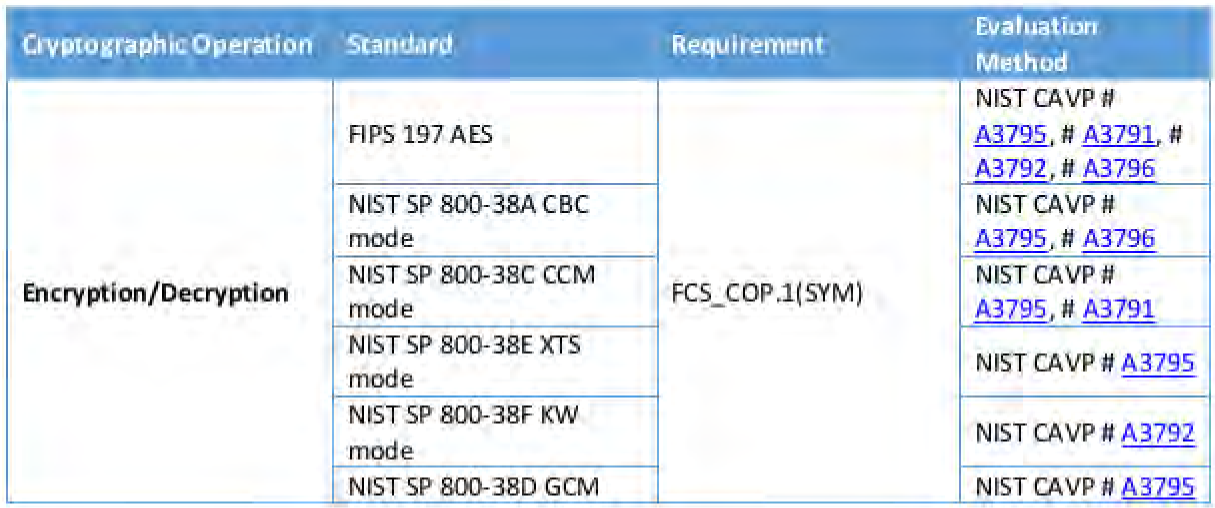


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3801, # A3797, # A3798, # A3802, # A4008, # A3748, # A3763, # A3936
	NIST SP 800-38A CBC mode		NIST CAVP # A3801, # A4008, # A3802, # A3936
	NIST SP 800-38C CCM mode		NIST CAVP # A3801, # A3797, # A4008, # A3748
	NIST SP 800-38E XTS mode		NIST CAVP # A3801, # A4008
	NIST SP 800-38F KW mode		NIST CAVP # A3798, # A3763
	NIST SP 800-38D GCM mode		NIST CAVP # A3801, # A4008
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP # A3801, # A4008
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3801, # A3802, # A4008, #A3799, # A3765, # A3936
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3801, #A3799, # A3800, # A3802, # A4008, # A3799, # A3765, # A3936
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3801, # A4008
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3801, # A3802	NIST CAVP # A3801, # A4008
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3801, # A3799, # A3802, # A4008, # A3765, # A3936
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3801, # A3799, # A4008, # A3936
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-	FCS_COP.1 (HASH)	NIST CAVP # A3801, # A4008

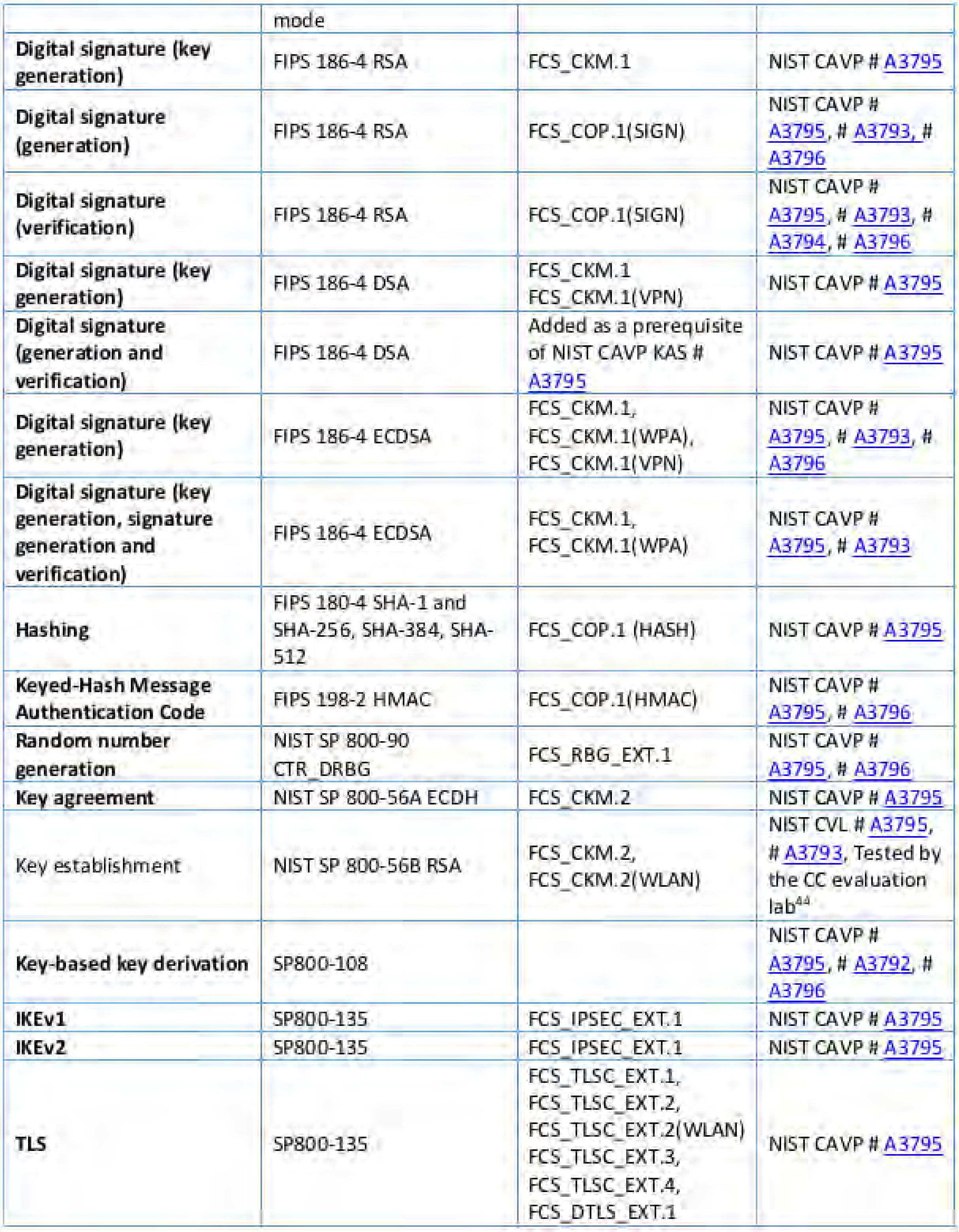


	512		
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3801, # A3802, # A4008, # A3936
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3801, # A3802, # A4008, # A3936
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3801, # A4008
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2, FCS_CKM.2(WLAN)	NIST CVL # A3801, # A3799, # A4008, # A3765, Tested by the CC evaluation lab[43]
Key-based key derivation	SP800-108		NIST CAVP # A3801, # A3798, # A3802, # A4008, # A3763, # A3936
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3801, # A4008
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3801, # A4008
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3801, # A4008

11.1.1.2 Cryptographic Algorithm Standards and Evaluation Methods for Windows 10 (version 22H2)

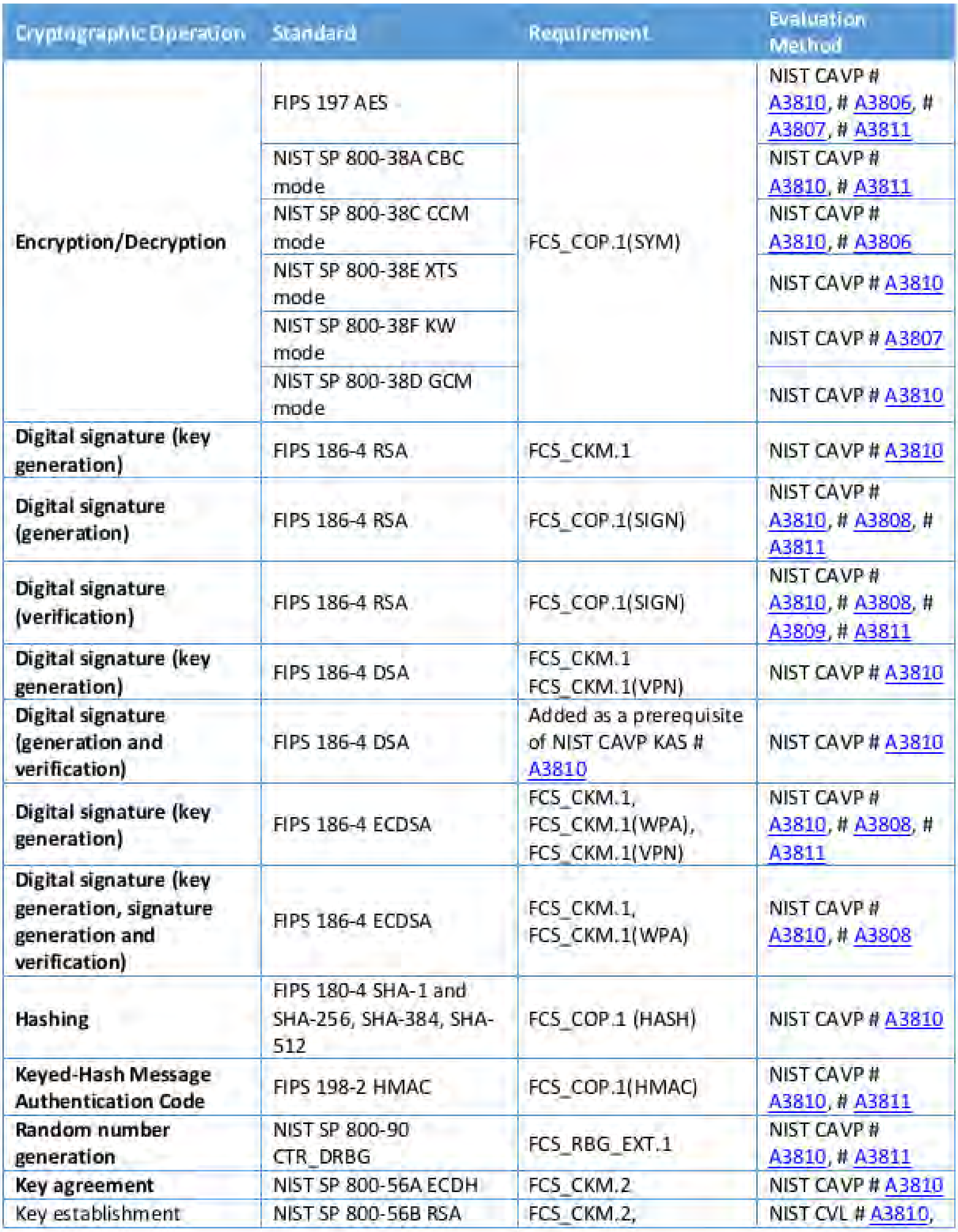


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3795, # A3791, # A3792, # A3796
	NIST SP 800-38A CBC mode		NIST CAVP # A3795, # A3796
	NIST SP 800-38C CCM mode		NIST CAVP # A3795, # A3791
	NIST SP 800-38E XTS mode		NIST CAVP # A3795
	NIST SP 800-38F KW mode		NIST CAVP # A3792
	NIST SP 800-38D GCM		NIST CAVP # A3795

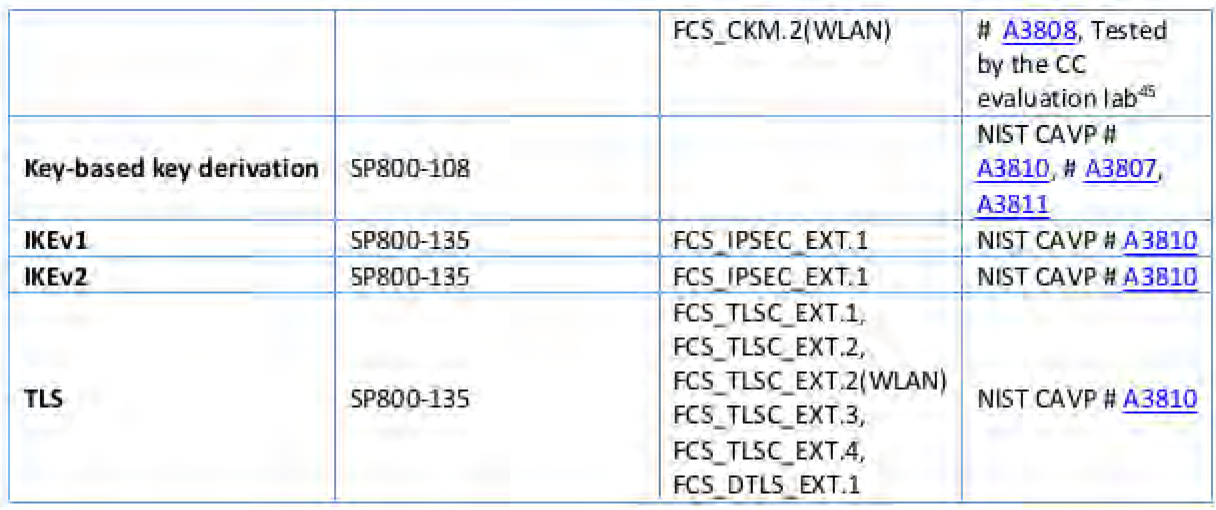


	mode		
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP # A3795
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3795, # A3793, # A3796
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3795, # A3793, # A3794, # A3796
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3795
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3795	NIST CAVP # A3795
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3795, # A3793, # A3796
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3795, # A3793
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3795
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3795, # A3796
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3795, # A3796
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3795
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2, FCS_CKM.2(WLAN)	NIST CVL # A3795, # A3793, Tested by the CC evaluation lab[44]
Key-based key derivation	SP800-108		NIST CAVP # A3795, # A3792, # A3796
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3795
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3795
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3795

11.1.1.3 Cryptographic Algorithm Standards and Evaluation Methods for Windows Server 2022 and Windows Server Datacenter: Azure Edition

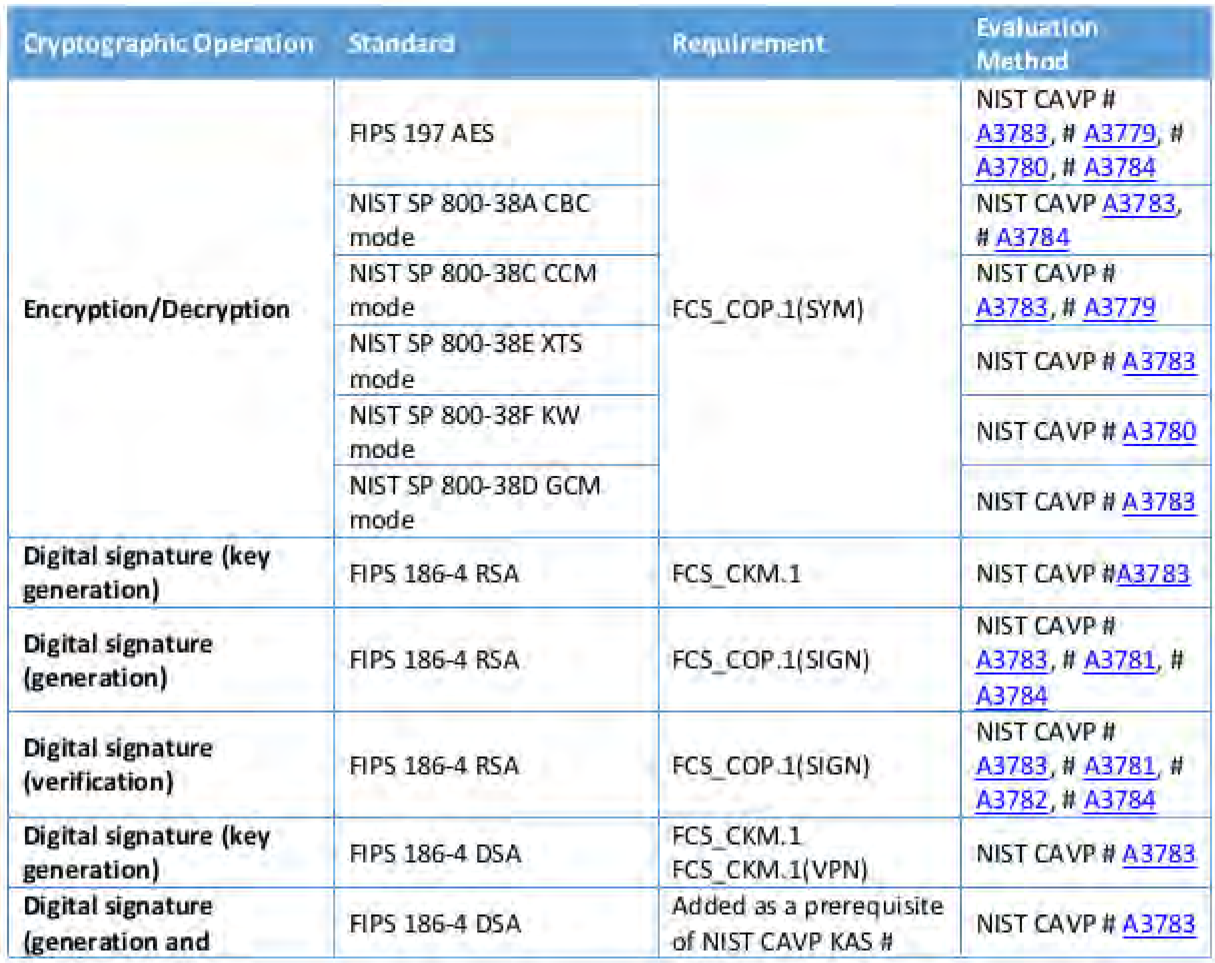


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3810, # A3806, # A3807, # A3811
	NIST SP 800-38A CBC mode		NIST CAVP # A3810, # A3811
	NIST SP 800-38C CCM mode		NIST CAVP # A3810, # A3806
	NIST SP 800-38E XTS mode		NIST CAVP # A3810
	NIST SP 800-38F KW mode		NIST CAVP # A3807
	NIST SP 800-38D GCM mode		NIST CAVP # A3810
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP # A3810
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3810, # A3808, # A3811
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3810, # A3808, # A3809, # A3811
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3810
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3810	NIST CAVP # A3810
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3810, # A3808, # A3811
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3810, # A3808
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3810
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3810, # A3811
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3810, # A3811
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3810
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2,	NIST CVL # A3810,

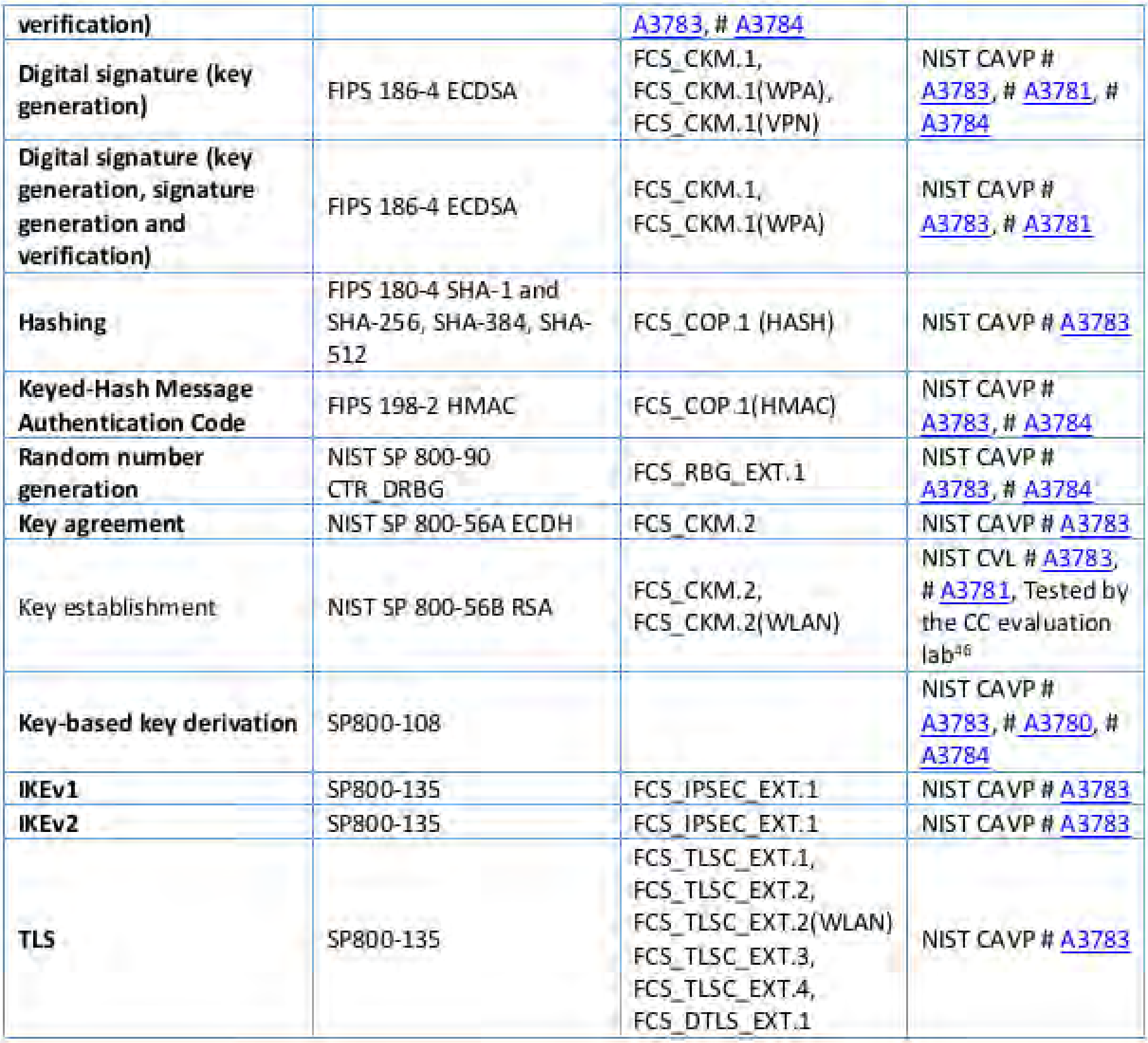


		FCS_CKM.2(WLAN)	# A3808, Tested by the CC evaluation lab[45]
Key-based key derivation	SP800-108		NIST CAVP # A3810, # A3807, A3811
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3810
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3810
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3810

11.1.1.4 Cryptographic Algorithm Standards and Evaluation Methods for Windows Server Azure Stack HCIv2 version 22H2

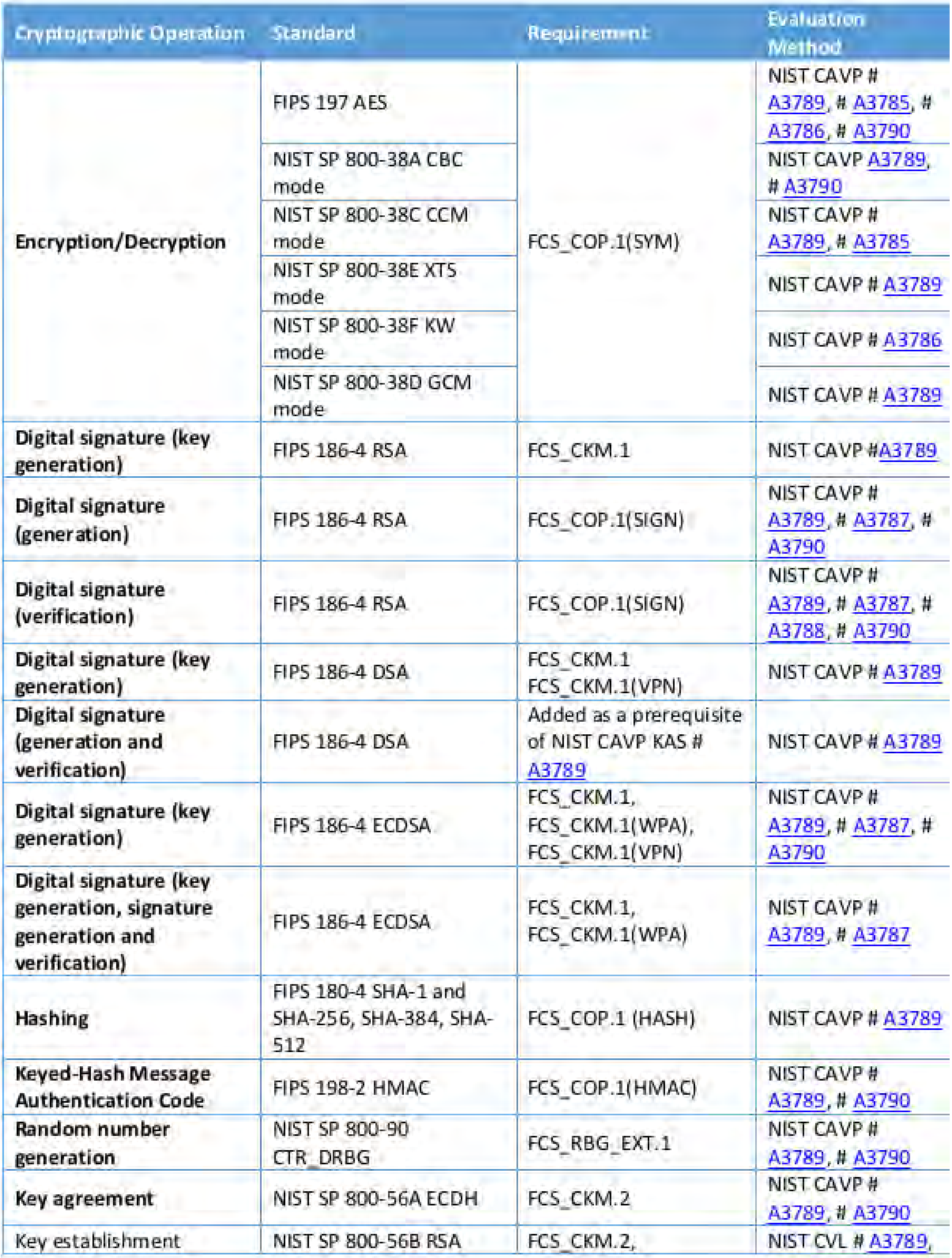


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3783, # A3779, # A3780, # A3784
	NIST SP 800-38A CBC mode		NIST CAVP A3783, # A3784
	NIST SP 800-38C CCM mode		NIST CAVP # A3783, # A3779
	NIST SP 800-38E XTS mode		NIST CAVP # A3783
	NIST SP 800-38F KW mode		NIST CAVP # A3780
	NIST SP 800-38D GCM mode		NIST CAVP # A3783
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP #A3783
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3783, # A3781, # A3784
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3783, # A3781, # A3782, # A3784
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3783
Digital signature (generation and	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS #	NIST CAVP # A3783

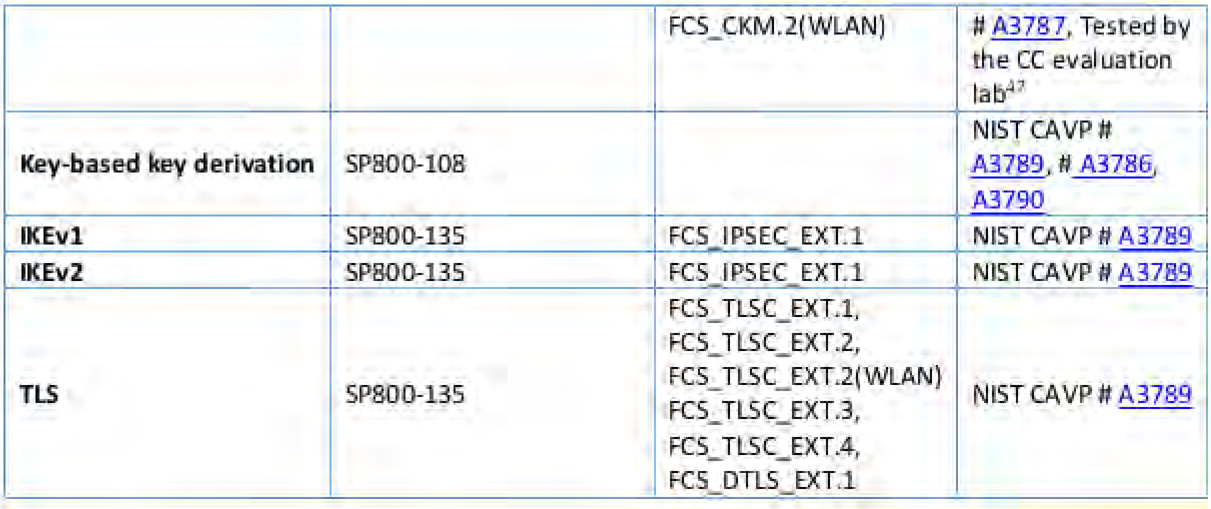


verification)		A3783, # A3784	
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3783, # A3781, # A3784
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3783, # A3781
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3783
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3783, # A3784
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3783, # A3784
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3783
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2, FCS_CKM.2(WLAN)	NIST CVL # A3783, # A3781, Tested by the CC evaluation lab[46]
Key-based key derivation	SP800-108		NIST CAVP # A3783, # A3780, # A3784
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3783
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3783
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3783

11.1.1.5 Cryptographic Algorithm Standards and Evaluation Methods for Azure Stack Hub and Azure Stack Edge



Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3789, # A3785, # A3786, # A3790
	NIST SP 800-38A CBC mode		NIST CAVP A3789, # A3790
	NIST SP 800-38C CCM mode		NIST CAVP # A3789, # A3785
	NIST SP 800-38E XTS mode		NIST CAVP # A3789
	NIST SP 800-38F KW mode		NIST CAVP # A3786
	NIST SP 800-38D GCM mode		NIST CAVP # A3789
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP #A3789
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3789, # A3787, # A3790
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3789, # A3787, # A3788, # A3790
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3789
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3789	NIST CAVP # A3789
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3789, # A3787, # A3790
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3789, # A3787
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3789
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3789, # A3790
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3789, # A3790
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3789, # A3790
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2,	NIST CVL # A3789,



		FCS_CKM.2(WLAN)	# A3787, Tested by the CC evaluation lab[47]
Key-based key derivation	SP800-108		NIST CAVP # A3789, # A3786, A3790
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3789
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3789
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3789

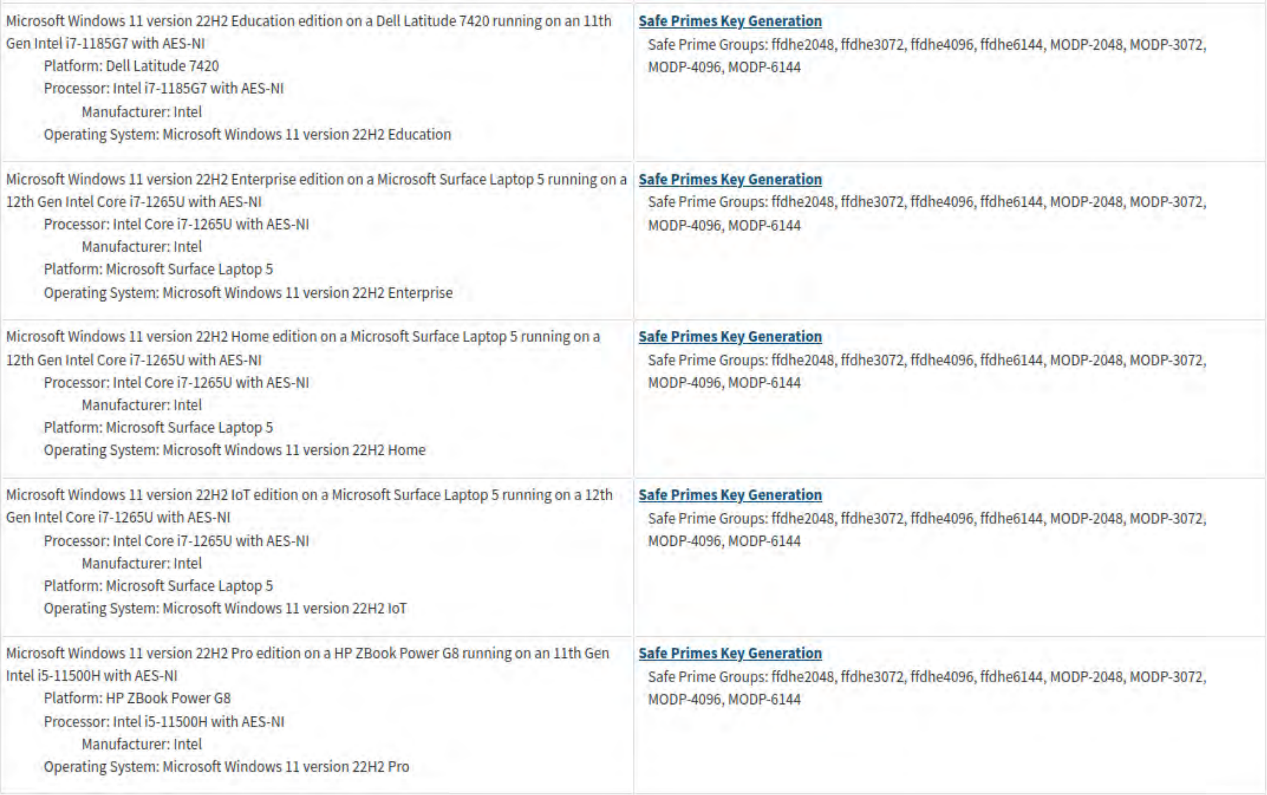
The ***Operational Guidance*** document, states that for the evaluated version the following security policy needs to be applied (Section 3.2.5):

- Local Policies \ Security Options\System cryptography: Use FIPS 140 compliant cryptographic algorithms, including encryption, hashing and signing algorithm.

After applying this policy, only FIPS certified algorithms can be used, including the key generation algorithms defined in the table above.

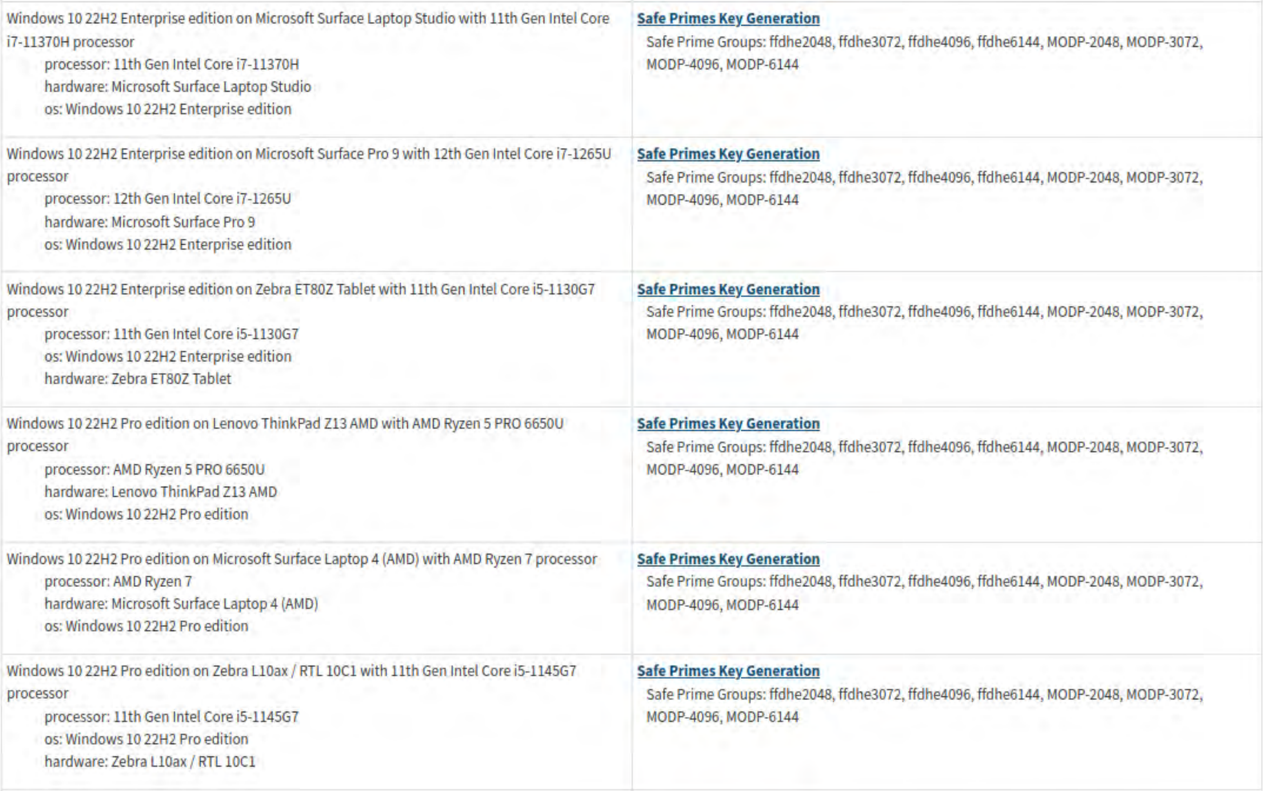
As part of the testing activity described below, the correctness of the cryptographic functionality has been demonstrated against the BOTAN tool. However, ffdhe groups are not available in BOTAN, and the laboratory has verified the implementation against the CAVP tool. Below, the CAVP certificates granted for this functionality are listed (extracted from the tables above)

11.1.1.6 Windows 11 version 22H2 (CAVP Cert. #A4008)



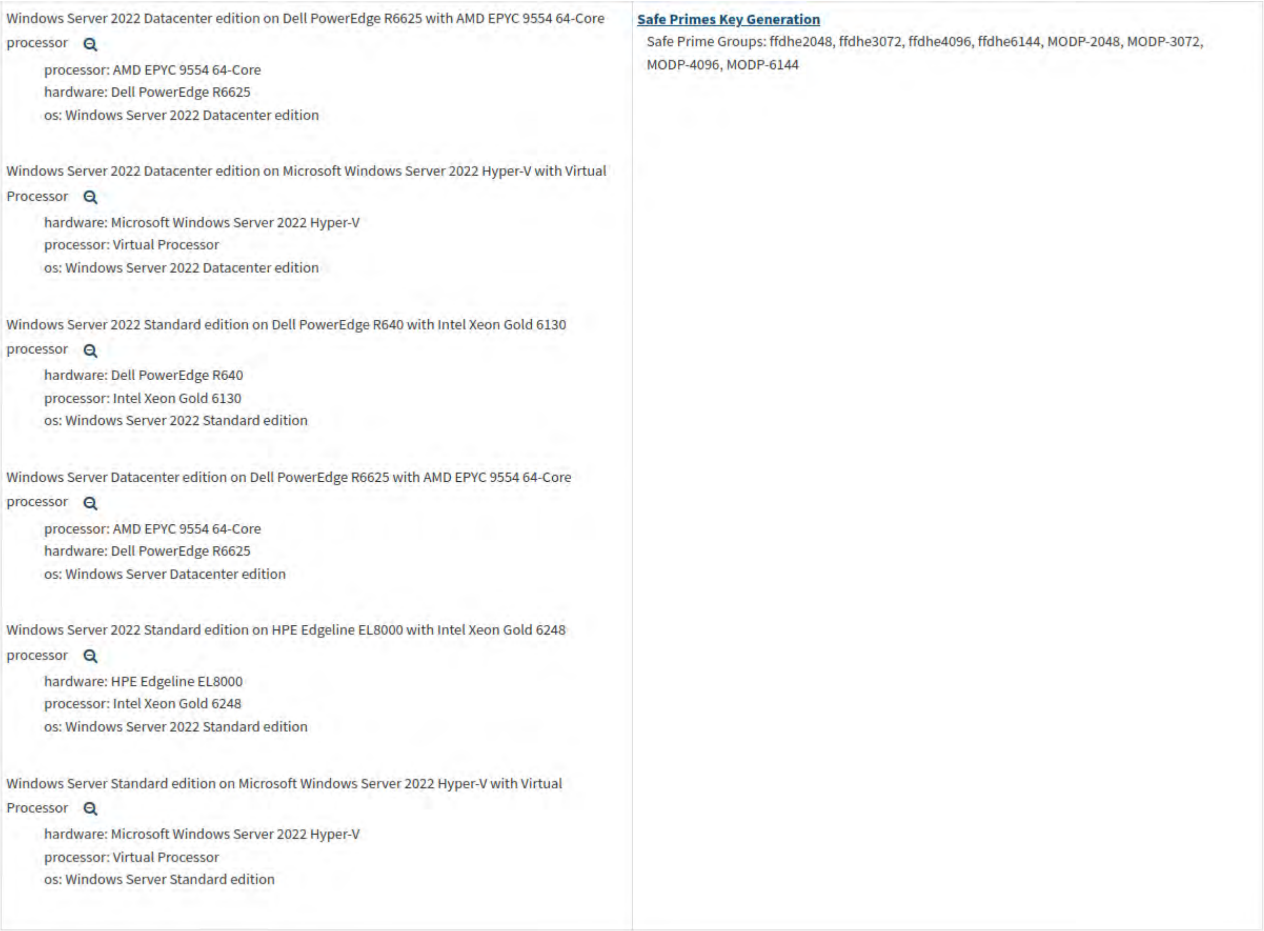
Microsoft Windows 11 version 22H2 Education edition on a Dell Latitude 7420 running on an 11th Gen Intel i7-1185G7 with AES-NI Platform: Dell Latitude 7420 Processor: Intel i7-1185G7 with AES-NI Manufacturer: Intel Operating System: Microsoft Windows 11 version 22H2 Education	**Safe Primes Key Generation** Safe Prime Groups: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, MODP-2048, MODP-3072, MODP-4096, MODP-6144
Microsoft Windows 11 version 22H2 Enterprise edition on a Microsoft Surface Laptop 5 running on a 12th Gen Intel Core i7-1265U with AES-NI Processor: Intel Core i7-1265U with AES-NI Manufacturer: Intel Platform: Microsoft Surface Laptop 5 Operating System: Microsoft Windows 11 version 22H2 Enterprise	**Safe Primes Key Generation** Safe Prime Groups: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, MODP-2048, MODP-3072, MODP-4096, MODP-6144
Microsoft Windows 11 version 22H2 Home edition on a Microsoft Surface Laptop 5 running on a 12th Gen Intel Core i7-1265U with AES-NI Processor: Intel Core i7-1265U with AES-NI Manufacturer: Intel Platform: Microsoft Surface Laptop 5 Operating System: Microsoft Windows 11 version 22H2 Home	**Safe Primes Key Generation** Safe Prime Groups: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, MODP-2048, MODP-3072, MODP-4096, MODP-6144
Microsoft Windows 11 version 22H2 IoT edition on a Microsoft Surface Laptop 5 running on a 12th Gen Intel Core i7-1265U with AES-NI Processor: Intel Core i7-1265U with AES-NI Manufacturer: Intel Platform: Microsoft Surface Laptop 5 Operating System: Microsoft Windows 11 version 22H2 IoT	**Safe Primes Key Generation** Safe Prime Groups: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, MODP-2048, MODP-3072, MODP-4096, MODP-6144
Microsoft Windows 11 version 22H2 Pro edition on a HP ZBook Power G8 running on an 11th Gen Intel i5-11500H with AES-NI Platform: HP ZBook Power G8 Processor: Intel i5-11500H with AES-NI Manufacturer: Intel Operating System: Microsoft Windows 11 version 22H2 Pro	**Safe Primes Key Generation** Safe Prime Groups: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, MODP-2048, MODP-3072, MODP-4096, MODP-6144

11.1.1.7 Windows 10 version 22H2 (CAVP Cert. #A3795)



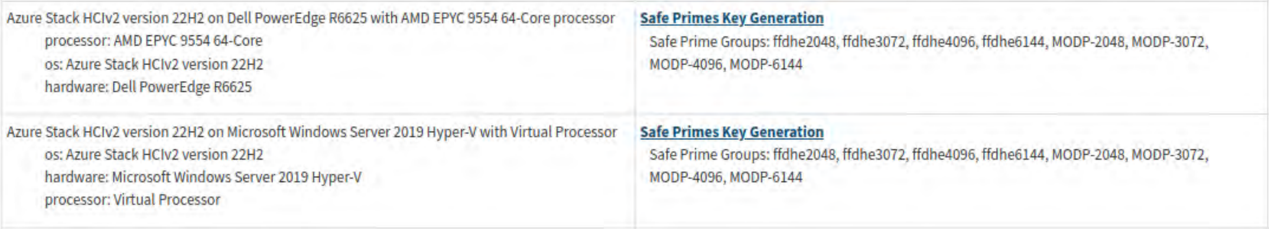
Windows 10 22H2 Enterprise edition on Microsoft Surface Laptop Studio with 11th Gen Intel Core i7-11370H processor processor: 11th Gen Intel Core i7-11370H hardware: Microsoft Surface Laptop Studio os: Windows 10 22H2 Enterprise edition	Safe Primes Key Generation Safe Prime Groups: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, MODP-2048, MODP-3072, MODP-4096, MODP-6144
Windows 10 22H2 Enterprise edition on Microsoft Surface Pro 9 with 12th Gen Intel Core i7-1265U processor processor: 12th Gen Intel Core i7-1265U hardware: Microsoft Surface Pro 9 os: Windows 10 22H2 Enterprise edition	Safe Primes Key Generation Safe Prime Groups: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, MODP-2048, MODP-3072, MODP-4096, MODP-6144
Windows 10 22H2 Enterprise edition on Zebra ET80Z Tablet with 11th Gen Intel Core i5-1130G7 processor processor: 11th Gen Intel Core i5-1130G7 os: Windows 10 22H2 Enterprise edition hardware: Zebra ET80Z Tablet	Safe Primes Key Generation Safe Prime Groups: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, MODP-2048, MODP-3072, MODP-4096, MODP-6144
Windows 10 22H2 Pro edition on Lenovo ThinkPad Z13 AMD with AMD Ryzen 5 PRO 6650U processor processor: AMD Ryzen 5 PRO 6650U hardware: Lenovo ThinkPad Z13 AMD os: Windows 10 22H2 Pro edition	Safe Primes Key Generation Safe Prime Groups: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, MODP-2048, MODP-3072, MODP-4096, MODP-6144
Windows 10 22H2 Pro edition on Microsoft Surface Laptop 4 (AMD) with AMD Ryzen 7 processor processor: AMD Ryzen 7 hardware: Microsoft Surface Laptop 4 (AMD) os: Windows 10 22H2 Pro edition	Safe Primes Key Generation Safe Prime Groups: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, MODP-2048, MODP-3072, MODP-4096, MODP-6144
Windows 10 22H2 Pro edition on Zebra L10ax / RTL 10C1 with 11th Gen Intel Core i5-1145G7 processor processor: 11th Gen Intel Core i5-1145G7 os: Windows 10 22H2 Pro edition hardware: Zebra L10ax / RTL 10C1	Safe Primes Key Generation Safe Prime Groups: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, MODP-2048, MODP-3072, MODP-4096, MODP-6144

11.1.1.8 Windows Server 2022 and Windows Server Datacenter: Azure Edition (CAVP Cert. #A3810)



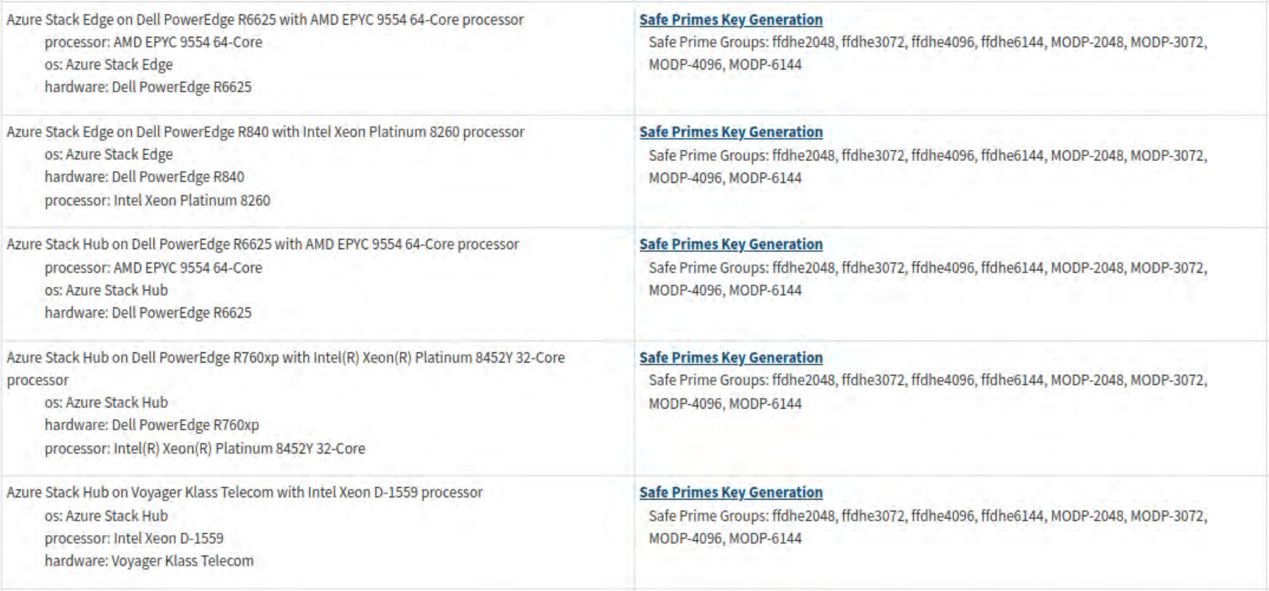
Windows Server 2022 Datacenter edition on Dell PowerEdge R6625 with AMD EPYC 9554 64-Core processor processor: AMD EPYC 9554 64-Core hardware: Dell PowerEdge R6625 os: Windows Server 2022 Datacenter edition Windows Server 2022 Datacenter edition on Microsoft Windows Server 2022 Hyper-V with Virtual Processor hardware: Microsoft Windows Server 2022 Hyper-V processor: Virtual Processor os: Windows Server 2022 Datacenter edition Windows Server 2022 Standard edition on Dell PowerEdge R640 with Intel Xeon Gold 6130 processor hardware: Dell PowerEdge R640 processor: Intel Xeon Gold 6130 os: Windows Server 2022 Standard edition Windows Server Datacenter edition on Dell PowerEdge R6625 with AMD EPYC 9554 64-Core processor processor: AMD EPYC 9554 64-Core hardware: Dell PowerEdge R6625 os: Windows Server Datacenter edition Windows Server 2022 Standard edition on HPE Edgeline EL8000 with Intel Xeon Gold 6248 processor hardware: HPE Edgeline EL8000 processor: Intel Xeon Gold 6248 os: Windows Server 2022 Standard edition Windows Server Standard edition on Microsoft Windows Server 2022 Hyper-V with Virtual Processor hardware: Microsoft Windows Server 2022 Hyper-V processor: Virtual Processor os: Windows Server Standard edition	**Safe Primes Key Generation** Safe Prime Groups: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, MODP-2048, MODP-3072, MODP-4096, MODP-6144

11.1.1.9 Windows Server Azure Stack HCIv2 version 22H2 (CAVP Cert. #A3783)



Azure Stack HCIv2 version 22H2 on Dell PowerEdge R6625 with AMD EPYC 9554 64-Core processor processor: AMD EPYC 9554 64-Core os: Azure Stack HCIv2 version 22H2 hardware: Dell PowerEdge R6625	**Safe Primes Key Generation** Safe Prime Groups: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, MODP-2048, MODP-3072, MODP-4096, MODP-6144
Azure Stack HCIv2 version 22H2 on Microsoft Windows Server 2019 Hyper-V with Virtual Processor os: Azure Stack HCIv2 version 22H2 hardware: Microsoft Windows Server 2019 Hyper-V processor: Virtual Processor	**Safe Primes Key Generation** Safe Prime Groups: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, MODP-2048, MODP-3072, MODP-4096, MODP-6144

11.1.1.10 Azure Stack Hub and Azure Stack Edge (CAVP Cert. #A3789)



Azure Stack Edge on Dell PowerEdge R6625 with AMD EPYC 9554 64-Core processor processor: AMD EPYC 9554 64-Core os: Azure Stack Edge hardware: Dell PowerEdge R6625	Safe Primes Key Generation Safe Prime Groups: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, MODP-2048, MODP-3072, MODP-4096, MODP-6144
Azure Stack Edge on Dell PowerEdge R840 with Intel Xeon Platinum 8260 processor os: Azure Stack Edge hardware: Dell PowerEdge R840 processor: Intel Xeon Platinum 8260	Safe Primes Key Generation Safe Prime Groups: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, MODP-2048, MODP-3072, MODP-4096, MODP-6144
Azure Stack Hub on Dell PowerEdge R6625 with AMD EPYC 9554 64-Core processor processor: AMD EPYC 9554 64-Core os: Azure Stack Hub hardware: Dell PowerEdge R6625	Safe Primes Key Generation Safe Prime Groups: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, MODP-2048, MODP-3072, MODP-4096, MODP-6144
Azure Stack Hub on Dell PowerEdge R760xp with Intel(R) Xeon(R) Platinum 8452Y 32-Core processor os: Azure Stack Hub hardware: Dell PowerEdge R760xp processor: Intel(R) Xeon(R) Platinum 8452Y 32-Core	Safe Primes Key Generation Safe Prime Groups: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, MODP-2048, MODP-3072, MODP-4096, MODP-6144
Azure Stack Hub on Voyager Klass Telecom with Intel Xeon D-1559 processor os: Azure Stack Hub processor: Intel Xeon D-1559 hardware: Voyager Klass Telecom	Safe Primes Key Generation Safe Prime Groups: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, MODP-2048, MODP-3072, MODP-4096, MODP-6144

11.1.2 Verdict

The evaluator considers that the TSS identifies the key sizes supported by each of the OS for every algorithm through its NIST certificates. Moreover, all the key generation algorithms (whose purpose is to be used as part of digital signatures processes) follow the same standard (*FIPS 186-4*).

The ***Operational Guidance*** document, defines the FIPS security policy to be applied. Once this policy is applied, only the approved key generation method described above can be used. No further configuration is needed to generate keys following the *Appendix B.1*, *B.3* and *B.4* of the *FIPS-PUB 186-4* standard.

Hence, the **PASS** verdict is assigned to the documentation review activity.

11.2 Test Activity

Based on the SFR instantiation included in the security target, the vendor has selected the following key generation method:

1. RSA scheme for key sizes of 2048-bit or greater (according to TSS section 2048 and 3072 bits).
2. ECDSA scheme using NIST curves P-256, P-384 and P-521
3. FFC scheme for key sizes of 2048-bit or greater (according to TSS section: MODP-2048, MODP-3072, MODP-4096, ffdhe2048, ffdhe3072, ffdhe4096 and ffdhe6144 groups).

In addition to the Common Criteria evaluation, the laboratory has also performed the CAVP validation for these and other algorithms. The general procedure that has been followed during the evaluation in order to demonstrate the correctness of the cryptographic functionality is as follows:

1. The laboratory has used the same test vectors used as part of the CAVP validation. For key generation algorithms, the following types of test are performed:

   - For RSA:
     - Generated Data Test (GDT). The main goal for these tests is verify the implementation of the RSA key generation operation. For this test, it is expected that the TOE generate RSA key pairs based on the provided key length and public exponent and return the value p, q, n, d, and e. Then, these values are verified using the known good implementation.
   - For ECDSA:
     - Algorithm Functional Test (AFT). The main goal for these tests is verify the implementation of the ECDSA key generation and key verification operations. For the key generation, it is expected that the TOE generates a key pair based on the approved provided curve. This information is later verified using the known good implementation. For key verification, it is expected that the TOE verify the correctness of a set of given key pairs based on an approved curve.
   - For FFC:
     - Algorithm Functional Test (AFT). The main goal for these tests is verify the implementation of the FFC key generation and key verification operations. For the key generation, it is expected that the TOE generates a key pair based on the provided safe prime group. This information is later verified using the known good implementation.

2. The laboratory has exercised the cryptographic functionalities of the TOE by invoking the appropriate API in order to resolve the test vectors. The result of this step is a .json file which includes the associated response generated by the TOE per each test vector.

3. The laboratory has created a testing tool in order to exercise the BOTAN implementation for the target cryptographic algorithms. This tool receives the initial .json file with the test vectors as well as the .json file obtained as a result of the step 2. After parsing the information, the testing tool invokes the BOTAN implementation for the tested algorithm and resolve each test vector. After that, the testing tool compares both results (BOTAN vs TOE) in order to determine whether the cryptographic algorithms is properly implemented or not. The results of the testing tool is an individual outcome for each test vector (PASS or FAIL) and a overall outcome (PASS is all the test vectors passed or FAIL if any of them failed).

   - Note: Since the ffdhe groups are not available in BOTAN, the laboratory has demonstrated the correctness of the cryptographic algorithm implementation by using CAVP as a reference implementation instead of BOTAN.

11.2.1 Test (Key Generation for FIPS PUB 186-4 RSA Schemes)

11.2.1.1 Setup

The following environment is required to perform the test in addition to the TOE:

- A computer with:
  - Operating System: Ubuntu 20.04
  - BOTAN Tool is installed with CCN policy in evaluator machine;
  - Test vectors are located in evaluator machine.

For the installation of the *Botan Tool with CCN policy 2.15.2* all the steps defined in the *Botan-CCN_Manual_Implementador_v1* document have been followed.

11.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

11.2.1.3 Results

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

11.2.1.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the test activity demonstrate that the TOE provides a valid implementation for the evaluated cryptographic algorithm, since it has been compared against a well-known implementation (BOTAN) as a reference implementation.

Therefore, the **PASS** verdict is assigned to the Test RSA KeyGen activity.

11.2.2 Test (Key Generation for Elliptic Curve Cryptography (ECC))

11.2.2.1 Setup

The following environment is required to perform the test in addition to the TOE:

- A computer with:
  - Operating System: Ubuntu 20.04

  - BOTAN Tool is installed with CCN policy in evaluator machine;
  - Test vectors are located in evaluator machine.

For the installation of the *Botan Tool with CCN policy 2.15.2* all the steps defined in the *Botan-CCN_Manual_Implementador_v1* document have been followed.

11.2.2.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

11.2.2.3 Results

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

11.2.2.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the test activity demonstrate that the TOE provides a well implementation for the evaluated cryptographic algorithms, since they have been compared against a well-known implementation (BOTAN) as a reference implementation.

Therefore, the **PASS** verdict is assigned to the Test Key Generation for Elliptic Curve Cryptography (ECC) activity.

11.2.3 Test (Key Generation for Finite-Field Cryptography (FFC))

11.2.3.1 Setup

The following environment is required to perform the test in addition to the TOE:

- A computer with:
  - Operating System: Ubuntu 20.04
  - BOTAN Tool is installed with CCN policy in evaluator machine;
  - Test vectors are located in evaluator machine.

For the installation of the *Botan Tool with CCN policy 2.15.2* all the steps defined in the *Botan-CCN_Manual_Implementador_v1* document have been followed.

11.2.3.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

11.2.3.3 Results

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

11.2.3.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the test activity demonstrate that the TOE provides a well implementation for the evaluated cryptographic algorithm, since it has been compared against a well-known implementation (BOTAN) as a reference implementation.

For ffdhe groups, which are not available in BOTAN, the laboratory has followed the same approach but using the CAVP implementation as a reference instead of BOTAN. The evaluator has verified that the responses generated by the TOE are the same as the ones expected by the CAVP tool. Additionally, the associated CAVP certificates (listed in the tables included within the Documentation Review Activity section) have been granted demonstrating the correctness of the algorithm implementation.

Therefore, the **PASS** verdict is assigned to the Test Key Generation for Finite-Field Cryptography (FFC) activity.

11.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to this FCS_CKM.1.1 requirement.

12 FCS_CKM.2.1(1)

The assurance activity for the **FCS_CKM.2.1(1)** requirement is stated as follows:

> The evaluator will ensure that the supported key establishment schemes correspond to the key generation schemes identified in FCS_CKM.1.1. If the ST specifies more than one scheme, the evaluator will examine the TSS to verify that it identifies the usage for each scheme.
>
> The evaluator will verify that the AGD guidance instructs the administrator how to configure the OS to use the selected key establishment scheme(s).
>
> Evaluation Activity Note: The following tests require the developer to provide access to a test platform that provides the evaluator with tools that are typically not found on factory products.
>
> **Key Establishment Schemes**
>
> The evaluator will verify the implementation of the key establishment schemes supported by the OS using the applicable tests below.
>
> **SP800-56A Key Establishment Schemes**
>
> The evaluator will verify the OS's implementation of SP800-56A key agreement schemes using the following Function and Validity tests. These validation tests for each key agreement scheme verify that the OS has implemented the components of the key agreement scheme according to the specifications in the Recommendation. These components include the calculation of the discrete logarithm cryptography (DLC) primitives (the shared secret value Z) and the calculation of the derived keying material (DKM) via the Key Derivation Function (KDF). If key confirmation is supported, the evaluator will also verify that the components of key confirmation have been implemented correctly, using the test procedures described below. This includes the parsing of the DKM, the generation of MAC data and the calculation of MAC tag.
>
> **Function Test**
>
> The Function test verifies the ability of the OS to implement the key agreement schemes correctly. To conduct this test the evaluator will generate or obtain test vectors from a known good implementation of the OS's supported schemes. For each supported key agreement scheme-key agreement role combination, KDF type, and, if supported, key confirmation role- key confirmation type combination, the tester shall generate 10 sets of test vectors. The data set consists of the NIST approved curve (ECC) per 10 sets of public keys. These keys are static, ephemeral or both depending on the scheme being tested.
>
> The evaluator will obtain the DKM, the corresponding OS's public keys (static and/or ephemeral), the MAC tag(s), and any inputs used in the KDF, such as the Other Information field OI and OS id fields.

If the OS does not use a KDF defined in SP 800-56A, the evaluator will obtain only the public keys and the hashed value of the shared secret.

The evaluator will verify the correctness of the TSF's implementation of a given scheme by using a known good implementation to calculate the shared secret value, derive the keying material DKM, and compare hashes or MAC tags generated from these values.

If key confirmation is supported, the OS shall perform the above for each implemented approved MAC algorithm.

Validity Test

The Validity test verifies the ability of the OS to recognize another party's valid and invalid key agreement results with or without key confirmation. To conduct this test, the evaluator will obtain a list of the supporting cryptographic functions included in the SP800-56A key agreement implementation to determine which errors the OS should be able to recognize. The evaluator generates a set of 30 test vectors consisting of data sets including domain parameter values or NIST approved curves, the evaluator's public keys, the OS's public/private key pairs, MAC tag, and any inputs used in the KDF, such as the other info and OS id fields.

The evaluator will inject an error in some of the test vectors to test that the OS recognizes invalid key agreement results caused by the following fields being incorrect: the shared secret value Z, the DKM, the other information field OI, the data to be MAC'd, or the generated MAC tag. If the OS contains the full or partial (only ECC) public key validation, the evaluator will also individually inject errors in both parties' static public keys, both parties' ephemeral public keys and the OS's static private key to assure the OS detects errors in the public key validation function and/or the partial key validation function (in ECC only). At least two of the test vectors shall remain unmodified and therefore should result in valid key agreement results (they should pass).

The OS shall use these modified test vectors to emulate the key agreement scheme using the corresponding parameters. The evaluator will compare the OS's results with the results using a known good implementation verifying that the OS detects these errors.

SP800-56B Key Establishment Schemes

The evaluator will verify that the TSS describes whether the OS acts as a sender, a recipient, or both for RSA-based key establishment schemes.

If the OS acts as a sender, the following assurance activity shall be performed to ensure the proper operation of every OS supported combination of RSA-based key establishment scheme:

To conduct this test the evaluator will generate or obtain test vectors from a known good implementation of the OS's supported schemes. For each combination of sup-

ported key establishment scheme and its options (with or without key confirmation if supported, for each supported key confirmation MAC function if key confirmation is supported, and for each supported mask generation function if KTS-OAEP is supported), the tester shall generate 10 sets of test vectors. Each test vector shall include the RSA public key, the plaintext keying material, any additional input parameters if applicable, the MAC key and MAC tag if key confirmation is incorporated, and the outputted ciphertext. For each test vector, the evaluator shall perform a key establishment encryption operation on the OS with the same inputs (in cases where key confirmation is incorporated, the test shall use the MAC key from the test vector instead of the randomly generated MAC key used in normal operation) and ensure that the outputted ciphertext is equivalent to the ciphertext in the test vector.

If the OS acts as a receiver, the following evaluation activities shall be performed to ensure the proper operation of every OS supported combination of RSA-based key establishment scheme:

To conduct this test the evaluator will generate or obtain test vectors from a known good implementation of the OS's supported schemes. For each combination of supported key establishment scheme and its options (with our without key confirmation if supported, for each supported key confirmation MAC function if key confirmation is supported, and for each supported mask generation function if KTS-OAEP is supported), the tester shall generate 10 sets of test vectors. Each test vector shall include the RSA private key, the plaintext keying material, any additional input parameters if applicable, the MAC tag in cases where key confirmation is incorporated, and the outputted ciphertext. For each test vector, the evaluator will perform the key establishment decryption operation on the OS and ensure that the outputted plaintext keying material is equivalent to the plaintext keying material in the test vector. In cases where key confirmation is incorporated, the evaluator will perform the key confirmation steps and ensure that the outputted MAC tag is equivalent to the MAC tag in the test vector.

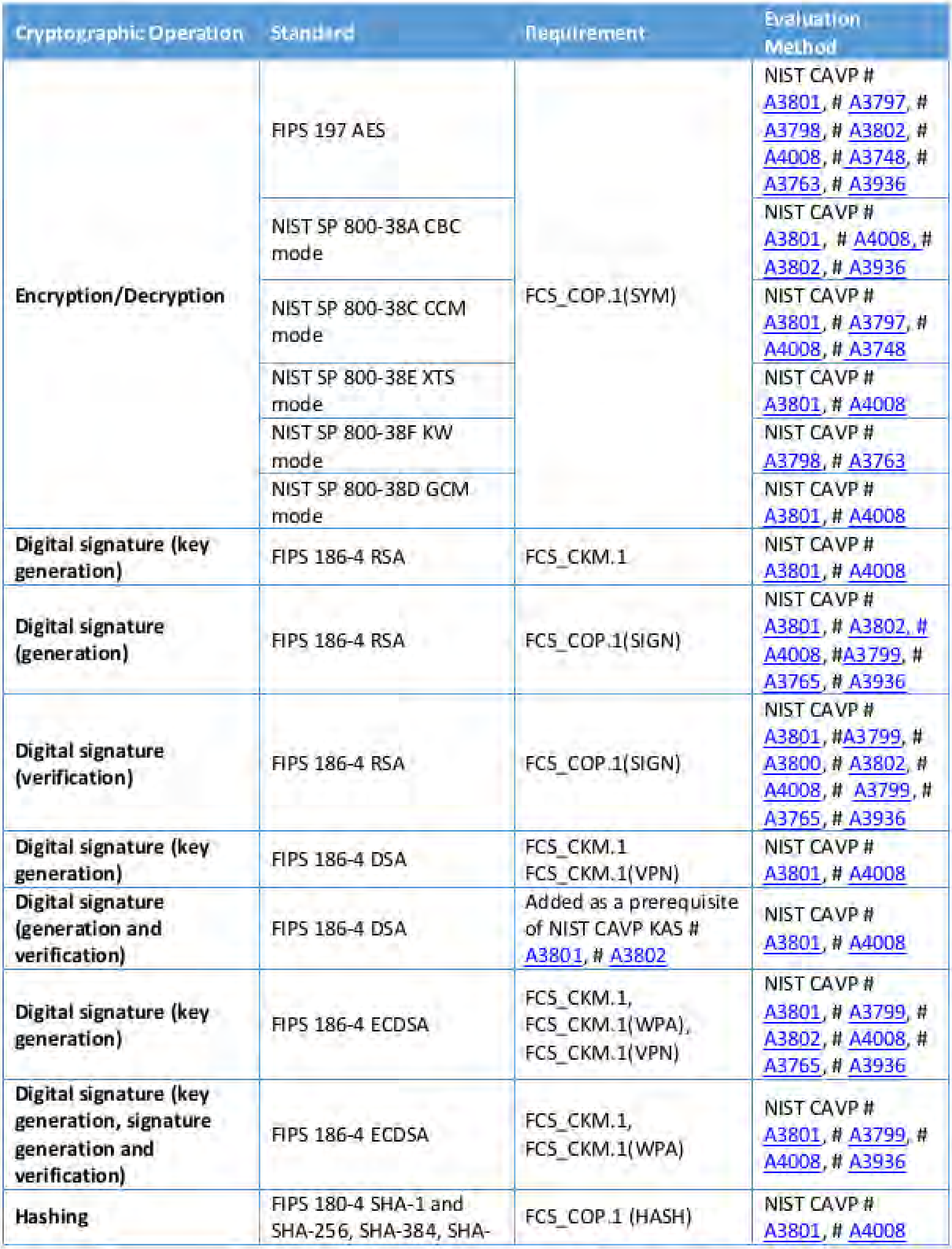
The evaluator will ensure that the TSS describes how the OS handles decryption errors. In accordance with NIST Special Publication 800-56B, the OS must not reveal the particular error that occurred, either through the contents of any outputted or logged error message or through timing variations. If KTS-OAEP is supported, the evaluator will create separate contrived ciphertext values that trigger each of the three decryption error checks described in NIST Special Publication 800-56B section 7.2.2.3, ensure that each decryption attempt results in an error, and ensure that any outputted or logged error message is identical for each. If KTS-KEM-KWS is supported, the evaluator will create separate contrived ciphertext values that trigger each of the three decryption error checks described in NIST Special Publication 800-56B section 7.2.3.3, ensure that each decryption attempt results in an error, and ensure that any outputted or logged error message is identical for each.

12.1 Documentation Review Activity

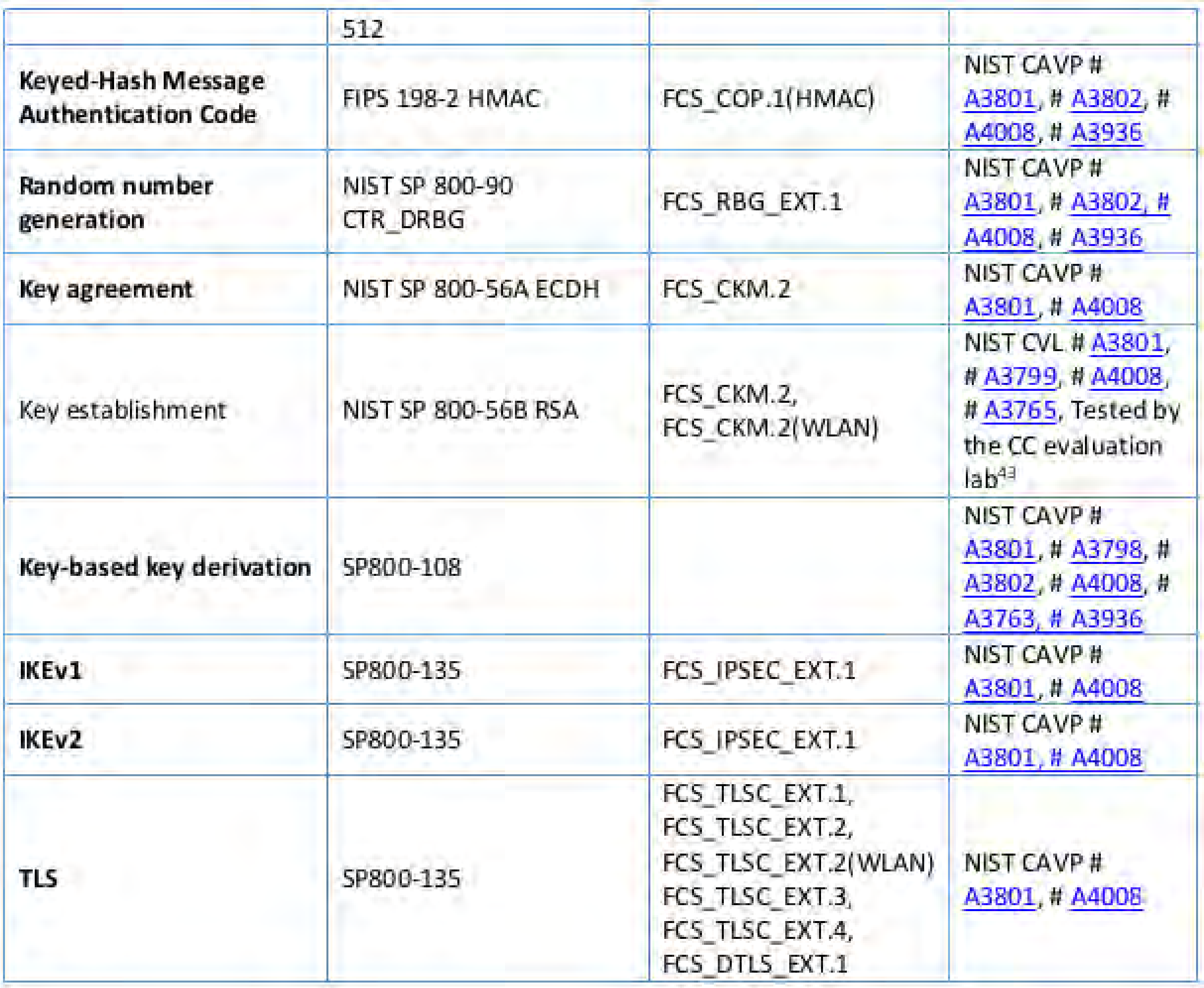
12.1.1 Findings

The evaluator has reviewed the ***Security Target*** document and the information provided in the TSS, section **6.2.2 Cryptographic Algorithm Validation**. This section includes the following tables of the cryptographic algorithms supported by Windows 11, Windows 10 versions, Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge.

12.1.1.1 Cryptographic Algorithm Standards and Evaluation Methods for Windows 11 (version 22H2)

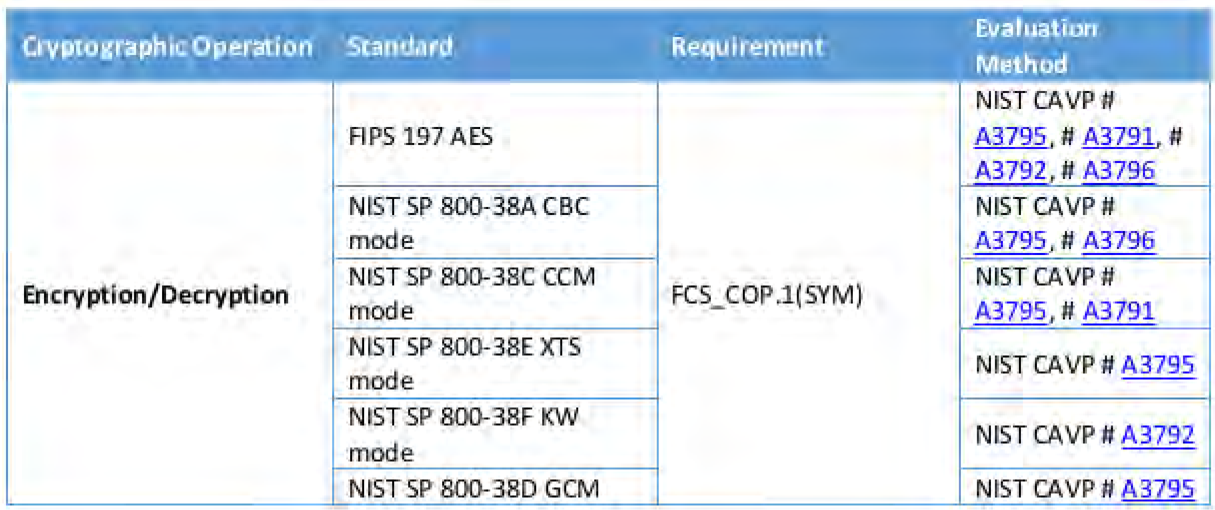


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3801, # A3797, # A3798, # A3802, # A4008, # A3748, # A3763, # A3936
	NIST SP 800-38A CBC mode		NIST CAVP # A3801, # A4008, # A3802, # A3936
	NIST SP 800-38C CCM mode		NIST CAVP # A3801, # A3797, # A4008, # A3748
	NIST SP 800-38E XTS mode		NIST CAVP # A3801, # A4008
	NIST SP 800-38F KW mode		NIST CAVP # A3798, # A3763
	NIST SP 800-38D GCM mode		NIST CAVP # A3801, # A4008
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP # A3801, # A4008
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3801, # A3802, # A4008, #A3799, # A3765, # A3936
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3801, #A3799, # A3800, # A3802, # A4008, # A3799, # A3765, # A3936
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3801, # A4008
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3801, # A3802	NIST CAVP # A3801, # A4008
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3801, # A3799, # A3802, # A4008, # A3765, # A3936
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3801, # A3799, # A4008, # A3936
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-	FCS_COP.1 (HASH)	NIST CAVP # A3801, # A4008

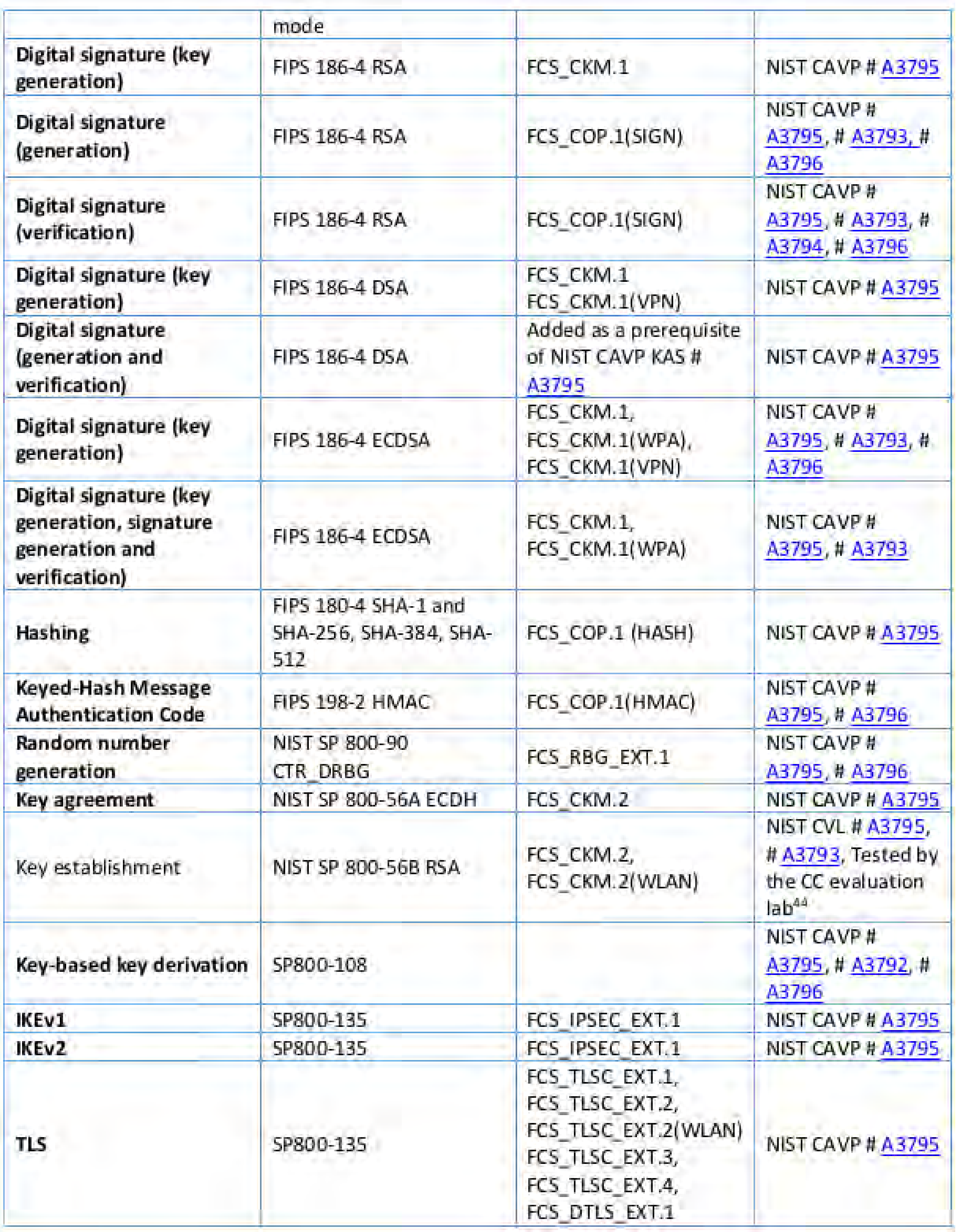


	512		
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3801, # A3802, # A4008, # A3936
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3801, # A3802, # A4008, # A3936
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3801, # A4008
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2, FCS_CKM.2(WLAN)	NIST CVL # A3801, # A3799, # A4008, # A3765, Tested by the CC evaluation lab[43]
Key-based key derivation	SP800-108		NIST CAVP # A3801, # A3798, # A3802, # A4008, # A3763, # A3936
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3801, # A4008
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3801, # A4008
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3801, # A4008

12.1.1.2 Cryptographic Algorithm Standards and Evaluation Methods for Windows 10 (version 22H2)

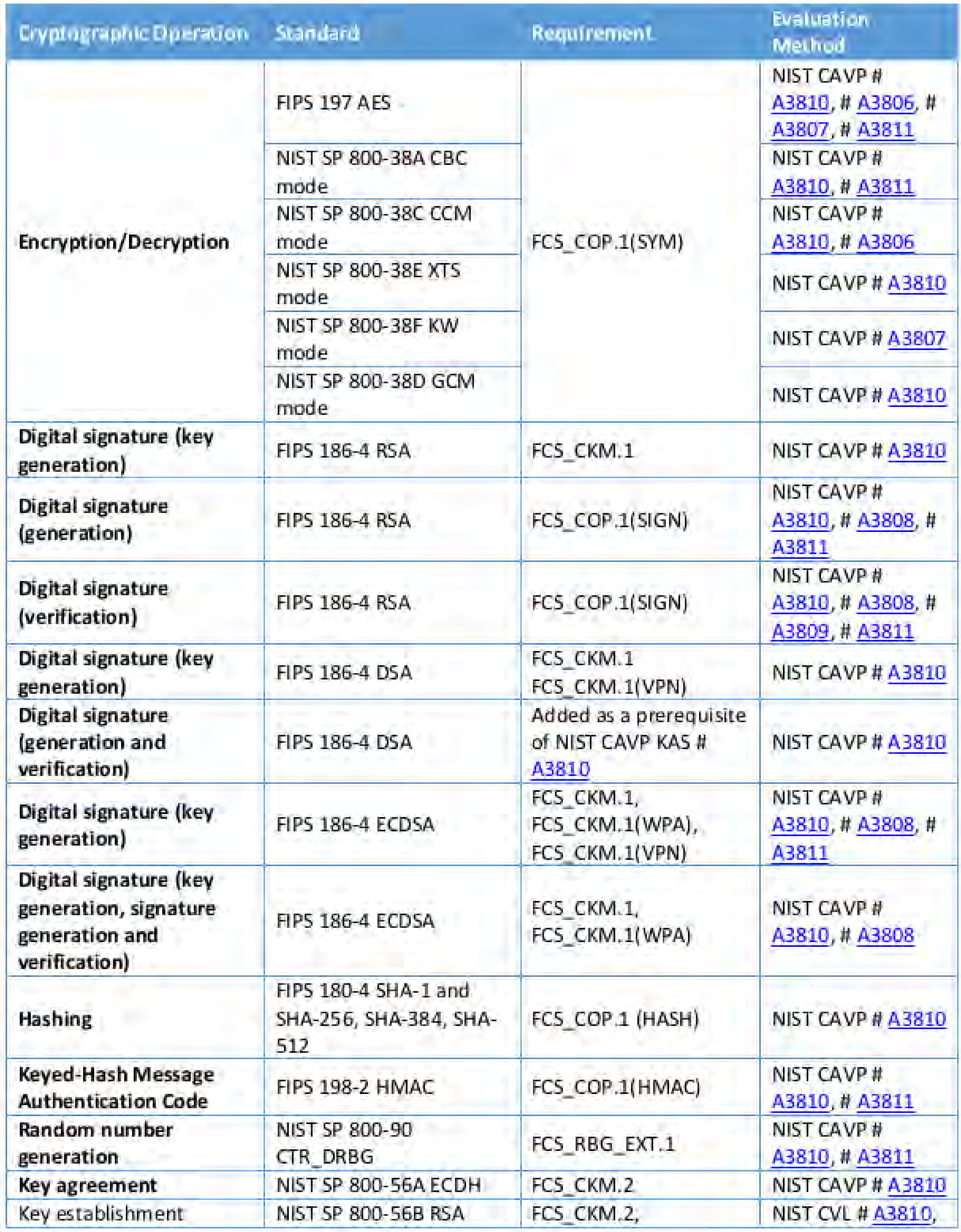


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3795, # A3791, # A3792, # A3796
	NIST SP 800-38A CBC mode		NIST CAVP # A3795, # A3796
	NIST SP 800-38C CCM mode		NIST CAVP # A3795, # A3791
	NIST SP 800-38E XTS mode		NIST CAVP # A3795
	NIST SP 800-38F KW mode		NIST CAVP # A3792
	NIST SP 800-38D GCM		NIST CAVP # A3795

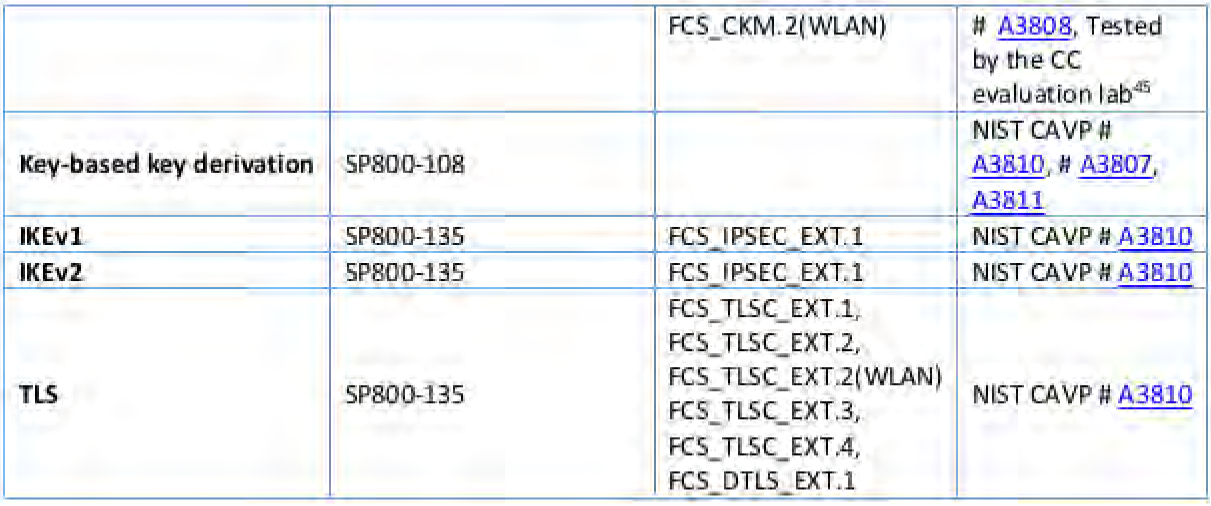


	mode		
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP # A3795
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3795, # A3793, # A3796
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3795, # A3793, # A3794, # A3796
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3795
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3795	NIST CAVP # A3795
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3795, # A3793, # A3796
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3795, # A3793
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3795
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3795, # A3796
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3795, # A3796
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3795
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2, FCS_CKM.2(WLAN)	NIST CVL # A3795, # A3793, Tested by the CC evaluation lab[44]
Key-based key derivation	SP800-108		NIST CAVP # A3795, # A3792, # A3796
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3795
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3795
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3795

12.1.1.3 Cryptographic Algorithm Standards and Evaluation Methods for Windows Server 2022 and Windows Server Datacenter: Azure Edition

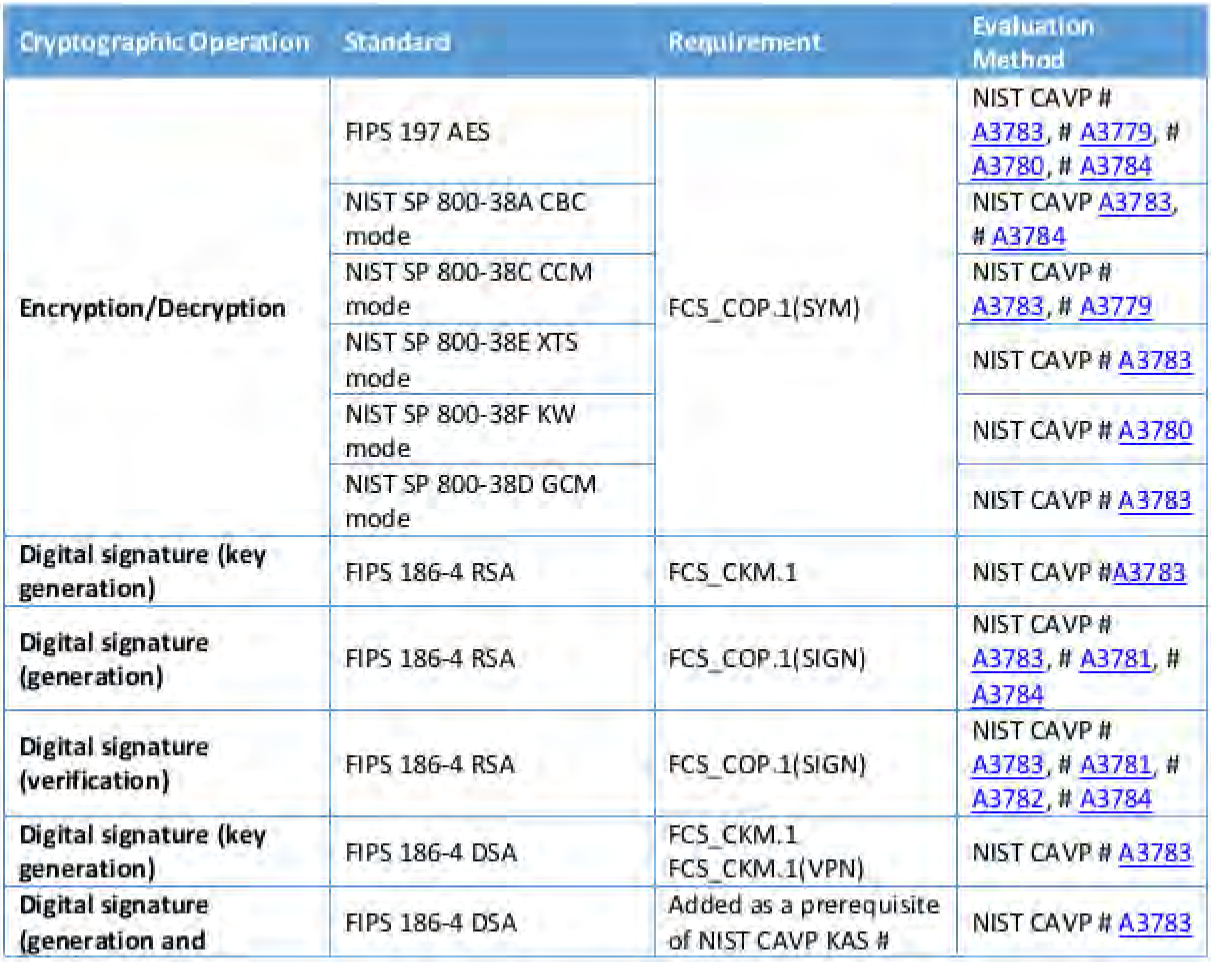


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3810, # A3806, # A3807, # A3811
	NIST SP 800-38A CBC mode		NIST CAVP # A3810, # A3811
	NIST SP 800-38C CCM mode		NIST CAVP # A3810, # A3806
	NIST SP 800-38E XTS mode		NIST CAVP # A3810
	NIST SP 800-38F KW mode		NIST CAVP # A3807
	NIST SP 800-38D GCM mode		NIST CAVP # A3810
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP # A3810
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3810, # A3808, # A3811
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3810, # A3808, # A3809, # A3811
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3810
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3810	NIST CAVP # A3810
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3810, # A3808, # A3811
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3810, # A3808
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3810
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3810, # A3811
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3810, # A3811
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3810
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2,	NIST CVL # A3810,

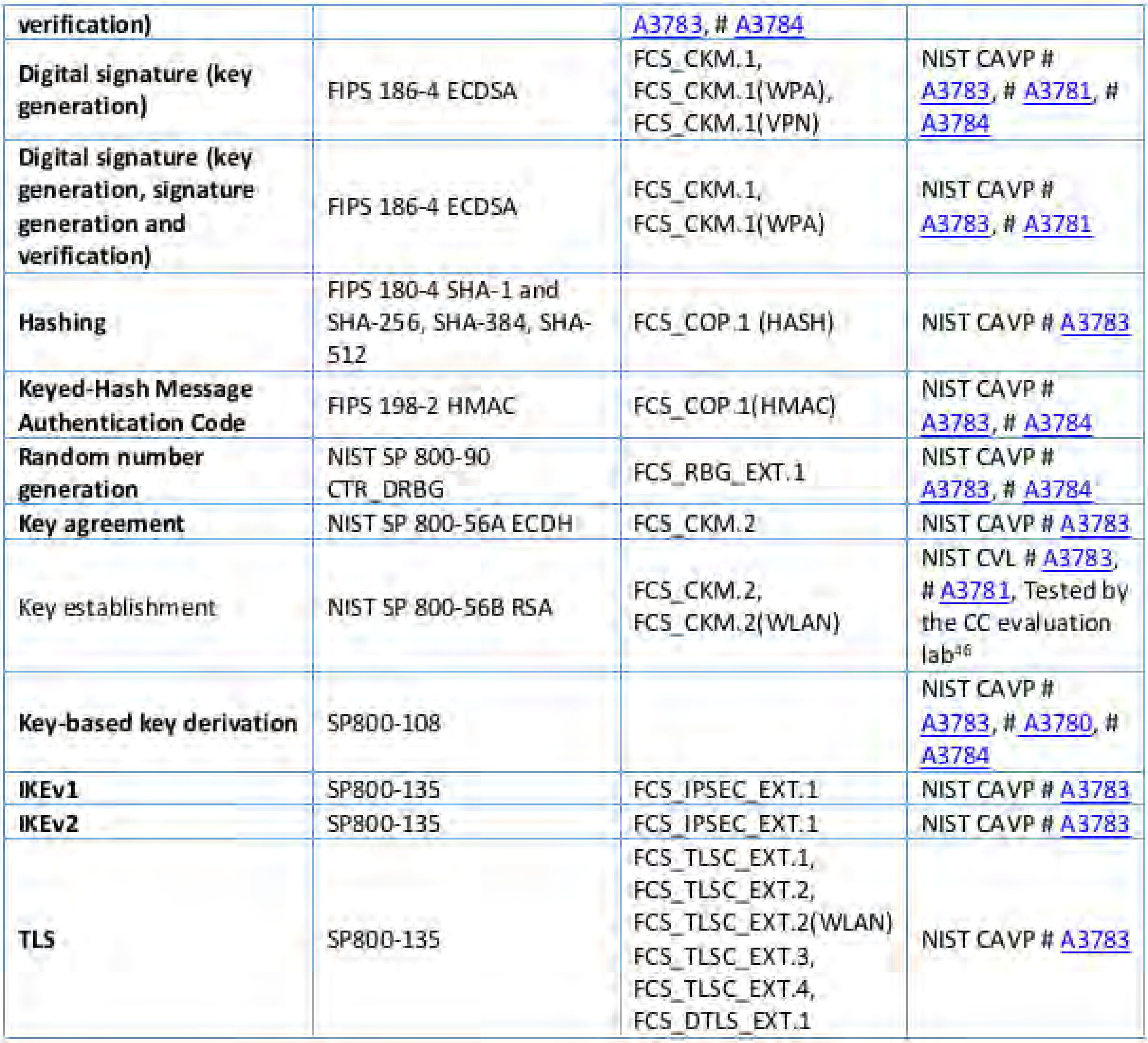


		FCS_CKM.2(WLAN)	# A3808, Tested by the CC evaluation lab[45]
Key-based key derivation	SP800-108		NIST CAVP # A3810, # A3807, A3811
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3810
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3810
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3810

12.1.1.4 Cryptographic Algorithm Standards and Evaluation Methods for Windows Server Azure Stack HCIv2 version 22H2

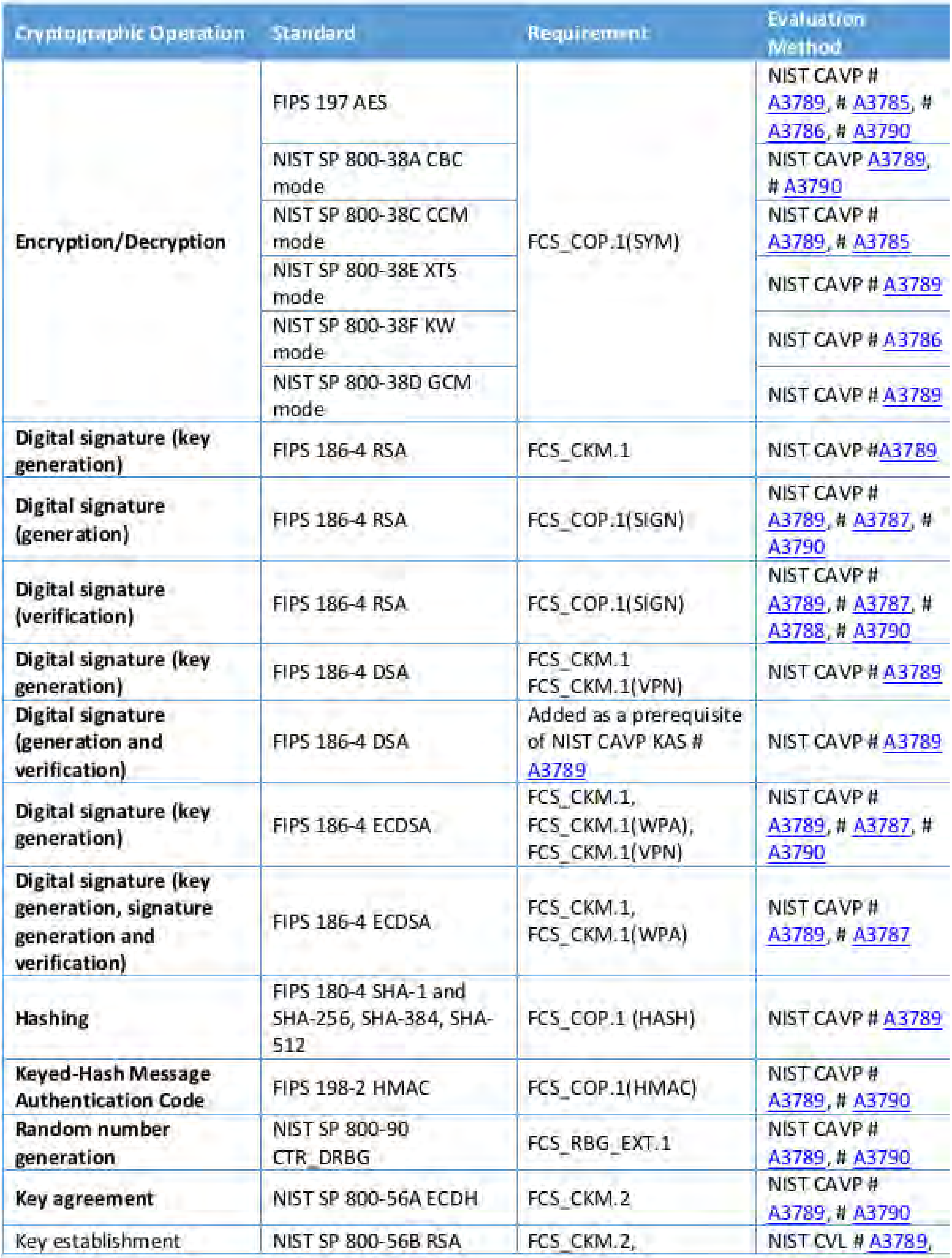


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3783, # A3779, # A3780, # A3784
	NIST SP 800-38A CBC mode		NIST CAVP A3783, # A3784
	NIST SP 800-38C CCM mode		NIST CAVP # A3783, # A3779
	NIST SP 800-38E XTS mode		NIST CAVP # A3783
	NIST SP 800-38F KW mode		NIST CAVP # A3780
	NIST SP 800-38D GCM mode		NIST CAVP # A3783
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP #A3783
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3783, # A3781, # A3784
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3783, # A3781, # A3782, # A3784
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3783
Digital signature (generation and	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS #	NIST CAVP # A3783

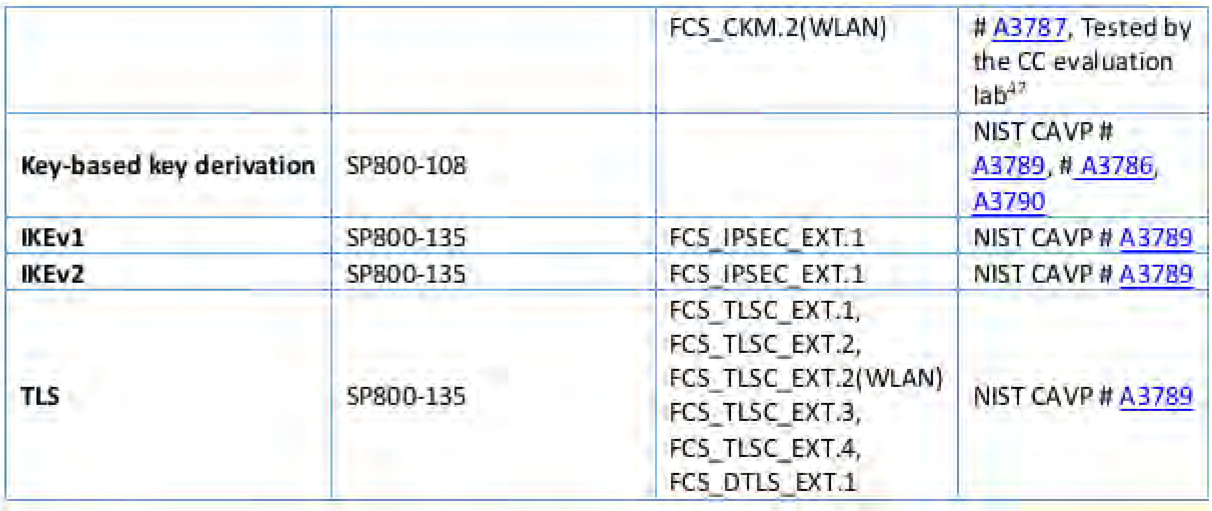


verification)		A3783, # A3784	
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3783, # A3781, # A3784
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3783, # A3781
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3783
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3783, # A3784
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3783, # A3784
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3783
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2, FCS_CKM.2(WLAN)	NIST CVL # A3783, # A3781, Tested by the CC evaluation lab[46]
Key-based key derivation	SP800-108		NIST CAVP # A3783, # A3780, # A3784
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3783
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3783
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3783

12.1.1.5 Cryptographic Algorithm Standards and Evaluation Methods for Azure Stack Hub and Azure Stack Edge



Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3789, # A3785, # A3786, # A3790
	NIST SP 800-38A CBC mode		NIST CAVP A3789, # A3790
	NIST SP 800-38C CCM mode		NIST CAVP # A3789, # A3785
	NIST SP 800-38E XTS mode		NIST CAVP # A3789
	NIST SP 800-38F KW mode		NIST CAVP # A3786
	NIST SP 800-38D GCM mode		NIST CAVP # A3789
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP #A3789
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3789, # A3787, # A3790
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3789, # A3787, # A3788, # A3790
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3789
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3789	NIST CAVP # A3789
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3789, # A3787, # A3790
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3789, # A3787
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3789
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3789, # A3790
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3789, # A3790
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3789, # A3790
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2,	NIST CVL # A3789,



		FCS_CKM.2(WLAN)	# A3787, Tested by the CC evaluation lab[47]
Key-based key derivation	SP800-108		NIST CAVP # A3789, # A3786, A3790
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3789
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3789
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3789

The vendor has specified the NIST CAVP certificates, where it is defined the key establishment scheme met for the fulfilment of the Special Publication *800-56A*.

The TSS distinguishes between three key establishment schemes: Diffie-Hellamand, the elliptic curve Diffie-Hellman (both used as part of TLS and IKE protocols) and the RSA-based which is used for establishing a shared secret key (the TOE can act both as a sender or recipient).

In addition, for the RSA-based key establishment scheme (*SP 800-56B*) the TSS states that, any decryption errors which occur during key establishment are presented to the user at a highly abstracted level.

The ***Operational Guidance*** document, states that for the evaluated version the following security policy needs to be applied (Section 3.2.5):

- Local Policies \ Security Options\System cryptography: Use FIPS 140 compliant cryptographic algorithms, including encryption, hashing and signing algorithm.

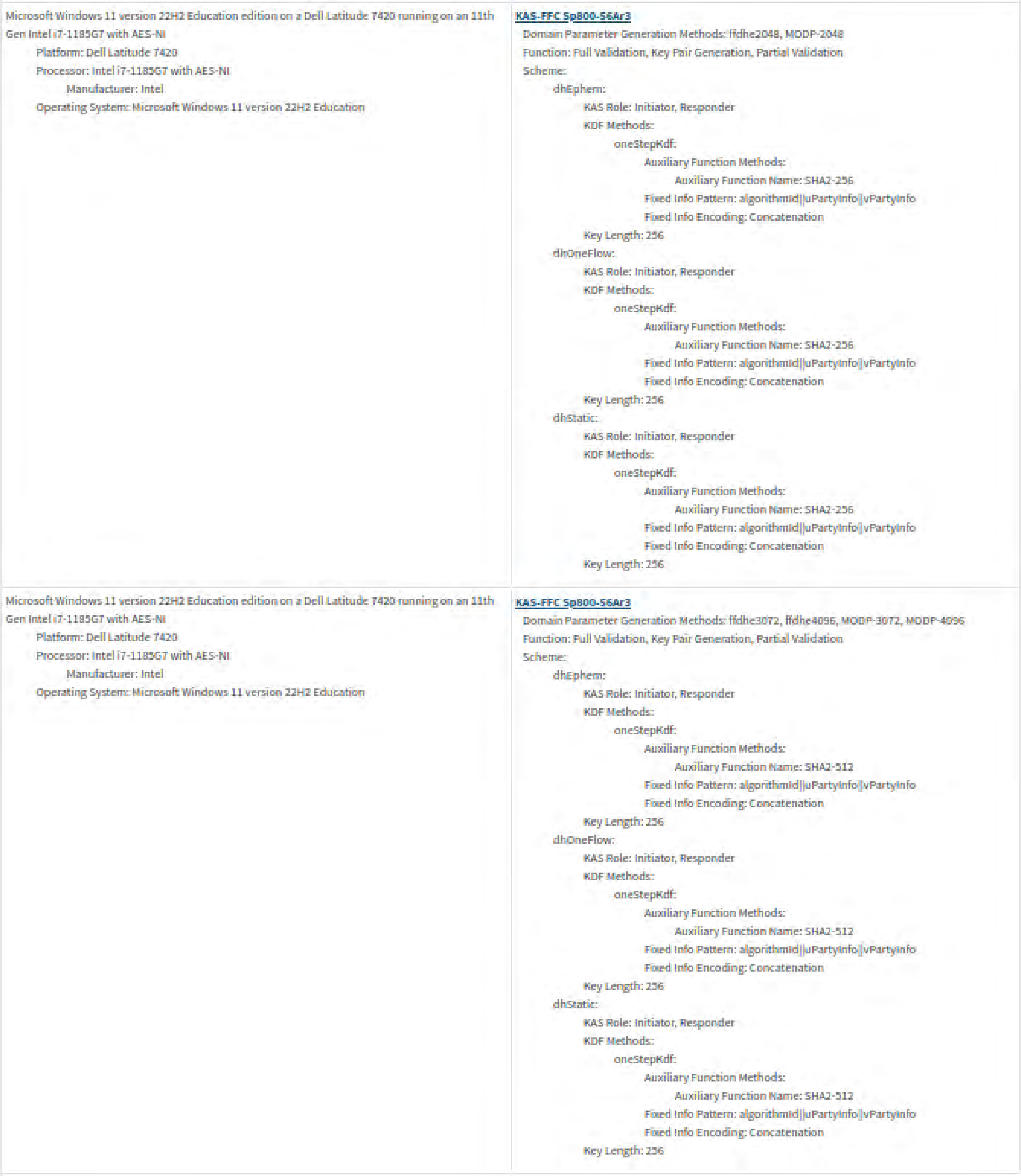
After applying this policy, only FIPS certified algorithms can be used, including the key agreement algorithms defined in the above table. In addition, the vendor has included the following wording, specifying that no further configuration is needed:

> *Windows performs RSA-based key establishment that meet NIST SP 800-56B, no configuration is necessary.*
>
> *Windows performs elliptic curve-based key schemes that meet NIST SP 800-56A, no configuration is necessary.*

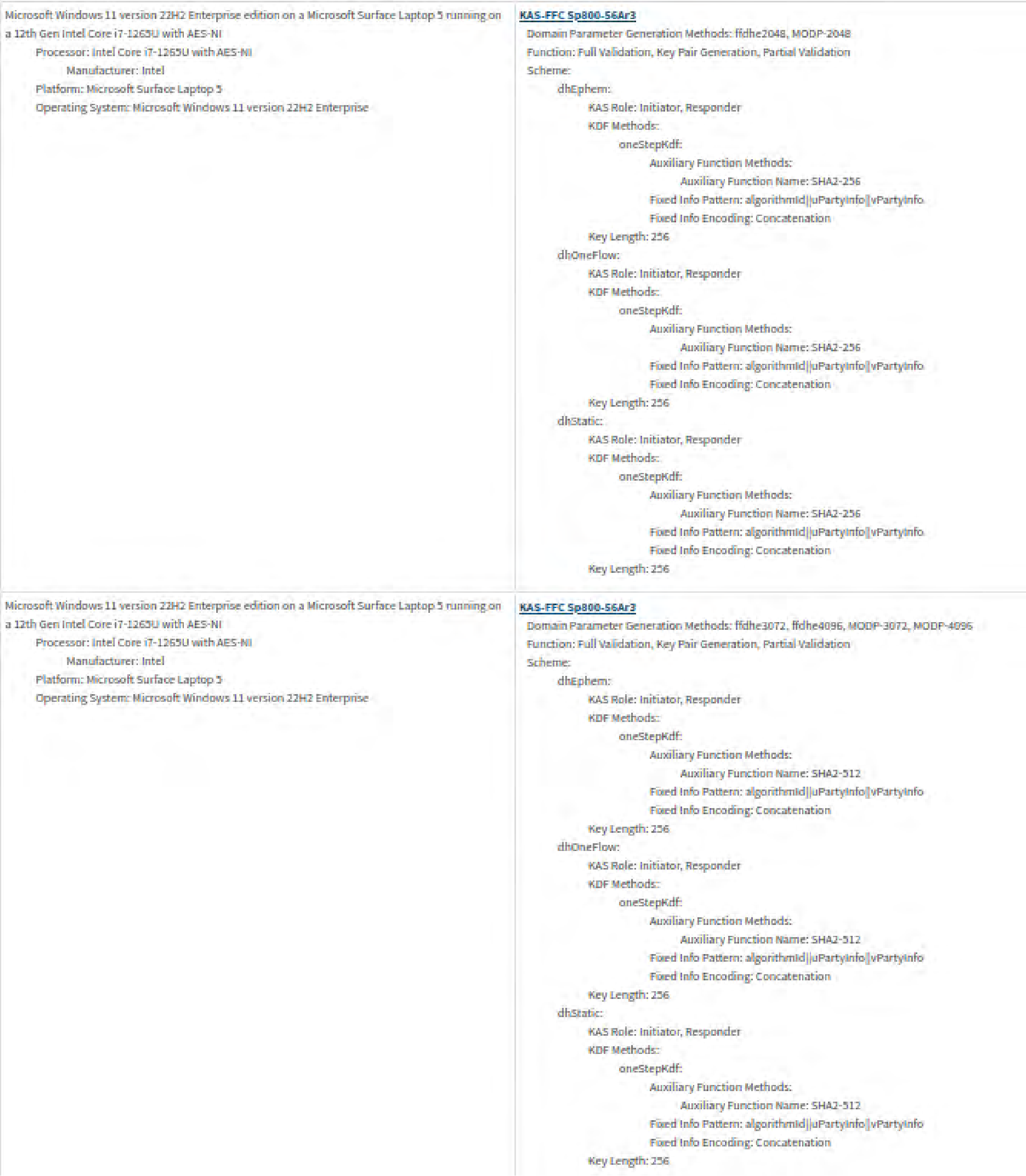
As to the Diffie-Hellman, the TSS also includes the key establishment using group 14 as required per IPSec connections. The TOE satisfies the fulfilment of the key establishment scheme *Diffie-Hellman group 14* as specified in the ***Security Target*** document. A complete explanation is provided with more detail in the *FCS_IPSEC_EXT.1.8* requirement.

Moreover, and as part of the testing activity described below, the correctness of the Diffie-Hellman cryptographic functionality has been demonstrated against the BOTAN tool. However, key establishment schemes using ffdhe groups are not available in BOTAN, and the laboratory has verified the implementation against the CAVP tool. Below, the CAVP certificates granted for this functionality are listed (extracted from the tables above)

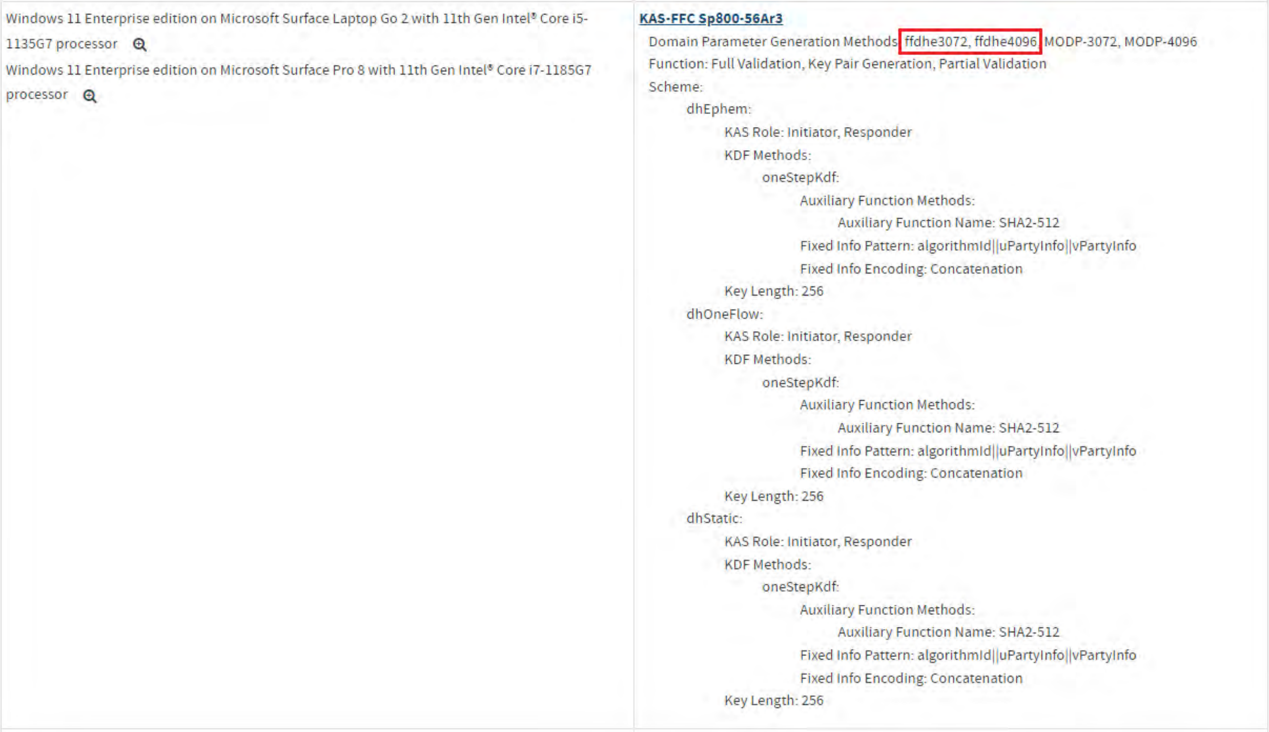
12.1.1.6 Windows 11 version 22H2 (CAVP Cert. #A4008)



Microsoft Windows 11 version 22H2 Education edition on a Dell Latitude 7420 running on an 11th Gen Intel i7-1185G7 with AES-NI Platform: Dell Latitude 7420 Processor: Intel i7-1185G7 with AES-NI Manufacturer: Intel Operating System: Microsoft Windows 11 version 22H2 Education	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe2048, MODP-2048 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256
Microsoft Windows 11 version 22H2 Education edition on a Dell Latitude 7420 running on an 11th Gen Intel i7-1185G7 with AES-NI Platform: Dell Latitude 7420 Processor: Intel i7-1185G7 with AES-NI Manufacturer: Intel Operating System: Microsoft Windows 11 version 22H2 Education	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe3072, ffdhe4096, MODP-3072, MODP-4096 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256



Microsoft Windows 11 version 22H2 Enterprise edition on a Microsoft Surface Laptop 5 running on a 12th Gen Intel Core i7-1265U with AES-NI Processor: Intel Core i7-1265U with AES-NI Manufacturer: Intel Platform: Microsoft Surface Laptop 5 Operating System: Microsoft Windows 11 version 22H2 Enterprise	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe2048, MODP-2048 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256
Microsoft Windows 11 version 22H2 Enterprise edition on a Microsoft Surface Laptop 5 running on a 12th Gen Intel Core i7-1265U with AES-NI Processor: Intel Core i7-1265U with AES-NI Manufacturer: Intel Platform: Microsoft Surface Laptop 5 Operating System: Microsoft Windows 11 version 22H2 Enterprise	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe3072, ffdhe4096, MODP-3072, MODP-4096 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256

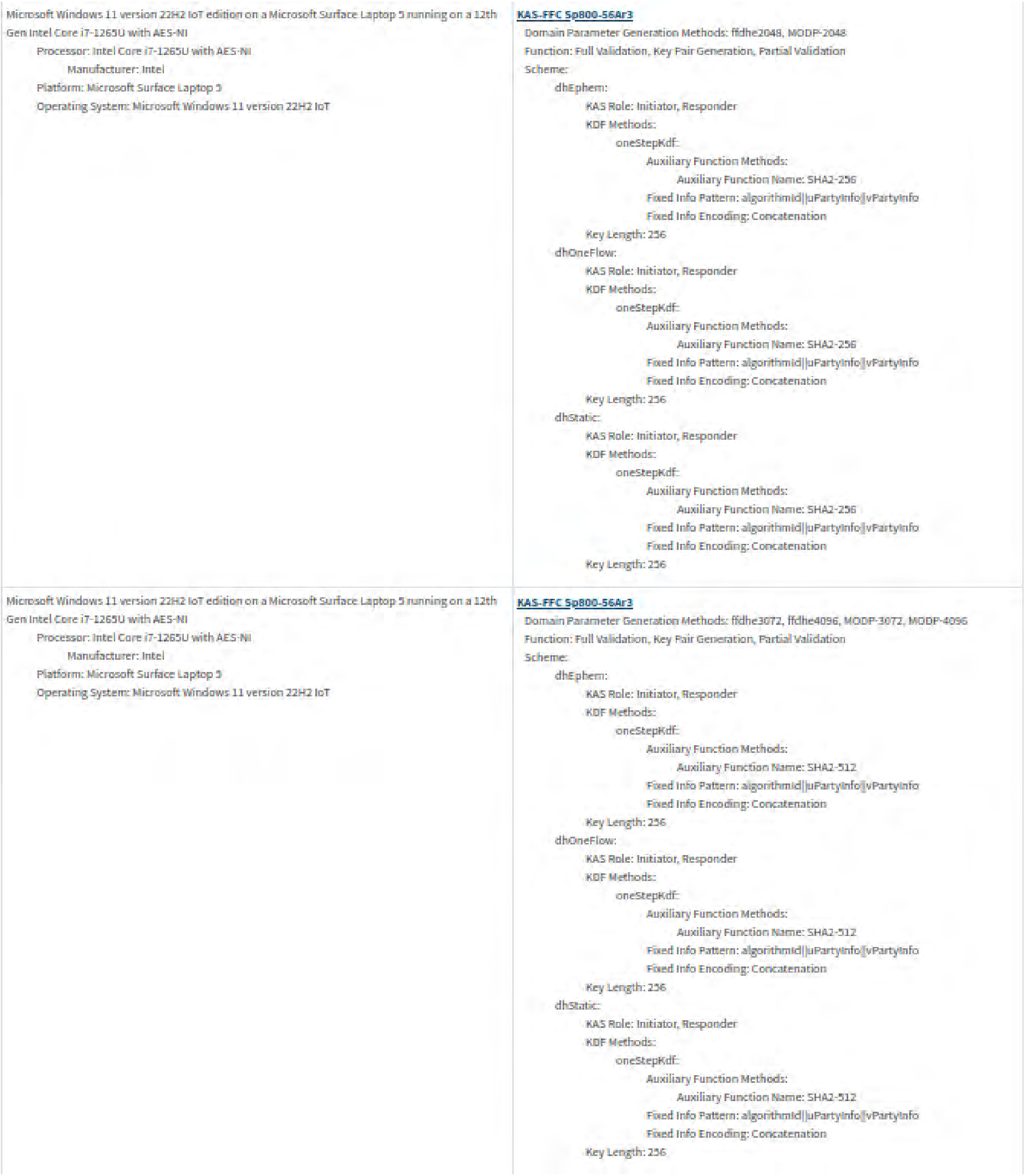


Windows 11 Enterprise edition on Microsoft Surface Laptop Go 2 with 11th Gen Intel® Core i5-1135G7 processor

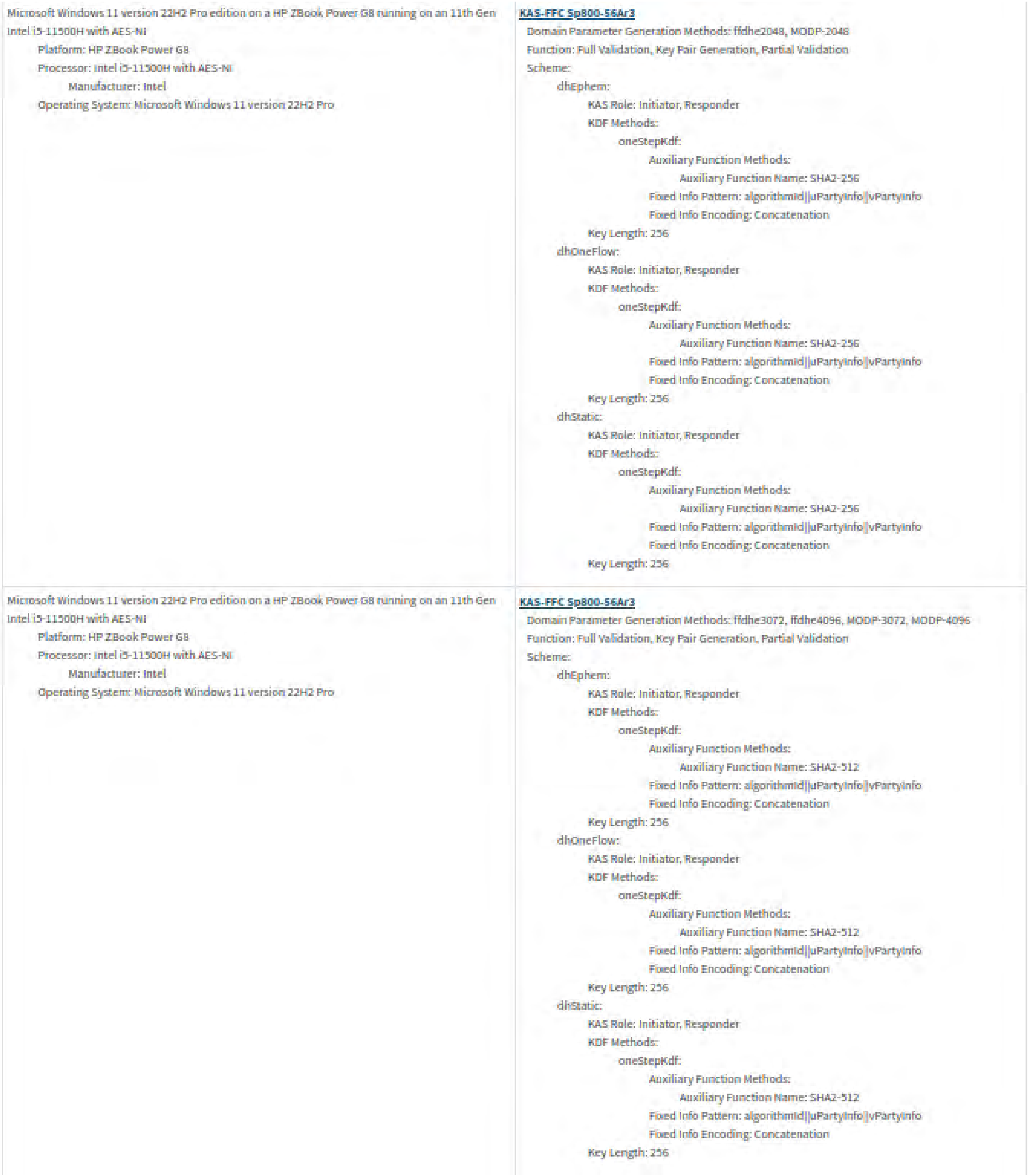
Windows 11 Enterprise edition on Microsoft Surface Pro 8 with 11th Gen Intel® Core i7-1185G7 processor

KAS-FFC Sp800-56Ar3

- Domain Parameter Generation Methods: ffdhe3072, ffdhe4096, MODP-3072, MODP-4096
- Function: Full Validation, Key Pair Generation, Partial Validation
- Scheme:
  - dhEphem:
    - KAS Role: Initiator, Responder
    - KDF Methods:
      - oneStepKdf:
        - Auxiliary Function Methods:
          - Auxiliary Function Name: SHA2-512
        - Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo
        - Fixed Info Encoding: Concatenation
    - Key Length: 256
  - dhOneFlow:
    - KAS Role: Initiator, Responder
    - KDF Methods:
      - oneStepKdf:
        - Auxiliary Function Methods:
          - Auxiliary Function Name: SHA2-512
        - Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo
        - Fixed Info Encoding: Concatenation
    - Key Length: 256
  - dhStatic:
    - KAS Role: Initiator, Responder
    - KDF Methods:
      - oneStepKdf:
        - Auxiliary Function Methods:
          - Auxiliary Function Name: SHA2-512
        - Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo
        - Fixed Info Encoding: Concatenation
    - Key Length: 256

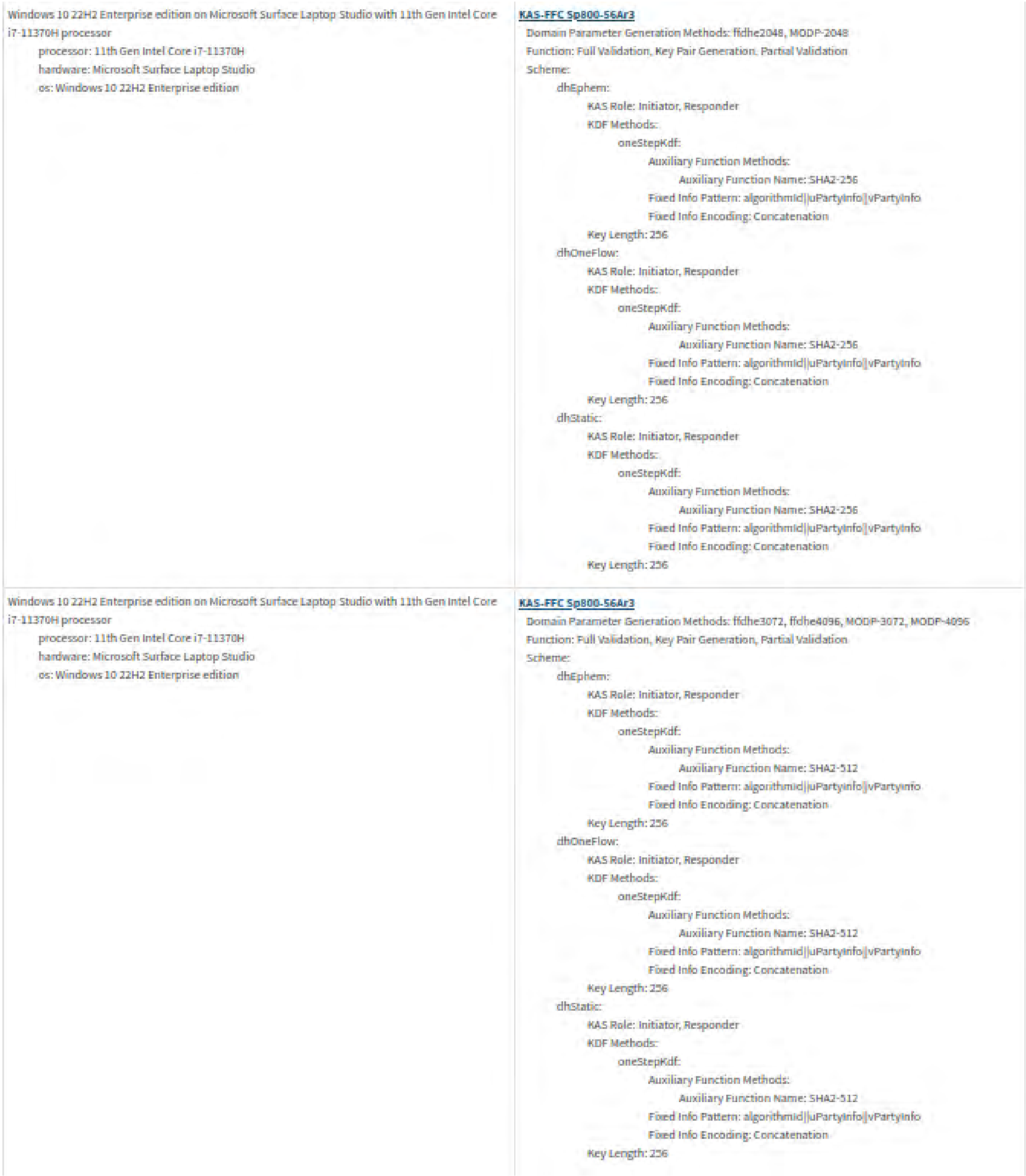


Microsoft Windows 11 version 22H2 IoT edition on a Microsoft Surface Laptop 5 running on a 12th Gen Intel Core i7-1265U with AES-NI Processor: Intel Core i7-1265U with AES-NI Manufacturer: Intel Platform: Microsoft Surface Laptop 5 Operating System: Microsoft Windows 11 version 22H2 IoT	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe2048, MODP-2048 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256
Microsoft Windows 11 version 22H2 IoT edition on a Microsoft Surface Laptop 5 running on a 12th Gen Intel Core i7-1265U with AES-NI Processor: Intel Core i7-1265U with AES-NI Manufacturer: Intel Platform: Microsoft Surface Laptop 5 Operating System: Microsoft Windows 11 version 22H2 IoT	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe3072, ffdhe4096, MODP-3072, MODP-4096 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256

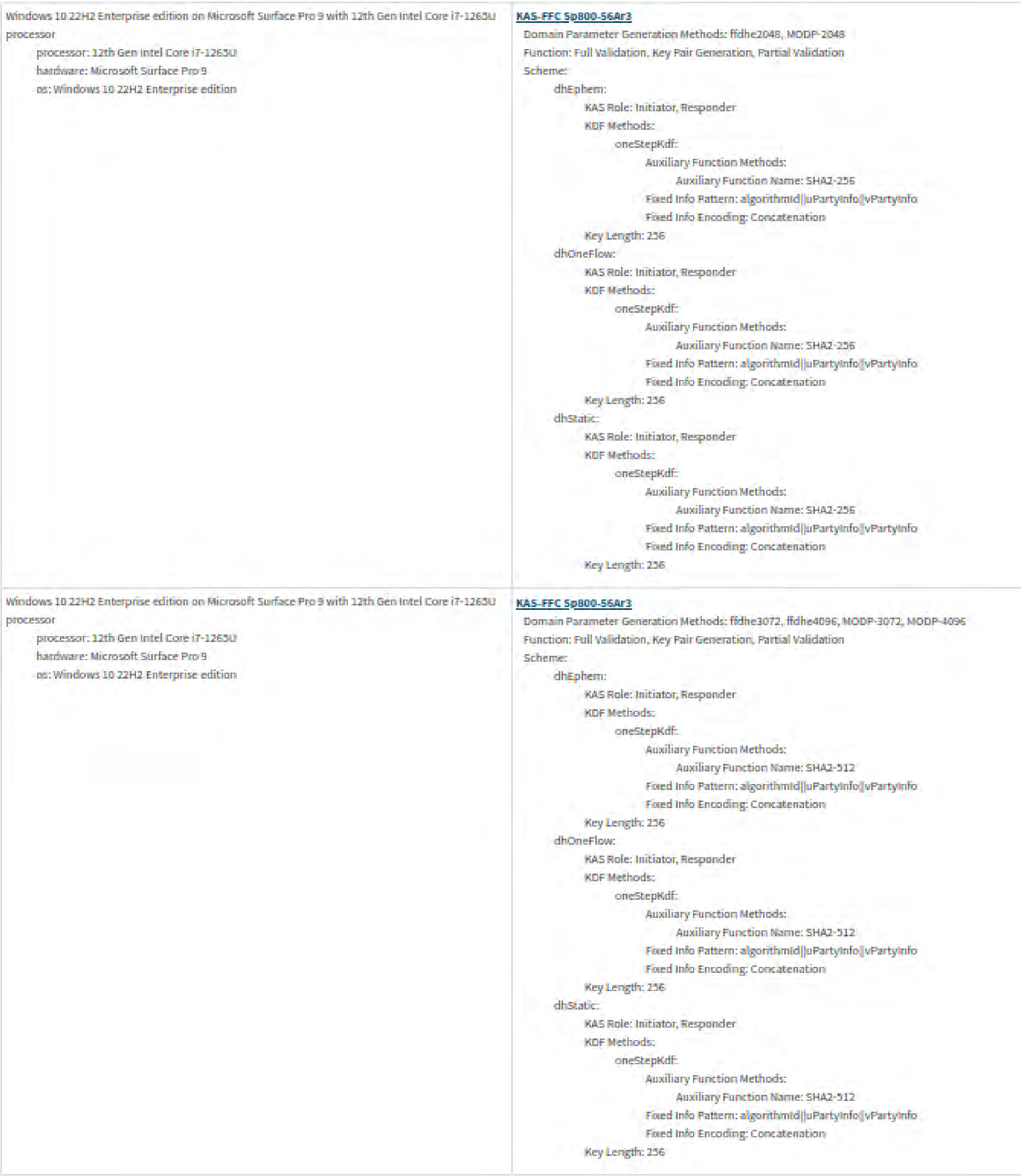


Microsoft Windows 11 version 22H2 Pro edition on a HP ZBook Power G8 running on an 11th Gen Intel i5-11500H with AES-NI Platform: HP ZBook Power G8 Processor: Intel i5-11500H with AES-NI Manufacturer: Intel Operating System: Microsoft Windows 11 version 22H2 Pro	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe2048, MODP-2048 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256
Microsoft Windows 11 version 22H2 Pro edition on a HP ZBook Power G8 running on an 11th Gen Intel i5-11500H with AES-NI Platform: HP ZBook Power G8 Processor: Intel i5-11500H with AES-NI Manufacturer: Intel Operating System: Microsoft Windows 11 version 22H2 Pro	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe3072, ffdhe4096, MODP-3072, MODP-4096 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256

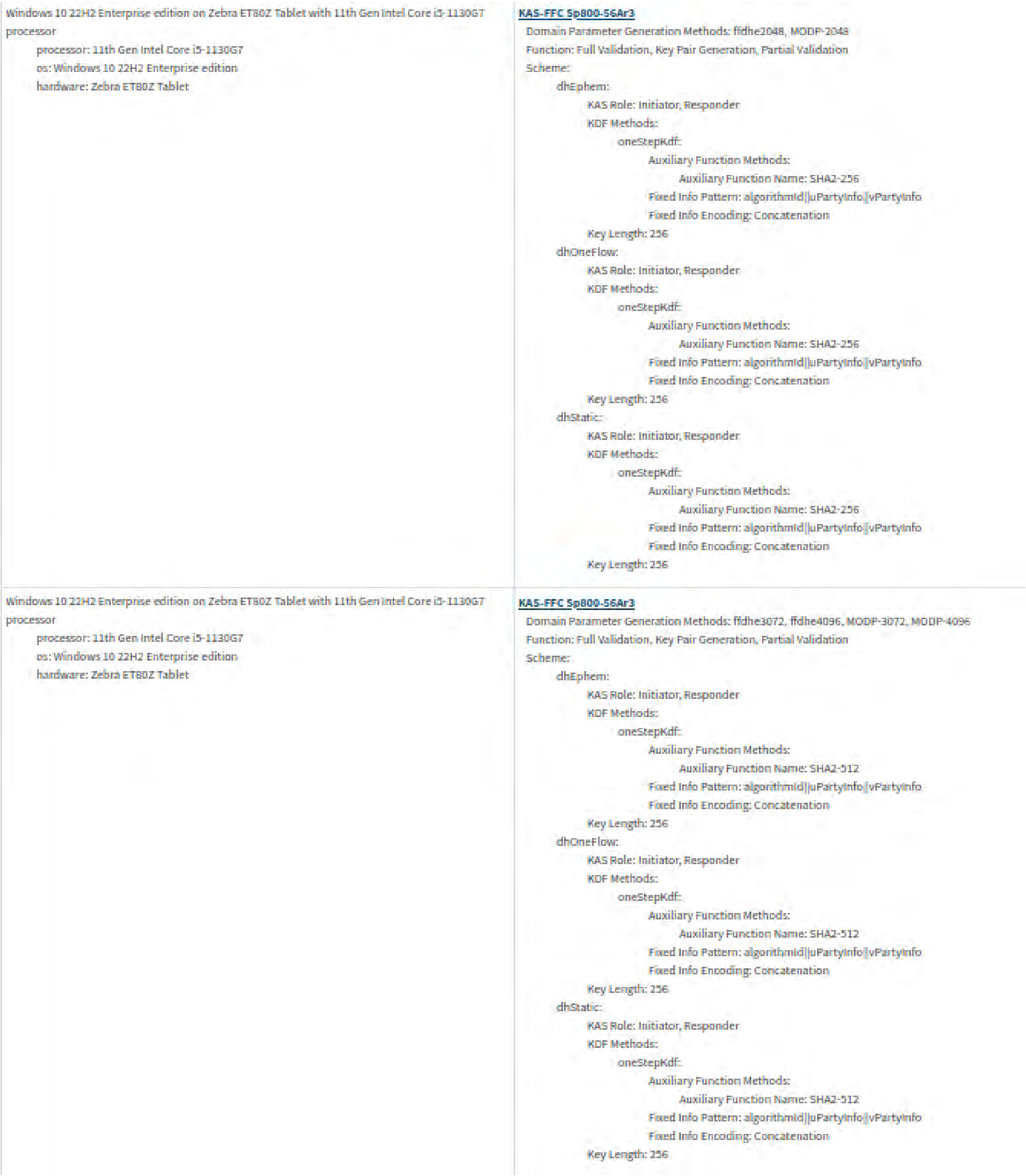
12.1.1.7 Windows 10 version 22H2 (CAVP Cert. #A3795)



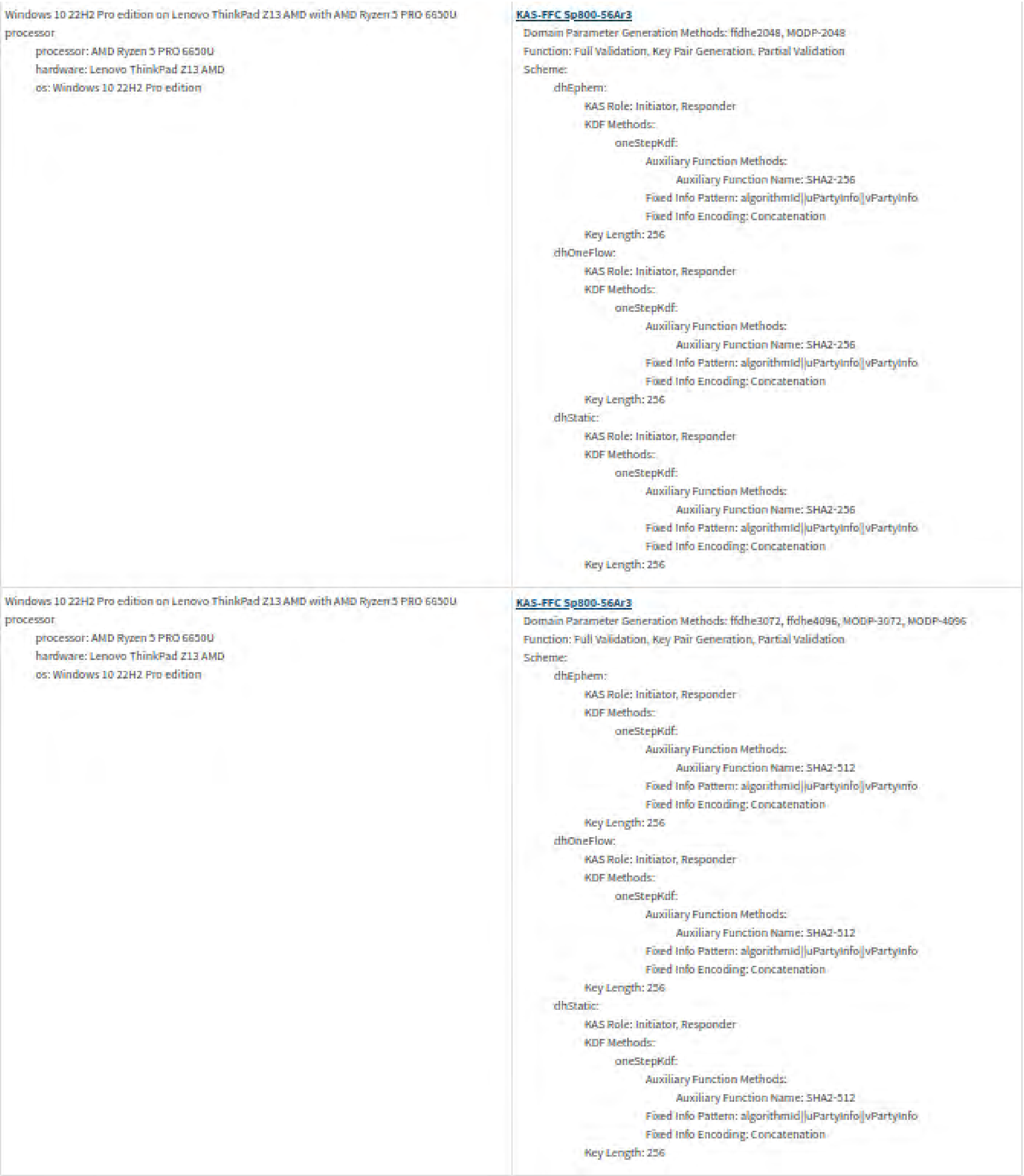
Windows 10 22H2 Enterprise edition on Microsoft Surface Laptop Studio with 11th Gen Intel Core i7-11370H processor processor: 11th Gen Intel Core i7-11370H hardware: Microsoft Surface Laptop Studio os: Windows 10 22H2 Enterprise edition	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe2048, MODP-2048 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256
Windows 10 22H2 Enterprise edition on Microsoft Surface Laptop Studio with 11th Gen Intel Core i7-11370H processor processor: 11th Gen Intel Core i7-11370H hardware: Microsoft Surface Laptop Studio os: Windows 10 22H2 Enterprise edition	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe3072, ffdhe4096, MODP-3072, MODP-4096 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256



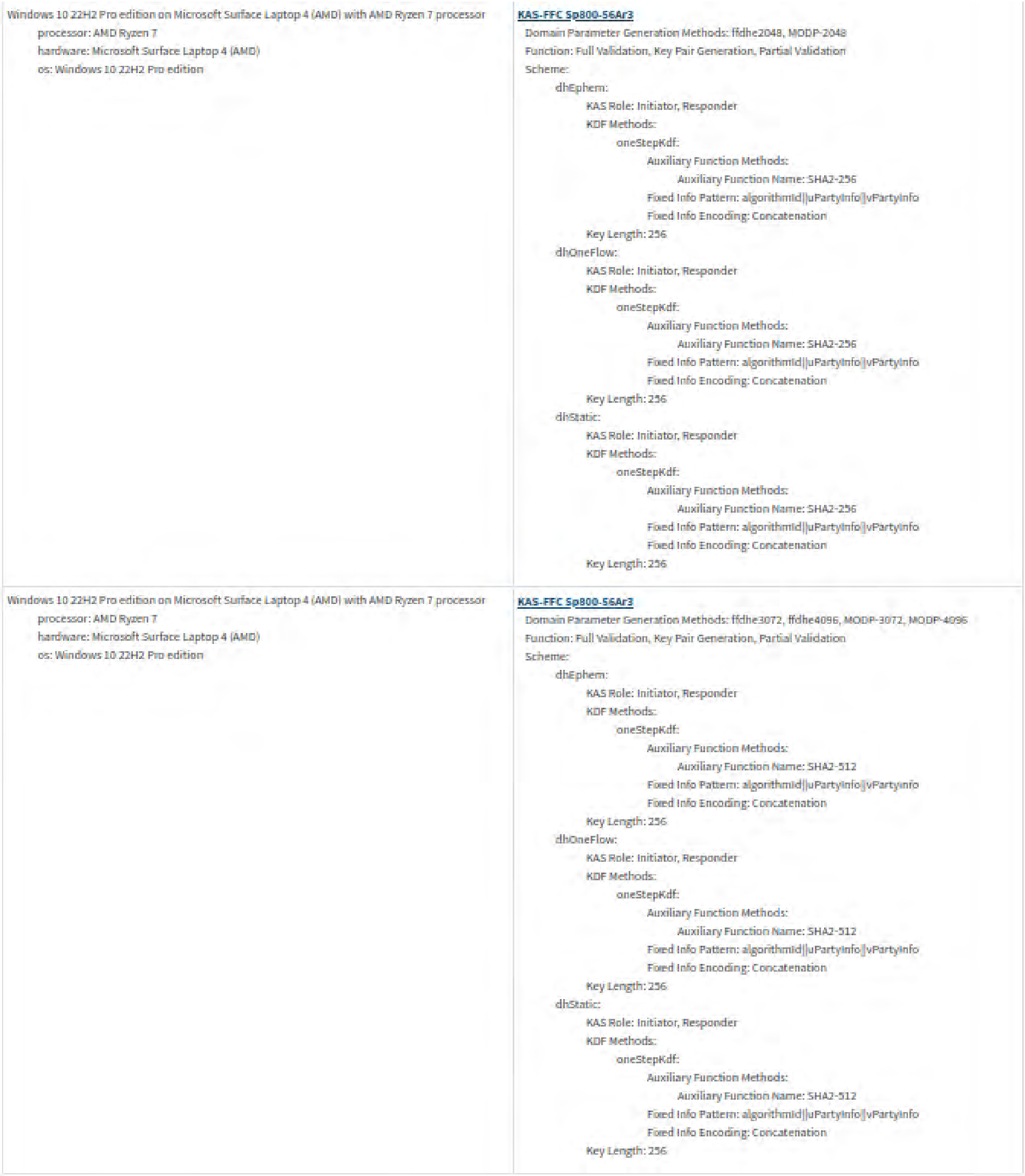
Windows 10 22H2 Enterprise edition on Microsoft Surface Pro 9 with 12th Gen Intel Core i7-1265U processor processor: 12th Gen Intel Core i7-1265U hardware: Microsoft Surface Pro 9 os: Windows 10 22H2 Enterprise edition	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe2048, MODP-2048 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256
Windows 10 22H2 Enterprise edition on Microsoft Surface Pro 9 with 12th Gen Intel Core i7-1265U processor processor: 12th Gen Intel Core i7-1265U hardware: Microsoft Surface Pro 9 os: Windows 10 22H2 Enterprise edition	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe3072, ffdhe4096, MODP-3072, MODP-4096 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256



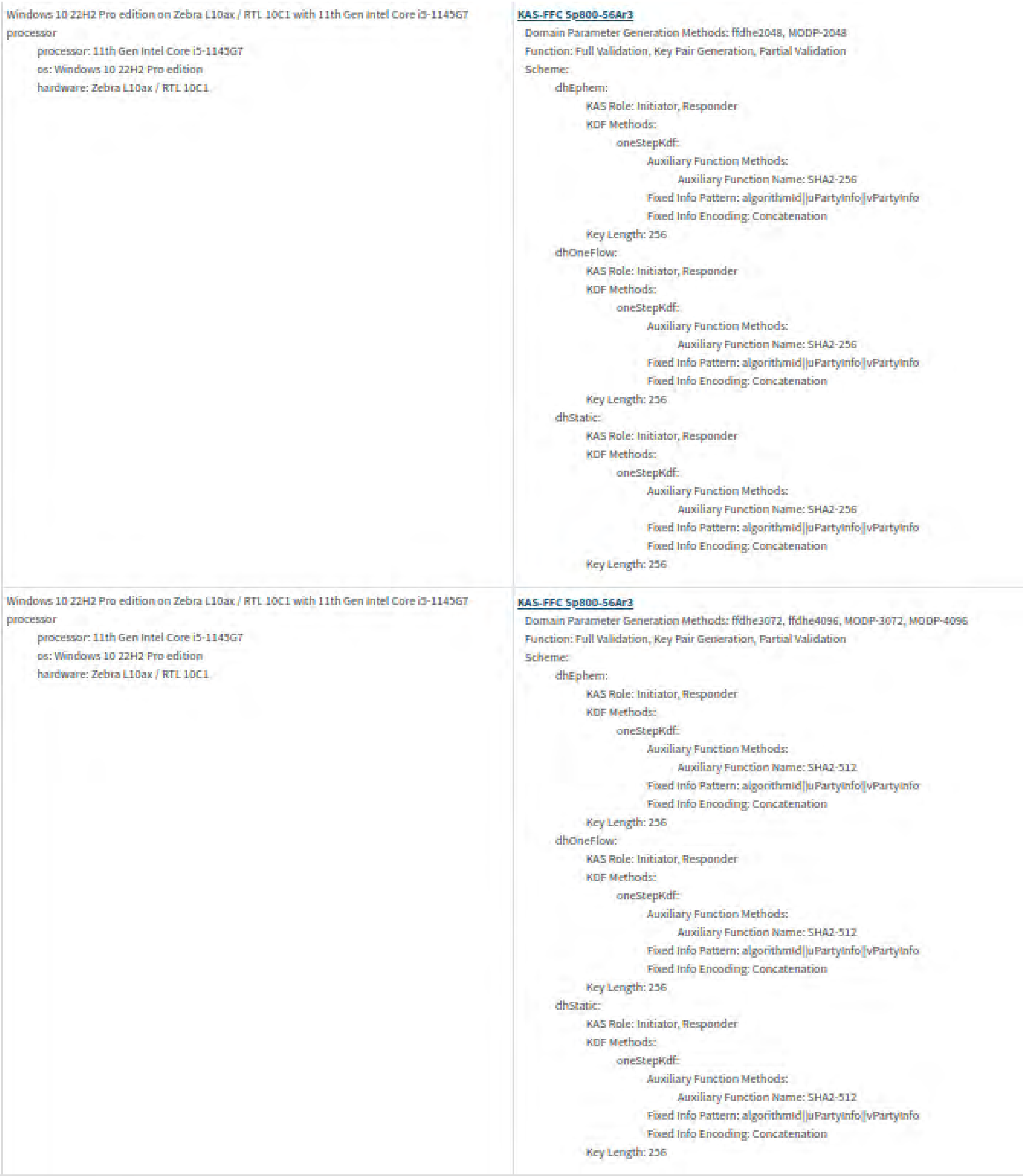
Windows 10 22H2 Enterprise edition on Zebra ET80Z Tablet with 11th Gen Intel Core i5-1130G7 processor processor: 11th Gen Intel Core i5-1130G7 os: Windows 10 22H2 Enterprise edition hardware: Zebra ET80Z Tablet	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe2048, MODP-2048 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256
Windows 10 22H2 Enterprise edition on Zebra ET80Z Tablet with 11th Gen Intel Core i5-1130G7 processor processor: 11th Gen Intel Core i5-1130G7 os: Windows 10 22H2 Enterprise edition hardware: Zebra ET80Z Tablet	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe3072, ffdhe4096, MODP-3072, MODP-4096 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256



Windows 10 22H2 Pro edition on Lenovo ThinkPad Z13 AMD with AMD Ryzen 5 PRO 6650U processor processor: AMD Ryzen 5 PRO 6650U hardware: Lenovo ThinkPad Z13 AMD os: Windows 10 22H2 Pro edition	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe2048, MODP-2048 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256
Windows 10 22H2 Pro edition on Lenovo ThinkPad Z13 AMD with AMD Ryzen 5 PRO 6650U processor processor: AMD Ryzen 5 PRO 6650U hardware: Lenovo ThinkPad Z13 AMD os: Windows 10 22H2 Pro edition	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe3072, ffdhe4096, MODP-3072, MODP-4096 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256

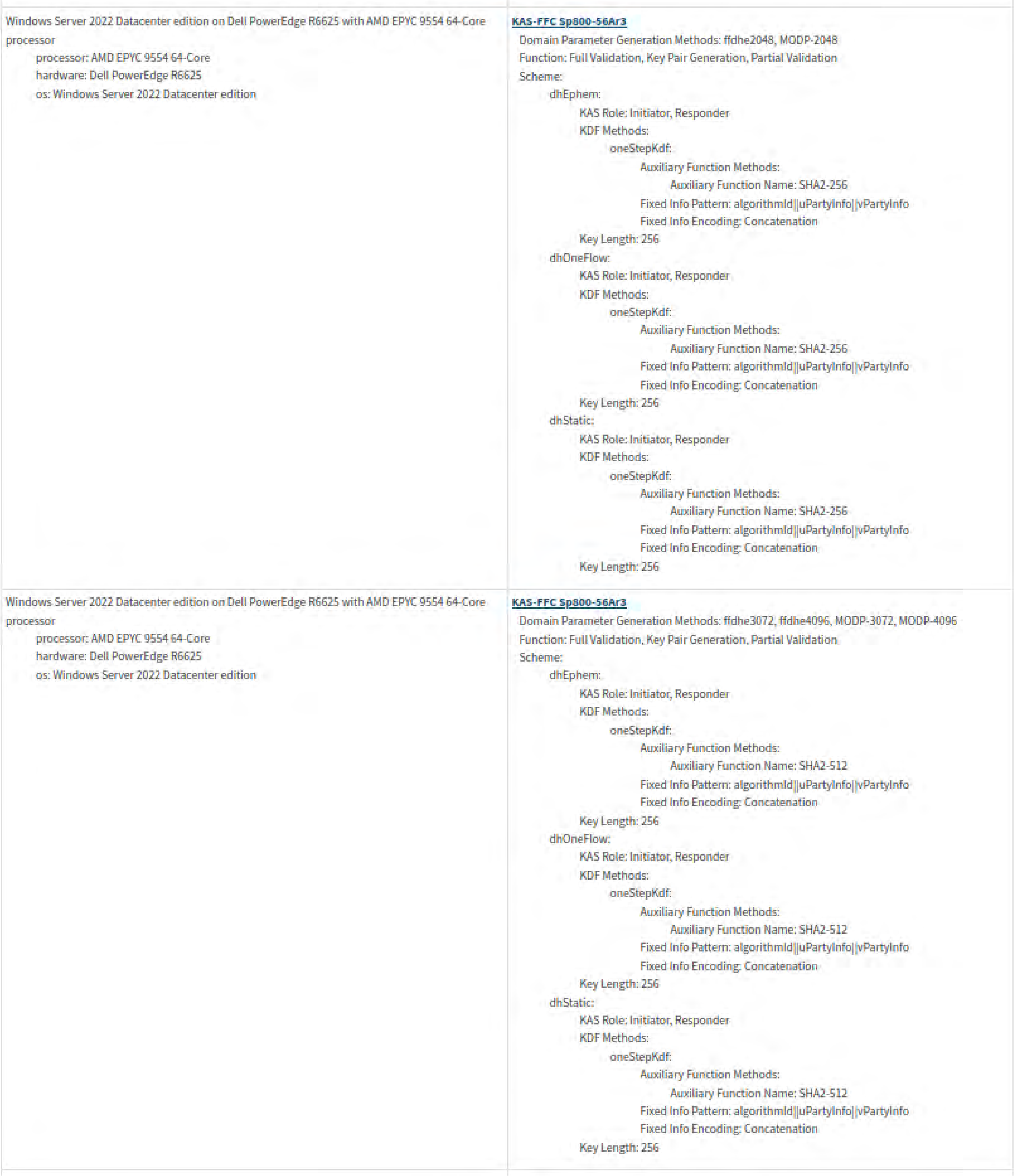


Windows 10 22H2 Pro edition on Microsoft Surface Laptop 4 (AMD) with AMD Ryzen 7 processor processor: AMD Ryzen 7 hardware: Microsoft Surface Laptop 4 (AMD) os: Windows 10 22H2 Pro edition	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe2048, MODP-2048 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256
Windows 10 22H2 Pro edition on Microsoft Surface Laptop 4 (AMD) with AMD Ryzen 7 processor processor: AMD Ryzen 7 hardware: Microsoft Surface Laptop 4 (AMD) os: Windows 10 22H2 Pro edition	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe3072, ffdhe4096, MODP-3072, MODP-4096 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256

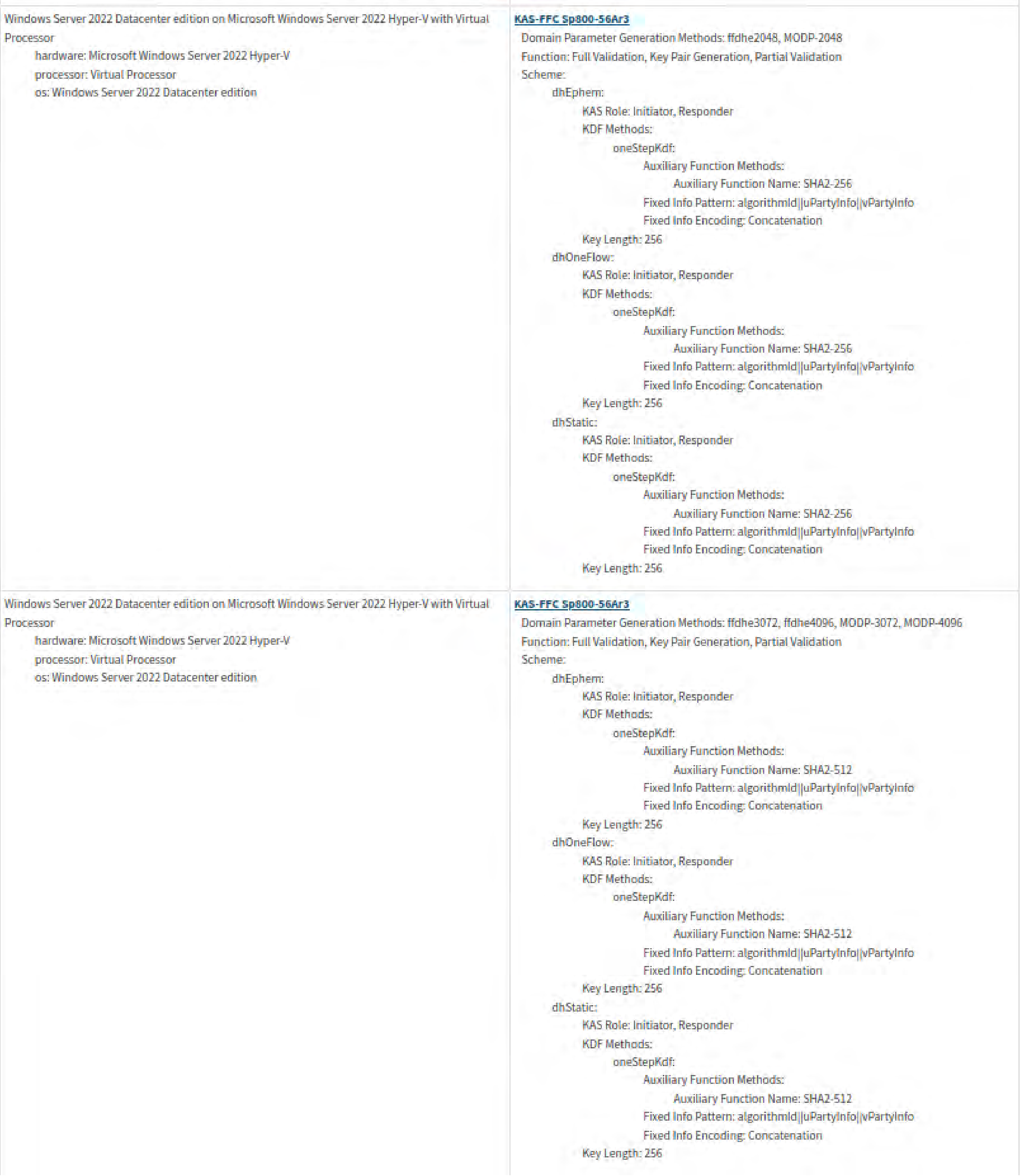


Windows 10 22H2 Pro edition on Zebra L10ax / RTL 10C1 with 11th Gen Intel Core i5-1145G7 processor processor: 11th Gen Intel Core i5-1145G7 os: Windows 10 22H2 Pro edition hardware: Zebra L10ax / RTL 10C1	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe2048, MODP-2048 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256
Windows 10 22H2 Pro edition on Zebra L10ax / RTL 10C1 with 11th Gen Intel Core i5-1145G7 processor processor: 11th Gen Intel Core i5-1145G7 os: Windows 10 22H2 Pro edition hardware: Zebra L10ax / RTL 10C1	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe3072, ffdhe4096, MODP-3072, MODP-4096 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256

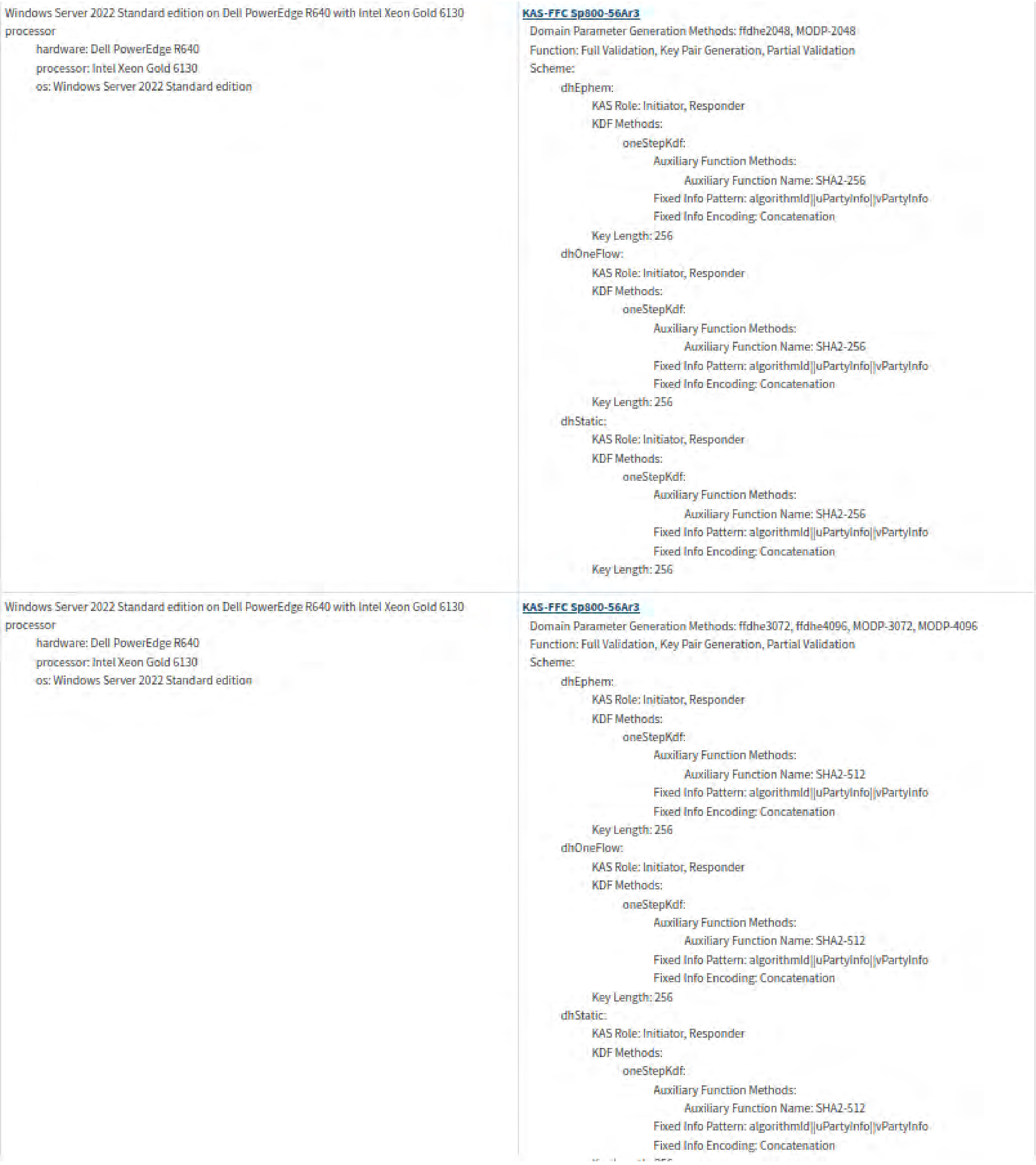
12.1.1.8 Windows Server 2022 and Windows Server Datacenter: Azure Edition (CAVP Cert. #A3810)



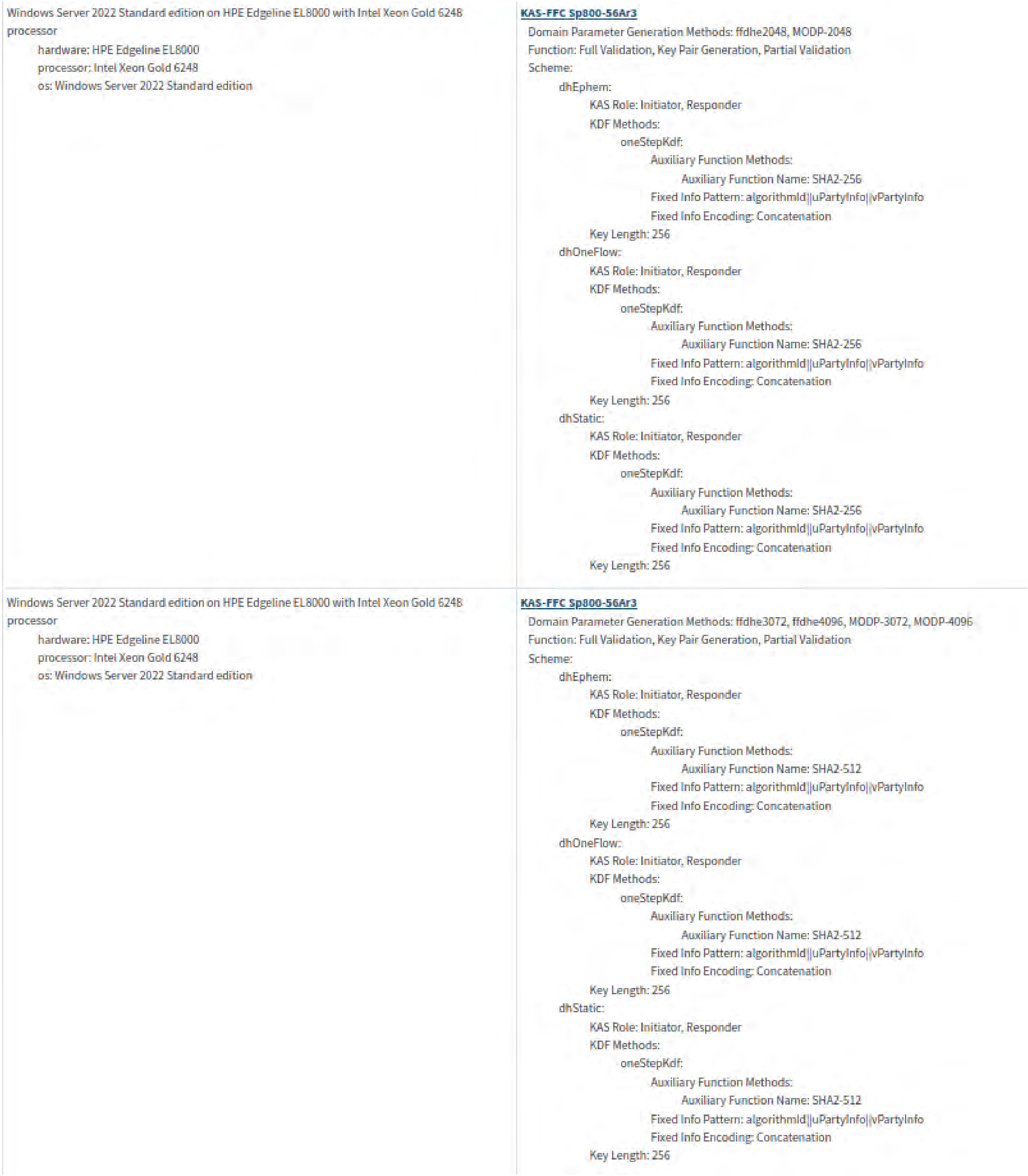
Windows Server 2022 Datacenter edition on Dell PowerEdge R6625 with AMD EPYC 9554 64-Core processor processor: AMD EPYC 9554 64-Core hardware: Dell PowerEdge R6625 os: Windows Server 2022 Datacenter edition	**KAS-FFC Sp800-56Ar3** Domain Parameter Generation Methods: ffdhe2048, MODP-2048 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256
Windows Server 2022 Datacenter edition on Dell PowerEdge R6625 with AMD EPYC 9554 64-Core processor processor: AMD EPYC 9554 64-Core hardware: Dell PowerEdge R6625 os: Windows Server 2022 Datacenter edition	**KAS-FFC Sp800-56Ar3** Domain Parameter Generation Methods: ffdhe3072, ffdhe4096, MODP-3072, MODP-4096 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256



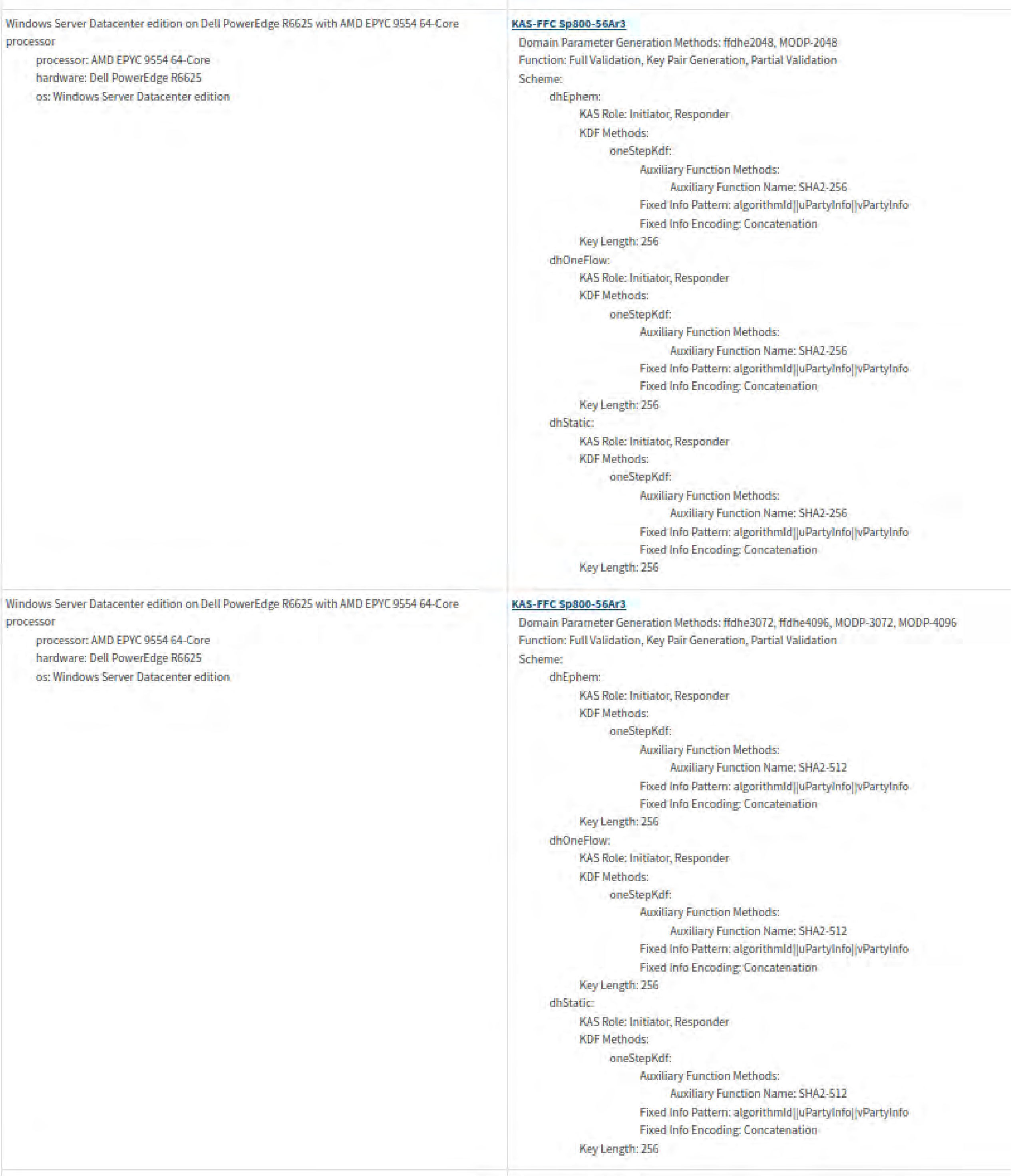
Windows Server 2022 Datacenter edition on Microsoft Windows Server 2022 Hyper-V with Virtual Processor hardware: Microsoft Windows Server 2022 Hyper-V processor: Virtual Processor os: Windows Server 2022 Datacenter edition	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe2048, MODP-2048 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256
Windows Server 2022 Datacenter edition on Microsoft Windows Server 2022 Hyper-V with Virtual Processor hardware: Microsoft Windows Server 2022 Hyper-V processor: Virtual Processor os: Windows Server 2022 Datacenter edition	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe3072, ffdhe4096, MODP-3072, MODP-4096 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256



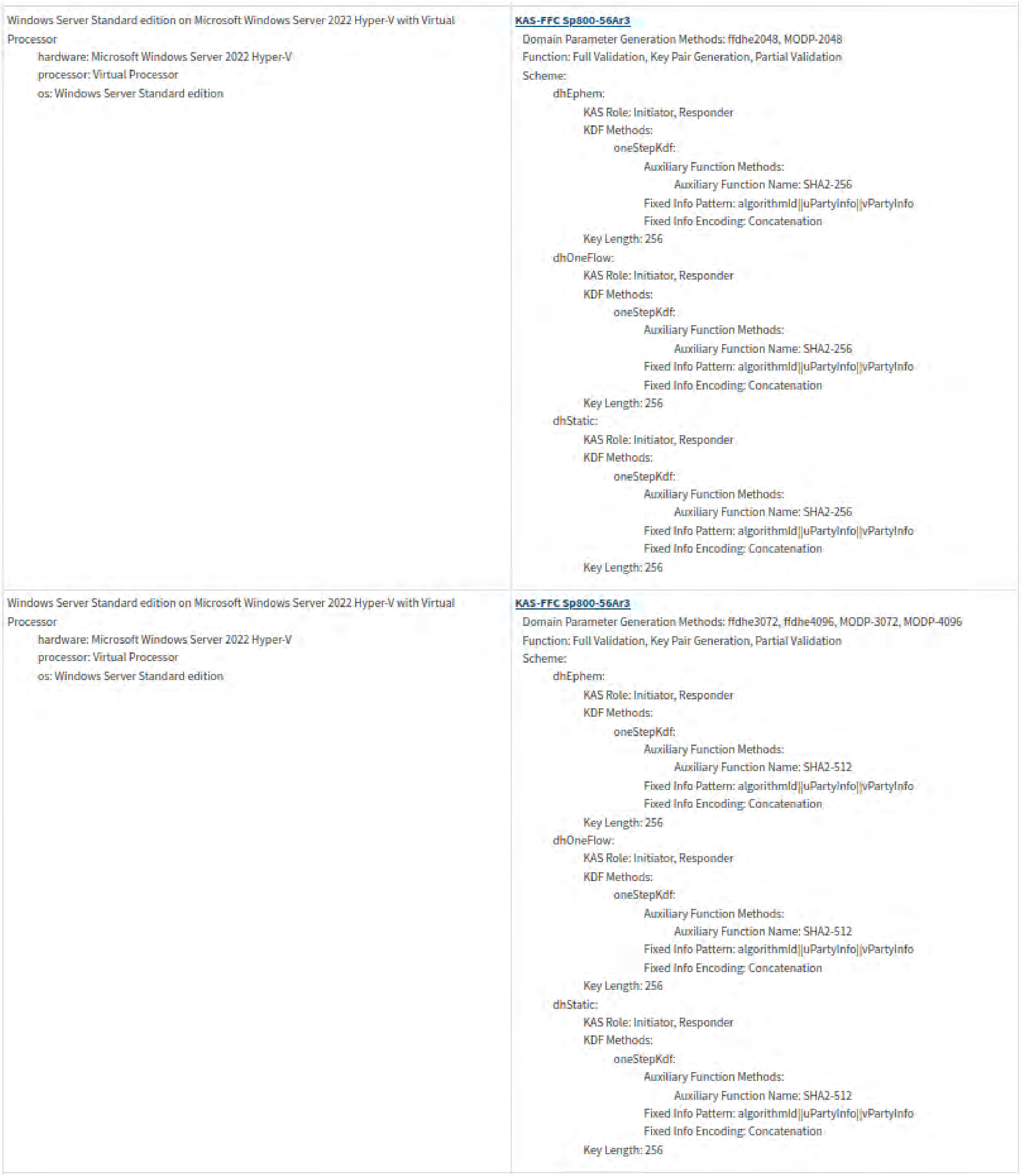
Windows Server 2022 Standard edition on Dell PowerEdge R640 with Intel Xeon Gold 6130 processor hardware: Dell PowerEdge R640 processor: Intel Xeon Gold 6130 os: Windows Server 2022 Standard edition	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe2048, MODP-2048 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256
Windows Server 2022 Standard edition on Dell PowerEdge R640 with Intel Xeon Gold 6130 processor hardware: Dell PowerEdge R640 processor: Intel Xeon Gold 6130 os: Windows Server 2022 Standard edition	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe3072, ffdhe4096, MODP-3072, MODP-4096 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation



Windows Server 2022 Standard edition on HPE Edgeline EL8000 with Intel Xeon Gold 6248 processor hardware: HPE Edgeline EL8000 processor: Intel Xeon Gold 6248 os: Windows Server 2022 Standard edition	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe2048, MODP-2048 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256
Windows Server 2022 Standard edition on HPE Edgeline EL8000 with Intel Xeon Gold 6248 processor hardware: HPE Edgeline EL8000 processor: Intel Xeon Gold 6248 os: Windows Server 2022 Standard edition	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe3072, ffdhe4096, MODP-3072, MODP-4096 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256

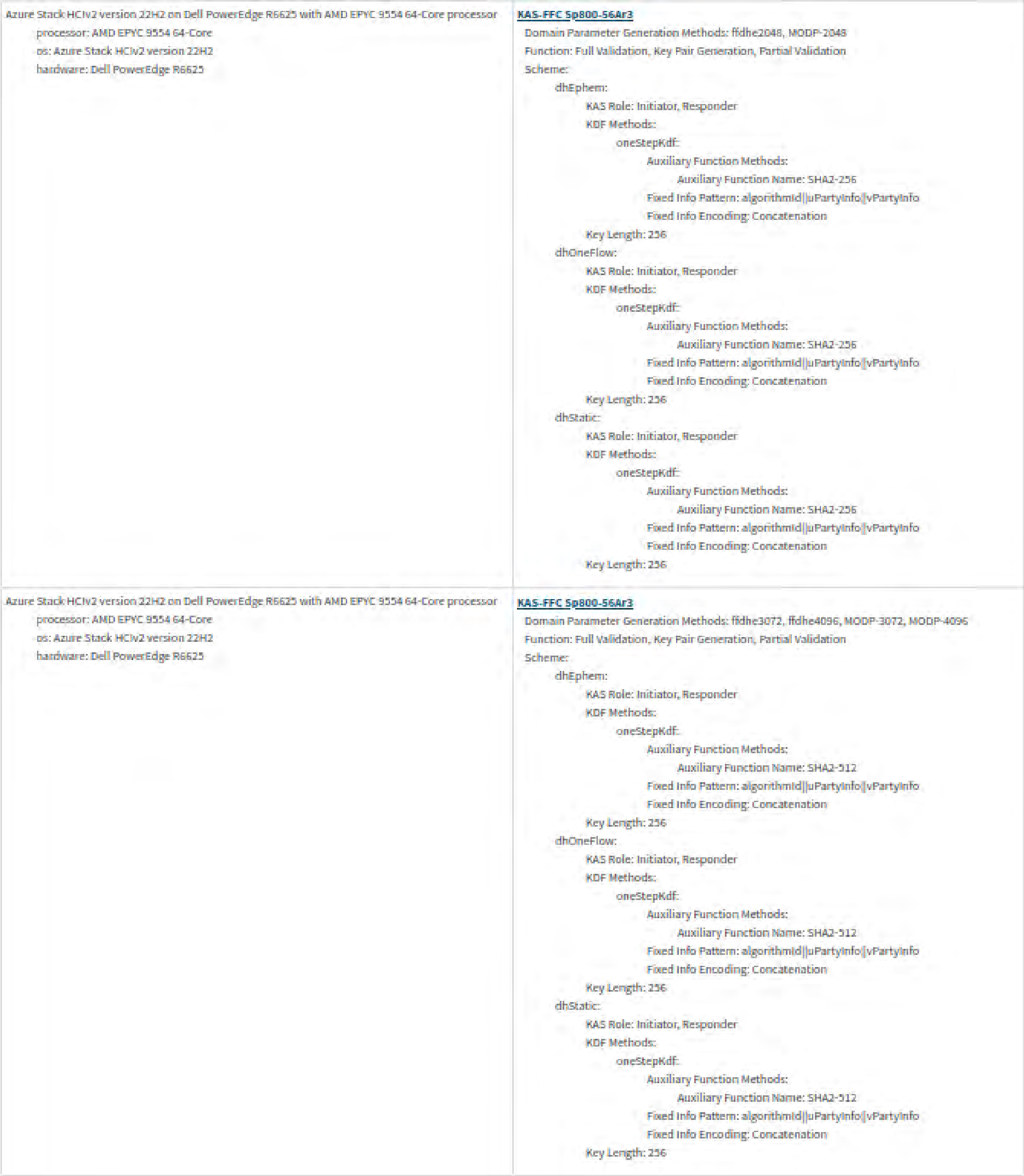


Windows Server Datacenter edition on Dell PowerEdge R6625 with AMD EPYC 9554 64-Core processor processor: AMD EPYC 9554 64-Core hardware: Dell PowerEdge R6625 os: Windows Server Datacenter edition	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe2048, MODP-2048 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256
Windows Server Datacenter edition on Dell PowerEdge R6625 with AMD EPYC 9554 64-Core processor processor: AMD EPYC 9554 64-Core hardware: Dell PowerEdge R6625 os: Windows Server Datacenter edition	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe3072, ffdhe4096, MODP-3072, MODP-4096 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256

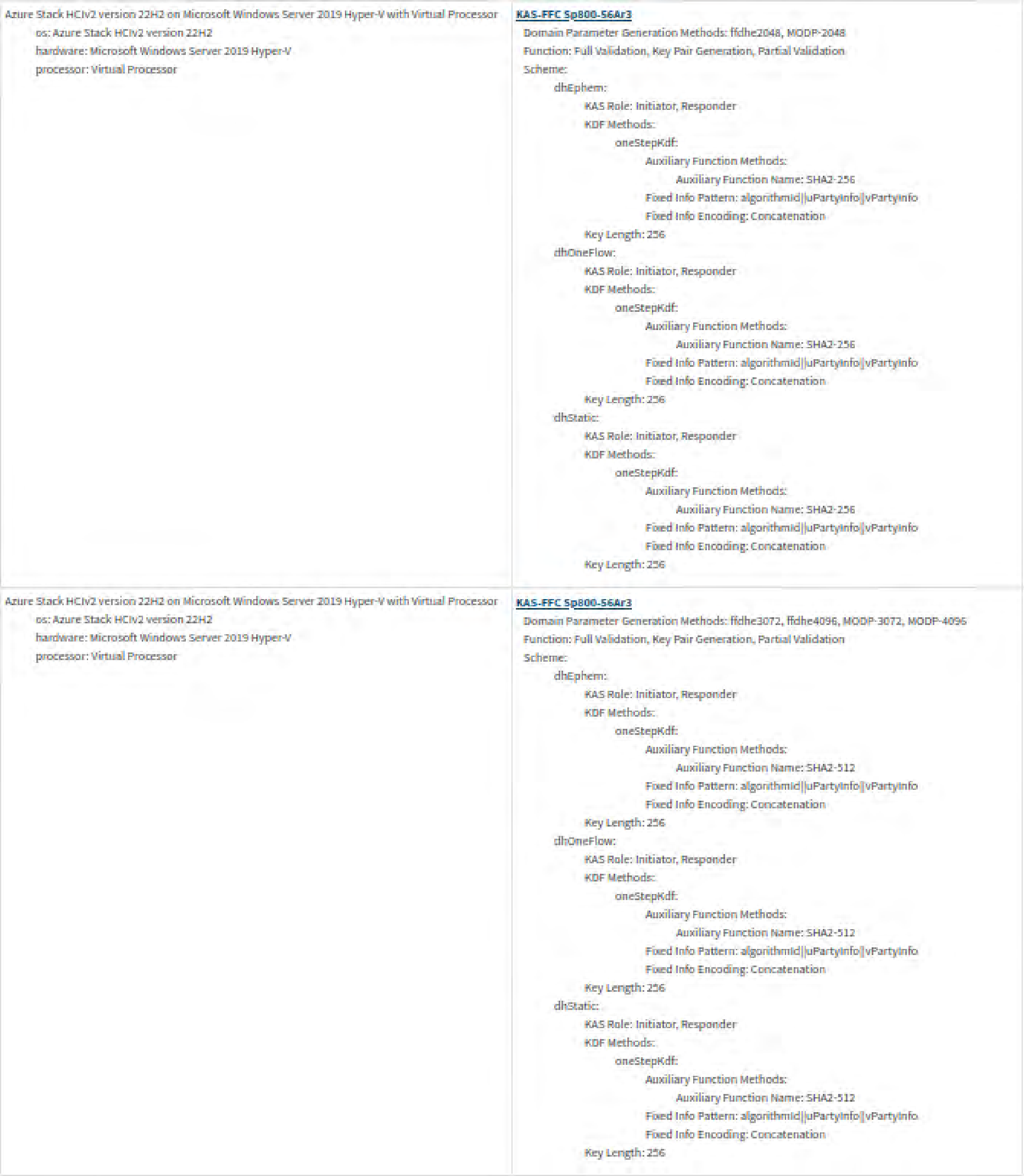


Windows Server Standard edition on Microsoft Windows Server 2022 Hyper-V with Virtual Processor hardware: Microsoft Windows Server 2022 Hyper-V processor: Virtual Processor os: Windows Server Standard edition	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe2048, MODP-2048 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256
Windows Server Standard edition on Microsoft Windows Server 2022 Hyper-V with Virtual Processor hardware: Microsoft Windows Server 2022 Hyper-V processor: Virtual Processor os: Windows Server Standard edition	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe3072, ffdhe4096, MODP-3072, MODP-4096 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256

12.1.1.9 Windows Server Azure Stack HCIv2 version 22H2 (CAVP Cert. #A3783)

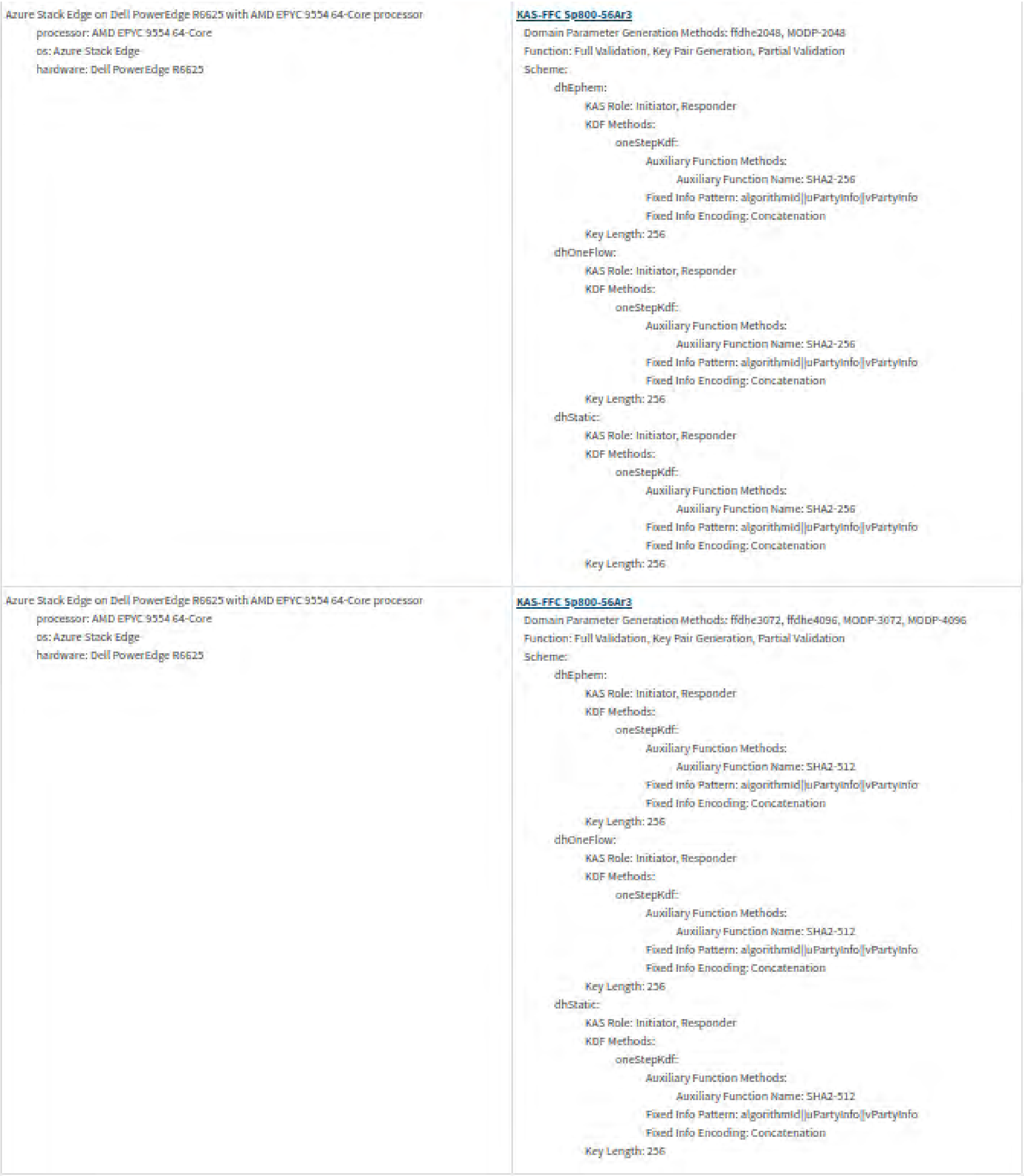


Azure Stack HCIv2 version 22H2 on Dell PowerEdge R6625 with AMD EPYC 9554 64-Core processor processor: AMD EPYC 9554 64-Core os: Azure Stack HCIv2 version 22H2 hardware: Dell PowerEdge R6625	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe2048, MODP-2048 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256
Azure Stack HCIv2 version 22H2 on Dell PowerEdge R6625 with AMD EPYC 9554 64-Core processor processor: AMD EPYC 9554 64-Core os: Azure Stack HCIv2 version 22H2 hardware: Dell PowerEdge R6625	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe3072, ffdhe4096, MODP-3072, MODP-4096 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256

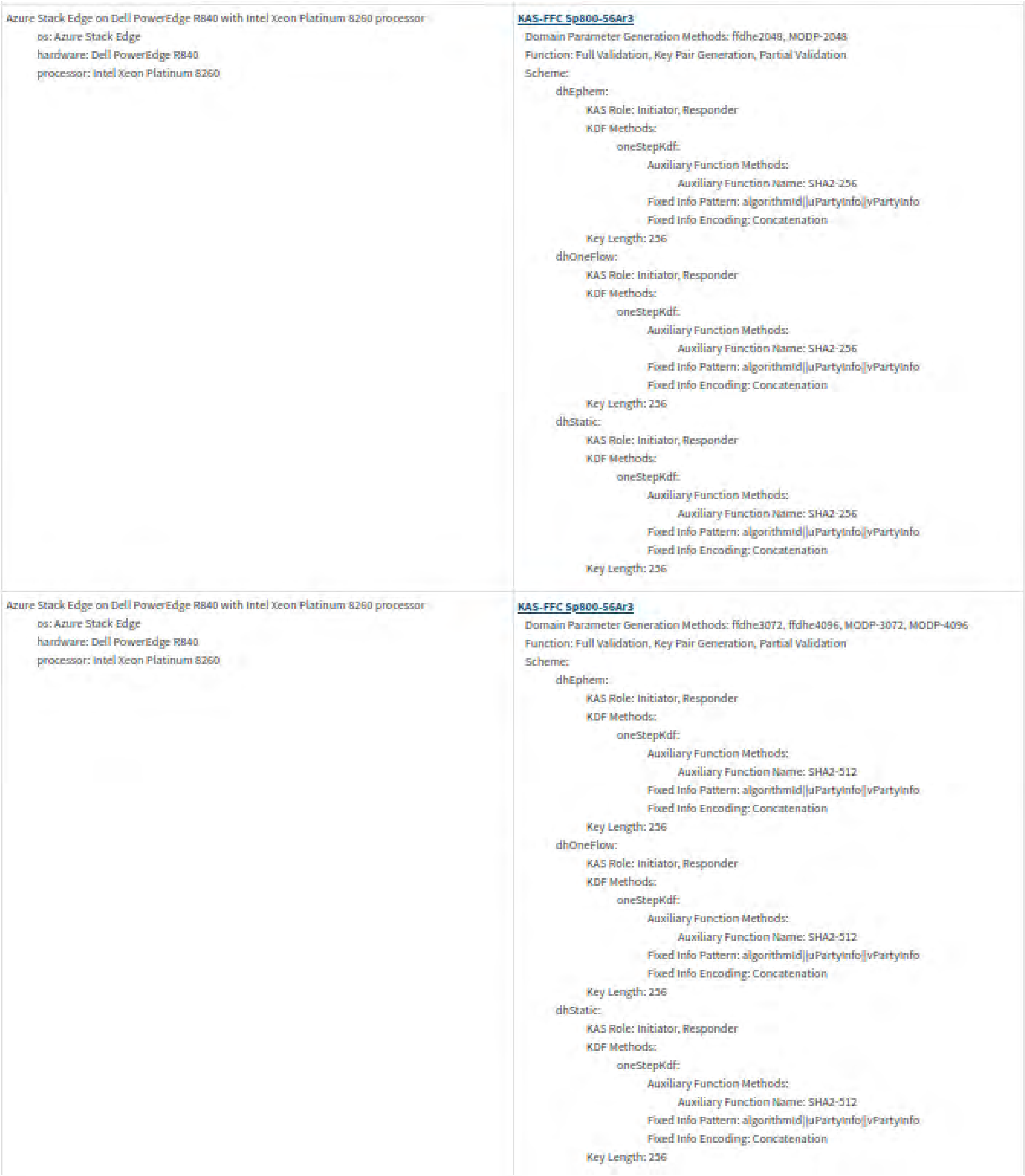


Azure Stack HCIv2 version 22H2 on Microsoft Windows Server 2019 Hyper-V with Virtual Processor os: Azure Stack HCIv2 version 22H2 hardware: Microsoft Windows Server 2019 Hyper-V processor: Virtual Processor	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe2048, MODP-2048 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256
Azure Stack HCIv2 version 22H2 on Microsoft Windows Server 2019 Hyper-V with Virtual Processor os: Azure Stack HCIv2 version 22H2 hardware: Microsoft Windows Server 2019 Hyper-V processor: Virtual Processor	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe3072, ffdhe4096, MODP-3072, MODP-4096 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256

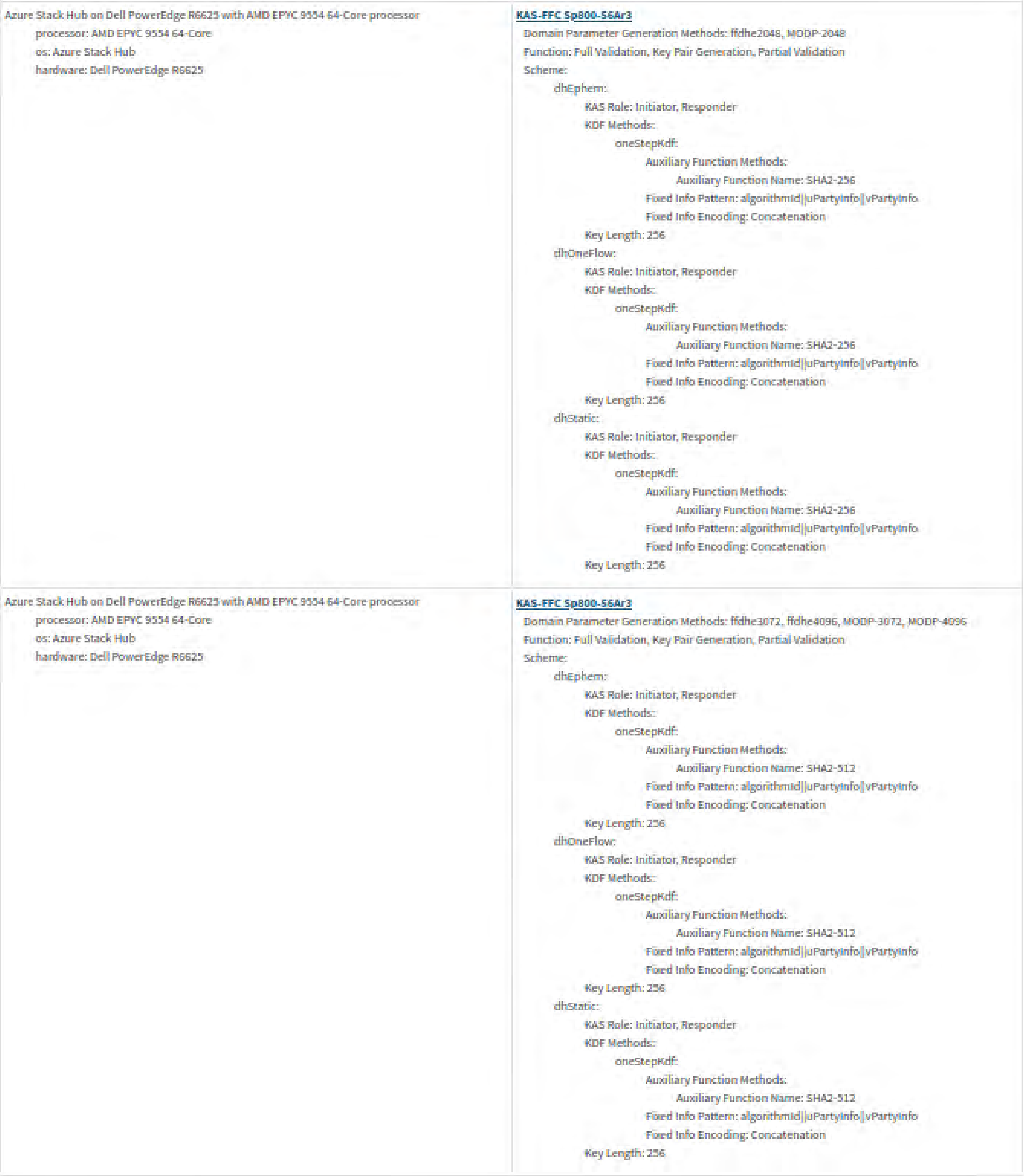
12.1.1.10 Azure Stack Hub and Azure Stack Edge (CAVP Cert. #A3789)



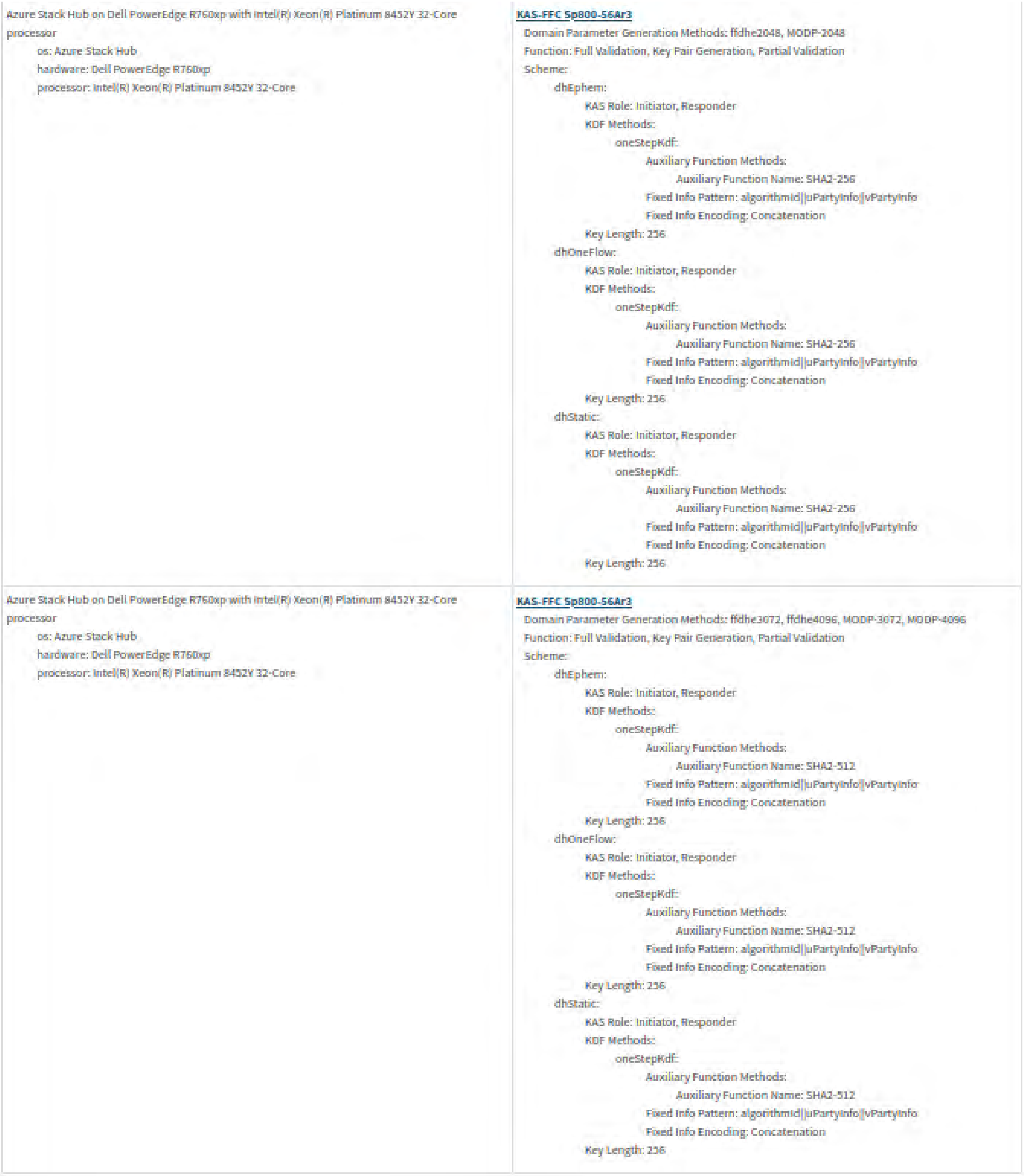
Azure Stack Edge on Dell PowerEdge R6625 with AMD EPYC 9554 64-Core processor processor: AMD EPYC 9554 64-Core os: Azure Stack Edge hardware: Dell PowerEdge R6625	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe2048, MODP-2048 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256
Azure Stack Edge on Dell PowerEdge R6625 with AMD EPYC 9554 64-Core processor processor: AMD EPYC 9554 64-Core os: Azure Stack Edge hardware: Dell PowerEdge R6625	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe3072, ffdhe4096, MODP-3072, MODP-4096 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256



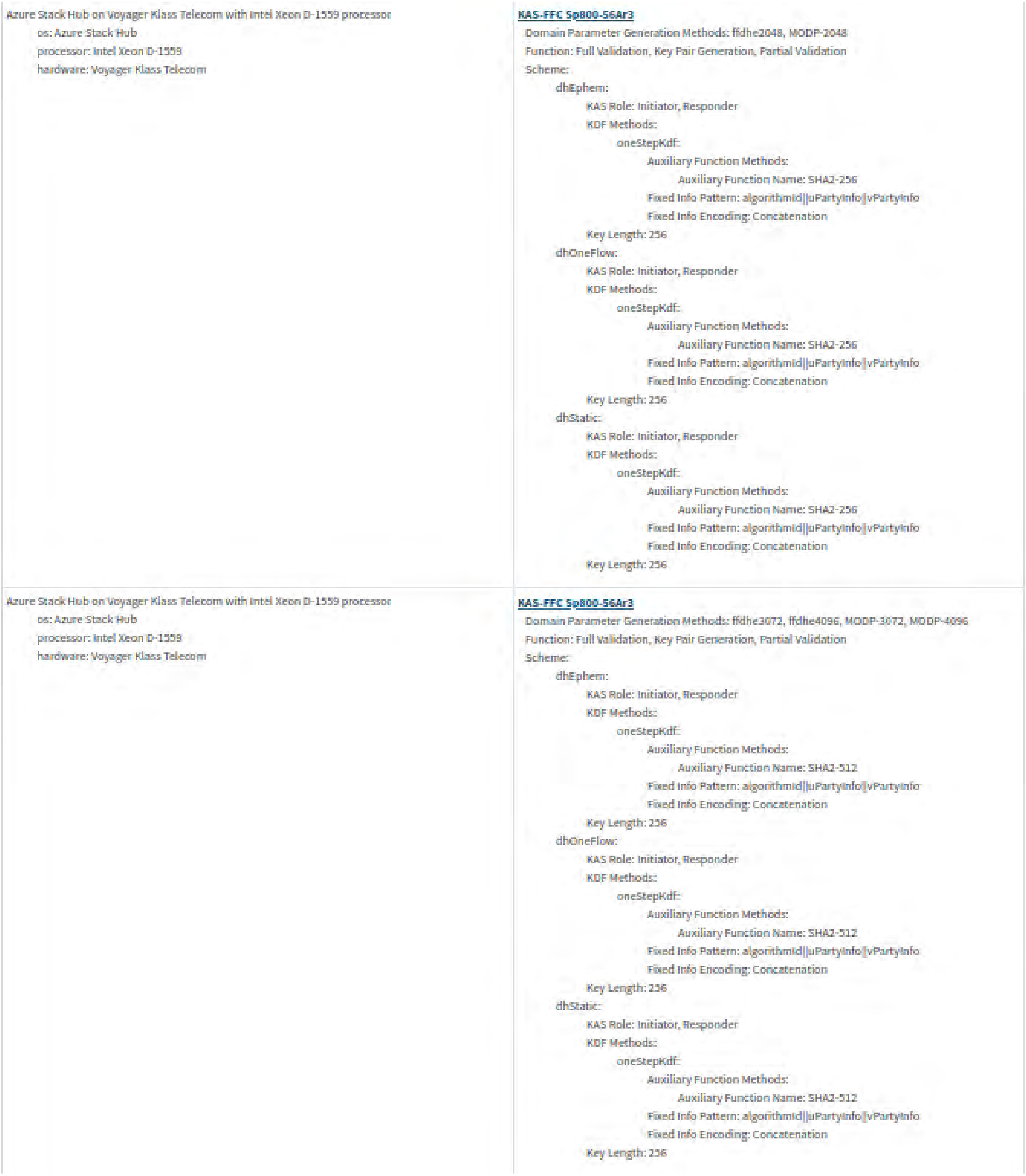
Azure Stack Edge on Dell PowerEdge R840 with Intel Xeon Platinum 8260 processor os: Azure Stack Edge hardware: Dell PowerEdge R840 processor: Intel Xeon Platinum 8260	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe2048, MODP-2048 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256
Azure Stack Edge on Dell PowerEdge R840 with Intel Xeon Platinum 8260 processor os: Azure Stack Edge hardware: Dell PowerEdge R840 processor: Intel Xeon Platinum 8260	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe3072, ffdhe4096, MODP-3072, MODP-4096 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256



Azure Stack Hub on Dell PowerEdge R6625 with AMD EPYC 9554 64-Core processor processor: AMD EPYC 9554 64-Core os: Azure Stack Hub hardware: Dell PowerEdge R6625	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe2048, MODP-2048 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256
Azure Stack Hub on Dell PowerEdge R6625 with AMD EPYC 9554 64-Core processor processor: AMD EPYC 9554 64-Core os: Azure Stack Hub hardware: Dell PowerEdge R6625	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe3072, ffdhe4096, MODP-3072, MODP-4096 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256



Azure Stack Hub on Dell PowerEdge R760xp with Intel(R) Xeon(R) Platinum 8452Y 32-Core processor os: Azure Stack Hub hardware: Dell PowerEdge R760xp processor: Intel(R) Xeon(R) Platinum 8452Y 32-Core	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe2048, MODP-2048 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256
Azure Stack Hub on Dell PowerEdge R760xp with Intel(R) Xeon(R) Platinum 8452Y 32-Core processor os: Azure Stack Hub hardware: Dell PowerEdge R760xp processor: Intel(R) Xeon(R) Platinum 8452Y 32-Core	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe3072, ffdhe4096, MODP-3072, MODP-4096 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256



Azure Stack Hub on Voyager Klass Telecom with Intel Xeon D-1559 processor os: Azure Stack Hub processor: Intel Xeon D-1559 hardware: Voyager Klass Telecom	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe2048, MODP-2048 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-256 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256
Azure Stack Hub on Voyager Klass Telecom with Intel Xeon D-1559 processor os: Azure Stack Hub processor: Intel Xeon D-1559 hardware: Voyager Klass Telecom	KAS-FFC Sp800-56Ar3 Domain Parameter Generation Methods: ffdhe3072, ffdhe4096, MODP-3072, MODP-4096 Function: Full Validation, Key Pair Generation, Partial Validation Scheme: dhEphem: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhOneFlow: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256 dhStatic: KAS Role: Initiator, Responder KDF Methods: oneStepKdf: Auxiliary Function Methods: Auxiliary Function Name: SHA2-512 Fixed Info Pattern: algorithmId||uPartyInfo||vPartyInfo Fixed Info Encoding: Concatenation Key Length: 256

12.1.2 Verdict

The evaluator considers that the TSS identifies all the key agreement schemes and its algorithms involved according to the *SP-800-56A* and *SP-800-56B* standards.

The AGD guidance defines the FIPS security policy to be applied. Once this policy is applied, only the key agreement schemes described above can be used. No more configuration is needed for using the supported key agreement schemes.

Hence, the **PASS** verdict is assigned to the documentation review activity.

12.2 Test Activity

Based on the SFR instantiation included in the security target, the vendor has selected the following key agreement methods:

1. ECDSA scheme based on NIST Special Publication 800-56A.
2. FFC scheme based on NIST Special Publication 800-56A.
3. RSA scheme using PKCS1-v1_5 as specified in RFC 8017, version 2.2.
4. Diffie-Hellman group 14 (demonstrated in *FCS_IPSEC_EXT.1.8* requirement, and therefore, no covered in this test description).

In addition to the Common Criteria evaluation, the laboratory has also performed the CAVP validation for these and other algorithms. The general procedure that has been followed during the evaluation in order to demonstrate the correctness of the cryptographic functionality is as follows:

1. The laboratory has used the same test vectors used as part of the CAVP validation. For ECC and FFC key agreement algorithms, the following types of test are performed:
   - Algorithm Functional Test (AFT). The main goal for these tests is verify the implementation of the key agreement method. For this test, it is expected that the TOE generates a key pair and using its generated public key, and the server public key including as an input, calculate the shared secret (dkm). Then, the same procedure shall be repeated in the known good implementation and the obtained shared secret is compared against the one generated by the TOE. This test are done for each type of scheme, key size or curve, and role (initiator or responder).
   - Validation Test. The main goal for these tests is to verify whether the implementation is able to identify when a key agreement is valid or not based on a set of inputs. For this test, it is expected that the TOE determine the validity of a key agreement based on the inputs received (a complete key pair, the server public key and the calculated shared secret). The shared secret shall be recomputed and compared with the given one, determining if the agreement has been done properly or not.
2. The laboratory has exercised the cryptographic functionalities of the TOE by invoking the appropriate API in order to resolve the test vectors. The result of this step is a .json file which includes the associated response generated by the TOE per each test vector.
3. The laboratory has created a testing tool in order to exercise the BOTAN implementation for the target cryptographic algorithms. This tool receives the initial .json file

with the test vectors as well as the .json file obtained as a result of the step 2. After parsing the information, the testing tool invokes the BOTAN implementation for the tested algorithm and resolve each test vector. After that, the testing tool compares both results (BOTAN vs TOE) in order to determine whether the cryptographic algorithms is properly implemented or not. The results of the testing tool is an individual outcome for each test vector (PASS or FAIL) and a overall outcome (PASS is all the test vectors passed or FAIL if any of them failed).

Finally for RSA scheme using PKCS1-v1_5, it has been directly tested against BOTAN. Given that the TOE can act as sender and recipient, both sides have been tested. The followed test procedure is described in *Test 3* section below.

12.2.1 Test 1 (KAS-ECC)

12.2.1.1 Setup

The following environment is required to perform the test in addition to the TOE:

- A computer with:
  - Operating System: Ubuntu 20.04
  - BOTAN Tool is installed with CCN policy in evaluator machine;
  - Test vectors are located in evaluator machine.

For the installation of the *Botan Tool with CCN policy 2.15.2* all the steps defined in the *Botan-CCN_Manual_Implementador_v1* document have been followed.

12.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

12.2.1.3 Results

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

12.2.1.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the test activity demonstrate that the TOE provides a well implementation for the evaluated cryptographic algorithm, since it has been compared against a well-known implementation (BOTAN) as a reference implementation.

Therefore, the **PASS** verdict is assigned to the **Test 1** activity.

12.2.2 Test 2 (KAS-FFC)

12.2.2.1 Setup

The following environment is required to perform the test in addition to the TOE:

- A computer with:
  - Operating System: Ubuntu 20.04
  - BOTAN Tool is installed with CCN policy in evaluator machine;
  - Test vectors are located in evaluator machine.

For the installation of the *Botan Tool with CCN policy 2.15.2* all the steps defined in the *Botan-CCN_Manual_Implementador_v1* document have been followed.

12.2.2.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

12.2.2.3 Results

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

12.2.2.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the test activity demonstrate that the TOE provides a well implementation for the evaluated cryptographic algorithm, since it has been compared against a well-known implementation (BOTAN) as a reference implementation.

For the key establishment schemes using ffdhe groups, which are not available in BOTAN, the laboratory has followed the same approach but using the CAVP implementation as a reference instead of BOTAN. The evaluator has verified that the responses generated by the TOE are the same as the ones expected by the CAVP tool. Additionally, the associated CAVP certificates (listed in the tables included within the Documentation Review Activity section) have been granted demonstrating the correctness of the algorithm implementation.

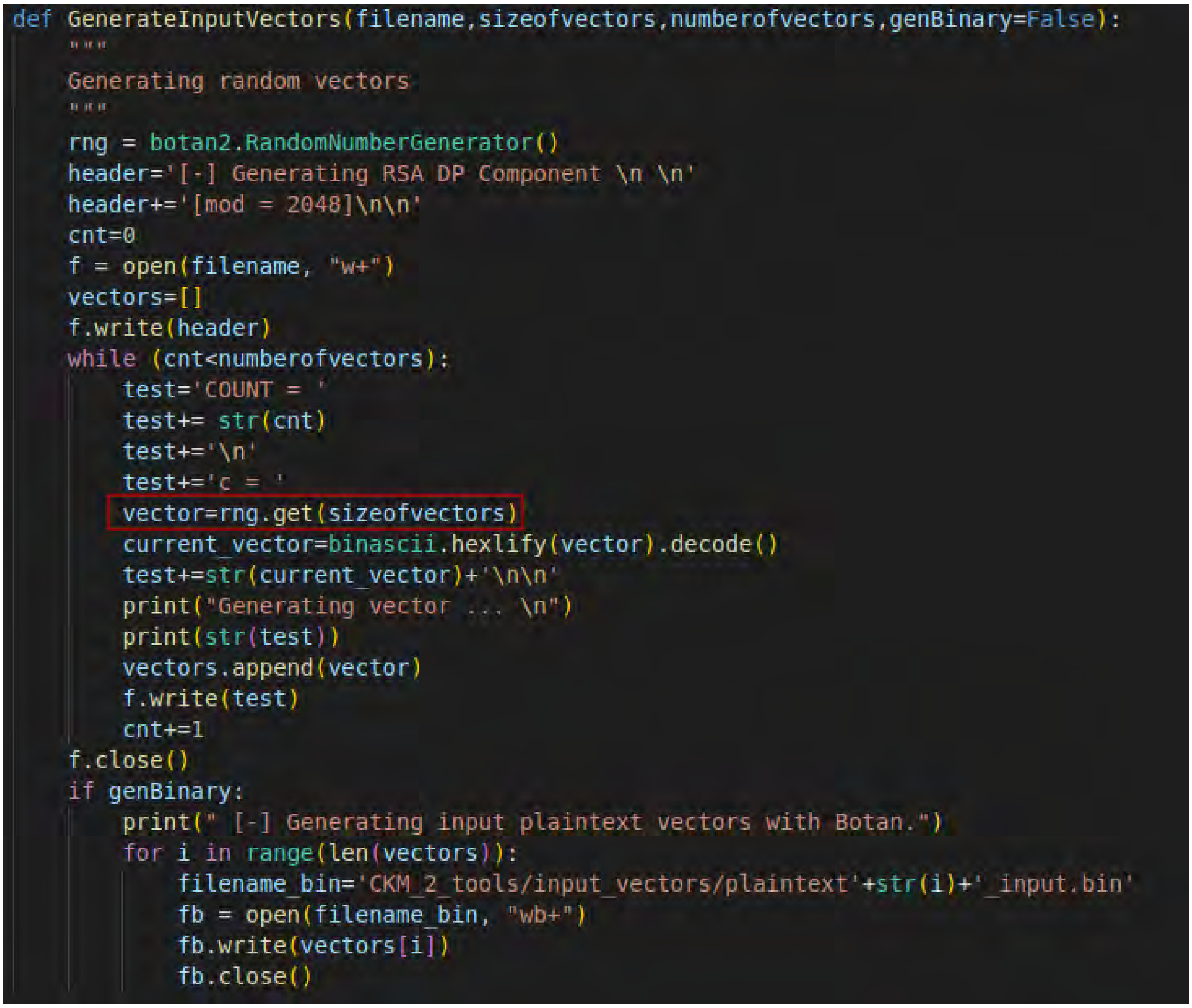
Therefore, the **PASS** verdict is assigned to the **Test 2** activity.

12.2.3 Test 3 (KAS-RSA)

12.2.3.1 Setup

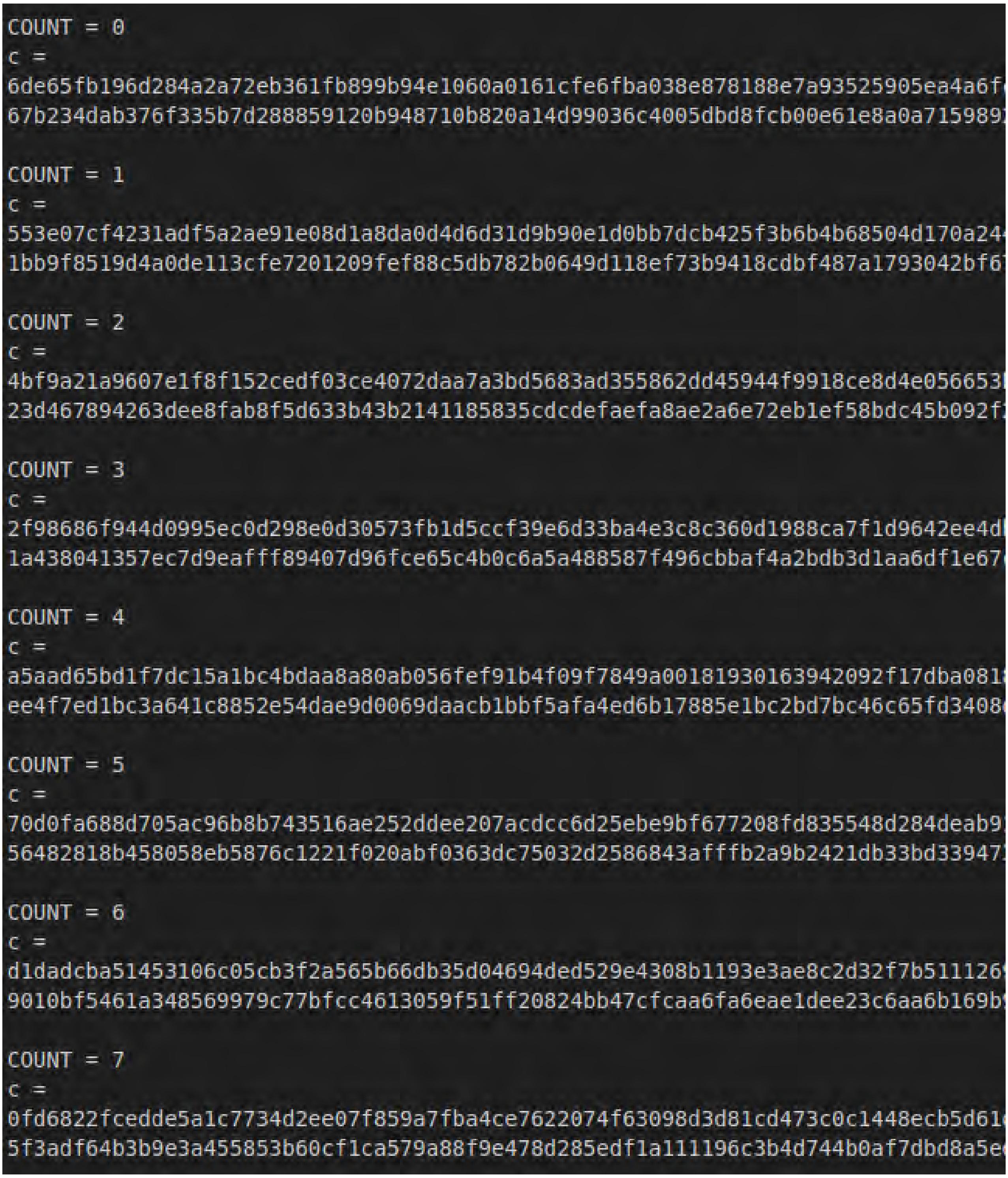
Based on the information provided in the *TSS*, it is assumed that neither the key confirmation nor the *KTS-OAEP* nor additional input parameters are supported. So, the testing is carried out only considering the *RSA key pair* (private and public key), plaintext and ciphertext.

Plaintext for the tests has been obtained from generate_inputs .py a script that uses Botan to generate a set of random input vectors:



```
def GenerateInputVectors(filename,sizeofvectors,numberofvectors,genBinary=False):
    """
    Generating random vectors
    """
    rng = botan2.RandomNumberGenerator()
    header='[-] Generating RSA DP Component \n \n'
    header+='[mod = 2048]\n\n'
    cnt=0
    f = open(filename, "w+")
    vectors=[]
    f.write(header)
    while (cnt<numberofvectors):
        test='COUNT = '
        test+= str(cnt)
        test+='\n'
        test+='c = '
        vector=rng.get(sizeofvectors)
        current_vector=binascii.hexlify(vector).decode()
        test+=str(current_vector)+'\n\n'
        print("Generating vector ... \n")
        print(str(test))
        vectors.append(vector)
        f.write(test)
        cnt+=1
    f.close()
    if genBinary:
        print(" [-] Generating input plaintext vectors with Botan.")
        for i in range(len(vectors)):
            filename_bin='CKM_2_tools/input_vectors/plaintext'+str(i)+'_input.bin'
            fb = open(filename_bin, "wb+")
            fb.write(vectors[i])
            fb.close()
```

Based on this configuration the following input vectors are generated (10 vectors of 2048 bits length, only the first 5 are shown although all of them are used for this evaluation):



```
COUNT = 0
c =
6de65fb196d284a2a72eb361fb899b94e1060a0161cfe6fba038e878188e7a93525905ea4a6f
67b234dab376f335b7d288859120b948710b820a14d99036c4005dbd8fcb00e61e8a0a715989

COUNT = 1
c =
553e07cf4231adf5a2ae91e08d1a8da0d4d6d31d9b90e1d0bb7dcb425f3b6b4b68504d170a24
1bb9f8519d4a0de113cfe7201209fef88c5db782b0649d118ef73b9418cdbf487a1793042bf6

COUNT = 2
c =
4bf9a21a9607e1f8f152cedf03ce4072daa7a3bd5683ad355862dd45944f9918ce8d4e056653
23d467894263dee8fab8f5d633b43b2141185835cdcdefaefa8ae2a6e72eb1ef58bdc45b092f

COUNT = 3
c =
2f98686f944d0995ec0d298e0d30573fb1d5ccf39e6d33ba4e3c8c360d1988ca7f1d9642ee4d
1a438041357ec7d9eafff89407d96fce65c4b0c6a5a488587f496cbbaf4a2bdb3d1aa6df1e67

COUNT = 4
c =
a5aad65bd1f7dc15a1bc4bdaa8a80ab056fef91b4f09f7849a0018193016394209 2f17dba081
ee4f7ed1bc3a641c8852e54dae9d0069daacb1bbf5afa4ed6b17885e1bc2bd7bc46c65fd3408

COUNT = 5
c =
70d0fa688d705ac96b8b743516ae252ddee207acdcc6d25ebe9bf677208fd835548d284deab9
56482818b458058eb5876c1221f020abf0363dc75032d2586843afffb2a9b2421db33bd33947

COUNT = 6
c =
d1dadcba51453106c05cb3f2a565b66db35d04694ded529e4308b1193e3ae8c2d32f7b511126
9010bf5461a348569979c77bfcc4613059f51ff20824bb47cfcaa6fa6eae1dee23c6aa6b169b

COUNT = 7
c =
0fd6822fcedde5a1c7734d2ee07f859a7fba4ce7622074f63098d3d81cd473c0c1448ecb5d61
5f3adf64b3b9e3a455853b60cf1ca579a88f9e478d285edf1a111196c3b4d744b0af7dbd8a5e
```

The following environment is required to perform the test in addition to the TOE:

- A computer with:
  - Operating System: Ubuntu 20.04
  - BOTAN Tool is installed with CCN policy in evaluator machine;

For the installation of the *Botan Tool with CCN policy 2.15.2* all the steps defined in the *Botan-CCN_Manual_Implementador_v1* document have been followed.

The Lab has developed two different applications for the Windows side: RSA_ENC.cpp, which receives a set of plaintext as input and generates a set of ciphertext; and RSA_DEC.cpp, which receives a set of ciphertext as input and decrypts them to obtain the set of plaintext. These applications have been developed based on the cryptographic APIs provided by the OS to test the RSA-based key establishment scheme conforming to the special publication 800-56B testing and using the scheme PKCS1-v1_5.

The Lab has developed two different scripts for the Linux side in order to perform the Botan verification: rsa_encrypt .py, which receives the public key, and one plaintext in a binary file as input and generates one ciphertext in a binary file as output; rsa_decrypt .py, which receives the private key, one ciphertext in a binary file as input and generates one ciphertext in a binary file as output.

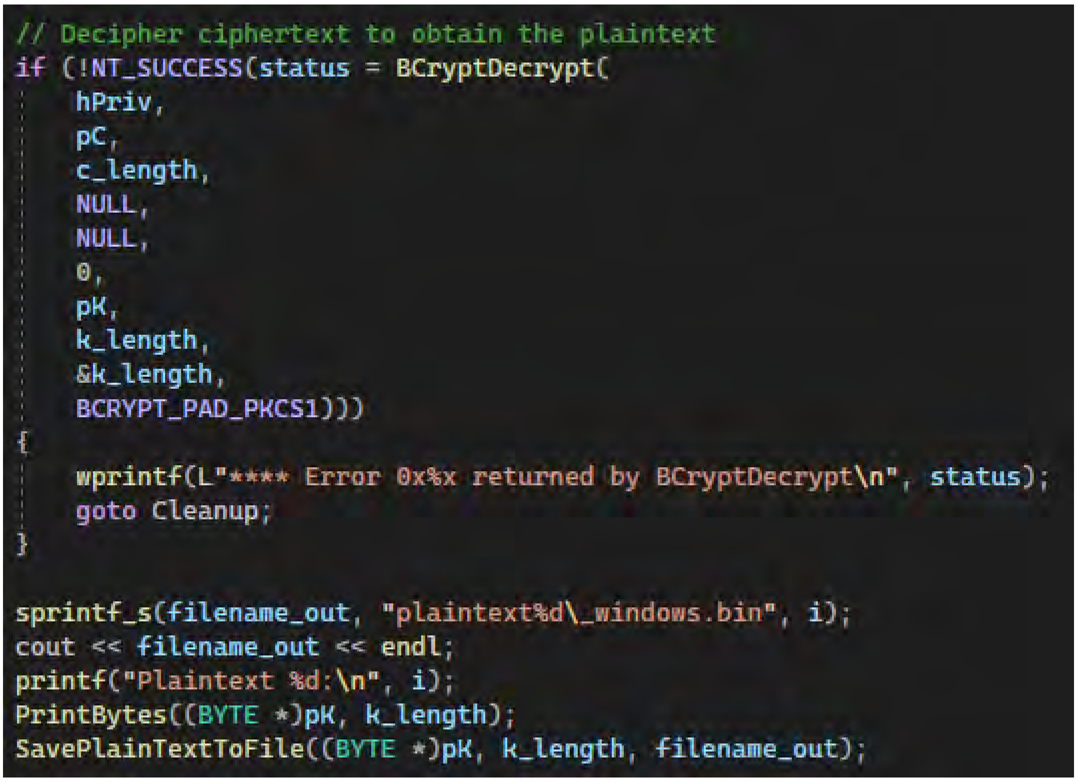
The test approach is described as follows:

RSA_ENC.cpp receives the generated vectors by the Botan tool as input (plaintext) and encrypts them using a valid key pair (public and private key). As result of this execution RSA_ENC.cpp generates a set of ciphertext. On the other hand, the evaluator executes *Botan Tool* to generate a new set of ciphertext using the same set of plaintext and key pair.

Once the two different set of ciphertext have been generated, they are swapped in order to perform the decrypt operation. It means that RSA_DEC.cpp receives the set of ciphertext generated by *Botan Tool* and *Botan Tool* receives the set of ciphertext generated by RSA_ENC.cpp. Both of these executions generate a set of plaintext, which are equal to each other and equal to the ones generated by Botan in the first step.

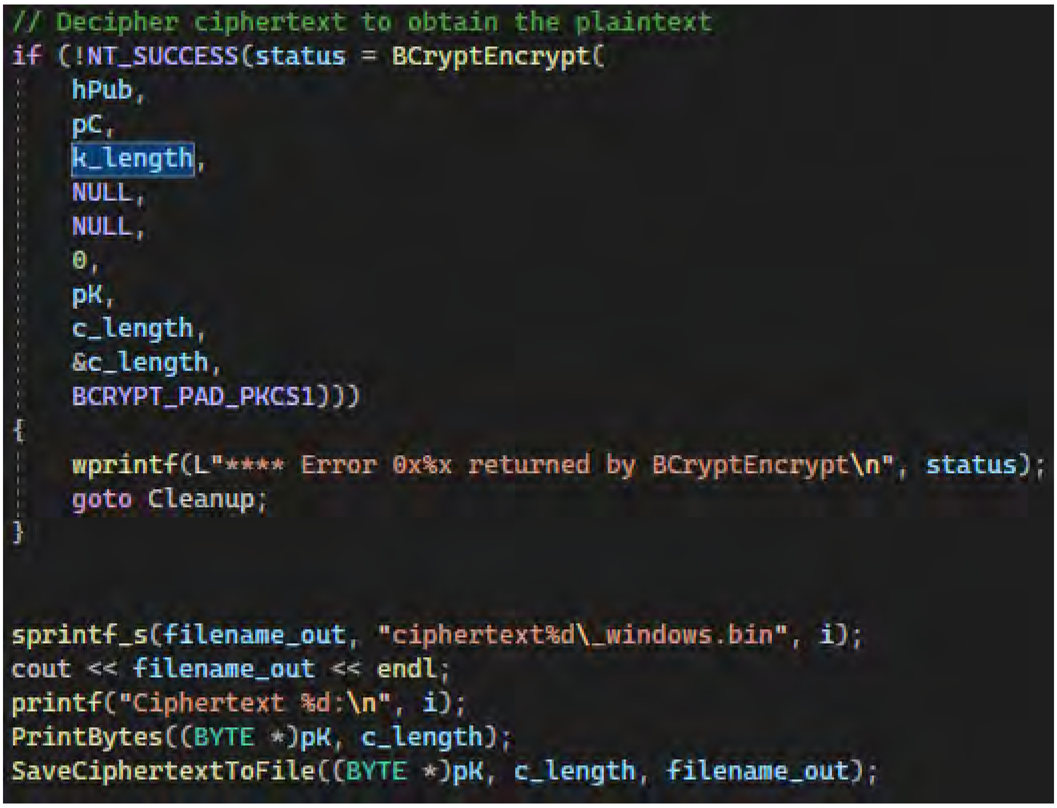
The following screenshots will show the source code used by the executable in the windows side:

- The RSA_DEC.cpp source code, where the main function is *BCryptDecrypt*:



```
// Decipher ciphertext to obtain the plaintext
if (!NT_SUCCESS(status = BCryptDecrypt(
    hPriv,
    pC,
    c_length,
    NULL,
    NULL,
    0,
    pK,
    k_length,
    &k_length,
    BCRYPT_PAD_PKCS1)))
{
    wprintf(L"**** Error 0x%x returned by BCryptDecrypt\n", status);
    goto Cleanup;
}

sprintf_s(filename_out, "plaintext%d\_windows.bin", i);
cout << filename_out << endl;
printf("Plaintext %d:\n", i);
PrintBytes((BYTE *)pK, k_length);
SavePlainTextToFile((BYTE *)pK, k_length, filename_out);
```

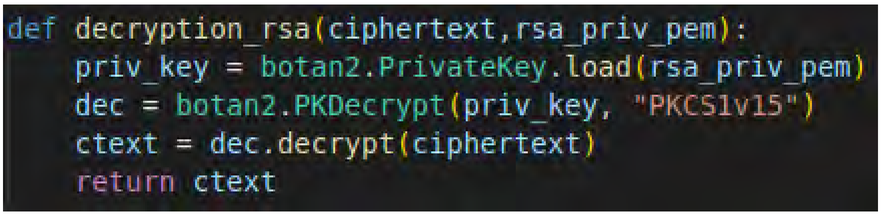
- The main function in RSA_ENC.cpp source code, which it is called *BCryptEncrypt*:



```
// Decipher ciphertext to obtain the plaintext
if (!NT_SUCCESS(status = BCryptEncrypt(
    hPub,
    pC,
    k_length,
    NULL,
    NULL,
    0,
    pK,
    c_length,
    &c_length,
    BCRYPT_PAD_PKCS1)))
{
    wprintf(L"**** Error 0x%x returned by BCryptEncrypt\n", status);
    goto Cleanup;
}


sprintf_s(filename_out, "ciphertext%d\_windows.bin", i);
cout << filename_out << endl;
printf("Ciphertext %d:\n", i);
PrintBytes((BYTE *)pK, c_length);
SaveCiphertextToFile((BYTE *)pK, c_length, filename_out);
```

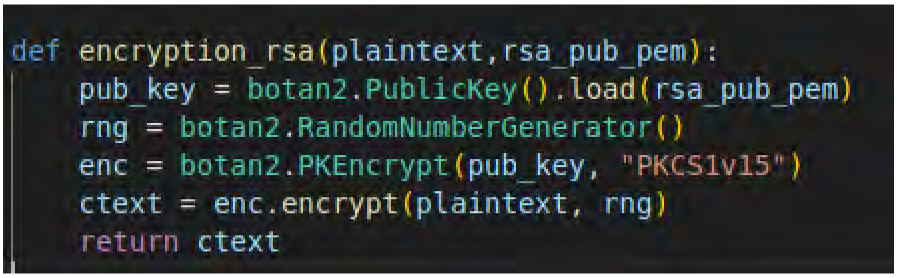
The following screenshots will show the source code used by the Botan Tool used in the Linux side:

- The main function in rsa_decrypt .py, which it is called *decryption_rsa*:



```
def decryption_rsa(ciphertext,rsa_priv_pem):
    priv_key = botan2.PrivateKey.load(rsa_priv_pem)
    dec = botan2.PKDecrypt(priv_key, "PKCS1v15")
    ctext = dec.decrypt(ciphertext)
    return ctext
```

- The main function in rsa_encrypt .py, which it is called *encryption_rsa*:



```
def encryption_rsa(plaintext,rsa_pub_pem):
    pub_key = botan2.PublicKey().load(rsa_pub_pem)
    rng = botan2.RandomNumberGenerator()
    enc = botan2.PKEncrypt(pub_key, "PKCS1v15")
    ctext = enc.encrypt(plaintext, rng)
    return ctext
```

12.2.3.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

12.2.3.3 Results

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

12.2.3.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the test activity demonstrate that the TOE provides a well implementation for the evaluated cryptographic algorithm, since it has been compared against a well-known implementation (BOTAN) as a reference implementation.

Therefore, the **PASS** verdict is assigned to the **Test 3** activity.

12.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FCS_CKM.2.1.

13 FCS_CKM_EXT.4

The assurance activity for the **FCS_CKM_EXT.4** requirement is stated as follows:

> **TSS**
>
> The evaluator examines the TSS to ensure it describes how the keys are managed in volatile memory. This description includes details of how each identified key is introduced into volatile memory (e.g. by derivation from user input, or by unwrapping a wrapped key stored in non-volatile memory) and how they are overwritten.
>
> The evaluator will check to ensure the TSS lists each type of key that is stored in in non-volatile memory, and identifies how the TOE interacts with the underlying platform to manage keys (e.g., store, retrieve, destroy). The description includes details on the method of how the TOE interacts with the platform, including an identification and description of the interfaces it uses to manage keys (e.g., file system APIs, platform key store APIs).
>
> If the ST makes use of the open assignment and fills in the type of pattern that is used, the evaluator examines the TSS to ensure it describes how that pattern is obtained and used. The evaluator shall verify that the pattern does not contain any CSPs.
>
> The evaluator will check that the TSS identifies any configurations or circumstances that may not strictly conform to the key destruction requirement.
>
> If the selection "destruction of all key encrypting keys protecting target key according to FCS_CKM_EXT.4.1, where none of the KEKs protecting the target key are derived" is included the evaluator shall examine the TOE's keychain in the TSS and identify each instance when a key is destroyed by this method. In each instance the evaluator shall verify all keys capable of decrypting the target key are destroyed in accordance with a specified key destruction method in FCS_CKM_EXT.4.1 The evaluator shall verify that all of the keys capable of decrypting the target key are not able to be derived to reestablish the keychain after their destruction.
>
> **Operational Guidance**
>
> There are a variety of concerns that may prevent or delay key destruction in some cases. The evaluator will check that the guidance documentation identifies configurations or circumstances that may not strictly conform to the key destruction requirement, and that this description is consistent with the relevant parts of the TSS and any other relevant Required Supplementary Information. The evaluator will check that the guidance documentation provides guidance on situations where key destruction may be delayed at the physical layer and how such situations can be avoided or mitigated if possible.

Some examples of what is expected to be in the documentation are provided here.

When the TOE does not have full access to the physical memory, it is possible that the storage may be implementing wear-leveling and garbage collection. This may create additional copies of the key that are logically inaccessible but persist physically. In this case, to mitigate this the drive should support the TRIM command and implements garbage collection to destroy these persistent copies when not actively engaged in other tasks.

Drive vendors implement garbage collection in a variety of different ways, as such there is a variable amount of time until data is truly removed from these solutions. There is a risk that data may persist for a longer amount of time if it is contained in a block with other data not ready for erasure. To reduce this risk, the operating system and file system of the OE should support TRIM, instructing the non-volatile memory to erase copies via garbage collection upon their deletion. If a RAID array is being used, only set-ups that support TRIM are utilized. If the drive is connected via PCI-Express, the operating system supports TRIM over that channel.

The drive should be healthy and contains minimal corrupted data and should be end-of-lifed before a significant amount of damage to drive health occurs, this minimizes the risk that small amounts of potentially recoverable data may remain in damaged areas of the drive.

- **Test 1:** Applied to each key held as in volatile memory and subject to destruction by overwrite by the TOE (whether or not the value is subsequently encrypted for storage in volatile or non-volatile memory). In the case where the only selection made for the destruction method key was removal of power, then this test is unnecessary. The evaluator will:

  1. Record the value of the key in the TOE subject to clearing.
  2. Cause the TOE to perform a normal cryptographic processing with the key from Step #1.
  3. Cause the TOE to clear the key.
  4. Cause the TOE to stop the execution but not exit.
  5. Cause the TOE to dump the entire memory of the TOE into a binary file.
  6. Search the content of the binary file created in Step #5 for instances of the known key value from Step #1.

  Steps 1-6 ensure that the complete key does not exist anywhere in volatile memory. If a copy is found, then the test fails.

- **Test 2:** Applied to each key help in non-volatile memory and subject to destruction by the TOE. The evaluator will use special tools (as needed), provided by the TOE developer if necessary, to ensure the tests function as intended.

1. Identify the purpose of the key and what access should fail when it is deleted. (e.g. the data encryption key being deleted would cause data decryption to fail.)
2. Cause the TOE to clear the key.
3. Have the TOE attempt the functionality that the cleared key would be necessary for.

The test succeeds if step 3 fails.

Tests 3 and 4 do not apply for the selection **instructing the underlying platform to destroy the representation of the key**, as the TOE has no visibility into the inner workings and completely relies on the underlying platform.

- **Test 3:** The following tests are used to determine the TOE is able to request the platform to overwrite the key with a TOE supplied pattern.

  Applied to each key held in non-volatile memory and subject to destruction by overwrite by the TOE. The evaluator will use a tool that provides a logical view of the media (e.g., MBR file system):

  1. Record the value of the key in the TOE subject to clearing.
  2. Cause the TOE to perform a normal cryptographic processing with the key from Step #1.
  3. Cause the TOE to clear the key.
  4. Search the logical view that the key was stored in for instances of the known key value from Step #1. If a copy is found, then the test fails.

- **Test 4:** Applied to each key held as non-volatile memory and subject to destruction by overwrite by the TOE. The evaluator will use a tool that provides a logical view of the media:

  1. Record the logical storage location of the key in the TOE subject to clearing.
  2. Cause the TOE to perform a normal cryptographic processing with the key from Step #1.
  3. Cause the TOE to clear the key.
  4. Read the logical storage location in Step #1 of non-volatile memory to ensure the appropriate pattern is utilized.

  The test succeeds if correct pattern is used to overwrite the key in the memory location. If the pattern is not found the test fails.

13.1 Documentation Review Activity

13.1.1 Findings

According to the SFR definition, only the key destruction method for volatile memory is selected. The evaluator has reviewed the information provided in TSS, section **6.2.2 Cryptographic Algorithm Validation**. This section includes the zeroization method for volatile memory. It is carried out using the *RtlSecureZeroMemory* function which overwrites with zeros the memory space indicated (the source code of this function is provided below). The TSS also states that:

> *Windows overwrites each intermediate storage area for plaintext key/critical cryptographic security parameter (i.e., any storage, such as memory buffers for the key or plaintext password which was typed by the user, that is included in the path of such data).*
>
> [...]
>
> *The following table describes the keys and secrets used for **networking and data protection**; when these ephemeral keys or secrets are no longer needed for a network session, due to either normal end of the session or abnormal termination, or after protecting sensitive data using DPAPI, they are deleted as described above and in section 5.1.2.4. Note that the administrative guidance precludes hibernating the computer and so these keys are not persisted into volatile storage.*
>
> [...]

Key	Description
Symmetric encryption/decryption keys	Keys used for AES (FIPS 197) encryption/decryption for IPsec ESP, TLS, Wi-Fi.
HMAC keys	Keys used for HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, and HMAC-SHA512 (FIPS 198-1) as part of IPsec.
Asymmetric ECDSA Public Keys	Keys used for the verification of ECDSA digital signatures using the P-256 , P-384, and P-521 curves (FIPS 186-4) for TLS, IPsec traffic, and peer authentication.
Asymmetric ECDSA Private Keys	Keys used for the calculation of ECDSA digital signatures using the P-256 , P-384, and P-521 curves (FIPS 186-4) for TLS, IPsec traffic and peer authentication.

Key	Description
Asymmetric RSA Public Keys	Keys used for the verification of RSA digital signatures (FIPS 186-4) for IPsec, TLS, Wi-Fi and signed product updates.
Asymmetric RSA Private Keys	Keys used for the calculation of RSA digital signatures (FIPS 186-4) for IPsec, TLS, and Wi-Fi as well as TPM-based health attestations. The key size can be 2048 or 3072 bits.
Asymmetric DSA Private Keys	Keys used for the calculation of DSA digital signatures (FIPS 186-4) for IPsec and TLS. The key size can be 2048 or 3072 bits.
Asymmetric DSA Public Keys	Keys used for the verification of DSA digital signatures (FIPS 186-4) for IPsec and TLS. The key size can be 2048 or 3072 bits.
DH Private and Public values	Private and public values using MODP-2048, MODP-3072, MODP-4096 for Diffie-Hellman key establishment for IKE with only MODP-2048; and ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144 Diffie-Hellman key establishment for TLS.
ECDH Private and Public values	Private and public values using the P-256, P-384, and P-521 curves in EC Diffie-Hellman key establishment for TLS and IKE.
DPAPI HMAC	**[Text intentionally left blank]**
DPAPI master secret	512-bit random value used by DPAPI.
DPAPI master AES key	256-bit encryption key that protects the DPAPI master secret.
DPAPI AES key	256-bit encryption key used by DPAPI.
DRBG seed	**[Text intentionally left blank]** seed for the main DRBG, zeroized during reseeding.

These keys are generated when they are needed using an approved RNG algorithm (according to *SP 800-90*) as part of the generation process.

In addition, neither the TSS nor the operational guidance identify any configuration or circumstances that do not strictly conform to the key destruction requirement.

13.1.2 Verdict

The evaluator considers that the TSS identifies for all volatile keys involved in the cryptographic processes under evaluation (*networking and DPAPI*), when are generated, the purpose of its usage and how are zeroized when they are no longer needed using the *RtlSecureZeroMemory* internal function. This information is in the TSS sections **6.2.1 Cryptographic Algorithms and Operations**, **6.2.2 Cryptographic Algorithm Validation** and **6.2.4 Protecting Data with DPAPI**.

Moreover, neither the TSS nor the ***Operational Guidance*** document, identify any configuration or circumstances that do not strictly conform to the key destruction requirement.

Due to this, the evaluator considers that the information provided in the TSS is enough and the requirements established in the assurance activity section are fulfilled. Hence, the **PASS** verdict is assigned to the documentation review activity.

13.2 Test Activity

13.2.1 Test 1

13.2.1.1 Setup

Before the test execution, the following setup conditions must be fulfilled:

- A Web Server supporting TLS 1.2 connections is available (*IIS*).
- A Web Client is available on the TOE (e.g. *Internet Explorer*).
- A Kernel debugging environment is configured.

13.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

13.2.1.3 Results

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

13.2.1.4 Verdict

After performing several tests, to confirm that the volatile keys defined by the vendor in the table 28 of the ***Security Target*** document are zeroized, the evaluator considers that the behaviour described by the vendor matches with the one obtained as result of the testing. Therefore, the evaluator assumes that the vendor position is valid for all keys listed.

Due to this, the evaluator considers that the result obtained from the test activity demonstrate the fulfilment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

13.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FCS_CKM_EXT.4.1 requirement.

14 FCS_COP.1.1(1)

The assurance activity for the **FCS_COP.1.1(3)** requirement is stated as follows:

> The evaluator will perform the following activities based on the selections in the ST.
>
> The following tests require the developer to provide access to a test application that provides the evaluator with tools that are typically not found in the production application.
>
> he evaluator will verify that the AGD documents contains instructions required to configure the OS to use the required modes and key sizes. The evaluator will execute all instructions as specified to configure the OS to the appropriate state. The evaluator will perform all of the following tests for each algorithm implemented by the OS and used to satisfy the requirements of this PP:
>
> **AES-CBC Known Answer Tests**
>
> There are four Known Answer Tests (KATs), described below. In all KATs, the plaintext, ciphertext, and IV values shall be 128-bit blocks. The results from each test may either be obtained by the evaluator directly or by supplying the inputs to the implementer and receiving the results in response. To determine correctness, the evaluator will compare the resulting values to those obtained by submitting the same inputs to a known good implementation.
>
> - KAT-1. To test the encrypt functionality of AES-CBC, the evaluator will supply a set of 10 plaintext values and obtain the ciphertext value that results from AES-CBC encryption of the given plaintext using a key value of all zeros and an IV of all zeros. Five plaintext values shall be encrypted with a 128-bit all-zeros key, and the other five shall be encrypted with a 256-bit all- zeros key. To test the decrypt functionality of AES-CBC, the evaluator will perform the same test as for encrypt, using 10 ciphertext values as input and AES-CBC decryption.
> - KAT-2. To test the encrypt functionality of AES-CBC, the evaluator will supply a set of 10 key values and obtain the ciphertext value that results from AES-CBC encryption of an all-zeros plaintext using the given key value and an IV of all zeros. Five of the keys shall be 128-bit keys, and the other five shall be 256-bit keys. To test the decrypt functionality of AES-CBC, the evaluator will perform the same test as for encrypt, using an all-zero ciphertext value as input and AES-CBC decryption.
> - KAT-3. To test the encrypt functionality of AES-CBC, the evaluator will supply the two sets of key values described below and obtain the ciphertext value that results from AES encryption of an all-zeros plaintext using the given key value and an IV of all zeros. The first set of keys shall have 128

128-bit keys, and the second set shall have 256 256-bit keys. Key i in each set shall have the leftmost i bits be ones and the rightmost N-i bits be zeros, for i in [1,N]. To test the decrypt functionality of AES-CBC, the evaluator will supply the two sets of key and ciphertext value pairs described below and obtain the plaintext value that results from AES-CBC decryption of the given ciphertext using the given key and an IV of all zeros. The first set of key/ciphertext pairs shall have 128 128-bit key/ciphertext pairs, and the second set of key/ciphertext pairs shall have 256 256-bit key/ciphertext pairs. Key i in each set shall have the leftmost i bits be ones and the rightmost N-i bits be zeros, for i in [1,N]. The ciphertext value in each pair shall be the value that results in an all-zeros plaintext when decrypted with its corresponding key.

- KAT-4. To test the encrypt functionality of AES-CBC, the evaluator will supply the set of 128 plaintext values described below and obtain the two ciphertext values that result from AES-CBC encryption of the given plaintext using a 128-bit key value of all zeros with an IV of all zeros and using a 256-bit key value of all zeros with an IV of all zeros, respectively. Plaintext value i in each set shall have the leftmost i bits be ones and the rightmost 128-i bits be zeros, for i in [1,128]. To test the decrypt functionality of AES-CBC, the evaluator will perform the same test as for encrypt, using ciphertext values of the same form as the plaintext in the encrypt test as input and AES-CBC decryption.

AES-CBC Multi-Block Message Test The evaluator will test the encrypt functionality by encrypting an i-block message where $1 < i \leq 10$. The evaluator will choose a key, an IV and plaintext message of length i blocks and encrypt the message, using the mode to be tested, with the chosen key and IV. The ciphertext shall be compared to the result of encrypting the same plaintext message with the same key and IV using a known good implementation. The evaluator will also test the decrypt functionality for each mode by decrypting an i-block message where $1 < i \leq 10$. The evaluator will choose a key, an IV and a ciphertext message of length i blocks and decrypt the message, using the mode to be tested, with the chosen key and IV. The plaintext shall be compared to the result of decrypting the same ciphertext message with the same key and IV using a known good implementation.

AES-CCM Tests The evaluator will test the generation-encryption and decryption-verification functionality of AES-CCM for the following input parameter and tag lengths:

- 128 bit and 256 bit keys
- Two payload lengths. One payload length shall be the shortest supported payload length, greater than or equal to zero bytes. The other payload

length shall be the longest supported payload length, less than or equal to 32 bytes (256 bits).

- Two or three associated data lengths . One associated data length shall be 0, if supported. One associated data length shall be the shortest supported payload length, greater than or equal to zero bytes. One associated data length shall be the longest supported payload length, less than or equal to 32 bytes (256 bits). If the implementation supports an associated data length of 2 16 bytes, an associated data length of 216 bytes shall be tested.
- Nonce lengths. All supported nonce lengths between 7 and 13 bytes, inclusive, shall be tested.
- Tag lengths. All supported tag lengths of 4, 6, 8, 10, 12, 14 and 16 bytes shall be tested.

To test the generation-encryption functionality of AES-CCM, the evaluator will perform the following four tests:

- **Test 1**: For EACH supported key and associated data length and ANY supported payload, nonce and tag length, the evaluator will supply one key value, one nonce value and 10 pairs of associated data and payload values and obtain the resulting ciphertext.
- **Test 2**: For EACH supported key and payload length and ANY supported associated data, nonce and tag length, the evaluator will supply one key value, one nonce value and 10 pairs of associated data and payload values and obtain the resulting ciphertext.
- **Test 3**: For EACH supported key and nonce length and ANY supported associated data, payload and tag length, the evaluator will supply one key value and 10 associated data, payload and nonce value 3-tuples and obtain the resulting ciphertext.
- **Test 4**: For EACH supported key and tag length and ANY supported associated data, payload and nonce length, the evaluator will supply one key value, one nonce value and 10 pairs of associated data and payload values and obtain the resulting ciphertext.

To determine correctness in each of the above tests, the evaluator will compare the ciphertext with the result of generation-encryption of the same inputs with a known good implementation.

To test the decryption-verification functionality of AES-CCM, for EACH combination of supported associated data length, payload length, nonce length and tag length, the evaluator shall supply a key value and 15 nonce, associated data and ciphertext 3-tuples and obtain either a FAIL result or a PASS result with the decrypted payload. The evaluator will supply 10 tuples that should FAIL and 5 that should PASS per set of 15.

Additionally, the evaluator will use tests from the IEEE 802.11-02/362r6 document "Proposed Test vectors for IEEE 802.11 TGi", dated September 10, 2002, Section 2.1 AESCCMP Encapsulation Example and Section 2.2 Additional AES CCMP Test Vectors to further verify the IEEE 802.11-2007 implementation of AES-CCMP. **AES-GCM Test** The evaluator will test the authenticated encrypt functionality of AES-GCM for each combination of the following input parameter lengths:

- 128 bit and 256 bit keys
- Two plaintext lengths. One of the plaintext lengths shall be a non-zero integer multiple of 128 bits, if supported. The other plaintext length shall not be an integer multiple of 128 bits, if supported.
- Three AAD lengths. One AAD length shall be 0, if supported . One AAD length shall be a non-zero integer multiple of 128 bits, if supported. One AAD length shall not be an integer multiple of 128 bits, if supported.
- Two IV lengths. If 96 bit IV is supported, 96 bits shall be one of the two IV lengths tested.

The evaluator will test the encrypt functionality using a set of 10 key, plaintext, AAD, and IV tuples for each combination of parameter lengths above and obtain the ciphertext value and tag that results from AES-GCM authenticated encrypt. Each supported tag length shall be tested at least once per set of 10. The IV value may be supplied by the evaluator or the implementation being tested, as long as it is known.

The evaluator will test the decrypt functionality using a set of 10 key, ciphertext, tag, AAD, and IV 5-tuples for each combination of parameter lengths above and obtain a Pass/Fail result on authentication and the decrypted plaintext if Pass. The set shall include five tuples that Pass and five that Fail.

The results from each test may either be obtained by the evaluator directly or by supplying the inputs to the implementer and receiving the results in response. To determine correctness, the evaluator will compare the resulting values to those obtained by submitting the same inputs to a known good implementation.

XTS-AES Test The evaluator will test the encrypt functionality of XTS-AES for each combination of the following input parameter lengths:

- 256 bit (for AES-128) and 512 bit (for AES-256) keys
- Three data unit (i.e., plaintext) lengths. One of the data unit lengths shall be a nonzero integer multiple of 128 bits, if supported. One of the data unit lengths shall be an integer multiple of 128 bits, if supported. The third data unit length shall be either the longest supported data unit length or 216 bits, whichever is smaller

using a set of 100 (key, plaintext and 128-bit random tweak value) 3-tuples and obtain the ciphertext that results from XTS-AES encrypt.

The evaluator may supply a data unit sequence number instead of the tweak value if the implementation supports it. The data unit sequence number is a base-10 number ranging between 0 and 255 that implementations convert to a tweak value internally.

The evaluator will test the decrypt functionality of XTS-AES using the same test as for encrypt, replacing plaintext values with ciphertext values and XTS-AES encrypt with XTSAES decrypt.

AES Key Wrap (AES-KW) and Key Wrap with Padding (AES-KWP) Test

The evaluator will test the authenticated encryption functionality of AES-KW forEACH combination of the following input parameter lengths:

- 128 and 256 bit key encryption keys (KEKs)
- Three plaintext lengths. One of the plaintext lengths shall be two semi-blocks (128 bits). One of the plaintext lengths shall be three semi-blocks (192 bits). The third data unit length shall be the longest supported plaintext length less than or equal to 64 semi-blocks (4096 bits).

using a set of 100 key and plaintext pairs and obtain the ciphertext that results from AES-KW authenticated encryption. To determine correctness, the evaluator will use the AES-KW authenticated-encryption function of a known good implementation.

The evaluator will test the authenticated-decryption functionality of AES-KW using the same test as for authenticated-encryption, replacing plaintext values with ciphertext values and AES-KW authenticated-encryption with AES-KW authenticated-decryption.

The evaluator will test the authenticated-encryption functionality of AES-KWP using the same test as for AES-KW authenticated-encryption with the following change in the three plaintext lengths:

- One plaintext length shall be one octet. One plaintext length shall be 20 octets (160 bits).
- One plaintext length shall be the longest supported plaintext length less than or equal to 512 octets (4096 bits).

The evaluator will test the authenticated-decryption functionality of AES-KWP using the same test as for AES-KWP authenticated-encryption, replacing plaintext values with ciphertext values and AES-KWP authenticated-encryption with AES-KWP authenticated-decryption.

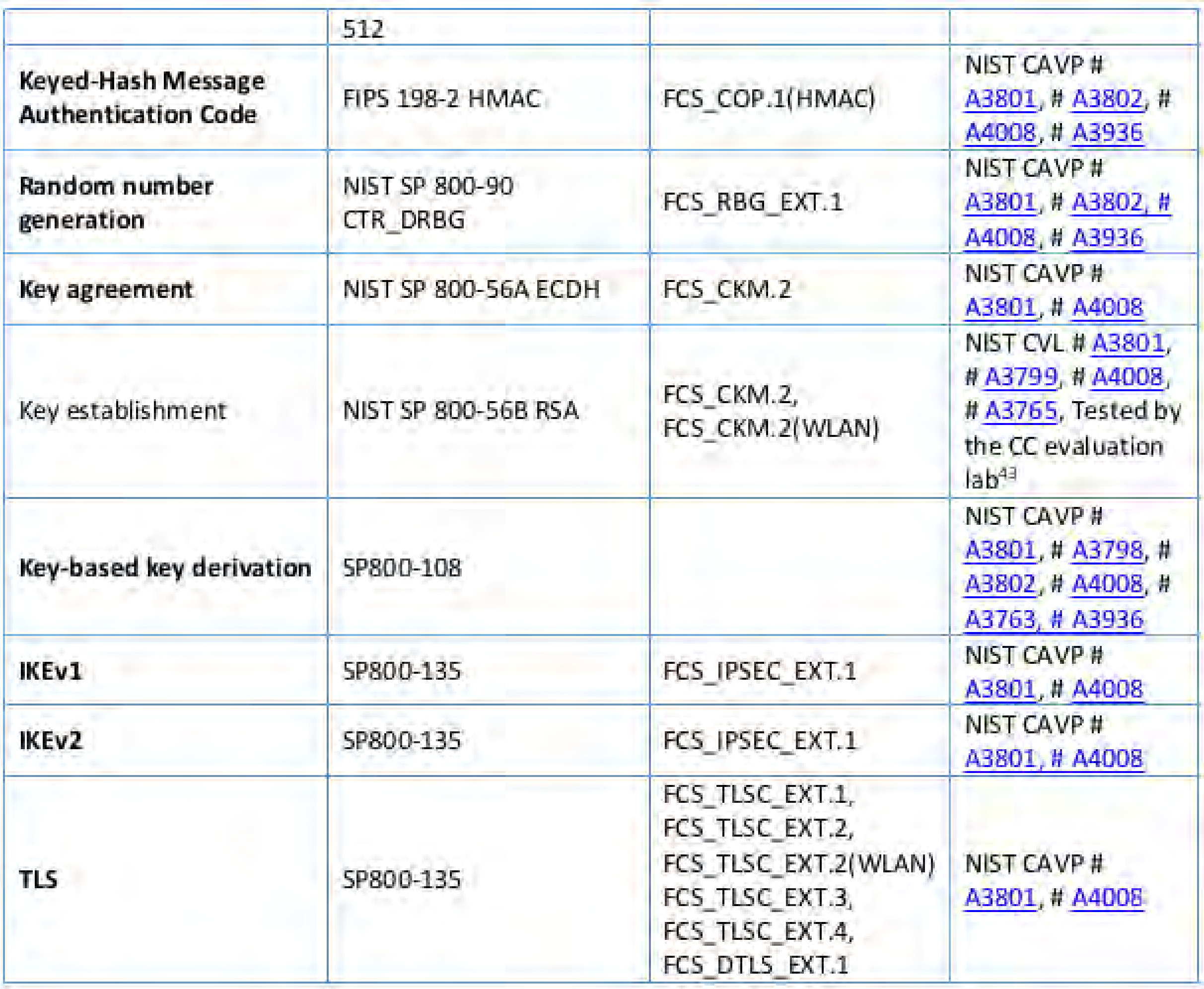
14.1 Documentation Review Activity

14.1.1 Findings

The evaluator has reviewed the ***Security Target*** document and the information provided in the TSS, section **6.2.2 Cryptographic Algorithm Validation**. This section includes the following tables of the cryptographic algorithms supported by Windows 11, Windows 10 versions, Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge.

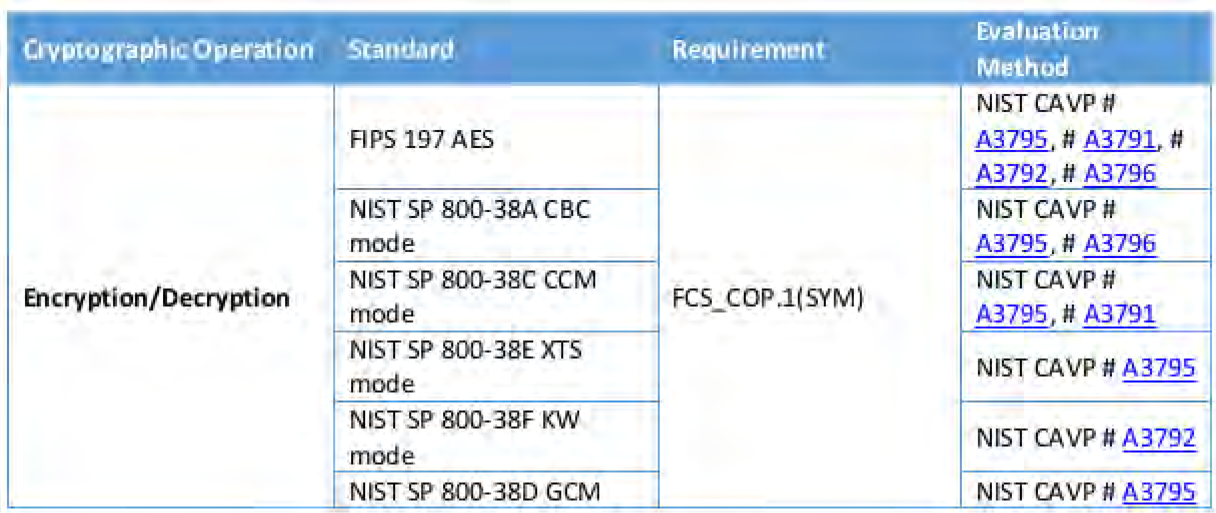
14.1.1.1 Cryptographic Algorithm Standards and Evaluation Methods for Windows 11 (version 22H2)

Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3801, # A3797, # A3798, # A3802, # A4008, # A3748, # A3763, # A3936
	NIST SP 800-38A CBC mode		NIST CAVP # A3801, # A4008, # A3802, # A3936
	NIST SP 800-38C CCM mode		NIST CAVP # A3801, # A3797, # A4008, # A3748
	NIST SP 800-38E XTS mode		NIST CAVP # A3801, # A4008
	NIST SP 800-38F KW mode		NIST CAVP # A3798, # A3763
	NIST SP 800-38D GCM mode		NIST CAVP # A3801, # A4008
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP # A3801, # A4008
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3801, # A3802, # A4008, #A3799, # A3765, # A3936
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3801, #A3799, # A3800, # A3802, # A4008, # A3799, # A3765, # A3936
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3801, # A4008
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3801, # A3802	NIST CAVP # A3801, # A4008
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3801, # A3799, # A3802, # A4008, # A3765, # A3936
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3801, # A3799, # A4008, # A3936
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-	FCS_COP.1 (HASH)	NIST CAVP # A3801, # A4008

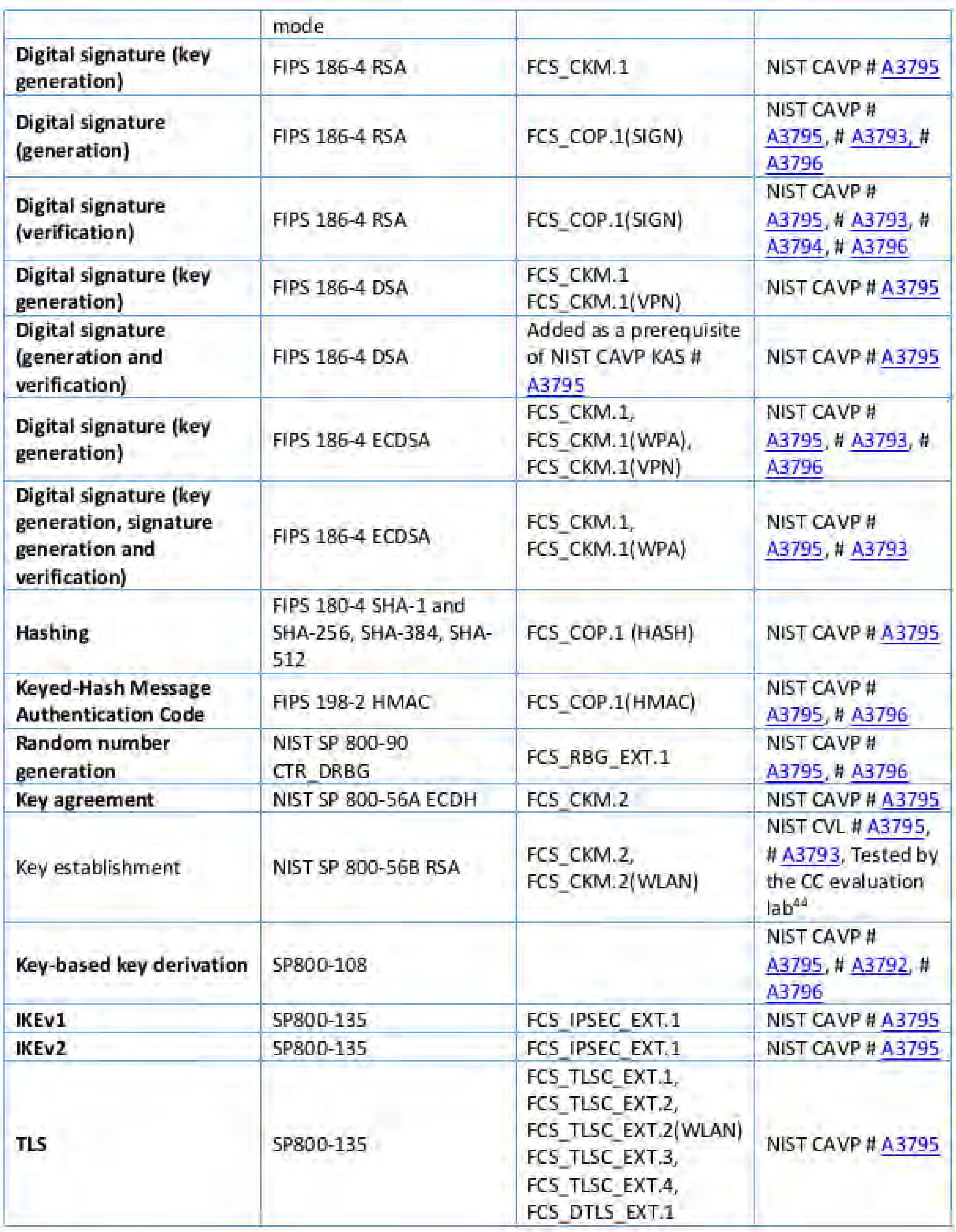


	512		
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3801, # A3802, # A4008, # A3936
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3801, # A3802, # A4008, # A3936
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3801, # A4008
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2, FCS_CKM.2(WLAN)	NIST CVL # A3801, # A3799, # A4008, # A3765, Tested by the CC evaluation lab[43]
Key-based key derivation	SP800-108		NIST CAVP # A3801, # A3798, # A3802, # A4008, # A3763, # A3936
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3801, # A4008
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3801, # A4008
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3801, # A4008

14.1.1.2 Cryptographic Algorithm Standards and Evaluation Methods for Windows 10 (version 22H2)

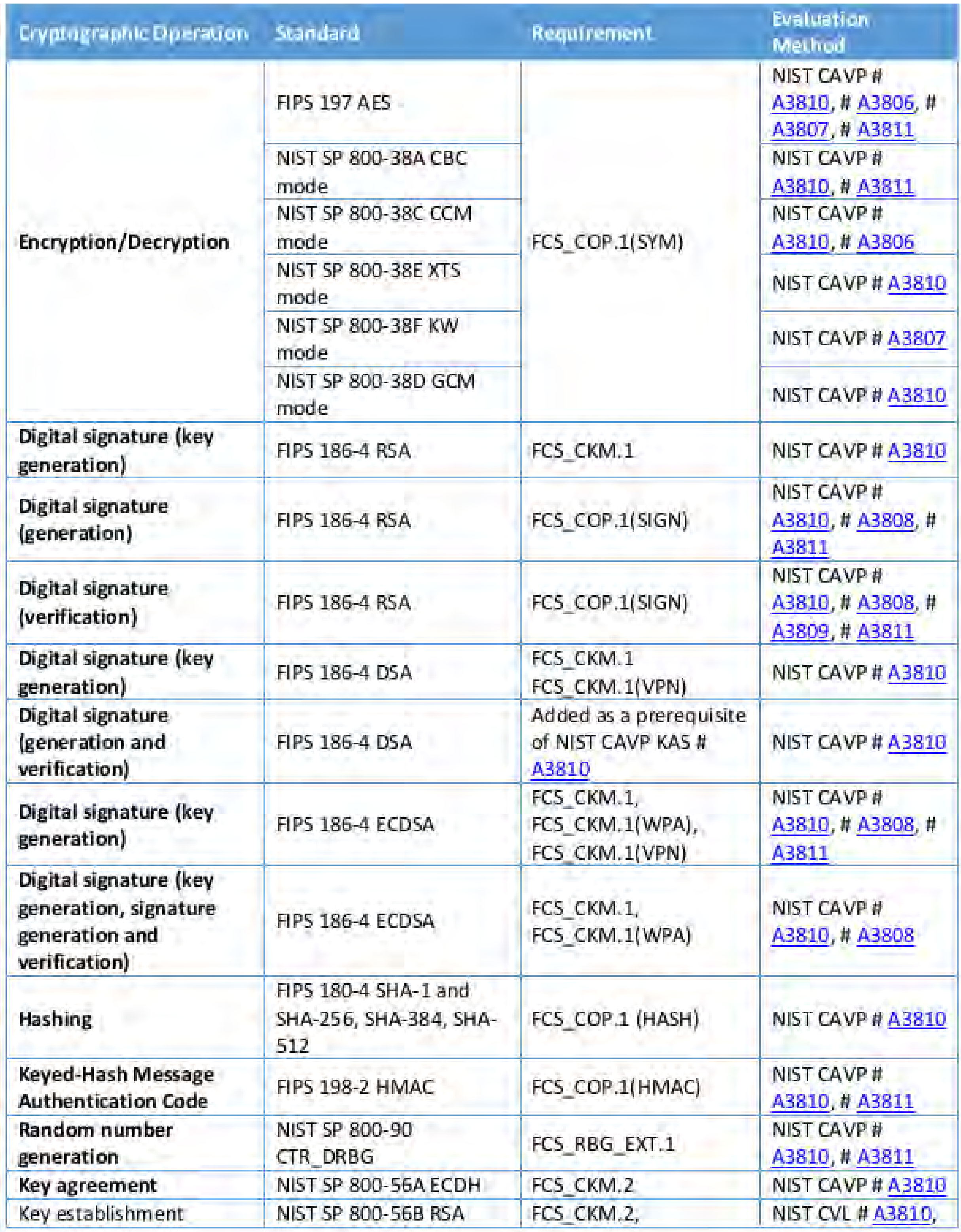


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3795, # A3791, # A3792, # A3796
	NIST SP 800-38A CBC mode		NIST CAVP # A3795, # A3796
	NIST SP 800-38C CCM mode		NIST CAVP # A3795, # A3791
	NIST SP 800-38E XTS mode		NIST CAVP # A3795
	NIST SP 800-38F KW mode		NIST CAVP # A3792
	NIST SP 800-38D GCM		NIST CAVP # A3795

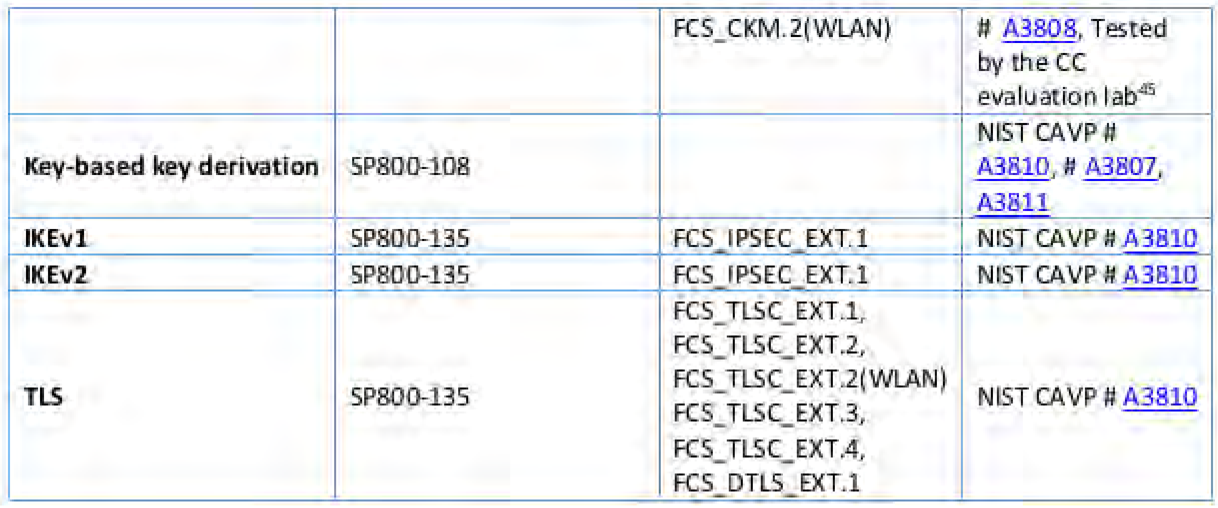


	mode		
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP # A3795
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3795, # A3793, # A3796
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3795, # A3793, # A3794, # A3796
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3795
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3795	NIST CAVP # A3795
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3795, # A3793, # A3796
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3795, # A3793
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3795
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3795, # A3796
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3795, # A3796
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3795
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2, FCS_CKM.2(WLAN)	NIST CVL # A3795, # A3793, Tested by the CC evaluation lab[44]
Key-based key derivation	SP800-108		NIST CAVP # A3795, # A3792, # A3796
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3795
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3795
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3795

14.1.1.3 Cryptographic Algorithm Standards and Evaluation Methods for Windows Server 2022 and Windows Server Datacenter: Azure Edition

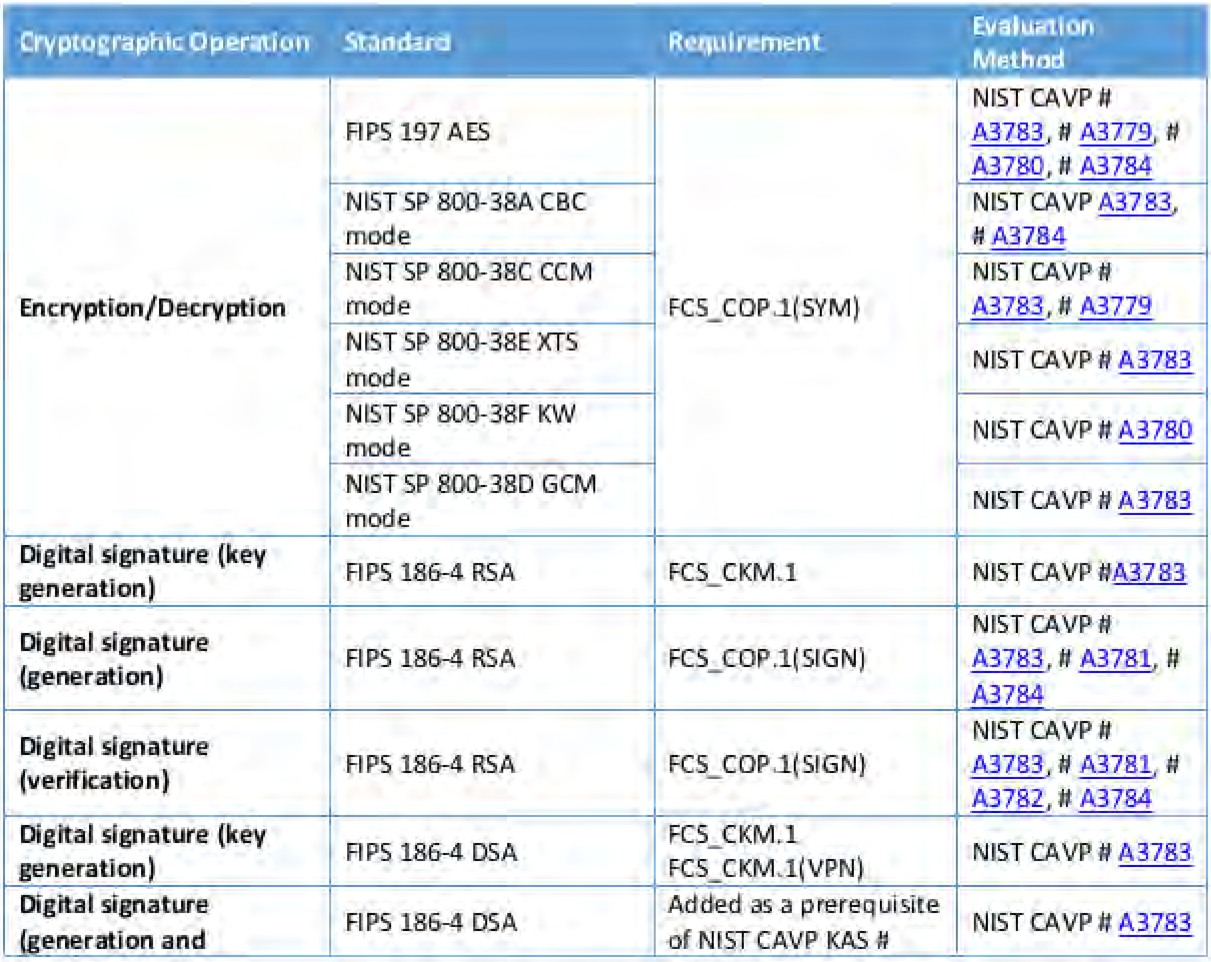


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3810, # A3806, # A3807, # A3811
	NIST SP 800-38A CBC mode		NIST CAVP # A3810, # A3811
	NIST SP 800-38C CCM mode		NIST CAVP # A3810, # A3806
	NIST SP 800-38E XTS mode		NIST CAVP # A3810
	NIST SP 800-38F KW mode		NIST CAVP # A3807
	NIST SP 800-38D GCM mode		NIST CAVP # A3810
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP # A3810
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3810, # A3808, # A3811
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3810, # A3808, # A3809, # A3811
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3810
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3810	NIST CAVP # A3810
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3810, # A3808, # A3811
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3810, # A3808
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3810
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3810, # A3811
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3810, # A3811
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3810
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2,	NIST CVL # A3810,

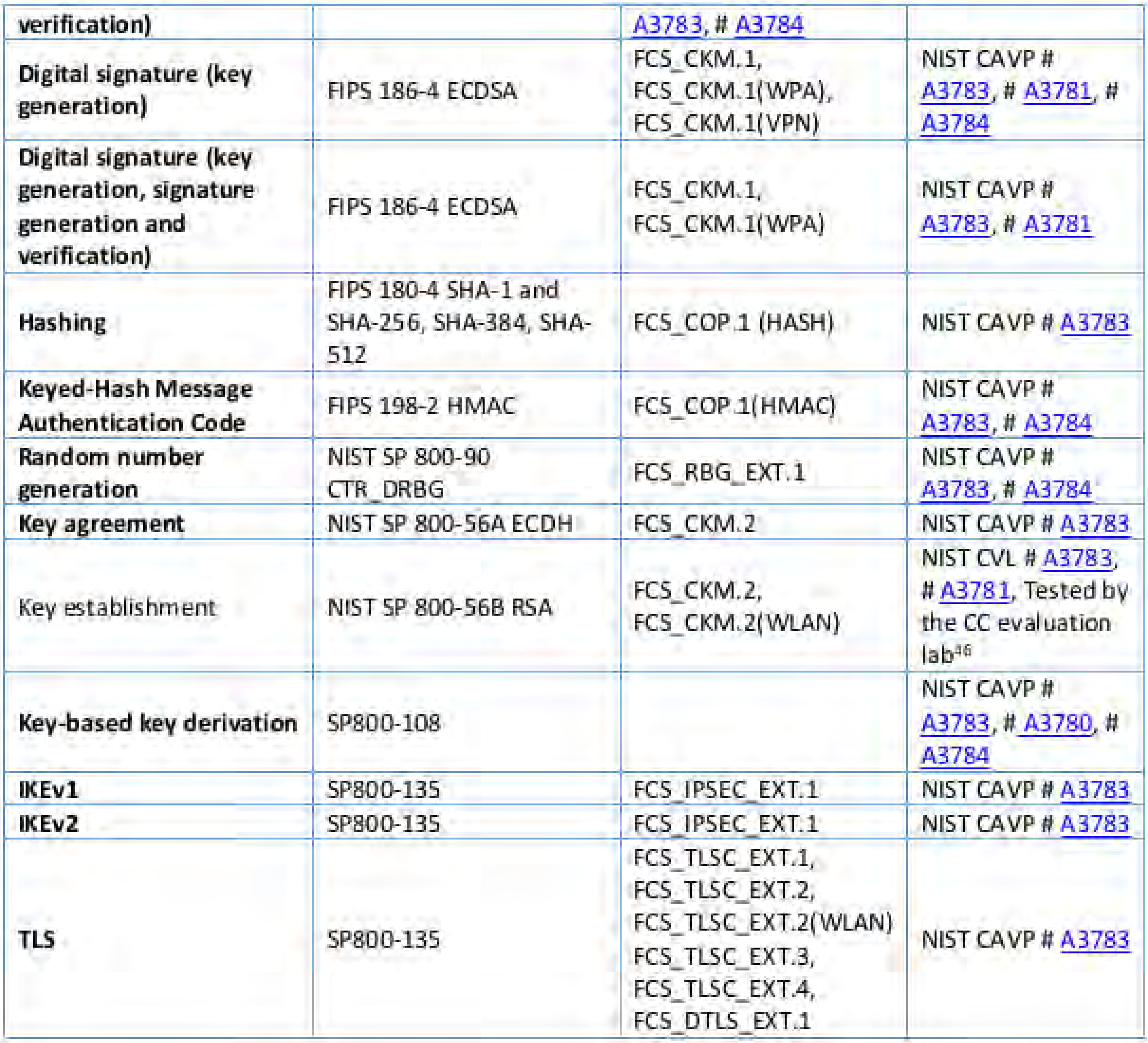


		FCS_CKM.2(WLAN)	# A3808, Tested by the CC evaluation lab[45]
Key-based key derivation	SP800-108		NIST CAVP # A3810, # A3807, A3811
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3810
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3810
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3810

14.1.1.4 Cryptographic Algorithm Standards and Evaluation Methods for Windows Server Azure Stack HCIv2 version 22H2

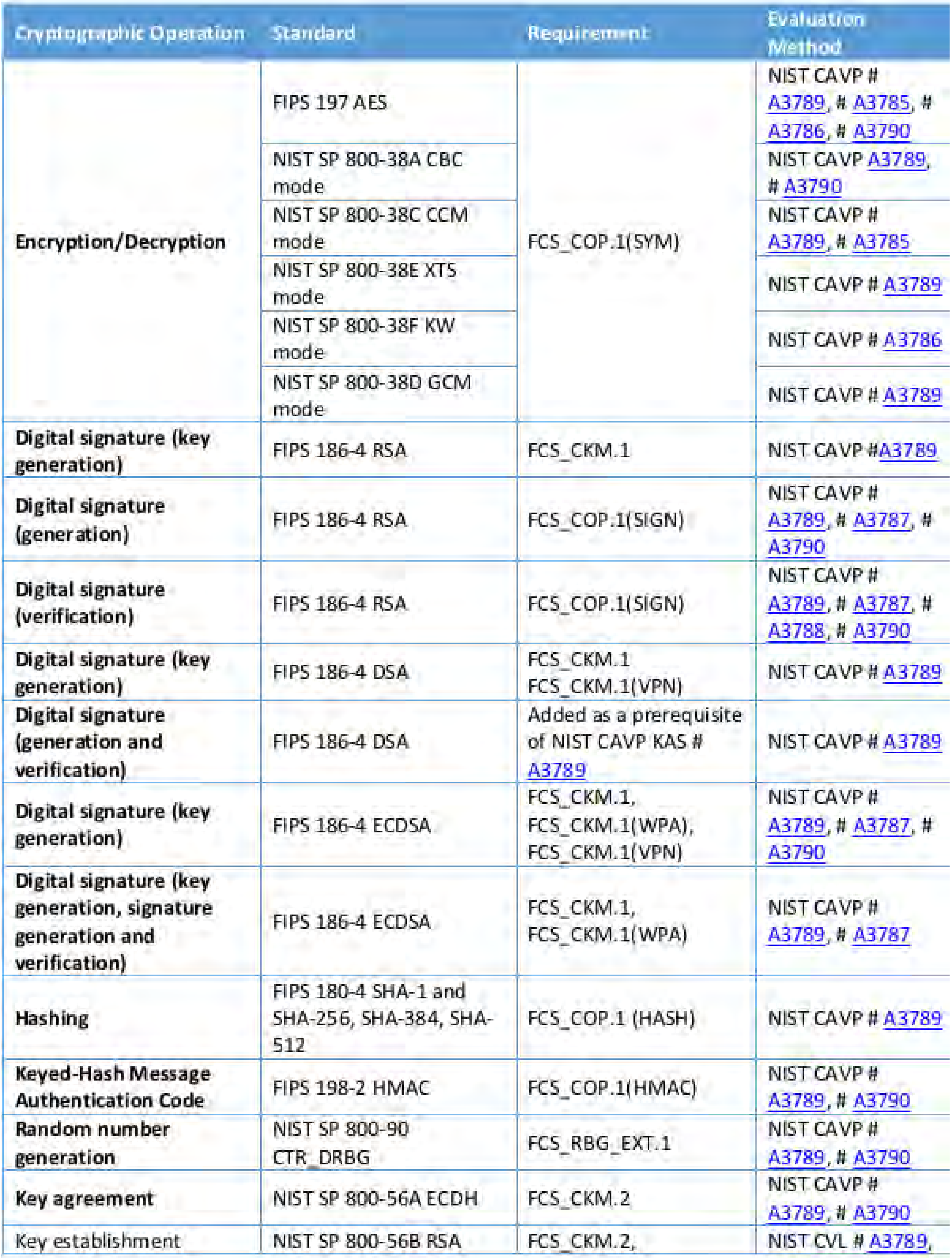


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3783, # A3779, # A3780, # A3784
	NIST SP 800-38A CBC mode		NIST CAVP A3783, # A3784
	NIST SP 800-38C CCM mode		NIST CAVP # A3783, # A3779
	NIST SP 800-38E XTS mode		NIST CAVP # A3783
	NIST SP 800-38F KW mode		NIST CAVP # A3780
	NIST SP 800-38D GCM mode		NIST CAVP # A3783
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP #A3783
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3783, # A3781, # A3784
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3783, # A3781, # A3782, # A3784
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3783
Digital signature (generation and	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS #	NIST CAVP # A3783

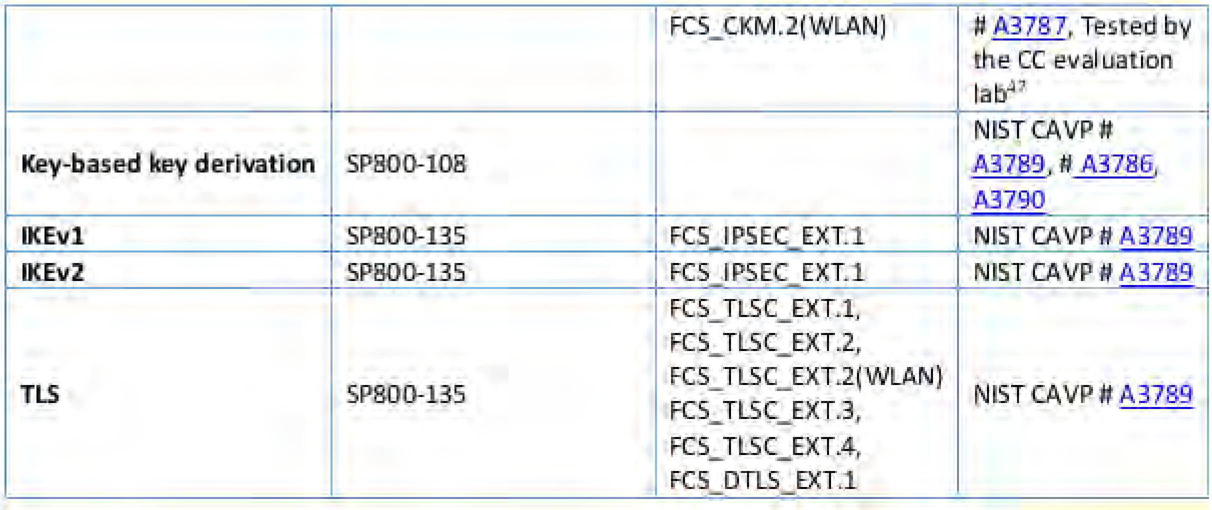


verification)		A3783, # A3784	
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3783, # A3781, # A3784
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3783, # A3781
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3783
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3783, # A3784
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3783, # A3784
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3783
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2, FCS_CKM.2(WLAN)	NIST CVL # A3783, # A3781, Tested by the CC evaluation lab[46]
Key-based key derivation	SP800-108		NIST CAVP # A3783, # A3780, # A3784
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3783
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3783
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3783

14.1.1.5 Cryptographic Algorithm Standards and Evaluation Methods for Azure Stack Hub and Azure Stack Edge



Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3789, # A3785, # A3786, # A3790
	NIST SP 800-38A CBC mode		NIST CAVP A3789, # A3790
	NIST SP 800-38C CCM mode		NIST CAVP # A3789, # A3785
	NIST SP 800-38E XTS mode		NIST CAVP # A3789
	NIST SP 800-38F KW mode		NIST CAVP # A3786
	NIST SP 800-38D GCM mode		NIST CAVP # A3789
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP #A3789
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3789, # A3787, # A3790
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3789, # A3787, # A3788, # A3790
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3789
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3789	NIST CAVP # A3789
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3789, # A3787, # A3790
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3789, # A3787
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3789
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3789, # A3790
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3789, # A3790
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3789, # A3790
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2,	NIST CVL # A3789,



		FCS_CKM.2(WLAN)	# A3787, Tested by the CC evaluation lab[47]
Key-based key derivation	SP800-108		NIST CAVP # A3789, # A3786, A3790
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3789
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3789
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3789

The ***Operational Guidance*** document, states that for the evaluated version the following security policy needs to be applied (Section 3.2.5):

- Local Policies \ Security Options\System cryptography: Use FIPS 140 compliant cryptographic algorithms, including encryption, hashing and signing algorithm.

After applying this policy, only FIPS certified algorithms can be used, including the AES algorithms defined in the tables above.

The TOE satisfies the fulfilment of the cryptographic algorithms, *AES-XTS, AES-CBC, AES-GCM, AES-CCMP, AES Key Wrap (KW), AES-CCM, AES-CCMP-256 and AES-GCMP-256* as specified in the ***Security Target*** document. A complete explanation is provided with more detail in the *FCS_CKM.1/WLAN* requirement.

14.1.2 Verdict

The assurance activity does not require any documentation information. Nevertheless, the evaluator has provided information about the Signature algorithms supported by the OS.

Hence, the **PASS** verdict is assigned to the documentation review activity.

14.2 Test Activity

Based on the SFR instantiation included in the security target, the vendor has selected the following AES modes:

1. AES-CBC
2. AES-GCM
3. AES-XTS

4. AES-KW
5. AES-CCM
6. AES-CCMP (according to IEEE 802.11ac-2013 is composed of CTR with CBC-MAC)
7. AES-GCMP (according to IEEE 802.11ac-2013 is composed of GCM with GMAC)

In addition to the Common Criteria evaluation, the laboratory has also performed the CAVP validation for these and other algorithms. The general procedure that has been followed during the evaluation in order to demonstrate the correctness of the cryptographic functionality is as follows:

1. The laboratory has used the same test vectors used as part of the CAVP validation. For symmetric algorithms, the following types of test are performed:

    - Algorithm Functional Test (AFT): The main goal for these tests is verify the implementation of the normal ‘encrypt’ or ‘decrypt’ operation. AFTs cause the implementation to exercise normal operations on a single block, multiple blocks, or partial blocks. In some cases random data is used, in others, static, predetermined tests are provided. AFTs of block cipher are designed to verify that the logical components of the cipher are operating correctly.

    - Monte Carlo Test (MCT). These tests exercise the implementation strenuous circumstances. The implementation must process the test vectors according to the correct algorithm and mode. MCTs can help detect potential memory leaks over time, and problems in allocation of resources, addressing variables, error handling and generally improper behavior in response to random inputs.

    - Counter Mode Test. Counter tests are specifically for counter modes (AES-CTR, used as part of AES-CCMP) and require an implementation to exercise their counter mechanism. The test vectors include a long message for encryption or decryption and back-compute the IVs used by the implementation. These IVs are then verified for uniqueness and an increasing (or decreasing) nature. The implementation processes these tests as normal algorithm functional tests.

2. The laboratory has exercised the cryptographic functionalities of the TOE by invoking the appropriate API in order to resolve the test vectors. The result of this step is a .json file which includes the associated response generated by the TOE per each test vector.

3. The laboratory has created a testing tool in order to exercise the BOTAN implementation for the target cryptographic algorithms. This tool receives the initial .json file with the test vectors as well as the .json file obtained as a result of the step 2. After parsing the information, the testing tool invokes the BOTAN implementation for the tested algorithm and resolve each test vector. After that, the testing tool compares both results (BOTAN vs TOE) in order to determine whether the cryptographic algorithms is properly implemented or not. The results of the testing tool is an individual outcome for each test vector (PASS or FAIL) and a overall outcome (PASS is all the test vectors passed or FAIL if any of them failed).

14.2.1 Test 1

14.2.1.1 Setup

The following environment is required to perform the test in addition to the TOE:

- A computer with:
  - Operating System: Ubuntu 20.04
  - BOTAN Tool is installed with CCN policy in evaluator machine;
  - Test vectors are located in evaluator machine.

For the installation of the *Botan Tool with CCN policy 2.15.2* all the steps defined in the *Botan-CCN_Manual_Implementador_v1* document have been followed.

14.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

14.2.1.3 Results

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

14.2.1.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the test activity demonstrate that the TOE provides a valid implementation for the evaluated cryptographic algorithms, since they have been compared against a well-known implementation (BOTAN) as a reference implementation.

Therefore, the **PASS** verdict is assigned to the test activity.

14.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to this FCS_COP.1.1(SYM) requirement.

15 FCS_COP.1.1(2)

The assurance activity for the **FCS_COP.1.1(2)** requirement is stated as follows:

> The evaluator will check that the association of the hash function with other application cryptographic functions (for example, the digital signature verification function) is documented in the TSS.
>
> The TSF hashing functions can be implemented in one of two modes. The first mode is the byte-oriented mode. In this mode the TSF only hashes messages that are an integral number of bytes in length; i.e., the length (in bits) of the message to be hashed is divisible by 8. The second mode is the bit-oriented mode. In this mode the TSF hashes messages of arbitrary length. As there are different tests for each mode, an indication is given in the following sections for the bit-oriented vs. the byte-oriented testmacs. The evaluator will perform all of the following tests for each hash algorithm implemented by the TSF and used to satisfy the requirements of this PP.
>
> The following tests require the developer to provide access to a test application that provides the evaluator with tools that are typically not found in the production application.
>
> - **Test 1:** Short Messages Test (Bit oriented Mode) - The evaluator will generate an input set consisting of m+1 messages, where m is the block length of the hash algorithm. The length of the messages range sequentially from 0 to m bits. The message text shall be pseudorandomly generated. The evaluator will compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.
> - **Test 2:** Short Messages Test (Byte oriented Mode) - The evaluator will generate an input set consisting of m/8+1 messages, where m is the block length of the hash algorithm. The length of the messages range sequentially from 0 to m/8 bytes, with each message being an integral number of bytes. The message text shall be pseudorandomly generated. The evaluator will compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.
> - **Test 3:** Selected Long Messages Test (Bit oriented Mode) - The evaluator will generate an input set consisting of m messages, where m is the block length of the hash algorithm. The length of the ith message is 512 + 99*i, where $1 \leq i \leq m$. The message text shall be pseudorandomly generated. The evaluator will compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

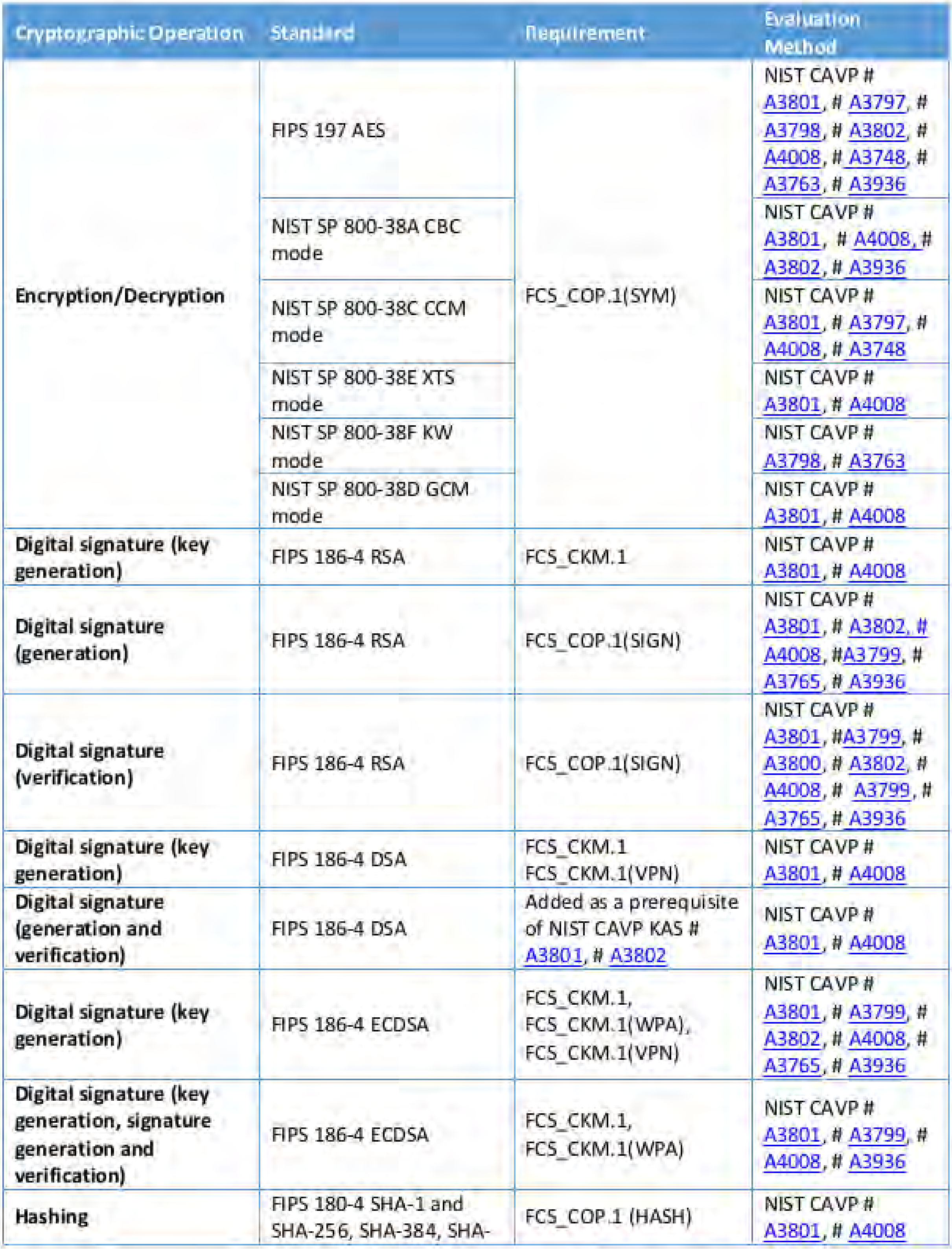
- **Test 4:** Selected Long Messages Test (Byte oriented Mode) - The evaluator will generate an input set consisting of m/8 messages, where m is the block length of the hash algorithm. The length of the ith message is 512 + 899i, where 1 $\leq$ i $\leq$ m/8. The message text shall be pseudorandomly generated. The evaluator will compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.
- **Test 5:** Pseudorandomly Generated Messages Test - This test is for byte-oriented implementations only. The evaluator will randomly generate a seed that is n bits long, where n is the length of the message digest produced by the hash function to be tested. The evaluator will then formulate a set of 100 messages and associated digests by following the algorithm provided in Figure 1 of [SHAVS]. The evaluator will then ensure that the correct result is produced when the messages are provided to the TSF.

15.1 Documentation Review Activity

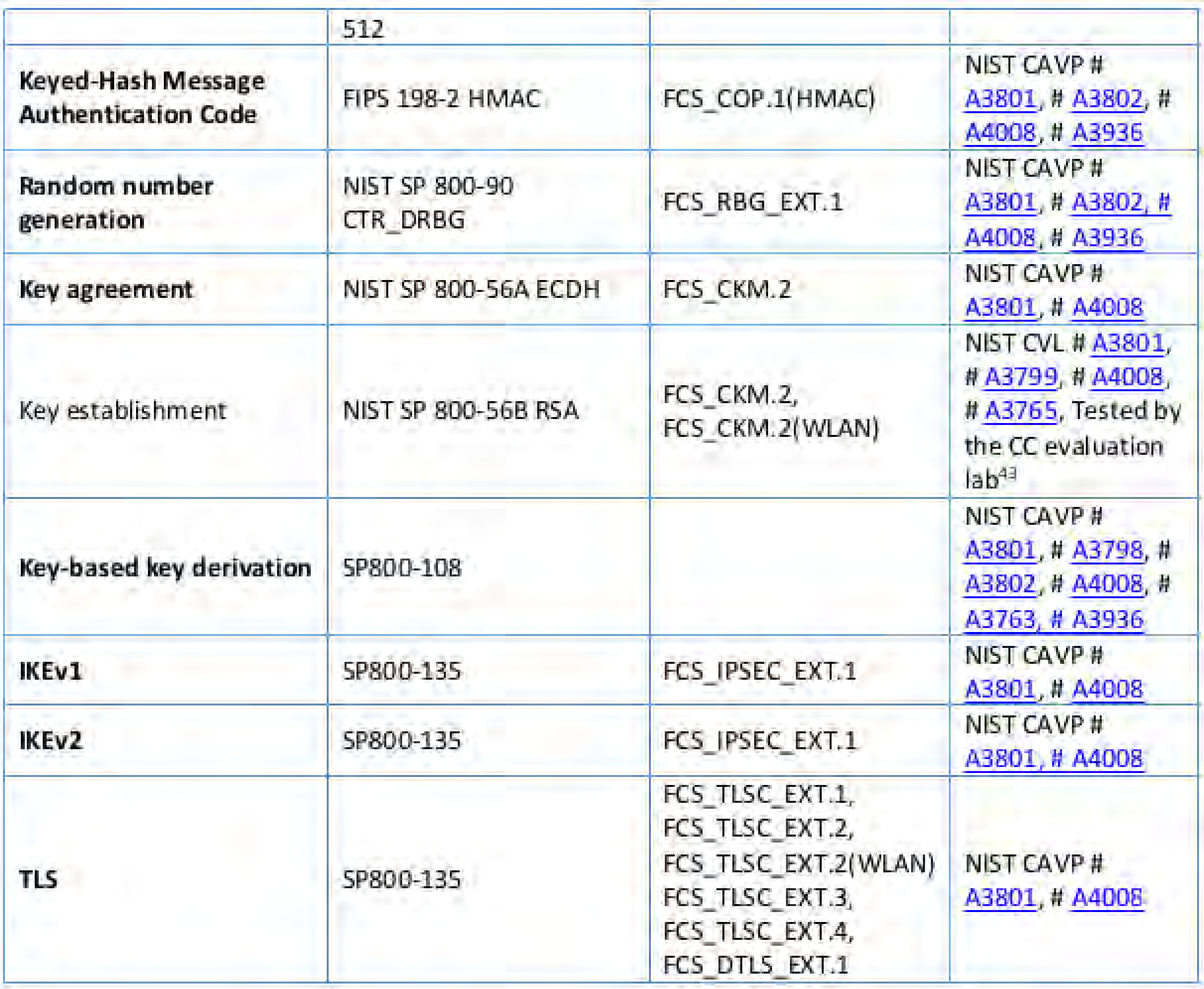
15.1.1 Findings

The evaluator has reviewed the ***Security Target*** document and the information provided in the TSS, section **6.2.2 Cryptographic Algorithm Validation**. This section includes the following tables of the cryptographic algorithms supported by Windows 11, Windows 10 versions, Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge.

15.1.1.1 Cryptographic Algorithm Standards and Evaluation Methods for Windows 11 (version 22H2)

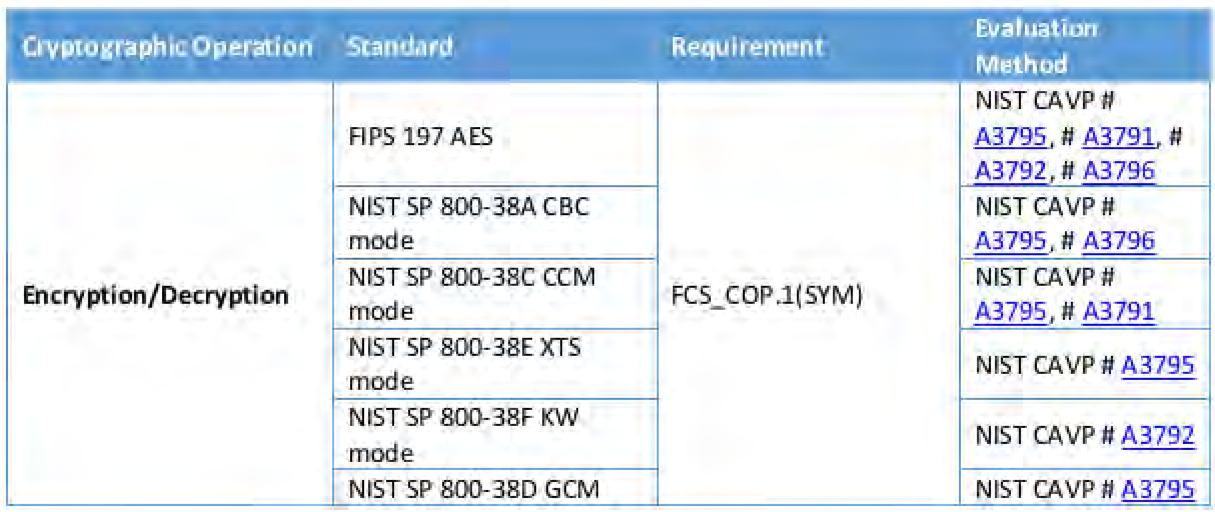


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3801, # A3797, # A3798, # A3802, # A4008, # A3748, # A3763, # A3936
	NIST SP 800-38A CBC mode		NIST CAVP # A3801, # A4008, # A3802, # A3936
	NIST SP 800-38C CCM mode		NIST CAVP # A3801, # A3797, # A4008, # A3748
	NIST SP 800-38E XTS mode		NIST CAVP # A3801, # A4008
	NIST SP 800-38F KW mode		NIST CAVP # A3798, # A3763
	NIST SP 800-38D GCM mode		NIST CAVP # A3801, # A4008
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP # A3801, # A4008
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3801, # A3802, # A4008, #A3799, # A3765, # A3936
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3801, #A3799, # A3800, # A3802, # A4008, # A3799, # A3765, # A3936
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3801, # A4008
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3801, # A3802	NIST CAVP # A3801, # A4008
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3801, # A3799, # A3802, # A4008, # A3765, # A3936
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3801, # A3799, # A4008, # A3936
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-	FCS_COP.1 (HASH)	NIST CAVP # A3801, # A4008

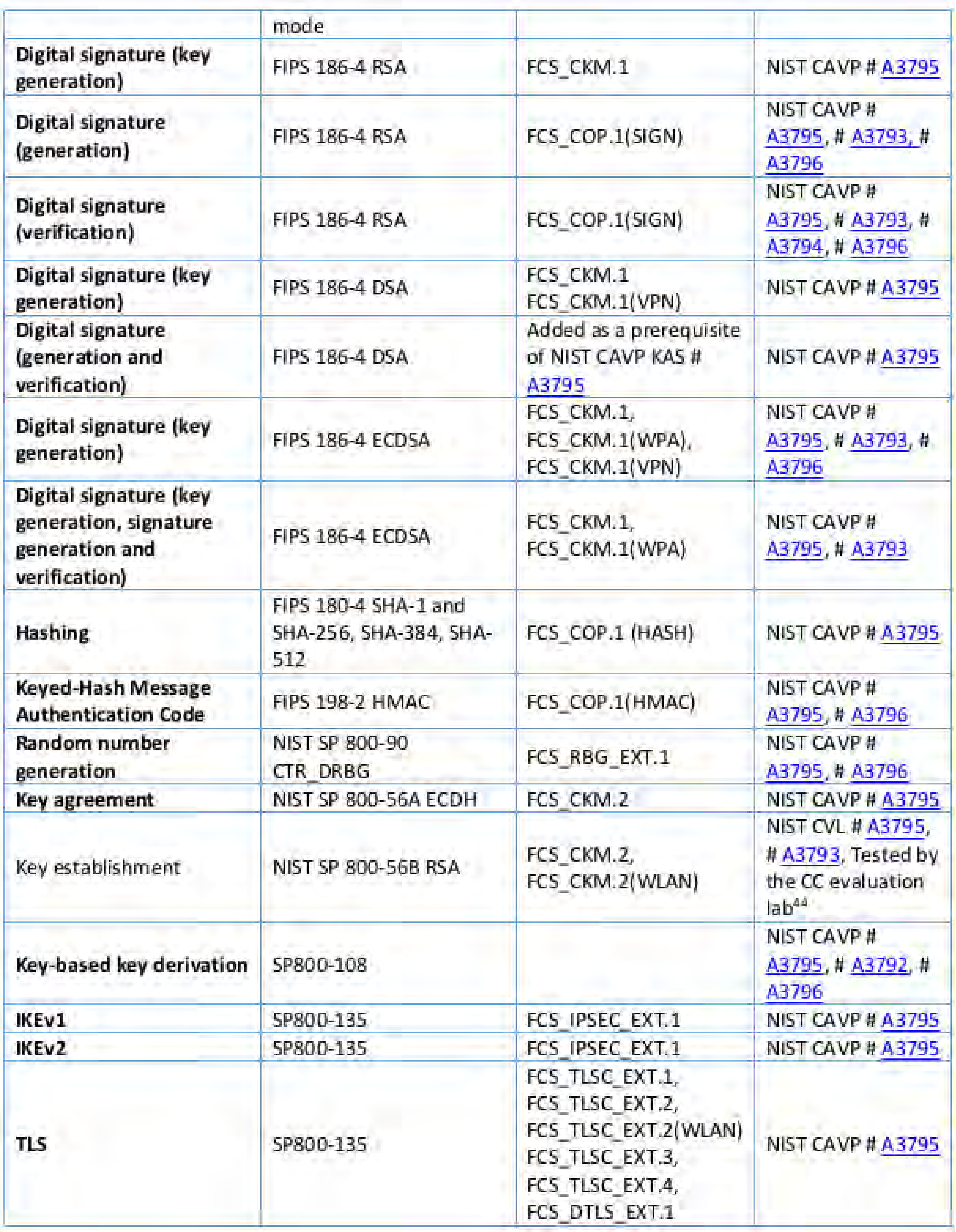


	512		
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3801, # A3802, # A4008, # A3936
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3801, # A3802, # A4008, # A3936
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3801, # A4008
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2, FCS_CKM.2(WLAN)	NIST CVL # A3801, # A3799, # A4008, # A3765, Tested by the CC evaluation lab[43]
Key-based key derivation	SP800-108		NIST CAVP # A3801, # A3798, # A3802, # A4008, # A3763, # A3936
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3801, # A4008
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3801, # A4008
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3801, # A4008

15.1.1.2 Cryptographic Algorithm Standards and Evaluation Methods for Windows 10 (version 22H2)

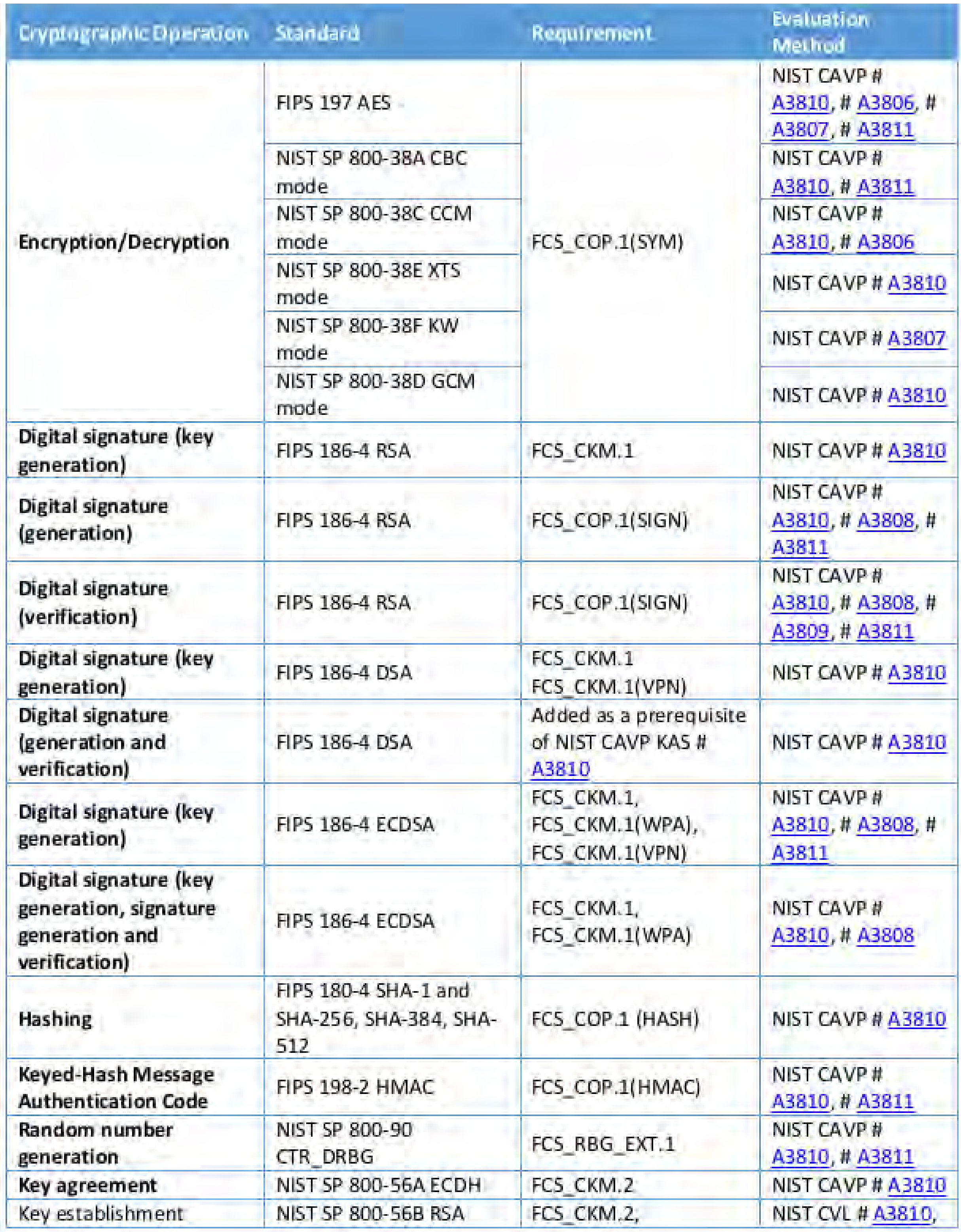


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3795, # A3791, # A3792, # A3796
	NIST SP 800-38A CBC mode		NIST CAVP # A3795, # A3796
	NIST SP 800-38C CCM mode		NIST CAVP # A3795, # A3791
	NIST SP 800-38E XTS mode		NIST CAVP # A3795
	NIST SP 800-38F KW mode		NIST CAVP # A3792
	NIST SP 800-38D GCM		NIST CAVP # A3795

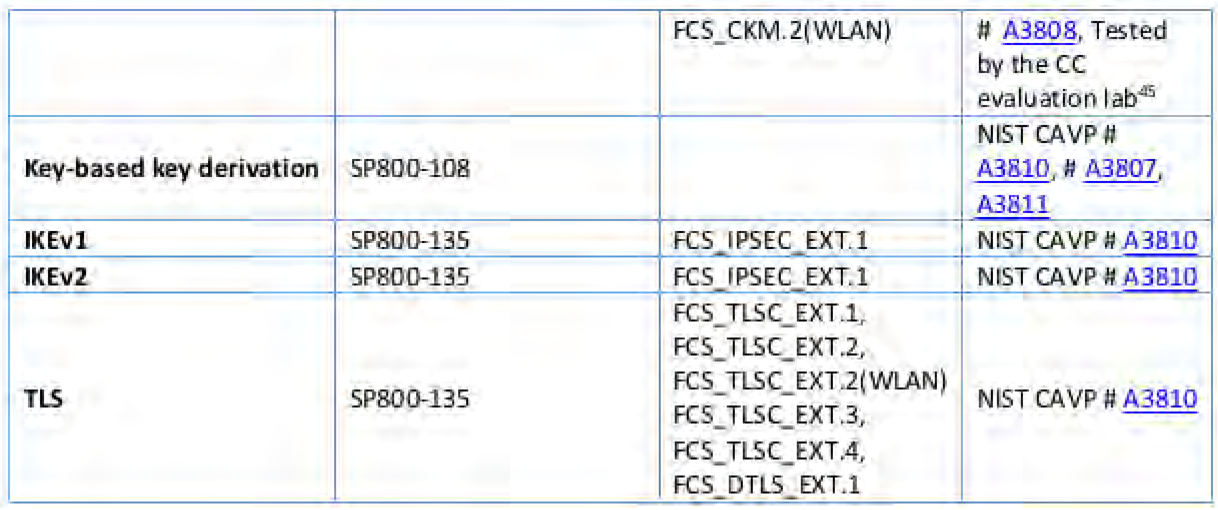


	mode		
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP # A3795
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3795, # A3793, # A3796
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3795, # A3793, # A3794, # A3796
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3795
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3795	NIST CAVP # A3795
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3795, # A3793, # A3796
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3795, # A3793
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3795
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3795, # A3796
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3795, # A3796
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3795
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2, FCS_CKM.2(WLAN)	NIST CVL # A3795, # A3793, Tested by the CC evaluation lab[44]
Key-based key derivation	SP800-108		NIST CAVP # A3795, # A3792, # A3796
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3795
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3795
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3795

15.1.1.3 Cryptographic Algorithm Standards and Evaluation Methods for Windows Server 2022 and Windows Server Datacenter: Azure Edition

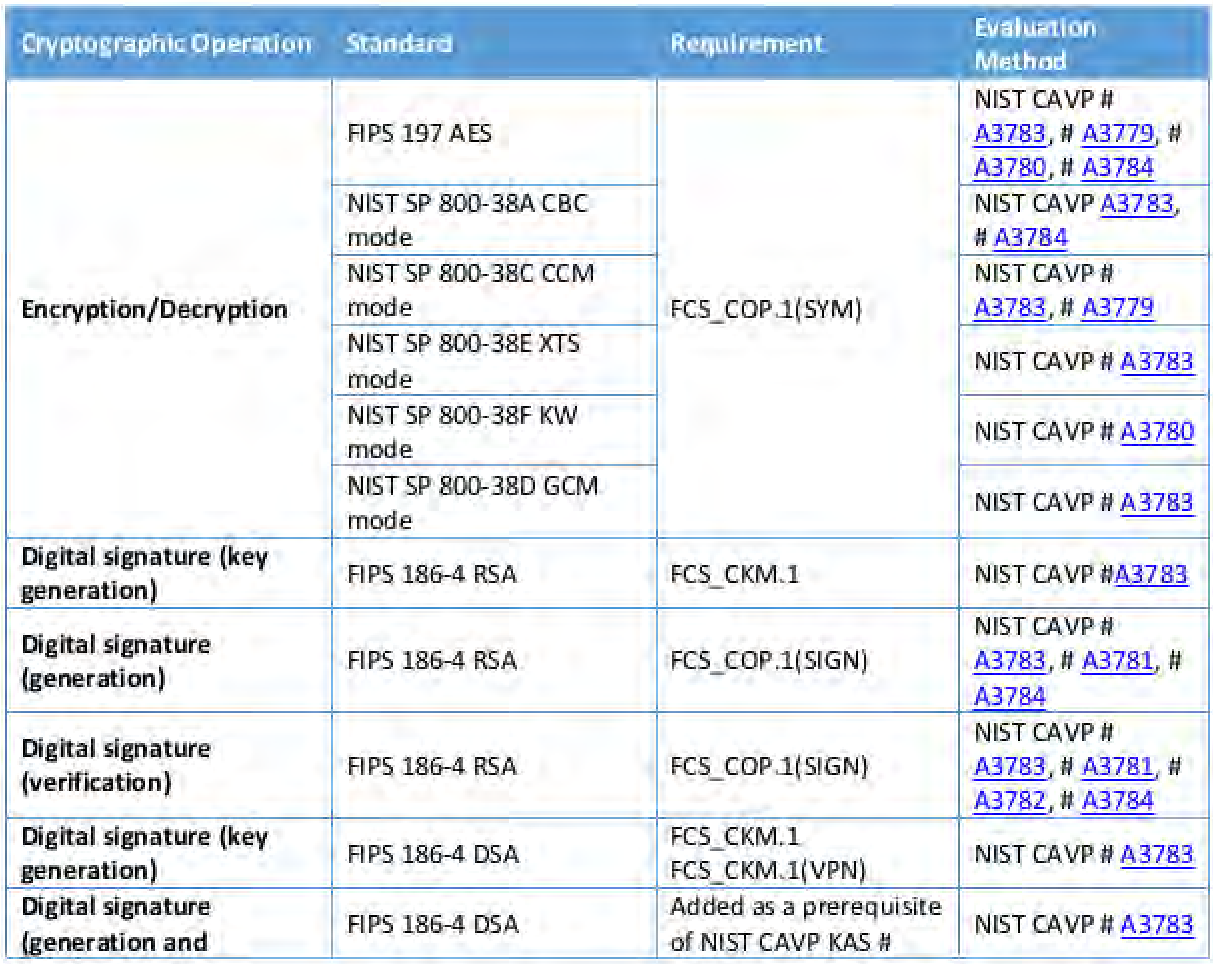


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3810, # A3806, # A3807, # A3811
	NIST SP 800-38A CBC mode		NIST CAVP # A3810, # A3811
	NIST SP 800-38C CCM mode		NIST CAVP # A3810, # A3806
	NIST SP 800-38E XTS mode		NIST CAVP # A3810
	NIST SP 800-38F KW mode		NIST CAVP # A3807
	NIST SP 800-38D GCM mode		NIST CAVP # A3810
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP # A3810
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3810, # A3808, # A3811
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3810, # A3808, # A3809, # A3811
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3810
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3810	NIST CAVP # A3810
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3810, # A3808, # A3811
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3810, # A3808
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3810
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3810, # A3811
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3810, # A3811
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3810
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2,	NIST CVL # A3810,

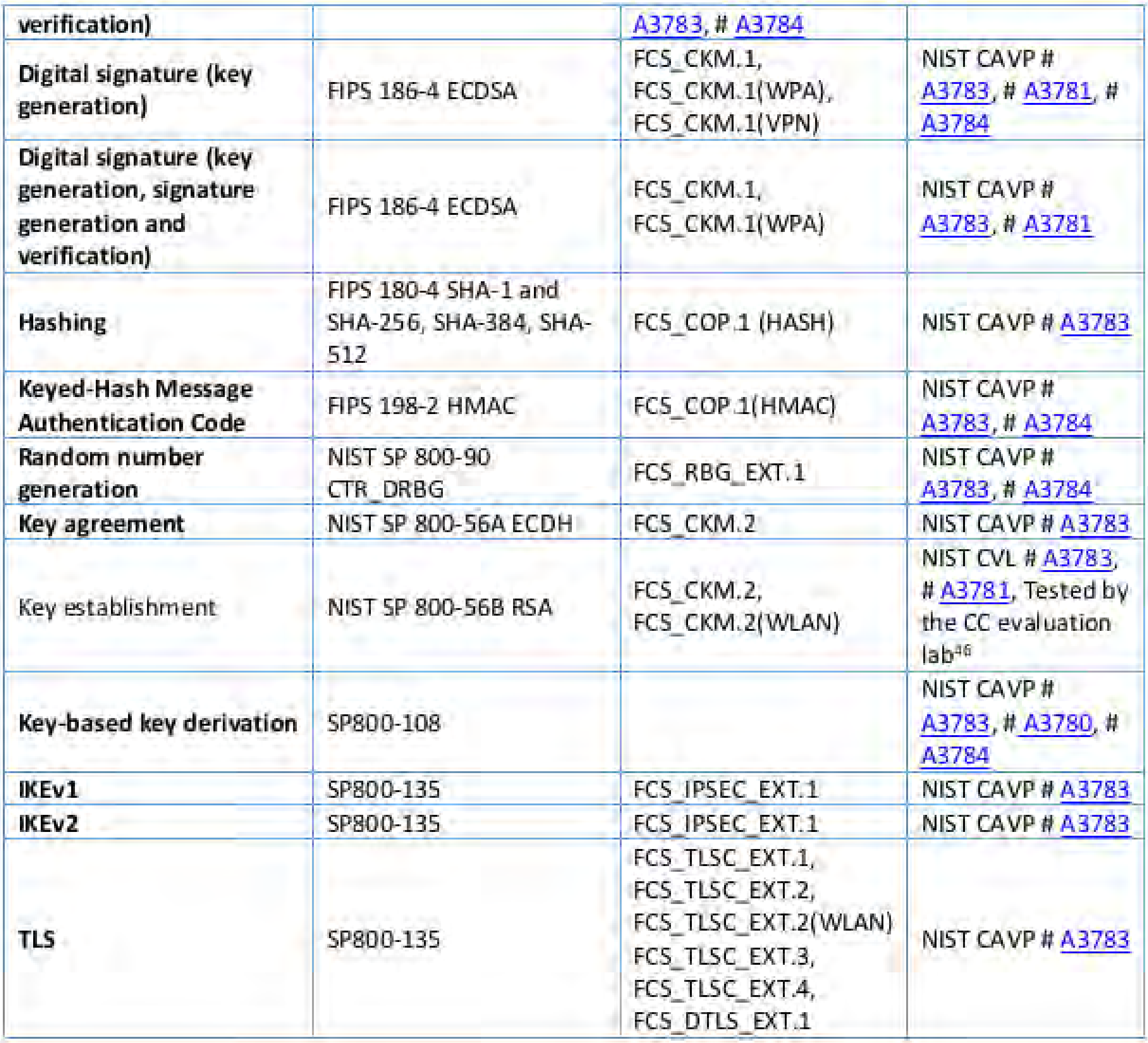


		FCS_CKM.2(WLAN)	# A3808, Tested by the CC evaluation lab[45]
Key-based key derivation	SP800-108		NIST CAVP # A3810, # A3807, A3811
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3810
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3810
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3810

15.1.1.4 Cryptographic Algorithm Standards and Evaluation Methods for Windows Server Azure Stack HCIv2 version 22H2

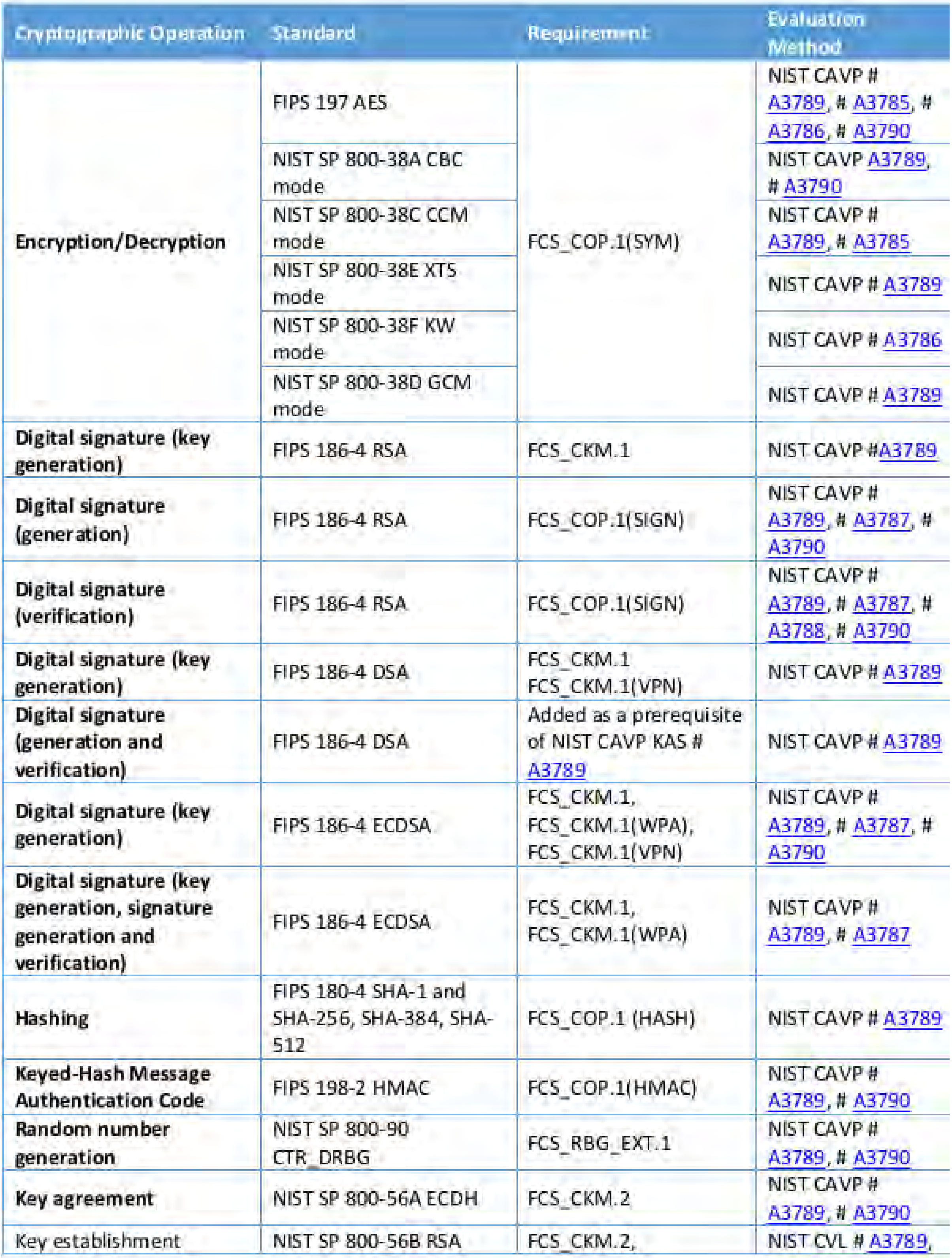


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3783, # A3779, # A3780, # A3784
	NIST SP 800-38A CBC mode		NIST CAVP A3783, # A3784
	NIST SP 800-38C CCM mode		NIST CAVP # A3783, # A3779
	NIST SP 800-38E XTS mode		NIST CAVP # A3783
	NIST SP 800-38F KW mode		NIST CAVP # A3780
	NIST SP 800-38D GCM mode		NIST CAVP # A3783
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP #A3783
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3783, # A3781, # A3784
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3783, # A3781, # A3782, # A3784
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3783
Digital signature (generation and	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS #	NIST CAVP # A3783

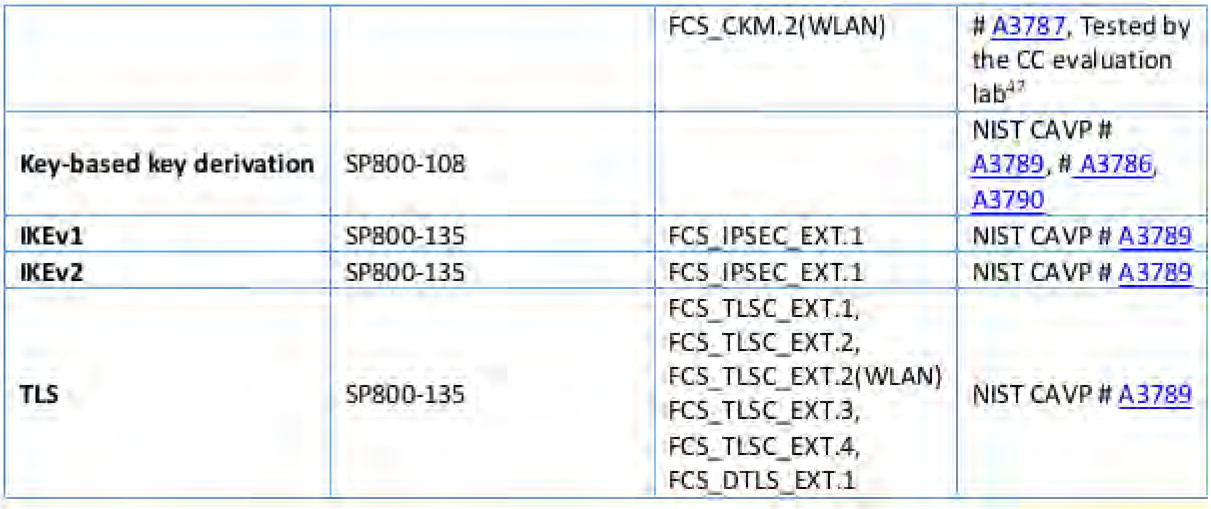


verification)		A3783, # A3784	
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3783, # A3781, # A3784
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3783, # A3781
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3783
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3783, # A3784
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3783, # A3784
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3783
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2, FCS_CKM.2(WLAN)	NIST CVL # A3783, # A3781, Tested by the CC evaluation lab[46]
Key-based key derivation	SP800-108		NIST CAVP # A3783, # A3780, # A3784
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3783
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3783
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3783

15.1.1.5 Cryptographic Algorithm Standards and Evaluation Methods for Azure Stack Hub and Azure Stack Edge



Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3789, # A3785, # A3786, # A3790
	NIST SP 800-38A CBC mode		NIST CAVP A3789, # A3790
	NIST SP 800-38C CCM mode		NIST CAVP # A3789, # A3785
	NIST SP 800-38E XTS mode		NIST CAVP # A3789
	NIST SP 800-38F KW mode		NIST CAVP # A3786
	NIST SP 800-38D GCM mode		NIST CAVP # A3789
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP #A3789
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3789, # A3787, # A3790
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3789, # A3787, # A3788, # A3790
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3789
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3789	NIST CAVP # A3789
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3789, # A3787, # A3790
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3789, # A3787
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3789
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3789, # A3790
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3789, # A3790
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3789, # A3790
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2,	NIST CVL # A3789,



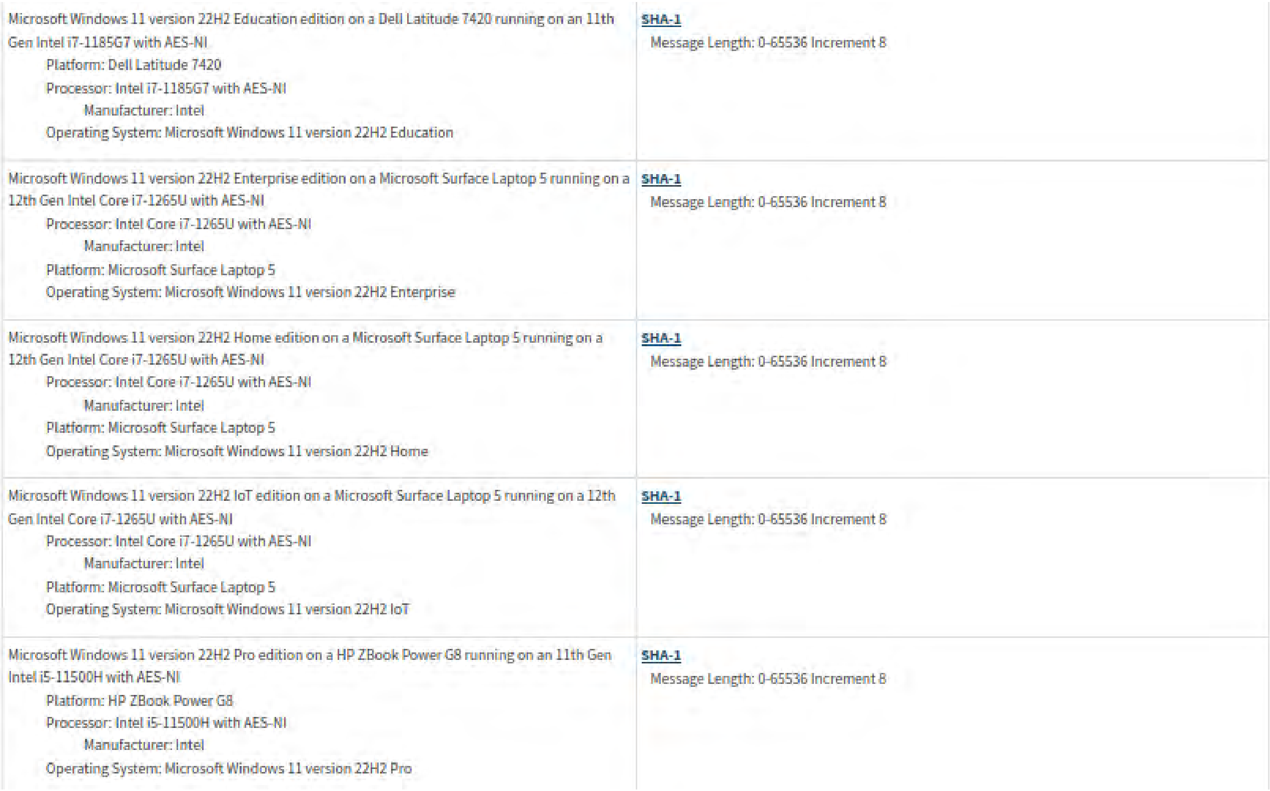
		FCS_CKM.2(WLAN)	# A3787, Tested by the CC evaluation lab[47]
Key-based key derivation	SP800-108		NIST CAVP # A3789, # A3786, A3790
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3789
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3789
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3789

In addition, in the same TSS section, the vendor has provided the following wordings regarding the usage of the hashing functions:

> An important feature of CNG is its native implementation of the Suite B algorithms, including algorithms for AES (128, 192, 256 key sizes), the SHA-1 and SHA-2 family (SHA-256, SHA-384 and SHA-512) of hashing algorithms, elliptic curve Diffie Hellman (ECDH), and elliptical curve DSA (ECDSA) over the NIST-standard prime curves P-256, P-384, and P-521.
>
> Protocols such as the Internet Key Exchange (IKE), and Transport Layer Security (TLS), make use of elliptic curve Diffie-Hellman (ECDH) included in Suite B as well as hashing functions.
>
> [...]
>
> Hashing is used by other FIPS Approved algorithms implemented in Windows (the hashed message authentication code, RSA, EC DSA signature services, Diffie-Hellman and elliptic curve Diffie-Hellman key agreement, and random bit generation).

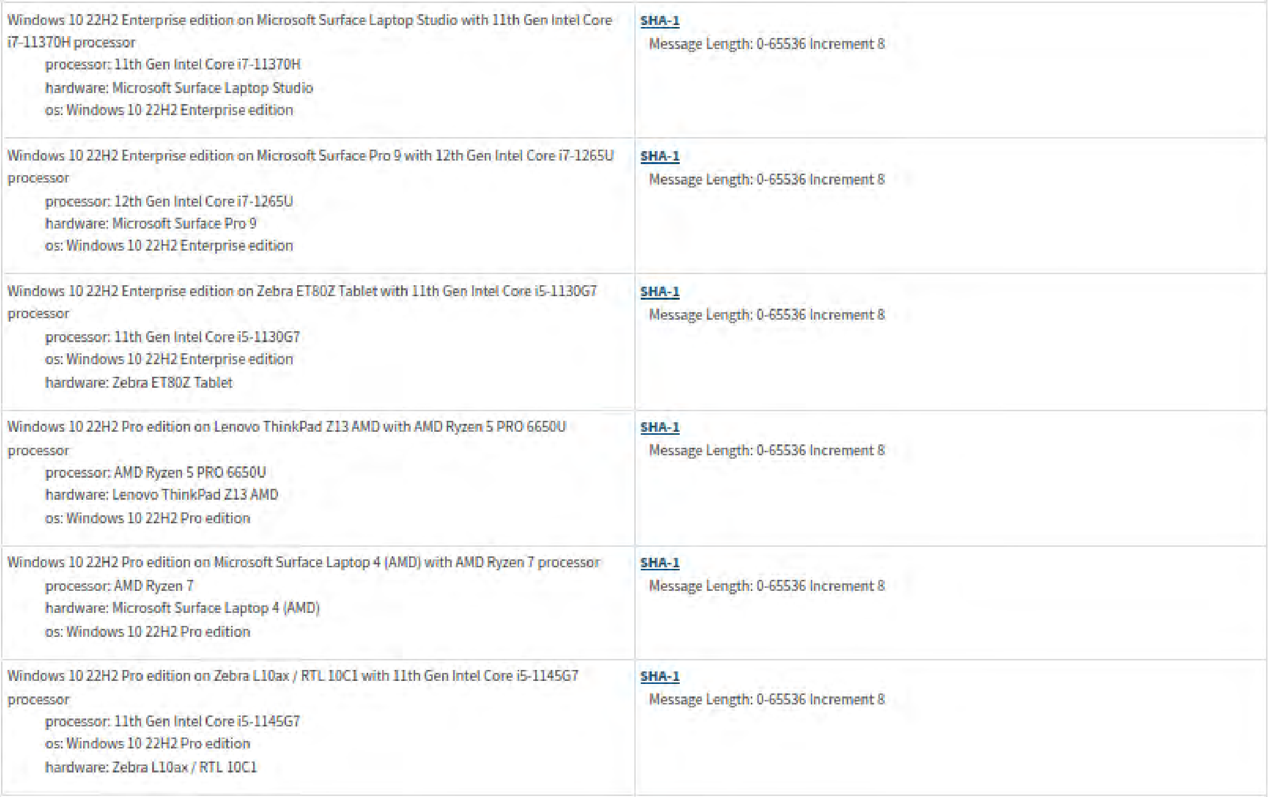
As part of the testing activity described below, the correctness of the cryptographic functionality has been demonstrated against the BOTAN tool. However, SHA-1 is not available in BOTAN, and the laboratory has verified the implementation against the CAVP tool. Below, the CAVP certificates granted for this functionality are listed (extracted from the tables above)

15.1.1.6 Windows 11 version 22H2 (CAVP Cert. #A4008)



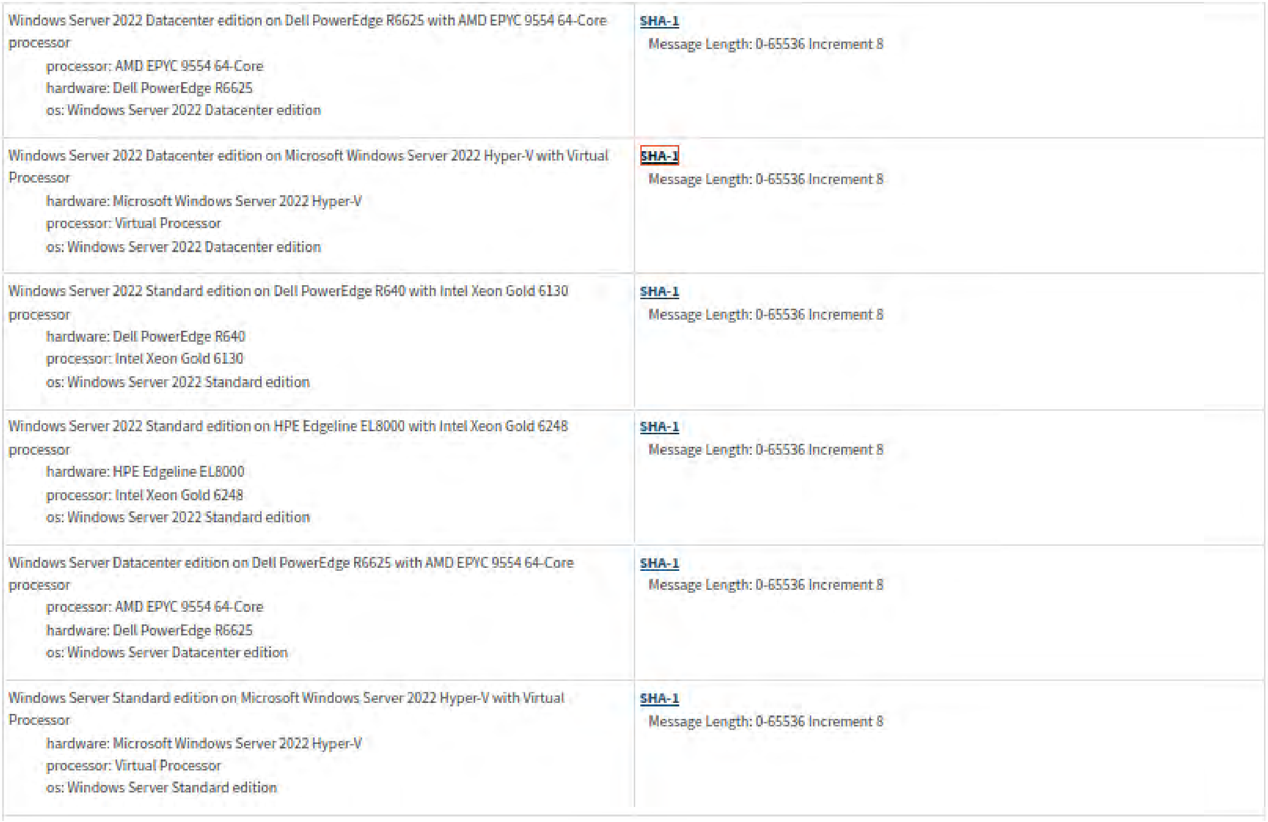
Microsoft Windows 11 version 22H2 Education edition on a Dell Latitude 7420 running on an 11th Gen Intel i7-1185G7 with AES-NI Platform: Dell Latitude 7420 Processor: Intel i7-1185G7 with AES-NI Manufacturer: Intel Operating System: Microsoft Windows 11 version 22H2 Education	SHA-1 Message Length: 0-65536 Increment 8
Microsoft Windows 11 version 22H2 Enterprise edition on a Microsoft Surface Laptop 5 running on a 12th Gen Intel Core i7-1265U with AES-NI Processor: Intel Core i7-1265U with AES-NI Manufacturer: Intel Platform: Microsoft Surface Laptop 5 Operating System: Microsoft Windows 11 version 22H2 Enterprise	SHA-1 Message Length: 0-65536 Increment 8
Microsoft Windows 11 version 22H2 Home edition on a Microsoft Surface Laptop 5 running on a 12th Gen Intel Core i7-1265U with AES-NI Processor: Intel Core i7-1265U with AES-NI Manufacturer: Intel Platform: Microsoft Surface Laptop 5 Operating System: Microsoft Windows 11 version 22H2 Home	SHA-1 Message Length: 0-65536 Increment 8
Microsoft Windows 11 version 22H2 IoT edition on a Microsoft Surface Laptop 5 running on a 12th Gen Intel Core i7-1265U with AES-NI Processor: Intel Core i7-1265U with AES-NI Manufacturer: Intel Platform: Microsoft Surface Laptop 5 Operating System: Microsoft Windows 11 version 22H2 IoT	SHA-1 Message Length: 0-65536 Increment 8
Microsoft Windows 11 version 22H2 Pro edition on a HP ZBook Power G8 running on an 11th Gen Intel i5-11500H with AES-NI Platform: HP ZBook Power G8 Processor: Intel i5-11500H with AES-NI Manufacturer: Intel Operating System: Microsoft Windows 11 version 22H2 Pro	SHA-1 Message Length: 0-65536 Increment 8

15.1.1.7 Windows 10 version 22H2 (CAVP Cert. #A3795)



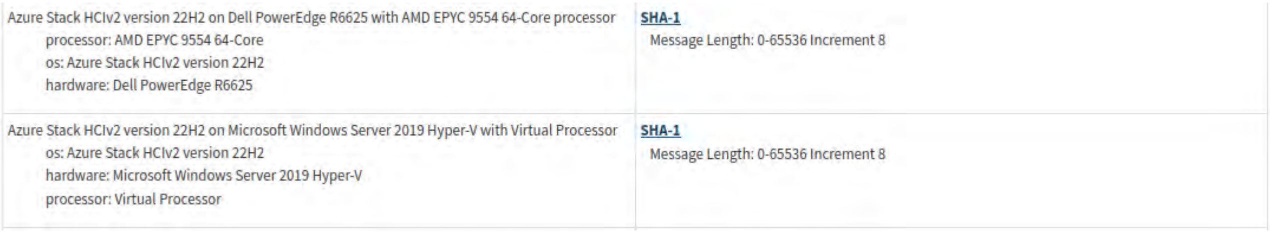
Windows 10 22H2 Enterprise edition on Microsoft Surface Laptop Studio with 11th Gen Intel Core i7-11370H processor processor: 11th Gen Intel Core i7-11370H hardware: Microsoft Surface Laptop Studio os: Windows 10 22H2 Enterprise edition	SHA-1 Message Length: 0-65536 Increment 8
Windows 10 22H2 Enterprise edition on Microsoft Surface Pro 9 with 12th Gen Intel Core i7-1265U processor processor: 12th Gen Intel Core i7-1265U hardware: Microsoft Surface Pro 9 os: Windows 10 22H2 Enterprise edition	SHA-1 Message Length: 0-65536 Increment 8
Windows 10 22H2 Enterprise edition on Zebra ET80Z Tablet with 11th Gen Intel Core i5-1130G7 processor processor: 11th Gen Intel Core i5-1130G7 os: Windows 10 22H2 Enterprise edition hardware: Zebra ET80Z Tablet	SHA-1 Message Length: 0-65536 Increment 8
Windows 10 22H2 Pro edition on Lenovo ThinkPad Z13 AMD with AMD Ryzen 5 PRO 6650U processor processor: AMD Ryzen 5 PRO 6650U hardware: Lenovo ThinkPad Z13 AMD os: Windows 10 22H2 Pro edition	SHA-1 Message Length: 0-65536 Increment 8
Windows 10 22H2 Pro edition on Microsoft Surface Laptop 4 (AMD) with AMD Ryzen 7 processor processor: AMD Ryzen 7 hardware: Microsoft Surface Laptop 4 (AMD) os: Windows 10 22H2 Pro edition	SHA-1 Message Length: 0-65536 Increment 8
Windows 10 22H2 Pro edition on Zebra L10ax / RTL 10C1 with 11th Gen Intel Core i5-1145G7 processor processor: 11th Gen Intel Core i5-1145G7 os: Windows 10 22H2 Pro edition hardware: Zebra L10ax / RTL 10C1	SHA-1 Message Length: 0-65536 Increment 8

15.1.1.8 Windows Server 2022 and Windows Server Datacenter: Azure Edition (CAVP Cert. #A3810)



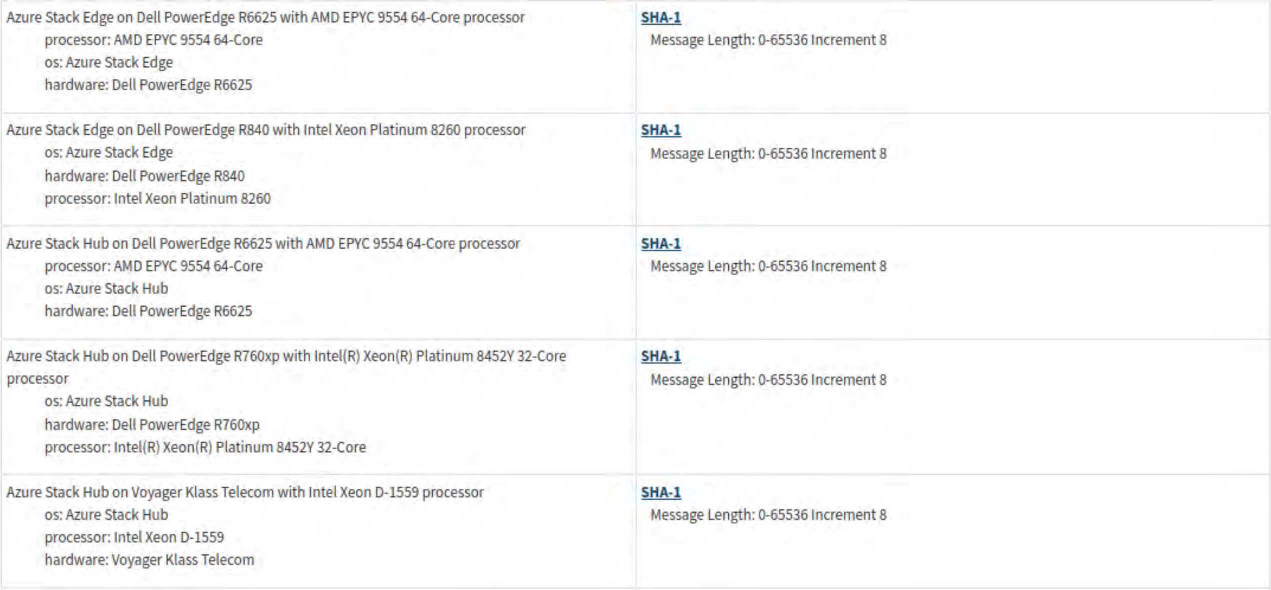
Windows Server 2022 Datacenter edition on Dell PowerEdge R6625 with AMD EPYC 9554 64-Core processor processor: AMD EPYC 9554 64-Core hardware: Dell PowerEdge R6625 os: Windows Server 2022 Datacenter edition	SHA-1 Message Length: 0-65536 Increment 8
Windows Server 2022 Datacenter edition on Microsoft Windows Server 2022 Hyper-V with Virtual Processor hardware: Microsoft Windows Server 2022 Hyper-V processor: Virtual Processor os: Windows Server 2022 Datacenter edition	SHA-1 Message Length: 0-65536 Increment 8
Windows Server 2022 Standard edition on Dell PowerEdge R640 with Intel Xeon Gold 6130 processor hardware: Dell PowerEdge R640 processor: Intel Xeon Gold 6130 os: Windows Server 2022 Standard edition	SHA-1 Message Length: 0-65536 Increment 8
Windows Server 2022 Standard edition on HPE Edgeline EL8000 with Intel Xeon Gold 6248 processor hardware: HPE Edgeline EL8000 processor: Intel Xeon Gold 6248 os: Windows Server 2022 Standard edition	SHA-1 Message Length: 0-65536 Increment 8
Windows Server Datacenter edition on Dell PowerEdge R6625 with AMD EPYC 9554 64-Core processor processor: AMD EPYC 9554 64-Core hardware: Dell PowerEdge R6625 os: Windows Server Datacenter edition	SHA-1 Message Length: 0-65536 Increment 8
Windows Server Standard edition on Microsoft Windows Server 2022 Hyper-V with Virtual Processor hardware: Microsoft Windows Server 2022 Hyper-V processor: Virtual Processor os: Windows Server Standard edition	SHA-1 Message Length: 0-65536 Increment 8

15.1.1.9 Windows Server Azure Stack HCIv2 version 22H2 (CAVP Cert. #A3783)



Azure Stack HCIv2 version 22H2 on Dell PowerEdge R6625 with AMD EPYC 9554 64-Core processor processor: AMD EPYC 9554 64-Core os: Azure Stack HCIv2 version 22H2 hardware: Dell PowerEdge R6625	SHA-1 Message Length: 0-65536 Increment 8
Azure Stack HCIv2 version 22H2 on Microsoft Windows Server 2019 Hyper-V with Virtual Processor os: Azure Stack HCIv2 version 22H2 hardware: Microsoft Windows Server 2019 Hyper-V processor: Virtual Processor	SHA-1 Message Length: 0-65536 Increment 8

15.1.1.10 Azure Stack Hub and Azure Stack Edge (CAVP Cert. #A3789)



Azure Stack Edge on Dell PowerEdge R6625 with AMD EPYC 9554 64-Core processor processor: AMD EPYC 9554 64-Core os: Azure Stack Edge hardware: Dell PowerEdge R6625	SHA-1 Message Length: 0-65536 Increment 8
Azure Stack Edge on Dell PowerEdge R840 with Intel Xeon Platinum 8260 processor os: Azure Stack Edge hardware: Dell PowerEdge R840 processor: Intel Xeon Platinum 8260	SHA-1 Message Length: 0-65536 Increment 8
Azure Stack Hub on Dell PowerEdge R6625 with AMD EPYC 9554 64-Core processor processor: AMD EPYC 9554 64-Core os: Azure Stack Hub hardware: Dell PowerEdge R6625	SHA-1 Message Length: 0-65536 Increment 8
Azure Stack Hub on Dell PowerEdge R760xp with Intel(R) Xeon(R) Platinum 8452Y 32-Core processor os: Azure Stack Hub hardware: Dell PowerEdge R760xp processor: Intel(R) Xeon(R) Platinum 8452Y 32-Core	SHA-1 Message Length: 0-65536 Increment 8
Azure Stack Hub on Voyager Klass Telecom with Intel Xeon D-1559 processor os: Azure Stack Hub processor: Intel Xeon D-1559 hardware: Voyager Klass Telecom	SHA-1 Message Length: 0-65536 Increment 8

15.1.2 Verdict

The evaluator considers that the TSS identifies the key hashing algorithms supported by each OS version as well as how these hashing algorithms are used with other cryptographic functions.

Hence, the **PASS** verdict is assigned to the documentation review activity.

15.2 Test Activity

Based on the SFR instantiation included in the security target, the vendor has selected the following SHA algorithms:

1. SHA-1
2. SHA-256
3. SHA-384
4. SHA-512

In addition to the Common Criteria evaluation, the laboratory has also performed the CAVP validation for these and other algorithms. The general procedure that has been followed during the evaluation in order to demonstrate the correctness of the cryptographic functionality is as follows:

1. The laboratory has used the same test vectors used as part of the CAVP validation. For hashing algorithms, the following types of test are performed:
    - Algorithm Functional Test (AFT). The main goal for these tests is verify the implementation of the hash operation. AFTs cause the implementation under test to

exercise normal operations on a single block, multiple blocks, or partial blocks. In all cases, random data is used. The functional tests are designed to verify that the logical components of the hash function (block chunking, block padding etc.) are operating correctly.

  - Monte Carlo Test (MCT). These tests exercise the implementation under stenuous circumstances. The implementation must process the test vectors according to the correct algorithm and mode. MCTs can help detect potential memory leaks over time, and problems in allocation of resources, addressing variables, error handling, and generally improper behavior in response to random inputs. Each MCT processes 100 pseudorandom tests.

2. The laboratory has exercised the cryptographic functionalities of the TOE by invoking the appropriate API in order to resolve the test vectors. The result of this step is a .json file which includes the associated response generated by the TOE per each test vector.
3. The laboratory has created a testing tool in order to exercise the BOTAN implementation for the target cryptographic algorithms. This tool receives the initial .json file with the test vectors as well as the .json file obtained as a result of the step 2. After parsing the information, the testing tool invokes the BOTAN implementation for the tested algorithm and resolve each test vector. After that, the testing tool compares both results (BOTAN vs TOE) in order to determine whether the cryptographic algorithms is properly implemented or not. The results of the testing tool is an individual outcome for each test vector (PASS or FAIL) and a overall outcome (PASS is all the test vectors passed or FAIL if any of them failed).
   - Note: Since SHA-1 is not available in BOTAN, the laboratory has demonstrated the correctness of the cryptographic algorithm implementation by using CAVP as a reference implementation instead of BOTAN.

15.2.1 Test 1

15.2.1.1 Setup

The following environment is required to perform the test in addition to the TOE:

- A computer with:
  - Operating System: Ubuntu 20.04
  - BOTAN Tool is installed with CCN policy in evaluator machine;
  - Test vectors are located in evaluator machine.

For the installation of the *Botan Tool with CCN policy 2.15.2* all the steps defined in the *Botan-CCN_Manual_Implementador_v1* document have been followed.

15.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

15.2.1.3 Results

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

15.2.1.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the test activity demonstrate that the TOE provides a valid implementation for the evaluated cryptographic algorithms, since they have been compared against a well-known implementation (BOTAN) as a reference implementation.

For SHA-1 algorithm, which is not available in BOTAN, the laboratory has followed the same approach but using the CAVP implementation as a reference instead of BOTAN. The evaluator has verified that the responses generated by the TOE are the same as the ones expected by the CAVP tool. Additionally, the associated CAVP certificates (listed in the tables included within the Documentation Review Activity section) have been granted demonstrating the correctness of the algorithm implementation.

Therefore, the **PASS** verdict is assigned to the test activity.

15.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to this FCS_COP.1.1(HASH) requirement.

16 FCS_COP.1.1(3)

The assurance activity for the **FCS_COP.1.1(3)** requirement is stated as follows:

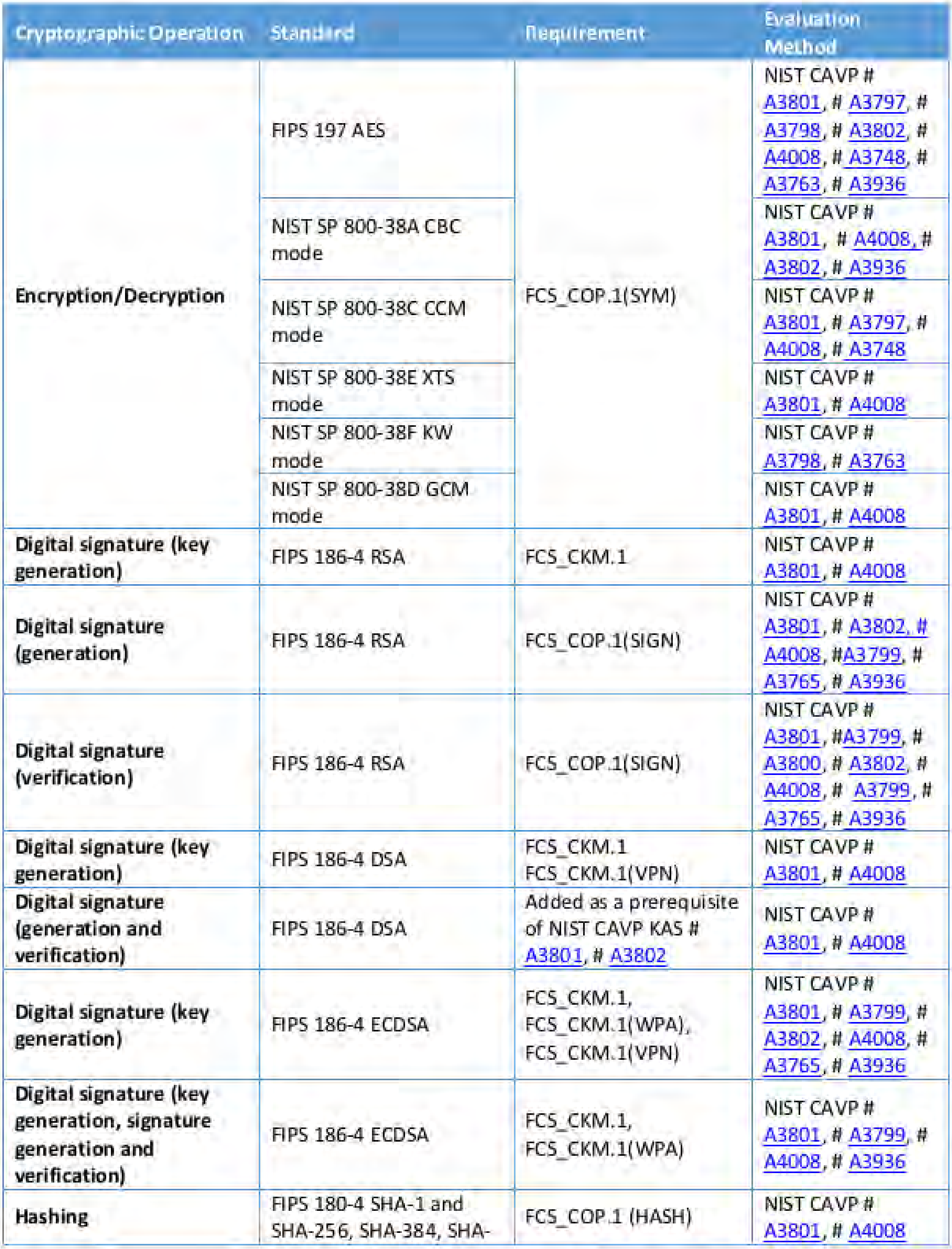
> The evaluator will perform the following activities based on the selections in the ST.
>
> The following tests require the developer to provide access to a test application that provides the evaluator with tools that are typically not found in the production application.
>
> **ECDSA Algorithm Tests**
>
> - **Test 1:** ECDSA FIPS 186-4 Signature Generation Test. For each supported NIST curve (i.e., P-256, P-384 and P-521) and SHA function pair, the evaluator will generate 10 1024-bit long messages and obtain for each message a public key and the resulting signature values R and S. To determine correctness, the evaluator will use the signature verification function of a known good implementation.
> - **Test 2:** ECDSA FIPS 186-4 Signature Verification Test. For each supported NIST curve (i.e., P-256, P-384 and P-521) and SHA function pair, the evaluator will generate a set of 10 1024-bit message, public key and signature tuples and modify one of the values (message, public key or signature) in five of the 10 tuples. The evaluator will verify that 5 responses indicate success and 5 responses indicate failure.
>
> **RSA Signature Algorithm Tests**
>
> - **Test 1:** Signature Generation Test. The evaluator will verify the implementation of RSA Signature Generation by the OS using the Signature Generation Test. To conduct this test the evaluator must generate or obtain 10 messages from a trusted reference implementation for each modulus size/SHA combination supported by the TSF. The evaluator will have the OS use its private key and modulus value to sign these messages. The evaluator will verify the correctness of the TSF's signature using a known good implementation and the associated public keys to verify the signatures.
> - **Test 2:** Signature Verification Test. The evaluator will perform the Signature Verification test to verify the ability of the OS to recognize another party's valid and invalid signatures. The evaluator will inject errors into the test vectors produced during the Signature Verification Test by introducing errors in some of the public keys, e, messages, IR format, and/or signatures. The evaluator will verify that the OS returns failure when validating each signature.

16.1 Documentation Review Activity

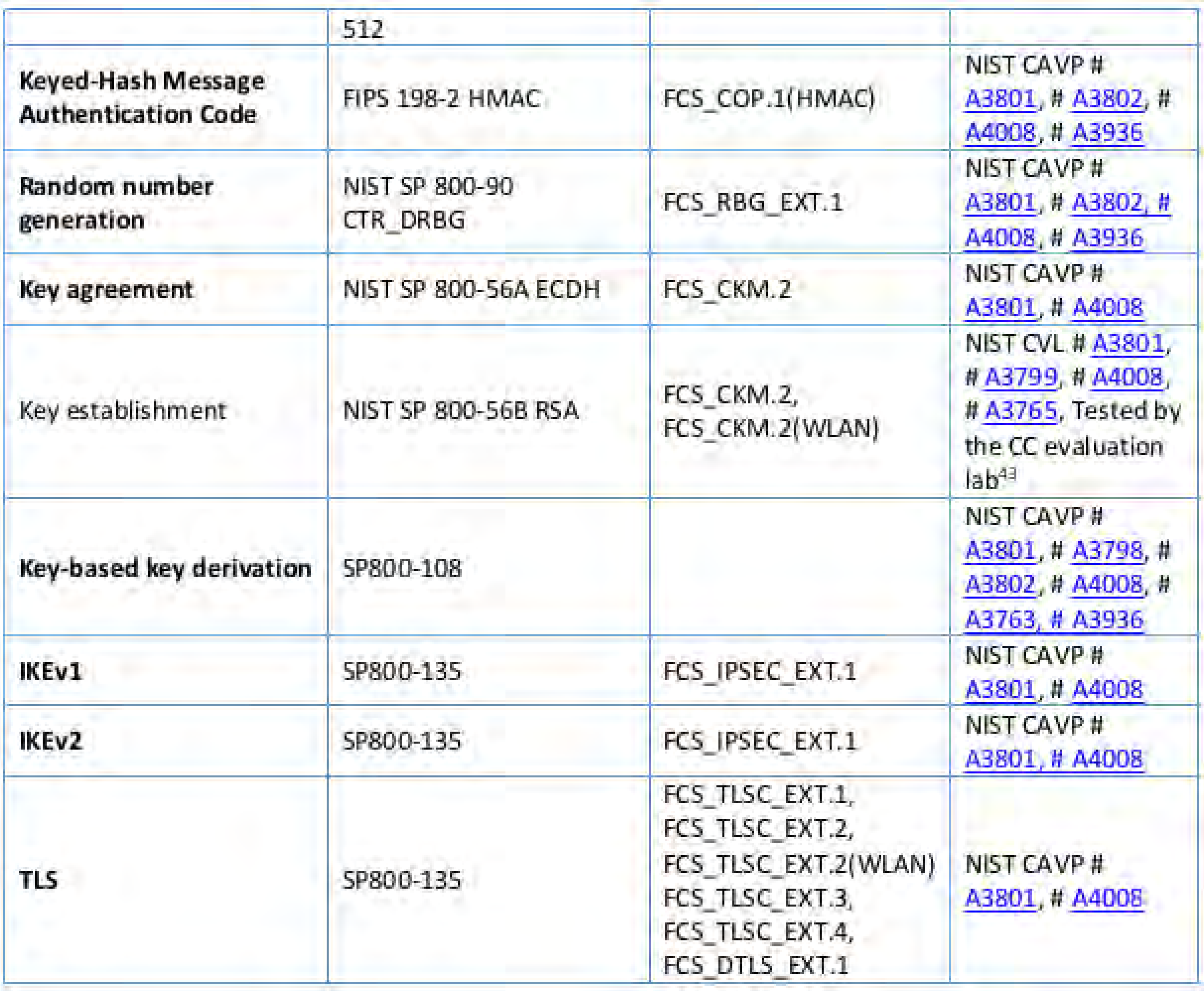
16.1.1 Findings

The evaluator has reviewed the ***Security Target*** document and the information provided in the TSS, section **6.2.2 Cryptographic Algorithm Validation**. This section includes the following tables of the cryptographic algorithms supported by Windows 11, Windows 10 versions, Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge.

16.1.1.1 Cryptographic Algorithm Standards and Evaluation Methods for Windows 11 (version 22H2)

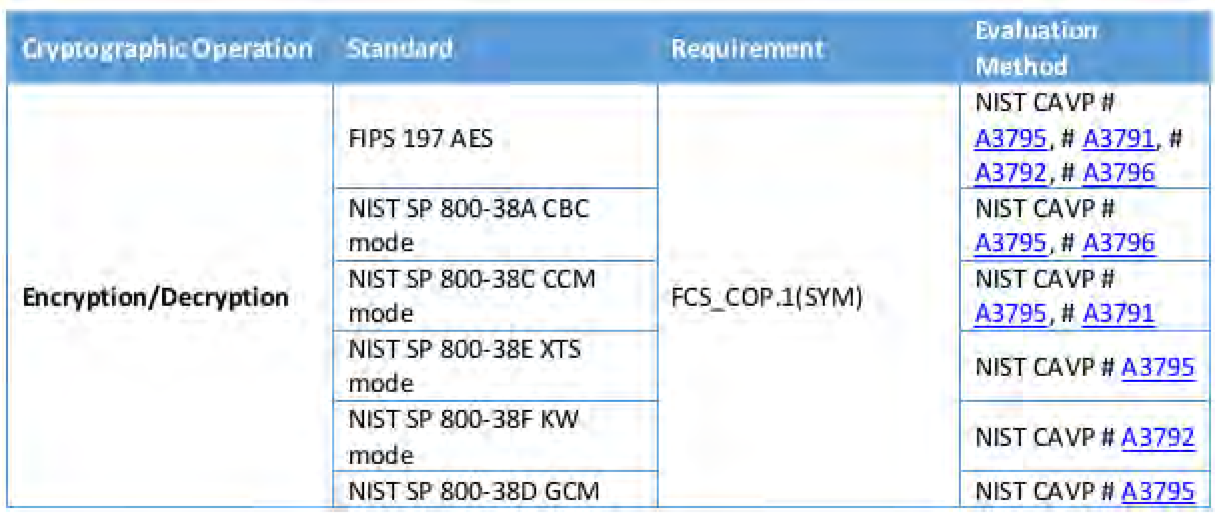


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3801, # A3797, # A3798, # A3802, # A4008, # A3748, # A3763, # A3936
	NIST SP 800-38A CBC mode		NIST CAVP # A3801, # A4008, # A3802, # A3936
	NIST SP 800-38C CCM mode		NIST CAVP # A3801, # A3797, # A4008, # A3748
	NIST SP 800-38E XTS mode		NIST CAVP # A3801, # A4008
	NIST SP 800-38F KW mode		NIST CAVP # A3798, # A3763
	NIST SP 800-38D GCM mode		NIST CAVP # A3801, # A4008
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP # A3801, # A4008
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3801, # A3802, # A4008, #A3799, # A3765, # A3936
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3801, #A3799, # A3800, # A3802, # A4008, # A3799, # A3765, # A3936
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3801, # A4008
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3801, # A3802	NIST CAVP # A3801, # A4008
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3801, # A3799, # A3802, # A4008, # A3765, # A3936
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3801, # A3799, # A4008, # A3936
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-	FCS_COP.1 (HASH)	NIST CAVP # A3801, # A4008

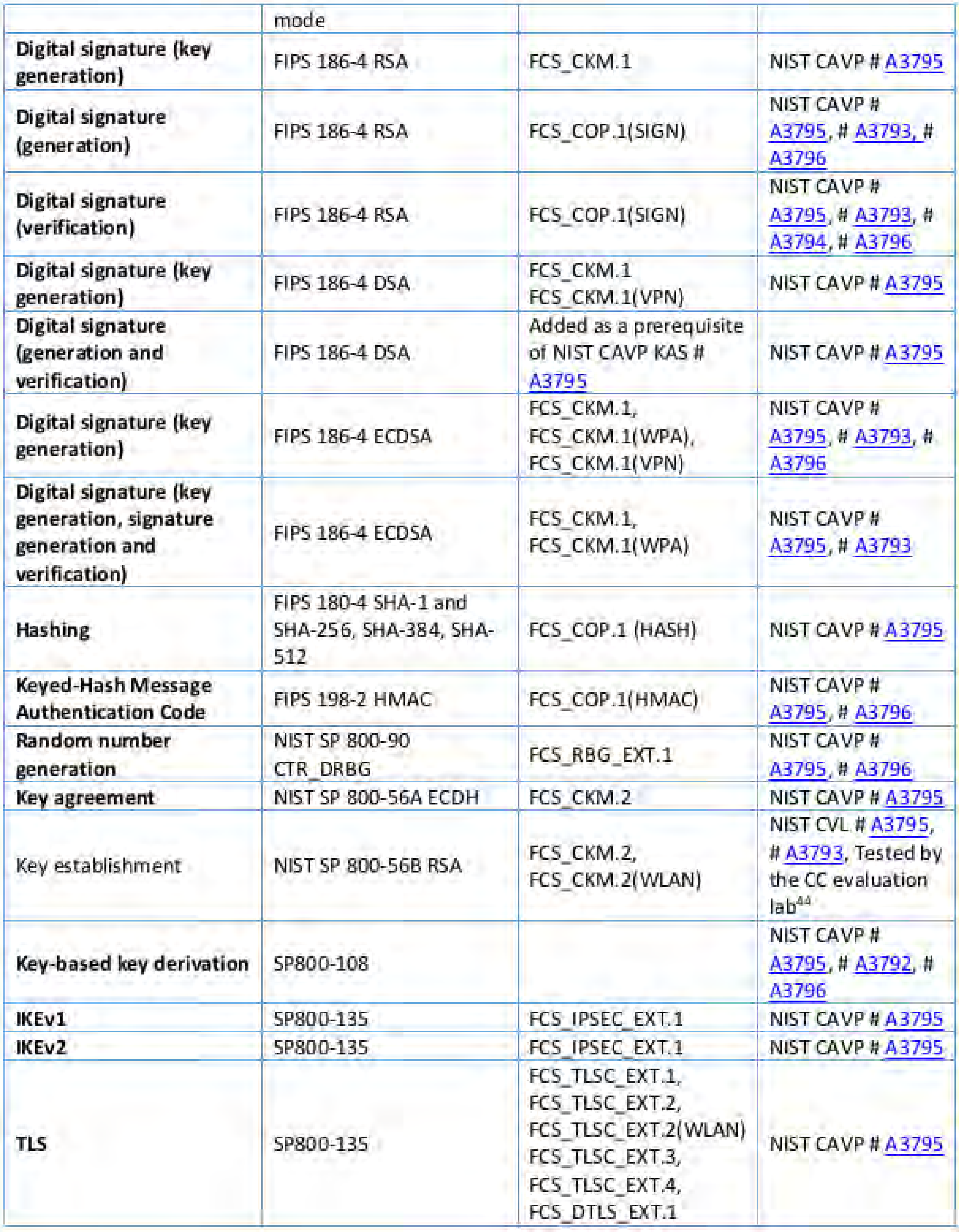


	512		
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3801, # A3802, # A4008, # A3936
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3801, # A3802, # A4008, # A3936
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3801, # A4008
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2, FCS_CKM.2(WLAN)	NIST CVL # A3801, # A3799, # A4008, # A3765, Tested by the CC evaluation lab[43]
Key-based key derivation	SP800-108		NIST CAVP # A3801, # A3798, # A3802, # A4008, # A3763, # A3936
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3801, # A4008
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3801, # A4008
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3801, # A4008

16.1.1.2 Cryptographic Algorithm Standards and Evaluation Methods for Windows 10 (version 22H2)

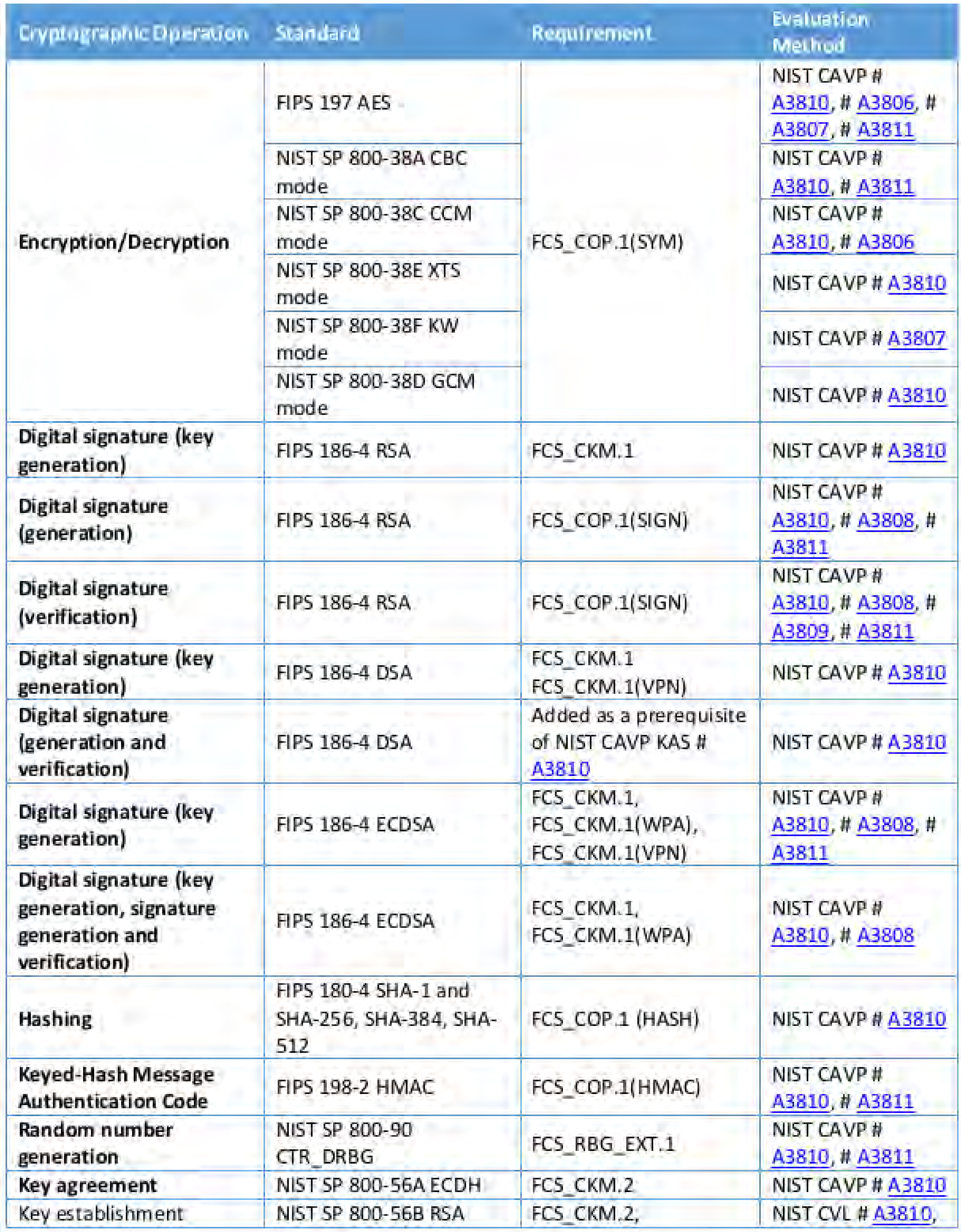


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3795, # A3791, # A3792, # A3796
	NIST SP 800-38A CBC mode		NIST CAVP # A3795, # A3796
	NIST SP 800-38C CCM mode		NIST CAVP # A3795, # A3791
	NIST SP 800-38E XTS mode		NIST CAVP # A3795
	NIST SP 800-38F KW mode		NIST CAVP # A3792
	NIST SP 800-38D GCM		NIST CAVP # A3795

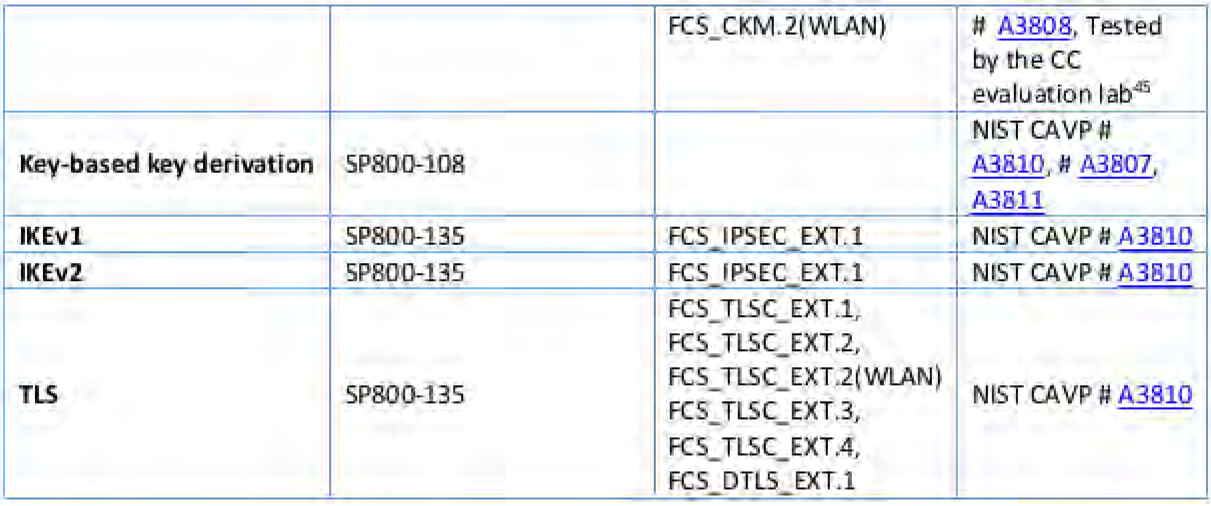


	mode		
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP # A3795
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3795, # A3793, # A3796
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3795, # A3793, # A3794, # A3796
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3795
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3795	NIST CAVP # A3795
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3795, # A3793, # A3796
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3795, # A3793
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3795
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3795, # A3796
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3795, # A3796
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3795
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2, FCS_CKM.2(WLAN)	NIST CVL # A3795, # A3793, Tested by the CC evaluation lab[44]
Key-based key derivation	SP800-108		NIST CAVP # A3795, # A3792, # A3796
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3795
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3795
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3795

16.1.1.3 Cryptographic Algorithm Standards and Evaluation Methods for Windows Server 2022 and Windows Server Datacenter: Azure Edition

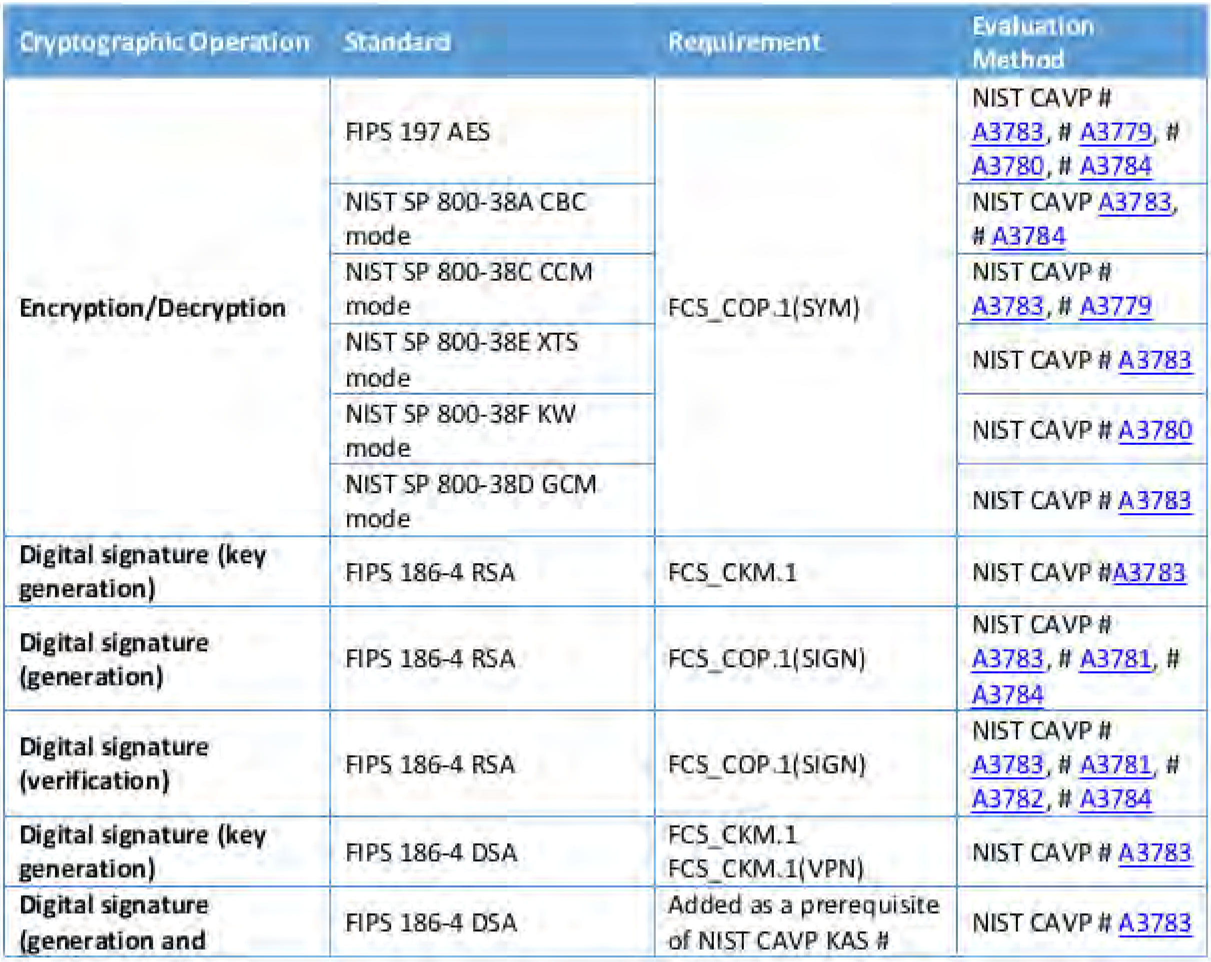


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3810, # A3806, # A3807, # A3811
	NIST SP 800-38A CBC mode		NIST CAVP # A3810, # A3811
	NIST SP 800-38C CCM mode		NIST CAVP # A3810, # A3806
	NIST SP 800-38E XTS mode		NIST CAVP # A3810
	NIST SP 800-38F KW mode		NIST CAVP # A3807
	NIST SP 800-38D GCM mode		NIST CAVP # A3810
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP # A3810
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3810, # A3808, # A3811
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3810, # A3808, # A3809, # A3811
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3810
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3810	NIST CAVP # A3810
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3810, # A3808, # A3811
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3810, # A3808
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3810
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3810, # A3811
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3810, # A3811
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3810
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2,	NIST CVL # A3810,

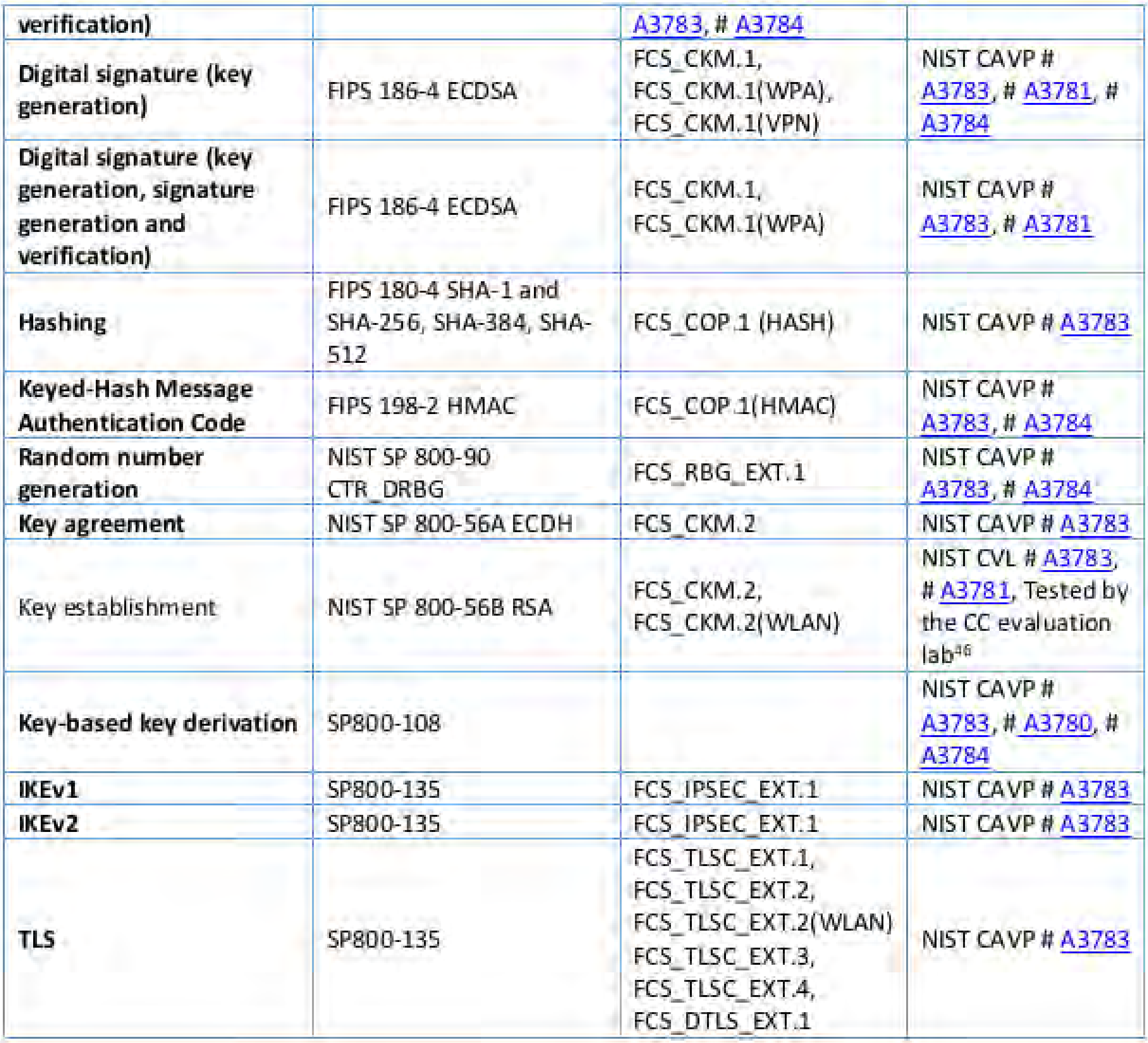


		FCS_CKM.2(WLAN)	# A3808, Tested by the CC evaluation lab[45]
Key-based key derivation	SP800-108		NIST CAVP # A3810, # A3807, A3811
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3810
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3810
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3810

16.1.1.4 Cryptographic Algorithm Standards and Evaluation Methods for Windows Server Azure Stack HCIv2 version 22H2

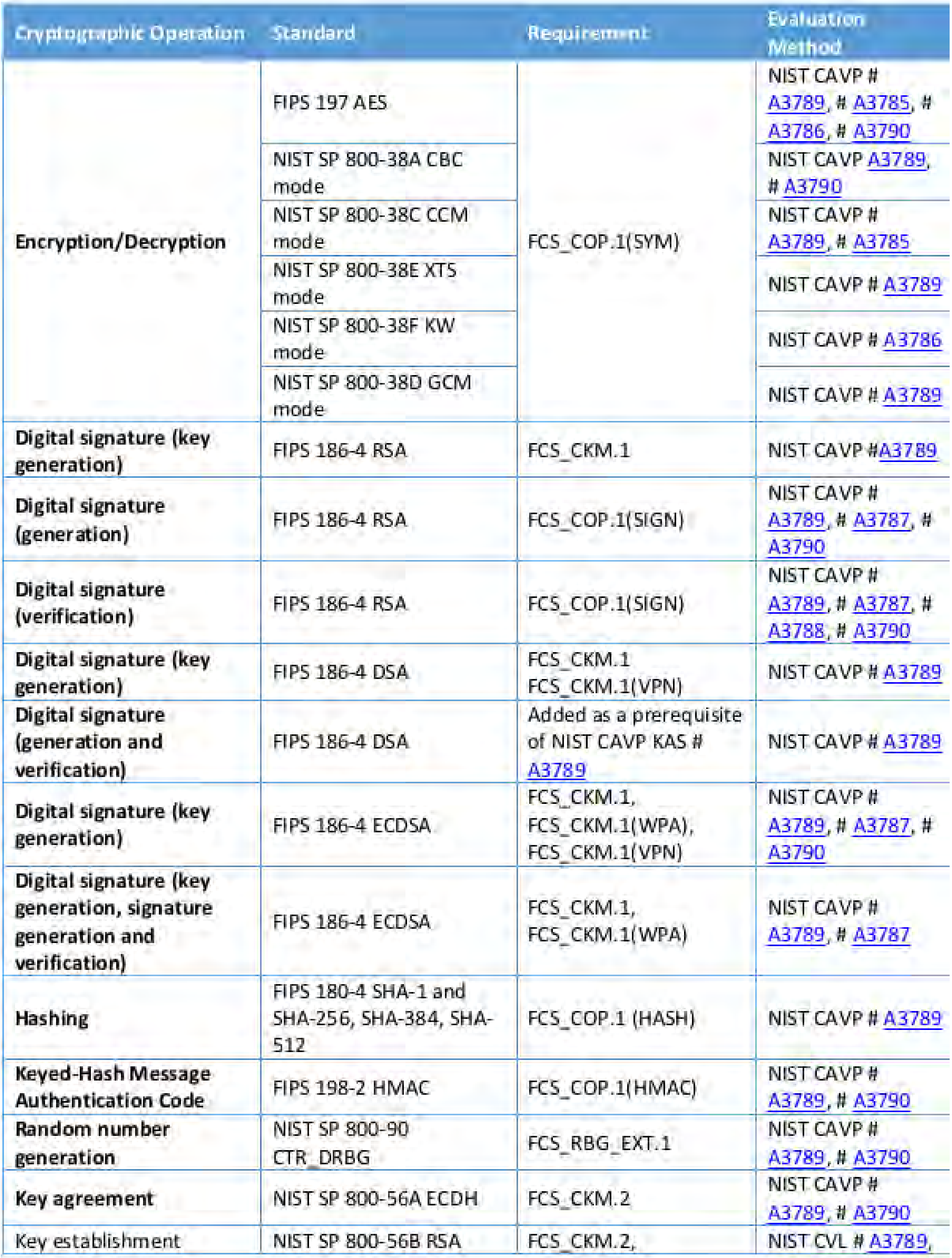


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3783, # A3779, # A3780, # A3784
	NIST SP 800-38A CBC mode		NIST CAVP A3783, # A3784
	NIST SP 800-38C CCM mode		NIST CAVP # A3783, # A3779
	NIST SP 800-38E XTS mode		NIST CAVP # A3783
	NIST SP 800-38F KW mode		NIST CAVP # A3780
	NIST SP 800-38D GCM mode		NIST CAVP # A3783
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP #A3783
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3783, # A3781, # A3784
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3783, # A3781, # A3782, # A3784
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3783
Digital signature (generation and	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS #	NIST CAVP # A3783

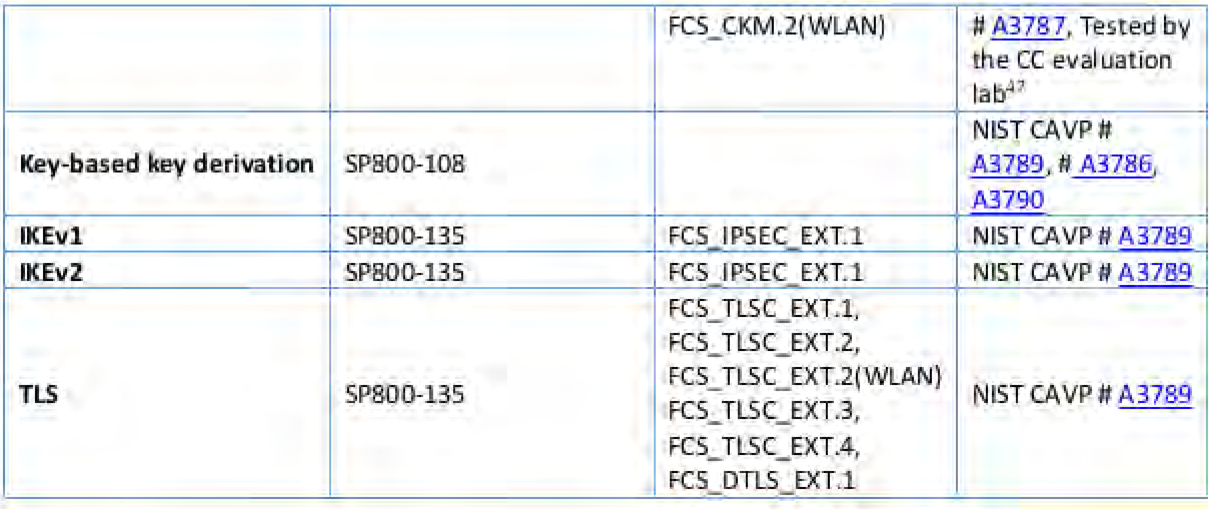


verification)		A3783, # A3784	
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3783, # A3781, # A3784
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3783, # A3781
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3783
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3783, # A3784
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3783, # A3784
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3783
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2, FCS_CKM.2(WLAN)	NIST CVL # A3783, # A3781, Tested by the CC evaluation lab[46]
Key-based key derivation	SP800-108		NIST CAVP # A3783, # A3780, # A3784
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3783
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3783
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3783

16.1.1.5 Cryptographic Algorithm Standards and Evaluation Methods for Azure Stack Hub and Azure Stack Edge



Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3789, # A3785, # A3786, # A3790
	NIST SP 800-38A CBC mode		NIST CAVP A3789, # A3790
	NIST SP 800-38C CCM mode		NIST CAVP # A3789, # A3785
	NIST SP 800-38E XTS mode		NIST CAVP # A3789
	NIST SP 800-38F KW mode		NIST CAVP # A3786
	NIST SP 800-38D GCM mode		NIST CAVP # A3789
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP #A3789
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3789, # A3787, # A3790
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3789, # A3787, # A3788, # A3790
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3789
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3789	NIST CAVP # A3789
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3789, # A3787, # A3790
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3789, # A3787
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3789
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3789, # A3790
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3789, # A3790
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3789, # A3790
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2,	NIST CVL # A3789,



		FCS_CKM.2(WLAN)	# A3787, Tested by the CC evaluation lab[47]
Key-based key derivation	SP800-108		NIST CAVP # A3789, # A3786, A3790
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3789
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3789
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3789

16.1.2 Verdict

The assurance activity does not require any documentation information. Nevertheless, the evaluator has provided information about the Signature algorithms supported by the OS.

Hence, the **PASS** verdict is assigned to the documentation review activity.

16.2 Test Activity

Based on the SFR instantiation included in the security target, the vendor has selected the following digital signature algorithms:

1. RSA Digital signature generation
2. RSA Digital signature verification
3. ECDSA Digital signature generation
4. ECDSA Digital signature verification

In addition to the Common Criteria evaluation, the laboratory has also performed the CAVP validation for these and other algorithms. The general procedure that has been followed during the evaluation in order to demonstrate the correctness of the cryptographic functionality is as follows:

1. The laboratory has used the same test vectors used as part of the CAVP validation. For digital signature algorithms, the following types of test are performed:
   - For ECDSA:
     - Algorithm Functional Test (AFT). The main goal for these tests is verify the implementation of the signature generation and signature verification operation. For the signature generation, it is expected that the TOE generates

valid signatures based on the provided message and the signature is then validated using the implementation reference by giving the communicated curve, public key and signature. For the signature verification, it is expected that the TOE verifies the validity of the given signatures together with the public key and message (or detect the error). These tests are performed for each combination of curves and hashes.

- For RSA:
  - Generated Data Test (GDT). The main goal for these tests is verify the implementation of the signature generation and signature verification operation. For the signature generation, it is expected that the TOE generate a key pair and a sign a provided message and the signature is then validated using the implementation reference by giving the public key and signature. For the signature verification, it is expected that the TOE verifies the validity of the given signatures together with the public key and message and return the outcome as a result of the operation (it could be pass or failed depending of the type of inputs). These tests are performed for each combination of modulus size and hashes.

2. The laboratory has exercised the cryptographic functionalities of the TOE by invoking the appropriate API in order to resolve the test vectors. The result of this step is a .json file which includes the associated response generated by the TOE per each test vector.
3. The laboratory has created a testing tool in order to exercise the BOTAN implementation for the target cryptographic algorithms. This tool receives the initial .json file with the test vectors as well as the .json file obtained as a result of the step 2. After parsing the information, the testing tool invokes the BOTAN implementation for the tested algorithm and resolve each test vector. After that, the testing tool compares both results (BOTAN vs TOE) in order to determine whether the cryptographic algorithms is properly implemented or not. The results of the testing tool is an individual outcome for each test vector (PASS or FAIL) and a overall outcome (PASS is all the test vectors passed or FAIL if any of them failed).

16.2.1 Test 1 Signature generation

16.2.1.1 Setup

The following environment is required to perform the test in addition to the TOE:

- A computer with:
  - Operating System: Ubuntu 20.04
  - BOTAN Tool is installed with CCN policy in evaluator machine;
  - Test vectors are located in evaluator machine.

For the installation of the *Botan Tool with CCN policy 2.15.2* all the steps defined in the *Botan-CCN_Manual_Implementador_v1* document have been followed.

16.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

16.2.1.3 Results

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

16.2.1.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the Test 1 activity demonstrate that the TOE provides a valid implementation for the evaluated cryptographic algorithms, since they have been compared against a well-known implementation (BOTAN) as a reference implementation.

Therefore, the **PASS** verdict is assigned to the Test 1 activity.

16.2.2 Test 2 Signature verification

16.2.2.1 Setup

The following environment is required to perform the test in addition to the TOE:

- A computer with:
  - Operating System: Ubuntu 20.04
  - BOTAN Tool is installed with CCN policy in evaluator machine;
  - Test vectors are located in evaluator machine.

For the installation of the *Botan Tool with CCN policy 2.15.2* all the steps defined in the *Botan-CCN_Manual_Implementador_v1* document have been followed.

16.2.2.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

16.2.2.3 Results

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

16.2.2.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the Test 2 activity demonstrate that the TOE provides a valid implementation for the evaluated cryptographic algorithms, since they have been compared against a well-known implementation (BOTAN) as a reference implementation.

Therefore, the **PASS** verdict is assigned to the Test 2 activity.

16.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to this FCS_COP.1.1(SIGN) requirement.

17 FCS_COP.1.1(4)

The assurance activity for the **FCS_COP.1.1(4)** requirement is stated as follows:

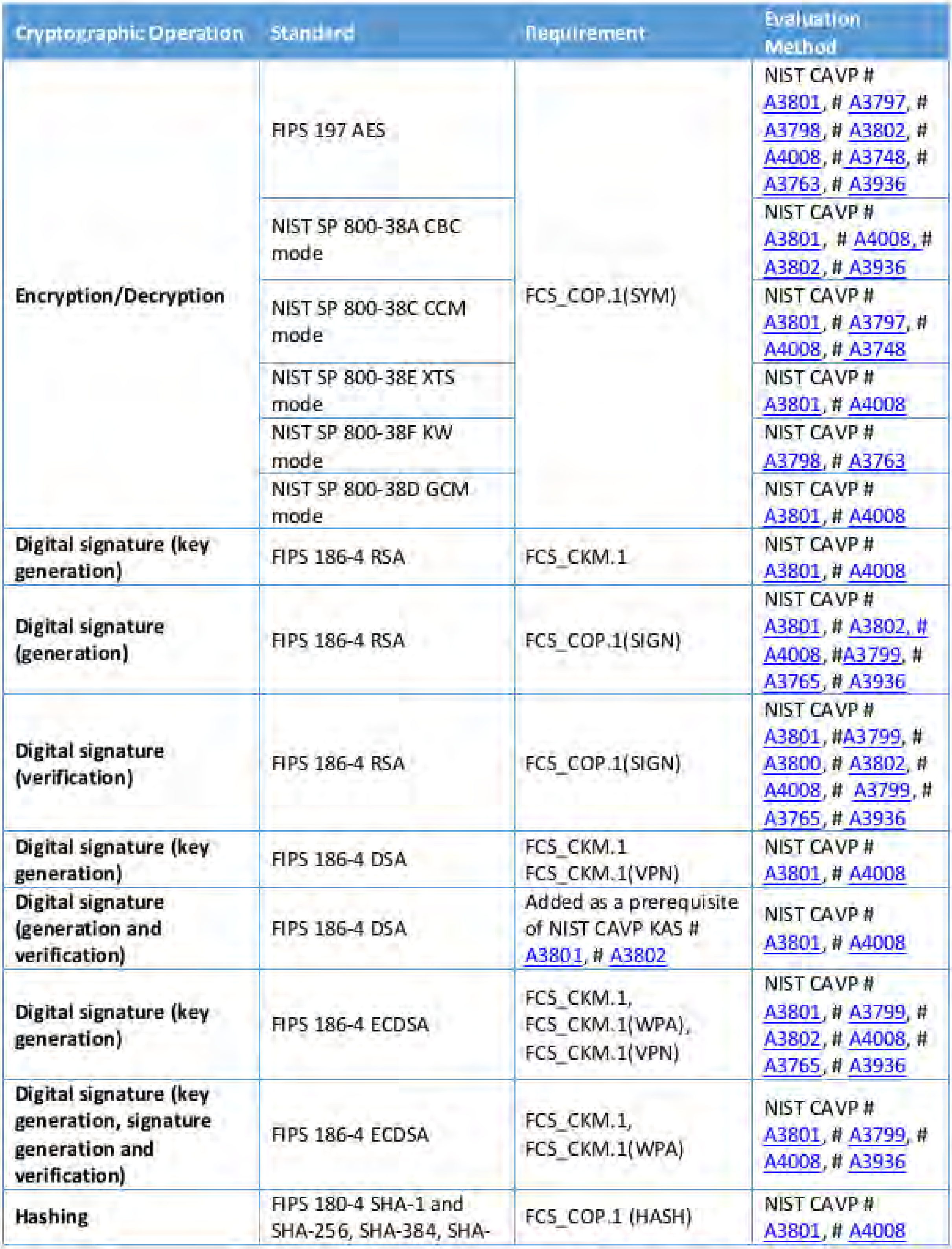
> The evaluator will perform the following activities based on the selections in the ST.
>
> For each of the supported parameter sets, the evaluator will compose 15 sets of test data. Each set shall consist of a key and message data. The evaluator will have the OS generate HMAC tags for these sets of test data. The resulting MAC tags shall be compared against the result of generating HMAC tags with the same key and IV using a known-good implementation.

17.1 Documentation Review Activity

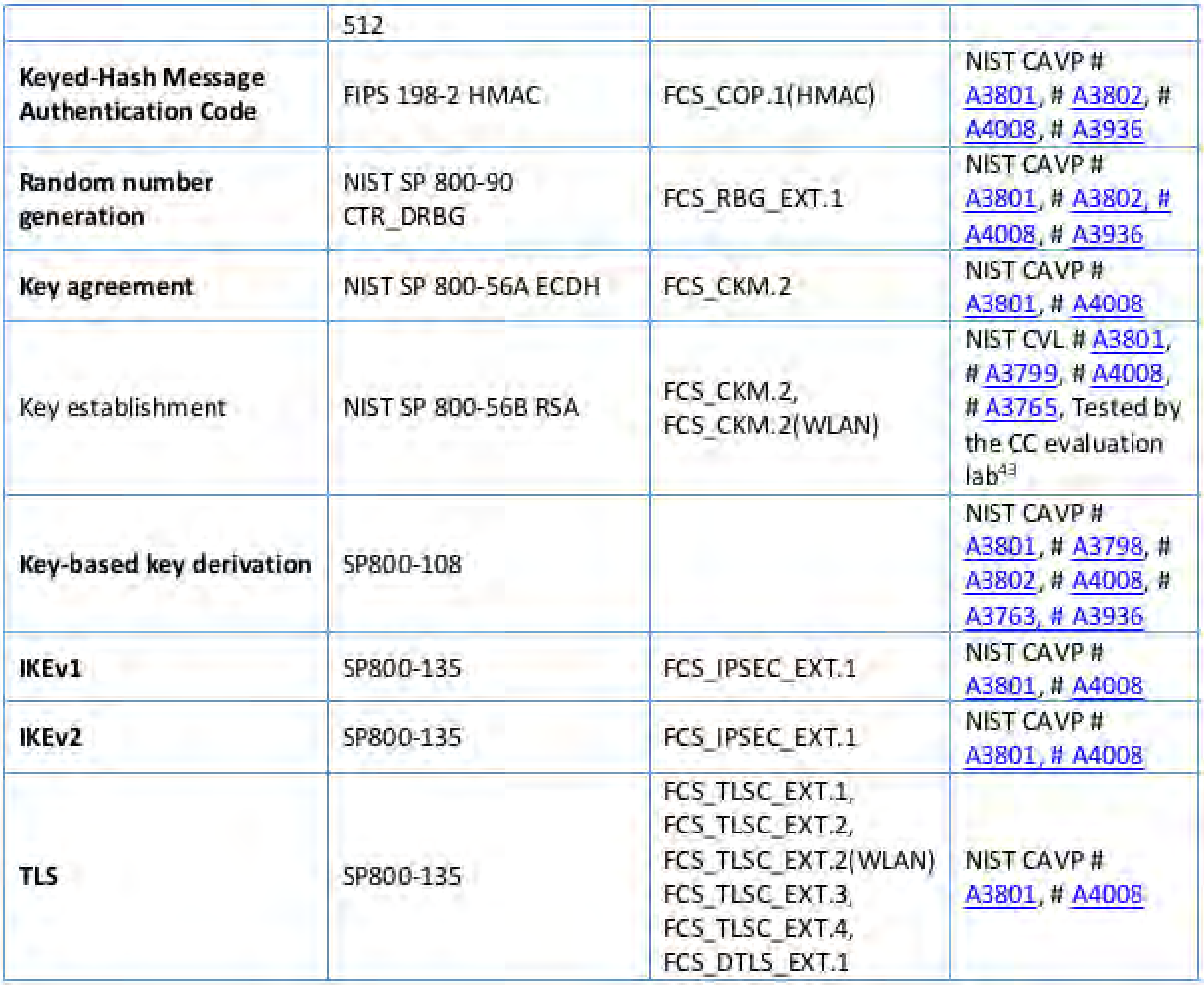
17.1.1 Findings

The evaluator has reviewed the ***Security Target*** document and the information provided in the TSS, section **6.2.2 Cryptographic Algorithm Validation**. This section includes the following tables of the cryptographic algorithms supported by Windows 11, Windows 10 versions, Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge.

17.1.1.1 Cryptographic Algorithm Standards and Evaluation Methods for Windows 11 (version 22H2)

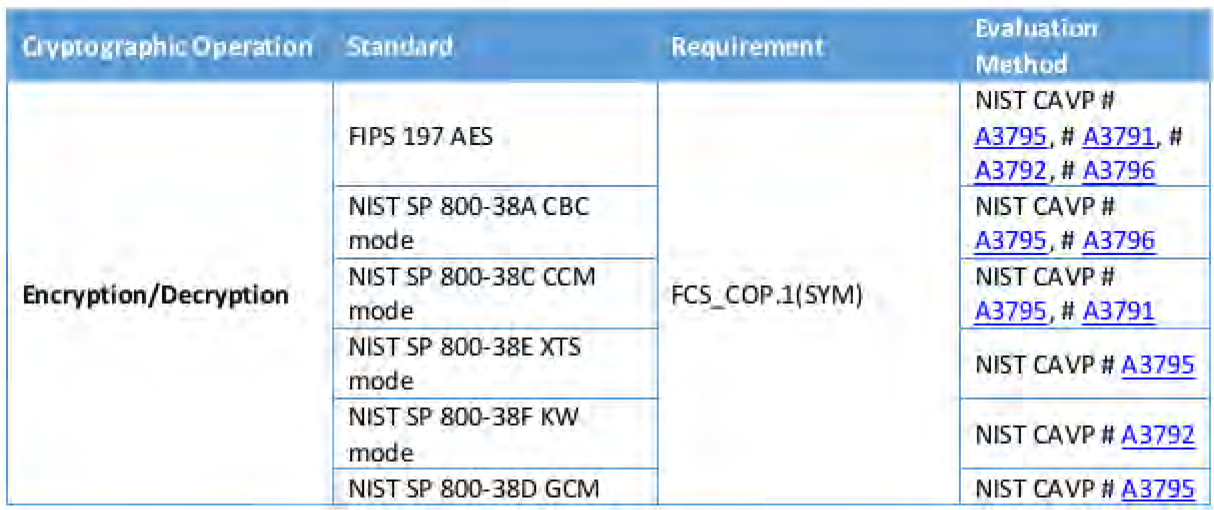


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3801, # A3797, # A3798, # A3802, # A4008, # A3748, # A3763, # A3936
	NIST SP 800-38A CBC mode		NIST CAVP # A3801, # A4008, # A3802, # A3936
	NIST SP 800-38C CCM mode		NIST CAVP # A3801, # A3797, # A4008, # A3748
	NIST SP 800-38E XTS mode		NIST CAVP # A3801, # A4008
	NIST SP 800-38F KW mode		NIST CAVP # A3798, # A3763
	NIST SP 800-38D GCM mode		NIST CAVP # A3801, # A4008
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP # A3801, # A4008
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3801, # A3802, # A4008, #A3799, # A3765, # A3936
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3801, #A3799, # A3800, # A3802, # A4008, # A3799, # A3765, # A3936
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3801, # A4008
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3801, # A3802	NIST CAVP # A3801, # A4008
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3801, # A3799, # A3802, # A4008, # A3765, # A3936
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3801, # A3799, # A4008, # A3936
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-	FCS_COP.1 (HASH)	NIST CAVP # A3801, # A4008

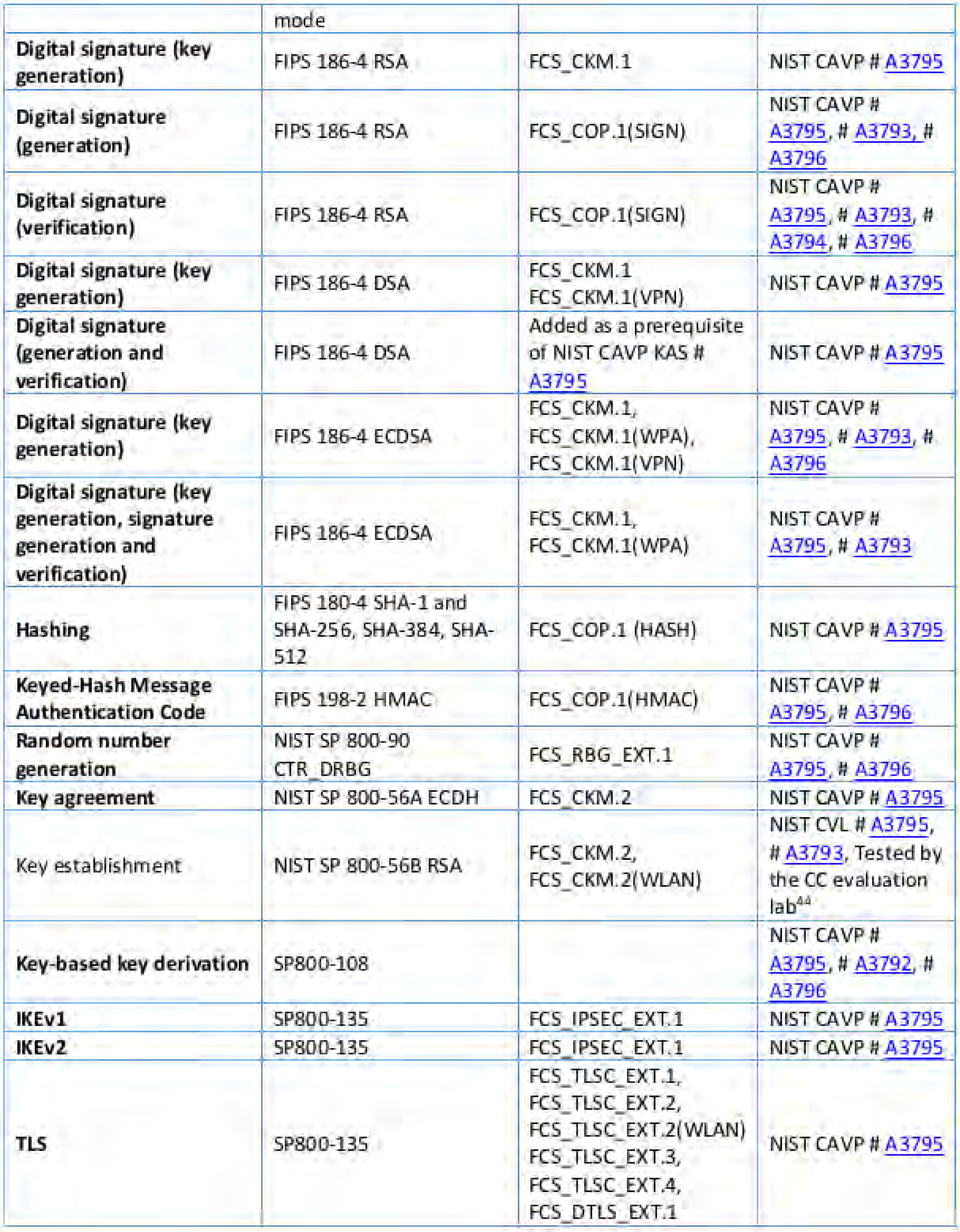


	512		
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3801, # A3802, # A4008, # A3936
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3801, # A3802, # A4008, # A3936
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3801, # A4008
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2, FCS_CKM.2(WLAN)	NIST CVL # A3801, # A3799, # A4008, # A3765, Tested by the CC evaluation lab[43]
Key-based key derivation	SP800-108		NIST CAVP # A3801, # A3798, # A3802, # A4008, # A3763, # A3936
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3801, # A4008
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3801, # A4008
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3801, # A4008

17.1.1.2 Cryptographic Algorithm Standards and Evaluation Methods for Windows 10 (version 22H2)

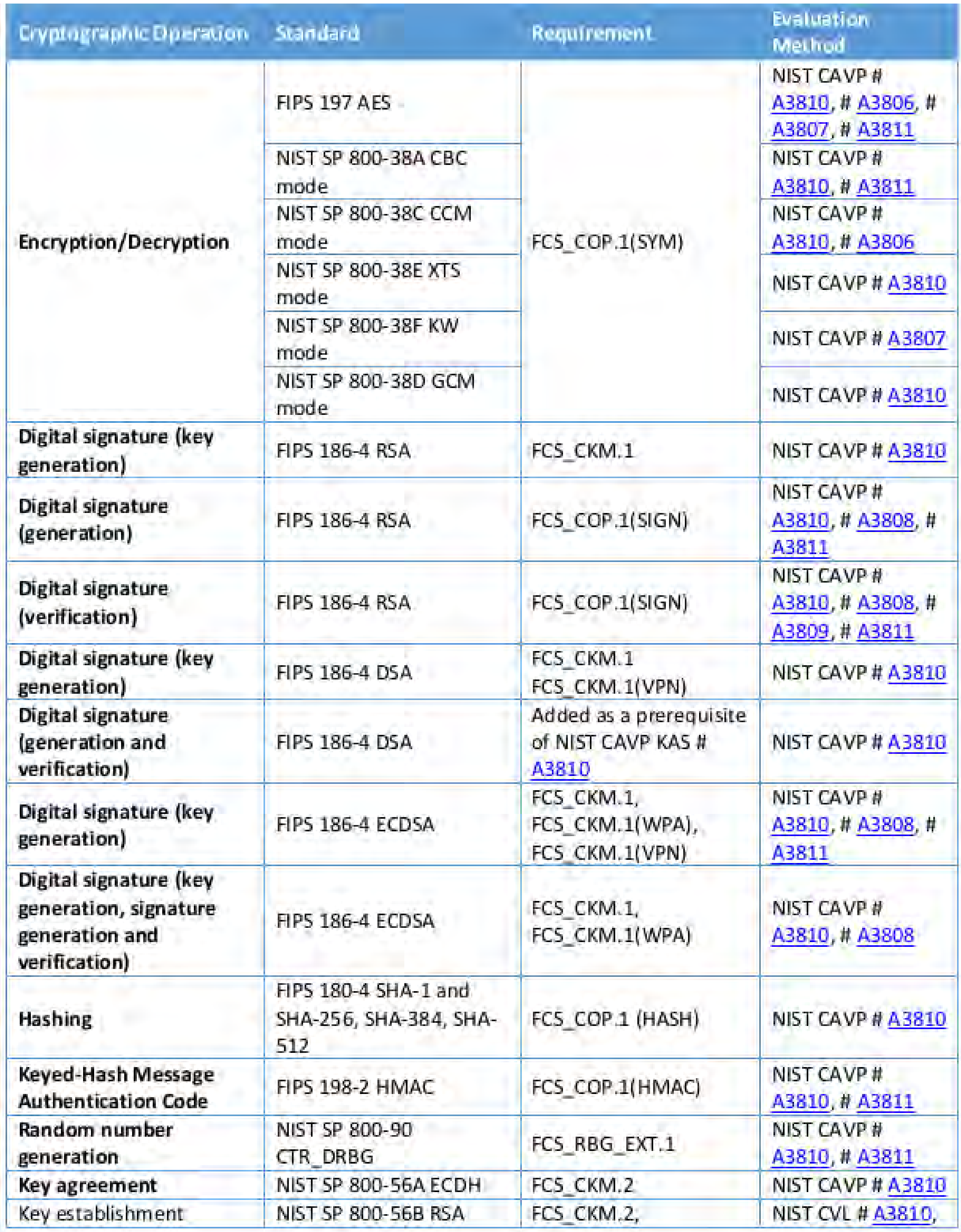


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3795, # A3791, # A3792, # A3796
	NIST SP 800-38A CBC mode		NIST CAVP # A3795, # A3796
	NIST SP 800-38C CCM mode		NIST CAVP # A3795, # A3791
	NIST SP 800-38E XTS mode		NIST CAVP # A3795
	NIST SP 800-38F KW mode		NIST CAVP # A3792
	NIST SP 800-38D GCM		NIST CAVP # A3795

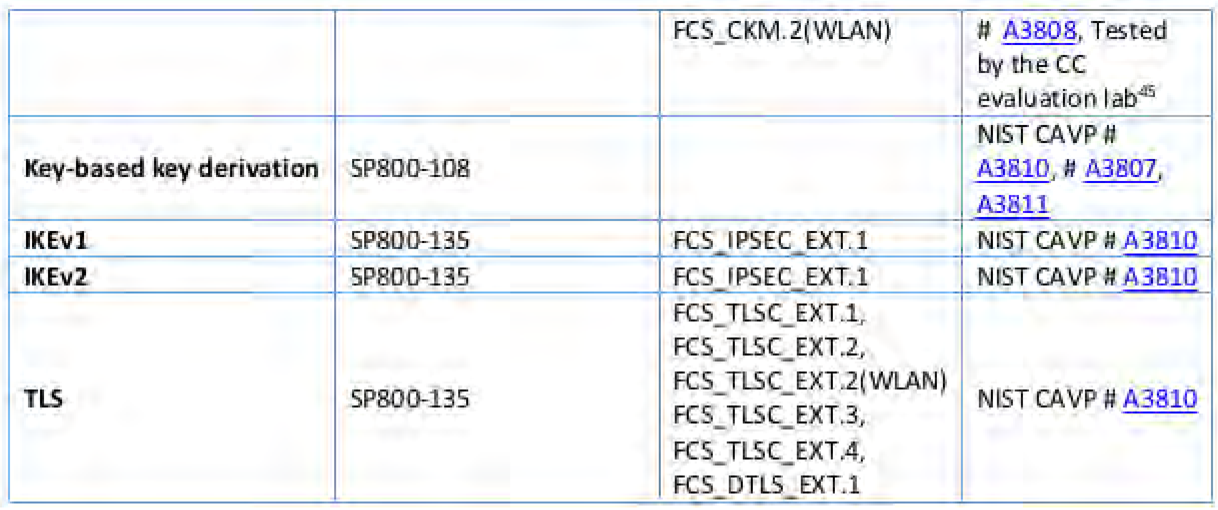


	mode		
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP # A3795
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3795, # A3793, # A3796
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3795, # A3793, # A3794, # A3796
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3795
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3795	NIST CAVP # A3795
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3795, # A3793, # A3796
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3795, # A3793
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3795
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3795, # A3796
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3795, # A3796
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3795
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2, FCS_CKM.2(WLAN)	NIST CVL # A3795, # A3793, Tested by the CC evaluation lab[44]
Key-based key derivation	SP800-108		NIST CAVP # A3795, # A3792, # A3796
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3795
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3795
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3795

17.1.1.3 Cryptographic Algorithm Standards and Evaluation Methods for Windows Server 2022 and Windows Server Datacenter: Azure Edition

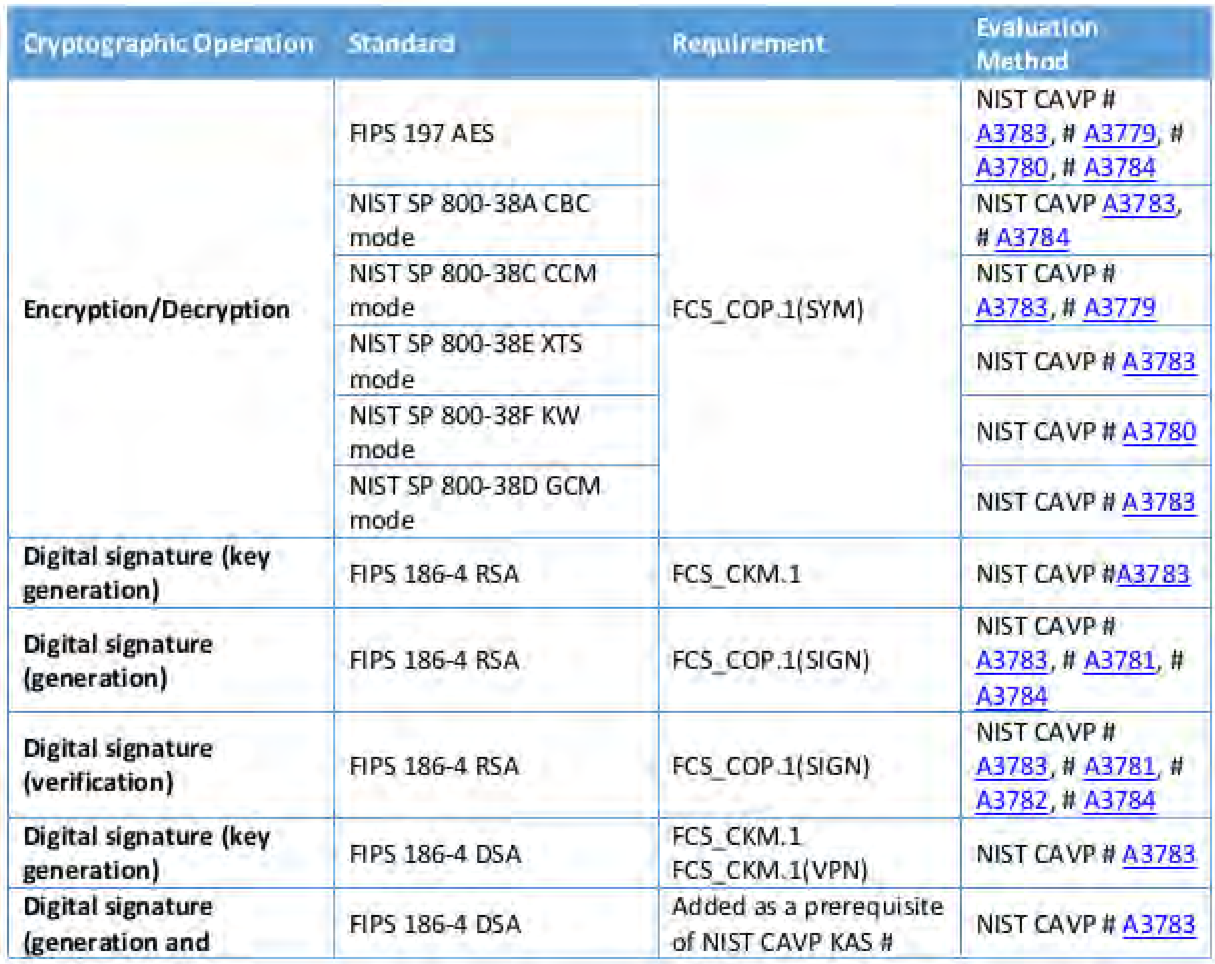


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3810, # A3806, # A3807, # A3811
	NIST SP 800-38A CBC mode		NIST CAVP # A3810, # A3811
	NIST SP 800-38C CCM mode		NIST CAVP # A3810, # A3806
	NIST SP 800-38E XTS mode		NIST CAVP # A3810
	NIST SP 800-38F KW mode		NIST CAVP # A3807
	NIST SP 800-38D GCM mode		NIST CAVP # A3810
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP # A3810
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3810, # A3808, # A3811
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3810, # A3808, # A3809, # A3811
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3810
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3810	NIST CAVP # A3810
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3810, # A3808, # A3811
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3810, # A3808
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3810
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3810, # A3811
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3810, # A3811
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3810
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2,	NIST CVL # A3810,

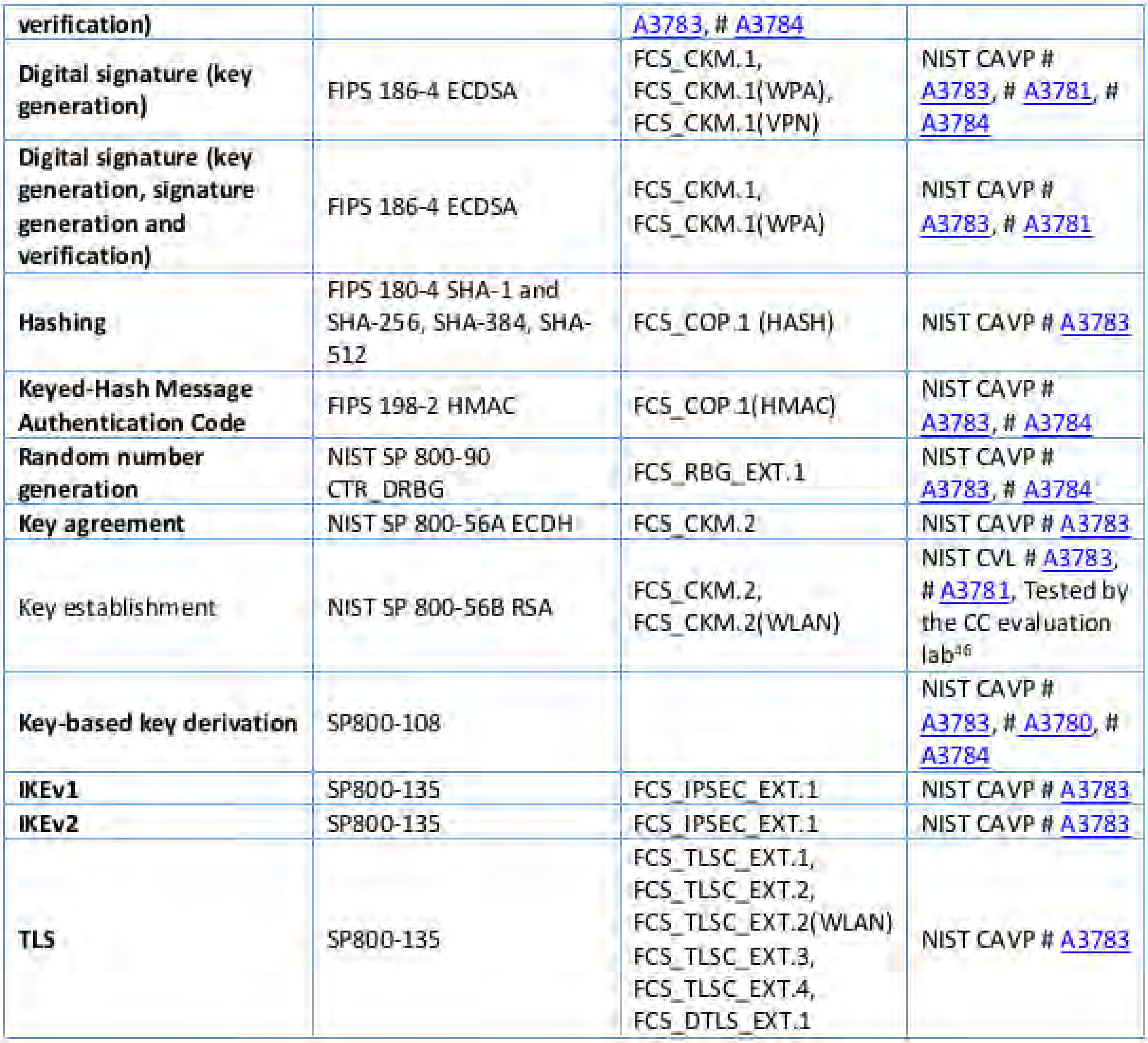


		FCS_CKM.2(WLAN)	# A3808, Tested by the CC evaluation lab[45]
Key-based key derivation	SP800-108		NIST CAVP # A3810, # A3807, A3811
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3810
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3810
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3810

17.1.1.4 Cryptographic Algorithm Standards and Evaluation Methods for Windows Server Azure Stack HCIv2 version 22H2

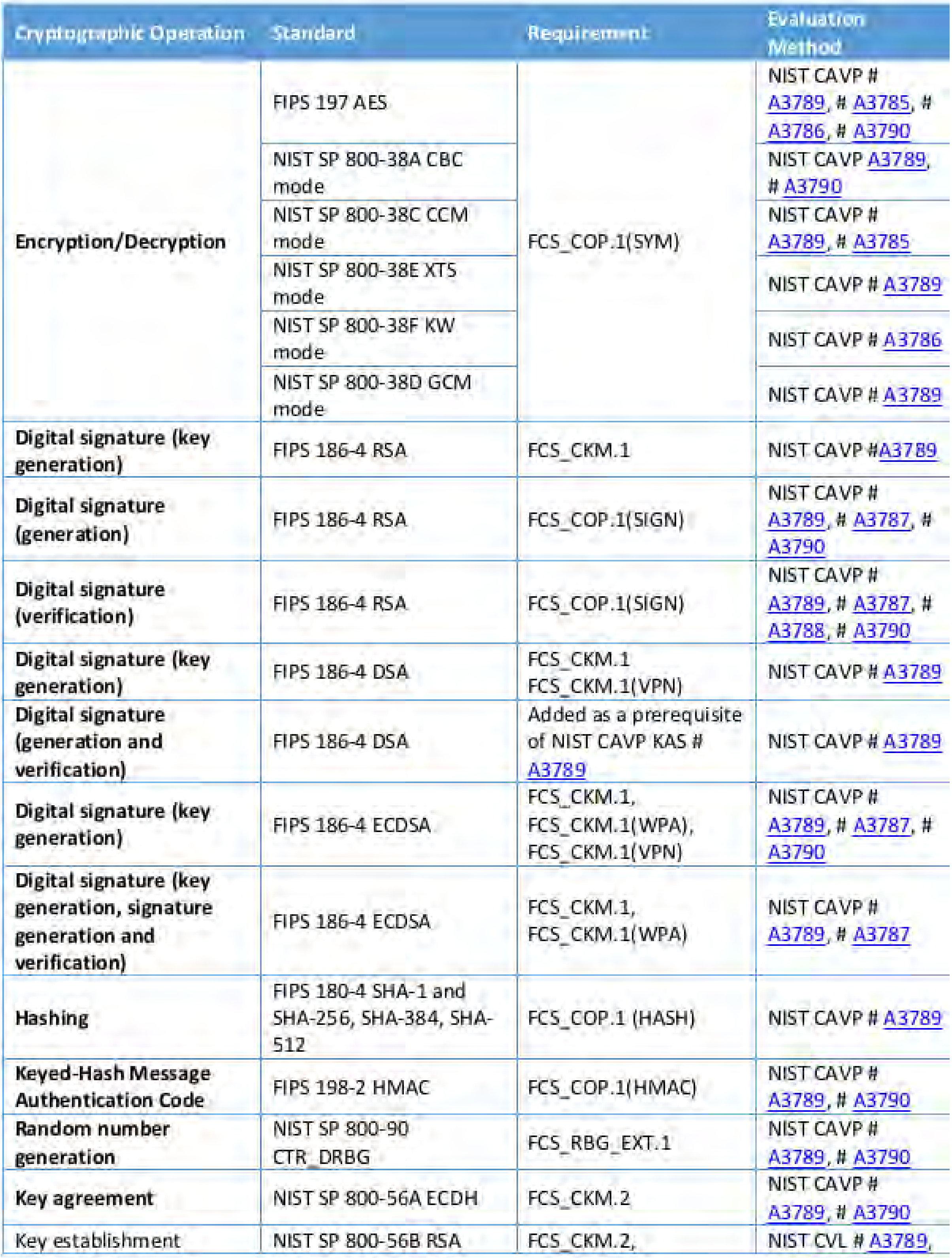


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3783, # A3779, # A3780, # A3784
	NIST SP 800-38A CBC mode		NIST CAVP A3783, # A3784
	NIST SP 800-38C CCM mode		NIST CAVP # A3783, # A3779
	NIST SP 800-38E XTS mode		NIST CAVP # A3783
	NIST SP 800-38F KW mode		NIST CAVP # A3780
	NIST SP 800-38D GCM mode		NIST CAVP # A3783
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP #A3783
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3783, # A3781, # A3784
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3783, # A3781, # A3782, # A3784
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3783
Digital signature (generation and	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS #	NIST CAVP # A3783

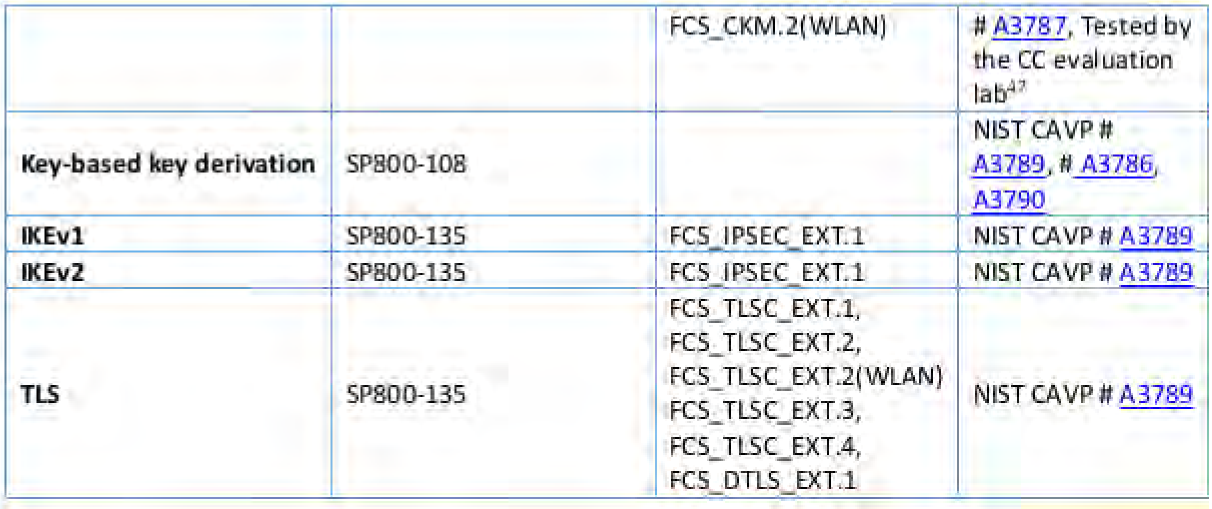


verification)		A3783, # A3784	
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3783, # A3781, # A3784
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3783, # A3781
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3783
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3783, # A3784
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3783, # A3784
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3783
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2, FCS_CKM.2(WLAN)	NIST CVL # A3783, # A3781, Tested by the CC evaluation lab[46]
Key-based key derivation	SP800-108		NIST CAVP # A3783, # A3780, # A3784
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3783
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3783
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3783

17.1.1.5 Cryptographic Algorithm Standards and Evaluation Methods for Azure Stack Hub and Azure Stack Edge



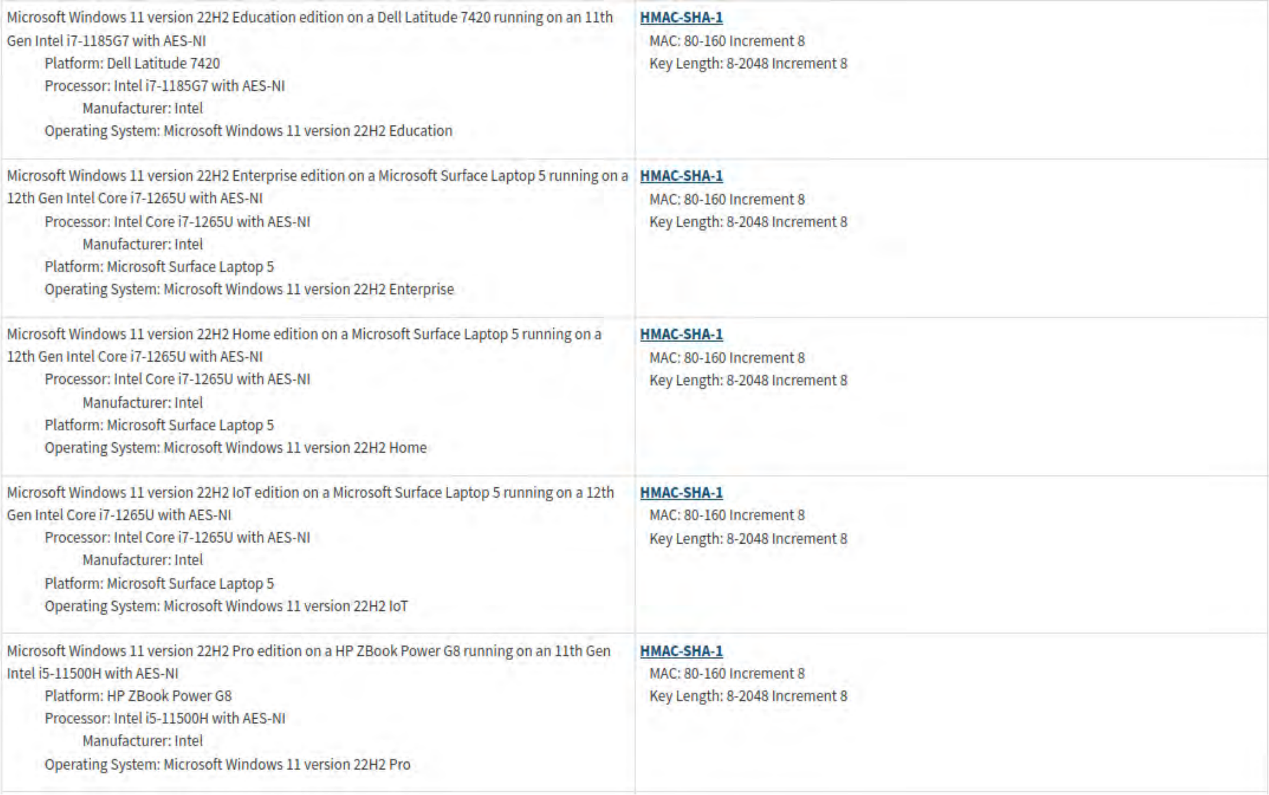
Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3789, # A3785, # A3786, # A3790
	NIST SP 800-38A CBC mode		NIST CAVP A3789, # A3790
	NIST SP 800-38C CCM mode		NIST CAVP # A3789, # A3785
	NIST SP 800-38E XTS mode		NIST CAVP # A3789
	NIST SP 800-38F KW mode		NIST CAVP # A3786
	NIST SP 800-38D GCM mode		NIST CAVP # A3789
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP #A3789
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3789, # A3787, # A3790
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3789, # A3787, # A3788, # A3790
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3789
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3789	NIST CAVP # A3789
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3789, # A3787, # A3790
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3789, # A3787
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3789
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3789, # A3790
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3789, # A3790
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3789, # A3790
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2,	NIST CVL # A3789,



		FCS_CKM.2(WLAN)	# A3787, Tested by the CC evaluation lab[47]
Key-based key derivation	SP800-108		NIST CAVP # A3789, # A3786, A3790
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3789
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3789
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3789

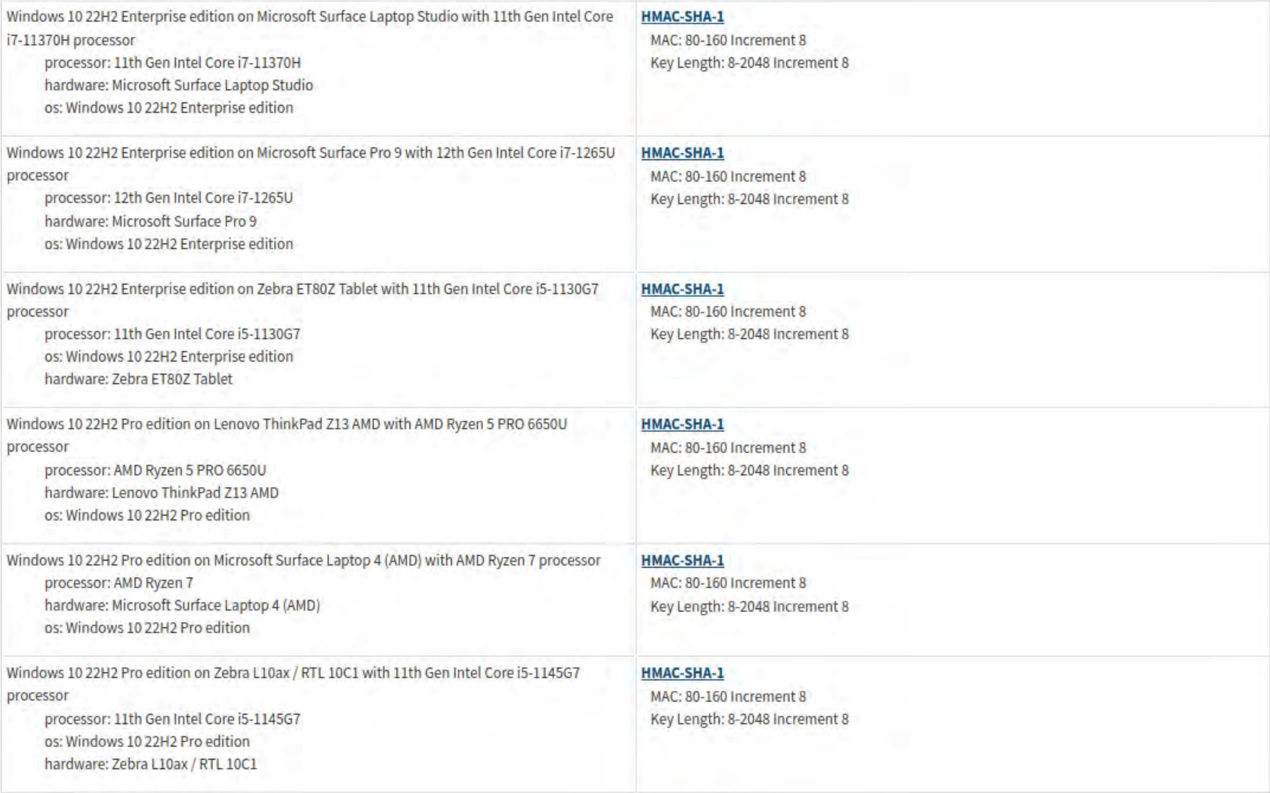
As part of the testing activity described below, the correctness of the cryptographic functionality has been demonstrated against the BOTAN tool. However, HMAC-SHA-1 is not available in BOTAN, and the laboratory has verified the implementation against the CAVP tool. Below, the CAVP certificates granted for this functionality are listed (extracted from the tables above)

17.1.1.6 Windows 11 version 22H2 (CAVP Cert. #A4008)



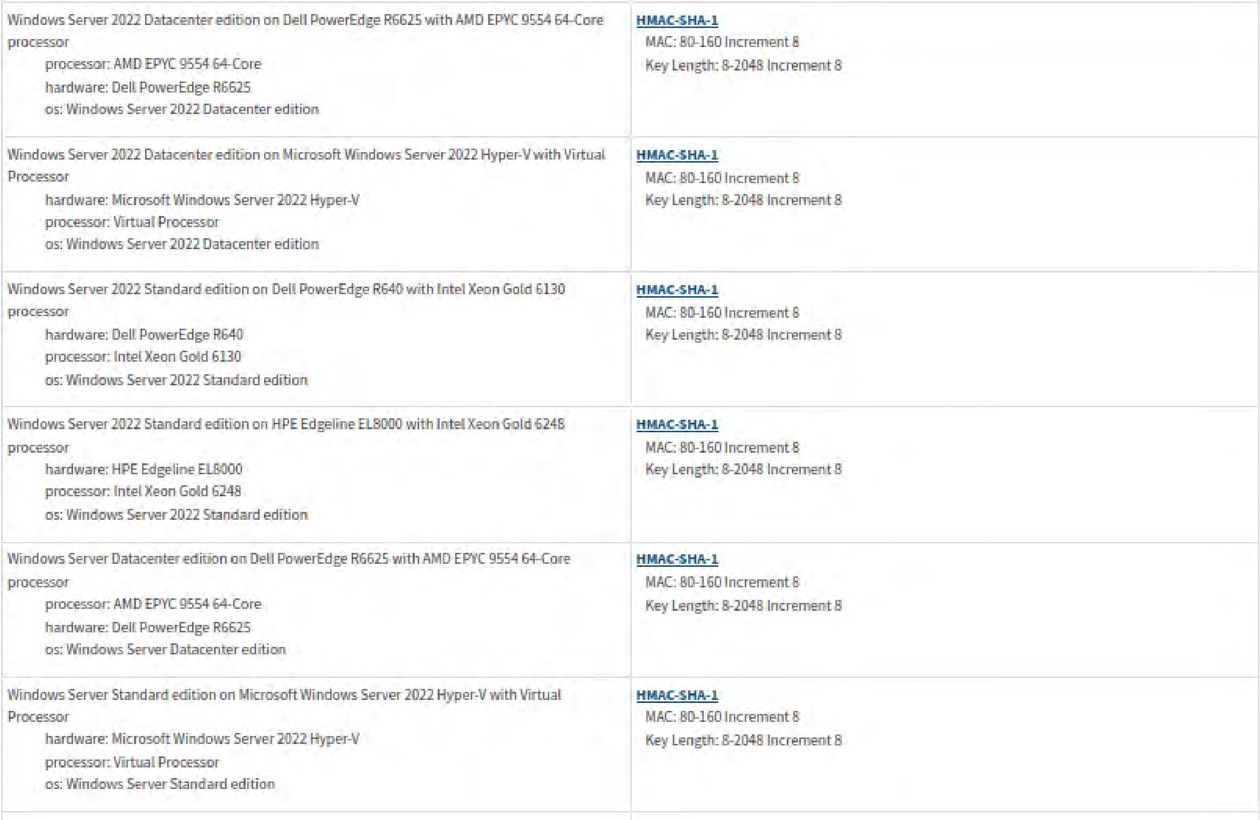
Microsoft Windows 11 version 22H2 Education edition on a Dell Latitude 7420 running on an 11th Gen Intel i7-1185G7 with AES-NI Platform: Dell Latitude 7420 Processor: Intel i7-1185G7 with AES-NI Manufacturer: Intel Operating System: Microsoft Windows 11 version 22H2 Education	**HMAC-SHA-1** MAC: 80-160 Increment 8 Key Length: 8-2048 Increment 8
Microsoft Windows 11 version 22H2 Enterprise edition on a Microsoft Surface Laptop 5 running on a 12th Gen Intel Core i7-1265U with AES-NI Processor: Intel Core i7-1265U with AES-NI Manufacturer: Intel Platform: Microsoft Surface Laptop 5 Operating System: Microsoft Windows 11 version 22H2 Enterprise	**HMAC-SHA-1** MAC: 80-160 Increment 8 Key Length: 8-2048 Increment 8
Microsoft Windows 11 version 22H2 Home edition on a Microsoft Surface Laptop 5 running on a 12th Gen Intel Core i7-1265U with AES-NI Processor: Intel Core i7-1265U with AES-NI Manufacturer: Intel Platform: Microsoft Surface Laptop 5 Operating System: Microsoft Windows 11 version 22H2 Home	**HMAC-SHA-1** MAC: 80-160 Increment 8 Key Length: 8-2048 Increment 8
Microsoft Windows 11 version 22H2 IoT edition on a Microsoft Surface Laptop 5 running on a 12th Gen Intel Core i7-1265U with AES-NI Processor: Intel Core i7-1265U with AES-NI Manufacturer: Intel Platform: Microsoft Surface Laptop 5 Operating System: Microsoft Windows 11 version 22H2 IoT	**HMAC-SHA-1** MAC: 80-160 Increment 8 Key Length: 8-2048 Increment 8
Microsoft Windows 11 version 22H2 Pro edition on a HP ZBook Power G8 running on an 11th Gen Intel i5-11500H with AES-NI Platform: HP ZBook Power G8 Processor: Intel i5-11500H with AES-NI Manufacturer: Intel Operating System: Microsoft Windows 11 version 22H2 Pro	**HMAC-SHA-1** MAC: 80-160 Increment 8 Key Length: 8-2048 Increment 8

17.1.1.7 Windows 10 version 22H2 (CAVP Cert. #A3795)



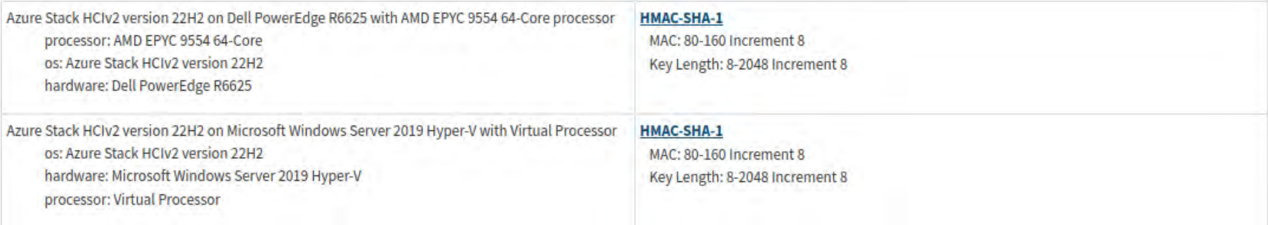
Windows 10 22H2 Enterprise edition on Microsoft Surface Laptop Studio with 11th Gen Intel Core i7-11370H processor processor: 11th Gen Intel Core i7-11370H hardware: Microsoft Surface Laptop Studio os: Windows 10 22H2 Enterprise edition	HMAC-SHA-1 MAC: 80-160 Increment 8 Key Length: 8-2048 Increment 8
Windows 10 22H2 Enterprise edition on Microsoft Surface Pro 9 with 12th Gen Intel Core i7-1265U processor processor: 12th Gen Intel Core i7-1265U hardware: Microsoft Surface Pro 9 os: Windows 10 22H2 Enterprise edition	HMAC-SHA-1 MAC: 80-160 Increment 8 Key Length: 8-2048 Increment 8
Windows 10 22H2 Enterprise edition on Zebra ET80Z Tablet with 11th Gen Intel Core i5-1130G7 processor processor: 11th Gen Intel Core i5-1130G7 os: Windows 10 22H2 Enterprise edition hardware: Zebra ET80Z Tablet	HMAC-SHA-1 MAC: 80-160 Increment 8 Key Length: 8-2048 Increment 8
Windows 10 22H2 Pro edition on Lenovo ThinkPad Z13 AMD with AMD Ryzen 5 PRO 6650U processor processor: AMD Ryzen 5 PRO 6650U hardware: Lenovo ThinkPad Z13 AMD os: Windows 10 22H2 Pro edition	HMAC-SHA-1 MAC: 80-160 Increment 8 Key Length: 8-2048 Increment 8
Windows 10 22H2 Pro edition on Microsoft Surface Laptop 4 (AMD) with AMD Ryzen 7 processor processor: AMD Ryzen 7 hardware: Microsoft Surface Laptop 4 (AMD) os: Windows 10 22H2 Pro edition	HMAC-SHA-1 MAC: 80-160 Increment 8 Key Length: 8-2048 Increment 8
Windows 10 22H2 Pro edition on Zebra L10ax / RTL 10C1 with 11th Gen Intel Core i5-1145G7 processor processor: 11th Gen Intel Core i5-1145G7 os: Windows 10 22H2 Pro edition hardware: Zebra L10ax / RTL 10C1	HMAC-SHA-1 MAC: 80-160 Increment 8 Key Length: 8-2048 Increment 8

17.1.1.8 Windows Server 2022 and Windows Server Datacenter: Azure Edition (CAVP Cert. #A3810)



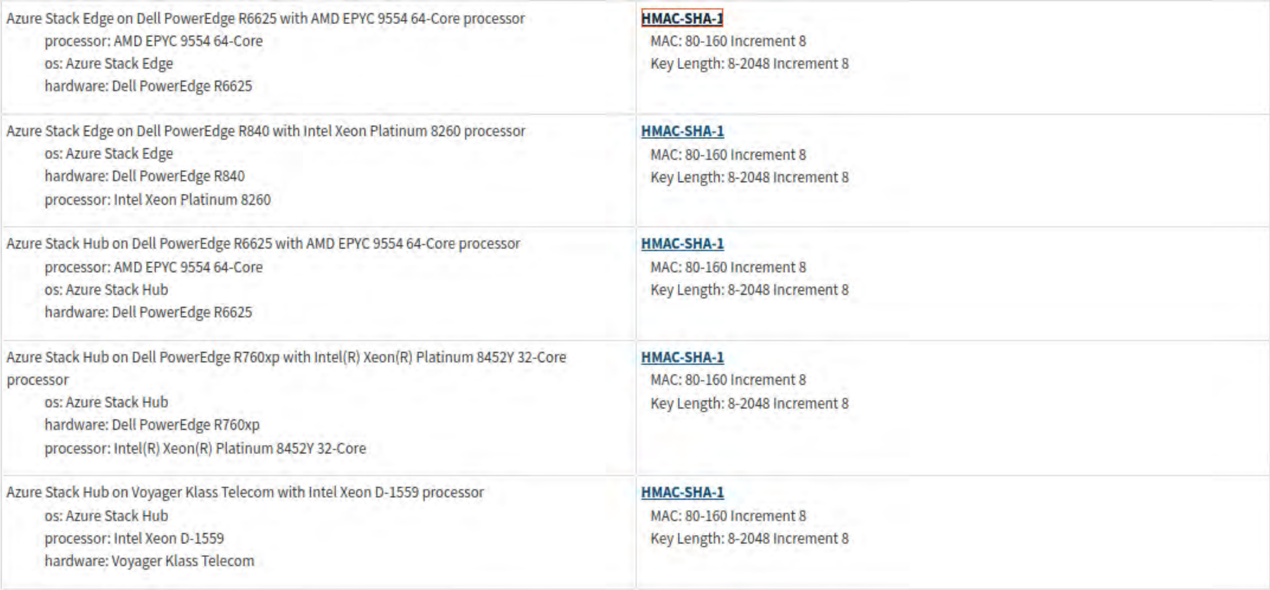
Windows Server 2022 Datacenter edition on Dell PowerEdge R6625 with AMD EPYC 9554 64-Core processor processor: AMD EPYC 9554 64-Core hardware: Dell PowerEdge R6625 os: Windows Server 2022 Datacenter edition	HMAC-SHA-1 MAC: 80-160 Increment 8 Key Length: 8-2048 Increment 8
Windows Server 2022 Datacenter edition on Microsoft Windows Server 2022 Hyper-V with Virtual Processor hardware: Microsoft Windows Server 2022 Hyper-V processor: Virtual Processor os: Windows Server 2022 Datacenter edition	HMAC-SHA-1 MAC: 80-160 Increment 8 Key Length: 8-2048 Increment 8
Windows Server 2022 Standard edition on Dell PowerEdge R640 with Intel Xeon Gold 6130 processor hardware: Dell PowerEdge R640 processor: Intel Xeon Gold 6130 os: Windows Server 2022 Standard edition	HMAC-SHA-1 MAC: 80-160 Increment 8 Key Length: 8-2048 Increment 8
Windows Server 2022 Standard edition on HPE Edgeline EL8000 with Intel Xeon Gold 6248 processor hardware: HPE Edgeline EL8000 processor: Intel Xeon Gold 6248 os: Windows Server 2022 Standard edition	HMAC-SHA-1 MAC: 80-160 Increment 8 Key Length: 8-2048 Increment 8
Windows Server Datacenter edition on Dell PowerEdge R6625 with AMD EPYC 9554 64-Core processor processor: AMD EPYC 9554 64-Core hardware: Dell PowerEdge R6625 os: Windows Server Datacenter edition	HMAC-SHA-1 MAC: 80-160 Increment 8 Key Length: 8-2048 Increment 8
Windows Server Standard edition on Microsoft Windows Server 2022 Hyper-V with Virtual Processor hardware: Microsoft Windows Server 2022 Hyper-V processor: Virtual Processor os: Windows Server Standard edition	HMAC-SHA-1 MAC: 80-160 Increment 8 Key Length: 8-2048 Increment 8

17.1.1.9 Windows Server Azure Stack HCIv2 version 22H2 (CAVP Cert. #A3783)



Azure Stack HCIv2 version 22H2 on Dell PowerEdge R6625 with AMD EPYC 9554 64-Core processor processor: AMD EPYC 9554 64-Core os: Azure Stack HCIv2 version 22H2 hardware: Dell PowerEdge R6625	HMAC-SHA-1 MAC: 80-160 Increment 8 Key Length: 8-2048 Increment 8
Azure Stack HCIv2 version 22H2 on Microsoft Windows Server 2019 Hyper-V with Virtual Processor os: Azure Stack HCIv2 version 22H2 hardware: Microsoft Windows Server 2019 Hyper-V processor: Virtual Processor	HMAC-SHA-1 MAC: 80-160 Increment 8 Key Length: 8-2048 Increment 8

17.1.1.10 Azure Stack Hub and Azure Stack Edge (CAVP Cert. #A3789)



Azure Stack Edge on Dell PowerEdge R6625 with AMD EPYC 9554 64-Core processor processor: AMD EPYC 9554 64-Core os: Azure Stack Edge hardware: Dell PowerEdge R6625	HMAC-SHA-1 MAC: 80-160 Increment 8 Key Length: 8-2048 Increment 8
Azure Stack Edge on Dell PowerEdge R840 with Intel Xeon Platinum 8260 processor os: Azure Stack Edge hardware: Dell PowerEdge R840 processor: Intel Xeon Platinum 8260	HMAC-SHA-1 MAC: 80-160 Increment 8 Key Length: 8-2048 Increment 8
Azure Stack Hub on Dell PowerEdge R6625 with AMD EPYC 9554 64-Core processor processor: AMD EPYC 9554 64-Core os: Azure Stack Hub hardware: Dell PowerEdge R6625	HMAC-SHA-1 MAC: 80-160 Increment 8 Key Length: 8-2048 Increment 8
Azure Stack Hub on Dell PowerEdge R760xp with Intel(R) Xeon(R) Platinum 8452Y 32-Core processor os: Azure Stack Hub hardware: Dell PowerEdge R760xp processor: Intel(R) Xeon(R) Platinum 8452Y 32-Core	HMAC-SHA-1 MAC: 80-160 Increment 8 Key Length: 8-2048 Increment 8
Azure Stack Hub on Voyager Klass Telecom with Intel Xeon D-1559 processor os: Azure Stack Hub processor: Intel Xeon D-1559 hardware: Voyager Klass Telecom	HMAC-SHA-1 MAC: 80-160 Increment 8 Key Length: 8-2048 Increment 8

17.1.2 Verdict

The assurance activity does not require any documentation information. Nevertheless, the evaluator has provided information about the HMAC algorithms supported by the OS.

Hence, the **PASS** verdict is assigned to the documentation review activity.

17.2 Test Activity

Based on the SFR instantiation included in the security target, the vendor has selected the following SHA algorithms:

1. HMAC-SHA-1
2. HMAC-SHA-256
3. HMAC-SHA-384
4. HMAC-SHA-512

In addition to the Common Criteria evaluation, the laboratory has also performed the CAVP validation for these and other algorithms. The general procedure that has been followed during the evaluation in order to demonstrate the correctness of the cryptographic functionality is as follows:

1. The laboratory has used the same test vectors used as part of the CAVP validation. For HMAC algorithms, the following types of test are performed:
    - Algorithm Functional Test (AFT). The main goal for these tests is verify the implementation of the MAC operation. The TOE processes all of HMAC by running

the randomly chosen key and message data through the HMAC algorithm and generating the corresponding HMAC tags.

2. The laboratory has exercised the cryptographic functionalities of the TOE by invoking the appropriate API in order to resolve the test vectors. The result of this step is a .json file which includes the associated response generated by the TOE per each test vector.
3. The laboratory has created a testing tool in order to exercise the BOTAN implementation for the target cryptographic algorithms. This tool receives the initial .json file with the test vectors as well as the .json file obtained as a result of the step 2. After parsing the information, the testing tool invokes the BOTAN implementation for the tested algorithm and resolve each test vector. After that, the testing tool compares both results (BOTAN vs TOE) in order to determine whether the cryptographic algorithms is properly implemented or not. The results of the testing tool is an individual outcome for each test vector (PASS or FAIL) and a overall outcome (PASS is all the test vectors passed or FAIL if any of them failed).
   - Note: Since HMAC-SHA-1 is not available in BOTAN, the laboratory has demonstrated the correctness of the cryptographic algorithm implementation by using CAVP as a reference implementation instead of BOTAN.

17.2.1 Test 1

17.2.1.1 Setup

The following environment is required to perform the test in addition to the TOE:

- A computer with:
  - Operating System: Ubuntu 20.04
  - Botan Tool is installed with CCN policy in evaluator machine;
  - Test vectors are located in evaluator machine.

For the installation of the *Botan Tool with CCN policy 2.15.2* all the steps defined in the *Botan-CCN_Manual_Implementador_v1* document have been followed.

17.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

17.2.1.3 Results

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

17.2.1.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the test activity demonstrate that the TOE provides a valid implementation for the evaluated cryptographic algorithms, since they have been compared against a well-known implementation (BOTAN) as a reference implementation.

For HMAC-SHA-1 algorithm, which is not available in BOTAN, the laboratory has followed the same approach but using the CAVP implementation as a reference instead of BOTAN. The evaluator has verified that the responses generated by the TOE are the same as the ones expected by the CAVP tool. Additionally, the associated CAVP certificates (listed in the tables included within the Documentation Review Activity section) have been granted demonstrating the correctness of the algorithm implementation.

Therefore, the **PASS** verdict is assigned to the test activity.

17.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to this FCS_COP.1.1(HMAC) requirement.

18 FCS_DTLS_EXT.1.1

The assurance activity for the **FCS_DTLS_EXT.1.1** requirement is stated as follows:

> **Test 1:** The evaluator will attempt to establish a connection with a DTLS server, observe the traffic with a packet analyzer, and verify that the connection succeeds and that the traffic is identified as DTLS.
>
> Other tests are performed in conjunction with the Assurance Activity listed for FCS_TLSC_EXT.1.

18.1 Documentation Review activity

18.1.1 Findings

Assurance activity does not state any documentation review activity for this requirement.

18.1.2 Verdict

Assurance activity does not state any documentation review activity for this requirement. Therefore, the **PASS** verdict is assigned to the documentation review activity.

18.2 Test Activity

To perform the TLS tests required by the Assurance Activities and check their correct outcome, different pieces of software were used:

1. Software acting as a DTLS server:

   a. *W10DtlsServerAutomator.ps1*, a Powershell script which automatically configures the DTLS server prior each test case execution (choosing between DTLS 1.0 or DTLS 1.2). This script allows the evaluator execute test cases using the software *WebServer.exe*

2. Software acting as a client from the TOE

   b. *W10ClientAutomator.ps1*, a Powershell script which automatically configures the TOE as a client prior each test case execution (choosing between DTLS 1.0 or DTLS 1.2 and setting the IP address of the DTLS server). This script allows the evaluator execute test cases using the software *WebClient.exe*.

Both *WebClient.exe* and *WebServer.exe* are written in C++ and use the native APIs from Windows to perform DTLS connections. The provided source code was examined to ensure that this claim is true. It could then be verified that the client tool follows the guidelines exposed in the "Creating a Secure Connection Using Schannel" document from MSDN.

Specifically, the key elements of a secure connection implementation using the system libraries were identified, and they are shown next. The fact that native functionality is being used is already hinted from the imported headers:

```
#include <tchar.h>
#include <stdio.h>
#include <stdlib.h>
#include <windows.h>
#include <winsock.h>
#include <wincrypt.h>
#include <wintrust.h>
#include <schannel.h>

#define SECURITY_WIN32
#include <security.h>
#include <sspi.h>
```

Especially interesting is the presence of *schannel* and *sspi*. The creation of a Schannel credential structure is also important, since it defines the protocol that will be used to establish the secure connection.

```
//
// Build Schannel credential structure. Currently, this sample only
// specifies the protocol to be used (and optionally the certificate,
// of course). Real applications may wish to specify other parameters
// as well.
//

ZeroMemory(&SchannelCred, sizeof(SchannelCred));

SchannelCred.dwVersion  = SCHANNEL_CRED_VERSION;
if(pCertContext)
{
    SchannelCred.cCreds     = 1;
    SchannelCred.paCred     = &pCertContext;
}

SchannelCred.grbitEnabledProtocols = dwProtocol;
```

This is later used to create an SSPI credentials handle, which is in turn used to initialize the security context with the corresponding method from the API:

```
// Create an SSPI credential.
//

Status = g_pSSPI->AcquireCredentialsHandleA(
                    NULL,                   // Name of principal
                    UNISP_NAME_A,           // Name of package
                    SECPKG_CRED_OUTBOUND,   // Flags indicating use
                    NULL,                   // Pointer to logon ID
                    &SchannelCred,          // Package specific data
                    NULL,                   // Pointer to GetKey() func
                    NULL,                   // Value to pass to GetKey()
                    phCreds,                // (out) Cred Handle
                    &tsExpiry);             // (out) Lifetime (optional)
if(Status != SEC_E_OK)
{
    printf("**** Error 0x%x returned by AcquireCredentialsHandle\n", Status);
    goto cleanup;
}
```

```
else
{
    scRet = g_pSSPI->InitializeSecurityContextA(
        phCreds,
        NULL,
        pszServerName,
        dwSSPIFlags,
        0,
        SECURITY_NATIVE_DREP,
        NULL,
        0,
        phContext,
        &OutBuffer,
        &dwSSPIOutFlags,
        &tsExpiry);
}

printf("SSPIFlags = %x\n", dwSSPIFlags);
printf("SSPIOutFlags = %x\n", dwSSPIOutFlags);

if(scRet != SEC_I_CONTINUE_NEEDED)
{
    printf("**** Error %d returned by InitializeSecurityContext (1)\n", scRet);
    return scRet;
}
```

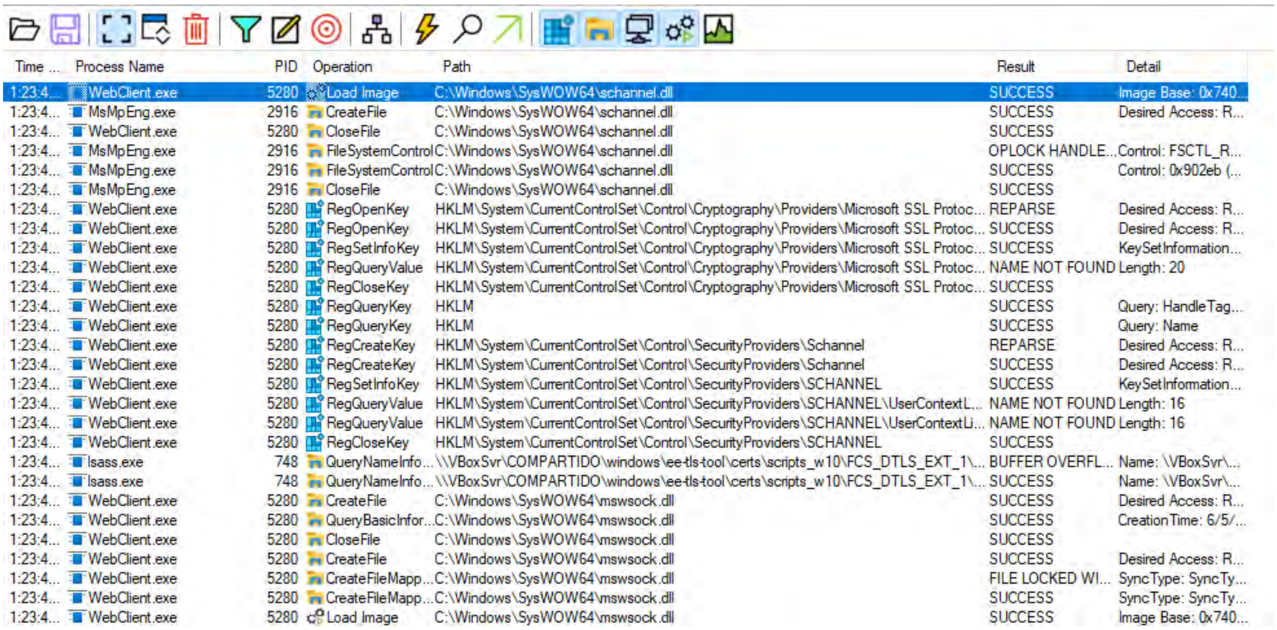
The other critical part of the DTLS connection procedure is the certificate validation performed by the client which, as it could also be observed, uses the native functionality from *wincrypt* provided by the *CertVerifyCertificateChainPolicy* method.

```
//
// Validate certificate chain.
//

ZeroMemory(&polHttps, sizeof(HTTPSPolicyCallbackData));
polHttps.cbStruct             = sizeof(HTTPSPolicyCallbackData);
polHttps.dwAuthType           = AUTHTYPE_SERVER;
polHttps.fdwChecks            = dwCertFlags;
polHttps.pwszServerName       = pwszServerName;

memset(&PolicyPara, 0, sizeof(PolicyPara));
PolicyPara.cbSize              = sizeof(PolicyPara);
PolicyPara.pvExtraPolicyPara = &polHttps;

memset(&PolicyStatus, 0, sizeof(PolicyStatus));
PolicyStatus.cbSize = sizeof(PolicyStatus);

if(!CertVerifyCertificateChainPolicy(
                        CERT_CHAIN_POLICY_SSL,
                        pChainContext,
                        &PolicyPara,
                        &PolicyStatus))
{
    Status = GetLastError();
    printf("Error 0x%x returned by CertVerifyCertificateChainPolicy!\n", Status);
    goto cleanup;
}
```

If an error is obtained in this step, the client aborts the connection (which in this case, since DTLS uses the UDP protocol, means that it just stops all communication with the server).

```
// Attempt to validate server certificate.
Status = VerifyServerCertificate(pRemoteCertContext,
                                 pszServerName,
                                 0);
if(Status)
{
    // The server certificate did not validate correctly. At this
    // point, we cannot tell if we are connecting to the correct
    // server, or if we are connecting to a "man in the middle"
    // attack server.

    // It is therefore best if we abort the connection.

    printf("**** Error authenticating HTTPS server credentials!\n", Status);
    printf("Terminating connection with server.\n");

    if (!fContinueAfterError)
    {
        goto cleanup;
    }
}
```

The Process Monitor tool was additionally used to check that the system libraries in charge of performing secure communications (e.g. *schannel.dll*) were loaded by *WebClient.exe* before performing network connections, effectively using the mechanism from the operating system.



Time ...	Process Name	PID	Operation	Path	Result	Detail
1:23:4...	WebClient.exe	5280	Load Image	C:\Windows\SysWOW64\schannel.dll	SUCCESS	Image Base: 0x740...
1:23:4...	MsMpEng.exe	2916	CreateFile	C:\Windows\SysWOW64\schannel.dll	SUCCESS	Desired Access: R...
1:23:4...	WebClient.exe	5280	CloseFile	C:\Windows\SysWOW64\schannel.dll	SUCCESS	
1:23:4...	MsMpEng.exe	2916	FileSystemControl	C:\Windows\SysWOW64\schannel.dll	OPLOCK HANDLE...	Control: FSCTL_R...
1:23:4...	MsMpEng.exe	2916	FileSystemControl	C:\Windows\SysWOW64\schannel.dll	SUCCESS	Control: 0x902eb (...
1:23:4...	MsMpEng.exe	2916	CloseFile	C:\Windows\SysWOW64\schannel.dll	SUCCESS	
1:23:4...	WebClient.exe	5280	RegOpenKey	HKLM\System\CurrentControlSet\Control\Cryptography\Providers\Microsoft SSL Protoc...	REPARSE	Desired Access: R...
1:23:4...	WebClient.exe	5280	RegOpenKey	HKLM\System\CurrentControlSet\Control\Cryptography\Providers\Microsoft SSL Protoc...	SUCCESS	Desired Access: R...
1:23:4...	WebClient.exe	5280	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Cryptography\Providers\Microsoft SSL Protoc...	SUCCESS	KeySetInformation...
1:23:4...	WebClient.exe	5280	RegQueryValue	HKLM\System\CurrentControlSet\Control\Cryptography\Providers\Microsoft SSL Protoc...	NAME NOT FOUND	Length: 20
1:23:4...	WebClient.exe	5280	RegCloseKey	HKLM\System\CurrentControlSet\Control\Cryptography\Providers\Microsoft SSL Protoc...	SUCCESS	
1:23:4...	WebClient.exe	5280	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
1:23:4...	WebClient.exe	5280	RegQueryKey	HKLM	SUCCESS	Query: Name
1:23:4...	WebClient.exe	5280	RegCreateKey	HKLM\System\CurrentControlSet\Control\SecurityProviders\Schannel	REPARSE	Desired Access: R...
1:23:4...	WebClient.exe	5280	RegCreateKey	HKLM\System\CurrentControlSet\Control\SecurityProviders\Schannel	SUCCESS	Desired Access: R...
1:23:4...	WebClient.exe	5280	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL	SUCCESS	KeySetInformation...
1:23:4...	WebClient.exe	5280	RegQueryValue	HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\UserContextL...	NAME NOT FOUND	Length: 16
1:23:4...	WebClient.exe	5280	RegQueryValue	HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\UserContextLi...	NAME NOT FOUND	Length: 16
1:23:4...	WebClient.exe	5280	RegCloseKey	HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL	SUCCESS	
1:23:4...	lsass.exe	748	QueryNameInfo...	\\VBoxSvr\COMPARTIDO\windows\ee-tls-tool\certs\scripts_w10\FCS_DTLS_EXT_1\...	BUFFER OVERFL...	Name: \VBoxSvr\...
1:23:4...	lsass.exe	748	QueryNameInfo...	\\VBoxSvr\COMPARTIDO\windows\ee-tls-tool\certs\scripts_w10\FCS_DTLS_EXT_1\...	SUCCESS	Name: \VBoxSvr\...
1:23:4...	WebClient.exe	5280	CreateFile	C:\Windows\SysWOW64\mswsock.dll	SUCCESS	Desired Access: R...
1:23:4...	WebClient.exe	5280	QueryBasicInfor...	C:\Windows\SysWOW64\mswsock.dll	SUCCESS	CreationTime: 6/5/...
1:23:4...	WebClient.exe	5280	CloseFile	C:\Windows\SysWOW64\mswsock.dll	SUCCESS	
1:23:4...	WebClient.exe	5280	CreateFile	C:\Windows\SysWOW64\mswsock.dll	SUCCESS	Desired Access: R...
1:23:4...	WebClient.exe	5280	CreateFileMapp...	C:\Windows\SysWOW64\mswsock.dll	FILE LOCKED WI...	SyncType: SyncTy...
1:23:4...	WebClient.exe	5280	CreateFileMapp...	C:\Windows\SysWOW64\mswsock.dll	SUCCESS	SyncType: SyncTy...
1:23:4...	WebClient.exe	5280	Load Image	C:\Windows\SysWOW64\mswsock.dll	SUCCESS	Image Base: 0x740...

Regarding the specific tests performed, some of them require modification of outgoing server messages in the DTLS connection. Unless otherwise noted, the test cases included in *WebServer.exe* were leveraged to perform those tests without the need of a MITM tool.

18.2.1 Test 1

In this test the evaluator will establish a connection to a DTLS Server and check that the connection succeeds and is identified as DTLS.

18.2.1.1 Setup

The following certificates shall be used to perform the assurance activities listed on the Protection Profile:

- CN = EE Test Root CA
- CN = test.epoche.es

The certificates listed form a valid certification path. The server certificate is available in pfx format and the root certificate is available in pem format.

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Server Machine (Windows Server Standard Edition)
- Client Machine (Platforms listed in the ST)

Both machines are in the same network with the following configuration:

- Server Machine, IP = 50.50.50.277
- Client Machine, IP = 50.50.50.155

Server machine shall contain the PowerShell script *W10DtlsServerAutomator.ps1* as well as the *WebServer.exe* tool also mentioned before.

Client machine shall contain the PowerShell script *W10ClientAutomator.ps1* and the *WebClient.exe* tool mentioned in the introduction to this section.

Moreover, the client machine shall have the secure configuration enabled, according to the section **3.2 Operational prerequisites** of the ***Operational Guidance*** document. The *Wireshark* network analyzer shall be installed on the client machine.

The approach to this test is going to be divided in two parts: - First part: test related to dtls 1.0 - Second part: test related to dtls 1.2

The first part of this test is not applicable to Windows 11 platforms due to dlts 1.0 not being supported on those platforms

18.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

18.2.1.3 Results

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

18.2.1.4 Verdict

From the results of the previous test, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

18.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FCS_DTLS_EXT.1.1.

19 FCS_DTLS_EXT.1.2

The assurance activity for the **FCS_DTLS_EXT.1.2** requirement is stated as follows:

> The evaluator will perform the assurance activities listed for FCS_TLSC_EXT.1.

19.1 Documentation Review activity

19.1.1 Findings

Assurance activity does not state any documentation review activity for this requirement.

19.1.2 Verdict

Assurance activity does not state any documentation review activity for this requirement. Therefore, the **PASS** verdict is assigned to the documentation review activity.

19.2 Test Activity

To perform the TLS tests required by the Assurance Activities and check their correct outcome, different pieces of software were used:

1. Software acting as a DTLS server:

   a. *W10DtlsServerAutomator.ps1*, a Powershell script which automatically configures the DTLS server prior each test case execution (choosing between DTLS 1.0 or DTLS 1.2). This script allows the evaluator execute test cases using the software *WebServer.exe*

2. Software acting as a client from the TOE

   b. *W10ClientAutomator.ps1*, a Powershell script which automatically configures the TOE as a client prior each test case execution (choosing between DTLS 1.0 or DTLS 1.2 and setting the IP address of the DTLS server). This script allows the evaluator execute test cases using the software *WebClient.exe*.

The documentation for FCS_DTLS_EXT.1.1 includes information about their suitability for this evaluation.

19.2.1 Test 1 - FCS_TLSC_EXT.1.1 for DTLS

19.2.1.1 Setup

The following certificates shall be used to perform the assurance activities listed on the Protection Profile:

- CN = EE Test Root CA
- CN = test.epoche.es

The listed certificates form a valid certification path. The server certificate is available in pfx format and the root certificate is available in pem format.

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Server Machine (Windows Server Standard Edition)
- Client Machine (Platforms listed in the ST)

Both machines are in the same network with the following configuration:

- Server Machine, IP = 50.50.50.227
- Client Machine, IP = 50.50.50.155

Server machine shall contain the PowerShell script *W10DtlsServerAutomator.ps1* as well as the *WebServer.exe* tool also mentioned before.

Client machine shall contain the PowerShell script *W10ClientAutomator.ps1* and the *WebClient.exe* tool mentioned in the introduction to this section.

Moreover, the client machine shall have the secure configuration enabled, according to the section **3.2 Operational prerequisites** of the ***Operational Guidance*** document. The *Wireshark* network analyzer shall be installed on the client machine.

The approach to this test is going to be divided in two parts: - First part: test related to dtls 1.0 - Second part: test related to dtls 1.2

The first part of this test is not applicable to Windows 11 platforms due to dlts 1.0 not being supported on those platforms

19.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

19.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

19.2.1.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 1** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 1** activity.

19.2.2 Test 2 - FCS_TLSC_EXT.1.1 for DTLS

19.2.2.1 Setup

The setup is identical to the one defined for Test 1.

19.2.2.2 Procedure

The procedure is identical to the one defined for Test 1.

19.2.2.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

19.2.2.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 2** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 2** activity.

19.2.3 Test 3 - FCS_TLSC_EXT.1.1 for DTLS

19.2.3.1 Setup

The setup is identical to the one defined for Test 1.

19.2.3.2 Procedure

The procedure is identical to the one defined for Test 1.

19.2.3.3 Results

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

19.2.3.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 3** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 3** activity.

19.2.4 Test 4 - FCS_TLSC_EXT.1.1 for DTLS

19.2.4.1 Setup

The setup is identical to the one defined for Test 1.

19.2.4.2 Procedure

The procedure is identical to the one defined for Test 1.

19.2.4.3 Results

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

19.2.4.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 4** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 4** activity.

19.2.5 Test 5.1 - FCS_TLSC_EXT.1.1 for DTLS

19.2.5.1 Setup

The setup is identical to the one defined for Test 1.

19.2.5.2 Procedure

The procedure is identical to the one defined for Test 1.

19.2.5.3 Results

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

19.2.5.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 5.1** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 5.1** activity.

19.2.6 Test 5.2 - FCS_TLSC_EXT.1.1 for DTLS

19.2.6.1 Setup

The setup is identical to the one defined for Test 1, although the IPs for this test are 10.10.10.30 for the client machine and 20.20.20.40 for the server machine.

19.2.6.2 Procedure

The procedure is identical to the one defined for Test 1.

19.2.6.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

19.2.6.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 5.2** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 5.2** activity.

19.2.7 Test 5.3 - FCS_TLSC_EXT.1.1 for DTLS

19.2.7.1 Setup

The setup is identical to the one defined for Test 1.

19.2.7.2 Procedure

The procedure is identical to the one defined for Test 1.

19.2.7.3 Results

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

19.2.7.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 5.3** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 5.3** activity.

19.2.8 Test 5.4 - FCS_TLSC_EXT.1.1 for DTLS

19.2.8.1 Setup

The setup is identical to the one defined for Test 1.

19.2.8.2 Procedure

The procedure is identical to the one defined for Test 1.

19.2.8.3 Results

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

19.2.8.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 5.4** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 5.4** activity.

19.2.9 Test 5.5 - FCS_TLSC_EXT.1.1 for DTLS

19.2.9.1 Setup

The setup is identical to the one defined for Test 1, but the IP addresses are 10.10.10.30 for the client and 10.10.10.40 for the server.

19.2.9.2 Procedure

The procedure is identical to the one defined for Test 1.

19.2.9.3 Results

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

19.2.9.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 5.5** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 5.5** activity.

19.2.10 Test 5.6 - FCS_TLSC_EXT.1.1 for DTLS

19.2.10.1 Setup

The setup is identical to the one defined for Test 1, but the IP addresses are 10.10.10.30 for the client and 10.10.10.40 for the server.

19.2.10.2 Procedure

The procedure is identical to the one defined for Test 1.

19.2.10.3 Results

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

19.2.10.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 5.6** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 5.6** activity.

19.2.11 Test 1 - FCS_TLSC_EXT.1.2 for DTLS

19.2.11.1 Setup

The following certificates, created automatically by *ee-tls-tool* and installed by *W10Client Automator.ps1*, shall be used to perform the assurance activities listed on the Protection Profile:

- CN = EE Test Root CA
- CN = invalid.epoche.es

The listed certificates form a valid certification path. The server certificate is available in pfx format and the root certificate is available in pem format.

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Server Machine (Windows Server Standard Edition)
- Client Machine (Platforms listed in the ST)

Both machines are in the same network with the following configuration:

- Server Machine, IP = 50.50.50.227
- Client Machine, IP = 50.50.50.155

Server machine shall contain the PowerShell script *W10DtlsServerAutomator.ps1* as well as the *WebServer.exe* tool also mentioned before.

Client machine shall contain the PowerShell script *W10ClientAutomator.ps1* and the *WebClient.exe* tool mentioned in the introduction to this section.

Moreover, the client machine shall have the secure configuration enabled, according to the section **3.2 Operational prerequisites** of the ***Operational Guidance***. The *Wireshark* network analyzer shall be installed on the client machine.

19.2.11.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

19.2.11.3 Results

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

19.2.11.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 1** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 1** activity.

19.2.12 Test 2 - FCS_TLSC_EXT.1.2 for DTLS

19.2.12.1 Setup

The setup is identical to the one defined for Test 1 (IPs configuration and installed tools). The certificate used for the connection is different than the one used for Test 1:

- CN = EE Test Root CA
- CN = test.epoche.es

19.2.12.2 Procedure

The procedure is identical to the one defined for Test 1.

19.2.12.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

19.2.12.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 2** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 2** activity.

19.2.13 Test 3 - FCS_TLSC_EXT.1.2 for DTLS

19.2.13.1 Setup

The setup is identical to the one defined for Test 2.

19.2.13.2 Procedure

The procedure is identical to the one defined for Test 2.

19.2.13.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

19.2.13.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 3** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 3** activity.

19.2.14 Test 4 - FCS_TLSC_EXT.1.2 for DTLS

19.2.14.1 Setup

The setup is identical to the one defined for Test 1.

19.2.14.2 Procedure

The procedure is identical to the one defined for Test 1.

19.2.14.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

19.2.14.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 4** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 4** activity.

19.2.15 Test 5.1 - FCS_TLSC_EXT.1.2 for DTLS

19.2.15.1 Setup

The setup is identical to the one defined for Test 1 (IPs configuration and installed tools). The certificate used for the connection is different than the one used for Test 1:

- CN = EE Test Root CA
- CN = foo.*.test.epoche.es

19.2.15.2 Procedure

The procedure is identical to the one defined for Test 1.

19.2.15.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

19.2.15.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 5.1** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 5.1** activity.

19.2.16 Test 5.2 - FCS_TLSC_EXT.1.2 for DTLS

19.2.16.1 Setup

The setup is identical to the one defined for Test 2.

19.2.16.2 Procedure

The procedure is identical to the one defined for Test 2.

19.2.16.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

19.2.16.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 5.2** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 5.2** activity.

19.2.17 Test 5.3 - FCS_TLSC_EXT.1.2 for DTLS

19.2.17.1 Setup

The setup is identical to the one defined for Test 2.

19.2.17.2 Procedure

The procedure is identical to the one defined for Test 2.

19.2.17.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

19.2.17.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 5.3** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 5.3** activity.

19.2.18 Test 1 - FCS_TLSC_EXT.1.3 for DTLS

19.2.18.1 Setup

The following certificates, created automatically by *ee-tls-tool* and installed by *W10Client Automator.ps1*, shall be used to perform the assurance activities listed on the Protection Profile:

- CN = EE Test Root CA
- CN = EE Test Intermediate CA 1
- CN = EE Test Intermediate CA 2
- CN = test.epoche.es

The listed certificates form a valid certification path. All certificates are available in pem format.

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Server Machine (Windows Server Standard Edition)
- Client Machine (Platforms listed in the ST)

The three machines are in the same network with the following configuration:

- Server Machine (Windows), IP = 50.50.50.227
- Client Machine, IP = 50.50.50.155

Windows Server machine shall contain the PowerShell script *W10DtlsServerAutomator.ps1* as well as the *WebServer.exe* tool also mentioned before.

Debian server shall have Python installed and the folder *ca* generated by *ee-tls-tool*.

Client machine shall contain the PowerShell script *W10ClientAutomator.ps1* and the *WebClient.exe* tool mentioned in the introduction to this section.

Moreover, the client machine shall have the secure configuration enabled, according to the section **3.2 Operational prerequisites** of the ***Operational Guidance***. The *Wireshark* network analyzer shall be installed on the client machine.

19.2.18.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

19.2.18.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

19.2.18.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 1** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 1** activity.

19.2.19 Test 2 - FCS_TLSC_EXT.1.3 for DTLS

19.2.19.1 Setup

The setup is identical to the one defined for Test 1 (IPs configuration and installed tools). The certificates used for the connection are different than the ones used for Test 1:For the next part, t

- CN = EE Test Root CA
- CN = EE Test Intermediate CA 1
- CN = EE Test Intermediate CA 2
- CN = test.epoche.es (revoked)

The listed certificates form a valid certification path. All certificates are available in pem format as well as pfx.

19.2.19.2 Procedure

The procedure is identical to the one defined for Test 1.

19.2.19.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

19.2.19.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 2** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 2** activity.

19.2.20 Test 3 - FCS_TLSC_EXT.1.3 for DTLS

19.2.20.1 Setup

The setup is identical to the one defined for Test 1 (IPs configuration and installed tools). The certificates used for the connection are different than the ones used for Test 1:

- CN = EE Test Root CA
- CN = EE Test Intermediate CA 1
- CN = EE Test Intermediate CA 2
- CN = test.epoche.es (expired certificate)

The listed certificates form a valid certification path. All certificates are available in pem format as well as pfx.

19.2.20.2 Procedure

The procedure is identical to the one defined for Test 1.

19.2.20.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

19.2.20.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 3** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 3** activity.

19.2.21 Test 4 - FCS_TLSC_EXT.1.3 for DTLS

19.2.21.1 Setup

The setup is identical to the one defined for Test 1 (IPs configuration and installed tools). The certificates used for the connection are different than the ones used for Test 1:

- CN = EE Test Root CA
- CN = test.epoche.es

The listed certificates form a valid certification path. The root certificate is available in pem format.

19.2.21.2 Procedure

The procedure is identical to the one defined for Test 1.

19.2.21.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

19.2.21.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 4** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 4** activity.

19.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to this FCS_DTLS_EXT.1.2.

20 FCS_RBG_EXT.1.1

The assurance activity for the **FCS_RBG_EXT.1.1** requirement is stated as follows:

> The evaluator will perform the following tests:
>
> The evaluator will perform 15 trials for the RNG implementation. If the RNG is configurable, the evaluator will perform 15 trials for each configuration. The evaluator will also confirm that the operational guidance contains appropriate instructions for configuring the RNG functionality.
>
> If the RNG has prediction resistance enabled, each trial consists of (1) instantiate DRBG, (2) generate the first block of random bits (3) generate a second block of random bits (4) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator will generate eight input values for each trial. The first is a count (0 - 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The next two are additional input and entropy input for the first call to generate. The final two are additional input and entropy input for the second call to generate. These values are randomly generated. "generate one block of random bits" means to generate random bits with number of returned bits equal to the Output Block Length (as defined in NIST SP 800-90A).
>
> If the RNG does not have prediction resistance, each trial consists of (1) instantiate DRBG, (2) generate the first block of random bits (3) reseed, (4) generate a second block of random bits (5) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator will generate eight input values for each trial. The first is a count (0 - 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The fifth value is additional input to the first call to generate. The sixth and seventh are additional input and entropy input to the call to reseed. The final value is additional input to the second generate call.
>
> The following list contains more information on some of the input values to be generated/selected by the evaluator.
>
> - **Entropy input:** The length of the entropy input value must equal the seed length.
> - **Nonce:** If a nonce is supported (CTR_DRBG with no Derivation Function does not use a nonce), the nonce bit length is one-half the seed length.
> - **Personalization string:** The length of the personalization string must be less than or equal to seed length. If the implementation only supports one personalization string length, then the same length can be used for both values. If more than one string length is support, the evaluator will use personalization strings of two different lengths. If the implementation does not use a personalization string, no value needs to be supplied.

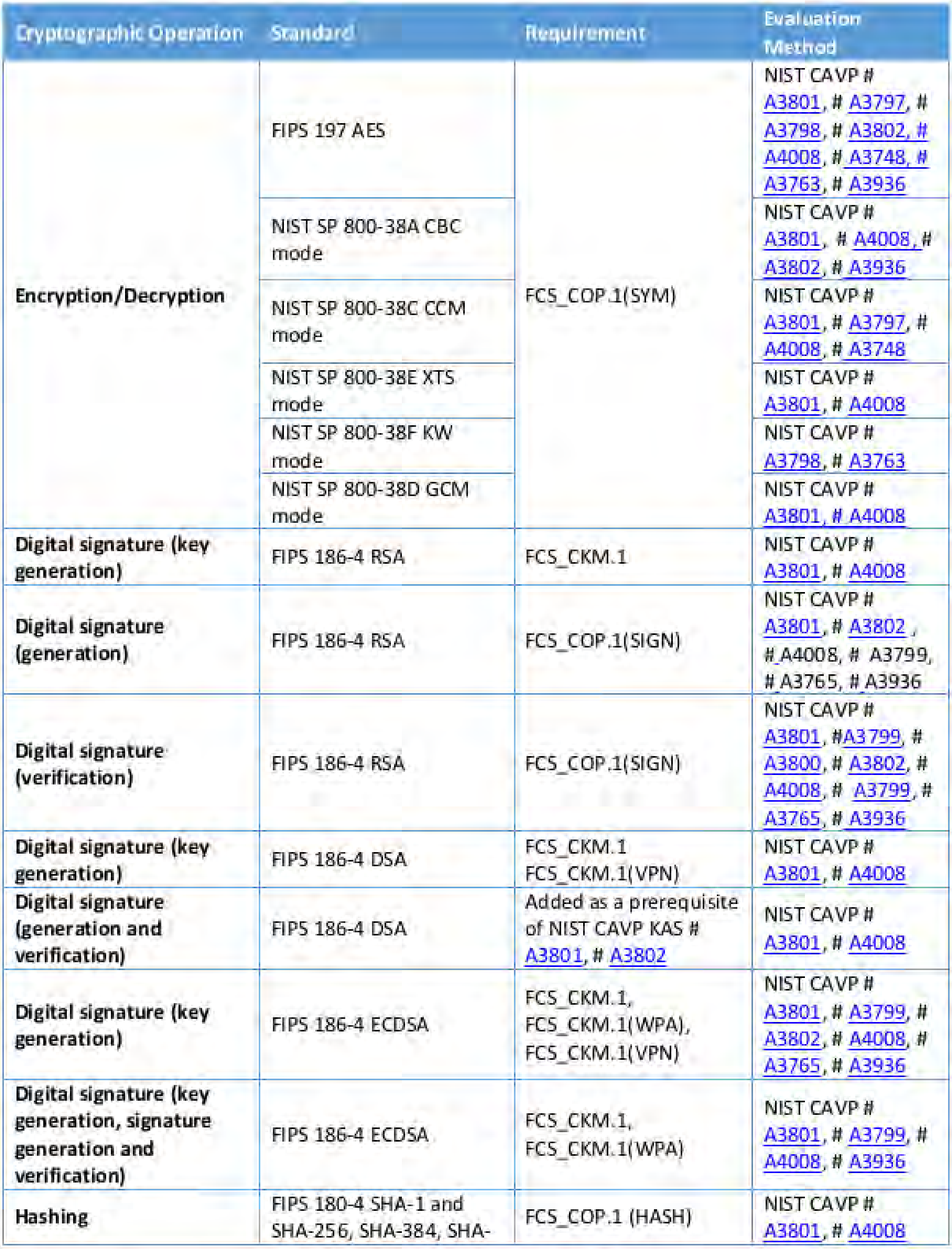
- **Additional input:** The additional input bit lengths have the same defaults and restrictions as the personalization string lengths.

20.1 Documentation Review Activity

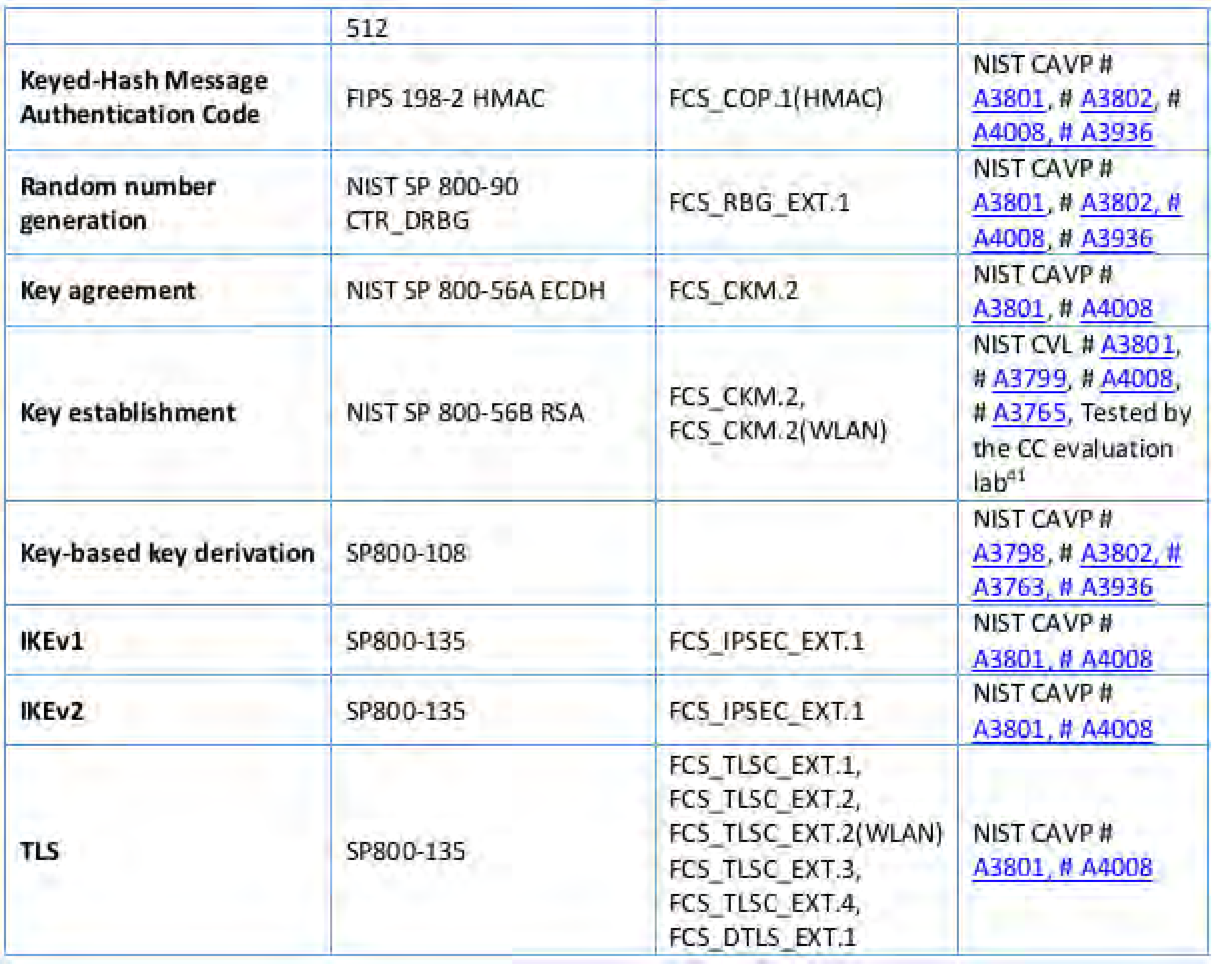
20.1.1 Findings

The evaluator has reviewed the ***Security Target*** document and the information provided in the TSS, section **6.2.2 Cryptographic Algorithm Validation**. This section includes the following tables of the cryptographic algorithms supported by Windows 11, Windows 10, Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge.

20.1.1.1 Cryptographic Algorithm Standards and Evaluation Methods for Windows 11 (version 22H2)

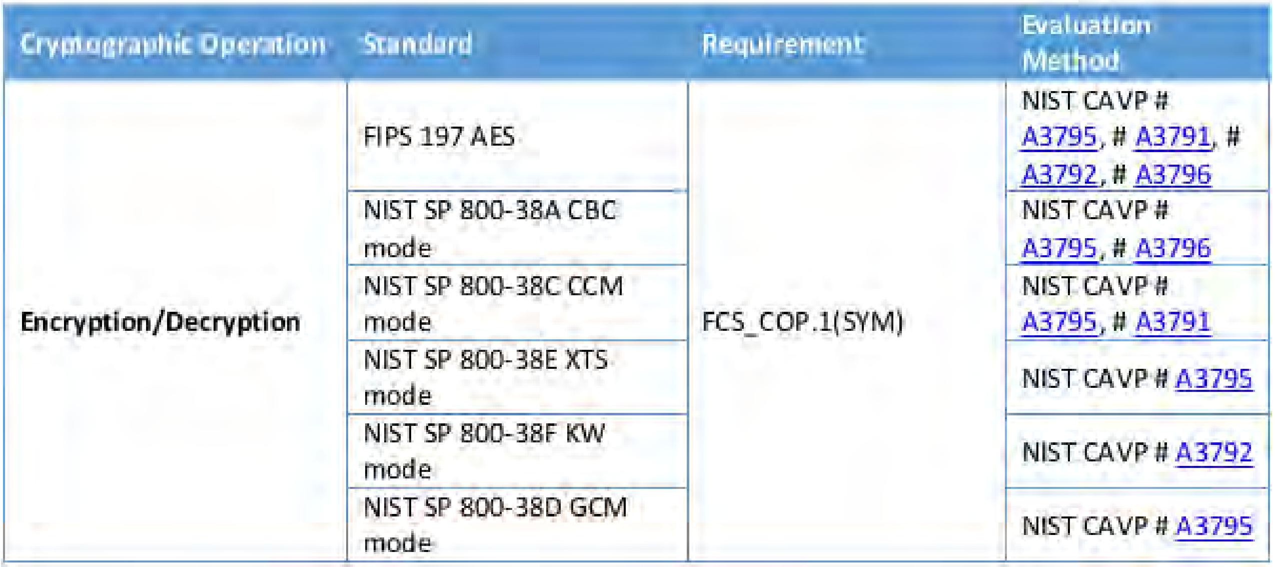


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3801, # A3797, # A3798, # A3802, # A4008, # A3748, # A3763, # A3936
	NIST SP 800-38A CBC mode		NIST CAVP # A3801, # A4008, # A3802, # A3936
	NIST SP 800-38C CCM mode		NIST CAVP # A3801, # A3797, # A4008, # A3748
	NIST SP 800-38E XTS mode		NIST CAVP # A3801, # A4008
	NIST SP 800-38F KW mode		NIST CAVP # A3798, # A3763
	NIST SP 800-38D GCM mode		NIST CAVP # A3801, # A4008
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP # A3801, # A4008
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3801, # A3802 , # A4008, # A3799, # A3765, # A3936
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3801, #A3799, # A3800, # A3802, # A4008, # A3799, # A3765, # A3936
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3801, # A4008
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3801, # A3802	NIST CAVP # A3801, # A4008
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3801, # A3799, # A3802, # A4008, # A3765, # A3936
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3801, # A3799, # A4008, # A3936
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-	FCS_COP.1 (HASH)	NIST CAVP # A3801, # A4008

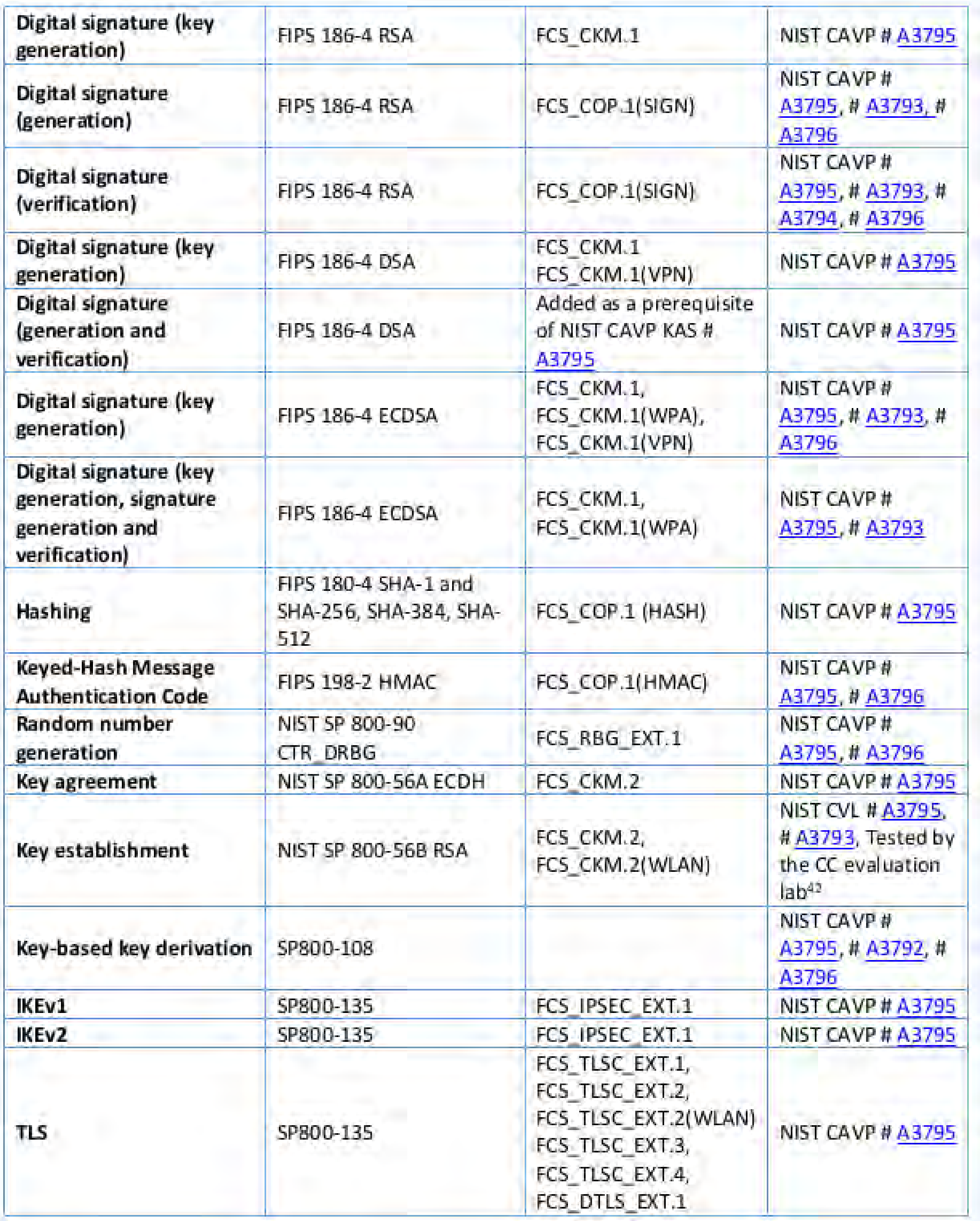


	512		
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3801, # A3802, # A4008, # A3936
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3801, # A3802, # A4008, # A3936
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3801, # A4008
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2, FCS_CKM.2(WLAN)	NIST CVL # A3801, # A3799, # A4008, # A3765, Tested by the CC evaluation lab[41]
Key-based key derivation	SP800-108		NIST CAVP # A3798, # A3802, # A3763, # A3936
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3801, # A4008
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3801, # A4008
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3801, # A4008

20.1.1.2 Cryptographic Algorithm Standards and Evaluation Methods for Windows 10 (version 22H2)

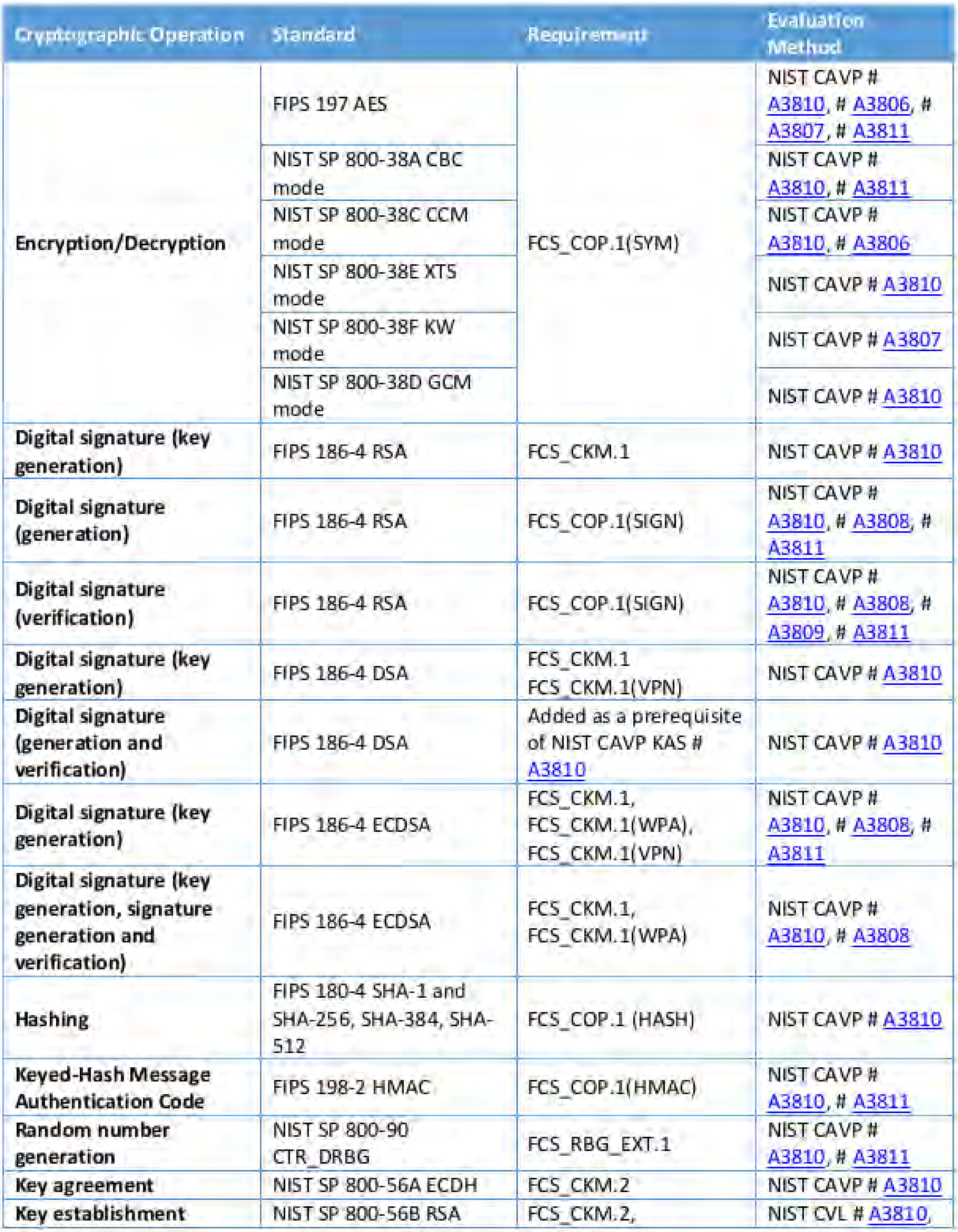


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3795, # A3791, # A3792, # A3796
	NIST SP 800-38A CBC mode		NIST CAVP # A3795, # A3796
	NIST SP 800-38C CCM mode		NIST CAVP # A3795, # A3791
	NIST SP 800-38E XTS mode		NIST CAVP # A3795
	NIST SP 800-38F KW mode		NIST CAVP # A3792
	NIST SP 800-38D GCM mode		NIST CAVP # A3795



Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP # A3795
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3795, # A3793, # A3796
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3795, # A3793, # A3794, # A3796
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3795
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3795	NIST CAVP # A3795
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3795, # A3793, # A3796
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3795, # A3793
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3795
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3795, # A3796
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3795, # A3796
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3795
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2, FCS_CKM.2(WLAN)	NIST CVL # A3795, # A3793, Tested by the CC evaluation lab[42]
Key-based key derivation	SP800-108		NIST CAVP # A3795, # A3792, # A3796
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3795
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3795
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3795

20.1.1.3 Cryptographic Algorithm Standards and Evaluation Methods for Windows Server 2022 and Windows Server Datacenter: Azure Edition

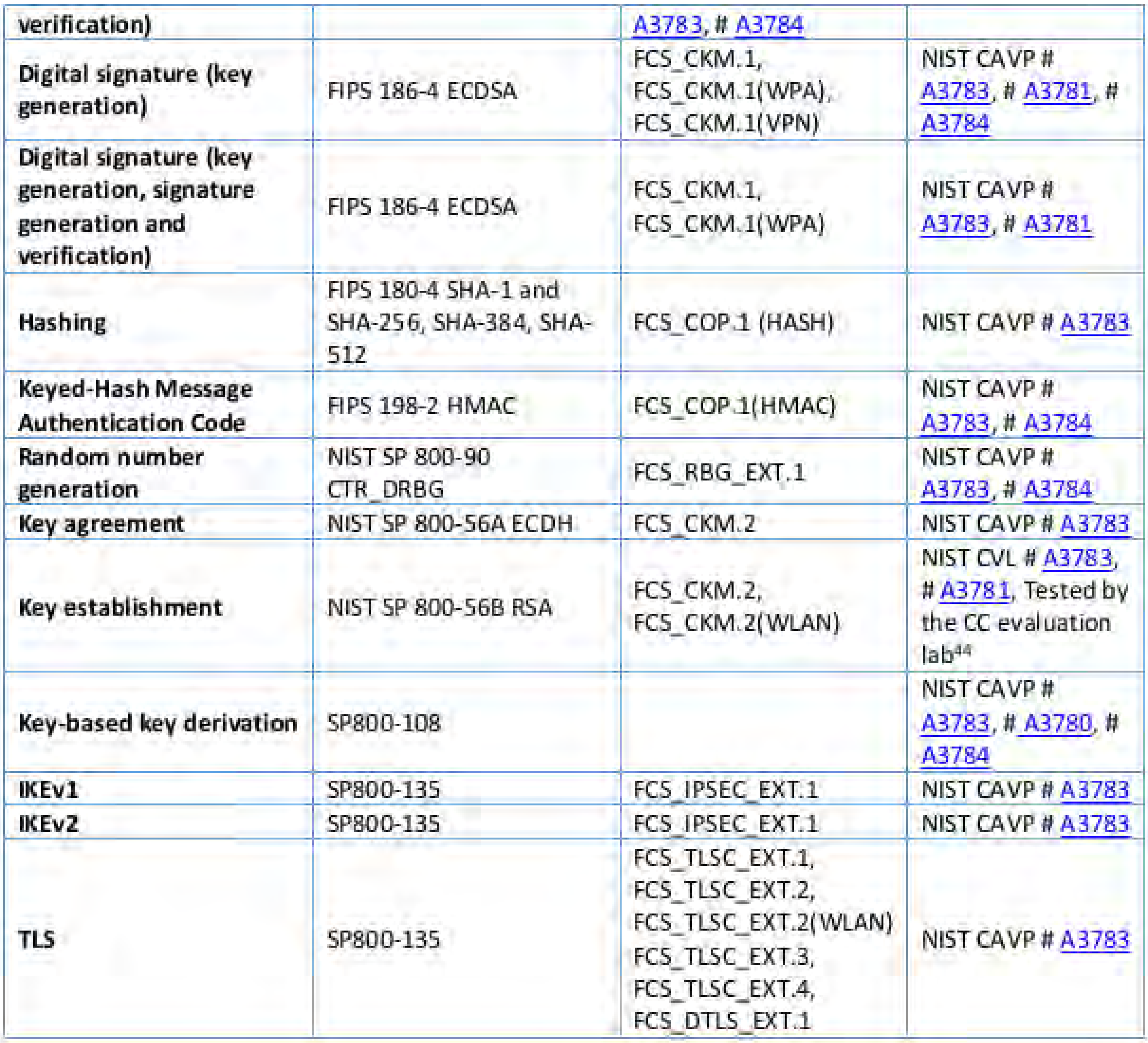


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3810, # A3806, # A3807, # A3811
	NIST SP 800-38A CBC mode		NIST CAVP # A3810, # A3811
	NIST SP 800-38C CCM mode		NIST CAVP # A3810, # A3806
	NIST SP 800-38E XTS mode		NIST CAVP # A3810
	NIST SP 800-38F KW mode		NIST CAVP # A3807
	NIST SP 800-38D GCM mode		NIST CAVP # A3810
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP # A3810
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3810, # A3808, # A3811
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3810, # A3808, # A3809, # A3811
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3810
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3810	NIST CAVP # A3810
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3810, # A3808, # A3811
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3810, # A3808
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3810
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3810, # A3811
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3810, # A3811
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3810
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2,	NIST CVL # A3810,

		FCS_CKM.2(WLAN)	# A3808, Tested by the CC evaluation lab[43]
Key-based key derivation	SP800-108		NIST CAVP # A3810, # A3807, A3811
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3810
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3810
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3810

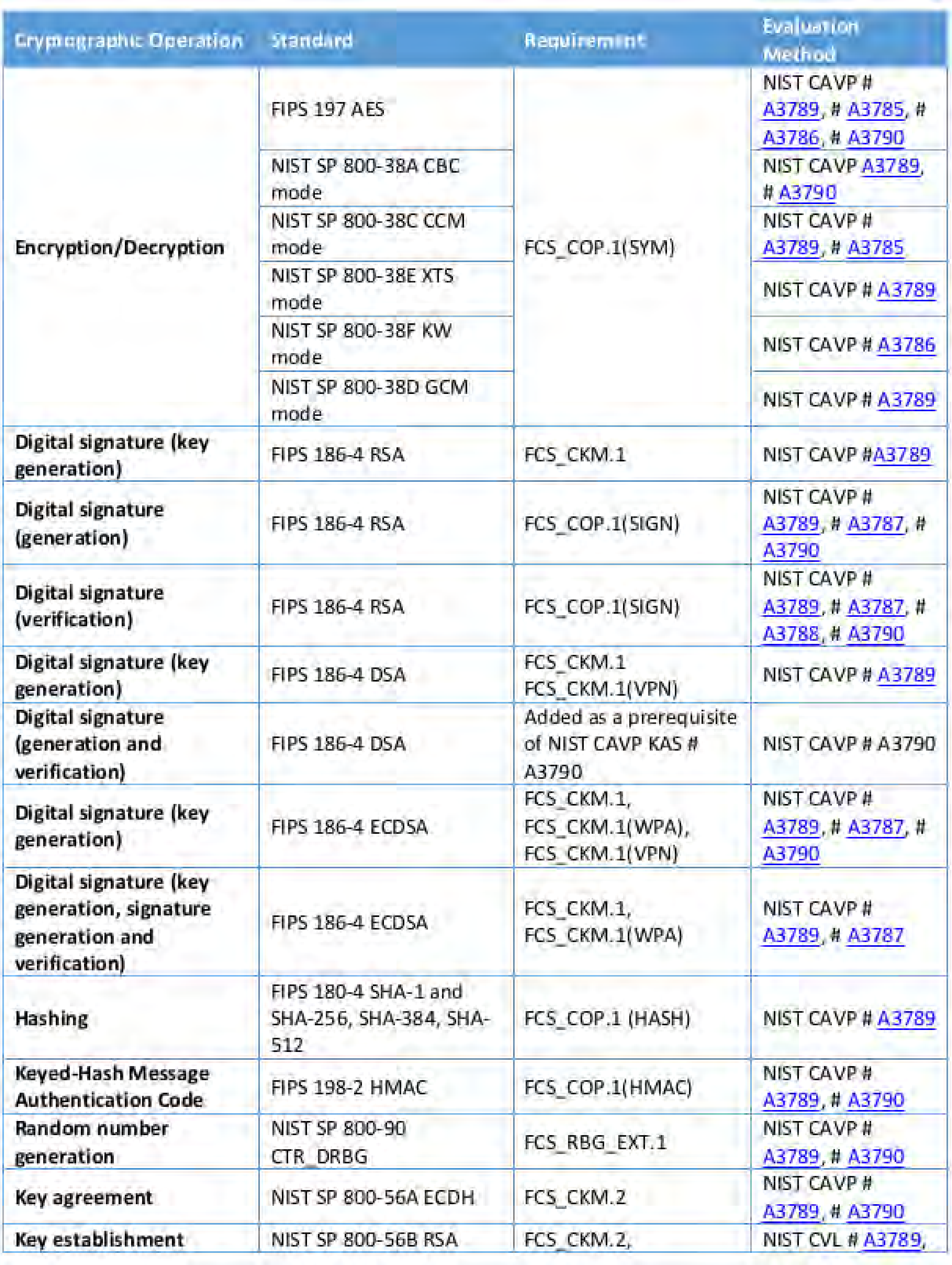
20.1.1.4 Cryptographic Algorithm Standards and Evaluation Methods for Windows Server Azure Stack HCIv2 version 22H2

Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3783, # A3779, # A3780, # A3784
	NIST SP 800-38A CBC mode		NIST CAVP A3783, # A3784
	NIST SP 800-38C CCM mode		NIST CAVP # A3783, # A3779
	NIST SP 800-38E XTS mode		NIST CAVP # A3783
	NIST SP 800-38F KW mode		NIST CAVP # A3780
	NIST SP 800-38D GCM mode		NIST CAVP # A3783
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP #A3783
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3783, # A3781, # A3784
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3783, # A3781, # A3782, # A3784
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3783
Digital signature (generation and	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS #	NIST CAVP # A3783

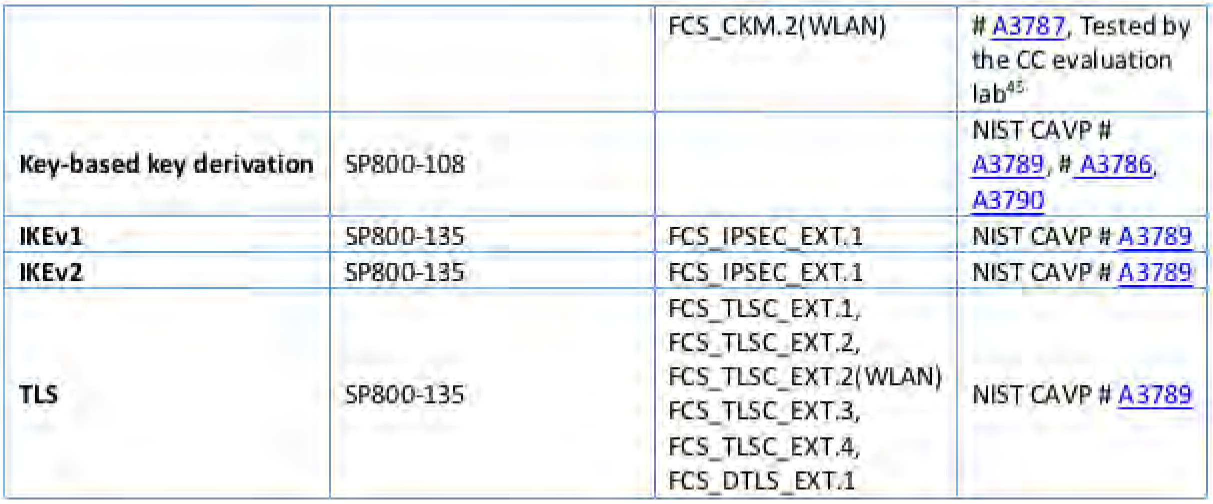


verification)		A3783, # A3784	
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3783, # A3781, # A3784
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3783, # A3781
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3783
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3783, # A3784
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3783, # A3784
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3783
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2, FCS_CKM.2(WLAN)	NIST CVL # A3783, # A3781, Tested by the CC evaluation lab[44]
Key-based key derivation	SP800-108		NIST CAVP # A3783, # A3780, # A3784
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3783
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3783
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3783

20.1.1.5 Cryptographic Algorithm Standards and Evaluation Methods for Azure Stack Hub and Azure Stack Edge



Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3789, # A3785, # A3786, # A3790
	NIST SP 800-38A CBC mode		NIST CAVP A3789, # A3790
	NIST SP 800-38C CCM mode		NIST CAVP # A3789, # A3785
	NIST SP 800-38E XTS mode		NIST CAVP # A3789
	NIST SP 800-38F KW mode		NIST CAVP # A3786
	NIST SP 800-38D GCM mode		NIST CAVP # A3789
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP #A3789
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3789, # A3787, # A3790
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3789, # A3787, # A3788, # A3790
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3789
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3790	NIST CAVP # A3790
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3789, # A3787, # A3790
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3789, # A3787
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3789
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3789, # A3790
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3789, # A3790
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3789, # A3790
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2,	NIST CVL # A3789,



		FCS_CKM.2(WLAN)	# A3787, Tested by the CC evaluation lab[45]
Key-based key derivation	SP800-108		NIST CAVP # A3789, # A3786, A3790
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3789
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3789
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3789

The ***Operational Guidance*** document, states that for the evaluated version the following security policy needs to be applied (Section 3.2.5):

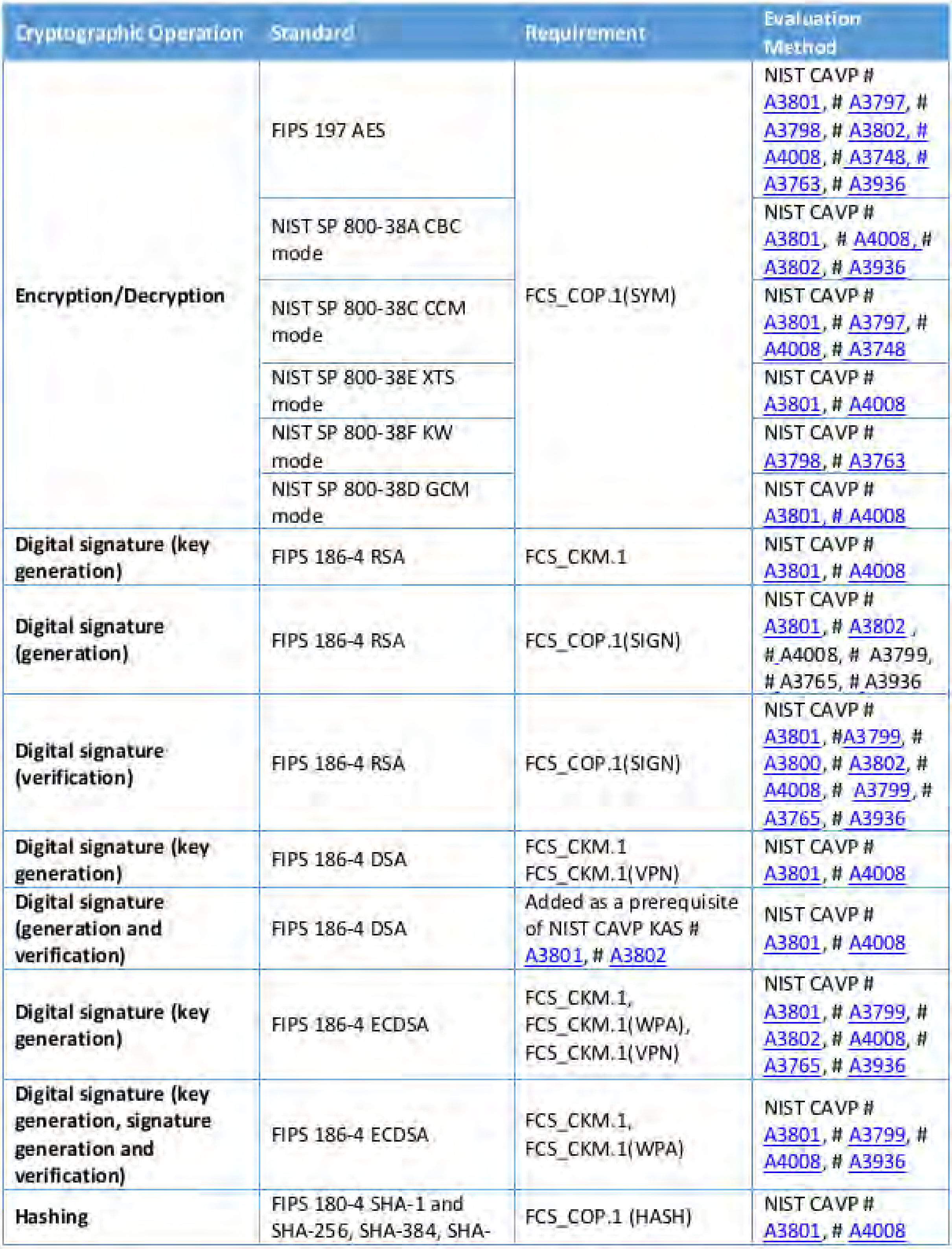
- Local Policies \ Security Options\System cryptography: Use FIPS 140 compliant cryptographic algorithms, including encryption, hashing and signing algorithm

After applying this policy, only FIPS certified algorithm can be used, including random number generation algorithms defined in the above table. The vendor has also included the following wording:

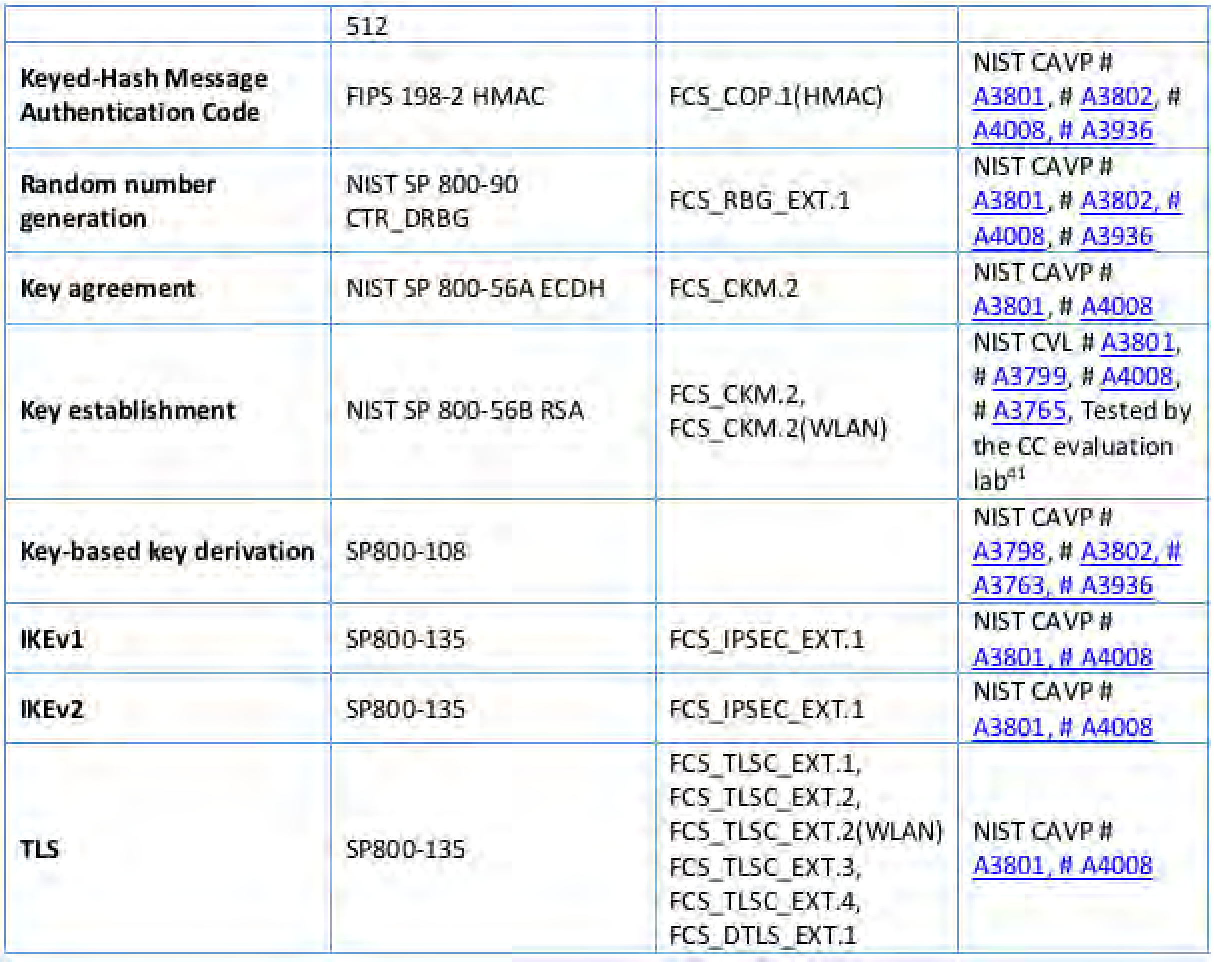
> Windows 10 automatically generate random bits according to SP-800-90A, no configuration is necessary.

As part of the testing activity described below, the correctness of the cryptographic functionality has been demonstrated against the BOTAN tool. However, CTR-DRBG is not available in BOTAN, and the laboratory has verified the implementation against the CAVP tool. Below, the CAVP certificates granted for this functionality are listed (extracted from the tables above)

20.1.1.6 Cryptographic Algorithm Standards and Evaluation Methods for Windows 11 (version 22H2)

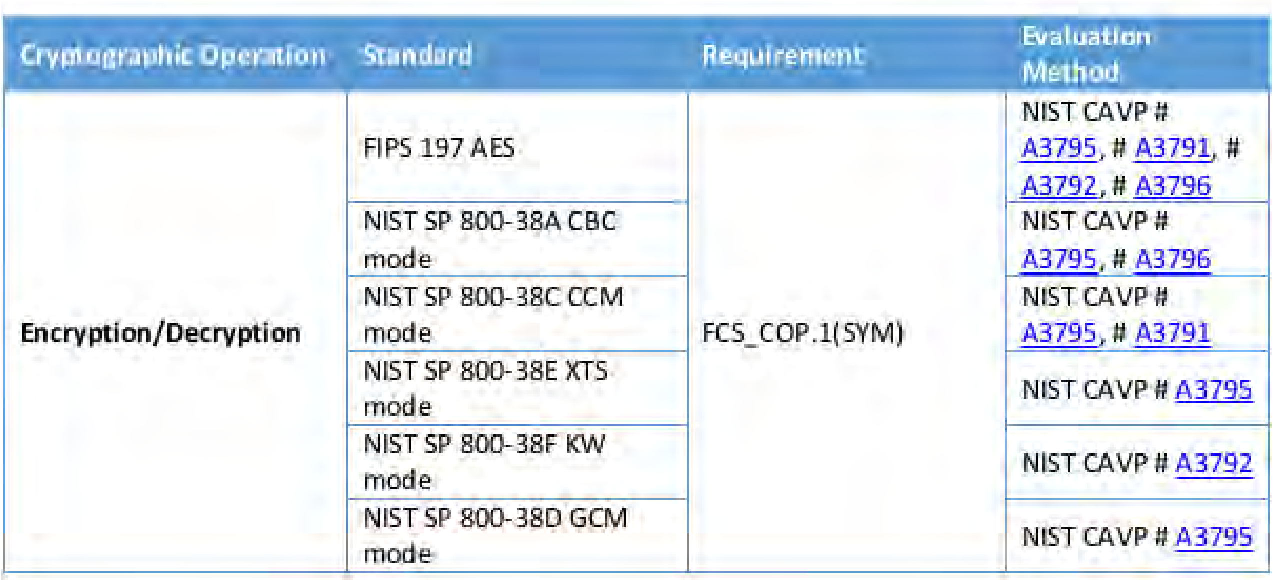


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3801, # A3797, # A3798, # A3802, # A4008, # A3748, # A3763, # A3936
	NIST SP 800-38A CBC mode		NIST CAVP # A3801, # A4008, # A3802, # A3936
	NIST SP 800-38C CCM mode		NIST CAVP # A3801, # A3797, # A4008, # A3748
	NIST SP 800-38E XTS mode		NIST CAVP # A3801, # A4008
	NIST SP 800-38F KW mode		NIST CAVP # A3798, # A3763
	NIST SP 800-38D GCM mode		NIST CAVP # A3801, # A4008
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP # A3801, # A4008
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3801, # A3802 , # A4008, # A3799, # A3765, # A3936
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3801, #A3799, # A3800, # A3802, # A4008, # A3799, # A3765, # A3936
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3801, # A4008
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3801, # A3802	NIST CAVP # A3801, # A4008
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3801, # A3799, # A3802, # A4008, # A3765, # A3936
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3801, # A3799, # A4008, # A3936
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-	FCS_COP.1 (HASH)	NIST CAVP # A3801, # A4008

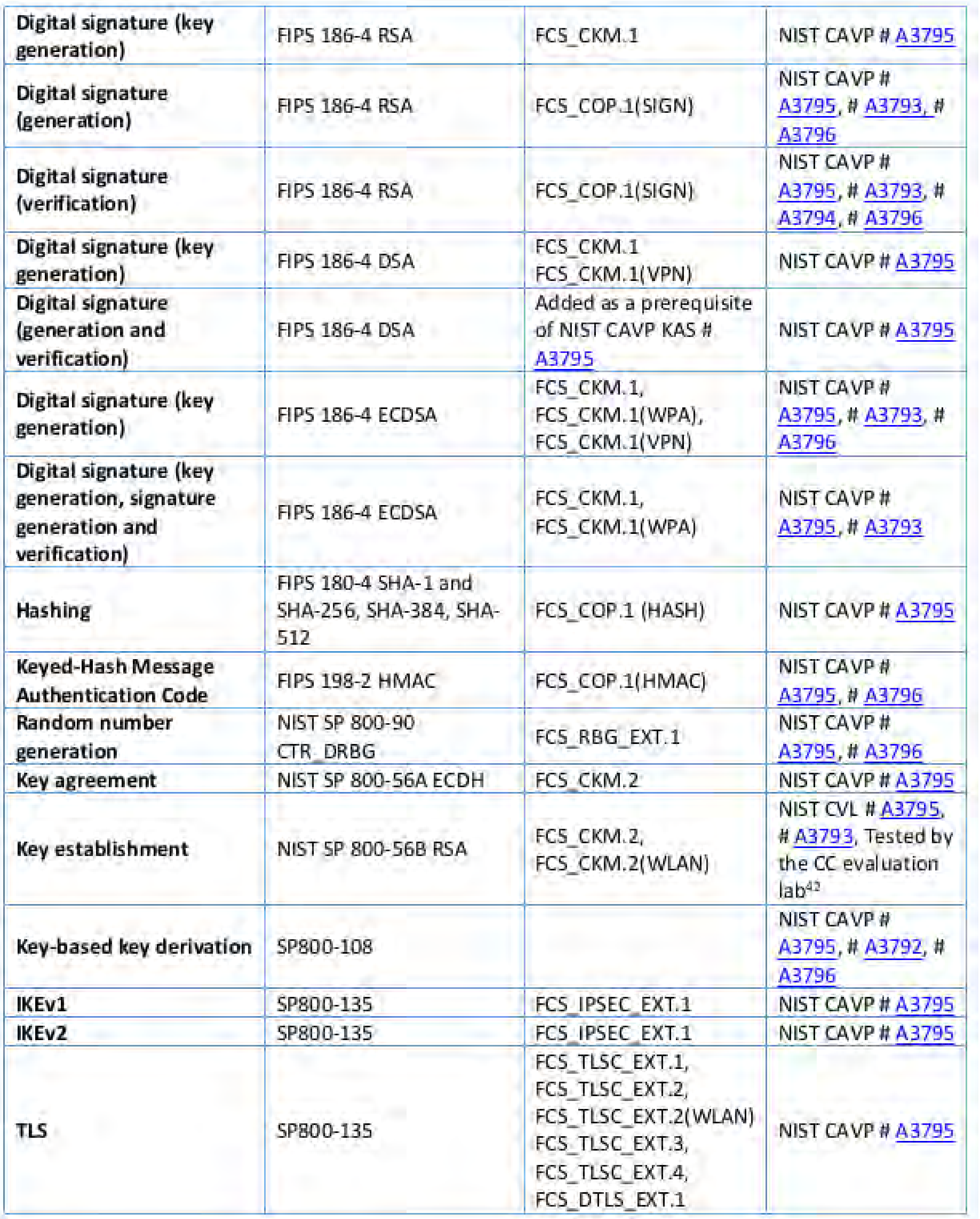


	512		
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3801, # A3802, # A4008, # A3936
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3801, # A3802, # A4008, # A3936
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3801, # A4008
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2, FCS_CKM.2(WLAN)	NIST CVL # A3801, # A3799, # A4008, # A3765, Tested by the CC evaluation lab[41]
Key-based key derivation	SP800-108		NIST CAVP # A3798, # A3802, # A3763, # A3936
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3801, # A4008
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3801, # A4008
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3801, # A4008

20.1.1.7 Cryptographic Algorithm Standards and Evaluation Methods for Windows 10 (version 22H2)

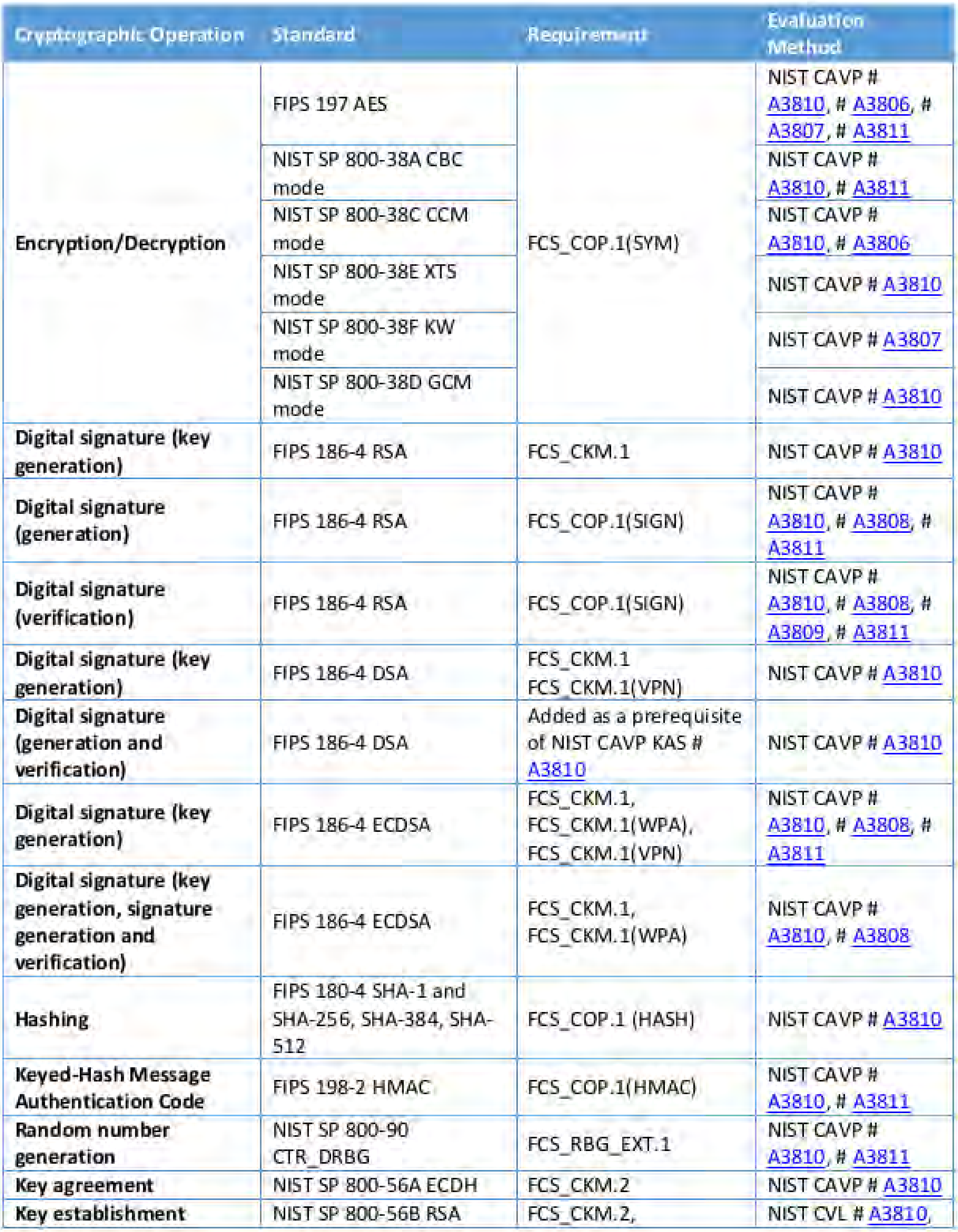


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3795, # A3791, # A3792, # A3796
	NIST SP 800-38A CBC mode		NIST CAVP # A3795, # A3796
	NIST SP 800-38C CCM mode		NIST CAVP # A3795, # A3791
	NIST SP 800-38E XTS mode		NIST CAVP # A3795
	NIST SP 800-38F KW mode		NIST CAVP # A3792
	NIST SP 800-38D GCM mode		NIST CAVP # A3795

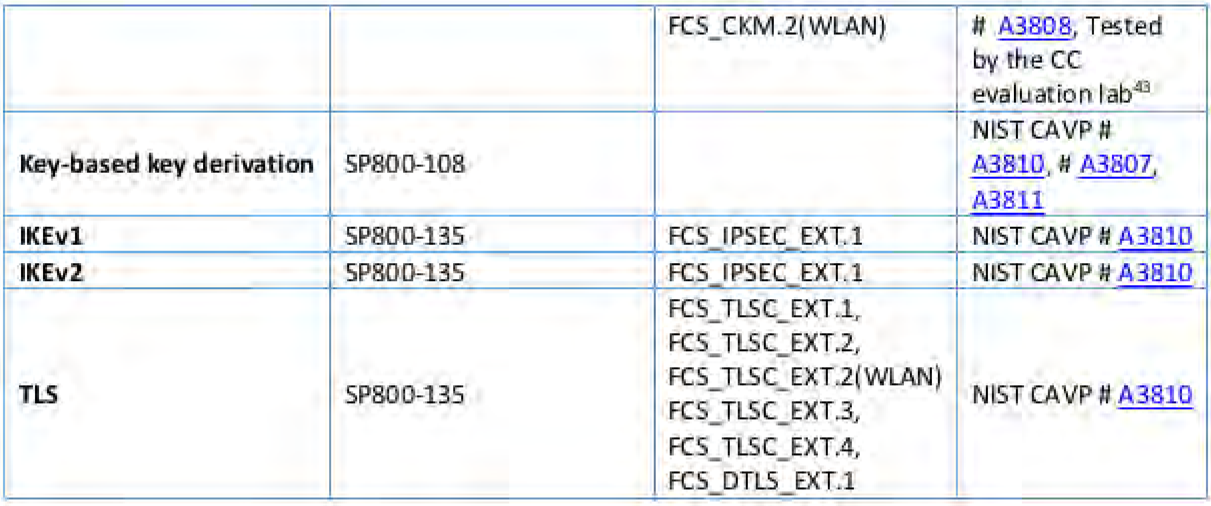


Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP # A3795
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3795, # A3793, # A3796
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3795, # A3793, # A3794, # A3796
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3795
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3795	NIST CAVP # A3795
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3795, # A3793, # A3796
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3795, # A3793
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3795
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3795, # A3796
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3795, # A3796
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3795
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2, FCS_CKM.2(WLAN)	NIST CVL # A3795, # A3793, Tested by the CC evaluation lab[42]
Key-based key derivation	SP800-108		NIST CAVP # A3795, # A3792, # A3796
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3795
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3795
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3795

20.1.1.8 Cryptographic Algorithm Standards and Evaluation Methods for Windows Server 2022 and Windows Server Datacenter: Azure Edition

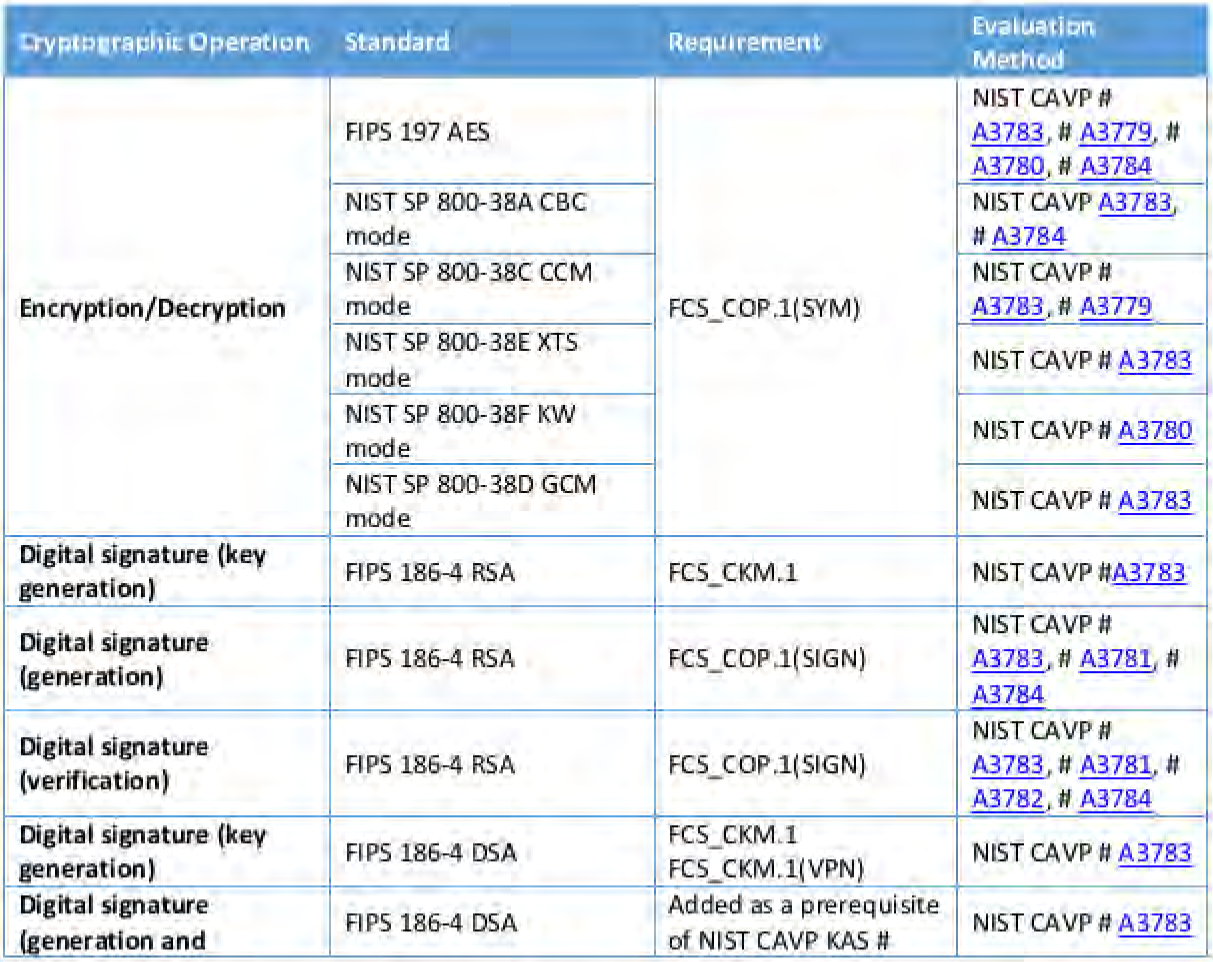


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3810, # A3806, # A3807, # A3811
	NIST SP 800-38A CBC mode		NIST CAVP # A3810, # A3811
	NIST SP 800-38C CCM mode		NIST CAVP # A3810, # A3806
	NIST SP 800-38E XTS mode		NIST CAVP # A3810
	NIST SP 800-38F KW mode		NIST CAVP # A3807
	NIST SP 800-38D GCM mode		NIST CAVP # A3810
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP # A3810
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3810, # A3808, # A3811
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3810, # A3808, # A3809, # A3811
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3810
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3810	NIST CAVP # A3810
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3810, # A3808, # A3811
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3810, # A3808
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3810
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3810, # A3811
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3810, # A3811
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3810
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2,	NIST CVL # A3810,

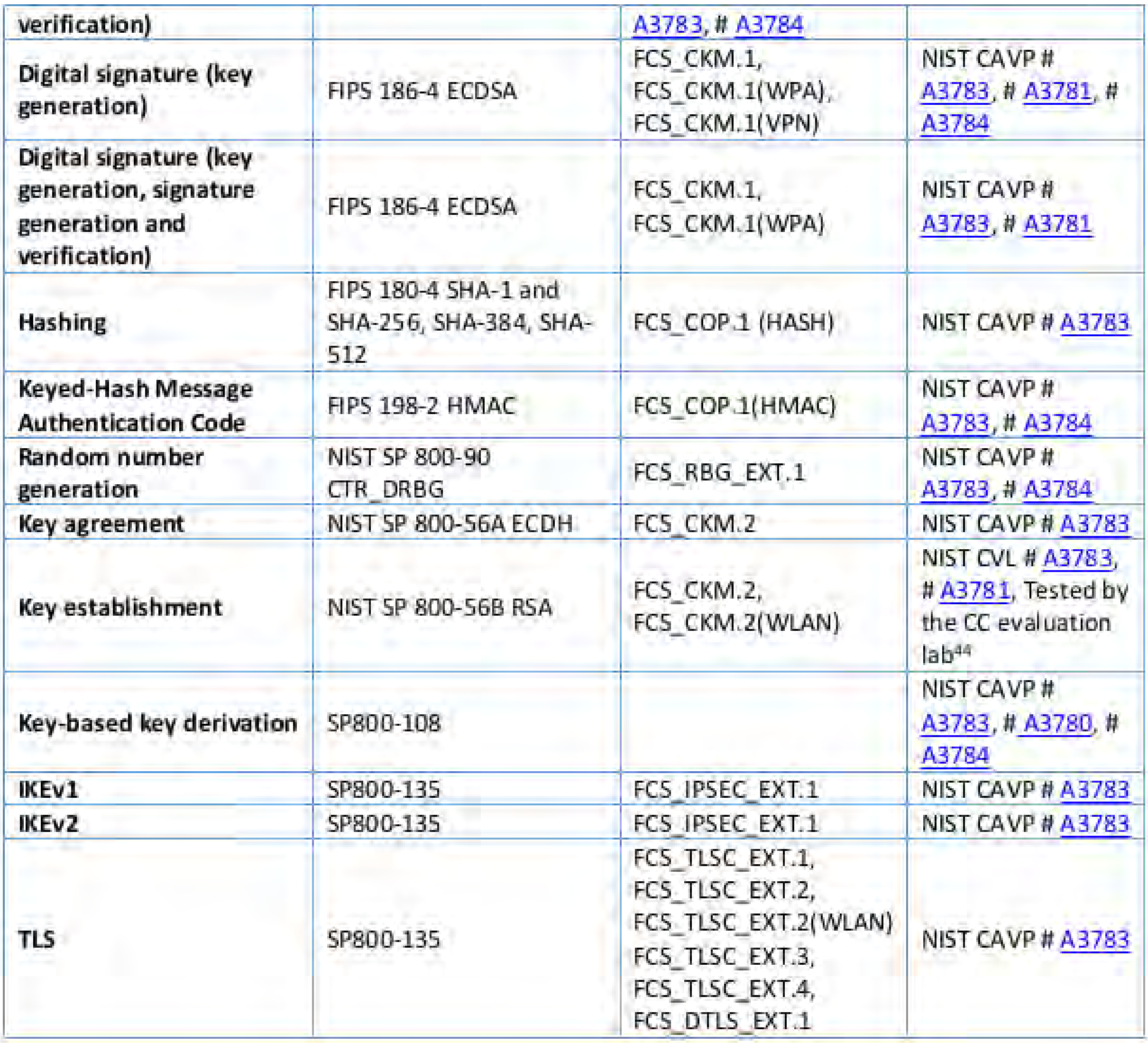


		FCS_CKM.2(WLAN)	# A3808, Tested by the CC evaluation lab[43]
Key-based key derivation	SP800-108		NIST CAVP # A3810, # A3807, A3811
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3810
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3810
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3810

20.1.1.9 Cryptographic Algorithm Standards and Evaluation Methods for Windows Server Azure Stack HCIv2 version 22H2

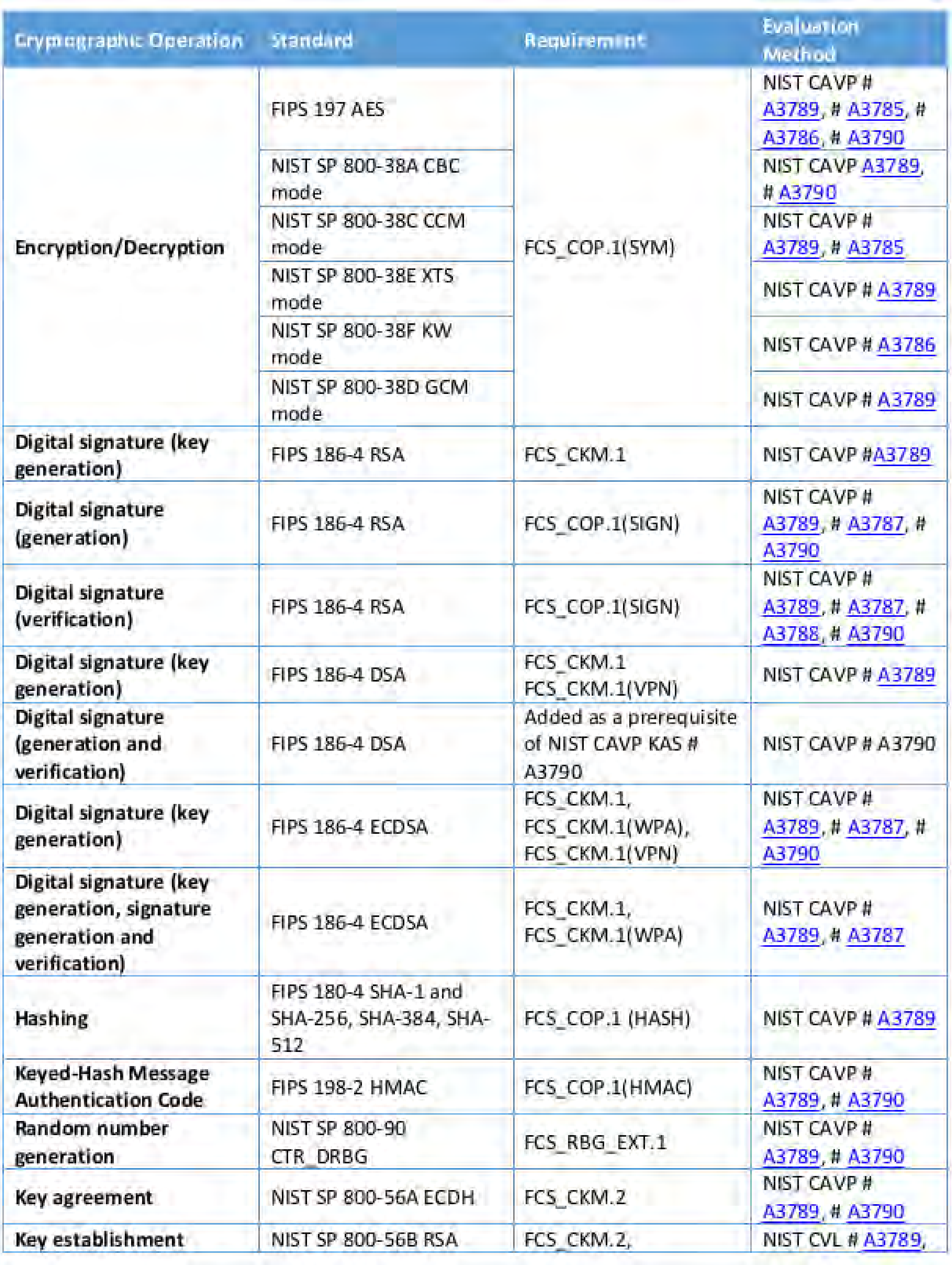


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3783, # A3779, # A3780, # A3784
	NIST SP 800-38A CBC mode		NIST CAVP A3783, # A3784
	NIST SP 800-38C CCM mode		NIST CAVP # A3783, # A3779
	NIST SP 800-38E XTS mode		NIST CAVP # A3783
	NIST SP 800-38F KW mode		NIST CAVP # A3780
	NIST SP 800-38D GCM mode		NIST CAVP # A3783
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP #A3783
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3783, # A3781, # A3784
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3783, # A3781, # A3782, # A3784
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3783
Digital signature (generation and	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS #	NIST CAVP # A3783

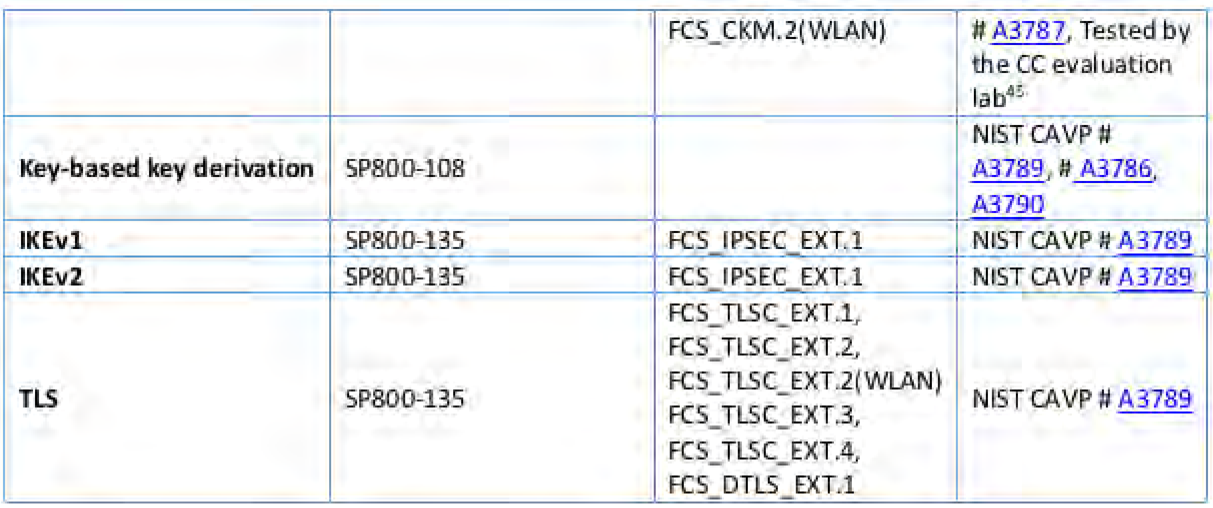


verification)		A3783, # A3784	
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3783, # A3781, # A3784
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3783, # A3781
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3783
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3783, # A3784
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3783, # A3784
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3783
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2, FCS_CKM.2(WLAN)	NIST CVL # A3783, # A3781, Tested by the CC evaluation lab[44]
Key-based key derivation	SP800-108		NIST CAVP # A3783, # A3780, # A3784
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3783
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3783
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3783

20.1.1.10 Cryptographic Algorithm Standards and Evaluation Methods for Azure Stack Hub and Azure Stack Edge



Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3789, # A3785, # A3786, # A3790
	NIST SP 800-38A CBC mode		NIST CAVP A3789, # A3790
	NIST SP 800-38C CCM mode		NIST CAVP # A3789, # A3785
	NIST SP 800-38E XTS mode		NIST CAVP # A3789
	NIST SP 800-38F KW mode		NIST CAVP # A3786
	NIST SP 800-38D GCM mode		NIST CAVP # A3789
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP #A3789
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3789, # A3787, # A3790
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3789, # A3787, # A3788, # A3790
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3789
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3790	NIST CAVP # A3790
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3789, # A3787, # A3790
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3789, # A3787
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3789
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3789, # A3790
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3789, # A3790
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3789, # A3790
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2,	NIST CVL # A3789,



		FCS_CKM.2(WLAN)	# A3787, Tested by the CC evaluation lab[45]
Key-based key derivation	SP800-108		NIST CAVP # A3789, # A3786, A3790
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3789
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3789
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3789

20.1.2 Verdict

The evaluator considers that the ***Operational Guidance*** document, defines how the FIPS security policy should be applied. Once this policy is enabled, only the approved random number generation algorithm described above can be used. No further configurations are needed to generate random bit according to NIST Special Publication 800-90A.

In addition, the evaluator has provided information about the Random number generation algorithm (*CTR_DRBG*) supported by the OS. The RNG implementation is the same (*CTR_DRBG*) which is conforming to NIST Special Publication *800-90A*.

Hence, the **PASS** verdict is assigned to the documentation review activity.

20.2 Test Activity

Based on the SFR instantiation included in the security target, the vendor has selected the following DRBG algorithms:

1. CTR-DRBG

In addition to the Common Criteria evaluation, the laboratory has also performed the CAVP validation for these and other algorithms. The general procedure that has been followed during the evaluation in order to demonstrate the correctness of the cryptographic functionality is as follows:

1. The laboratory has used the same test vectors used as part of the CAVP validation. For random number generator algorithm, the following types of test are performed:
   - Algorithm Functional Test (AFT). The main goal for these tests is verify the implementation of the random number generator functions (instantiation, generation

and reseed). It is expected that the TOE instantiate a DRBG using the provided input (entropy input, nonce, personalization string and additional input) and generate a random bitstring. The reseed process is also verified, if applicable.

2. The laboratory has exercised the cryptographic functionalities of the TOE by invoking the appropriate API in order to resolve the test vectors. The result of this step is a .json file which includes the associated response generated by the TOE per each test vector.
3. The laboratory has created a testing tool in order to exercise the BOTAN implementation for the target cryptographic algorithms. This tool receives the initial .json file with the test vectors as well as the .json file obtained as a result of the step 2. After parsing the information, the testing tool invokes the BOTAN implementation for the tested algorithm and resolve each test vector. After that, the testing tool compares both results (BOTAN vs TOE) in order to determine whether the cryptographic algorithms is properly implemented or not. The results of the testing tool is an individual outcome for each test vector (PASS or FAIL) and a overall outcome (PASS is all the test vectors passed or FAIL if any of them failed).
   - Note: Since CTR-DRBG is not available in BOTAN, the laboratory has demonstrated the correctness of the cryptographic algorithm implementation by using CAVP as a reference implementation instead of BOTAN.

20.2.1 Test 1

20.2.1.1 Setup

The following environment is required to perform the test in addition to the TOE:

- A computer with:
  - Operating System: Ubuntu 20.04
  - Test vectors are located in evaluator machine.

20.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

20.2.2 Results

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

20.2.2.1 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the test activity demonstrate that the TOE provides a valid implementation for the evaluated cryptographic algorithm, since they have been compared against a well-known implementation as a reference implementation.

Since CTR-DRBG algorithm is not available in BOTAN, the laboratory has followed the same approach but using the CAVP implementation as a reference instead of BOTAN. The evaluator has verified that the responses generated by the TOE are the same as the ones expected by the CAVP tool. Additionally, the associated CAVP certificates (listed in the tables included within the Documentation Review Activity section) have been granted demonstrating the correctness of the algorithm implementation.

Therefore, the **PASS** verdict is assigned to the test activity.

20.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to this FCS_RBG_EXT.1.1 requirement.

21 FCS_RBG_EXT.1.2

The assurance activity for the **FCS_RBG_EXT.1.2** requirement is stated as follows:

> Documentation shall be produced - and the evaluator will perform the activities - in accordance with Appendix E - Entropy Documentation and Assessment and the Clarification to the Entropy Documentation and Assessment Annex.
>
> In the future, specific statistical testing (in line with NIST SP 800-90B) will be required to verify the entropy estimates.

21.1 Documentation Review Activity

21.1.1 Findings

The vendor has provided the following documentation regarding the entropy:

- ***RNG Design***.
- ***Entropy Validation***.
- ***Security Target***.

The information provided in these documents describes with the expected level of detail how the entropy source is generated based on different entropy pools such as Interrupt timings or TPM, the available API functions that can process this entropy for a random number generation (*CTR_DRBG*), etc. In short, the life-cycle of the entropy is specified.

In addition, the ***Security Target*** document, includes more information about how the entropy source is health-tested before use, as shown in the following statement provided in the section **6.2.1 Cryptographic Algorithms and Operations**:

> *[..] Windows has different entropy sources (deterministic and nondeterministic) which produce entropy data that is used for random numbers generation. In particular, this entropy data together with other data (such as the nonce) seed the DRBG algorithm. The entropy pool is populated using the following values*:
>
> - *An initial entropy value from a seed file provided to the Windows OS Loader at boot time (512 bits of entropy).*
> - *A calculated value based on the high-resolution CPU cycle counter which fires after every 1024 interrupts (a continuous source providing 16384 bits of entropy).*
> - *Random values gathered periodically from the Trusted Platform Module (TPM), (320 bits of entropy on boot, Text intentionally left blank).*
> - *Random values gathered periodically by calling the RDRAND CPU instruction, (256 bits of entropy, Text intentionally left blank).*

> *The entropy data is obtained from the entropy sources in a raw format and is health-tested before using it as input for the DRBG. Text intentionally left blank.*

Moreover, the vendor has also provided the following document: *Entropy Validation on Windows 10, Windows 11, Windows Server, Azure Stack HCI, Hub and Edge for GP OS Evaluation*. This document contains information about the statistical tests performed on the entropy sources taking into account all platforms under evaluation, the statistical tests results are shown in the following tables:

Images has been intentionally eliminated for this public version.

21.1.2 Verdict

The evaluator considers that the ***RNG Design*** document describes in detail how the lifecycle of the entropy used by the OS works. In addition, the information provided in the ***Security Target*** document, at TSS section ***6.2.1 Cryptographic Algorithms and Operations***, about how the entropy source is health-tested before using it comparing the generated entropy blocks between them, is clear. The evaluator has also checked the statistical tests results provided in the ***Entropy Validation*** document, verifying that at least all the platforms and the operating systems under evaluation have been considered.

Due to this, the evaluator considers that the information provided in all these documents is enough for the fulfilment of the content requirement established in the Appendix E - Entropy Documentation and Assessment of the Protection Profile.

Hence, the **PASS** verdict is assigned to the documentation review activity.

21.2 Test Activity

The assurance activity does not require any testing activities. Therefore, the **PASS** verdict is assigned.

21.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to this FCS_RBG_EXT.1.2 requirement.

22 FCS_STO_EXT.1.1

The assurance activity for the **FCS_STO_EXT.1.1** requirement is stated as follows:

> The evaluator will check the TSS to ensure that it lists all persistent sensitive data for which the OS provides a storage capability. For each of these items, the evaluator will confirm that the TSS lists for what purpose it can be used, and how it is stored. The evaluator will confirm that cryptographic operations used to protect the data occur as specified in FCS_COP.1(1).
>
> The evaluator will also consult the developer documentation to verify that an interface exists for applications to securely store credentials.

22.1 Documentation Review Activity

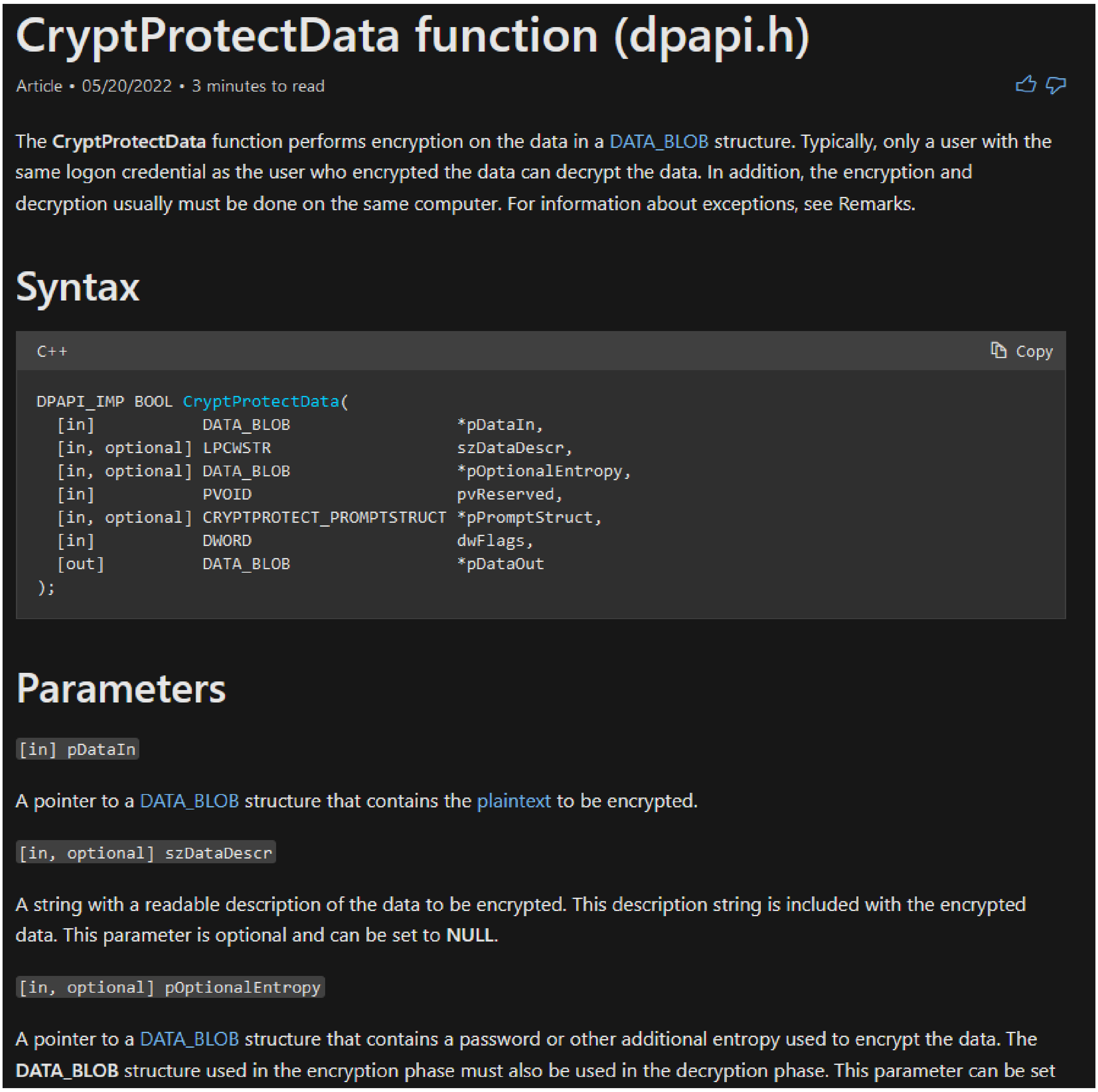
22.1.1 Findings

The evaluator has reviewed the section **6.2.4. Protecting Data with DPAPI** of the ***Security Target*** document. This section states that Windows provides the *Data Protection API*, CNG DPAPI, which can be used to protect any persistent data which the developer deems to be sensitive.

DPAPI uses the *AES-CBC* algorithm to encrypt and decrypt the sensitive information. Once the sensitive information has been encrypted, it is stored in a directory which is part of the user's profile.

DPAPI provides two functions to encrypt (*CryptProtectData* function) and decrypt (*CryptUnprotectData* function) data. This section of the TSS also includes a link to the Microsoft Developer Network (*MSDN*) where detailed information about the usage of these API functions is provided. The following images, which have been obtained from the *MSDN* website, describe the syntax of these API functions:

CryptProtectData:



CryptProtectData function (dpapi.h)

Article • 05/20/2022 • 3 minutes to read

The **CryptProtectData** function performs encryption on the data in a DATA_BLOB structure. Typically, only a user with the same logon credential as the user who encrypted the data can decrypt the data. In addition, the encryption and decryption usually must be done on the same computer. For information about exceptions, see Remarks.

Syntax

```
DPAPI_IMP BOOL CryptProtectData(
  [in]           DATA_BLOB                 *pDataIn,
  [in, optional] LPCWSTR                   szDataDescr,
  [in, optional] DATA_BLOB                 *pOptionalEntropy,
  [in]           PVOID                     pvReserved,
  [in, optional] CRYPTPROTECT_PROMPTSTRUCT *pPromptStruct,
  [in]           DWORD                     dwFlags,
  [out]          DATA_BLOB                 *pDataOut
);
```

Parameters

`[in] pDataIn`

A pointer to a DATA_BLOB structure that contains the plaintext to be encrypted.

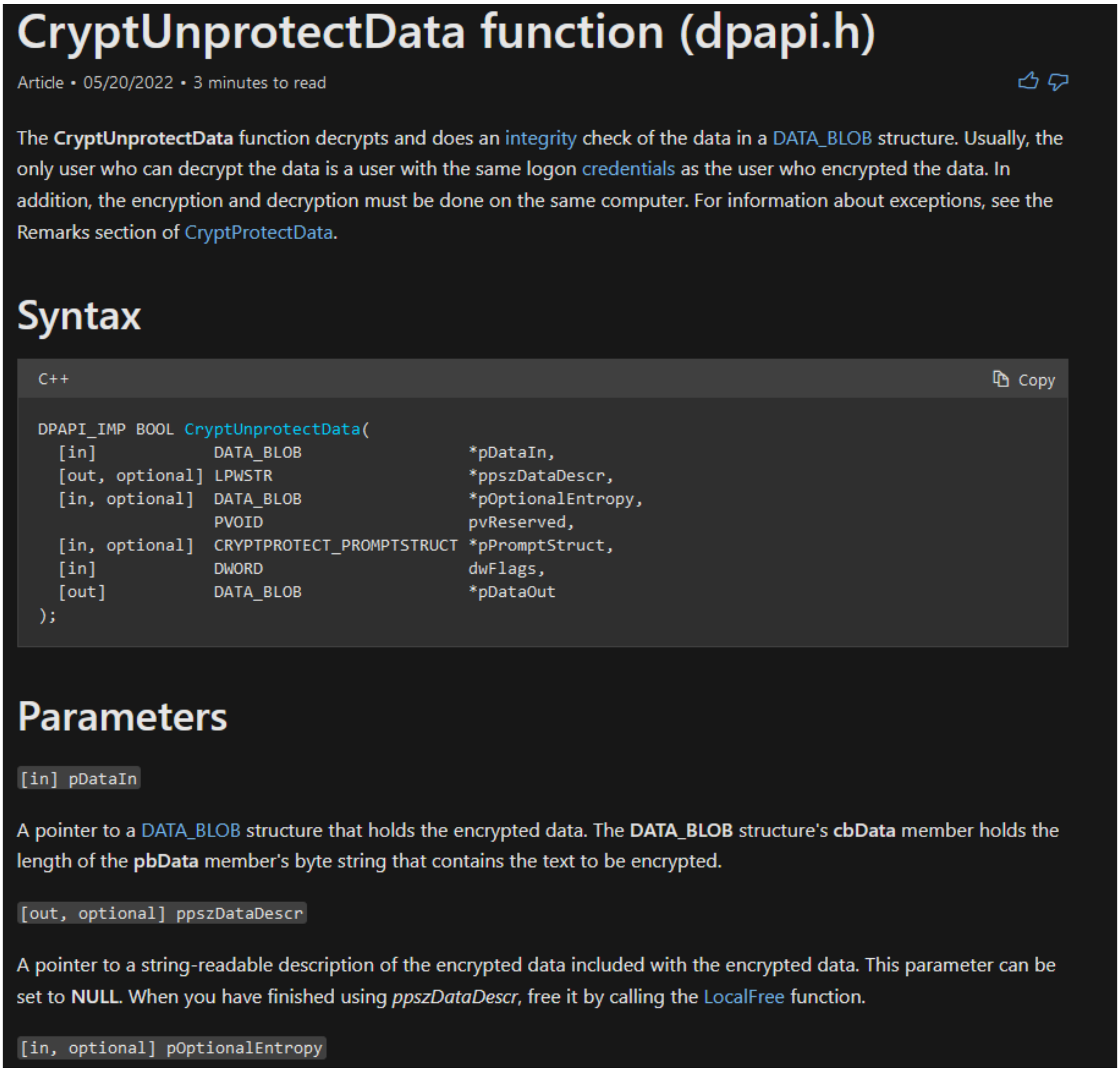
`[in, optional] szDataDescr`

A string with a readable description of the data to be encrypted. This description string is included with the encrypted data. This parameter is optional and can be set to **NULL**.

`[in, optional] pOptionalEntropy`

A pointer to a DATA_BLOB structure that contains a password or other additional entropy used to encrypt the data. The **DATA_BLOB** structure used in the encryption phase must also be used in the decryption phase. This parameter can be set

CryptUnprotectData:



CryptUnprotectData function (dpapi.h)

Article • 05/20/2022 • 3 minutes to read

The **CryptUnprotectData** function decrypts and does an integrity check of the data in a DATA_BLOB structure. Usually, the only user who can decrypt the data is a user with the same logon credentials as the user who encrypted the data. In addition, the encryption and decryption must be done on the same computer. For information about exceptions, see the Remarks section of CryptProtectData.

Syntax

```
DPAPI_IMP BOOL CryptUnprotectData(
  [in]            DATA_BLOB                 *pDataIn,
  [out, optional] LPWSTR                    *ppszDataDescr,
  [in, optional]  DATA_BLOB                 *pOptionalEntropy,
                  PVOID                     pvReserved,
  [in, optional]  CRYPTPROTECT_PROMPTSTRUCT *pPromptStruct,
  [in]            DWORD                     dwFlags,
  [out]           DATA_BLOB                 *pDataOut
);
```

Parameters

`[in] pDataIn`

A pointer to a DATA_BLOB structure that holds the encrypted data. The **DATA_BLOB** structure's **cbData** member holds the length of the **pbData** member's byte string that contains the text to be encrypted.

`[out, optional] ppszDataDescr`

A pointer to a string-readable description of the encrypted data included with the encrypted data. This parameter can be set to **NULL**. When you have finished using *ppszDataDescr*, free it by calling the LocalFree function.

`[in, optional] pOptionalEntropy`

22.1.2 Verdict

The evaluator considers that the TSS provides enough information related to the method used for sensitive data protection. The vendor states that any persistent data which the developer deems to be sensitive can be protected using DPAPI. After protecting the data, the information is stored in a directory inside the user’s profile.

The vendor has also identified the available interfaces for data protection (*CryptProtectData* and *CryptUnprotectData*), as well as the cryptographic algorithm used, AES-256-CBC, which is one of the selected in the FCS_COP.1(SYM) requirement.

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfilment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

22.2 Test Activity

The assurance activity does not require any testing activities. However the evaluator has carried out a test to verify the API functionality.

22.2.1 Test 1

22.2.1.1 Setup

Before the test execution, the following setup condition must be fulfilled:

- A C++ compiler or an IDE with a C++ compiler (e.g. *Microsoft Visual Studio 2022*)

22.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

22.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

22.2.1.4 Verdict

As it can be appreciated in the obtained results, the evaluator has been able to encrypt and decrypt data using the functions provided by DPAPI.

The evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

22.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FCS_STO_EXT.1.

23 FCS_TLSC_EXT.1.1

The assurance activity for the **FCS_TLSC_EXT.1.1** requirement is stated as follows:

> The evaluator will check the description of the implementation of this protocol in the TSS to ensure that the cipher suites supported are specified. The evaluator will check the TSS to ensure that the cipher suites specified include those listed for this component. The evaluator will also check the operational guidance to ensure that it contains instructions on configuring the OS so that TLS conforms to the description in the TSS.
>
> The evaluator will also perform the following tests:
>
> **Test 1**: The evaluator will establish a TLS connection using each of the cipher suites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of an EAP session. It is sufficient to observe the successful negotiation of a cipher suite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic in an attempt to discern the cipher suite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).
>
> **Test 2**: The evaluator will attempt to establish the connection using a server with a server certificate that contains the Server Authentication purpose in the extendedKeyUsage field and verify that a connection is established. The evaluator will then verify that the client rejects an otherwise valid server certificate that lacks the Server Authentication purpose in the extendedKeyUsage field and a connection is not established. Ideally, the two certificates should be identical except for the extendedKeyUsage field.
>
> **Test 3**: The evaluator will send a server certificate in the TLS connection that does not match the server-selected cipher suite (for example, send a ECDSA certificate while using the TLS_RSA_WITH_AES_128_CBC_SHA cipher suite or send a RSA certificate while using one of the ECDSA cipher suites.) The evaluator will verify that the OS disconnects after receiving the server's Certificate handshake message.
>
> **Test 4**: The evaluator will configure the server to select the TLS_NULL_WITH_NULL_NULL cipher suite and verify that the client denies the connection.
>
> **Test 5**: The evaluator will perform the following modifications to the traffic:
>
> - **Test 5.1**: Change the TLS version selected by the server in the Server Hello to a non-supported TLS version (for example 1.3 represented by the two bytes 03 04) and verify that the client rejects the connection.
> - **Test 5.2**: Modify at least one byte in the server's nonce in the Server Hello handshake message, and verify that the client rejects the Server Key Ex-

change handshake message (if using a DHE or ECDHE cipher suite) or that the server denies the client's Finished handshake message.

- **Test 5.3**: Modify the server's selected cipher suite in the Server Hello handshake message to be a cipher suite not presented in the Client Hello handshake message. The evaluator will verify that the client rejects the connection after receiving the Server Hello.
- **Test 5.4**: If an ECDHE or DHE ciphersuite is selected, modify the signature block in the Server's Key Exchange handshake message, and verify that the client rejects the connection after receiving the Server Key Exchange message.
- **Test 5.5**: Modify a byte in the Server Finished handshake message, and verify that the client sends a fatal alert upon receipt and does not send any application data.
- **Test 5.6**: Send a garbled message from the Server after the Server has issued the Change Cipher Spec message and verify that the client denies the connection.

23.1 Documentation Review activity

23.1.1 Findings

Section **6.2.3.1 TLS, HTTPS, DTLS, EAP-TLS** of the TSS, in the ***Security Target*** document, provides a website where the different cipher suites supported by the *Schannel* library are described.

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246,
- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 5246,
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246,
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246,
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288,
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288,
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289,
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289.

These cipher suites match with the selected ones in the requirement definition. The cipher suites listed above are a subset of the ones implemented in the *Schannel* library, as it can be checked in the previous URL.

Moreover, section **4.3 Managing Transport Layer Security (TLS)** of the ***Operational Guidance*** document describes how to configure these TLS cipher suites. The information can be found in the following MSDN link:

- MSDN Link 1

Selection of TLS cipher suites in the TLS handshake process is performed according to the order defined which can be configured as described in the link listed above.

23.1.2 Verdict

The evaluator considers that the evidences defined above and obtained during the documentation review demonstrate the fulfilment of the requirement established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the documentation review activity.

23.2 Test Activity

To perform the TLS tests required by the Assurance Activities and check their correct outcome, different pieces of software were used:

1. Software acting as a TLS server:
   a. *ee-tls-tool*, a command line tool developed by the evaluation laboratory in order to create a TLS server which is automatically configured prior each test case execution.
2. Software acting as a client from the TOE
   b. *W10ClientAutomator.ps1*, a Powershell script which automatically configures the TOE as a client prior each test case execution. This script allows the evaluator execute test cases using:
      i. different web browsers that come bundled with the TOE (i.e. Internet Explorer and Microsoft Edge).
      ii. *TlsClientTest*, a command line tool developed by the evaluation laboratory. This tool provides more information about the concrete point where SSL validation failed in case of connection error.

Using *TlsClientTest* tool, the evaluator is able to identify the main cause when the SSL connection fails. Also, testing with web browser, while providing less failure output, allow the evaluator to validate the obtained findings in scenarios closer to the real ones a TOE user may encounter.

TlsCientTest tool was developed in C# using the System.Net.Security classes from .NET Framework to perform SSL connections, closely based on an example from Microsoft's MSDN. It effectively uses the authentication mechanism from the OS, which is the target of the evaluation.

Special care was taken to verify this claim, so several checks were performed for confirmation after the tool was developed. First, some code snippets are shown for reference.

Importing the security libraries:

```
using System;
using System.Collections;
using System.Net;
using System.Net.Security;
using System.Net.Sockets;
using System.Security.Authentication;
using System.Text;
using System.Security.Cryptography.X509Certificates;
using System.IO;
```

Establishing the TLS 1.2 connection, importing client certificates in the process (if there are any):

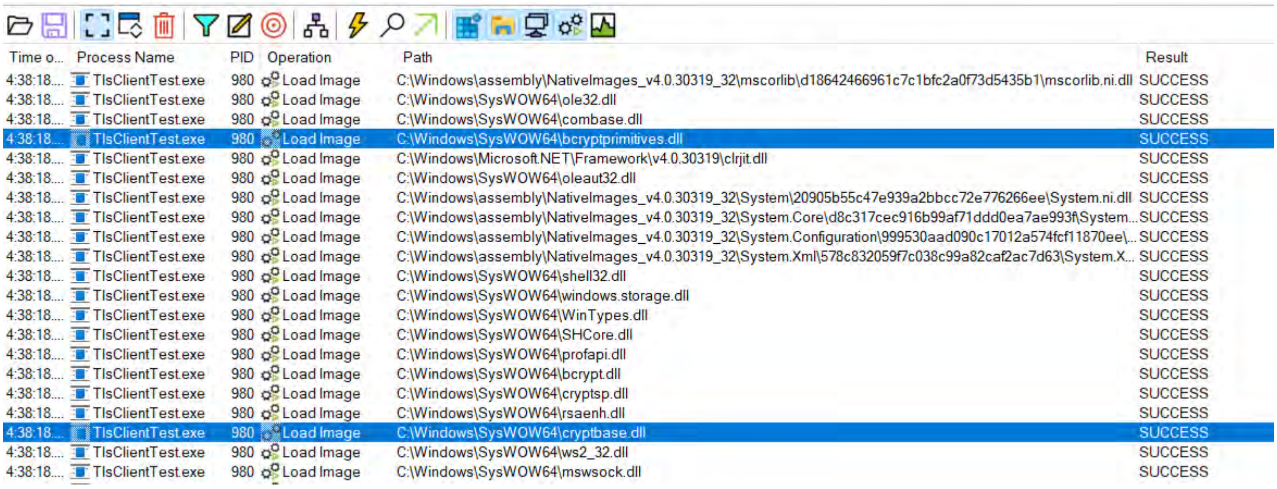
```
SslStream sslStream = new SslStream(
    client.GetStream(),
   false,
   new RemoteCertificateValidationCallback(ValidateServerCertificate),
   null
);

// Load available certificates in store, including client certificates
X509CertificateCollection certCollection = new X509CertificateCollection();
X509Store store = new X509Store(StoreLocation.CurrentUser);
store.Open(OpenFlags.ReadOnly);
foreach (X509Certificate cert in store.Certificates)
{
    certCollection.Add(cert);
}
store.Close();
    // The server name must match the name on the server certificate.
try
{
    sslStream.AuthenticateAsClient(serverName, certCollection, SslProtocols.Tls12,
        checkCertificateRevocation);
}
catch (Exception e)
{
    Console.WriteLine("Exception: {0}\r\n", e.Message);
    if (e.InnerException != null)
    {
        Console.WriteLine("Inner exception: {0}", e.InnerException.Message);
    }
    Console.WriteLine("Authentication failed — closing the connection.\r\n");
    client.Close();
    return;
}
```

Rejecting the connection if certificate validation fails, printing failure output:

```
// The following method is invoked by the RemoteCertificateValidationDelegate.
public static bool ValidateServerCertificate(
    object sender,
    X509Certificate certificate,
    X509Chain chain,
    SslPolicyErrors sslPolicyErrors)
{
    if (sslPolicyErrors == SslPolicyErrors.None)
        return true;

    Console.WriteLine("Certificate error: {0} \n", sslPolicyErrors);
    foreach (X509ChainStatus status in chain.ChainStatus)
    {
        Console.WriteLine("Chain status: {0}", status.StatusInformation);
    }

    // Do not allow this client to communicate with unauthenticated servers.
    return false;
}
```

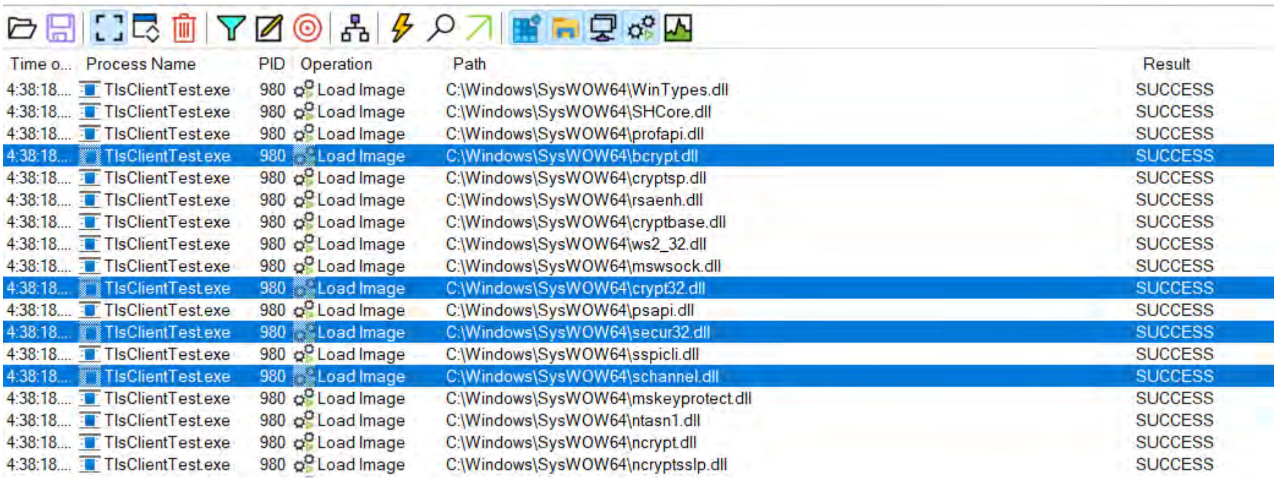
Process Monitor from Windows Sysinternals is used to verify that the Operating System shared libraries related to TLS and cryptography are being used when performing a connection with this tool.

First, the tool's launch is observed, where the different DLLs needed are loaded. Among them we can find libraries such as *cryptbase.dll* and *bcryptprimitives.dll*.



Time o...	Process Name	PID	Operation	Path	Result
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\d18642466961c7c1bfc2a0f73d5435b1\mscorlib.ni.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\ole32.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\combase.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\bcryptprimitives.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\Microsoft.NET\Framework\v4.0.30319\clrjit.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\oleaut32.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\assembly\NativeImages_v4.0.30319_32\System\20905b55c47e939a2bbcc72e776266ee\System.ni.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\d8c317cec916b99af71ddd0ea7ae993f\System...	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\999530aad090c17012a574fcf11870ee\...	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\578c832059f7c038c99a82caf2ac7d63\System.X...	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\shell32.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\windows.storage.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\WinTypes.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\SHCore.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\profapi.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\bcrypt.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\cryptsp.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\rsaenh.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\cryptbase.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\ws2_32.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\mswsock.dll	SUCCESS

During the TCP connection it can be observed how other key DLLs are leveraged. Some of them are *crypt32.dll*, *secur32.dll*, *schannel.dll* and *bcrypt.dll*.



Time o...	Process Name	PID	Operation	Path	Result
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\WinTypes.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\SHCore.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\profapi.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\bcrypt.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\cryptsp.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\rsaenh.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\cryptbase.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\ws2_32.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\mswsock.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\crypt32.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\psapi.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\secur32.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\sspicli.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\schannel.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\mskeyprotect.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\ntasn1.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\ncrypt.dll	SUCCESS
4:38:18....	TlsClientTest.exe	980	Load Image	C:\Windows\SysWOW64\ncryptsslp.dll	SUCCESS

Moreover, by enabling *Schannel event logging* as indicated by the vendor, the evaluator can observe in the *Windows Event Viewer* that the connections are performed via *Schannel*.

W10ClientAutomator.ps1 has been developed to automatically configure the TOE (i.e. certificates installation, validation or revocation) for each test case. After executing the script, a menu is prompted in order to select which requirement is going to be tested.

After choosing the requirement, the script automatically set the configuration on TOE using auxiliary functions to install, remove or revoke the certificates required to perform each test cases.

Finally, each requirement has a function in which all the test defined in the Assurance Activity are executed.

23.2.1 Test 1

23.2.1.1 Setup

The following certificates, created automatically by *ee-tls-tool* and installed by *W10ClientAutomator* shall be used to perform the assurance activities listed on the Protection Profile:

- CN = EE Test Root CA
- CN = test.epoche.es

The listed certificates form a valid certification path. The root certificate is available in pem format.

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Server Machine (Debian 9 Stretch)
- Client Machine (Platforms listed in the ST)

Both machines are in the same network with the following configuration:

- Server Machine, IP = 50.50.50.227
- Client Machine, IP = 50.50.50.155

Server machine contains the *ee-tls-tool* software, a test suite for TLS and X509 Common Criteria evaluations. It acts as a TLS server configured according to each test. In addition, the *Wireshark* network analyzer is installed on the server machine.

The client machine shall contain the PowerShell script *W10ClientAutomator.ps1* and the *TlsClientTest* tool, which uses the System.Net. Security classes from .Net framework to perform SSL connections, effectively using the authentication mechanism from the OS.

Moreover, the client machine shall have the secure configuration enabled, according to the section **3.2 Operational prerequisites** of the ***Operational Guidance***.

23.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

23.2.1.3 Results

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

23.2.1.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 1** activity demonstrate the fulfillment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 1** activity.

23.2.2 Test 2

23.2.2.1 Setup

The setup is identical to the one defined for Test 1.

23.2.2.2 Procedure

The procedure is identical to the one defined for Test 1.

23.2.2.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

23.2.2.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 2** activity demonstrate the fulfillment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 2** activity.

23.2.3 Test 3

23.2.3.1 Setup

The setup is identical to the one defined for Test 1, but the IP address for the server is 50.50.50.220.

23.2.3.2 Procedure

The procedure is identical to the one defined for Test 1.

23.2.3.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

23.2.3.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 3** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 3** activity.

23.2.4 Test 4

23.2.4.1 Setup

The setup is identical to the one defined for Test 1.

23.2.4.2 Procedure

The procedure is identical to the one defined for Test 1.

23.2.4.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

23.2.4.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 4** activity demonstrate the fulfillment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 4** activity.

23.2.5 Test 5.1

23.2.5.1 Setup

The setup is identical to the one defined for Test 1 but the IP address for the server is 50.50.50.220.

23.2.5.2 Procedure

The procedure is identical to the one defined for Test 1.

23.2.5.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

23.2.5.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 5.1** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 5.1** activity.

23.2.6 Test 5.2

23.2.6.1 Setup

The setup is identical to the one defined for Test 1.

23.2.6.2 Procedure

The procedure is identical to the one defined for Test 1.

23.2.6.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

23.2.6.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 5.2** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 5.2** activity.

23.2.7 Test 5.3

23.2.7.1 Setup

The setup is identical to the one defined for Test 1.

23.2.7.2 Procedure

The procedure is identical to the one defined for Test 1.

23.2.7.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

23.2.7.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 5.3** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 5.3** activity.

23.2.8 Test 5.4

23.2.8.1 Setup

The setup is identical to the one defined for Test 1, but IP addresses for this test are 50.50.50.100 for the server and 50.50.50.227 for the client.

23.2.8.2 Procedure

The procedure is identical to the one defined for Test 1.

23.2.8.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

23.2.8.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 5.4** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 5.4** activity.

23.2.9 Test 5.5

23.2.9.1 Setup

The setup is identical to the one defined for Test 1, but IP addresses for this test are 50.50.50.100 for the server and 50.50.50.227 for the client.

23.2.9.2 Procedure

The setup is identical to the one defined for Test 1.

23.2.9.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

23.2.9.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 5.5** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 5.5** activity.

23.2.10 Test 5.6

23.2.10.1 Setup

The setup is identical to the one defined for Test 1, but IP addresses for this test are 50.50.50.100 for the server and 50.50.50.227 for the client.

23.2.10.2 Procedure

The setup is identical to the one defined for Test 1.

23.2.10.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

23.2.10.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 5.6** activity demonstrate the fulfillment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 5.6** activity.

23.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to this FCS_TLSC_EXT.1.1.

24 FCS_TLSC_EXT.1.2

The assurance activity for the **FCS_TLSC_EXT.1.2** requirement is stated as follows:

> The evaluator will ensure that the TSS describes the client's method of establishing all reference identifiers from the application-configured reference identifier, including which types of reference identifiers are supported (e.g. Common Name, DNS Name, URI Name, Service Name, or other application-specific Subject Alternative Names) and whether IP addresses and wildcards are supported. The evaluator will ensure that this description identifies whether and the manner in which certificate pinning is supported or used by the OS. The evaluator will verify that the AGD guidance includes instructions for setting the reference identifier to be used for the purposes of certificate validation in TLS.
>
> The evaluator will configure the reference identifier according to the AGD guidance and perform the following tests during a TLS connection:
>
> **Test 1**: The evaluator will present a server certificate that does not contain an identifier in either the Subject Alternative Name (SAN) or Common Name (CN) that matches the reference identifier. The evaluator will verify that the connection fails.
>
> **Test 2**: The evaluator will present a server certificate that contains a CN that matches the reference identifier,contains the SAN extension, but does not contain an identifier in the SAN that matches the reference identifier. The evaluator shall verify that the connection fails. The evaluator will repeat this test for each supported SAN type.
>
> **Test 3** [conditional]: If the TOE does not mandate the presence of the SAN extension, the evaluator shall present a server certificate that contains a CN that matches the reference identifier and does not contain the SAN extension. The evaluator shall verify that the connection succeeds. If the TOE does mandate the presence of the SAN extension, this Test shall be omitted.
>
> **Test 4**: The evaluator will present a server certificate that contains a CN that does not match the reference identifier but does contain an identifier in the SAN that matches. The evaluator will verify that the connection succeeds.
>
> **Test 5**: The evaluator will perform the following wildcard tests with each supported type of reference identifier:
>
> - **Test 5.1**: The evaluator will present a server certificate containing a wildcard that is not in the left-most label of the presented identifier (e.g. foo.*.example.com) and verify that the connection fails.
> - **Test 5.2**: The evaluator will present a server certificate containing a wildcard in the left-most label but not preceding the public suffix (e.g. *.example.com). The evaluator will configure the reference identifier with a sin-

gle left-most label (e.g. foo.example.com) and verify that the connection succeeds. The evaluator will configure the reference identifier without a left-most label as in the certificate (e.g. example.com) and verify that the connection fails. The evaluator will configure the reference identifier with two left-most labels (e.g. bar.foo.example.com) and verify that the connection fails.

- **Test 5.3**: The evaluator will present a server certificate containing a wildcard in the left-most label immediately preceding the public suffix (e.g. *.com). The evaluator will configure the reference identifier with a single left-most label (e.g. foo.com) and verify that the connection fails. The evaluator will configure the reference identifier with two left-most labels (e.g. bar.foo.com) and verify that the connection fails.

Test 6: [conditional] If URI or Service name reference identifiers are supported, the evaluator will configure the DNS name and the service identifier. The evaluator will present a server certificate containing the correct DNS name and service identifier in the URIName or SRVName fields of the SAN and verify that the connection succeeds. The evaluator will repeat this test with the wrong service identifier (but correct DNS name) and verify that the connection fails.

Test 7: [conditional] If pinned certificates are supported the evaluator will present a certificate that does not match the pinned certificate and verify that the connection fails.

24.1 Documentation Review activity

24.1.1 Findings

Section **6.2.3.1 TLS, HTTPS, DTLS, EAP-TLS** of the TSS in the ***Security Target*** document includes the following statements:

> "The reference identifier in Windows for TLS is the DNS name or IP address of the remote server, which is compared against the DNS name as presented identifier in the Subject Alternative Name (SAN) or the Subject Name of the certificate. There is no configuration of the reference identifier.
>
> A certificate that uses a wildcard in the leftmost portion of the resource identifier (i.e., *.contoso.com) can be accepted for authentication, otherwise the certificate will be deemed invalid. Windows does not provide a general-purpose capability to "pin" TLS certificates."

The same information is provided in section **4.3 Managing Transport Layer Security (TLS)** of the ***Operational Guidance*** document. Both documents state that there is no configuration of the reference identifier, and the reference identifier is taken as the DNS name or the

IP address of the remote server. It is also stated that DNS names are supported as SAN type and as Common Name in the certificate´s Subject Name field. 3 Also, it is indicated that IP addresses and wildcards are supported. Finally, it is also specified that Windows does not provide the capability to pin TLS certificates.

24.1.2 Verdict

The evaluator considers that the evidences defined above and obtained during the documentation review demonstrate the fulfilment of the requirement established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the documentation review activity.

24.2 Test Activity

To perform the TLS tests required by the Assurance Activities and check their correct outcome, different pieces of software were used:

1. Software acting as a TLS server:
   a. *ee-tls-tool*, a command line tool developed by the evaluation laboratory in order to create a TLS server which is automatically configured prior each test case execution.
2. Software acting as a client from the TOE
   b. *W10ClientAutomator.ps1*, a Powershell script which automatically configures the TOE as a client prior each test case execution. This script allows the evaluator execute test cases using:
      i. different web browsers that come bundled with the TOE (i.e. Internet Explorer and Microsoft Edge).
      ii. *TlsClientTest*, a command line tool developed by the evaluation laboratory. This tool provides more information about the concrete point where SSL validation failed in case of connection error.

Information about their suitability for this evaluation is given in the introduction to FCS_ TLSC_EXT.1.1.

24.2.1 Test 1

24.2.1.1 Setup

The following certificates, created automatically by *ee-tls-tool* and installed by *W10ClientAutomator*
shall be used to perform the assurance activities listed on the Protection Profile:

- CN = EE Test Root CA
- CN = invalid.epoche.es

The listed certificates form a valid certification path. The root certificate is available in pem format.

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Server Machine (Debian 9 Stretch)
- Client Machine (Platforms listed in the ST)

Both machines are in the same network with the following configuration:

- Server Machine, IP = 50.50.50.227
- Client Machine, IP = 50.50.50.155

Server machine contains the *ee-tls-tool* software, a test suite for TLS and X509 Common Criteria evaluations. It acts as a TLS server configured according to each test. In addition, the *Wireshark* network analyzer is installed on the server machine.

The client machine shall contain the PowerShell script *W10ClientAutomator.ps1* and the *TlsClientTest* tool, which uses the System.Net. Security classes from .Net framework to perform SSL connections, effectively using the authentication mechanism from the OS.

Moreover, the client machine shall have the secure configuration enabled, according to the section **3.2 Operational prerequisites** of the ***Operational Guidance***.

24.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

24.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

24.2.1.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 1** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 1** activity.

24.2.2 Test 2

24.2.2.1 Setup

The setup is identical to the one defined for Test 1 (IPs configuration and installed tools). The certificate used for the connection is different than the one used for Test 1:

- CN = EE Test Root CA
- CN = test.epoche.es

The listed certificates form a valid certification path. The root certificate is available in pem format.

24.2.2.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

24.2.2.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

24.2.2.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 2** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 2** activity.

24.2.3 Test 3

24.2.3.1 Setup

The setup is identical to the one defined for Test 2.

24.2.3.2 Procedure

The procedure is identical to the one defined for Test 2.

24.2.3.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

24.2.3.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 3** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 3** activity.

24.2.4 Test 4

24.2.4.1 Setup

The setup is identical to the one defined for Test 1.

24.2.4.2 Procedure

The procedure is identical to the one defined for Test 1.

24.2.4.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

24.2.4.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 4** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 4** activity.

24.2.5 Test 5.1

24.2.5.1 Setup

The setup is identical to the one defined for Test 1 (IPs configuration and installed tools). The certificate used for the connection is different than the one used for Test 1:

- CN = EE Test Root CA
- CN = foo.*.test.epoche.es

The listed certificates form a valid certification path. The root certificate is available in pem format.

24.2.5.2 Procedure

The procedure is identical to the one defined for Test 1.

24.2.5.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

24.2.5.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 5.1** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 5.1** activity.

24.2.6 Test 5.2

24.2.6.1 Setup

The setup is identical to the one defined for Test 1 (IPs configuration and installed tools). The certificate used for the connection is different than the one used for Test 1:

- CN = EE Test Root CA
- CN = *.test.epoche.es

The listed certificates form a valid certification path. The root certificate is available in pem format.

24.2.6.2 Procedure

The procedure is identical to the one defined for Test 1.

24.2.6.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

24.2.6.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 5.2** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 5.2** activity.

24.2.7 Test 5.3

24.2.7.1 Setup

The setup is identical to the one defined for Test 1 (IPs configuration and installed tools). The certificate used for the connection is different than the one used for Test 1:

- CN = EE Test Root CA
- CN = *.es

The listed certificates form a valid certification path. The root certificate is available in pem format.

24.2.7.2 Procedure

The procedure is identical to the one defined for Test 1.

24.2.7.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

24.2.7.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 5.3** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 5.3** activity.

24.2.8 Test 6

This test is a conditional test and as stated in the section **6.2.3.1 TLS, HTTPS, DTLS, EAP-TLS** of the ***Security Target***:

> "The reference identifier in Windows for TLS is the DNS name or IP address of the remote server, which is compared against the DNS name as presented identifier in the Subject Alternative Name (SAN) or the Subject Name of the certificate. There is no configuration of the reference identifier."

Therefore, this test not applicable in this evaluation since the condition is not met.

24.2.9 Test 7

This test is a conditional test and as stated in the section **6.2.3.1 TLS, HTTPS, DTLS, EAP-TLS** of the ***Security Target***:

> "A certificate that uses a wildcard in the leftmost portion of the resource identifier (i.e., *.contoso.com) can be accepted for authentication, otherwise the certificate will be deemed invalid. Windows does not provide a general-purpose capability to "pin" TLS certificates."

Therefore, this test not applicable in this evaluation since the condition is not met.

24.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to this FCS_TLSC_EXT.1.2.

25 FCS_TLSC_EXT.1.3

The assurance activity for the **FCS_TLSC_EXT.1.3** requirement is stated as follows:

> The evaluator will use TLS as a function to verify that the validation rules in FIA_X509_EXT.1.1 are adhered to and shall perform the following additional test:
>
> **Test 1**: The evaluator will demonstrate that a peer using a certificate without a valid certification path results in an authenticate failure. Using the administrative guidance, the evaluator will then load the trusted CA certificate(s) needed to validate the peer's certificate, and demonstrate that the connection succeeds. The evaluator then shall delete one of the CA certificates, and show that the connection fails.
>
> **Test 2**: The evaluator will demonstrate that a peer using a certificate which has been revoked results in an authentication failure.
>
> **Test 3**: The evaluator will demonstrate that a peer using a certificate which has passed its expiration date results in an authentication failure.
>
> **Test 4**: the evaluator will demonstrate that a peer using a certificate which does not have a valid identifier shall result in an authentication failure.

25.1 Documentation Review activity

25.1.1 Findings

Assurance activity does not state any documentation review activity for this requirement.

25.1.2 Verdict

Assurance activity does not state any documentation review activity for this requirement. Therefore, the **PASS** verdict is assigned to the documentation review activity.

25.2 Test Activity

To perform the TLS tests required by the Assurance Activities and check their correct outcome, different pieces of software were used:

1. Software acting as a TLS server:
   a. *ee-tls-tool*, a command line tool developed by the evaluation laboratory in order to create a TLS server which is automatically configured prior each test case execution.

2. Software acting as a client from the TOE
   b. *W10ClientAutomator.ps1*, a Powershell script which automatically configures the TOE as a client prior each test case execution. This script allows the evaluator execute test cases using:
      i. different web browsers that come bundled with the TOE (i.e. Internet Explorer and Microsoft Edge).
      ii. *TlsClientTest*, a command line tool developed by the evaluation laboratory. This tool provides more information about the concrete point where SSL validation failed in case of connection error.

Information about their suitability for this evaluation is given in the introduction to FCS_ TLSC_EXT.1.1.

25.2.1 Test 1

25.2.1.1 Setup

The following certificates, created automatically by *ee-tls-tool* and \ installed by *W10ClientAutomator.ps1*, shall be used to perform the assurance activities listed on the Protection Profile:

- CN = EE Test Root CA
- CN = EE Test Intermediate CA 1
- CN = EE Test Intermediate CA 2
- CN = test.epoche.es

The listed certificates form a valid certification path. All certificates are available in pem format.

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Server Machine (Debian 9 Stretch)
- Client Machine (Platforms listed in the ST)

These two machines are in the same network with the following configuration:

- Server Machine, IP = 50.50.50.227
- Client Machine, IP = 50.50.50.155

Server machine contains the *ee-tls-tool* software, a test suite for TLS and X509 Common Criteria evaluations. It acts as a TLS server configured according to each test. In addition, the *Wireshark* network analyzer is installed on the server machine.

The client machine shall contain the PowerShell script *W10ClientAutomator.ps1* and the *TlsClientTest* tool, which uses the System.Net. Security classes from .Net framework to perform SSL connections, effectively using the authentication mechanism from the OS.

Moreover, the client machine shall have the secure configuration enabled, according to the section **3.2 Operational prerequisites** of the ***Operational Guidance***.

25.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

25.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

25.2.1.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 1** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 1** activity.

25.2.2 Test 2

25.2.2.1 Setup

The setup is identical to the one defined for Test 1 (IPs configuration and installed tools). The certificates used for the connection are different than the ones used for Test 1:

- CN = EE Test Root CA
- CN = EE Test Intermediate CA 1
- CN = EE Test Intermediate CA 2
- CN = test.epoche.es (revoked)

The listed certificates form a valid certification path. All certificates are available in pem format as well as pfx.

25.2.2.2 Procedure

The procedure is identical to the one defined for Test 1.

25.2.2.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

25.2.2.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 2** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 2** activity.

25.2.3 Test 3

25.2.3.1 Setup

The setup is identical to the one defined for Test 1 (IPs configuration and installed tools). The certificates used for the connection are different than the ones used for Test 1:

- CN = EE Test Root CA
- CN = EE Test Intermediate CA 1
- CN = EE Test Intermediate CA 2
- CN = test.epoche.es (expired certificate)

The listed certificates form a valid certification path. All certificates are available in pem format.

25.2.3.2 Procedure

The procedure is identical to the one defined for Test 1.

25.2.3.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

25.2.3.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 3** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 3** activity.

25.2.4 Test 4

25.2.4.1 Setup

The setup is identical to the one defined for Test 1 (IPs configuration and installed tools). The certificates used for the connection are different than the ones used for Test 1:

- CN = EE Test Root CA
- CN = test.epoche.es

The listed certificates form a valid certification path. The root certificate is available in pem format.

25.2.4.2 Procedure

The procedure is identical to the one defined for Test 1.

25.2.4.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

25.2.4.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 4** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 4** activity.

25.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to this FCS_TLSC_EXT.1.3.

26 FCS_TLSC_EXT.2.1

The assurance activity for the **FCS_TLSC_EXT.2.1** requirement is stated as follows:

> The evaluator will verify that TSS describes support for the Supported Groups Extension and whether the required behavior is performed by default or may be configured. If the TSS indicates that support for the Supported Groups Extension must be configured to meet the requirement, the evaluator will verify that AGD guidance includes configuration instructions for the Supported Groups Extension.
>
> The evaluator will also perform the following test:
>
> The evaluator will configure a server to perform ECDHE key exchange using each of the TOE's supported curves and shall verify that the TOE successfully connects to the server.

26.1 Documentation Review activity

26.1.1 Findings

Section **6.2.3.1 TLS, HTTPS, DTLS, EAP-TLS** of the ***Security Target*** document states that Windows automatically includes the Elliptic Curve Extension as part of the Client Hello message. The elliptic curves supported by default are *secp256r1* and *secp384r1*. The elliptic curve *secp521r1* is disabled by default, but it can be enabled by following the ***Operational Guidance***.

Concretely, section **4.3.6 Configuring with group policy** of the ***Operational Guidance*** indicates that the Local Policy Editor can be used to configure the curves in the Elliptic Curve Extension by editing the ECC Curve Order list, enabling and ordering the desired cipher suites.

26.1.2 Verdict

The evaluator considers that the evidences defined above and obtained during the documentation review demonstrate the fulfilment of the requirement established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the documentation review activity.

26.2 Test Activity

To perform the TLS tests required by the Assurance Activities and check their correct outcome, different pieces of software were used:

1. Software acting as a TLS server:

   a. *ee-tls-tool*, a command line tool developed by the evaluation laboratory in order to create a TLS server which is automatically configured prior each test case execution.

2. Software acting as a client from the TOE

   b. *W10ClientAutomator.ps1*, a Powershell script which automatically configures the TOE as a client prior each test case execution. This script allows the evaluator execute test cases using:

      i. different web browsers that come bundled with the TOE (i.e. Internet Explorer and Microsoft Edge).

      ii. *TlsClientTest*, a command line tool developed by the evaluation laboratory. This tool provides more information about the concrete point where SSL validation failed in case of connection error.

Information about their suitability for this evaluation is given in the introduction to FCS_ TLSC_EXT.1.1.

26.2.1 Test 1

26.2.1.1 Setup

The following certificates, created automatically by *ee-tls-tool* and installed by \ *W10ClientAutomator.ps1*, shall be used to perform the assurance activities listed on the Protection Profile:

- CN = dekra-test.es

or

- CN = test.epoche.es

The listed certificates form a valid certification path. All certificates are available in pem format.

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Server Machine (Debian 9 Stretch)
- Client Machine (Platforms listed in the ST)

These two machines are in the same network with the following configuration:

- Server Machine, IP = 50.50.50.220
- Client Machine, IP = 50.50.50.210

Server machine contains the openssl software, a test suite for TLS and X509. It can be configured as TLS server. In addition, the *Wireshark* network analyzer is installed on the server machine.

The client machine shall contain the PowerShell script *W10ClientAutomator.ps1* and the *TlsClientTest* tool, which uses the System.Net. Security classes from .Net framework to perform SSL connections, effectively using the authentication mechanism from the OS.

Moreover, the client machine shall have the secure configuration enabled, according to the section **3.2 Operational prerequisites** of the ***Operational Guidance***.

26.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

26.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

26.2.1.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 1** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 1** activity.

26.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to this FCS_TLSC_EXT.2.1.

27 FCS_TLSC_EXT.3.1

The assurance activity for the **FCS_TLSC_EXT.3.1** requirement is stated as follows:

> The evaluator will verify that TSS describes the signature_algorithm extension and whether the required behavior is performed by default or may be configured. If the TSS indicates that the signature_algorithm extension must be configured to meet the requirement, the evaluator will verify that AGD guidance includes configuration of the signature_algorithm extension.
>
> The evaluator will also perform the following test:
>
> The evaluator will configure the server to send a certificate in the TLS connection that is not supported according to the Client's HashAlgorithm enumeration within the signature_algorithms extension (for example, send a certificate with a SHA-1 signature). The evaluator will verify that the OS disconnects after receiving the server's Certificate handshake message.

27.1 Documentation Review activity

27.1.1 Findings

Section **6.2.3.1 TLS, HTTPS, DTLS, EAP-TLS** of the ***Security Target*** document states that Windows uses the following signature algorithms by default in the "Client Hello" message:

- SHA256
- SHA384
- SHA512

It is also stated that this list of accepted algorithms can be modified by editing a registry key. Section **4.3.8 Managing signature algorithms and key length with the Windows registry** of the ***Operational Guidance*** document provides the concrete key where the status and order of these algorithms can be modified, which is:

- HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Control \ \Cryptography \Configuration \Local \SSL \00010003

Therefore, this allows the user to set up the evaluated configuration by disabling SHA1 for TLS connections.

27.1.2 Verdict

The evaluator considers that the evidences defined above and obtained during the documentation review demonstrate the fulfilment of the requirement established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the documentation review activity.

27.2 Test Activity

To perform the TLS tests required by the Assurance Activities and check their correct outcome, different pieces of software were used:

1. Software acting as a TLS server:
   a. *ee-tls-tool*, a command line tool developed by the evaluation laboratory in order to create a TLS server which is automatically configured prior each test case execution.
2. Software acting as a client from the TOE
   b. *W10ClientAutomator.ps1*, a Powershell script which automatically configures the TOE as a client prior each test case execution. This script allows the evaluator execute test cases using:
      i. different web browsers that come bundled with the TOE (i.e. Internet Explorer and Microsoft Edge).
      ii. *TlsClientTest*, a command line tool developed by the evaluation laboratory. This tool provides more information about the concrete point where SSL validation failed in case of connection error.

Information about their suitability for this evaluation is given in the introduction to FCS_ TLSC_EXT.1.1.

27.2.1 Test 1

27.2.1.1 Setup

The following certificates, created automatically by *ee-tls-tool* and installed by W10ClientAutomator shall be used to perform the assurance activities listed on the Protection Profile:

- CN = EE Test Root CA
- CN = test.epoche.es
- CN = EE Client
- CN = MyNewCert

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Server Machine (Debian 9 Stretch)
- Client Machine (Platforms listed in the ST)

These two machines are in the same network with the following configuration:

- Server Machine, IP = 50.50.50.220
- Client Machine, IP = 50.50.50.210

Server machine contains the *ee-tls-tool* software, a test suite for TLS and X509 Common Criteria evaluations. It acts as a TLS server configured according to each test. In addition, the *Wireshark* network analyzer is installed on the server machine.

The client machine shall contain the PowerShell script *W10ClientAutomator.ps1* and the *TlsClientTest* tool, which uses the System.Net. Security classes from .Net framework to perform SSL connections, effectively using the authentication mechanism from the OS.

Moreover, the client machine shall have the secure configuration enabled, according to the section **3.2 Operational prerequisites** of the ***Operational Guidance***.

27.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

27.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

27.2.1.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 1** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 1** activity.

27.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to this FCS_TLSC_EXT.3.1.

28 FCS_TLSC_EXT.4.1

The assurance activity for the **FCS_TLSC_EXT.4.1** requirement is stated as follows:

> The evaluator will ensure that the TSS description required per FIA_X509_EXT.2.1 includes the use of client-side certificates for TLS mutual authentication.
>
> The evaluator will verify that the AGD guidance required per FIA_X509_EXT.2.1 includes instructions for configuring the client-side certificates for TLS mutual authentication.
>
> The evaluator will also perform the following test:
>
> - **Test 1**: The evaluator shall establish a connection to a peer server that is not configured for mutual authentication (i.e. does not send Server's Certificate Request (type 13) message). The evaluator observes the negotiation of a TLS channel and confirms that the TOE did not send Client's Certificate message (type 11) during handshake.
> - **Test 2**: The evaluator shall establish a connection to a peer server with a shared trusted root that is configured for mutual authentication (i.e. it sends Server's Certificate Request (type 13) message). The evaluator observes negotiation of a TLS channel and confirms that the TOE responds with a non-empty client's Certificate message (type 11) and Certificate Verify (type 15) message.

28.1 Documentation Review activity

28.1.1 Findings

Section **6.2.3.1 TLS, HTTPS, DTLS, EAP-TLS** of the ***Security Target*** document states that:

> *"The TOE implements TLS to enable a trusted network path that is used for client and server authentication, as well as HTTPS"*

Also, section **4.2.1 Client certificates and Certificate Authorities** of the ***Operational Guidance*** document includes the indicated steps needed to import a certificate, valid for client certificates.

28.1.2 Verdict

The evaluator considers that the evidences defined above and obtained during the documentation review demonstrate the fulfilment of the requirement established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the documentation review activity.

28.2 Test Activity

To perform the TLS tests required by the Assurance Activities and check their correct outcome, different pieces of software were used:

1. Software acting as a TLS server:

   a. *ee-tls-tool*, a command line tool developed by the evaluation laboratory in order to create a TLS server which is automatically configured prior each test case execution.

2. Software acting as a client from the TOE

   b. *W10ClientAutomator.ps1*, a Powershell script which automatically configures the TOE as a client prior each test case execution. This script allows the evaluator execute test cases using:

      i. different web browsers that come bundled with the TOE (i.e. Internet Explorer and Microsoft Edge).

      ii. *TlsClientTest*, a command line tool developed by the evaluation laboratory. This tool provides more information about the concrete point where SSL validation failed in case of connection error.

Information about their suitability for this evaluation is given in the introduction to FCS_TLSC_EXT.1.1.

28.2.1 Test 1

28.2.1.1 Setup

The following certificates, created automatically by *ee-tls-tool* and installed by \ *W10ClientAutomator.ps1*, shall be used to perform the assurance activities listed on the Protection Profile:

- CN = EE Test Root CA
- CN = test.epoche.es

The listed certificates form a valid certification path. The root certificate is available in pem format.

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Server Machine (Debian 9 Stretch)
- Client Machine (Platforms listed in the ST)

These two machines are in the same network with the following configuration:

- Server Machine, IP = 50.50.50.220
- Client Machine, IP = 50.50.50.210

Server machine contains the *ee-tls-tool* software, a test suite for TLS and X509 Common Criteria evaluations. It acts as a TLS server configured according to each test. In addition, the *Wireshark* network analyzer is installed on the server machine.

The client machine shall contain the PowerShell script *W10ClientAutomator.ps1* and the *TlsClientTest* tool, which uses the System.Net. Security classes from .Net framework to perform SSL connections, effectively using the authentication mechanism from the OS.

Moreover, the client machine shall have the secure configuration enabled, according to the section **3.2 Operational prerequisites** of the ***Operational Guidance***.

28.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

28.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

28.2.1.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 1** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 1** activity.

28.2.2 Test 2

28.2.2.1 Setup

The following certificates, created automatically by *ee-tls-tool* and installed by \ *W10ClientAutomator.ps1*, shall be used to perform the assurance activities listed on the Protection Profile:

- CN = EE Test Root CA
- CN = test.epoche.es
- CN = EE Client (client certificate with friendly name “EE Client Certificate”)

The listed certificates form a valid certification path. The root certificate is available in pem format, the client certificate in pfx format, and the other one will be sent by the server.

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Server Machine (Debian 9 Stretch)
- Client Machine (Platforms listed in the ST)

These two machines are in the same network with the following configuration:

- Server Machine, IP = 50.50.50.220
- Client Machine, IP = 50.50.50.210

Server machine contains the *ee-tls-tool* software, a test suite for TLS and X509 Common Criteria evaluations. It acts as a TLS server configured according to each test. In addition, the *Wireshark* network analyzer is installed on the server machine.

The client machine shall contain the PowerShell script *W10ClientAutomator.ps1* and the *TlsClientTest* tool, which uses the System.Net. Security classes from .Net framework to perform SSL connections, effectively using the authentication mechanism from the OS.

Moreover, the client machine shall have the secure configuration enabled, according to the section **3.2 Operational prerequisites** of the ***Operational Guidance***.

28.2.2.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

28.2.2.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE’s behavior is as expected and detailed in the security target [ST004].

28.2.2.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 2** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 2** activity.

28.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to this FCS_TLSC_EXT.4.1.

29 FDP_ACF_EXT.1.1

The assurance activity for the **FDP_ACF_EXT.1.1** requirement is stated as follows:

> The evaluator will confirm that the TSS comprehensively describes the access control policy enforced by the OS. The description must include the rules by which accesses to particular files and directories are determined for particular users. The evaluator will inspect the TSS to ensure that it describes the access control rules in such detail that given any possible scenario between a user and a file governed by the OS the access control decision is unambiguous.
>
> The evaluator will create two new standard user accounts on the system and conduct the following tests:
>
> - **Test 1:** The evaluator will authenticate to the system as the first user and create a file within that user's home directory. The evaluator will then log off the system and log in as the second user. The evaluator will then attempt to read the file created in the first user's home directory. The evaluator will ensure that the read attempt is denied.
> - **Test 2:** The evaluator will authenticate to the system as the first user and create a file within that user's home directory. The evaluator will then log off the system and log in as the second user. The evaluator will then attempt to modify the file created in the first user's home directory. The evaluator will ensure that the modification is denied.
> - **Test 3:** The evaluator will authenticate to the system as the first user and create a file within that user's user directory. The evaluator will then log off the system and log in as the second user. The evaluator will then attempt to delete the file created in the first user's home directory. The evaluator will ensure that the deletion is denied.
> - **Test 4:** The evaluator will authenticate to the system as the first user. The evaluator will attempt to create a file in the second user's home directory. The evaluator will ensure that the creation of the file is denied.
> - **Test 5:** The evaluator will authenticate to the system as the first user and attempt to modify the file created in the first user's home directory. The evaluator will ensure that the modification of the file is accepted.
> - **Test 6:** The evaluator will authenticate to the system as the first user and attempt to delete the file created in the first user's directory. The evaluator will ensure that the deletion of the file is accepted.

29.1 Documentation Review Activity

29.1.1 Findings

The evaluator has reviewed the section **6.3.1. Discretionary Access Control** of the ***Security Target*** document, which is related to the access control policy and how these policies are applied to files and folders in the operating system.

This section is composed by the following main subsections:

- 6.3.1.1 Subject DAC Attributes
- 6.3.1.2 Object DAC Attributes
- 6.3.1.3 DAC Enforcement Algorithm
- 6.3.1.4 Default DAC Protection

The first and second subsections include a brief description about the security attributes for a subject and for an object.

The third one includes a step-by-step description about the algorithm used to determine whether a user has access to one file or not. This section also includes information regarding the kind of permissions that are checked at each step of the algorithm.

The fourth one includes information about the default access rules assigned to all new objects. This section also includes information about how the inheritance rules work.

Finally, the following subsections are also included in the **6.3.1. Discretionary Access Control** section.

- 6.3.1.5 DAC Management
- 6.3.1.6 Reference Mediation

In these subsections it is described the functions that manages the DACL and how the system obtains a handle for the objects.

29.1.2 Verdict

The evaluator has reviewed the information provided in the TSS section **6.3.1. Discretionary Access Control** and considers that the access control policies enforced by the operating system are properly described. This description contains enough information to allow the evaluator determine how the access control policies are applied to folders and files in the operating system, allowing or denying the access.

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfilment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

29.2 Test Activity

Throughout the following tests, attempts to create, read, write and delete a test file will be performed using different users and permissions.

29.2.1 Test 1, Test 2, Test 3, Test 4, Test 5 and Test 6

29.2.1.1 Setup

Before the test execution, the following setup condition must be fulfilled:

- User accounts with user names *userFDP1* and *userFDP2* shall not exist.
- The *PowerShell* execution policy shall be configured to allow the execution of *PowerShell* scripts. To do it, execute in a *Powershell* terminal with administrator rights the command:

  ```
  Set-ExecutionPolicy Unrestricted -Force
  ```

- Script *FDP_ACF_EXT.ps1* shall be available.

29.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

29.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Panasonic CF-33 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R840 with Azure Stack Edge (build 10.0.17784.1068)
- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)

- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Voyager Klaas Telecom with Azure Stack Hub (build 10.0.17784.1068)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

29.2.1.4 Verdict

As it can be observed in the above section, the obtained behaviours match with the ones described in the assurance activity section. Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 1, Test 2, Test 3, Test4, Test 5 and Test 6** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1, Test 2, Test 3, Test 4, Test 5 and Test 6**.

29.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FDP_ACF_EXT.1.1.

30 FIA_AFL.1.1

The assurance activity for the **FIA_AFL.1.1** requirement is stated as follows:

> The evaluator will set an administrator-configurable threshold for failed attempts, or note the ST-specified assignment. The evaluator will then (per selection) repeatedly attempt to authenticate with an incorrect password, PIN, or certificate until the number of attempts reaches the threshold. Note that the authentication attempts and lockouts must also be logged as specified in FAU_GEN.1.

30.1 Documentation Review Activity

30.1.1 Findings

The related assurance activity does not define any action for this requirement.

30.1.2 Verdict

The related assurance activity does not define any action for this requirement. Therefore, the **PASS** verdict is assigned to the documentation review activity.

30.2 Test Activity

The assurance activity states that a threshold for failed authentication attempts shall be configured by the OS administrator. After that, the evaluator will then repeatedly attempt to authenticate with an incorrect password until the threshold is reached.

This test is done at the same time as *FIA_AFL1.2* requirement.

30.2.1 Test

30.2.1.1 Setup

The applicable setup for this test is covered in the Test Activity section for *FIA_AFL.1.2* requirement.

30.2.1.2 Procedure

This test is done at the same time as *FIA_AFL1.2*.

30.2.1.3 Results

The results for this test are included in the Test Activity section for *FIA_AFL.1.2* requirement.

30.2.1.4 Verdict

The verdict for this test is assigned in the Test Activity section for FIA_AFL.1.2 requirement.

30.3 Final Verdict

The final verdict for this requirement is assigned in Test Activity section for the FIA_AFL.1.2 requirement.

31 FIA_AFL.1.2

The assurance activity for the **FIA_AFL.1.2** requirement is stated as follows:

> **Test 1:** The evaluator will attempt to authenticate repeatedly to the system with a known bad password. Once the defined number of failed authentication attempts has been reached the evaluator will ensure that the account that was being used for testing has had the actions detailed in the assignment list above applied to it. The evaluator will ensure that an event has been logged to the security event log detailing that the account has had these actions applied.
>
> **Test 2:** The evaluator will attempt to authenticate repeatedly to the system with a known bad certificate. Once the defined number of failed authentication attempts has been reached the evaluator will ensure that the account that was being used for testing has had the actions detailed in the assignment list above applied to it. The evaluator will ensure that an event has been logged to the security event log detailing that the account has had these actions applied.
>
> **Test 3:** The evaluator will attempt to authenticate repeatedly to the system using both a bad password and a bad certificate. Once the defined number of failed authentication attempts has been reached the evaluator will ensure that the account that was being used for testing has had the actions detailed in the assignment list above applied to it. The evaluator will ensure that an event has been logged to the security event log detailing that the account has had these actions applied.

31.1 Documentation Review Activity

31.1.1 Findings

The related assurance activity does not define any action for this requirement.

31.1.2 Verdict

The related assurance activity does not define any action for this requirement. Therefore, the **PASS** verdict is assigned to the documentation review activity.

31.2 Test Activity

During this test, the evaluator will attempt to authenticate repeatedly to the system with a known bad password. Once the threshold for failed authentication attempts limit is reached, the evaluator will ensure that the account is locked. In addition, the audit events will be analysed to demonstrate the fulfilment of the requirement *FAU_GEN.1* related with lock and unlock of user accounts.

31.2.1 Test 1

31.2.1.1 Setup

Before the test execution, the following setup conditions must be fulfilled:

- A user account with user name *userFIA* shall not exist.
- An administrator account shall be available.
- The *PowerShell* execution policy shall be configured to allow the execution of *PowerShell* scripts. To do it, execute in a *Powershell* terminal with administrator rights the command:

  ```
  Set-ExecutionPolicy Unrestricted -Force
  ```

- Scripts *FIA_AFL_1_2_Setup.ps1* and *FIA_AFL_1_2_Audit.ps1* shall be available.
- Additionally, for OE-protected storage, Windows 10 and Windows 11 can authenticate users with a Windows Hello PIN which is backed by a TPM. The evaluated platforms with a valid TPM must be configured with Windows Hello PIN authentication too.

For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions, the computer shall be domain-joined and the domain user '*standard*' shall be created. These platforms does not support Windows Hello PIN.

31.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

31.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Panasonic CF-33 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R840 with Azure Stack Edge (build 10.0.17784.1068)

- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- HPE Edgeline EL8000 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

31.2.1.4 Verdict

The evaluator has performed invalid authentication attempts using a known bad password or PIN until the configured threshold has been reached. Once the user account has been locked, the evaluator has unlocked this account using a user account with administrator rights.

As the above images state, the user account has been locked successfully after the configured threshold is reached. Additionally, both invalid authentication attempts and the account lockout events have been audited as specified in *FAU_GEN.1*.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

31.2.2 Test 2 & Test 3

31.2.2.1 Setup

These tests are not applicable in this evaluation due to the selection made for the SFR definition in the final version of the ***Security Target*** document.

31.2.2.2 Procedure

These tests are not applicable in this evaluation due to the selection made for the SFR definition in the final version of the ***Security Target*** document.

31.2.2.3 Results

These tests are not applicable in this evaluation due to the selection made for the SFR definition in the final version of the ***Security Target*** document.

31.2.2.4 Verdict

These tests are not applicable in this evaluation due to the selection made for the SFR definition in the final version of the ***Security Target*** document.

31.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FIA_AFL.1.1 and FIA_AFL.1.2.

32 FIA_UAU.5.1

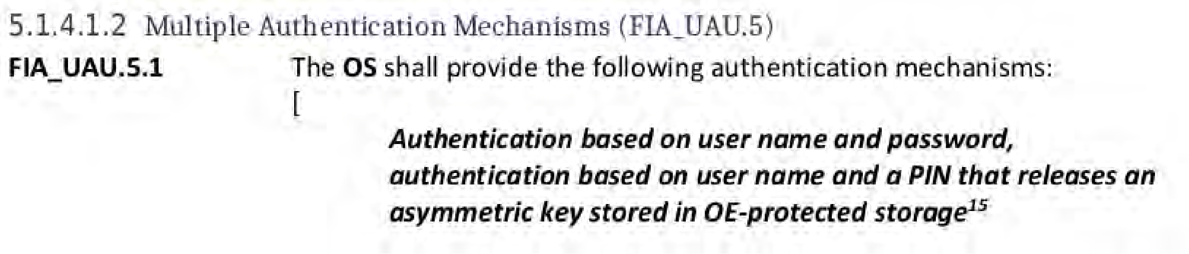
The assurance activity for the **FIA_UAU.5.1** requirement is stated as follows:

> If user name and password authentication is selected, the evaluator will configure the OS with a known user name and password and conduct the following tests:
>
> - **Test 1:** The evaluator will attempt to authenticate to the OS using the known user name and password. The evaluator will ensure that the authentication attempt is successful.
> - **Test 2:** The evaluator will attempt to authenticate to the OS using the known user name but an incorrect password. The evaluator will ensure that the authentication attempt is unsuccessful.
>
> If user name and PIN that releases an asymmetric key is selected, the evaluator will examine the TSS for guidance on supported protected storage and will then configure the TOE or OE to establish a PIN which enables release of the asymmetric key from the protected storage (such as a TPM, a hardware token, or isolated execution environment) with which the OS can interface. The evaluator will then conduct the following tests:
>
> - **Test 1:** The evaluator will attempt to authenticate to the OS using the known user name and PIN. The evaluator will ensure that the authentication attempt is successful.
> - **Test 2:** The evaluator will attempt to authenticate to the OS using the known user name but an incorrect PIN. The evaluator will ensure that the authentication attempt is unsuccessful.
>
> If X.509 certificate authentication is selected, the evaluator will generate an X.509v3 certificate for a user with the Client Authentication Enhanced Key Usage field set. The evaluator will provision the OS for authentication with the X.509v3 certificate. The evaluator will ensure that the certificates are validated by the OS as per FIA_X509_EXT.1.1 and then conduct the following tests:
>
> - **Test 1:** The evaluator will attempt to authenticate to the OS using the X.509v3 certificate. The evaluator will ensure that the authentication attempt is successful.
> - **Test 2:** The evaluator will generate a second certificate identical to the first except for the public key and any values derived from the public key. The evaluator will attempt to authenticate to the OS with this certificate. The evaluator will ensure that the authentication attempt is unsuccessful.

32.1 Documentation Review Activity

32.1.1 Findings

The ***Security Target*** document, defines the available authentication mechanisms available in its section **5.1.4.1.2 Multiple Authentication Mechanisms (FIA_UAU.5)**.



5.1.4.1.2 Multiple Authentication Mechanisms (FIA_UAU.5)

FIA_UAU.5.1 The **OS** shall provide the following authentication mechanisms:
[

Authentication based on user name and password, authentication based on user name and a PIN that releases an asymmetric key stored in OE-protected storage[15]

The evaluator has reviewed the respective TSS section (**6.4 Identification and Authentication**) of the ***Security Target*** document, where it is described which authentication mechanism is supported by each Windows OS edition. From the previous section, the following information can be extracted:

- All Windows editions supports authentication based on username and password.
- Additionally, for OE-protected storage, Windows 10 & Windows 11 can authenticate users with a Windows Hello PIN which is backed by a TPM.
- For Windows 10, Windows 11, Windows Server 2022, Azure Stack Hub and Azure Stack Edge editions, a physical/virtual smart card can be also used.

In addition, the ***Operational Guidance*** document, includes also in its section **4.8 Managing authentication methods** the necessary information and supporting documentation to set up or configure the environment for each authentication mechanism.

32.1.2 Verdict

The evaluator has reviewed the ***Security Target*** document and has reviewed each authentication mechanism available and the information on the TSS about the supported protected storage. Moreover, the ***Operational Guidance*** document, has been also analysed, checking the setup and configuration procedures for each authentication mechanism.

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfilment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

32.2 Test Activity

The evaluator will attempt authenticate to the OS using a known user name and the correct password or PIN. Then the evaluator will repeat the process using a known user name but an incorrect password or PIN. The evaluator will ensure that the authentication is successful in the first test and fails in the second.

32.2.1 Test 1 & Test 2 - Username and password

32.2.1.1 Setup

Before the test execution, the following setup condition must be fulfilled:

- A standard user account with user name *userFIA* shall not exist.
- The *PowerShell* execution policy shall be configured to allow the execution of *PowerShell* scripts. To do it, execute in a *Powershell* terminal with administrator rights the command:

  ```
  Set-ExecutionPolicy Unrestricted -Force
  ```

- Script *FIA_UAU_5_1_Test1and2.ps1* shall be available.

32.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

32.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Panasonic CF-33 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R840 with Azure Stack Edge (build 10.0.17784.1068)
- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)

- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- HPE Edgeline EL8000 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

32.2.1.4 Verdict

The evaluator has performed an authentication attempt using a valid user name and password that has been completed successfully. Afterwards, the evaluator has performed another authentication attempt but this time, using an invalid password, ensuring that this authentication attempt failed.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 1 and Test 2 - Username and password** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1 and Test 2 - Username and password**.

32.2.2 Test 1 & Test 2 - Username and a PIN that releases an asymmetric key stored in OE-protected storage (TPM)

32.2.2.1 Setup

Before the test execution, the following setup condition must be fulfilled:

- A standard user account with user name *userFIA* shall exist. This account shall belong to default *Users* group.
- The platform to be tested shall count with a TPM or a virtual TPM.

- The *PowerShell* execution policy shall be configured to allow the execution of *PowerShell* scripts. To do it, execute in a *Powershell* terminal with administrator rights the command:

  ```
  Set-ExecutionPolicy Unrestricted -Force
  ```

- Script *FIA_UAU_5_1_Test1and2_PIN.ps1* shall be available.

Note: The following procedure cannot be performed on Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions.

32.2.2.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

32.2.2.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Panasonic CF-33 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R840 with Azure Stack Edge (build 10.0.17784.1068)
- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- HPE Edgeline EL8000 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)

- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

32.2.2.4 Verdict

The evaluator has performed an authentication attempt using the user name and the correct PIN and it has been completed successfully. Afterwards, the evaluator has performed other authentication attempt, but this time using an invalid PIN. The evaluator has ensured that the authentication attempt is invalid.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 1 and Test 2 - Username and a PIN (TPM)** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1 and Test 2 - Username and a PIN (TPM)**.

32.2.3 Test 1 & Test 2 - Username and a PIN that releases an asymmetric key stored in OE-protected storage (Smart Card)

32.2.3.1 Setup

To do this test, the evaluator shall have set a Public Key Infrastructure as well as access to the PIV/CAC smart cards.

To perform this test, the evaluated platforms shall be joined to the domain controller.

This test is not applicable for Windows Server 21H2 and Azure Stack HCIv2 operating systems.

Before the test execution, the following setup condition must be fulfilled:

- The *PowerShell* execution policy shall be configured to allow the execution of *PowerShell* scripts. To do it, execute in a *Powershell* terminal with administrator rights the command:

  ```
  Set-ExecutionPolicy Unrestricted -Force
  ```

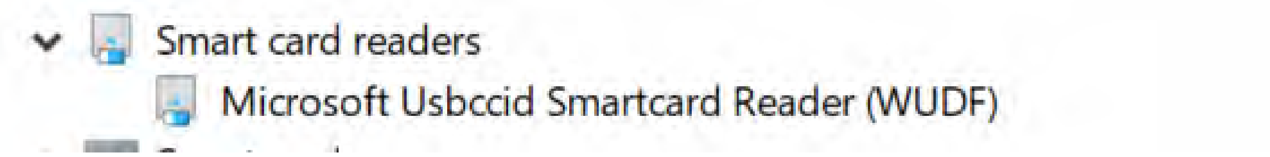
- Script *FIA_UAU_5_1_Test1and2_SC.ps1* shall be available.
- The evaluated platform must be joined to a domain. The steps required to join a computer to a domain are described in *Test 11* for *FMT_MOF_EXT.1* requirement.

Once the evaluated platform has been joined to the domain controller, the following steps must be performed according to the authentication method used (physical smart card or virtual smart card).

32.2.3.1.1 Authentication using a physical smart card

The following steps must be carried out by the evaluator in order to configure the authentication using physical smart cards:

- Login the user account that will be used and connect the smart card reader to the computer. To check that the drivers are correctly installed go to *Device Manager* (*WIN + X, then press m key*). The information about the smart card reader and the smart card shall be displayed here:



  Note: Physical Smart card issues may arise related to the drivers for the smart card or the smart card itself.

  If this is the case, go to the device vendor website or the *Microsoft Update Catalog* to download and install the latest drivers.

  For example, for a *Gemalto IdPrime* card, the drivers can be found in the *Microsoft Update Catalog* using the device manufacture (*Gemalto*) as the query parameter:

  Microsoft Update Catalog for Gemalto

  The files downloaded with .cab extension must be extracted and used to install the drivers for *'Unknown smart card'* in Computer Managment/Device Manager. After that, the Smart card shall be immediately available for log in on TOE.

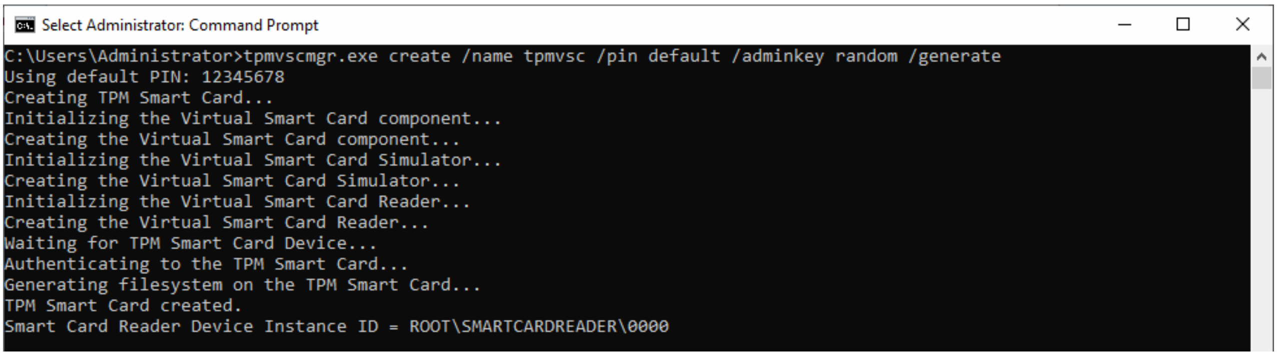
32.2.3.1.2 Authentication using a virtual smart card

The following steps must be carried out by the evaluator to configure the authentication using virtual smart cards:

- Open a Command Line terminal with administrator rights and type the following command to create a virtual smart card.

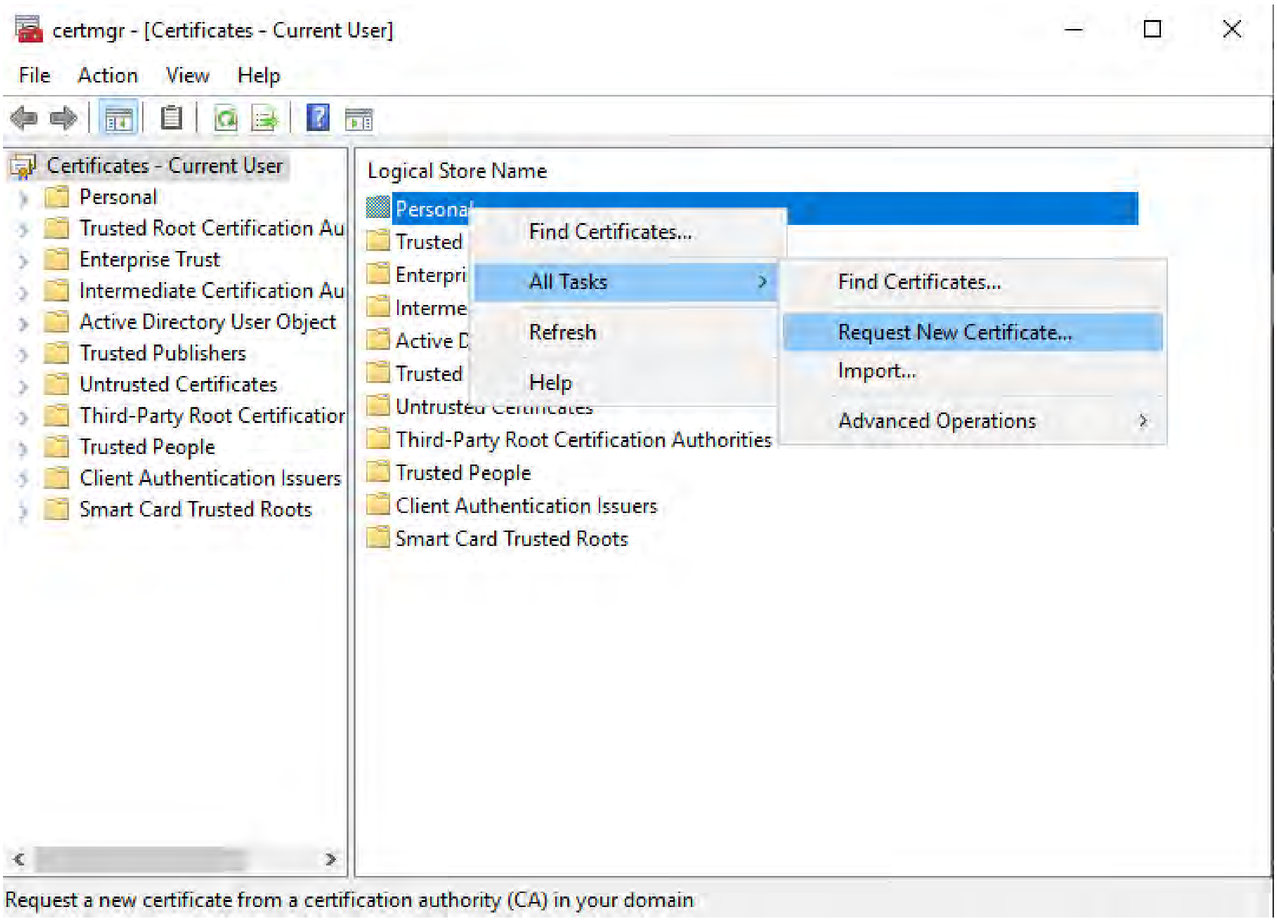
  ```
  tpmvscmgr.exe create /name tpmvsc /pin default /adminkey random /generate
  ```

- This command only works in platforms with a valid TPM. The default PIN for the virtual smart card is *123456768*.



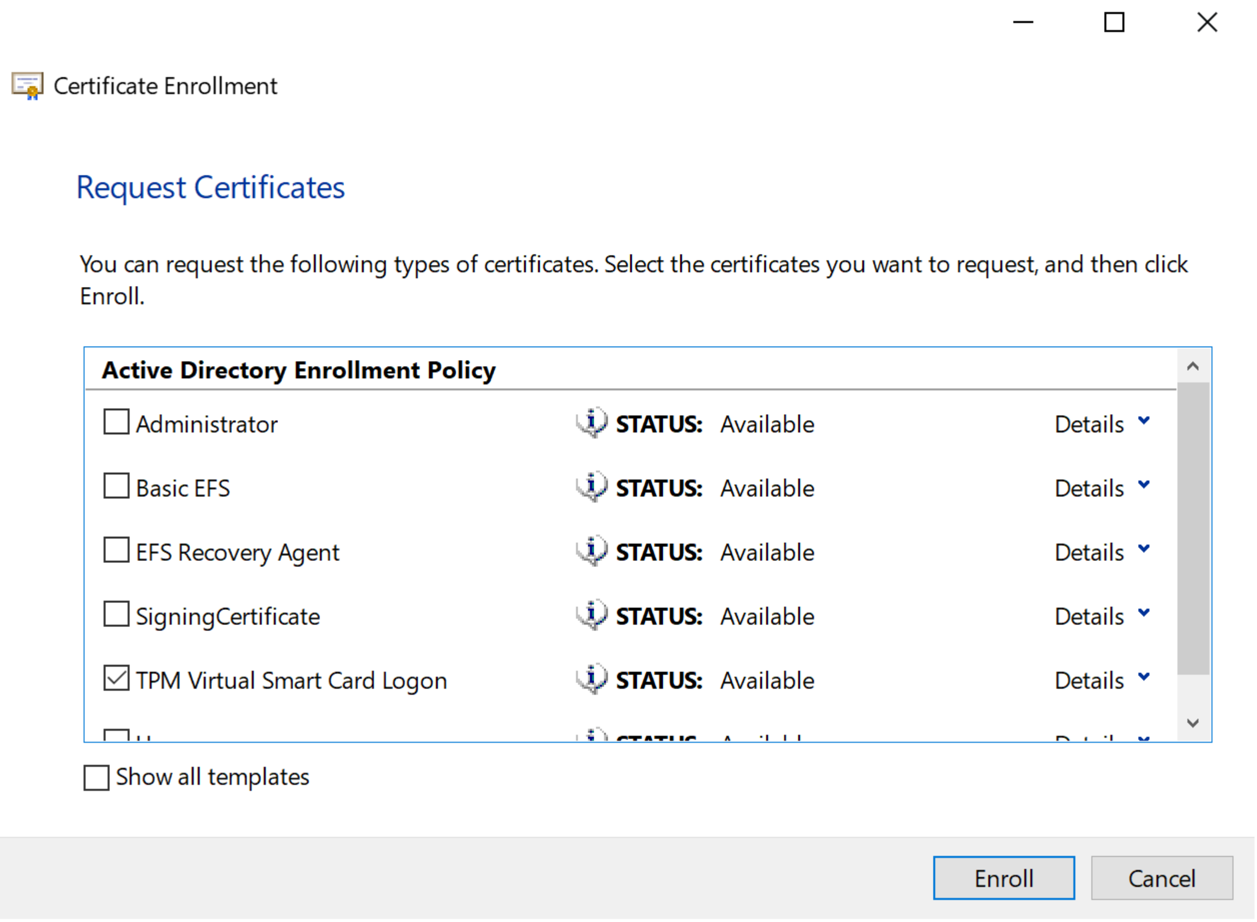
```
C:\Users\Administrator>tpmvscmgr.exe create /name tpmvsc /pin default /adminkey random /generate
Using default PIN: 12345678
Creating TPM Smart Card...
Initializing the Virtual Smart Card component...
Creating the Virtual Smart Card component...
Initializing the Virtual Smart Card Simulator...
Creating the Virtual Smart Card Simulator...
Initializing the Virtual Smart Card Reader...
Creating the Virtual Smart Card Reader...
Waiting for TPM Smart Card Device...
Authenticating to the TPM Smart Card...
Generating filesystem on the TPM Smart Card...
TPM Smart Card created.
Smart Card Reader Device Instance ID = ROOT\SMARTCARDREADER\0000
```

- Enroll the certificate to the virtual smart card with the help of the *Certificate Manager* tool (*WIN + R* and then type *certmgr.msc*).
- Then right-click over *Personal*, and select *All Task -> Request New Certificate*.



Request a new certificate from a certification authority (CA) in your domain

- Follow the wizard, clicking the *'Next'* button twice, on the *'Request Certificates'* screen select *'TPM Virtual Smart Card Logon'* and *'Enroll'*, Enter the PIN when asked.



Certificate Enrollment

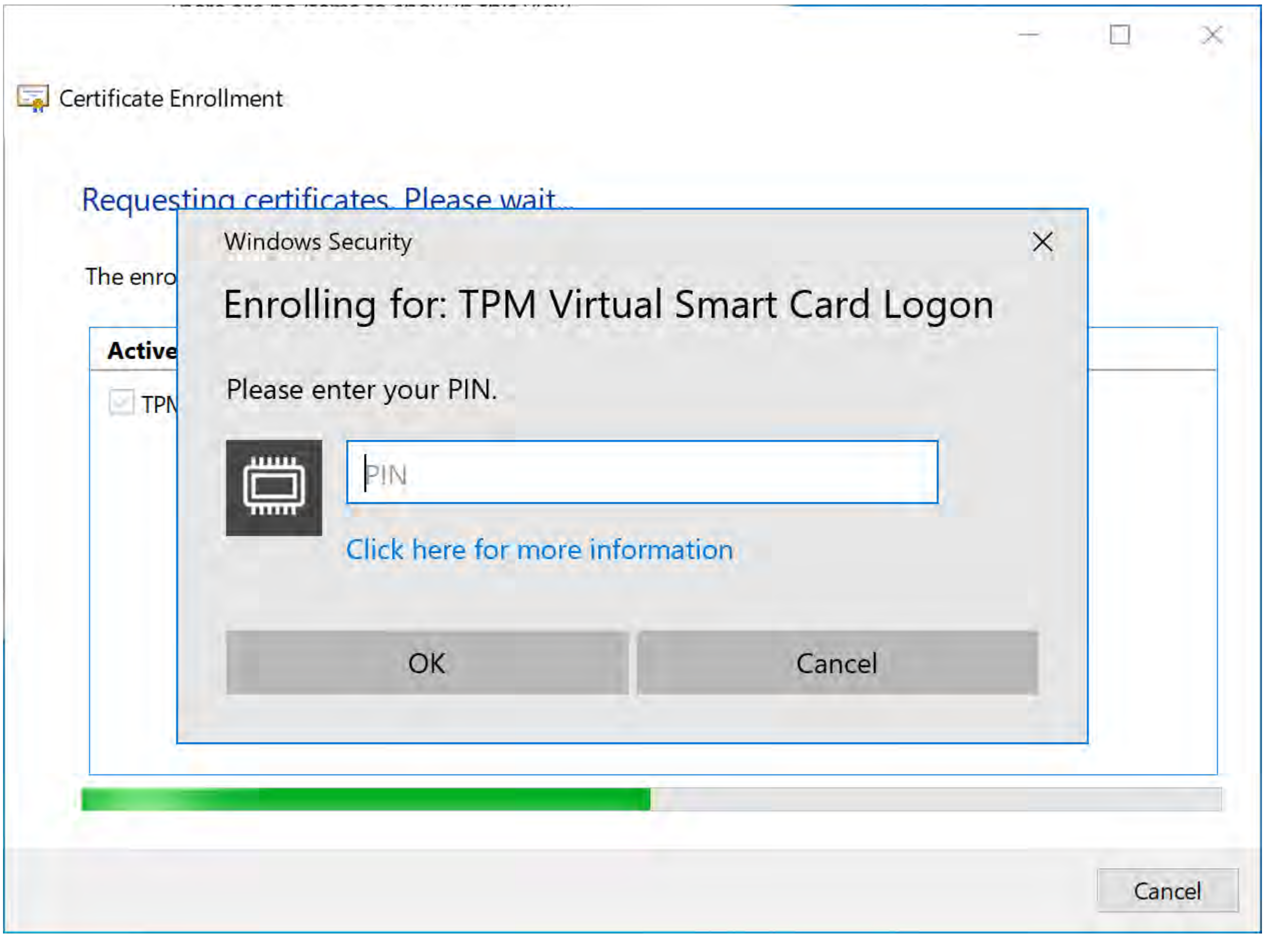
Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

Active Directory Enrollment Policy

□ Administrator	**STATUS:** Available	Details
□ Basic EFS	**STATUS:** Available	Details
□ EFS Recovery Agent	**STATUS:** Available	Details
□ SigningCertificate	**STATUS:** Available	Details
☑ TPM Virtual Smart Card Logon	**STATUS:** Available	Details

□ Show all templates



Certificate Enrollment

Requesting certificates. Please wait...

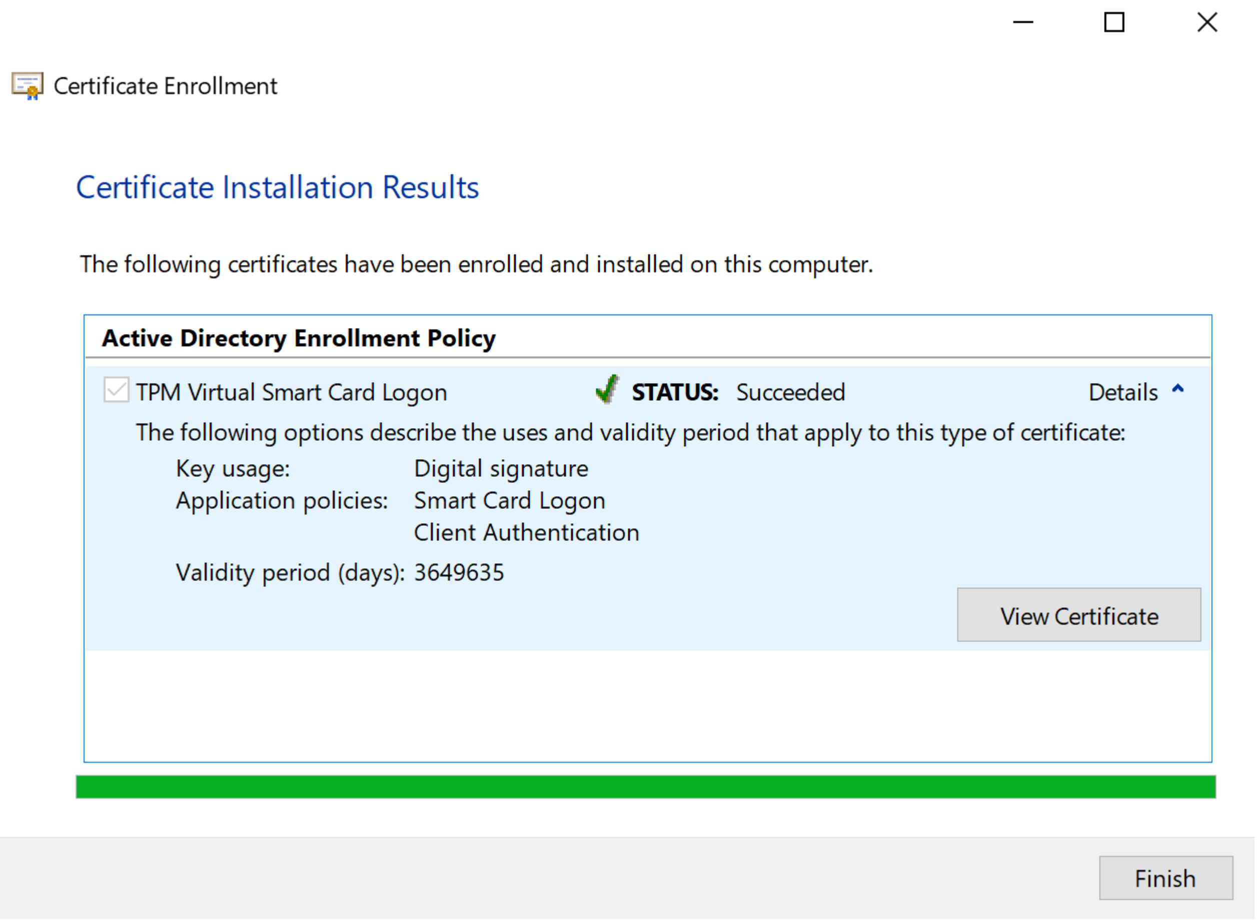
The enro

Windows Security

Enrolling for: TPM Virtual Smart Card Logon

Please enter your PIN.

- If the process has been completed successfully, the following screen shall be shown.



Certificate Enrollment

Certificate Installation Results

The following certificates have been enrolled and installed on this computer.

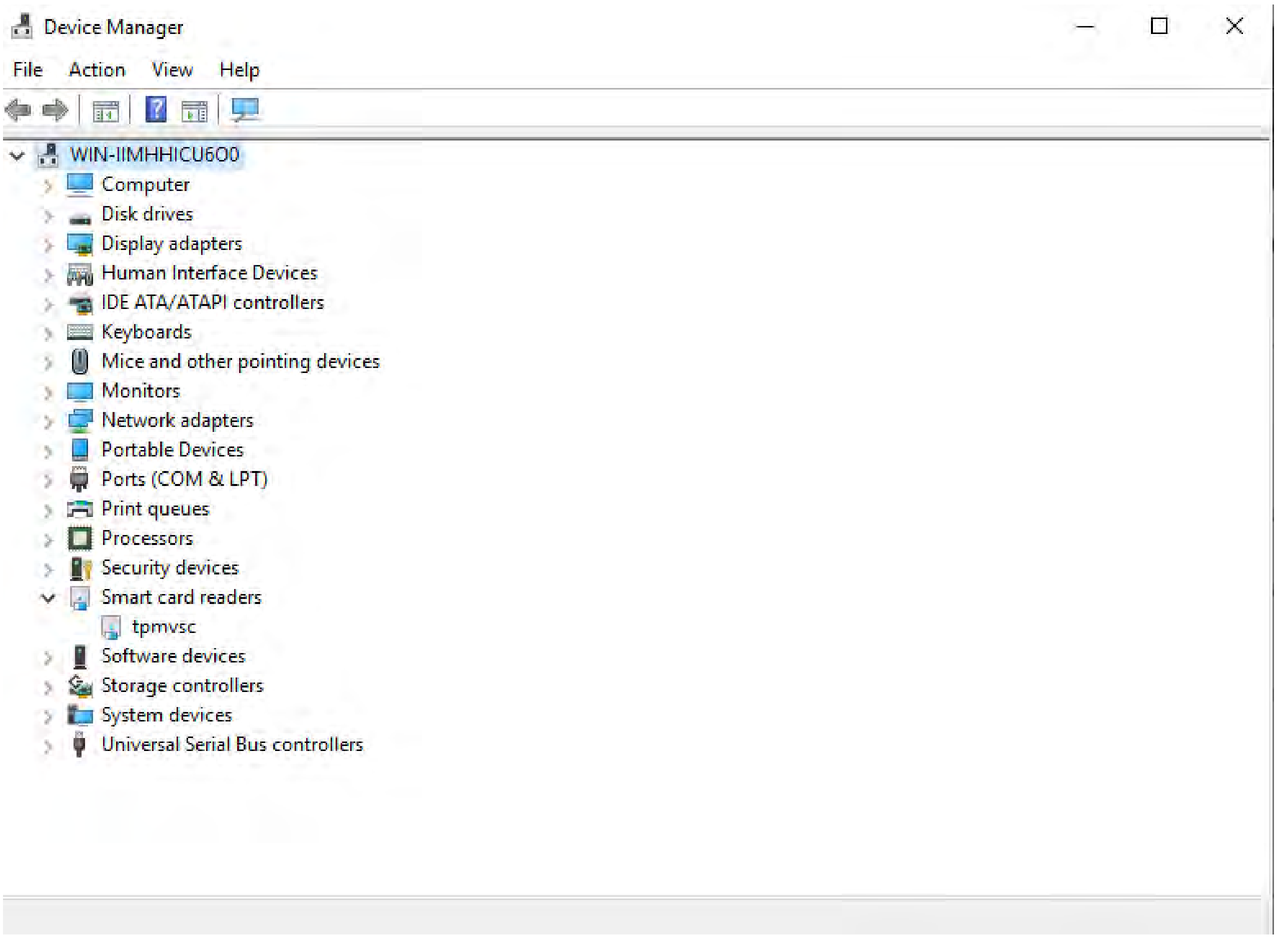
Active Directory Enrollment Policy

☑ TPM Virtual Smart Card Logon ✓ **STATUS:** Succeeded Details ^

The following options describe the uses and validity period that apply to this type of certificate:

Key usage: Digital signature
Application policies: Smart Card Logon
Client Authentication
Validity period (days): 3649635

- To check that the virtual smart card ready is correctly deployed, go to the *Device Manager* tool (*WIN + X, then press m key*). The information about the virtual smart card reader shall be as follows:



- Sign out to go back the login screen.

32.2.3.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

32.2.3.3 Results

The evaluator has performed this test on all the canonical platforms (except the ones not applicable described in the setup section) as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)

- Panasonic CF-33 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R840 with Azure Stack Edge (build 10.0.17784.1068)

The evaluator has obtained the same results in all tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

32.2.3.4 Verdict

The evaluator has performed an authentication attempt using the correct smart card credentials (*User name and PIN*) and it has been completed successfully. Afterwards, the evaluator has performed another authentication attempt, but this time, using an incorrect smart card credential (*Invalid PIN*). The evaluator has ensured that the authentication attempt is invalid.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 1 and Test 2 - Username and a PIN (Smart Card)** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1 and Test 2 - Username and a PIN (Smart Card)**.

32.2.4 Test 1 & Test 2 - X.509 Certificates

32.2.4.1 Setup

These tests are not applicable in this evaluation due to the assignment made for the SFR definition in the final version of the ***Security Target*** document.

32.2.4.2 Procedure

These tests are not applicable in this evaluation due to the assignment made for the SFR definition in the final version of the ***Security Target*** document.

32.2.4.3 Results

These tests are not applicable in this evaluation due to the assignment made for the SFR definition in the final version of the ***Security Target*** document.

32.2.4.4 Verdict

These tests are not applicable in this evaluation due to the assignment made for the SFR definition in the final version of the ***Security Target*** document.

32.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FIA_UAU.5.1.

33 FIA_UAU.5.2

The assurance activity for the **FIA_UAU.5.2** requirement is stated as follows:

> The evaluator will ensure that the TSS describes each mechanism provided to support user authentication and the rules describing how the authentication mechanism(s) provide authentication.
>
> The evaluator will verify that configuration guidance for each authentication mechanism is addressed in the AGD guidance.
>
> - **Test 1:** For each authentication mechanism selected, the evaluator will enable that mechanism and verify that it can be used to authenticate the user at the specified authentication factor interfaces.
> - **Test 2:** For each authentication mechanism rule, the evaluator will ensure that the authentication mechanism(s) behave as documented in the TSS.

33.1 Documentation Review Activity

33.1.1 Findings

The evaluator has reviewed the ***Security Target*** document, section **6.4 Identification and Authentication**, which contains the following information:

> *Password-based authentication to Windows succeeds when the credential provided by the user matches the stored protected representation of the password; Windows Hello and smart cards both use PIN-based authentication to unlock a protected resource, a private key, the stored representation of the PIN is protected by the Secure Kernel.*
>
> *Password authentication can be used for interactive, service, and network logons and to initiate the "change password" screen; the Windows Hello PIN, physical and virtual smart cards can be used for interactive logons; and the Windows Hello PIN is used to re-authenticate the user when the user chooses to change their PIN.*
>
> *When the authentication succeeds, the user will be logged onto their desktop, their screen unlocked, or their authentication factors changed depending whether the user logged onto the computer, the display was locked, or the PIN or password was to be changed.*

As it can be observed, the provided information includes a description about all the authentication mechanisms supported by the TOE. This section also contains a brief description about the rules describing how the authentication mechanisms work as well as the results of a successful authentication.

Moreover, the ***Operational Guidance*** document, includes the section **4.8 Managing authentication methods**, in which the configuration guidance is addressed for each authentication mechanisms supported by the TOE (password, PIN and Smart Cards).

33.1.2 Verdict

The evaluator has reviewed the ***Security Target*** document and has reviewed the information provided within section **6.4 Identification and Authentication**. This section contains enough information to allow the evaluator to understand how the authentication mechanisms work, as well as, the results of a successful authentication. Moreover, the ***Operational Guidance*** document, also includes configuration guidance for each authentication mechanisms supported by the TOE.

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfilment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

33.2 Test Activity

The evaluator will ensure that each authentication mechanism supported by the OS authenticates the user and behaves as described in the AGD guidance.

33.2.1 Test 1

33.2.1.1 Setup

The applicable setup for this test is covered in the Test Activity section for *FIA_UAU.5.1* requirement.

33.2.1.2 Procedure

This test is done at the same time as *FIA_UAU.5.1*.

33.2.1.3 Results

The results for this test are included in the Test Activity section for *FIA_UAU.5.1* requirement.

33.2.1.4 Verdict

The verdict for this test is assigned in the Test Activity section for *FIA_UAU.5.1* requirement.

33.2.2 Test 2

33.2.2.1 Setup

Before the test execution, the following setup condition must be fulfilled:

- A standard user account with user name *userTest* shall exist. This account shall belong to default *Users* group.

33.2.2.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

33.2.2.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Panasonic CF-33 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R840 with Azure Stack Edge (build 10.0.17784.1068)
- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- HPE Edgeline EL8000 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

The evaluator has obtained the same results in all tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

33.2.2.4 Verdict

The evaluator has managed each authentication method supported. All of them have been properly configured as described in the ***Operational Guidance*** document.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 2** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 2.**

33.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to this FIA_UAU.5.2 requirement.

34 FIA_X509_EXT.1.1

The assurance activity for the **FIA_X509_EXT.1.1** requirement is stated as follows:

> The evaluator will ensure the TSS describes where the check of validity of the certificates takes place. The evaluator ensures the TSS also provides a description of the certificate path validation algorithm.
>
> The tests described must be performed in conjunction with the other certificate services assurance activities, including the functions in FIA_X509_EXT.2.1. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. The evaluator will create a chain of at least four certificates: the node certificate to be tested, two Intermediate CAs, and the self-signed Root CA.
>
> - **Test 1**: The evaluator shall demonstrate that validating a certificate without a valid certification path results in the function failing, for each of the following reasons, in turn: by establishing a certificate path in which one of the issuing certificates is not a CA certificate, by omitting the basicConstraints field in one of the issuing certificates, by setting the basicConstraints field in an issuing certificate to have CA=False, by omitting the CA signing bit of the key usage field in an issuing certificate, and by setting the path length field of a valid CA field to a value strictly less than the certificate path. The evaluator shall then establish a valid certificate path consisting of valid CA certificates, and demonstrate that the function succeeds. The evaluator shall then remove trust in one of the CA certificates, and show that the function fails.
> - **Test 2**: The evaluator will demonstrate that validating an expired certificate results in the function failing.
> - **Test 3**: The evaluator will test that the OS can properly handle revoked certificates - conditional on whether CRL, OCSP, OCSP stapling, or OCSP multi-stapling is selected; if multiple methods are selected, then a test shall be performed for each method. The evaluator will test revocation of the node certificate and revocation of the intermediate CA certificate (i.e. the intermediate CA certificate should be revoked by the root CA). If OCSP stapling per RFC 6066 is the only supported revocation method, testing revocation of the intermediate CA certificate is omitted. The evaluator will ensure that a valid certificate is used, and that the validation function succeeds. The evaluator then attempts the test with a certificate that has been revoked (for each method chosen in the selection) to ensure when the certificate is no longer valid that the validation function fails.
> - **Test 4**: If any OCSP option is selected, the evaluator shall configure the OCSP server or use a man-in-the-middle tool to present a certificate that

does not have the OCSP signing purpose and verify that validation of the OCSP response fails. If CRL is selected, the evaluator shall configure the CA to sign a CRL with a certificate that does not have the cRLsign key usage bit set and verify that validation of the CRL fails.

- **Test 5**: The evaluator shall modify any byte in the first eight bytes of the certificate and demonstrate that the certificate fails to validate. (The certificate will fail to parse correctly.)
- **Test 6**: The evaluator shall modify any byte in the last byte of the certificate and demonstrate that the certificate fails to validate. (The signature on the certificate will not validate.)
- **Test 7**: The evaluator shall modify any byte in the public key of the certificate and demonstrate that the certificate fails to validate. (The signature of the certificate will not validate.)

34.1 Documentation Review activity

34.1.1 Findings

The evaluator has reviewed the section **6.4.1 X.509 Certificate Validation and Generation** of the ***Security Target***, where it is stated that all components in the system use the same subcomponent for performing certificate validation. More details are given on the provided URL, where the API used to check the validity of the X509 certificates is described. Concretely, this task is performed by Crypt32. lib and Wincrypt.h.

This section also provides information about the certification path algorithm which, according to this document, follows RFC 5280 section.

34.1.2 Verdict

The evaluator considers that the evidences defined above and obtained during the documentation review demonstrate the fulfilment of the requirement established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the documentation review activity.

34.2 Test Activity

To perform the TLS tests required by the Assurance Activities and check their correct outcome, different pieces of software were used:

1. Software acting as a TLS server:

a. *ee-tls-tool*, a command line tool developed by the evaluation laboratory in order to create a TLS server which is automatically configured prior each test case execution.

2. Software acting as a client from the TOE:

b. *W10ClientAutomator.ps1*, a Powershell script which automatically configures the TOE as a client prior each test case execution. This script allows the evaluator execute test cases using:

   i. different web browsers that come bundled with the TOE (i.e. Internet Explorer and Microsoft Edge).

   ii. *TlsClientTest*, a command line tool developed by the evaluation laboratory. This tool provides more information about the concrete point where SSL validation failed in case of connection error.

Additionaly, to perform Test 1.d is necessary to use the following software:

3. Software to modify packets

c. *Rehtse* , a MITM tool developed by the evaluation laboratory in order to modify packets on the fly.

Information about their suitability for this evaluation is given in the introduction to FCS_TLSC_EXT.1.1.

34.2.1 Test 1

34.2.1.1 Setup

The following certificates, created automatically by *ee-tls-tool_v2* and installed by *W10ClientAutomator.ps1*, shall be used to perform the assurance activities listed on the Protection Profile:

- CN = EE Test Root CA
- CN = EE Test Intermediate CA 1
- CN = EE Test Intermediate CA 2
- CN = test.epoche.es

The listed certificates form a valid certification path. All certificates are available in `pem` format.

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Server Machine (Debian 11 Bullseye)
- Client Machine (Canonical platforms listed in the ST)

These two machines are in the same network with the following configuration:

- Server Machine, IP = 50.50.50.220, 10.10.10.12 for test 1.d
- Client Machine, IP = 50.50.50.210, 20.20.20.40 for test 1.d

Server machine contains the *ee-tls-tool_v2* software, a test suite for TLS and X509 Common Criteria evaluations. It acts as a TLS server configured according to each test. In addition, the *Wireshark* network analyzer is installed on the server machine.

The client machine shall contain the PowerShell script *W10ClientAutomator.ps1* and the *TlsClientTest* tool, which uses the System.Net. Security classes from .Net framework to perform SSL connections, effectively using the authentication mechanism from the OS.

The MITM machine contains the *Rehtse* software to modify packets.

Moreover, the client machine shall have the secure configuration enabled, according to the section **3.2 Operational prerequisites** of the ***Operational Guidance***.

34.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

34.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

34.2.1.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 1** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 1** activity.

34.2.2 Test 2

34.2.2.1 Setup

The setup is identical to the one defined for Test 1 (IPs configuration and installed tools). The certificate used for the connection is different than the one used for Test 1:

- CN = EE Test Root CA
- CN = EE Test Intermediate CA 1
- CN = EE Test Intermediate CA 2
- CN = test.epoche.es (expired certificate)

The listed certificates form a valid certification path. All certificates are available in pem format.

34.2.2.2 Procedure

The procedure is identical to the one defined for Test 1.

34.2.2.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

34.2.2.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 2** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 2** activity.

34.2.3 Test 3

34.2.3.1 Setup

The following certificates, created automatically by *ee-tls-tool* and installed by W10ClientAutomator shall be used to perform the assurance activities listed on the Protection Profile:

- CN = EE Test Root CA
- CN = EE Test Intermediate CA 1 (non-revoked)
- CN = EE Test Intermediate CA 1 (revoked)
- CN = EE Test Intermediate CA 2
- CN = test.epoche.es (non-revoked)
- CN = test.epoche.es (revoked)

The certificates listed form a valid certification path. All certificates are available in pem format as well as pfx.

Additionally the following OCSP signing certificates are added:

- CN = ocsp.test.epoche.es (signed by the root CA)
- CN = ocsp.test.epoche.es (signed by intermediate CA 1)
- CN = ocsp.test.epoche.es (signed by intermediate CA 2)

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Server Machine, CRL Server (Debian 11 bullseye)
- Client Machine (Canonical platforms listed in the ST)

For OCSP and OCSP stapling tests, the following machine is added:

- Web Server, OCSP Server (Windows Server 2022 DataCenter)

These machines are in separate networks with the following configuration, one for OCSP stapling and another one for every other test:

Regular tests:

- Server Machine/CRL Server, IP = 50.50.50.220
- Client Machine, IP = 50.50.50.155, 50.50.50.210
- Web/OCSP Server, IP = 50.50.50.227

OCSP stapling tests have been performed in localhost.

Server machine contains the *ee-tls-tool* software, a test suite for TLS and X509 Common Criteria evaluations. It acts as a TLS server configured according to each test. In addition, the *Wireshark* network analyzer is installed on the server machine.

The client machine shall contain the PowerShell script *W10ClientAutomator.ps1* and the *TlsClientTest* tool, which uses the System.Net. Security classes from .Net framework to perform SSL connections, effectively using the authentication mechanism from the OS. Furthermore, the client machine shall have the secure configuration enabled, according to the section **3.2 Operational prerequisites** of the ***Operational Guidance***.

Moreover, the following additional scripts are needed to perform the test case:

- For CRL (on CRL server machine):
  - *1_startCRLServer_norevocation.sh*: This script starts the CRL server in which there is no revoked certificate.
  - *2_startCRLServer_servercert_revocation.sh*: This script starts the CRL server in which the server certificate is revoked.
  - *3_startCRLserver_intermediate1_revocation.sh*: This script starts the CRL server in which a intermediate certificate is revoked.

- For OCSP (on OCSP Server machine):
  - *configureServer.ps1:* Powershell script which shall be executed on the OCSP Server machine. This scripts automatically modifies the revocation configuration depending on the performed test (no revocation, server certificate revoked or intermediate certificate revoked).

Moreover, the Web/OCSP server machine shall have the following Windows Server roles installed:

- Internet Information Services (web server)
- Online Responder (OCSP server)

If they are not installed, the provided script *configureWindowsServerForOCSPandOCSPStapling.ps1* automatically installs and configures the IIS role along with the correct certificates. However, the Online Responder role requires some degree of manual configuration, indicated next.

The Online Responder role shall first be installed as follows:

- After running *configureWindowsServerForOCSPandOCSPStapling.ps1* on the Windows Server machine, open the Server Manager from the task bar.
- From the Server Manager Dashboard select "Manage" and then "Add Roles and Features".
- Click next until the "Select server roles" screen.
- Inside "Active Directory Certificate Services", select "Online Responder".
- Click next until the installation is finished, accepting the suggested extra elements in the process.
- Configure the Online Responder if prompted in the results screen (no input is needed to do so).

Before configuring the Online Responder, the certificate revocation lists (CRLs) need to be made available:

- Copy the contents from "ee-tls-tool/certs/X509_EXT.1.1/ca" (it includes the CRLs) inside "C:\inetpub\wwwroot".
- From the Server Manager Dashboard select "Tools" and then "Internet Information Services (IIS) Manager".
- On the left panel, click on "Default Web Site" below the system's name and "Sites".
- On the central panel, double click on "MIME Types".
- On the right panel, click "Add...".
- Under "File name extension", type ".pem".
- Under "MIME type", type "application/pki-crl" and click "OK".

Read permission for the OCSP private keys needs to be granted to the "NETWORK SERVICE" account as follows:

- Open mmc.exe (e.g. by opening the start menu, typing "mmc" and then pressing enter).

- On the "File" menu, click "Add/Remove Snap-in...".
- In the "Available snap-ins" panel, select "Certificates".
- Press "Add".
- In the "Certificates snap-in" dialog box, select "Computer Account" and click next.
- Select "Local Computer" and press "Finish".
- Press "OK".
- In the console tree, open "Personal" and then "Certificates". The three certificates with CN = ocsp. test . epoche.es will appear inside the presented list.
- Right click on one of them and select "All tasks" and then "Manage Private Keys...".
- In the "Security" tab presented, click "Add...".
- Enter "NETWORK SERVICE" as the object name.
- Check that the "NETWORK SERVICE" group now appears with read access.
- Repeat the process with the two remaining OCSP signing certificates.

The Online Responder service can now be configured as shown next:

- From the Server Manager Dashboard select "Tools" and then "Online Responder Management".
- On the left panel, right click on "Revocation Configuration" and then click on "Add Revocation Configuration".
- Click "Next" on the first screen.
- On the "Name the Revocation Configuration" screen, type "EE Root CA" (could be any name) and click "Next".
- On the "Select CA Certificate Location" screen, select "Select a Certificate from the Local certificate store" and click "Next".
- On the "Choose CA Certificate" screen, click "Browse..." and select the root CA (CN = EE Test Root CA). Then click "Next".
- On the "Select Signing Certificate" screen, select "Manually select a signing certificate" and click "Next". An error might appear; it can be ignored.
- On the "Revocation Provider" screen, click "Provider...".
- Below the "Base CRLs" list, click "Add...".
- Type http://localhost/crl/ca_before_revocation.crl.pem and click "OK".
- Repeat from step 2, for the intermediate certificate 1. Type "EE Intermediate CA 1" instead, select "EE Test Intermediate CA 1" and type http://localhost/intermediate1/crl/intermed
- Repeat from step 2, for the intermediate certificate 2. Type "EE Intermediate CA 2" instead, select "EE Test Intermediate CA 2" and type http://localhost/intermediate1/intermediat
before_revocation.crl.pem.
- On the left panel, select the system under "Array configuration".
- On the centre panel, for every one of the three configurations created, click them and then select "Assign Signing Certificate" on the right panel, selecting the corresponding OCSP signing certificate (e.g. for configuration "EE Intermediate CA 2" select the one with CN = ocsp. test . epoche.es that was signed by "EE Test Intermediate CA 2").
- On the left panel, right click on "Array configuration" and then "Refresh Revocation Data".

- Click on the top-most element in the left panel (starting with "Online Responder:").
- The centre panel should show the status of the three configurations added, and they all should be shown as "Working".

It is also important to configure the server machine so the delta CRL configuration is enabled. This can be achieved by accessing the server properties using the IIS and checking its corresponding option. Otherwise, OCSP communication cannot be achieved.

In the Windows Server machine, "C:\Windows\System32\drivers\etc\hosts" shall be modified so that it contains two lines specifying the IPs for test.epoche.es and ocsp.test.epoche.es, which will vary depending on whether the configuration for OCSP stapling is being used or not, since it uses another network. Finally, reboot the Windows Server machine for OCSP stapling to be enabled. The script running in the client machine handles this task automatically so there are no further actions needed in this regard.

34.2.3.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

34.2.3.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

34.2.3.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 3** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 3** activity.

34.2.4 Test 4

34.2.4.1 Setup

The following certificates, created automatically by *ee-tls-tool* and installed by W10ClientAutomato shall be used to perform the assurance activities listed on the Protection Profile:

- CN = EE Test Root CA
- CN = EE Test Intermediate CA 1
- CN = EE Test Intermediate CA 2 (no cRLSign key usage bit)
- CN = test.epoche.es

The certificates listed form a valid certification path. All certificates are available in pem format as well as pfx.

Additionally, the following OCSP signing certificates are added:

- CN = ocsp.test.epoche.es (signed by the root CA)
- CN = ocsp.test.epoche.es (signed by intermediate CA 1)
- CN = ocsp.test.epoche.es (signed by intermediate CA 2)

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Server Machine, CRL Server (Debian 11 Bullseye)
- Client Machine (Canonical platforms listed in the ST)

For the OCSP test, the following machines are added:

- OCSP Server (Windows Server 2022 Datacenter)
- MITM Machine (Kali Linux)

These machines are in different networks depending on the test, with the following configurations:

CRL configuration:

- Server Machine/CRL Server, IP = 50.50.50.220
- Client Machine, IP = 50.50.50.155

OCSP configuration:

- Server Machine/CRL Server, IP = 10.10.10.21
- Client Machine, IP = 10.10.10.30
- OCSP Server, IP = 20.20.20.40

Server machine contains the *ee-tls-tool* software, a test suite for TLS and X509 Common Criteria evaluations. It acts as a TLS server configured according to each test. In addition, the *Wireshark* network analyzer is installed on the server machine.

The client machine shall contain the PowerShell script *W10ClientAutomator.ps1* and the *TlsClientTest* tool, which uses the System.Net. Security classes from .Net framework to perform SSL connections, effectively using the authentication mechanism from the OS. Furthermore, the client machine shall have the secure configuration enabled, according to the section **3.2 Operational prerequisites** of the ***Operational Guidance***.

Moreover, the following additional script is needed to perform the test case:

- For CRL (on CRL server machine):
  - *startCRLServer_intermediate2_noCRLSignKeyUsageBit.sh*: This script starts the CRL server in which a CRL signed by a CA without cRLsign key usage bit is provided.

The MITM machine shall act as a switch between the OCSP Server and the rest of the network, which means that its IP address does not play any role. It shall contain the *Rehtse* tool, a tool developed by the evaluator which is capable of modifying packets being routed through the machine on the fly, according to some criteria defined by regular expressions and BPF filters.

The Windows Server machine shall have the Online Responder role installed. To install it and configure it, see the Setup section for Test 3.

Lastly, on the Windows Server machine, "C:\Windows\System32\drivers\etc\hosts" shall be modified so that it contains a line with the appropriate name and IP addresses.

34.2.4.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

34.2.4.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

34.2.4.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 4** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 4** activity.

34.2.5 Test 5

34.2.5.1 Setup

The setup is identical to the one defined for Test 1, but the IP address for the client is 50.50.50.155.

34.2.5.2 Procedure

The procedure is identical to the one defined for Test 1.

34.2.5.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

34.2.5.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 5** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 5** activity.

34.2.6 Test 6

34.2.6.1 Setup

The setup is identical to the one defined for Test 1 but the IP address for the client is 50.50.50.155.

34.2.6.2 Procedure

The procedure is identical to the one defined for Test 1.

34.2.6.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

34.2.6.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 6** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 6** activity.

34.2.7 Test 7

34.2.7.1 Setup

The setup is identical to the one defined for Test 1 but the IP address for the client is 50.50.50.155.

34.2.7.2 Procedure

The procedure is identical to the one defined for Test 1.

34.2.7.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

34.2.7.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 7** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 7** activity.

34.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to this FIA_X509_EXT.1.1.

35 FIA_X509_EXT.1.2

The assurance activity for the **FIA_X509_EXT.1.2** requirement is stated as follows:

> The tests described must be performed in conjunction with the other certificate services assurance activities, including the functions in FIA_X509_EXT.2.1. The evaluator will create a chain of at least four certificates: the node certificate to be tested, two Intermediate CAs, and the self-signed Root CA.
>
> - **Test 1**: The evaluator will construct a certificate path, such that the certificate of the CA issuing the OS's certificate does not contain the basicConstraints extension. The validation of the certificate path fails.
> - **Test 2**: The evaluator will construct a certificate path, such that the certificate of the CA issuing the OS's certificate has the CA flag in the basicConstraints extension not set. The validation of the certificate path fails.
> - **Test 3**: The evaluator will construct a certificate path, such that the certificate of the CA issuing the OS's certificate has the CA flag in the basicConstraints extension set to TRUE. The validation of the certificate path succeeds.

35.1 Documentation Review activity

35.1.1 Findings

Assurance activity does not state any documentation review activity for this requirement.

35.1.2 Verdict

Assurance activity does not state any documentation review activity for this requirement. Therefore, the **PASS** verdict is assigned to the documentation review activity.

35.2 Test Activity

To perform the TLS tests required by the Assurance Activities and check their correct outcome, different pieces of software were used:

1. Software acting as a TLS server:

   a. *ee-tls-tool*, a command line tool developed by the evaluation laboratory in order to create a TLS server which is automatically configured prior each test case execution.

2. Software acting as a client from the TOE
   b. *W10ClientAutomator.ps1*, a Powershell script which automatically configures the TOE as a client prior each test case execution. This script allows the evaluator execute test cases using:
      i. different web browsers that come bundled with the TOE (i.e. Internet Explorer and Microsoft Edge).
      ii. *TlsClientTest*, a command line tool developed by the evaluation laboratory. This tool provides more information about the concrete point where SSL validation failed in case of connection error.

Information about their suitability for this evaluation is given in the introduction to FCS_TLSC_EXT.1.1.

35.2.1 Test 1

35.2.1.1 Setup

The following certificates, created automatically by *ee-tls-tool* and installed by W10ClientAutomato shall be used to perform the assurance activities listed on the Protection Profile:

- CN = EE Test Root CA
- CN = EE Test Intermediate CA 1
- CN = EE Test Intermediate CA 2 (no *basicConstraints* extension)
- CN = test.epoche.es

The certificates listed form a valid certification path. The root certificate is available in pem format, the other ones will be sent by the server.

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Server Machine (Debian 11 Bullseye)
- Client Machine (Canonical platforms listed in the ST)

Both machines are in the same network with the following configuration:

- Server Machine, IP = 50.50.50.220
- Client Machine, IP = 50.50.50.155

Server machine contains the *ee-tls-tool* software, a test suite for TLS and X509 Common Criteria evaluations. It acts as a TLS server configured according to each test. In addition, the *Wireshark* network analyzer is installed on the server machine.

The client machine shall contain the PowerShell script *W10ClientAutomator.ps1* and the *TlsClientTest* tool, which uses the System.Net. Security classes from .Net framework to perform SSL connections, effectively using the authentication mechanism from the OS.

Moreover, the client machine shall have the secure configuration enabled, according to the section **3.2 Operational prerequisites** of the ***Operational Guidance***.

35.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

35.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

35.2.1.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 1** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 1** activity.

35.2.2 Test 2

35.2.2.1 Setup

The setup is identical to the one defined for Test 1 (IPs configuration and installed tools). The certificate used for the connection is different than the one used for Test 1:

- CN = EE Test Root CA
- CN = EE Test Intermediate CA 1
- CN = EE Test Intermediate CA 2 (CA flag not set in basicConstraints extension)
- CN = test.epoche.es

The certificates listed form a valid certification path. The root certificate is available in pem format, the other ones will be sent by the server.

35.2.2.2 Procedure

The procedure is identical to the one defined for Test 1.

35.2.2.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

35.2.2.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 2** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 2** activity.

35.2.3 Test 3

35.2.3.1 Setup

The setup is identical to the one defined for Test 1 (IPs configuration and installed tools). The certificate used for the connection is different than the one used for Test 1:

- CN = EE Test Root CA
- CN = EE Test Intermediate CA 1
- CN = EE Test Intermediate CA 2 (basicConstraints with CA flag set to true)
- CN = test.epoche.es

The certificates listed form a valid certification path. The root certificate is available in pem format, the other ones will be sent by the server.

35.2.3.2 Procedure

The procedure is identical to the one defined for Test 1.

35.2.3.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

35.2.3.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 3** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 3** activity.

35.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to this FIA_X509_EXT.1.2.

36 FIA_X509_EXT.2.1

The assurance activity for the **FIA_X509_EXT.2.1** requirement is stated as follows:

> The evaluator will acquire or develop an application that uses the OS TLS mechanism with an X.509v3 certificate. The evaluator will then run the application and ensure that the provided certificate is used to authenticate the connection.
>
> The evaluator will repeat the activity for any other selections listed.

36.1 Documentation Review activity

36.1.1 Findings

Assurance activity does not state any documentation review activity for this requirement.

36.1.2 Verdict

Assurance activity does not state any documentation review activity for this requirement. Therefore, the **PASS** verdict is assigned to the documentation review activity.

36.2 Test Activity

To perform the TLS tests required by the Assurance Activities and check their correct outcome, different pieces of software were used:

1. Software acting as a TLS server:

    a. *ee-tls-tool*, a command line tool developed by the evaluation laboratory in order to create a TLS server which is automatically configured prior each test case execution.

2. Software acting as a client from the TOE

    b. *W10ClientAutomator.ps1*, a Powershell script which automatically configures the TOE as a client prior each test case execution. This script allows the evaluator execute test cases using:

        i. different web browsers that come bundled with the TOE (i.e. Internet Explorer and Microsoft Edge).

        ii. *TlsClientTest*, a command line tool developed by the evaluation laboratory. This tool provides more information about the concrete point where SSL validation failed in case of connection error.

Information about their suitability for this evaluation is given in the introduction to FCS_TLSC_EXT.1.1.

36.2.1 Test 1

36.2.1.1 Setup

The following certificates, created automatically by *ee-tls-tool* and installed by W10ClientAutomator shall be used to perform the assurance activities listed on the Protection Profile:

- CN = EE TestRoot CA
- CN = EE Test Intermediate CA 1
- CN = EE Test Intermediate CA 2
- CN = test.epoche.es
- CN = EE Client (client certificate with friendly name "EE Client Certificate")

The listed certificates form a valid certification path. The root certificate is available in pem format, the client certificate in pfx format, and the other ones will be sent by the server.

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Server Machine (Debian 11 Bullseye)
- Client Machine (Platforms listed in the ST)

Both machines are in the same network with the following configuration:

- Server Machine, IP = 50.50.50.220
- Client Machine, IP = 50.50.50.155

Server machine contains the *ee-tls-tool* software, a test suite for TLS and X509 Common Criteria evaluations. It acts as a TLS server configured according to each test. In addition, the *Wireshark* network analyzer is installed on the server machine.

The client machine shall contain the PowerShell script *W10ClientAutomator.ps1* and the *TlsClientTest* tool, which uses the System.Net. Security classes from .Net framework to perform SSL connections, effectively using the authentication mechanism from the OS.

Moreover, the client machine shall have the secure configuration enabled, according to the section **3.2 Operational prerequisites** of the ***Operational Guidance***.

36.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

36.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

36.2.1.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 1** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 1** activity.

36.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to this FIA_X509_EXT.2.1.

37 FMT_MOF_EXT.1.1 & FMT_SMF_EXT.1.1

The assurance activity for the **FMT_MOF_EXT.1** and **FMT_SMF_EXT.1** requirements is stated as follows:

> **FMT_MOF_EXT.1:** The evaluator shall verify that the TSS describes those management functions that are restricted to Administrators, including how the user is prevented from performing those functions, or not able to use any interfaces that allow access to that function.
>
> - **Test 1:** For each function that is indicated as restricted to the administrator, the evaluation shall perform the function as an administrator, as specified in the Operational Guidance, and determine that it has the expected effect as outlined by the Operational Guidance and the SFR. The evaluator shall then perform the function (or otherwise attempt to access the function) as a non-administrator and observe that they are unable to invoke that functionality.
>
> **FMT_SMF_EXT.1:** The evaluator will verify that every management function captured in the ST is described in the operational guidance and that the description contains the information required to perform the management duties associated with the management function. The evaluator will test the operating system's ability to provide the management functions by configuring the operating system and testing each option selected from above. The evaluator is expected to test these functions in all the ways in which the ST and guidance documentation state the configuration can be managed.

37.1 Documentation Review Activity

37.1.1 Findings

The evaluator has reviewed the ***Security Target*** document to identify all the management functions defined by the vendor. These functions are listed in the section **6.5 Security Management** of the TSS, as it can be observed in the following image extracted from the ***Security Target*** document:

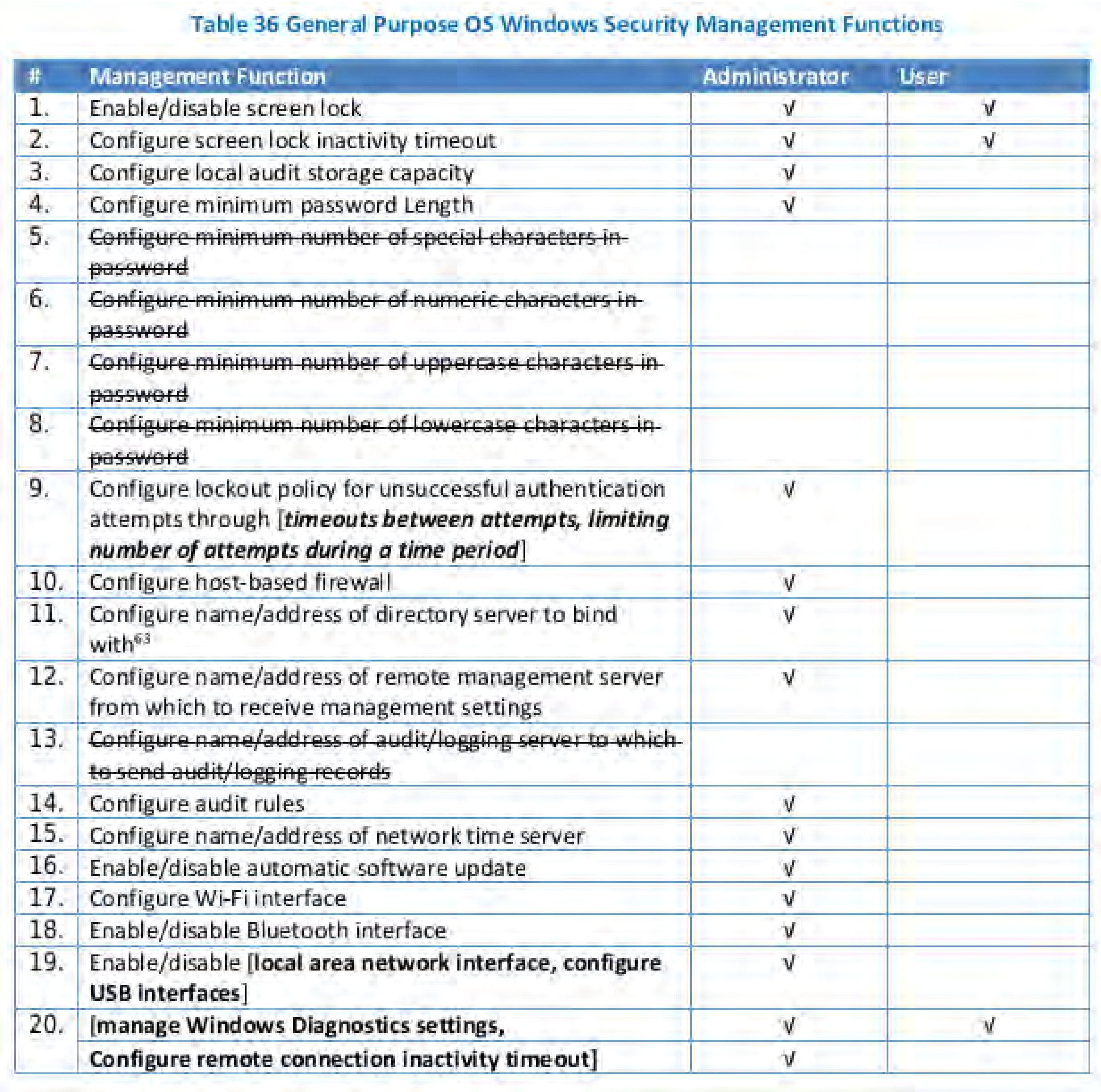
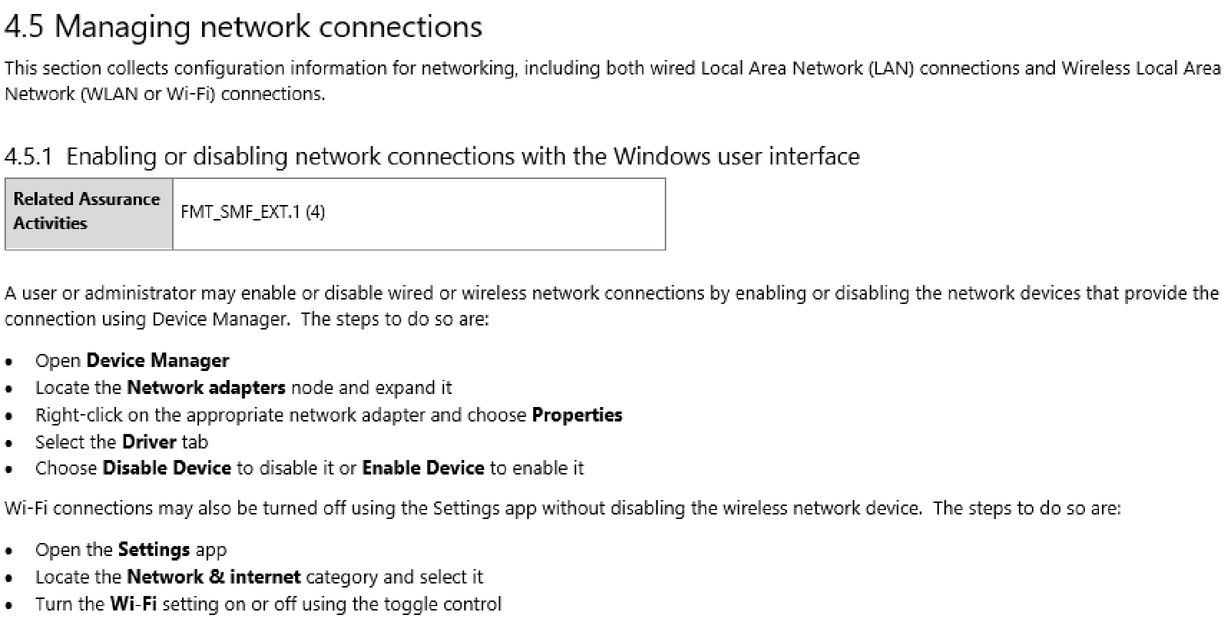


Table 36 General Purpose OS Windows Security Management Functions

#	Management Function	Administrator	User
1.	Enable/disable screen lock	√	√
2.	Configure screen lock inactivity timeout	√	√
3.	Configure local audit storage capacity	√	
4.	Configure minimum password Length	√	
5.	~~Configure minimum number of special characters in password~~		
6.	~~Configure minimum number of numeric characters in password~~		
7.	~~Configure minimum number of uppercase characters in password~~		
8.	~~Configure minimum number of lowercase characters in password~~		
9.	Configure lockout policy for unsuccessful authentication attempts through [***timeouts between attempts, limiting number of attempts during a time period***]	√	
10.	Configure host-based firewall	√	
11.	Configure name/address of directory server to bind with[63]	√	
12.	Configure name/address of remote management server from which to receive management settings	√	
13.	~~Configure name/address of audit/logging server to which to send audit/logging records~~		
14.	Configure audit rules	√	
15.	Configure name/address of network time server	√	
16.	Enable/disable automatic software update	√	
17.	Configure Wi-Fi interface	√	
18.	Enable/disable Bluetooth interface	√	
19.	Enable/disable [**local area network interface, configure USB interfaces**]	√	
20.	[**manage Windows Diagnostics settings,**	√	√
	Configure remote connection inactivity timeout]	√	

In addition, the evaluator has also reviewed the ***Operational Guidance*** document, which includes within its section **4. Managing evaluated features** all the management functions explained throughout the document. In addition, for each management function, it is described all the available methods to configure each function, as well as, the applicable roles and Windows 10, Windows 11, Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions.



4.5 Managing network connections

This section collects configuration information for networking, including both wired Local Area Network (LAN) connections and Wireless Local Area Network (WLAN or Wi-Fi) connections.

4.5.1 Enabling or disabling network connections with the Windows user interface

Related Assurance Activities	FMT_SMF_EXT.1 (4)

A user or administrator may enable or disable wired or wireless network connections by enabling or disabling the network devices that provide the connection using Device Manager. The steps to do so are:

- Open **Device Manager**
- Locate the **Network adapters** node and expand it
- Right-click on the appropriate network adapter and choose **Properties**
- Select the **Driver** tab
- Choose **Disable Device** to disable it or **Enable Device** to enable it

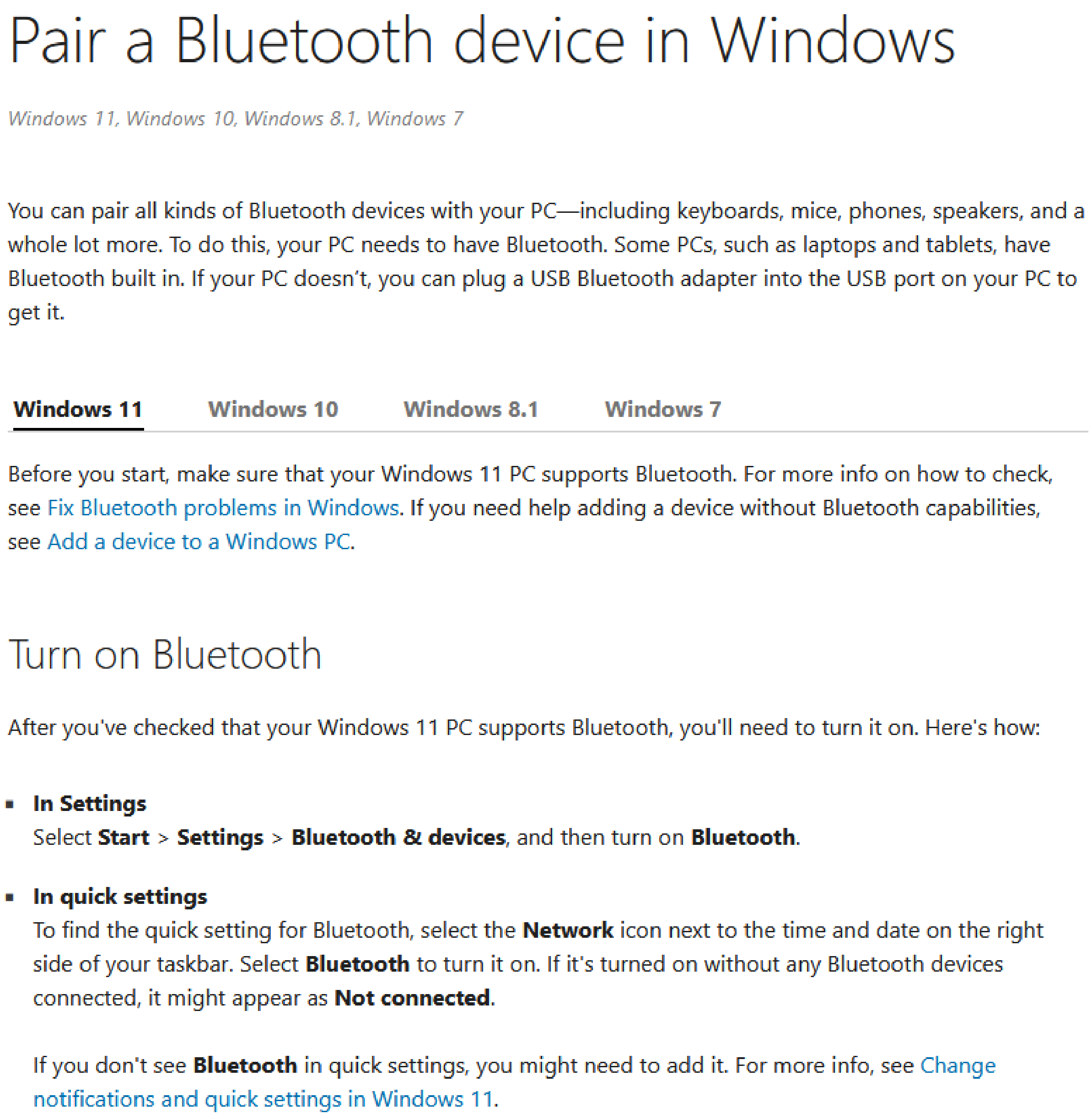
Wi-Fi connections may also be turned off using the Settings app without disabling the wireless network device. The steps to do so are:

- Open the **Settings** app
- Locate the **Network & internet** category and select it
- Turn the **Wi-Fi** setting on or off using the toggle control

For each of these management functions, the ***Operational Guidance*** document, includes links to the OS vendor support site, where information about how to configure each of these functions is provided.

These links also provides information about managing these functions either with a standard user or as administrator, specifying the different steps needed for each one. Moreover, the managements functions contains instructions for Windows 10, Windows 11, Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions, in the cases that is needed a different management approach for each of them.

This is an example of the information provided in the vendor website about how to pair a bluetooth device:



Pair a Bluetooth device in Windows

Windows 11, Windows 10, Windows 8.1, Windows 7

You can pair all kinds of Bluetooth devices with your PC—including keyboards, mice, phones, speakers, and a whole lot more. To do this, your PC needs to have Bluetooth. Some PCs, such as laptops and tablets, have Bluetooth built in. If your PC doesn't, you can plug a USB Bluetooth adapter into the USB port on your PC to get it.

Before you start, make sure that your Windows 11 PC supports Bluetooth. For more info on how to check, see Fix Bluetooth problems in Windows. If you need help adding a device without Bluetooth capabilities, see Add a device to a Windows PC.

Turn on Bluetooth

After you've checked that your Windows 11 PC supports Bluetooth, you'll need to turn it on. Here's how:

- **In Settings**
  Select **Start** > **Settings** > **Bluetooth & devices**, and then turn on **Bluetooth**.
- **In quick settings**
  To find the quick setting for Bluetooth, select the **Network** icon next to the time and date on the right side of your taskbar. Select **Bluetooth** to turn it on. If it's turned on without any Bluetooth devices connected, it might appear as **Not connected**.

  If you don't see **Bluetooth** in quick settings, you might need to add it. For more info, see Change notifications and quick settings in Windows 11.

37.1.2 Verdict

The evaluator considers that all the security management functions declared in the ***Security Target*** document are properly defined in the ***Operational Guidance*** document, providing enough information to allow the evaluator to perform each management function.

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfilment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

37.2 Test Activity

37.2.1 Test 1 - Enable/Disable Screen Lock

The screen lock will be enabled and disabled during this test case.

37.2.1.1 Setup

Before the test execution, the following setup condition must be fulfilled:

- A user account with no administrator rights shall exist. This user shall belong to the default *Users* group.
- A user account with administrator rights shall exist. This account shall belong to the default *Administrators* group.
- The *PowerShell* execution policy shall be configured to allow the execution of *PowerShell* scripts.

37.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

37.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)

- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)

- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

37.2.1.4 Verdict

As the above results state, the user with administrator rights and without administrator rights can enable and disable the screen lock.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

37.2.2 Test 2 - Configure Screen Lock Inactivity Timeout

The screen lock inactivity timeout will be configured during this test case.

37.2.2.1 Setup

The applicable setup for this test is the same as the defined one for Test 1.

37.2.2.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

37.2.2.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

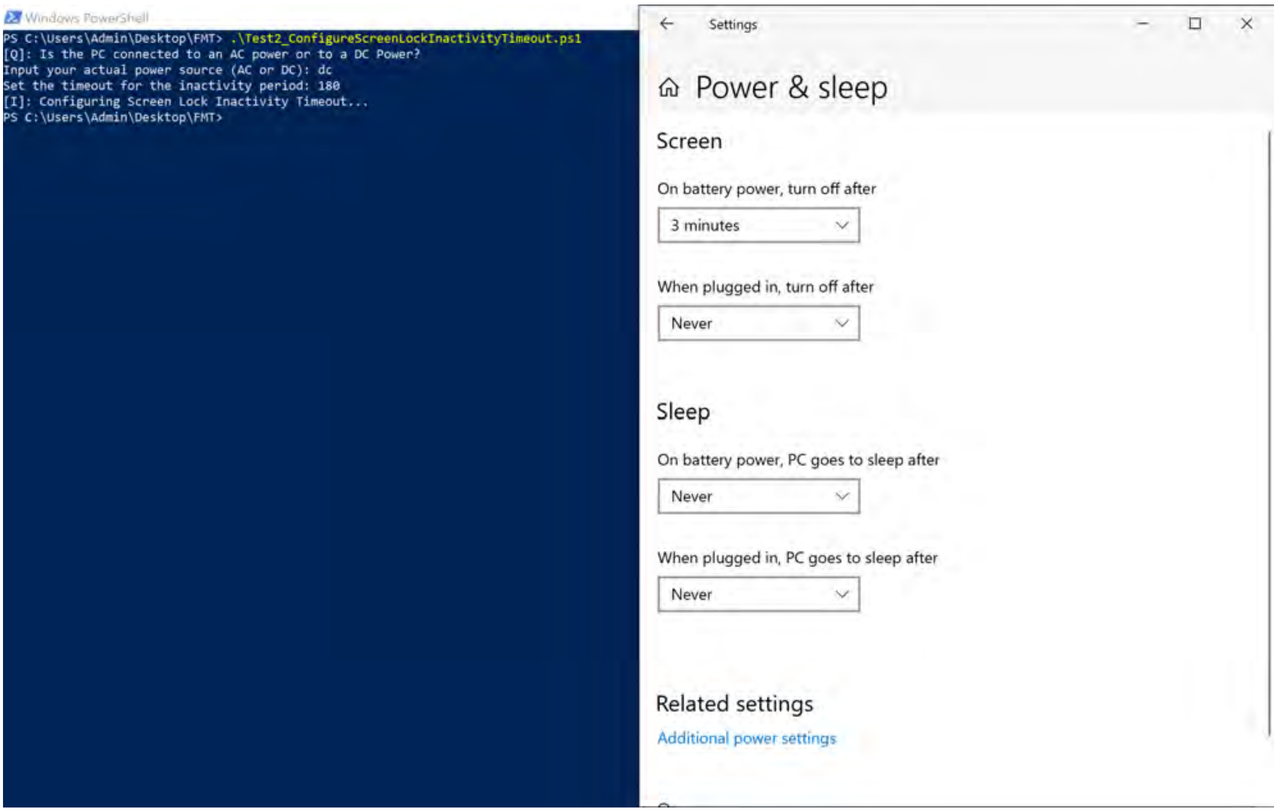
- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)

- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

37.2.2.3.1 Windows 10 platforms:



```
PS C:\Users\Admin\Desktop\FMT> .\Test2_ConfigureScreenLockInactivityTimeout.ps1
[Q]: Is the PC connected to an AC power or to a DC Power?
Input your actual power source (AC or DC): dc
Set the timeout for the inactivity period: 180
[I]: Configuring Screen Lock Inactivity Timeout...
PS C:\Users\Admin\Desktop\FMT>
```

Screen

On battery power, turn off after: 3 minutes

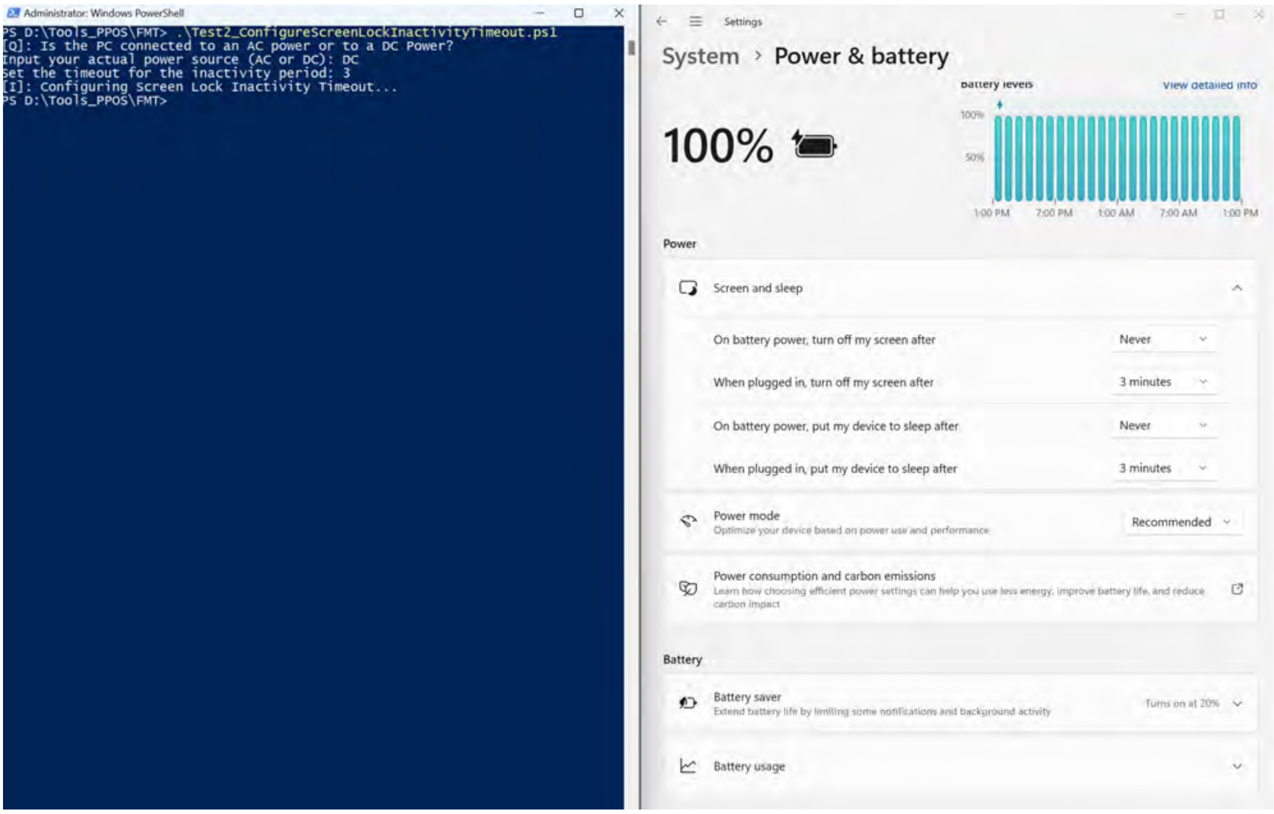
When plugged in, turn off after: Never

Sleep

On battery power, PC goes to sleep after: Never

When plugged in, PC goes to sleep after: Never

37.2.2.3.2 Windows 11 platforms:



Administrator: Windows PowerShell

```
PS D:\Tools_PPOS\FMT> .\Test2_ConfigureScreenLockInactivityTimeout.ps1
[Q]: Is the PC connected to an AC power or to a DC Power?
Input your actual power source (AC or DC): DC
Set the timeout for the inactivity period: 3
[I]: Configuring Screen Lock Inactivity Timeout...
PS D:\Tools_PPOS\FMT>
```

Settings

System › Power & battery

100%

Power

Screen and sleep

On battery power, turn off my screen after: Never

When plugged in, turn off my screen after: 3 minutes

On battery power, put my device to sleep after: Never

When plugged in, put my device to sleep after: 3 minutes

Power mode: Recommended
Optimize your device based on power use and performance

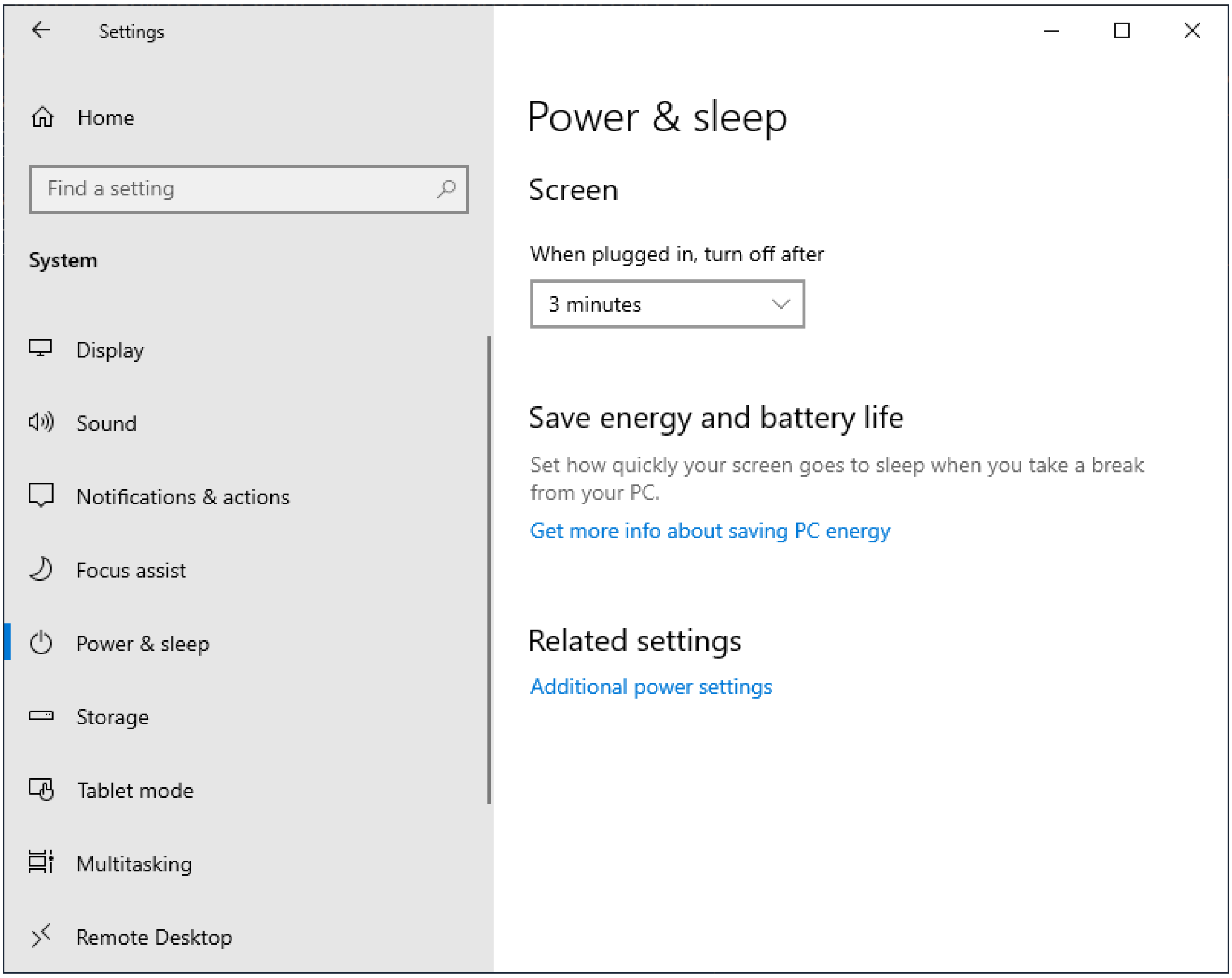
Power consumption and carbon emissions
Learn how choosing efficient power settings can help you use less energy, improve battery life, and reduce carbon impact

Battery

Battery saver: Turns on at 20%
Extend battery life by limiting some notifications and background activity

Battery usage

37.2.2.3.3 Windows Server platforms (21H2, 2022, Hub, Edge, HCIv2):



Power & sleep

Screen

When plugged in, turn off after

3 minutes

Save energy and battery life

Set how quickly your screen goes to sleep when you take a break from your PC.

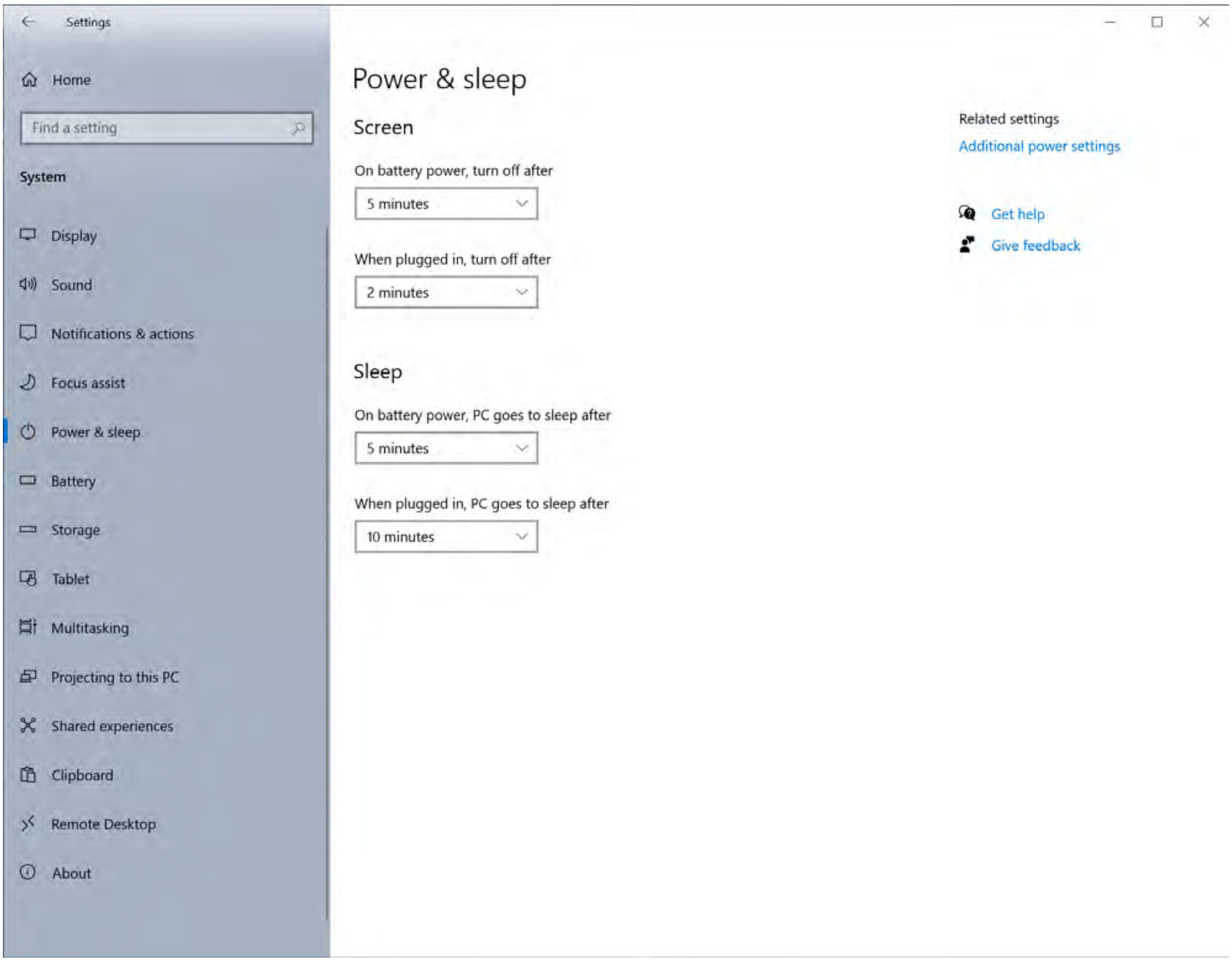
Get more info about saving PC energy

Related settings

Additional power settings

The same results were obtained with the user without administrator rights. As stated in the table of the *Findings* section, standard users can also configure the screen lock inactivity timeout.

37.2.2.3.4 Windows 10 platforms:



Power & sleep

Screen

On battery power, turn off after: 5 minutes

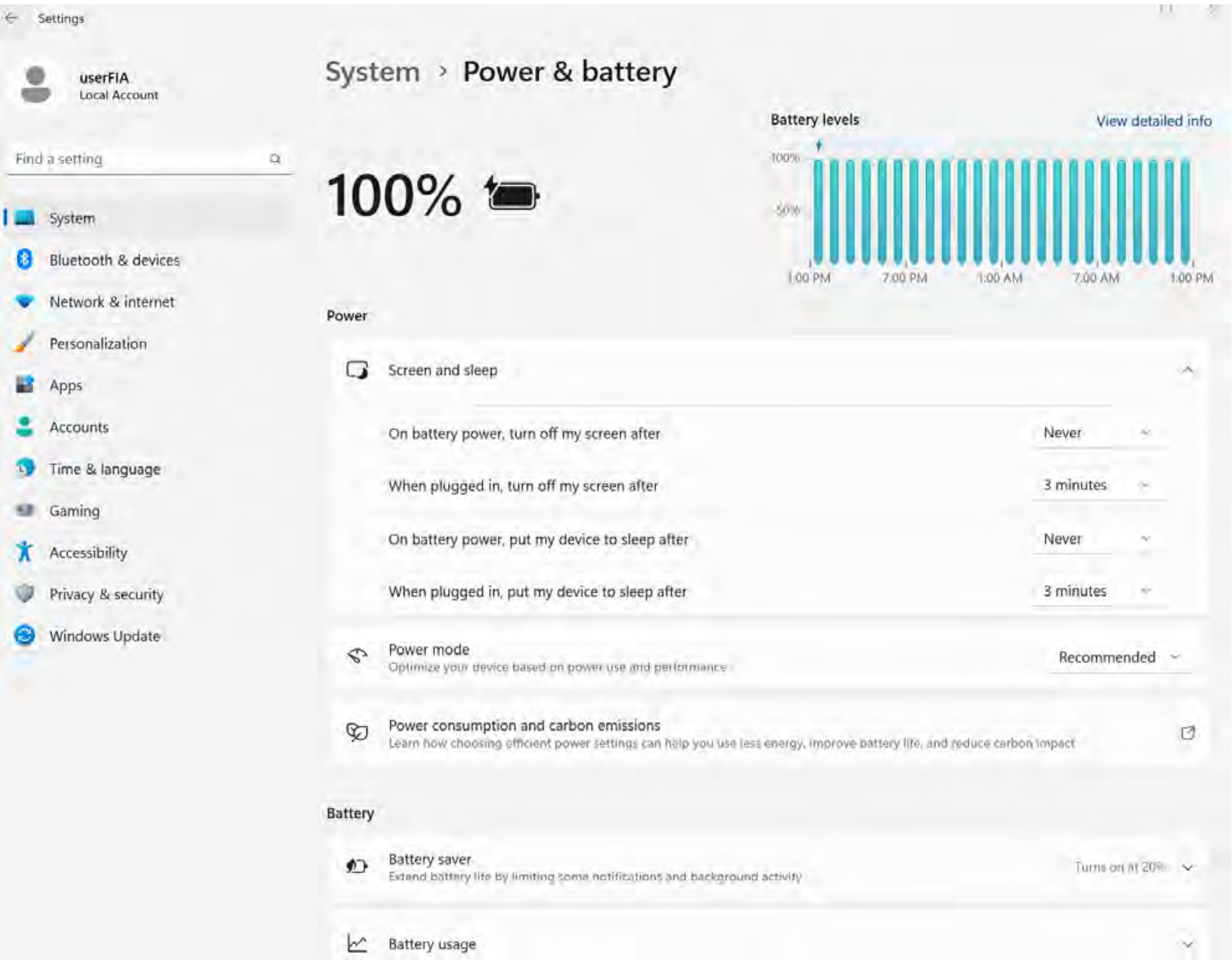
When plugged in, turn off after: 2 minutes

Sleep

On battery power, PC goes to sleep after: 5 minutes

When plugged in, PC goes to sleep after: 10 minutes

37.2.2.3.5 Windows 11 platforms:



100%

Power

Screen and sleep

On battery power, turn off my screen after: Never

When plugged in, turn off my screen after: 3 minutes

On battery power, put my device to sleep after: Never

When plugged in, put my device to sleep after: 3 minutes

Power mode
Optimize your device based on power use and performance: Recommended

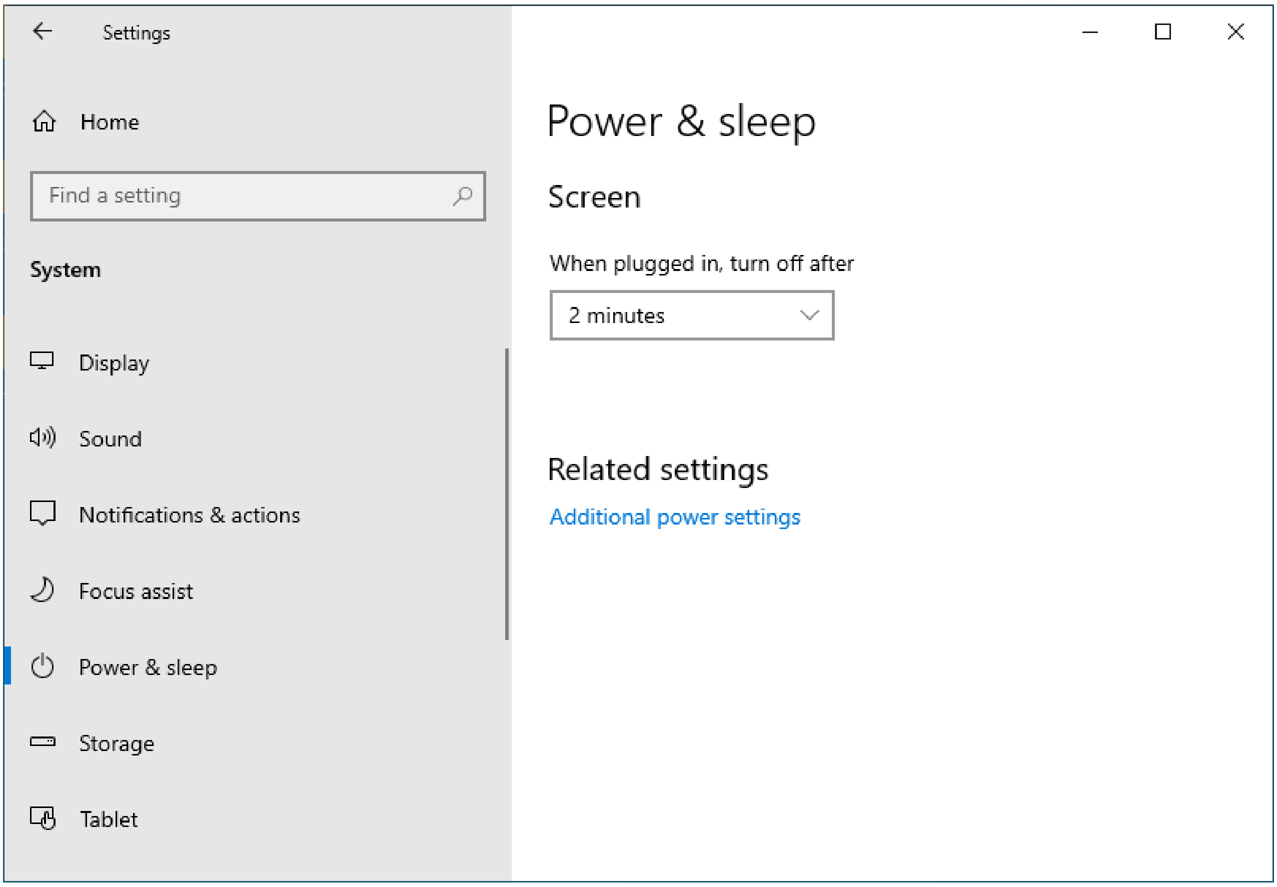
Power consumption and carbon emissions
Learn how choosing efficient power settings can help you use less energy, improve battery life, and reduce carbon impact

Battery

Battery saver
Extend battery life by limiting some notifications and background activity: Turns on at 20%

Battery usage

37.2.2.3.6 Windows Server platforms (21H2, 2022, Hub, Edge, HCIv2):



Power & sleep

Screen

When plugged in, turn off after

2 minutes

Related settings

Additional power settings

The evaluator has obtained the same result for both users, the screen has been blocked after the configured inactivity time is reached.

37.2.2.4 Verdict

As the above results state, both users with administrator rights and without administrator rights can configure the screen lock inactivity timeout.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 2** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 2**.

37.2.3 Test 3 - Configure Local Audit Storage Capacity

The local audit storage capacity will be configured during this test case.

37.2.3.1 Setup

The applicable setup for this test is the same as the defined one for Test 1.

37.2.3.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

37.2.3.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)

- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

37.2.3.4 Verdict

As the above results state, the audit storage capacity can only be modified by a user with administrator rights.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 3** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 3**.

37.2.4 Test 4 - Configure Minimum Password Length

A minimum password length will be configured during this test case.

37.2.4.1 Setup

The applicable setup for this test is the same as the defined one for Test 1.

37.2.4.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

37.2.4.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)

- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)

- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

37.2.4.4 Verdict

As the above results state, the minimum password length can only be modified by a user with administrator rights.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 4** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 4**.

37.2.5 Test 9 - Configure Lockout Policy for Unsuccessful Authentication Attempts through Timeouts between Attempts, Limiting Number of Attempts During a Time Period

The lockout policy for unsuccessful authentication will be configured during this test case.

37.2.5.1 Setup

The applicable setup for this test is the same as the defined one for Test 1.

37.2.5.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

37.2.5.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)

- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

37.2.5.4 Verdict

As the above results state, the lockout policy for unsuccessful authentication attempts can only be modified by a user with administrator rights.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 9** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 9**.

37.2.6 Test 10 - Configure Host-based Firewall

The host-based firewall will be configured during this test case.

37.2.6.1 Setup

The applicable setup for this test is the same as the defined one for Test 1.

37.2.6.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

37.2.6.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)

- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

37.2.6.4 Verdict

As the above results state, the firewall configuration can only be modified by a user with administrator rights.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 10** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 10**.

37.2.7 Test 11 - Configure Name/Address of Directory Server to Bind with

The evaluator will configure the name/address of directory server to bind with and remote management server during this test case.

37.2.7.1 Setup

The applicable setup for this test is the same as the defined one for Test 1.

To configure a domain controller, the applicable setup for this test is described in *Configuring Domain Controller and Certificate Authority (13 Apr 2017)* document.

On the platforms with Windows Server and Azure editions, once these platforms are joined to the domain, the domain controller can be configured as a remote management server. Therefore, they can receive management settings without using a MDM server (which is not supported on those editions). The procedure used to join these platforms to the domain will be described in this test activity, whereas, the procedure to receive management settings will be explained in detail in the test activity: *Test 12 - Configure name/address of remote management server from which to receive management settings*.

37.2.7.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

37.2.7.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)

- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

37.2.7.4 Verdict

As the above results state, a computer can only be joined to a domain using a user with administrator rights. When a user without administrator rights is used, a prompt asking for the administrator password is shown or the join to domain option does not appear.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 11** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 11**.

37.2.8 Test 12 - Configure Name/Address of Remote Management Server from Which to Receive Management Settings

The evaluator will configure the name/address of remote management server during this test case.

37.2.8.1 Setup

The applicable setup for this test is the same as the defined one for Test 1.

Additionally, a MDM Server running in another machine is necessary. For this test case, a MDM Server provided by the vendor has been used.

To enroll a device with a MDM, the evaluator has followed the applicable setup and steps described in the links provided in section **2.4.1 Remote administration using modern device management (MDM)** of the ***Operational Guidance*** document.

On the platforms with Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions, once these platforms are joined to the domain, the domain controller can be configured as a remote management server. Therefore, they can receive management settings without using a MDM server (which is not supported on Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions). The procedure used to join these platforms to the domain it is described in the test activity: *Test 11 - Configure name/address of directory server to bind with*, whereas, the procedure to receive management settings will be explained in detail in this test activity.

37.2.8.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

37.2.8.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)

- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)

- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

37.2.8.4 Verdict

As the above results state, a computer can only be enrolled into a remote management server using a user with administrator rights. When a user without administrator rights is used, an insufficient privileges error message is shown.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 12** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 12**.

37.2.9 Test 14 - Configure Audit Rules

The audit rules will be configured during this test case.

37.2.9.1 Setup

The applicable setup for this test is the same as the defined one for Test 1.

37.2.9.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

37.2.9.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)

- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

37.2.9.4 Verdict

As the above results state, the audit rules can only be configured using a user with administrator rights.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 14** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 14**.

37.2.10 Test 15 - Configure Name/Address of Network Time Server

The name and address of a Network Time Server will be configured during this test case

37.2.10.1 Setup

The applicable setup for this test is the same as the defined one for Test 1.

37.2.10.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

37.2.10.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)

- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

37.2.10.4 Verdict

As the above results state, the name or address of the network time server can only be modified by a user with administrator rights.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 15** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 15**.

37.2.11 Test 16 - Enable/Disable Automatic Software Update

The automatic software update will be enabled and disabled during this test case.

37.2.11.1 Setup

The applicable setup for this test is the same as the defined one for Test 1.

37.2.11.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

37.2.11.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)

- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

37.2.11.4 Verdict

As the above results state, the automatic software update can only be enabled or disabled using a user with administrator rights.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 16** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 16**.

37.2.12 Test 17 - Configure Wi-Fi interface

The Wi-Fi interface will be configured during this test case.

37.2.12.1 Setup

The applicable setup for this test is the same as the defined one for Test 1.

To perform this test, the platforms should have a Wi-Fi interface available.

37.2.12.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

37.2.12.3 Results

The evaluator has performed this test on all the canonical platforms (except the ones without Wi-Fi adapter) as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

37.2.12.4 Verdict

As the above results state, a Wi-Fi interface can only be enabled or disabled using a user with administrator rights.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 17** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 17**.

37.2.13 Test 18 - Enable/Disable Bluetooth interface

The Bluetooth interface will be enabled and disabled during this test case.

37.2.13.1 Setup

The applicable setup for this test is the same as the defined one for Test 1.

In addition, to perform this test, the platforms should have a Bluetooth interface available.

37.2.13.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

37.2.13.3 Results

The evaluator has performed this test on all the canonical platforms (except the ones without Wi-Fi adapter) as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

37.2.13.4 Verdict

As the above results state, a Bluetooth interface can only be enabled or disabled using a user with administrator rights.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 18** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 18**.

37.2.14 Test 19 - Enable/Disable Local Area Network interface

The Local Area Network interface will be enabled and disabled during this test case.

37.2.14.1 Setup

The applicable setup for this test is the same as the defined one for Test 1.

37.2.14.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

37.2.14.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)

- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)

- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

37.2.14.4 Verdict

As the above results state, a Local Area Network interface can only be configured by a user with administrator rights.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 19** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 19**.

37.2.15 Test 19 (2) - Configure USB interfaces

The USB interfaces will be configured during this test case.

37.2.15.1 Setup

The applicable setup for this test is the same as the defined one for Test 1.

37.2.15.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

37.2.15.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)

- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

37.2.15.4 Verdict

As the above result state, the configuration of USB interfaces can only be modified by a user with administrator rights.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 19 (2)** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 19 (2)**.

37.2.16 Test 20 - Manage Windows Diagnostics settings

Windows Diagnostics settings will be configured during this test case.

37.2.16.1 Setup

The applicable setup for this test is the same as the defined one for Test 1.

37.2.16.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

37.2.16.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)

- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

37.2.16.4 Verdict

As the above results state, only users with administrator rights can manage the Windows diagnostic data and choose between *Basic* and *Full* diagnostic data mode.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 20** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 20**.

37.2.17 Test 20 (2) - Configure Remote Connection Inactivity Timeout

Remote connection inactivity timeout will be configured during this test case.

37.2.17.1 Setup

The applicable setup for this test is the same as the defined one for Test 1.

37.2.17.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

37.2.17.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)

- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)

- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

37.2.17.4 Verdict

As the above results state, the remote connection inactivity timeout can only be modified by a user with administrator rights.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 20 (2)** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 20 (2)**.

37.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FMT_MOF_EXT.1.1-FMT_SMF_EXT.1.1.

38 FPT_ACF_EXT.1.1

The assurance activity for the **FPT_ACF_EXT.1.1** requirement is stated as follows:

> The evaluator will confirm that the TSS specifies the locations of kernel drivers/modules, security audit logs, shared libraries, system executables, and system configuration files. Every file does not need to be individually identified, but the system's conventions for storing and protecting such files must be specified. The evaluator will create an unprivileged user account. Using this account, the evaluator will ensure that the following tests result in a negative outcome (i.e., the action results in the OS denying the evaluator permission to complete the action):
>
> - **Test 1:** The evaluator will attempt to modify all kernel drivers and modules.
> - **Test 2:** The evaluator will attempt to modify all security audit logs generated by the logging subsystem.
> - **Test 3:** The evaluator will attempt to modify all shared libraries that are used throughout the system.
> - **Test 4:** The evaluator will attempt to modify all system executables.
> - **Test 5:** The evaluator will attempt to modify all system configuration files.
> - **Test 6:** The evaluator will attempt to modify any additional components selected.

38.1 Documentation Review Activity

38.1.1 Findings

The evaluator has reviewed the section **6.6.2.Protection of OS binaries, Audit and Configuration Data** of the ***Security Target*** document. This section states that kernel, device drivers (*.sys files*), system executables (*.exe files*), and dynamically loadable libraries (*.dll files*) are stored in \%systemRoot%\system32 directory and subdirectories.

Additionally, the TSS also states that audit logs are stored in %systemRoot%\system32\winevt and configuration files are located at %systemRoot%\system32\config.

In addition, an explanation on how the permissions are applied over these kinds of files is given. Standard users have permissions to read and execute kernel, device drivers, system executables and libraries, and they are not authorized to access audit logs and configuration files. However, administrator users have permissions to write and modify kernel, device drivers, system executables and libraries, and have full control over audit logs and configuration files.

38.1.2 Verdict

The evaluator considers that the TSS provides enough information related to where kernel, device drivers, system executables, libraries, configuration files, and audit logs are stored in the system and how the permissions are applied over these files.

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfilment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

38.2 Test Activity

38.2.1 Test 1

The evaluator will attempt to modify all kernel drivers and modules during this test case.

38.2.1.1 Setup

Before the test execution, the following setup condition must be fulfilled:

- A user account without administrator rights shall be available.
- The *PowerShell* execution policy shall be configured to allow the execution of *PowerShell* scripts. To do it, execute in a *Powershell* terminal with administrator rights the command:

  ```
  Set-ExecutionPolicy Unrestricted -Force
  ```

- Scripts *Test1_FPT_ACF_EXT_1_1.ps1*, *Test2_FPT_ACF_EXT_1_1.ps1*, *Test3_FPT_ACF_EXT_1_1.ps1*, *Test4_FPT_ACF_EXT_1_1.ps1* and *Test5_FPT_ACF_EXT_1_1.ps1* shall be available.

38.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

38.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Panasonic CF-33 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R840 with Azure Stack Edge (build 10.0.17784.1068)
- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Voyager Klaas Telecom with Azure Stack Hub (build 10.0.17784.1068)
- HPE Edgeline EL8000 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results in all tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE’s behavior is as expected and detailed in the security target [ST004].

38.2.1.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

38.2.2 Test 2

The evaluator will attempt to modify all security audit logs during this test case.

38.2.2.1 Setup

The applicable setup for this test is the same as the defined one for Test 1.

38.2.2.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

38.2.2.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Panasonic CF-33 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R840 with Azure Stack Edge (build 10.0.17784.1068)
- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Voyager Klaas Telecom with Azure Stack Hub (build 10.0.17784.1068)
- HPE Edgeline EL8000 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587

The evaluator has obtained the same results in all tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

38.2.2.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 2** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 2**.

38.2.3 Test 3

The evaluator will attempt to modify all shared libraries during this test case.

38.2.3.1 Setup

The applicable setup for this test is the same as the defined one for Test 1.

38.2.3.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

38.2.3.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Panasonic CF-33 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R840 with Azure Stack Edge (build 10.0.17784.1068)
- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Voyager Klaas Telecom with Azure Stack Hub (build 10.0.17784.1068)
- HPE Edgeline EL8000 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)

- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results in all tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

38.2.3.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 3** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 3**.

38.2.4 Test 4

The evaluator will attempt to modify all system executable files during this test case.

38.2.4.1 Setup

The applicable setup for this test is the same as the defined one for Test 1.

38.2.4.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

38.2.4.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Panasonic CF-33 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R840 with Azure Stack Edge (build 10.0.17784.1068)
- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)

- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Voyager Klaas Telecom with Azure Stack Hub (build 10.0.17784.1068)
- HPE Edgeline EL8000 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results in all tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

38.2.4.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 4** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 4**.

38.2.5 Test 5

The evaluator will attempt to modify all system configuration files during this test case.

38.2.5.1 Setup

The applicable setup for this test is the same as the defined one for Test 1.

38.2.5.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

38.2.5.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Panasonic CF-33 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R840 with Azure Stack Edge (build 10.0.17784.1068)
- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Voyager Klaas Telecom with Azure Stack Hub (build 10.0.17784.1068)
- HPE Edgeline EL8000 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results in all tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

38.2.5.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 5** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 5**.

38.2.6 Test 6

The evaluator will attempt to modify additional selected components during this test case.

38.2.6.1 Setup

This test is not applicable due to the assignment (**None**) made by the vendor in the ***Security Target*** document.

38.2.6.2 Procedure

This test is not applicable due to the assignment (**None**) made by the vendor in the ***Security Target*** document.

38.2.6.3 Results

This test is not applicable due to the assignment (**None**) made by the vendor in the ***Security Target*** document.

38.2.6.4 Verdict

This test is not applicable due to the assignment made (**None**) by the vendor in the ***Security Target*** document.

38.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FPT_ACF_EXT.1.1.

39 FPT_ACF_EXT.1.2

The assurance activity for the **FPT_ACF_EXT.1.2** requirement is stated as follows:

> The evaluator will create an unprivileged user account. Using this account, the evaluator will ensure that the following tests result in a negative outcome (i.e., the action results in the OS denying the evaluator permission to complete the action):
>
> - **Test 1:** The evaluator will attempt to read security audit logs generated by the auditing subsystem
> - **Test 2:** The evaluator will attempt to read system-wide credential repositories
> - **Test 3:** The evaluator will attempt to read any other object specified in the assignment

39.1 Documentation Review Activity

39.1.1 Findings

The related assurance activity does not define any action for this requirement.

39.1.2 Verdict

The related assurance activity does not define any action for this requirement. Therefore, the **PASS** verdict is assigned to the documentation review activity.

39.2 Test Activity

39.2.1 Test 1

The evaluator will attempt to read all the security audit logs during this test case.

39.2.1.1 Setup

Before the test execution, the following setup condition must be fulfilled:

- A user account without administrator rights shall be available.
- The *PowerShell* execution policy shall be configured to allow the execution of *PowerShell* scripts. To do it, execute in a *Powershell* terminal with administrator rights the command:

```
Set-ExecutionPolicy Unrestricted -Force
```

- Scripts *Test1_FPT_ACF_EXT_1_2.ps1* and *Test2_FPT_ACF_EXT_1_2.ps1* shall be available.

39.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

39.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Panasonic CF-33 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R840 with Azure Stack Edge (build 10.0.17784.1068)
- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Voyager Klaas Telecom with Azure Stack Hub (build 10.0.17784.1068)
- HPE Edgeline EL8000 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results in all tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

39.2.1.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

39.2.2 Test 2

The evaluator will attempt to read system-wide credential repositories during this test case.

39.2.2.1 Setup

The applicable setup for this test is the same as the defined one for Test 1.

39.2.2.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

39.2.2.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Panasonic CF-33 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R840 with Azure Stack Edge (build 10.0.17784.1068)
- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Voyager Klaas Telecom with Azure Stack Hub (build 10.0.17784.1068)
- HPE Edgeline EL8000 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results in all tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

39.2.2.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 2** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 2**.

39.2.3 Test 3

The evaluator will attempt to read additional selected objects during this test case.

39.2.3.1 Setup

This test is not applicable due to the assignment (**None**) made by the vendor in the ***Security Target*** document.

39.2.3.2 Procedure

This test is not applicable due to the assignment (**None**) made by the vendor in the ***Security Target*** document.

39.2.3.3 Results

This test is not applicable due to the assignment (**None**) made by the vendor in the ***Security Target*** document.

39.2.3.4 Verdict

This test is not applicable due to the assignment (**None**) made by the vendor in the ***Security Target*** document.

39.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FPT_ACF_EXT.1.2.

40 FPT_ASLR_EXT.1.1

The assurance activity for the **FPT_ASLR_EXT.1.1** requirement is stated as follows:

> The evaluator will select 3 executables included with the TSF. If the TSF includes a web browser it must be selected. If the TSF includes a mail client it must be selected. For each of these apps, the evaluator will launch the same executables on two separate instances of the OS on identical hardware and compare all memory mapping locations. The evaluator will ensure that no memory mappings are placed in the same location. If the rare chance occurs that two mappings are the same for a single executable and not the same for the other two, the evaluator will repeat the test with that executable to verify that in the second test the mappings are different. This test can also be completed on the same hardware and rebooting between application launches.

40.1 Documentation Review Activity

40.1.1 Findings

The related assurance activity does not define any action for this requirement.

40.1.2 Verdict

The related assurance activity does not define any action for this requirement. Therefore, the **PASS** verdict is assigned to the documentation review activity.

40.2 Test Activity

Three different executables included with the TSF will be launched in order to verify that no memory mappings are placed in the same location for two different instances of the same executable.

40.2.1 Test 1

40.2.1.1 Setup

Before the test execution, the following setup condition must be fulfilled:

- *VMMap* tool (a Sysinternal utility that provides the ability to analyze the physical memory) shall be available.

The three executables, which shall be used during the test execution and included with the TSF, are the following:

- Command Prompt (*cmd.exe*).
- Microsoft Edge (*MicrosoftEdge.exe*). For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions, the Notepad application (*notepad.exe*) will be used instead.
- Mail App (a Trusted Windows Store App, whose process name is *HxOutlook.exe*). For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions, the Registry Editor application (*regedit.exe*) will be used instead.

40.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

40.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, all the supplementary platforms have been also tested.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

40.2.1.4 Verdict

As it can be observed in the above images in all cases the memory assigned to one process is different. Therefore, from the results of the previous test, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

40.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FPT_ASLR_EXT.1.1.

41 FPT_SBOP_EXT.1.1

The assurance activity for the **FPT_SBOP_EXT.1.1** requirement is stated as follows:

> For stack-based OSes, the evaluator will determine that the TSS contains a description of stack-based buffer overflow protections used by the OS. These are referred to by a variety of terms, such as stack cookie, stack guard, and stack canaries. The TSS must include a rationale for any binaries that are not protected in this manner. The evaluator will also perform the following test:
>
> - **Test 1:** The evaluator will inventory the kernel, libraries, and application binaries to determine those that do not implement stack-based buffer overflow protections. This list should match up with the list provided in the TSS.
>
> For OSes that store parameters/variables separately from control flow values, the evaluator will verify that the TSS describes what data structures control values, parameters, and variables are stored. The evaluator will also ensure that the TSS includes a description of the safeguards that ensure parameters and variables do not intermix with control flow values.

41.1 Documentation Review Activity

41.1.1 Findings

The evaluator has reviewed the information provided in TSS, section **6.6.3 Protection From Implementation Weaknesses**. This section includes a list about the protections implemented by the TOE. (e.g. *Data Execution Prevention (DEP)* or *Address Space Layout Randomization (ASLR)*).

This TSS section states that all Windows binaries and Windows Store Applications implement stack buffer overrun protection by being compiled with the */GS* option. Moreover, *Windows Store* Applications are checked if they are compiled or not with the buffer overrun protection before ingesting them into the *Windows Store*.

Related to the Windows binaries files, the TSS lists the files which are not compiled with the buffer overrun protection. Including for all of them, a rationale explaining its exclusion. These files are the following:

- *ntoskrnl.exe*, *ntkrla57.exe*, *winload.exe*, *winresume.exe*, *tcblaunch.exe*, *tcbloader.dll*, *hvloader.exe*, *wintrust.dll* and *manageci.dll*.
  - These files are loaded before the stack buffer overrun protection mechanism is operational. Therefore, these files are not compiled with this option.
  - Text intentionally left blank.

41.1.2 Verdict

The evaluator considers that the TSS provides enough information related to the stack-base overflow protections implemented by the TOE.

In addition, the TSS has indicated that all windows binaries and Windows Apps have been compiled with the */GS* option except four files (*ntoskrnl.exe*, *ntkrla57.exe*, *winload.exe*, *winresume.exe*, *tcblaunch.exe*, *tcbloader.dll*, *hvloader.exe*, *wintrust.dll* and *manageci.dll*.). A rationale explaining why these files have not been compiled with */GS* option has been provided.

Hence, the **PASS** verdict is assigned to the documentation review activity.

41.2 Test Activity

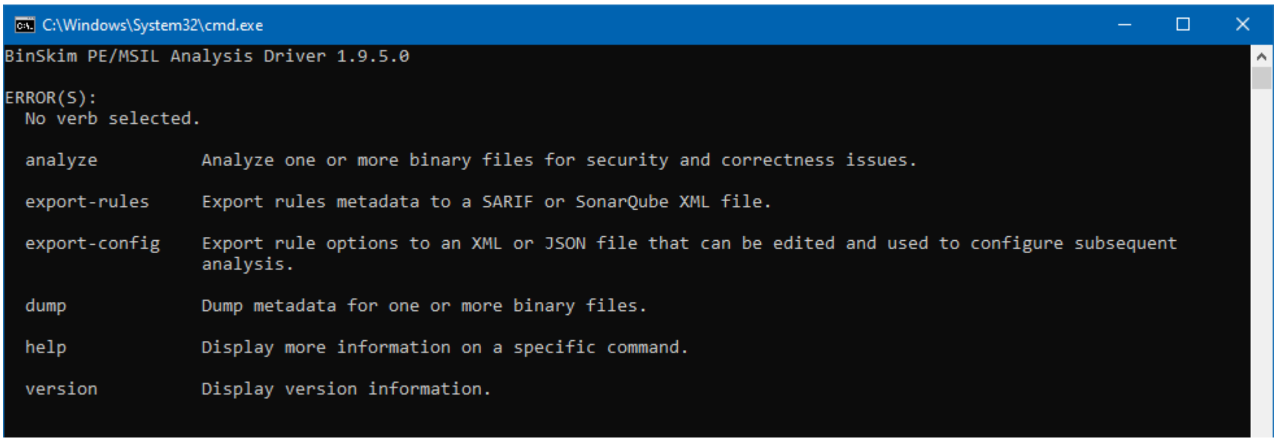
41.2.1 Test 1

41.2.1.1 Setup

To do this test, the evaluator shall have access to the *BinSkim* tool and the private symbols to analyze the system binaries to find out whether they have been compiled with stack-based overflow protections or not.

The following tools are available to the evaluator:

- *Copy-SystemFiles.ps1*: This PowerShell scripts allow the evaluator to copy all the system executables, drivers and libraries stored in the system folder %windir%\System32, maintaining its tree directory structure.
- *BinSkimmer*: an internal tool developed by the vendor, that allows to check the system binaries gathered by the previous scripts, by using the BinSkim utility.



```
BinSkim PE/MSIL Analysis Driver 1.9.5.0

ERROR(S):
  No verb selected.

  analyze          Analyze one or more binary files for security and correctness issues.

  export-rules     Export rules metadata to a SARIF or SonarQube XML file.

  export-config    Export rule options to an XML or JSON file that can be edited and used to configure subsequent
                   analysis.

  dump             Dump metadata for one or more binary files.

  help             Display more information on a specific command.

  version          Display version information.
```

41.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

41.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, all the supplementary platforms have been also tested.

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

41.2.1.4 Verdict

As it can be observed the obtained results have been the same as the ones expected according to the TSS definition. Therefore, from the results of the previous test, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

41.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FPT_SBOP_EXT.1.1.

42 FPT_SRP_EXT.1.1

The assurance activity for the **FPT_SRP_EXT.1.1** requirement is stated as follows:

> For each selection specified in the ST, the evaluator will ensure that the corresponding tests result in a negative outcome (i.e., the action results in the OS denying the evaluator permission to complete the action):
>
> - **Test 1:** The evaluator will configure the OS to only allow code execution from the core OS directories. The evaluator will then attempt to execute code from a directory that is in the allowed list. The evaluator will ensure that the code they attempted to execute has been executed.
> - **Test 2:** The evaluator will configure the OS to only allow code execution from the core OS directories. The evaluator will then attempt to execute code from a directory that is not in the allowed list. The evaluator will ensure that the code they attempted to execute has not been executed.
> - **Test 3:** The evaluator will configure the OS to only allow code that has been signed by the OS vendor to execute. The evaluator will then attempt to execute code signed by the OS vendor. The evaluator will ensure that the code they attempted to execute has been executed.
> - **Test 4:** The evaluator will configure the OS to only allow code that has been signed by the OS vendor to execute. The evaluator will then attempt to execute code signed by another digital authority. The evaluator will ensure that the code they attempted to execute has not been executed.
> - **Test 5:** The evaluator will configure the OS to allow execution of a specific application based on version. The evaluator will then attempt to execute the same version of the application. The evaluator will ensure that the code they attempted to execute has been executed.
> - **Test 6:** The evaluator will configure the OS to allow execution of a specific application based on version. The evaluator will then attempt to execute an older version of the application. The evaluator will ensure that the code they attempted to execute has not been executed.
> - **Test 7:** The evaluator will configure the OS to allow execution based on the hash of the application executable. The evaluator will then attempt to execute the application with the matching hash. The evaluator will ensure that the code they attempted to execute has been executed.
> - **Test 8:** The evaluator will configure the OS to allow execution based on the hash of the application executable. The evaluator will modify the application in such a way that the application hash is changed. The evaluator will then attempt to execute the application with the matching hash. The evaluator will ensure that the code they attempted to execute has not been executed.

42.1 Documentation Review Activity

42.1.1 Findings

The related assurance activity does not define any action for this requirement.

42.1.2 Verdict

The related assurance activity does not define any action for this requirement. Therefore, the **PASS** verdict is assigned to the documentation review activity.

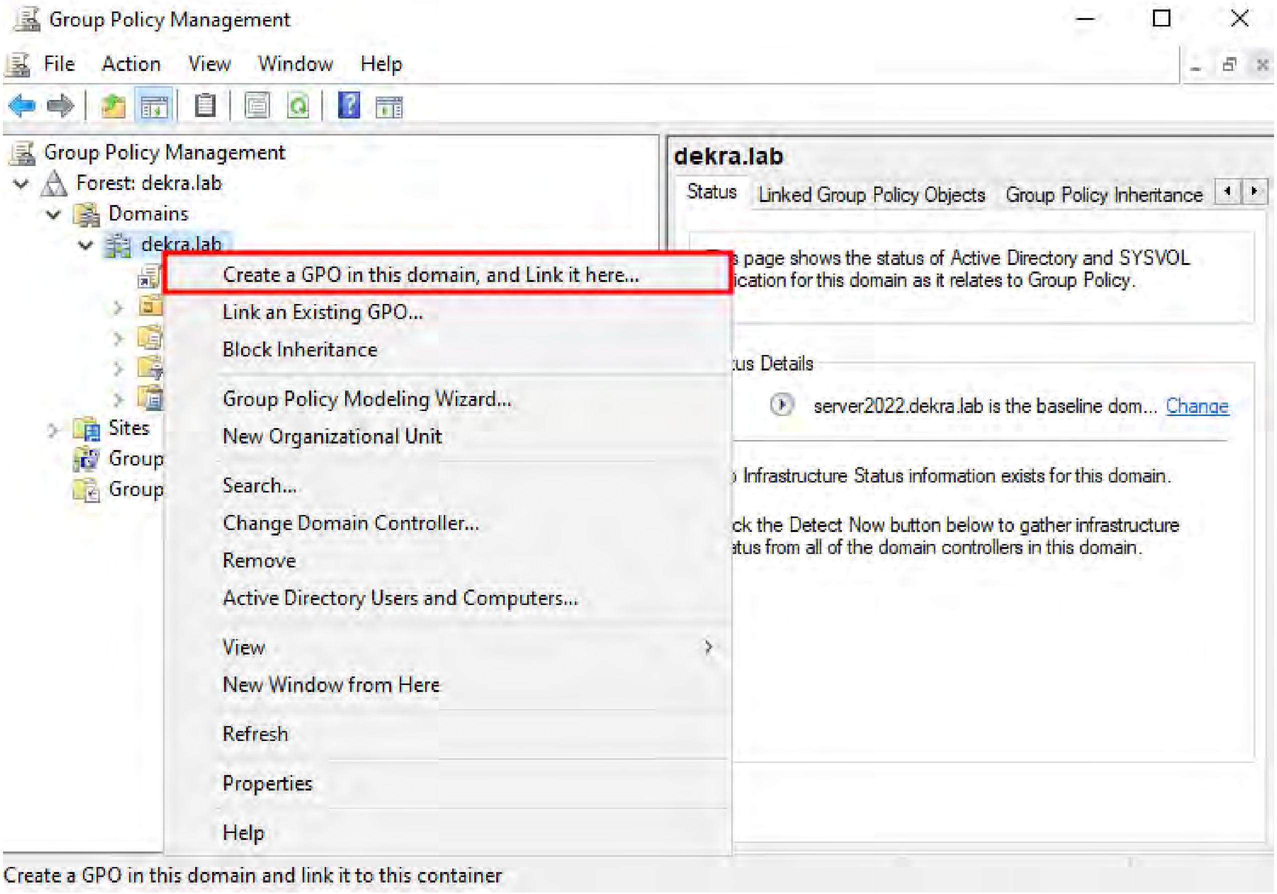
42.2 Test Activity

To perform the test activities described below over the Azure Stack HCIv2 edition, the following setup condition must be fulfilled:

- The platform must be joined to a domain. The steps required to join this computer to a domain are described in *Test 11 for FMT_MOF_EXT.1* requirement.

Once the platform is domain-joined, the following steps shall be performed to configure the Software Restriction Policies through a GPO (*Group Policy Object*).

- On the domain computer, open the *Group Policy Management* tool (*WIN+R* and then type "*gpmc.msc*").
- Navigate through the forest and select the name of your domain controller. Right click over it and select *Create a GPO in this domain, and Link it here...* option.



s page shows the status of Active Directory and SYSVOL ication for this domain as it relates to Group Policy.

us Details

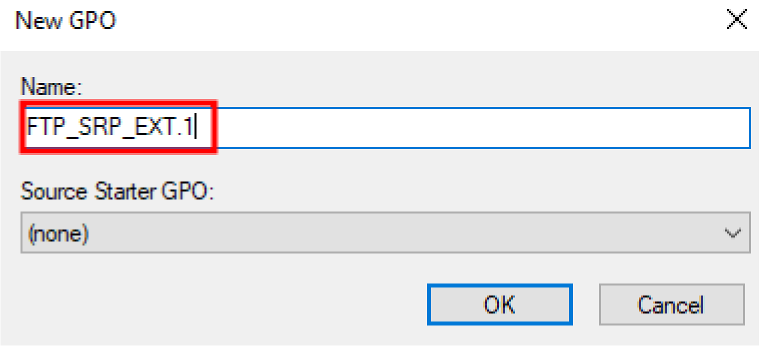
server2022.dekra.lab is the baseline dom...

Infrastructure Status information exists for this domain.

ck the Detect Now button below to gather infrastructure atus from all of the domain controllers in this domain.

Create a GPO in this domain and link it to this container

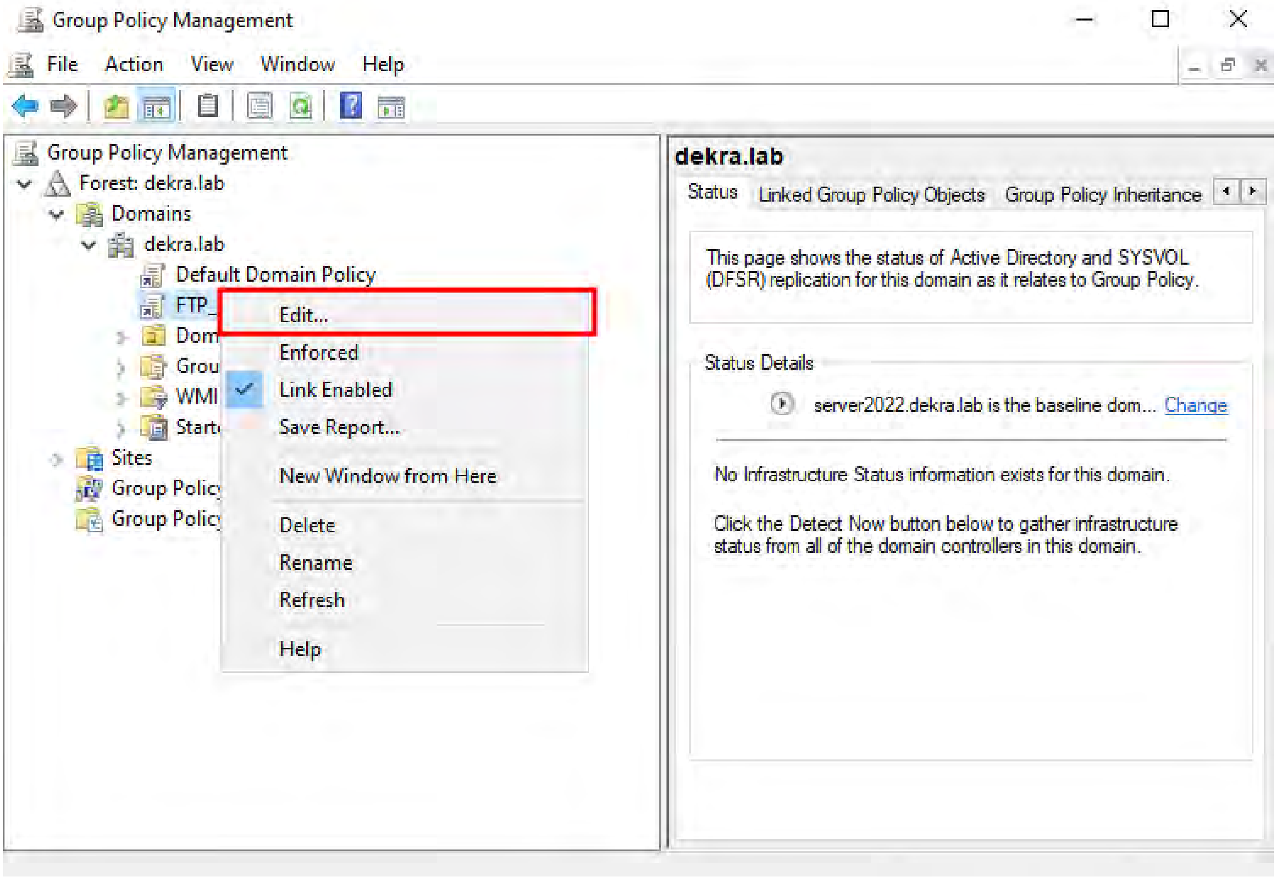
- Then, a new window will appear asking for a GPO name. Type any name, e.g. *Test FTP_SRP_EXT.1*, and click the *OK* button.



Name: FTP_SRP_EXT.1

Source Starter GPO: (none)

- Afterwards, on the GPO created in the previous steps, right click on it and select the *Edit* option.



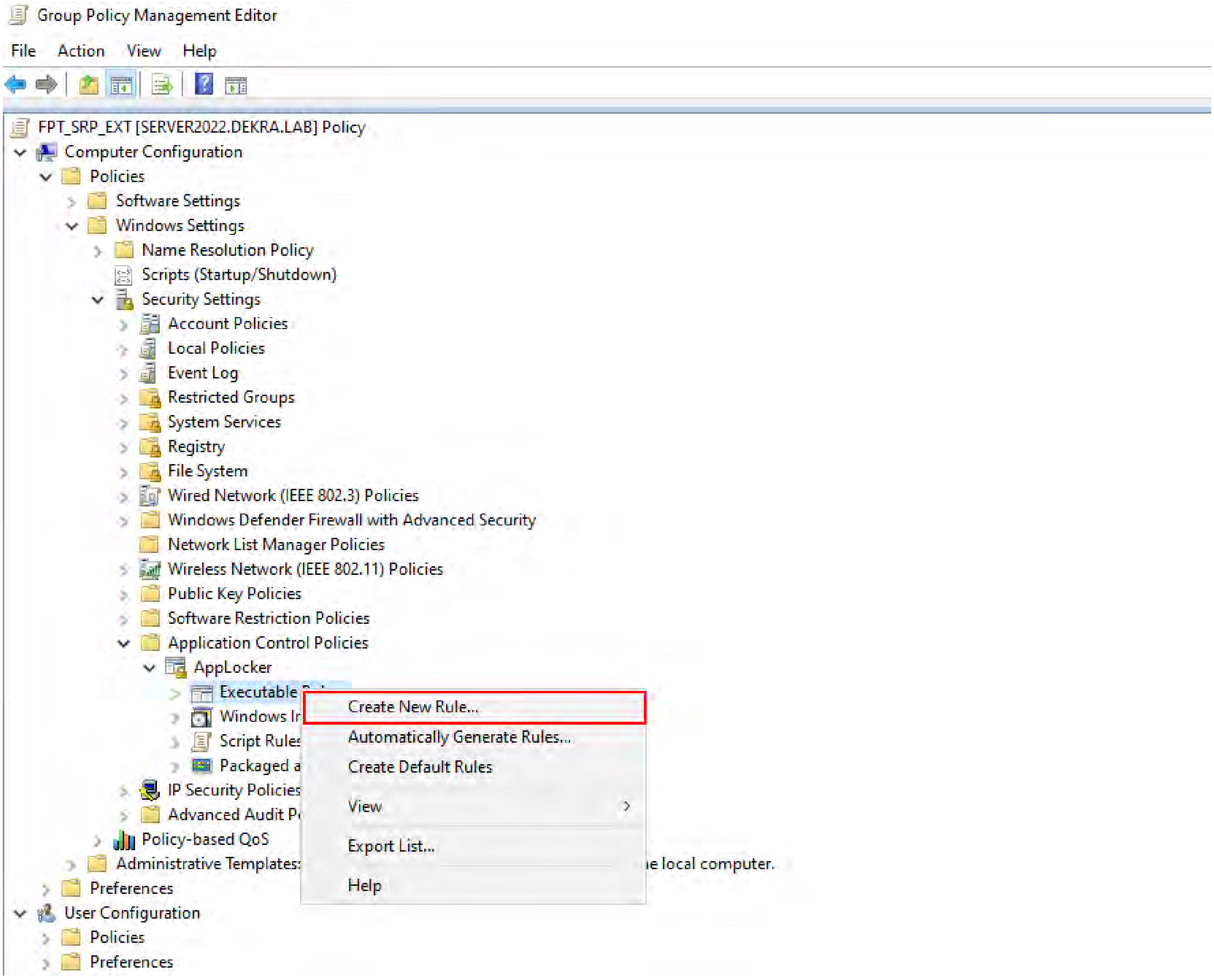
This page shows the status of Active Directory and SYSVOL (DFSR) replication for this domain as it relates to Group Policy.

server2022.dekra.lab is the baseline dom...

No Infrastructure Status information exists for this domain.

Click the Detect Now button below to gather infrastructure status from all of the domain controllers in this domain.

- After that, the evaluator shall navigate to *Computer Configuration* -> *Policies* -> *Windows Settings* -> *Security Settings* -> *Application Control Policies* -> *AppLocker* and enabling the *Remove Task manager* option.



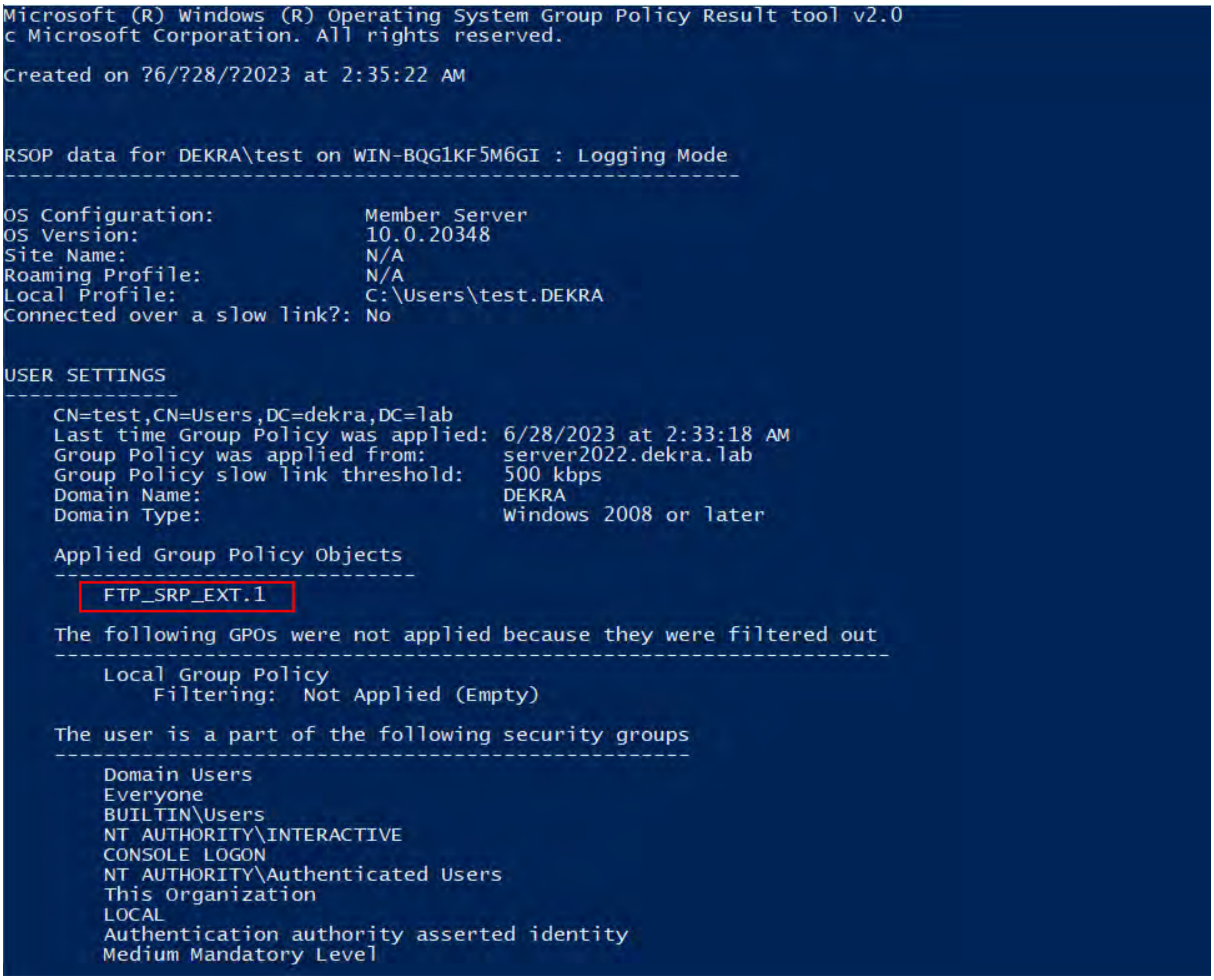
The following procedures

- These GPOs are configured the same way as described below (*Skipping the first step*). Once the GPOs are configured, they are deployed automatically over all the Authenticated computers joined to the domain.
- In some cases, the policy is not successfully deployed. To force the correct deployment on the remote computer, execute the following command:

```
gpupdate /force
```

- To verify on the domain-joined computer the correct deployment of a GPO, the following command can be executed:

```
gpresult /r
```



```
Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
c Microsoft Corporation. All rights reserved.

Created on ?6/?28/?2023 at 2:35:22 AM


RSOP data for DEKRA\test on WIN-BQG1KF5M6GI : Logging Mode
-----------------------------------------------------------

OS Configuration:            Member Server
OS Version:                  10.0.20348
Site Name:                   N/A
Roaming Profile:             N/A
Local Profile:               C:\Users\test.DEKRA
Connected over a slow link?: No


USER SETTINGS
--------------
    CN=test,CN=Users,DC=dekra,DC=lab
    Last time Group Policy was applied: 6/28/2023 at 2:33:18 AM
    Group Policy was applied from:      server2022.dekra.lab
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        DEKRA
    Domain Type:                        Windows 2008 or later

    Applied Group Policy Objects
    -----------------------------
        FTP_SRP_EXT.1

    The following GPOs were not applied because they were filtered out
    -------------------------------------------------------------------
        Local Group Policy
            Filtering:  Not Applied (Empty)

    The user is a part of the following security groups
    ---------------------------------------------------
        Domain Users
        Everyone
        BUILTIN\Users
        NT AUTHORITY\INTERACTIVE
        CONSOLE LOGON
        NT AUTHORITY\Authenticated Users
        This Organization
        LOCAL
        Authentication authority asserted identity
        Medium Mandatory Level
```

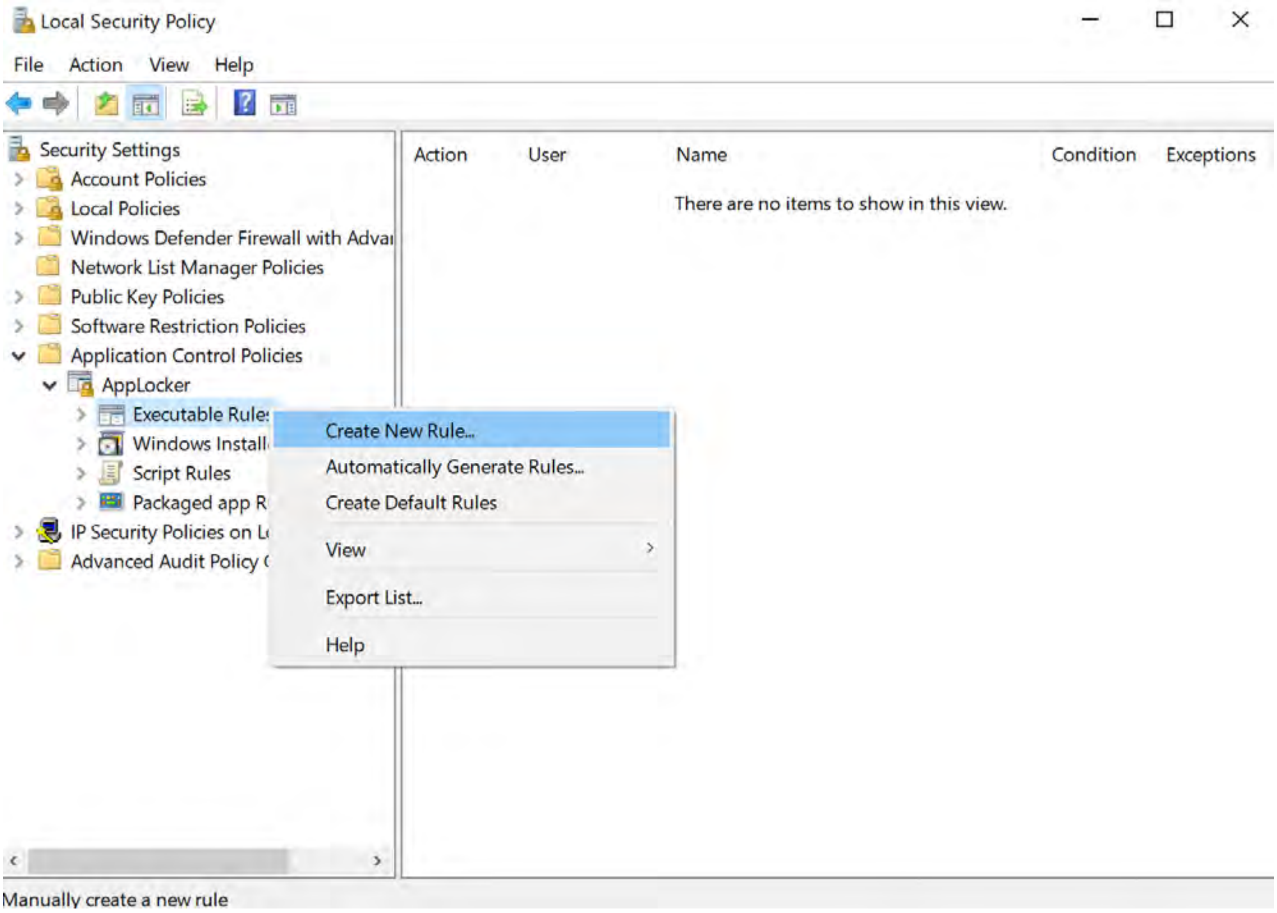
42.2.1 Test 1 & Test 2

This test configures the OS to only allow code execution from the core OS directories. An application will be executed, first from a directory in the whitelist, then from a directory in the blacklist.

42.2.1.1 Setup

To execute this test, an Application Control Policy must be enabled. To do that, the evaluator should perform these next steps:

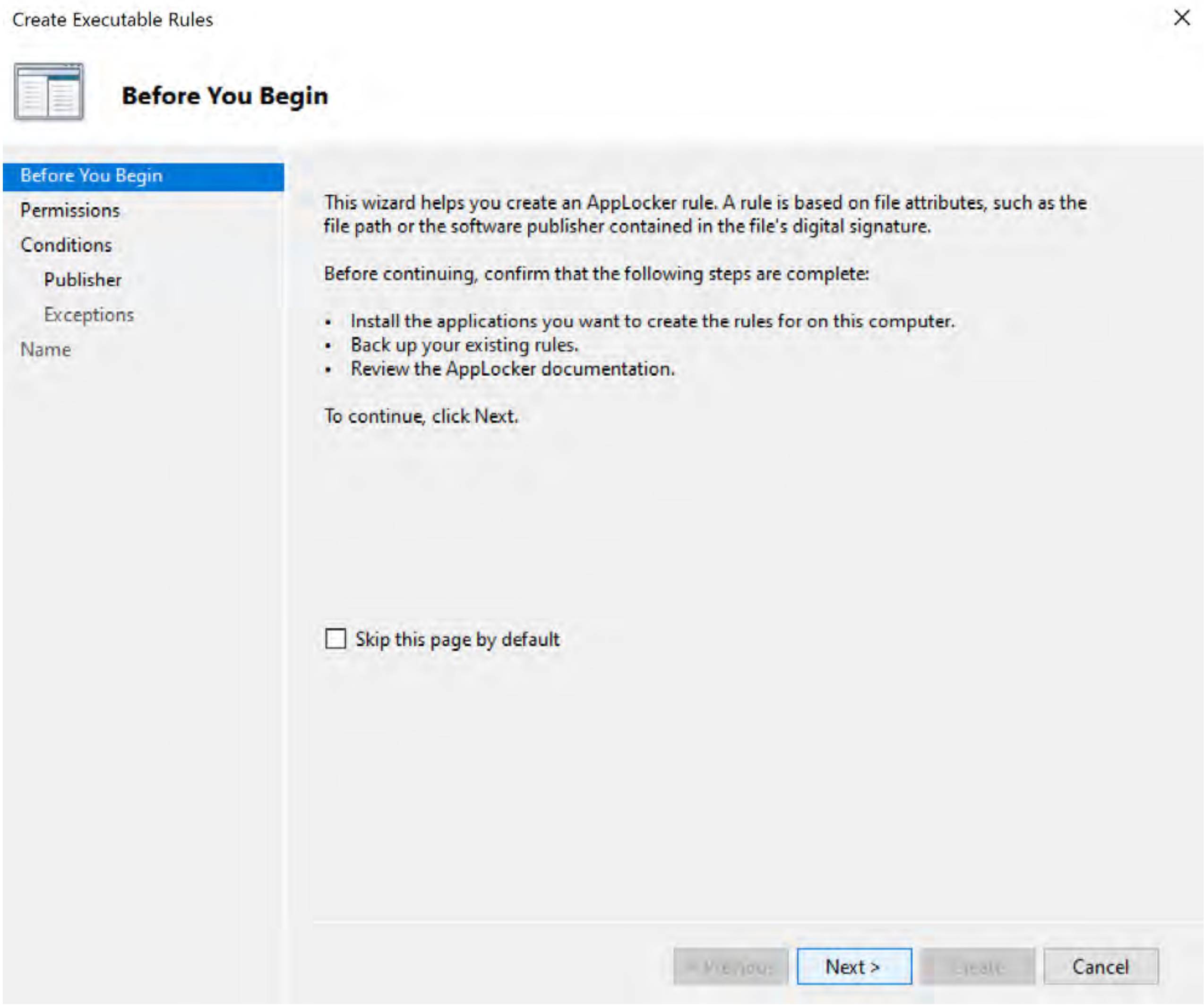
- Open the *Local Security Policy* Window (*WIN* + *R*, then type *secpol.msc*)
- Go to *Security Settings* -> *Application Control Policies* -> *AppLocker* -> *Executable Rules*. Right-click on it and select *Create New Rule...*



There are no items to show in this view.

Manually create a new rule

- Then, click *next*.



This wizard helps you create an AppLocker rule. A rule is based on file attributes, such as the file path or the software publisher contained in the file's digital signature.

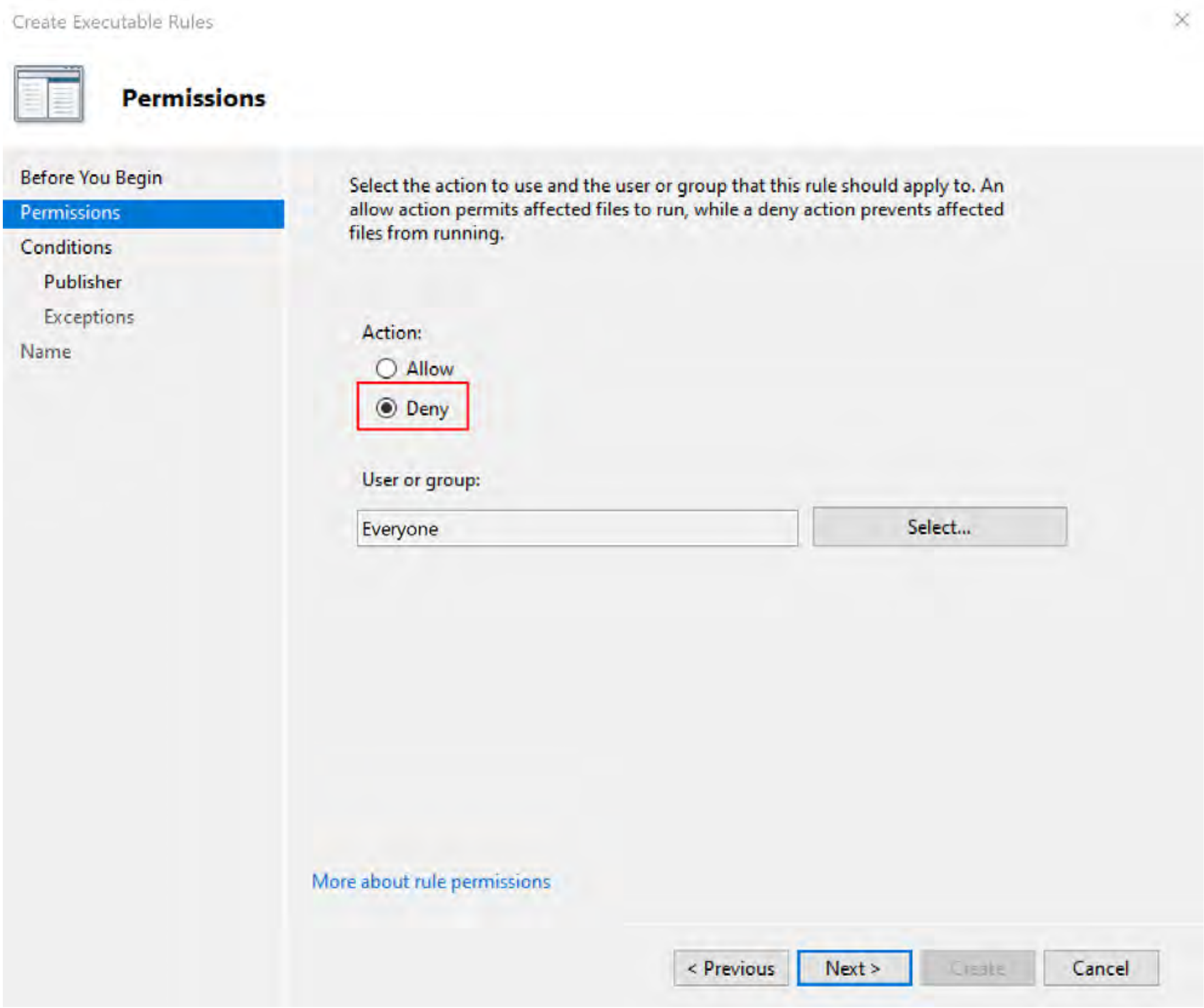
Before continuing, confirm that the following steps are complete:

- Install the applications you want to create the rules for on this computer.
- Back up your existing rules.
- Review the AppLocker documentation.

To continue, click Next.

□ Skip this page by default

- Select *Deny*.

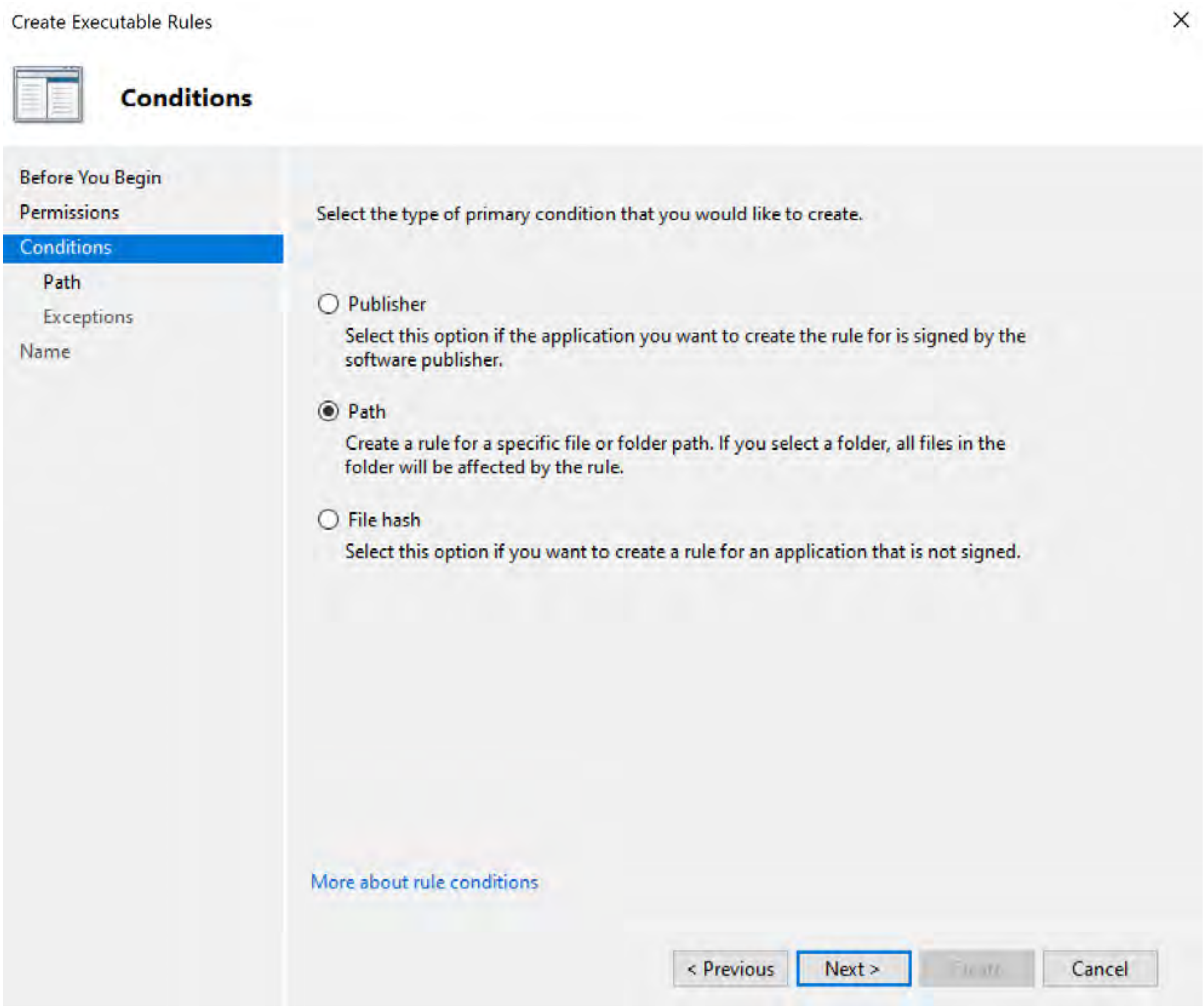


Select the action to use and the user or group that this rule should apply to. An allow action permits affected files to run, while a deny action prevents affected files from running.

Action:
○ Allow
● Deny

User or group:
Everyone
Select...

- Select *Path*, and then browse and select the *Desktop* folder.



Conditions

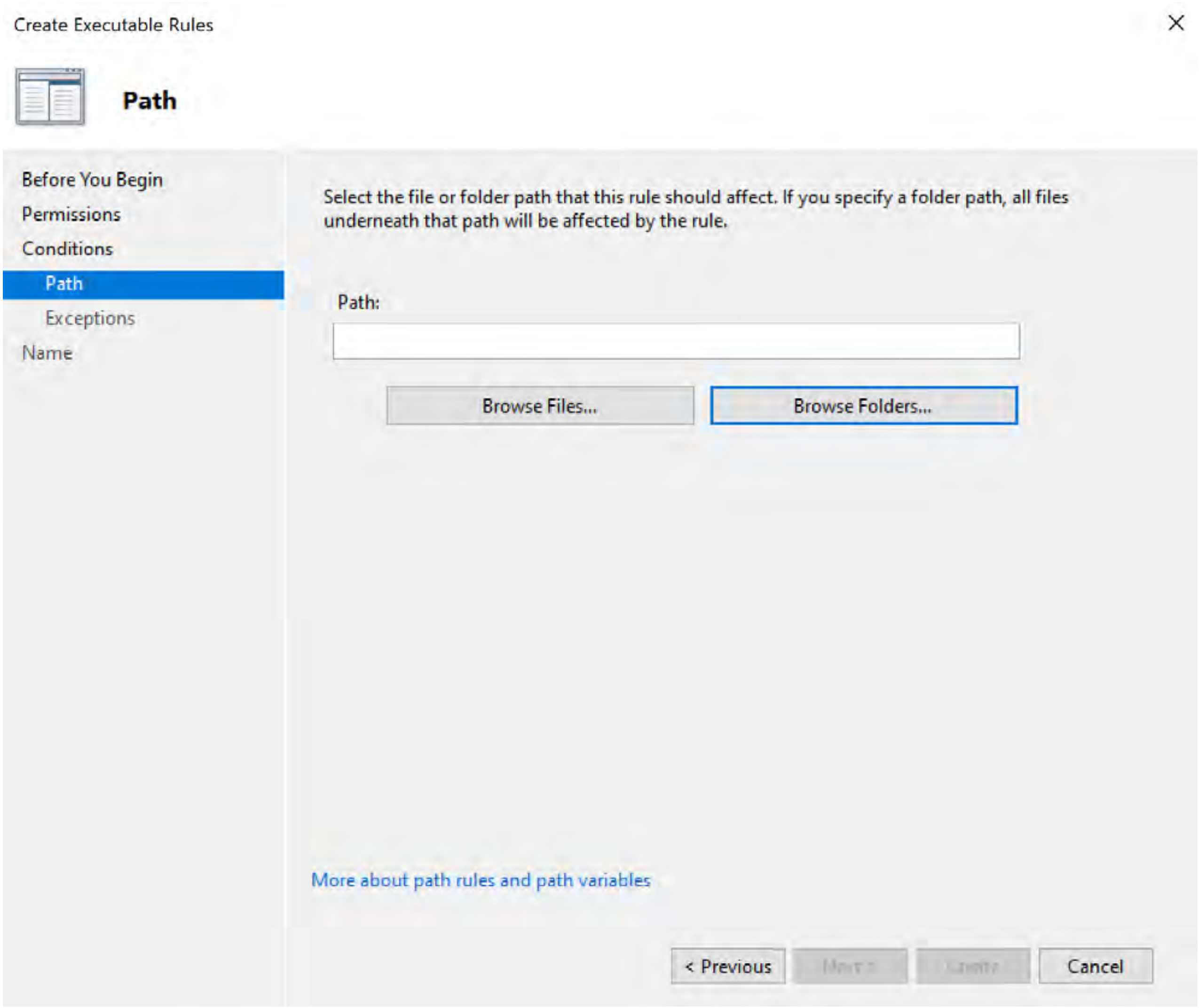
Select the type of primary condition that you would like to create.

○ Publisher
Select this option if the application you want to create the rule for is signed by the software publisher.

● Path
Create a rule for a specific file or folder path. If you select a folder, all files in the folder will be affected by the rule.

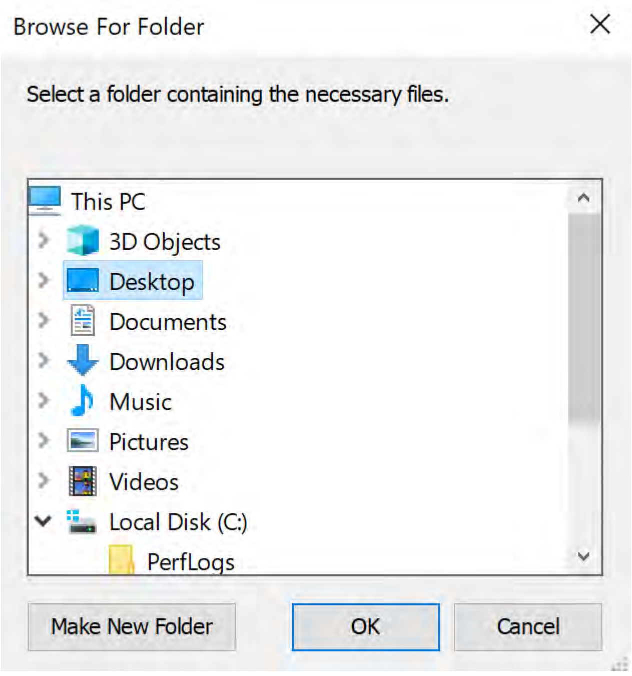
○ File hash
Select this option if you want to create a rule for an application that is not signed.

More about rule conditions



Select the file or folder path that this rule should affect. If you specify a folder path, all files underneath that path will be affected by the rule.

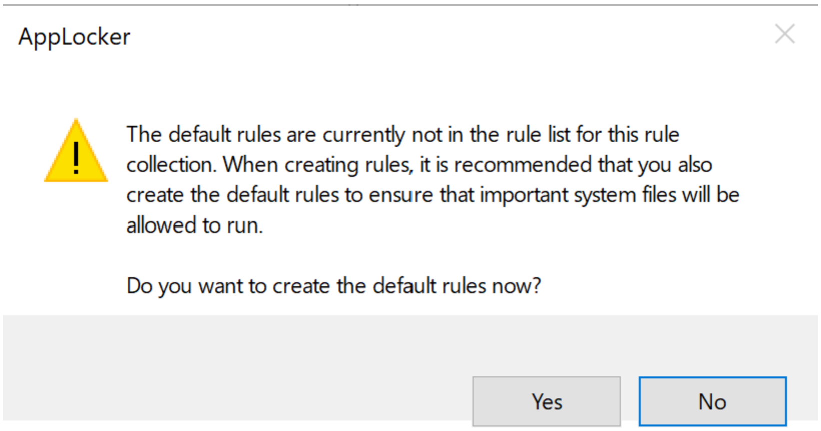
Path:



Browse For Folder

Select a folder containing the necessary files.

- Select *Yes* in the warning message that will prompt.



AppLocker

The default rules are currently not in the rule list for this rule collection. When creating rules, it is recommended that you also create the default rules to ensure that important system files will be allowed to run.

Do you want to create the default rules now?

- Restart to apply the changes.

Open the *Services* Window (*WIN + R*, then type *services.msc*) - Select *Application Identity*, right-click on it and select *Start* (this step must be performed for all test cases related with this SFR).

```
![gpo_13](./gpos/fpt_srp_ext.1.1/media/test1_2.8.png)
```

Once this Application Control Policy is enabled, there is only a path that disallows code execution: the *Desktop* Folder.

In addition, *VSCodeUserSetup-x64-1.78.2.exe* executable will be used for the test execution. This executables must be available in the target machine:

The *VSCodeUserSetup-x64-1.78.2.exe* executable shall be copied to the Desktop directory. Another copy of the file can be placed in any other directory.

42.2.1.2 Setup

42.2.1.3 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

42.2.1.4 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

42.2.1.5 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 1 and Test 2** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1 and Test 2**.

42.2.2 Test 3 & Test 4

This test configures the OS to only allow code that has been signed by the OS vendor to execute. Two applications will be executed, the first one signed by the OS vendor and the second one signed by another digital authority.

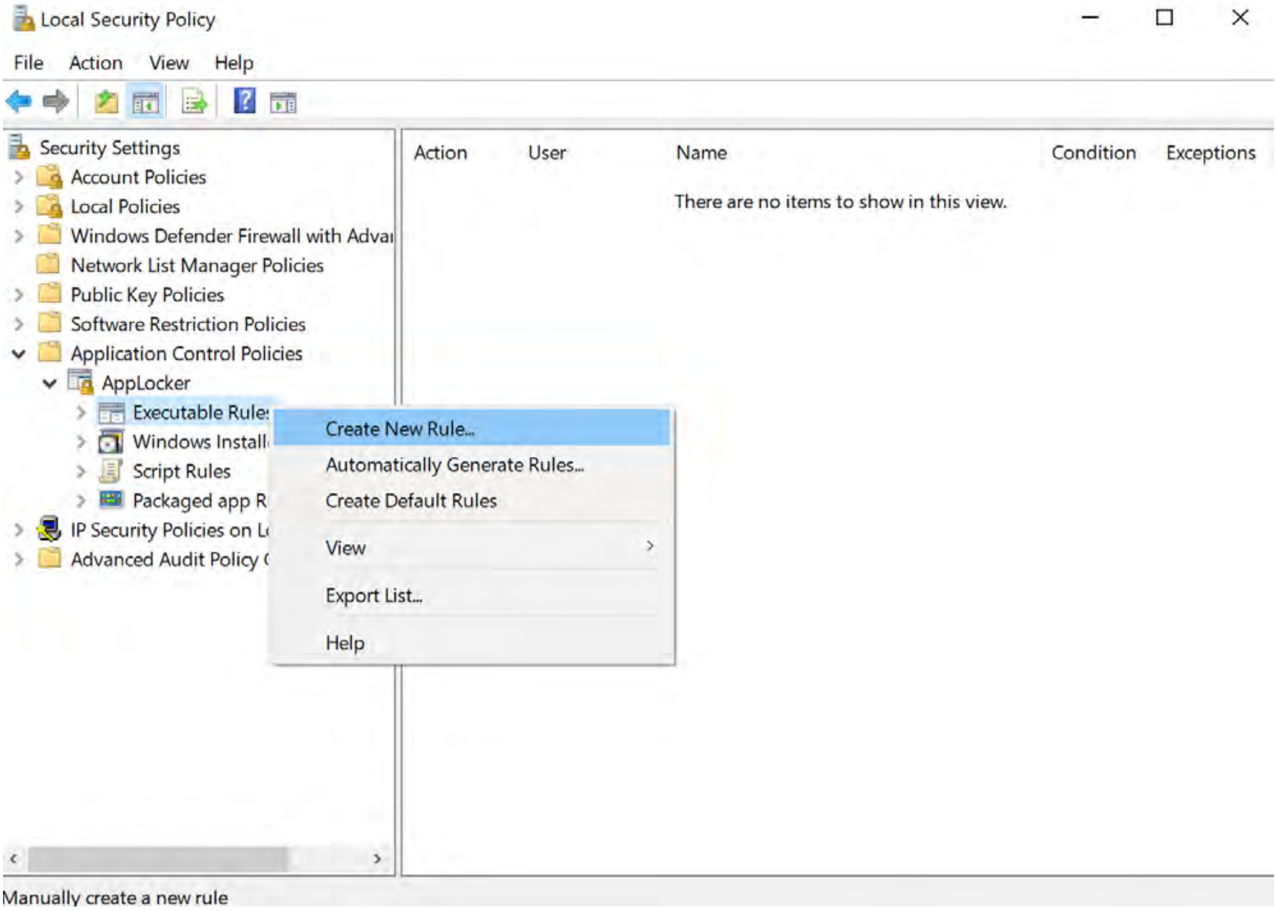
42.2.2.1 Setup

The two executables used in the previous test will be used again for the test execution. These executables must be available in the target machine:

- *Firefox Setup 114.0.2.exe*
- *VSCodeUserSetup-x64-1.78.2.exe*

To execute this test, an Application Control Policy must be enabled. To do that, the evaluator should perform these next steps.

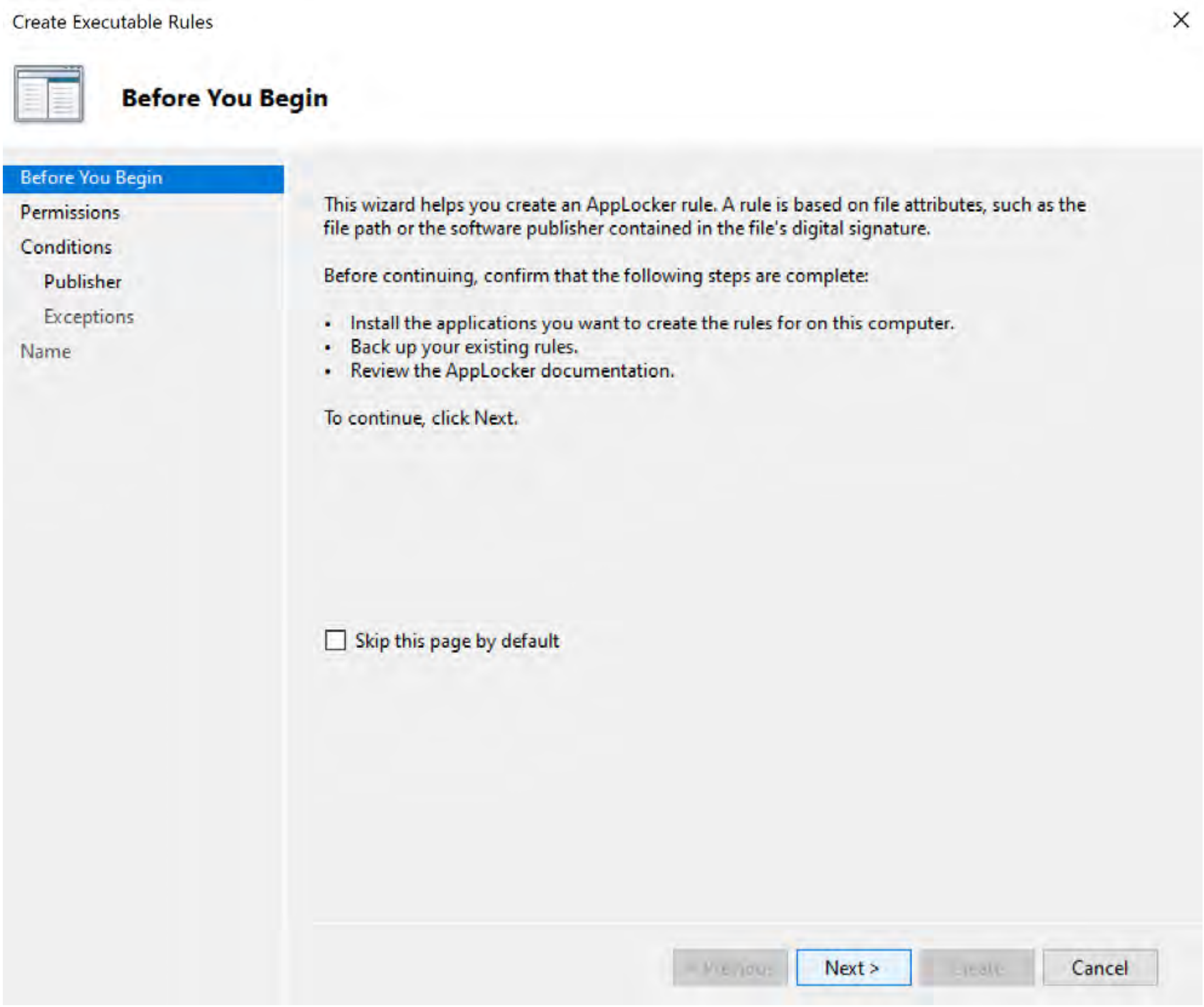
- Open the *Local Security Policy* Window (*WIN* + *R*, then type *secpol.msc*)
- Go to *Security Settings* -> *Application Restriction Policies* -> *AppLocker* -> *Executable Rules*. Right-click on it and select *Create New Rule...*



There are no items to show in this view.

Manually create a new rule

- Then, click *next*.



Create Executable Rules

Before You Begin

This wizard helps you create an AppLocker rule. A rule is based on file attributes, such as the file path or the software publisher contained in the file's digital signature.

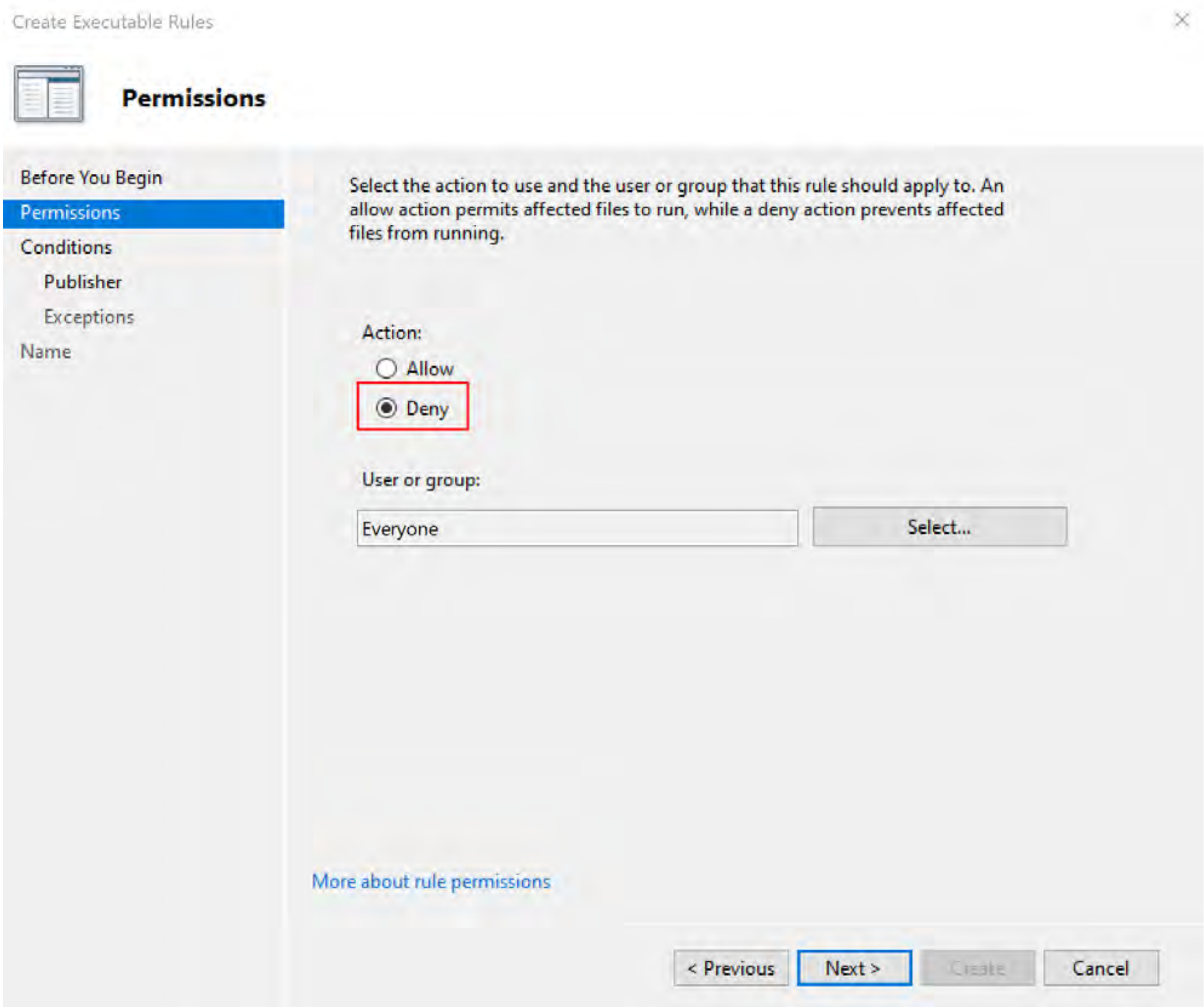
Before continuing, confirm that the following steps are complete:

- Install the applications you want to create the rules for on this computer.
- Back up your existing rules.
- Review the AppLocker documentation.

To continue, click Next.

□ Skip this page by default

- Select *Deny*.

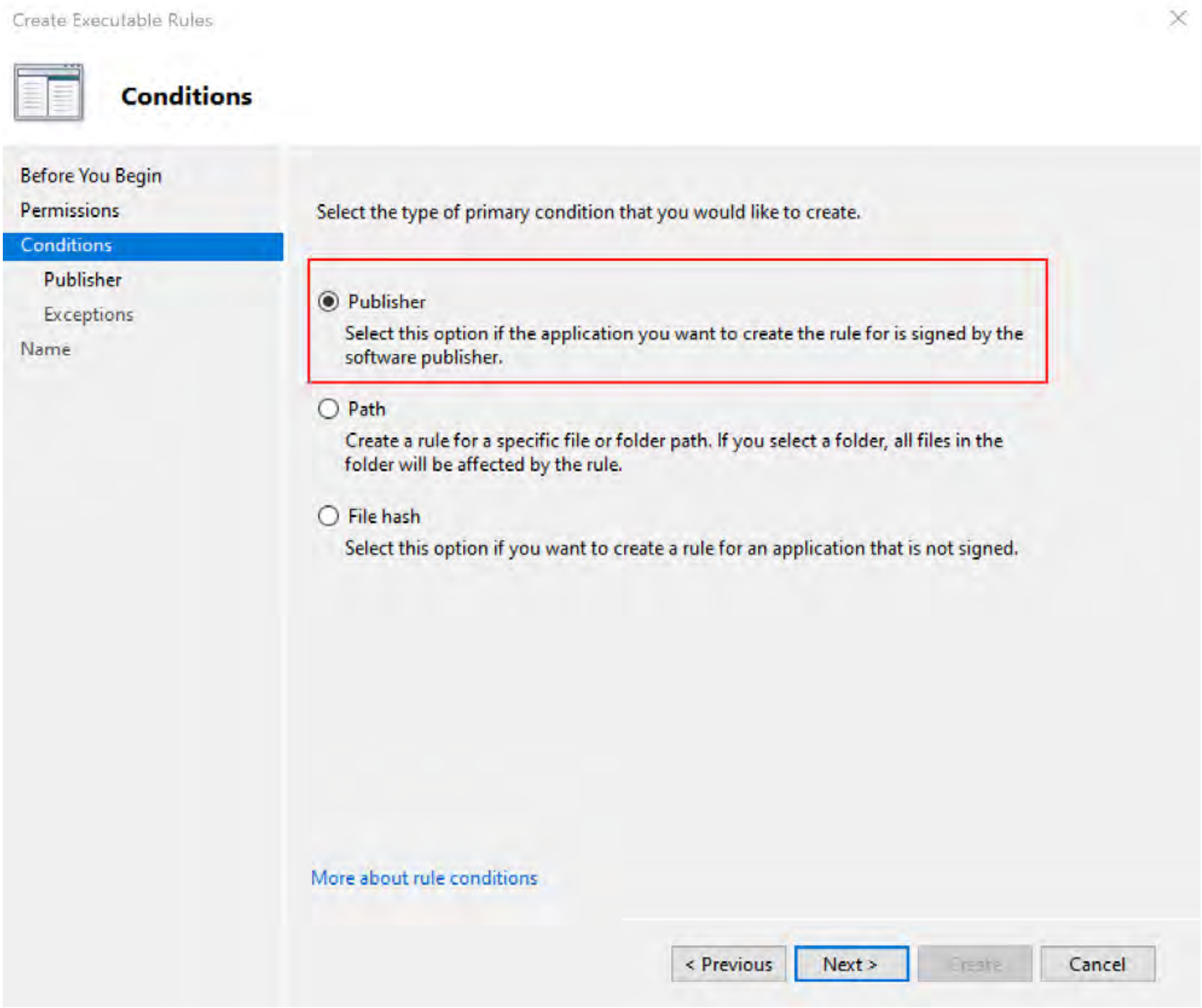


Select the action to use and the user or group that this rule should apply to. An allow action permits affected files to run, while a deny action prevents affected files from running.

Action:
○ Allow
● Deny

User or group:
Everyone

- Select *Publisher*, browse and select *Firefox Setup 114.0.2.exe* and select *Publisher* with the slider as shown below:

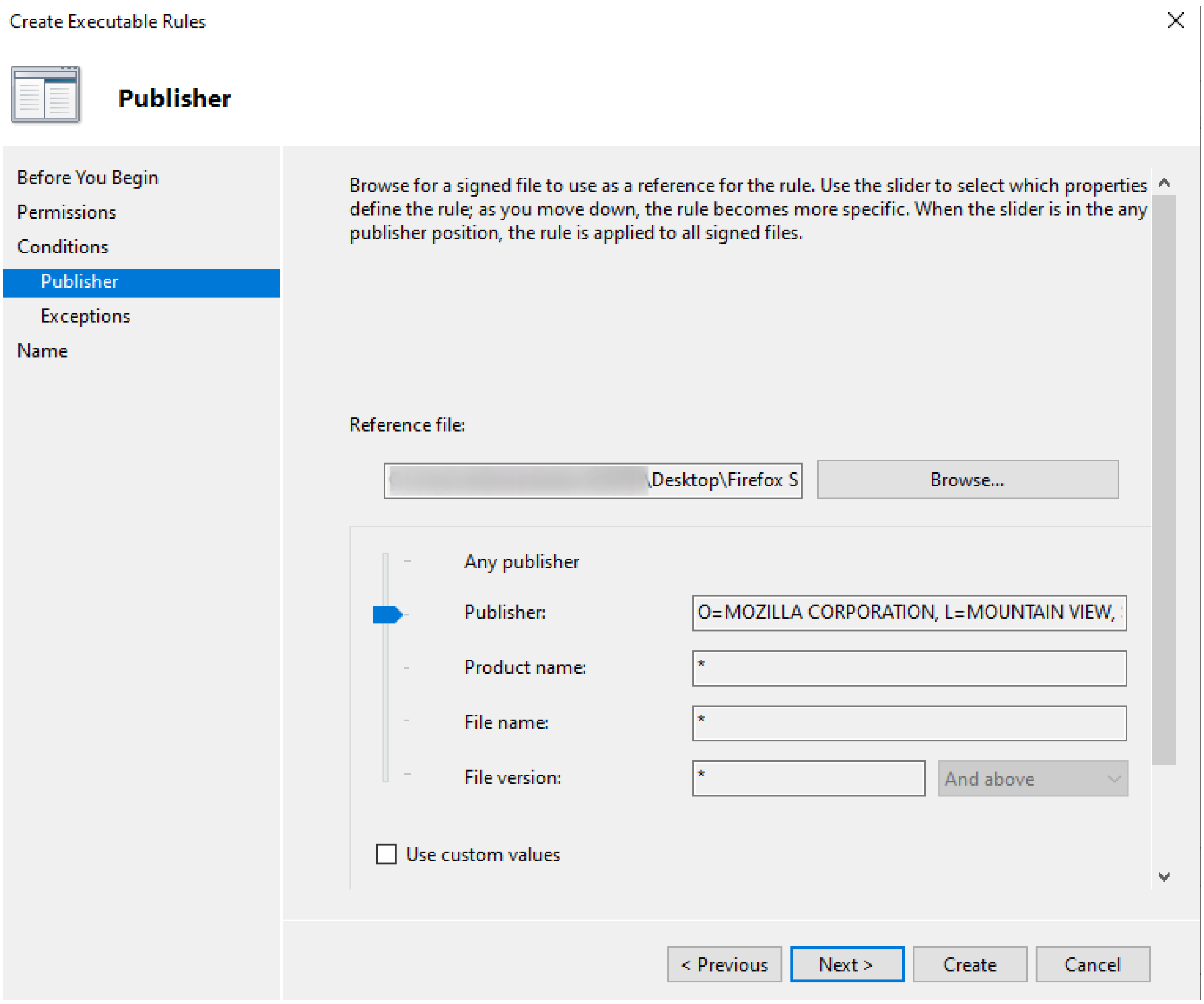


Select the type of primary condition that you would like to create.

● Publisher
Select this option if the application you want to create the rule for is signed by the software publisher.

○ Path
Create a rule for a specific file or folder path. If you select a folder, all files in the folder will be affected by the rule.

○ File hash
Select this option if you want to create a rule for an application that is not signed.



Create Executable Rules

Publisher

Browse for a signed file to use as a reference for the rule. Use the slider to select which properties define the rule; as you move down, the rule becomes more specific. When the slider is in the any publisher position, the rule is applied to all signed files.

Reference file:

[redacted]\Desktop\Firefox S

Any publisher

Publisher: O=MOZILLA CORPORATION, L=MOUNTAIN VIEW,

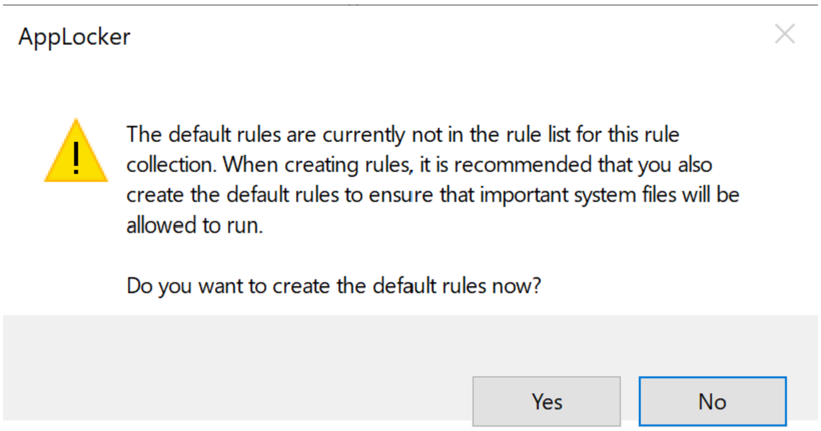
Product name: *

File name: *

File version: * And above

☐ Use custom values

- Select *Yes* in the warning message that will prompt.



AppLocker

The default rules are currently not in the rule list for this rule collection. When creating rules, it is recommended that you also create the default rules to ensure that important system files will be allowed to run.

Do you want to create the default rules now?

- Restart to apply the changes.

Open the *Services* Window (*WIN + R*, then type *services.msc*) - Select *Application Identity*, right-click on it and select *Start*.

```
![gpo_13](./gpos/fpt_srp_ext.1.1/media/test1_2.8.png)
```

<–>

Once this Application Control Policy is enabled, only the applications signed with the allowed publisher will allow code execution.

42.2.2.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

42.2.2.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

42.2.2.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 3 and Test 4** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 3 and Test 4**.

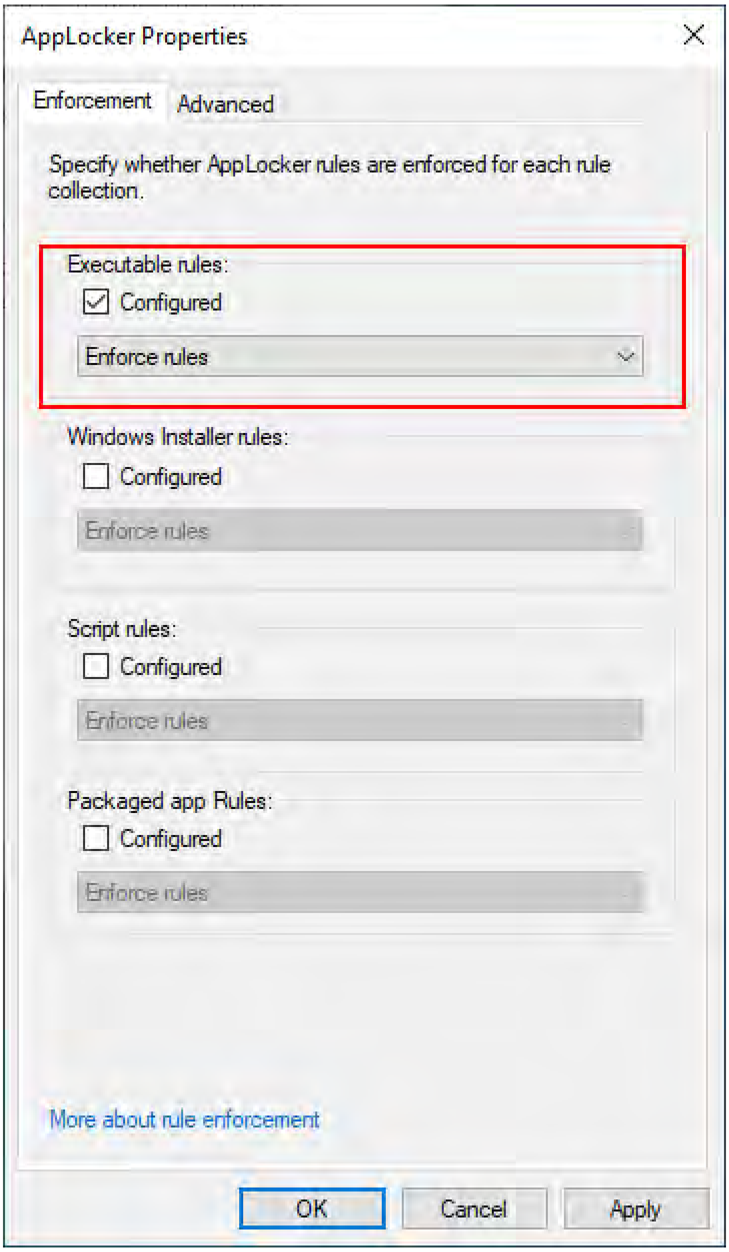
42.2.3 Test 5 & Test 6

This test configures the OS to only allow to execute a specific version of an application. First the specified version will be executed and after that an older version will be attempted to install.

42.2.3.1 Setup

These tests shall be performed using the *Applocker* policy described below:

- First, *Applocker* shall be configured to enforce the execution rules. To do that, go to the *Local Security Policy* tool and go to *Application Control Policies-> Applocker*. *Right-click* on it, select the *Properties* option and configure it as follows:



AppLocker Properties

Enforcement | Advanced

Specify whether AppLocker rules are enforced for each rule collection.

Executable rules:
☑ Configured
Enforce rules

Windows Installer rules:
☐ Configured
Enforce rules

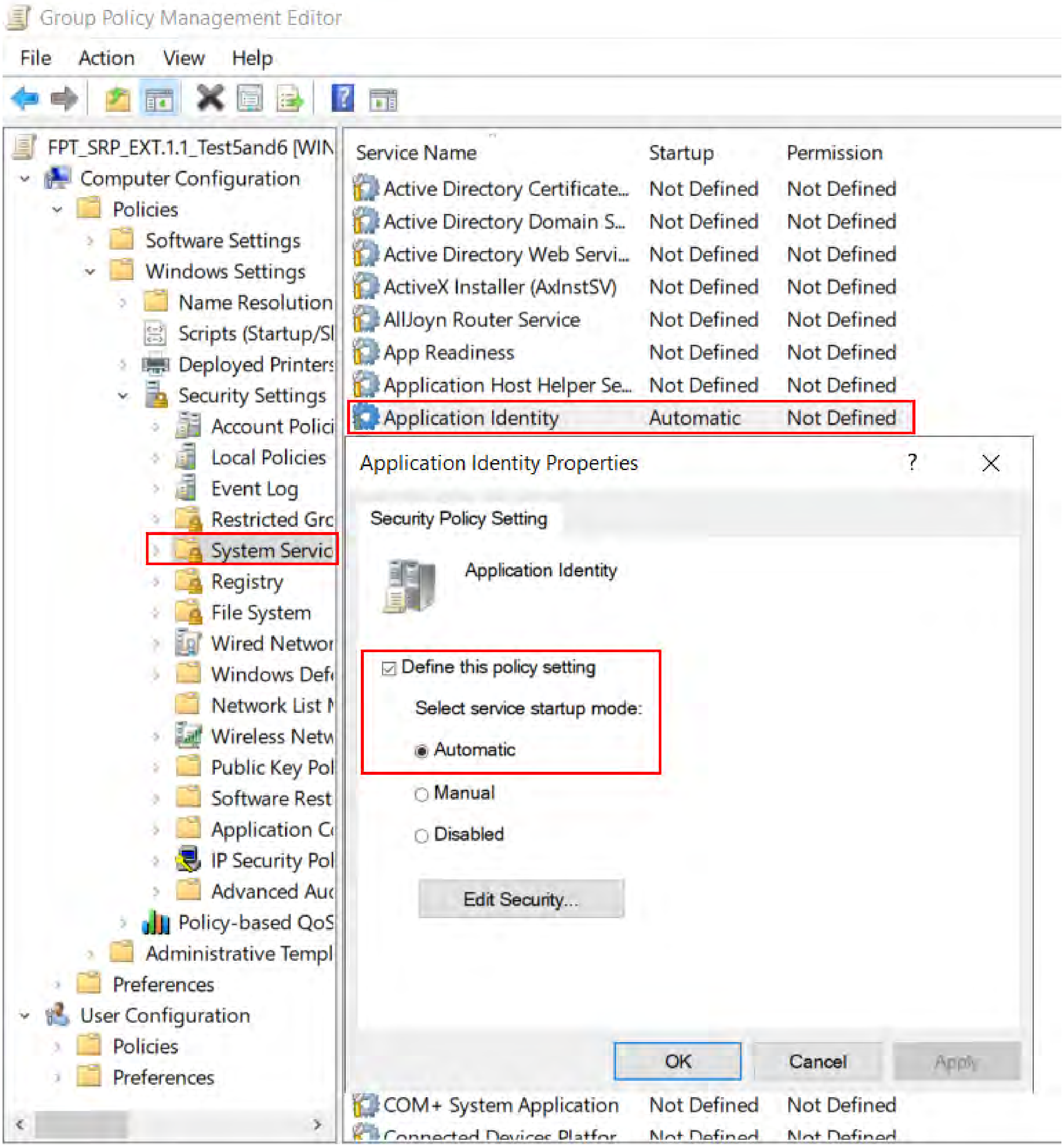
Script rules:
☐ Configured
Enforce rules

Packaged app Rules:
☐ Configured
Enforce rules

More about rule enforcement

- *Application Identity Service* must be running.

On Azure Stack HCIv2 platform, the service can be started with a GPO following the same steps described at the beginning of the test activity. The GPO should be configured as shown in the following image:



Service Name	Startup	Permission
Active Directory Certificate...	Not Defined	Not Defined
Active Directory Domain S...	Not Defined	Not Defined
Active Directory Web Servi...	Not Defined	Not Defined
ActiveX Installer (AxInstSV)	Not Defined	Not Defined
AllJoyn Router Service	Not Defined	Not Defined
App Readiness	Not Defined	Not Defined
Application Host Helper Se...	Not Defined	Not Defined
Application Identity	Automatic	Not Defined
COM+ System Application	Not Defined	Not Defined
Connected Devices Platfor	Not Defined	Not Defined

Application Identity Properties

Security Policy Setting

Application Identity

☑ Define this policy setting

Select service startup mode:

● Automatic

○ Manual

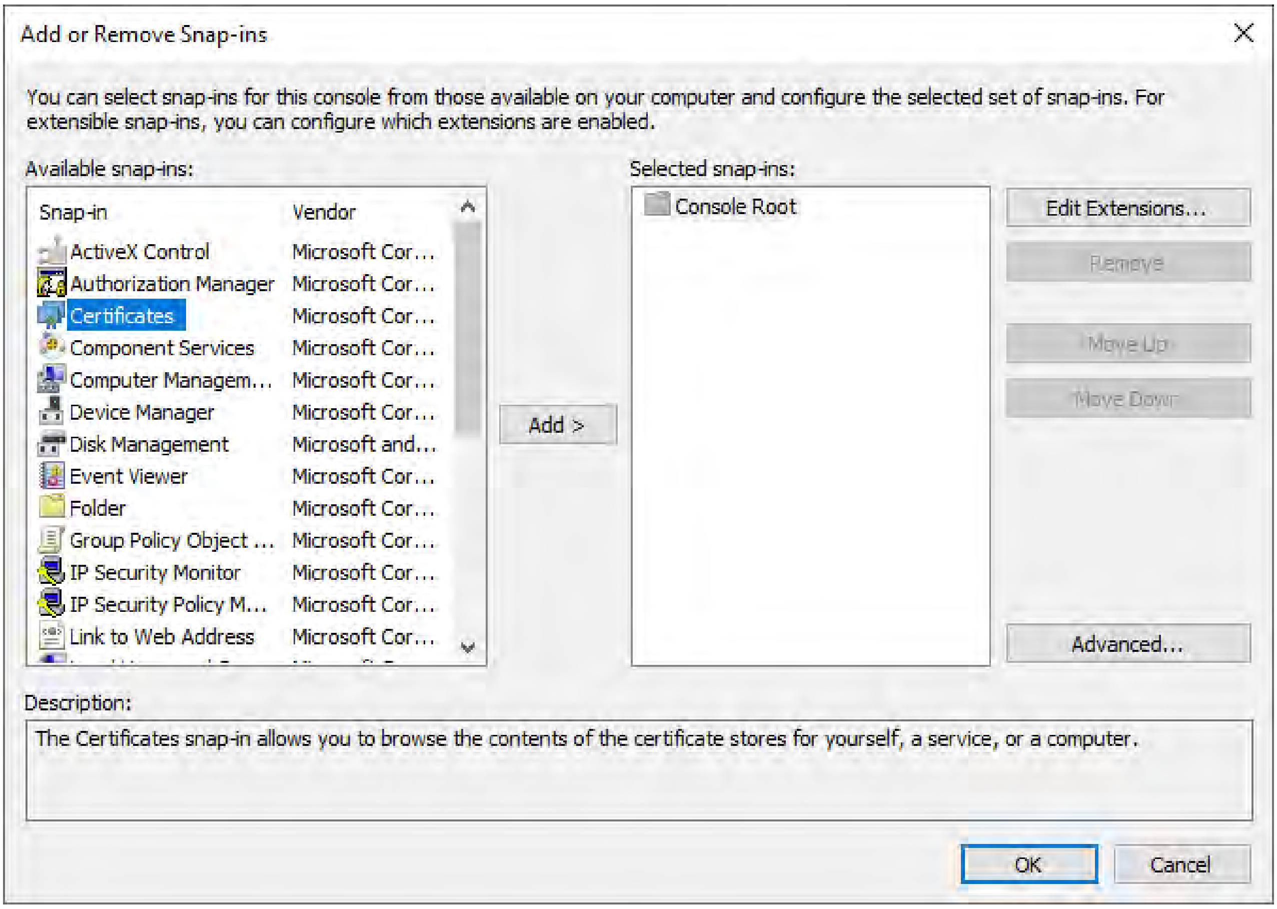
○ Disabled

The following executables created by the evaluator shall be available in the evaluated platforms:

- *TestConsolev10.exe*
- *TestConsolev11.exe*

These executables files are self-signed. Before the version-based rule is created, the evaluator shall include this self-signed certificate into the *Trusted Root Certification Authorities Store*. These are the necessary steps to do it:

- Open the Microsoft Management Console tool: (*WIN+R*, then type *mmc*)
- Go to *File -> Add/Remove Snap-in...* (*Control + M*) to add the Certificates snap-in to the viewer. To configure it, follow these steps:
  - Add the *Certificates* Snap-in:

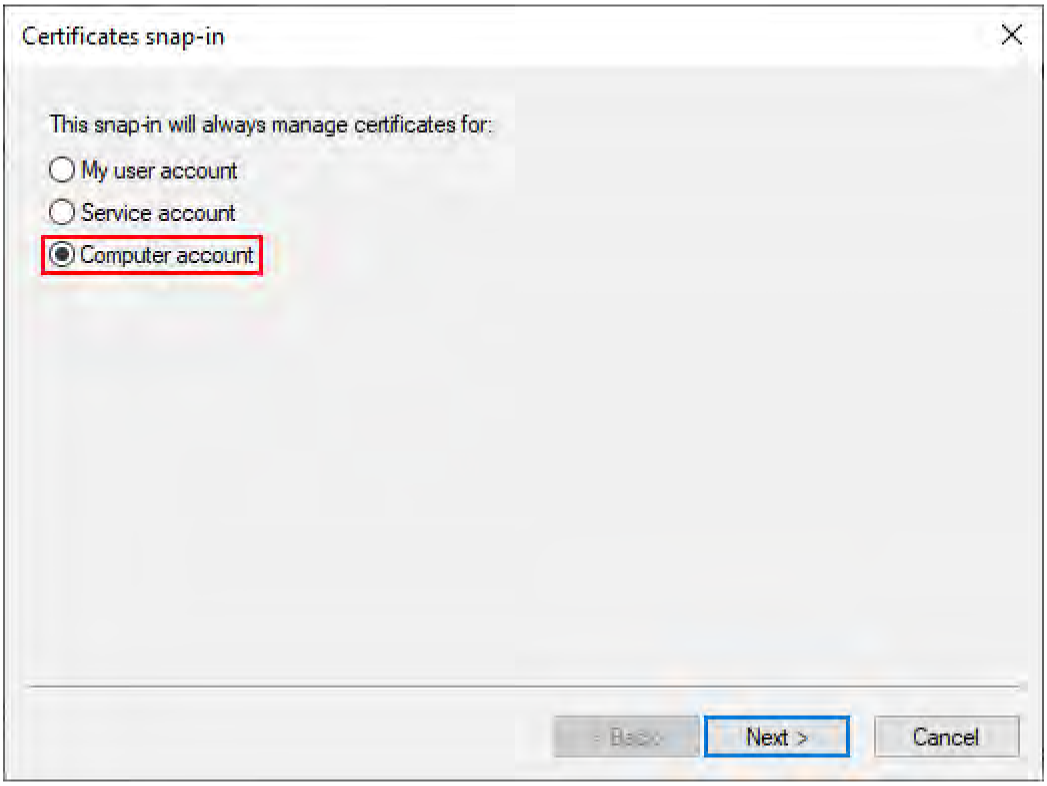


You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

  - Select the checkbox: *Computer account*.

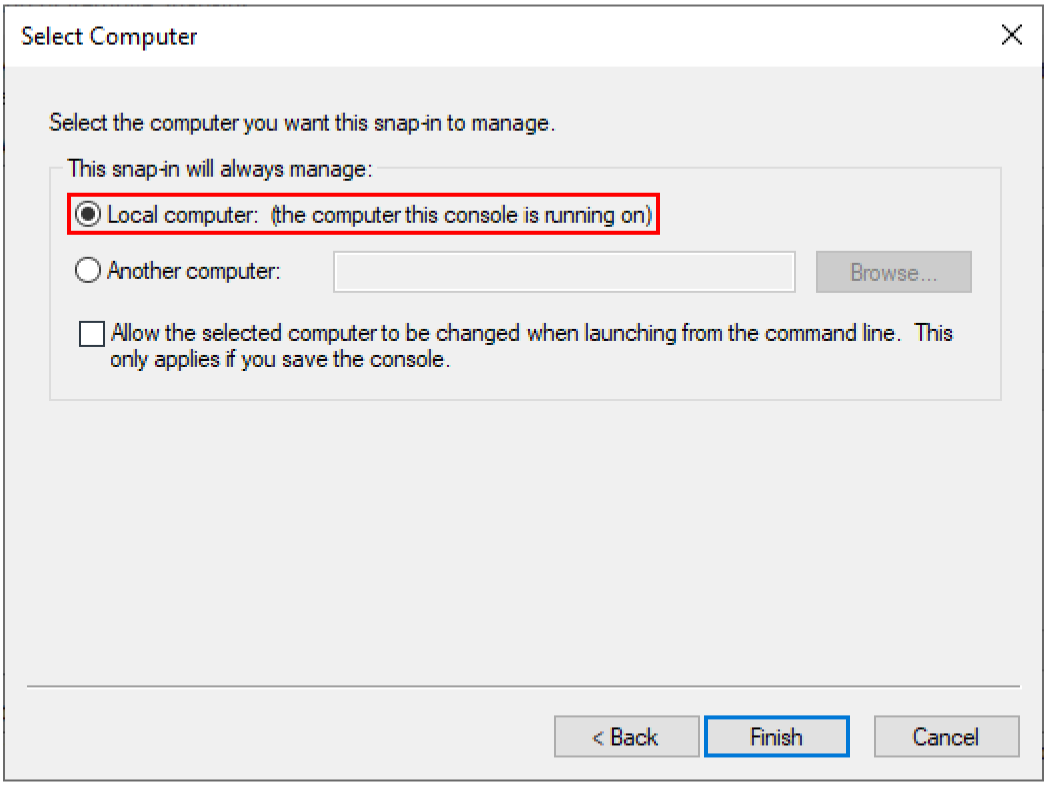


Certificates snap-in

This snap-in will always manage certificates for:

○ My user account
○ Service account
● Computer account

– Select the checkbox: *Local Computer*.



Select Computer

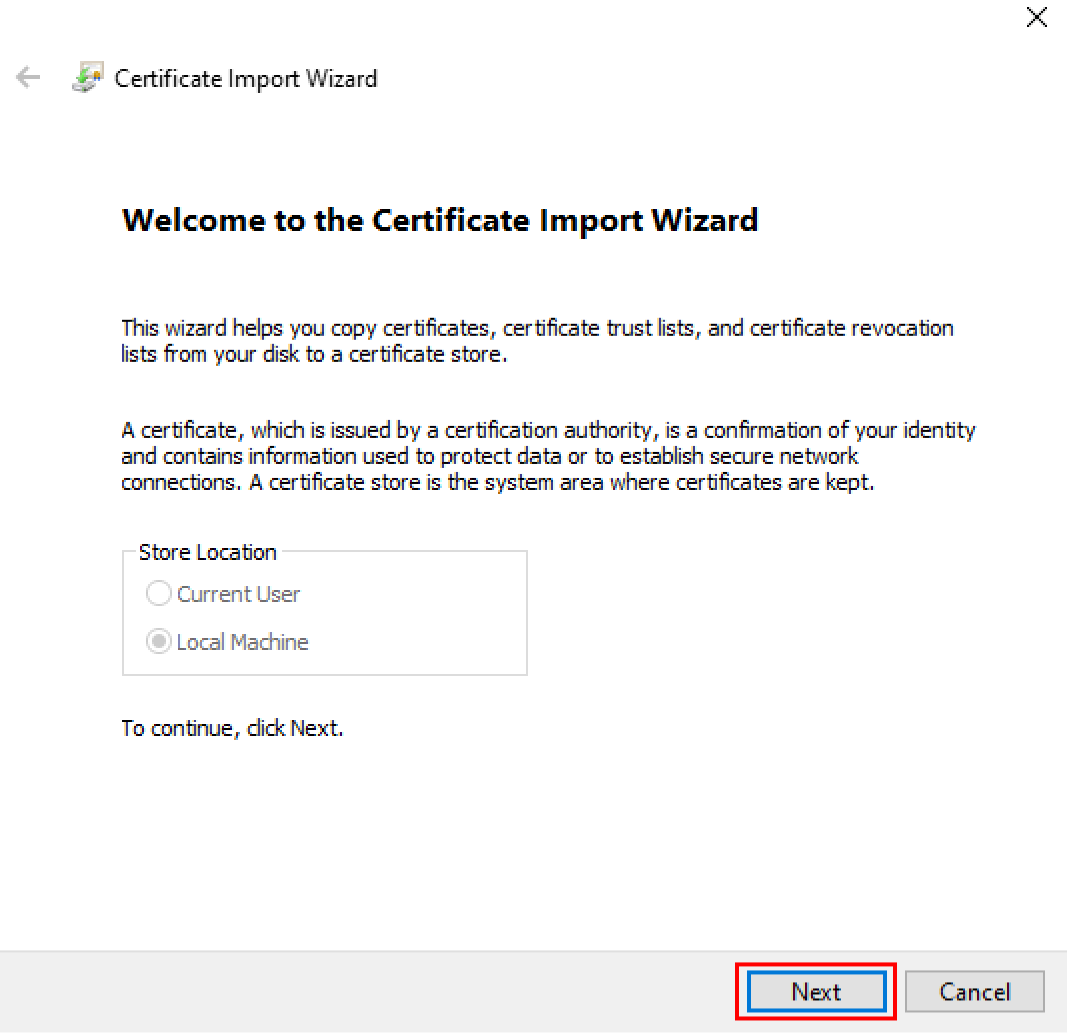
Select the computer you want this snap-in to manage.

This snap-in will always manage:

● Local computer: (the computer this console is running on)
○ Another computer:

☐ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

- Go to *Trusted Root Certification Authorities* -> *Certificates*. Then, right-click in *Actions* -> *All tasks* -> *Import...* and follow the wizard to import the test certificate.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

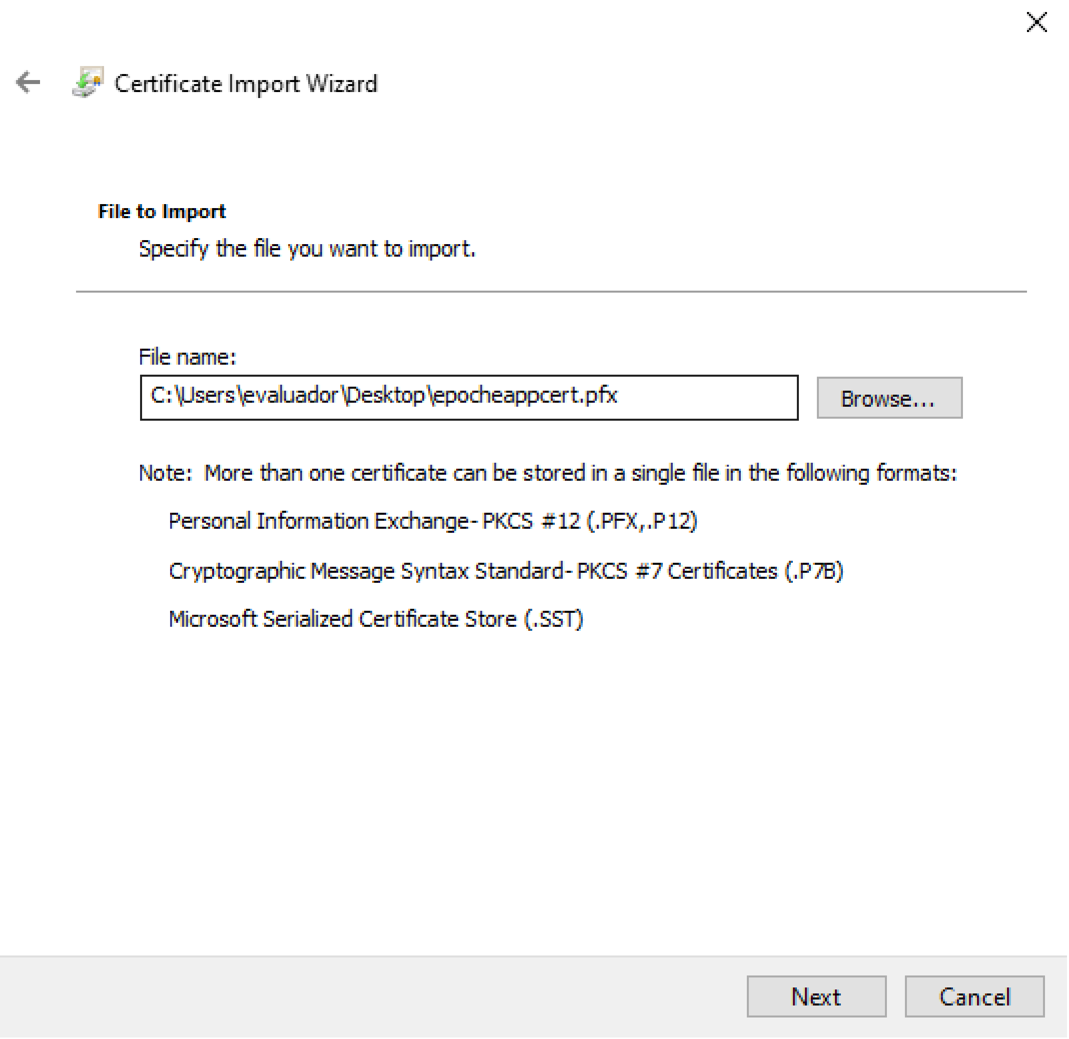
Store Location

○ Current User

● Local Machine

To continue, click Next.

- Browse the certificate.



File to Import

Specify the file you want to import.

File name:

C:\Users\evaluador\Desktop\epocheappcert.pfx

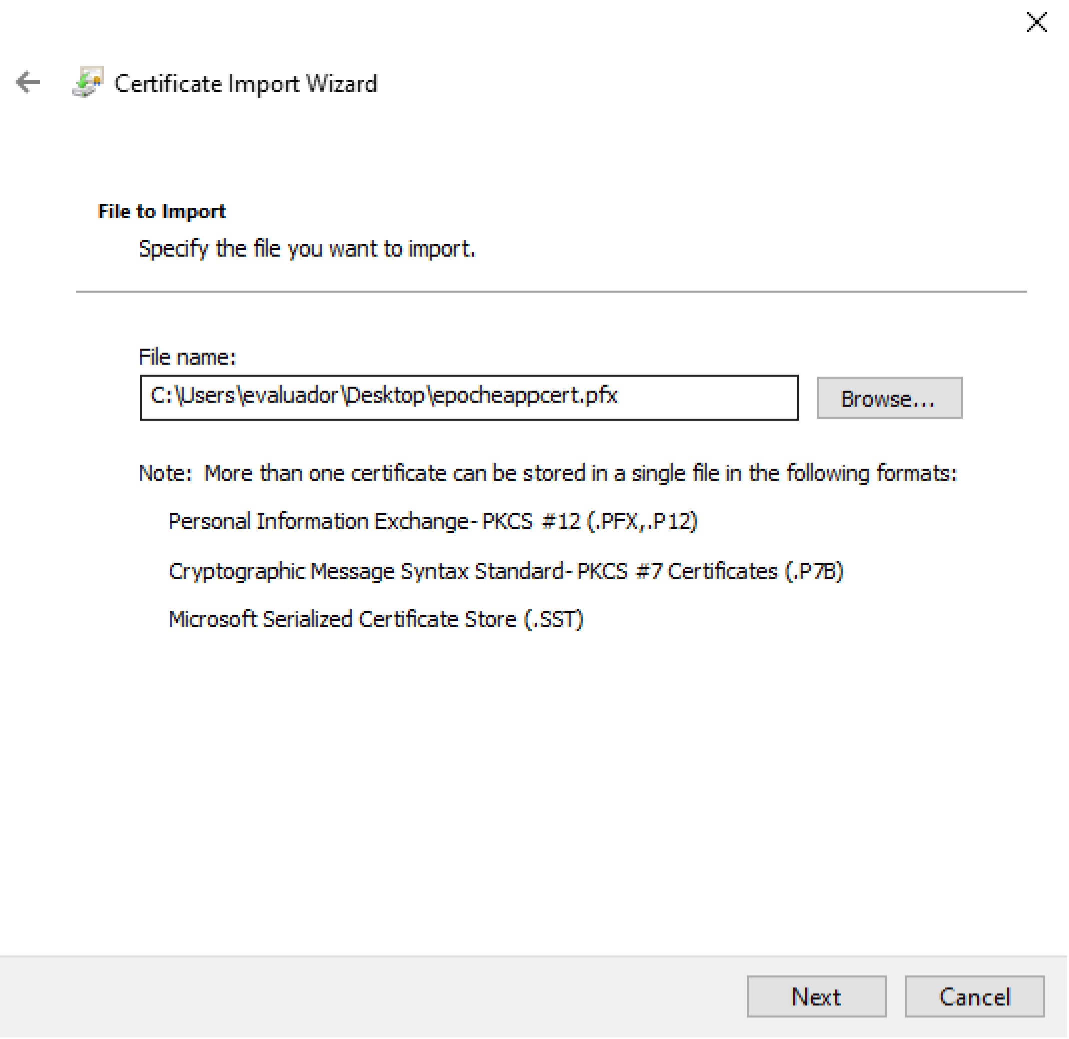
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

- Introduce the private key password.



File to Import

Specify the file you want to import.

File name:
C:\Users\evaluador\Desktop\epocheappcert.pfx

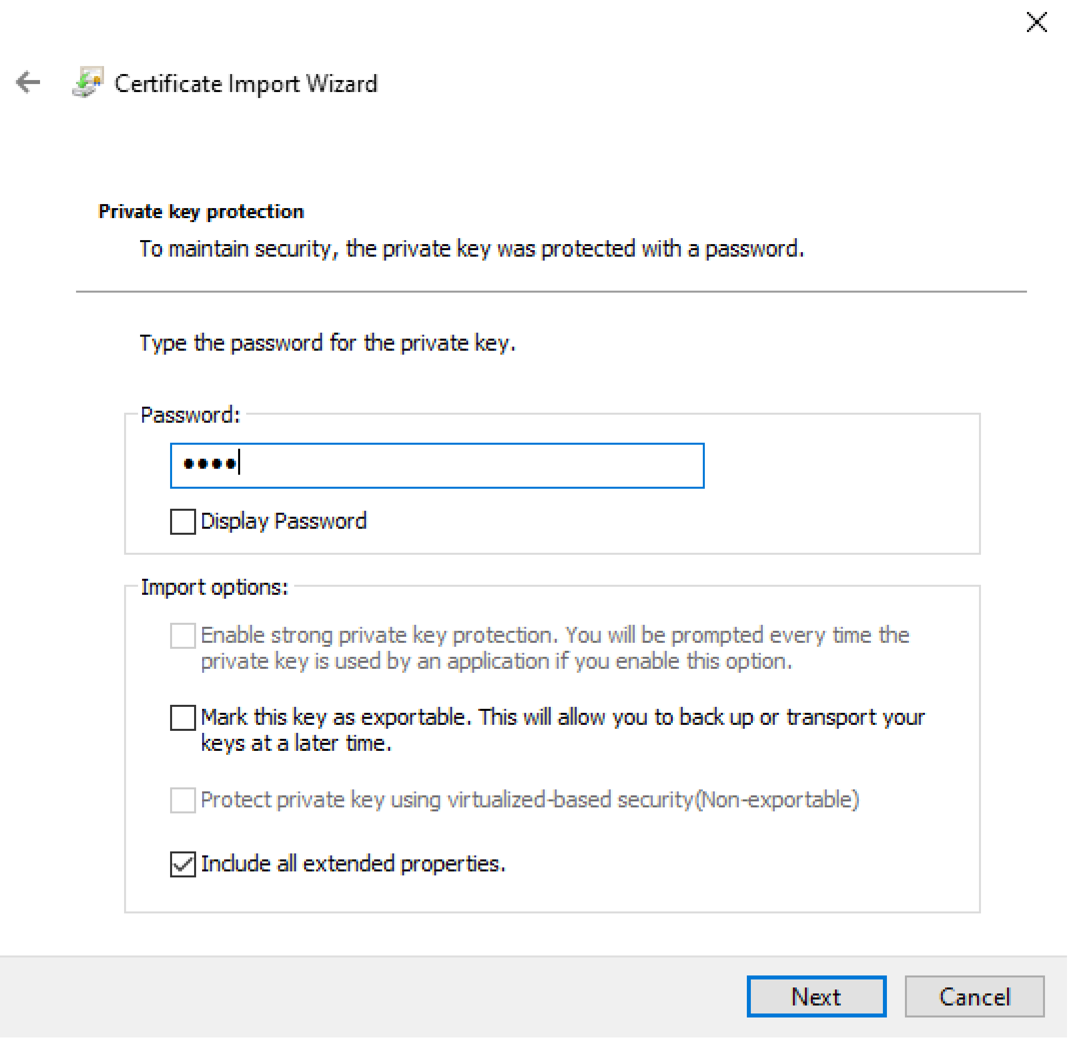
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

- Place it in the *Trusted Root Certification Authorities*



Certificate Import Wizard

Private key protection

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

••••

□ Display Password

Import options:

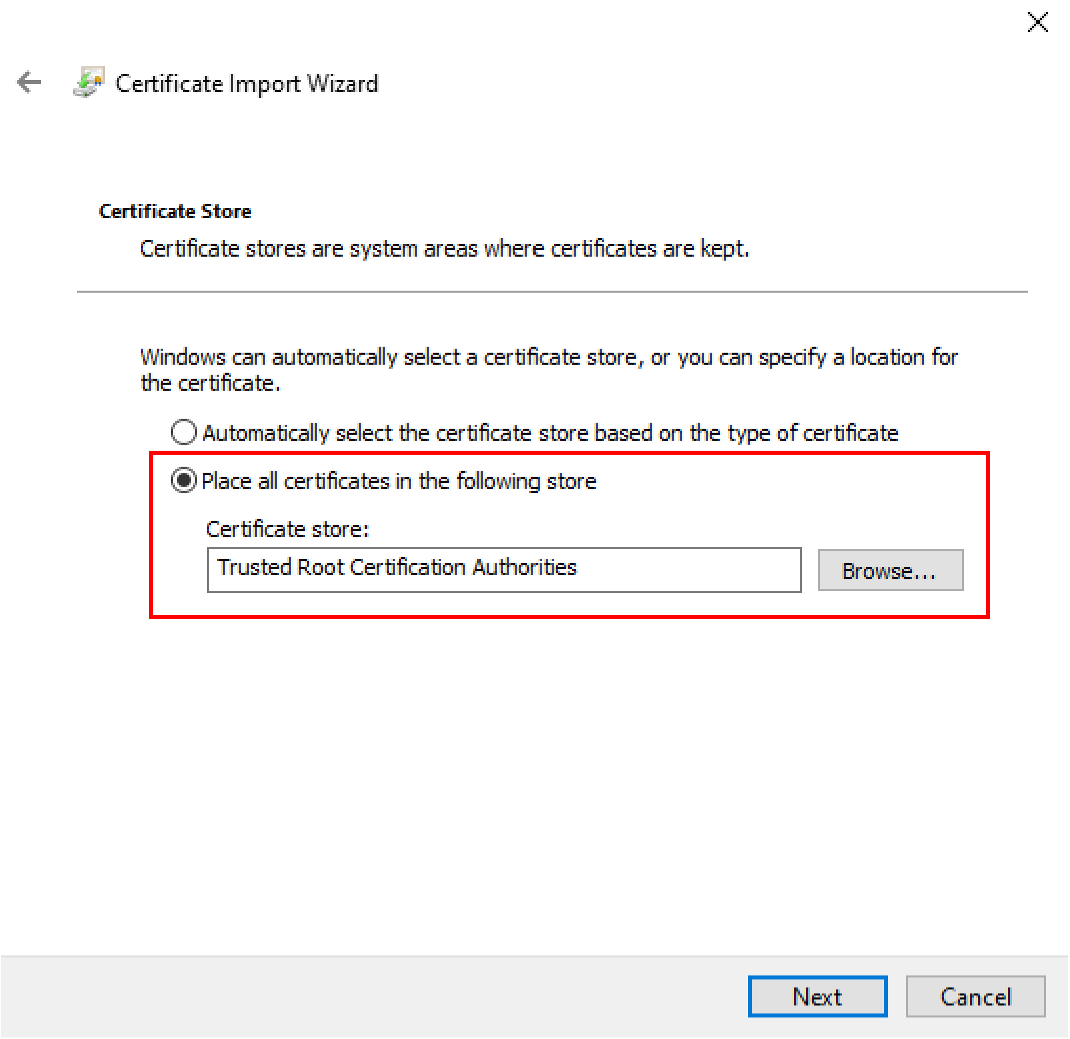
□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

□ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

□ Protect private key using virtualized-based security(Non-exportable)

☑ Include all extended properties.

- Finally, click *Next* and then *Finish*.



Certificate Import Wizard

Certificate Store

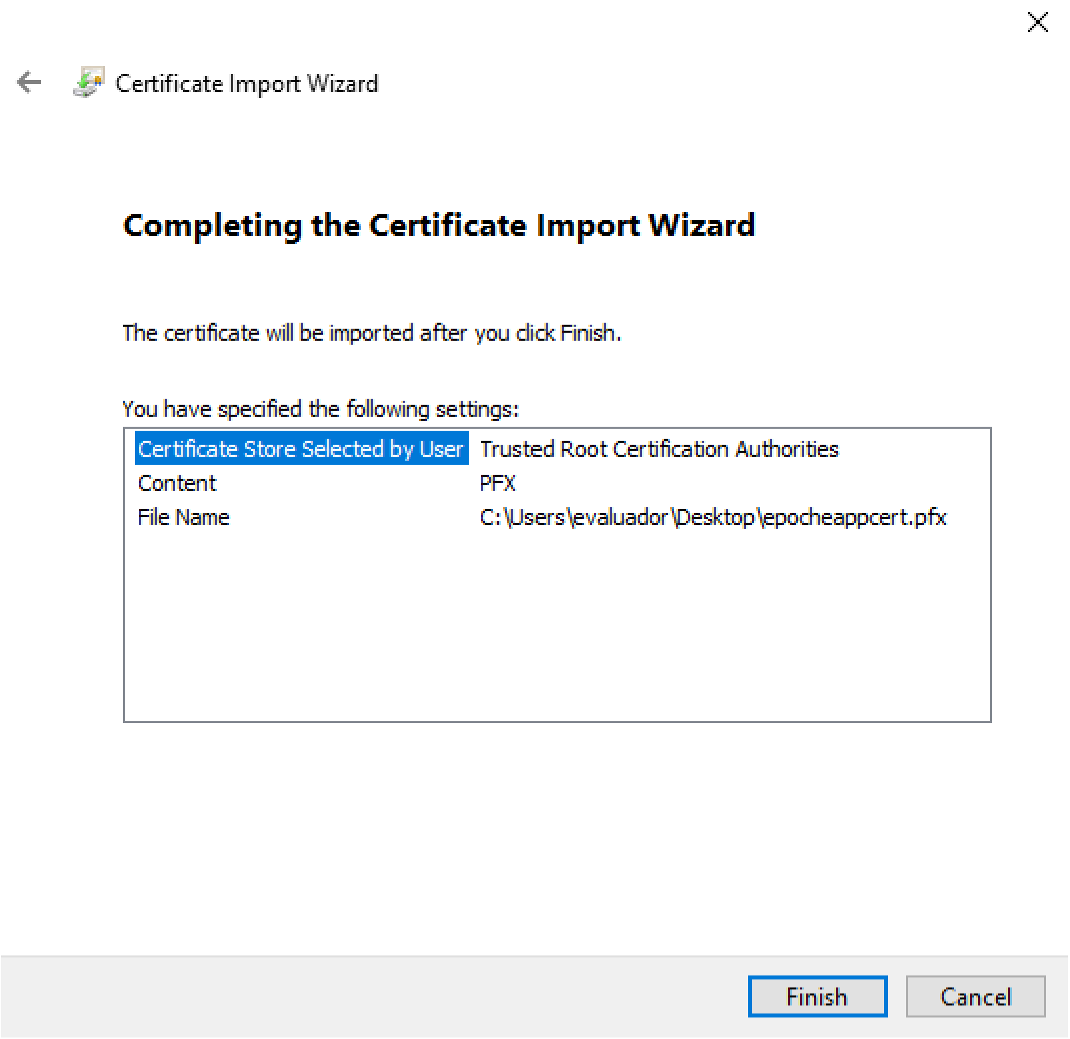
Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities



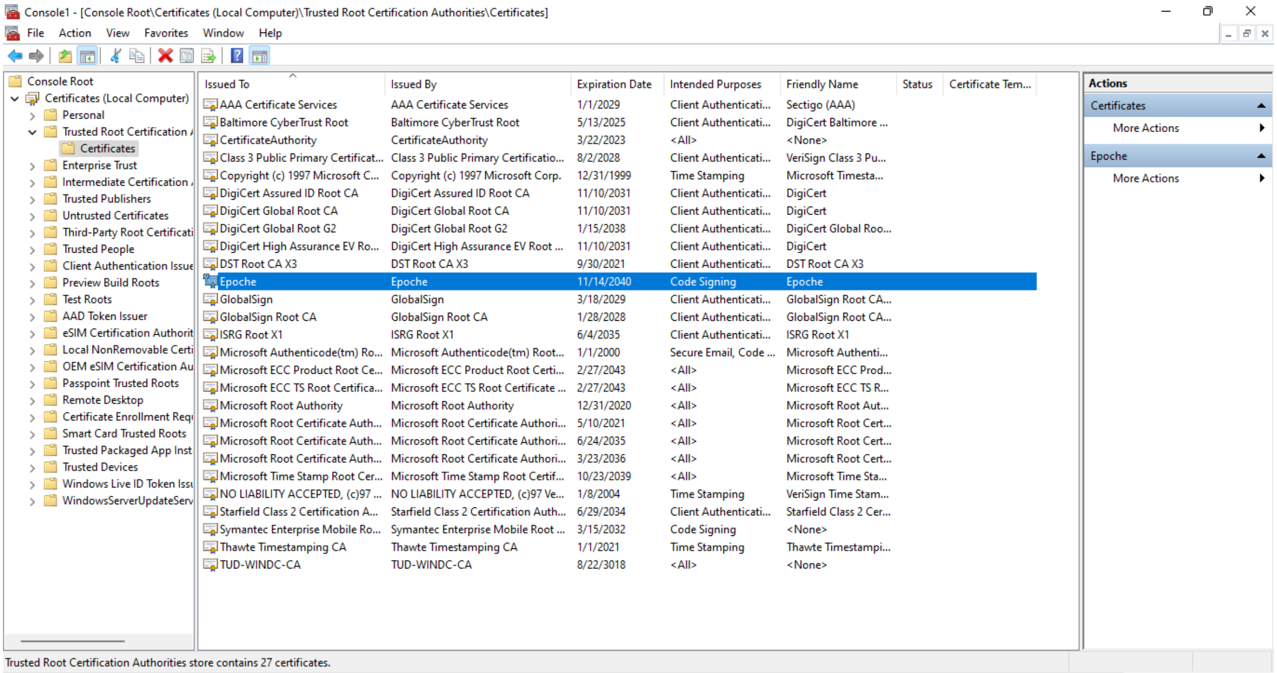
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	PFX
File Name	C:\Users\evaluador\Desktop\epocheappcert.pfx

- Additionally, check that the certificate has been correctly added to the *Trusted Root Certification Authorities* store:



Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification A
Certificates
Enterprise Trust
Intermediate Certification A
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificati
Trusted People
Client Authentication Issue
Preview Build Roots
Test Roots
AAD Token Issuer
eSIM Certification Authorit
Local NonRemovable Certi
OEM eSIM Certification Au
Passpoint Trusted Roots
Remote Desktop
Certificate Enrollment Requ
Smart Card Trusted Roots
Trusted Packaged App Inst
Trusted Devices
Windows Live ID Token Issu
WindowsServerUpdateServ
Actions
Certificates
More Actions
Epoche
More Actions

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem...
AAA Certificate Services	AAA Certificate Services	1/1/2029	Client Authenticati...	Sectigo (AAA)		
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/13/2025	Client Authenticati...	DigiCert Baltimore ...		
CertificateAuthority	CertificateAuthority	3/22/2023	<All>	<None>		
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/2/2028	Client Authenticati...	VeriSign Class 3 Pu...		
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/31/1999	Time Stamping	Microsoft Timesta...		
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/10/2031	Client Authenticati...	DigiCert		
DigiCert Global Root CA	DigiCert Global Root CA	11/10/2031	Client Authenticati...	DigiCert		
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Client Authenticati...	DigiCert Global Roo...		
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	11/10/2031	Client Authenticati...	DigiCert		
DST Root CA X3	DST Root CA X3	9/30/2021	Client Authenticati...	DST Root CA X3		
Epoche	Epoche	11/14/2040	Code Signing	Epoche		
GlobalSign	GlobalSign	3/18/2029	Client Authenticati...	GlobalSign Root CA...		
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Client Authenticati...	GlobalSign Root CA...		
ISRG Root X1	ISRG Root X1	6/4/2035	Client Authenticati...	ISRG Root X1		
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	1/1/2000	Secure Email, Code ...	Microsoft Authenti...		
Microsoft ECC Product Root Ce...	Microsoft ECC Product Root Certi...	2/27/2043	<All>	Microsoft ECC Prod...		
Microsoft ECC TS Root Certifica...	Microsoft ECC TS Root Certificate ...	2/27/2043	<All>	Microsoft ECC TS R...		
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>	Microsoft Root Aut...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	5/10/2021	<All>	Microsoft Root Cert...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	6/24/2035	<All>	Microsoft Root Cert...		
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	3/23/2036	<All>	Microsoft Root Cert...		
Microsoft Time Stamp Root Cer...	Microsoft Time Stamp Root Certif...	10/23/2039	<All>	Microsoft Time Sta...		
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 Ve...	1/8/2004	Time Stamping	VeriSign Time Stam...		
Starfield Class 2 Certification A...	Starfield Class 2 Certification Auth...	6/29/2034	Client Authenticati...	Starfield Class 2 Cer...		
Symantec Enterprise Mobile Ro...	Symantec Enterprise Mobile Root ...	3/15/2032	Code Signing	<None>		
Thawte Timestamping CA	Thawte Timestamping CA	1/1/2021	Time Stamping	Thawte Timestampi...		
TUD-WINDC-CA	TUD-WINDC-CA	8/22/3018	<All>	<None>		

Trusted Root Certification Authorities store contains 27 certificates.

On Azure Stack HCIv2 the certificate should be added following the same previous steps to the GPO rule.

42.2.3.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

42.2.3.3 Results

The evaluator has performed this test on all the canonical platforms (except the ones with Pro ediion) as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

42.2.3.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 5 and Test 6** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 5 and Test 6**.

42.2.4 Test 7 & Test 8

This test configures the OS to only allow code execution based on the hash of the application executable. First, an application with a hashed which match with the one configured will be executed. After that, the application will be modified to change the hash before being executed.

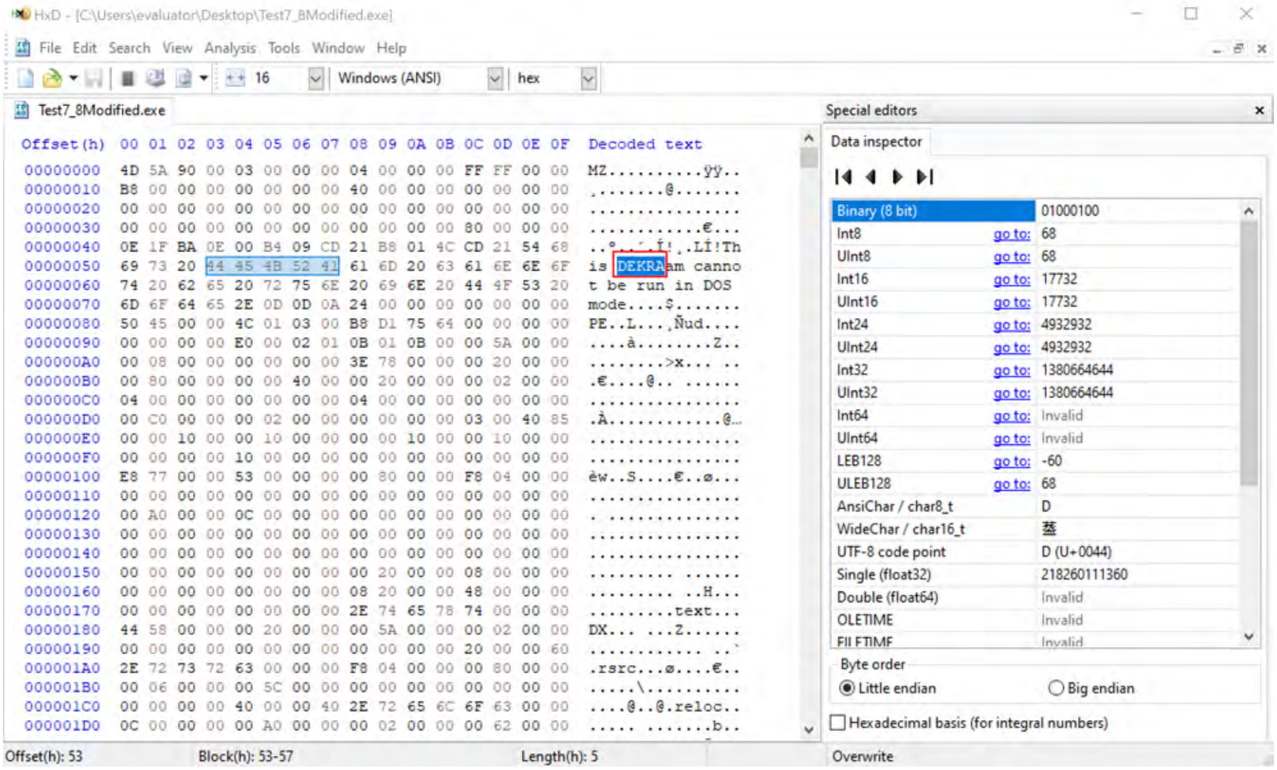
42.2.4.1 Setup

Ahexadecimal editor (e.g. *HxD*) must be installed in order to modify the original executable file.

To perform these tests, two executable files have been created to use during the tests execution:

- *Test7_8.exe*
- *Test7_8Modified.exe*

The executable file (*Test7_8Modified.exe*) has been modified with the hexadecimal editor (e.g *HxD*).


HxD - [C:\Users\evaluator\Desktop\Test7_8Modified.exe]
File Edit Search View Analysis Tools Window Help
16
Windows (ANSI)
hex
Test7_8Modified.exe
Special editors
Data inspector

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..........ÿÿ..
00000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ¸.......@.......
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00  ............€...
00000040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..º..´.Í!¸.LÍ!Th
00000050  69 73 20 44 45 4B 52 41 61 6D 20 63 61 6E 6E 6F  is DEKRAam canno
00000060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS 
00000070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
00000080  50 45 00 00 4C 01 03 00 B8 D1 75 64 00 00 00 00  PE..L...¸Ñud....
00000090  00 00 00 00 E0 00 02 01 0B 01 0B 00 00 5A 00 00  ....à........Z..
000000A0  00 08 00 00 00 00 00 00 3E 78 00 00 00 20 00 00  ........>x... ..
000000B0  00 80 00 00 00 00 40 00 00 20 00 00 00 02 00 00  .€....@.. ......
000000C0  04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00  ................
000000D0  00 C0 00 00 00 02 00 00 00 00 00 00 03 00 40 85  .À............@…
000000E0  00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00  ................
000000F0  00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00  ................
00000100  E8 77 00 00 53 00 00 00 00 80 00 00 F8 04 00 00  èw..S....€..ø...
00000110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000120  00 A0 00 00 0C 00 00 00 00 00 00 00 00 00 00 00  . ..............
00000130  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000140  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000150  00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00  ......... ......
00000160  00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00  ......... ..H...
00000170  00 00 00 00 00 00 00 00 2E 74 65 78 74 00 00 00  .........text...
00000180  44 58 00 00 00 20 00 00 00 5A 00 00 00 02 00 00  DX... ...Z......
00000190  00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60  ............ ..`
000001A0  2E 72 73 72 63 00 00 00 F8 04 00 00 00 80 00 00  .rsrc...ø....€..
000001B0  00 06 00 00 00 5C 00 00 00 00 00 00 00 00 00 00  .....\..........
000001C0  00 00 00 00 40 00 00 40 2E 72 65 6C 6F 63 00 00  ....@..@.reloc..
000001D0  0C 00 00 00 00 A0 00 00 00 02 00 00 00 62 00 00  ..... .......b..

Offset(h): 53    Block(h): 53-57    Length(h): 5
```

Binary (8 bit)		01000100
Int8	go to:	68
UInt8	go to:	68
Int16	go to:	17732
UInt16	go to:	17732
Int24	go to:	4932932
UInt24	go to:	4932932
Int32	go to:	1380664644
UInt32	go to:	1380664644
Int64	go to:	Invalid
UInt64	go to:	Invalid
LEB128	go to:	-60
ULEB128	go to:	68
AnsiChar / char8_t		D
WideChar / char16_t		䕄
UTF-8 code point		D (U+0044)
Single (float32)		218260111360
Double (float64)		Invalid
OLETIME		Invalid
FILETIME		Invalid

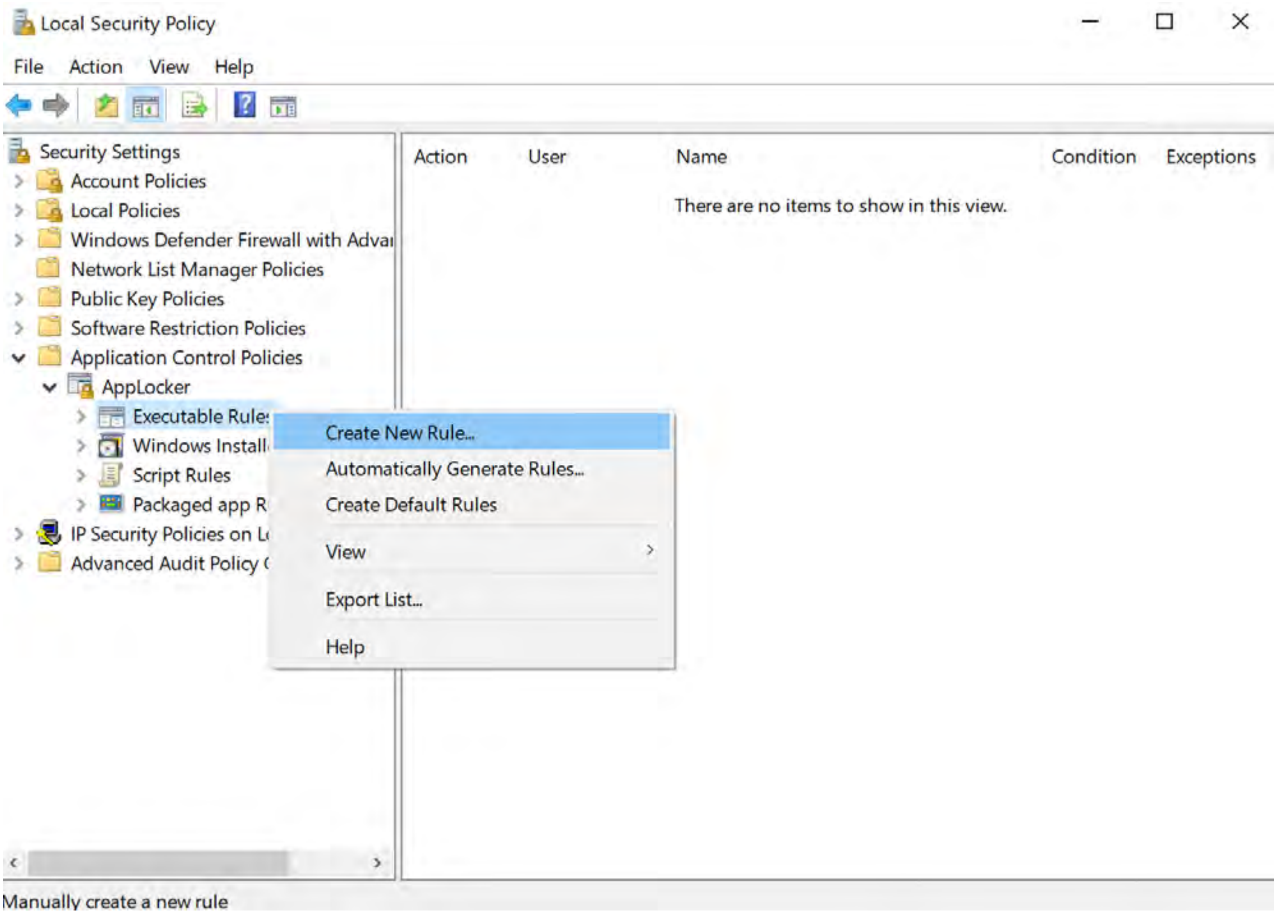
Byte order
● Little endian ○ Big endian

□ Hexadecimal basis (for integral numbers)

Overwrite

Then, a new hash-based application restriction rule is needed. To create it, the evaluator shall perform these following steps:

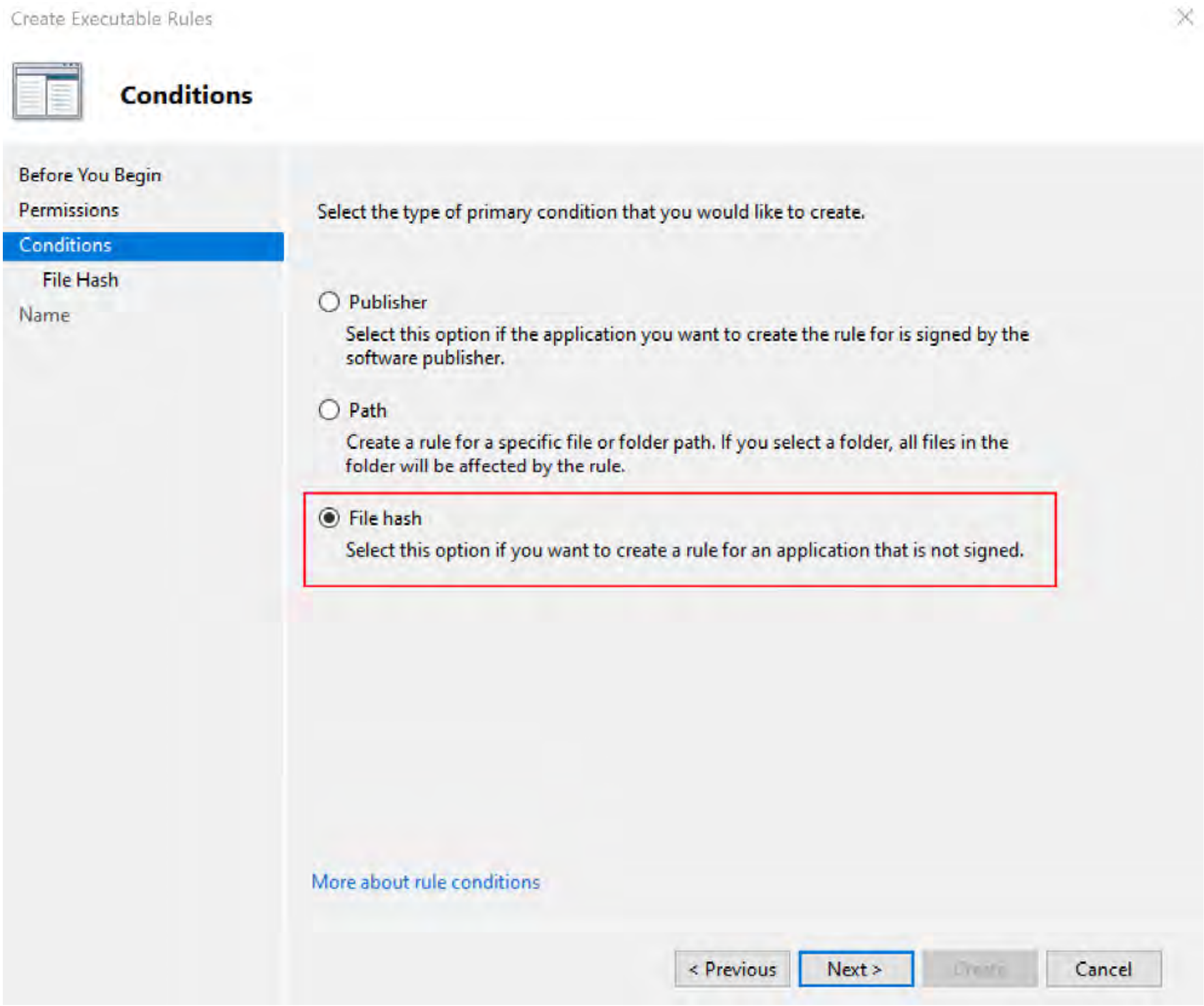
- Open the *Local Security Policy*. (*WIN+r*, then type *secpol.msc*)
- Go to *Security Settings -> Application Restriction Policies -> AppLocker -> Executable Rules*. Right-click on it and select *Create New Rule...*



There are no items to show in this view.

Manually create a new rule

- Click over *Next* and then select *Allow*. Then, click on *Next* again. In *Conditions* select *File Hash*.



Create Executable Rules

Conditions

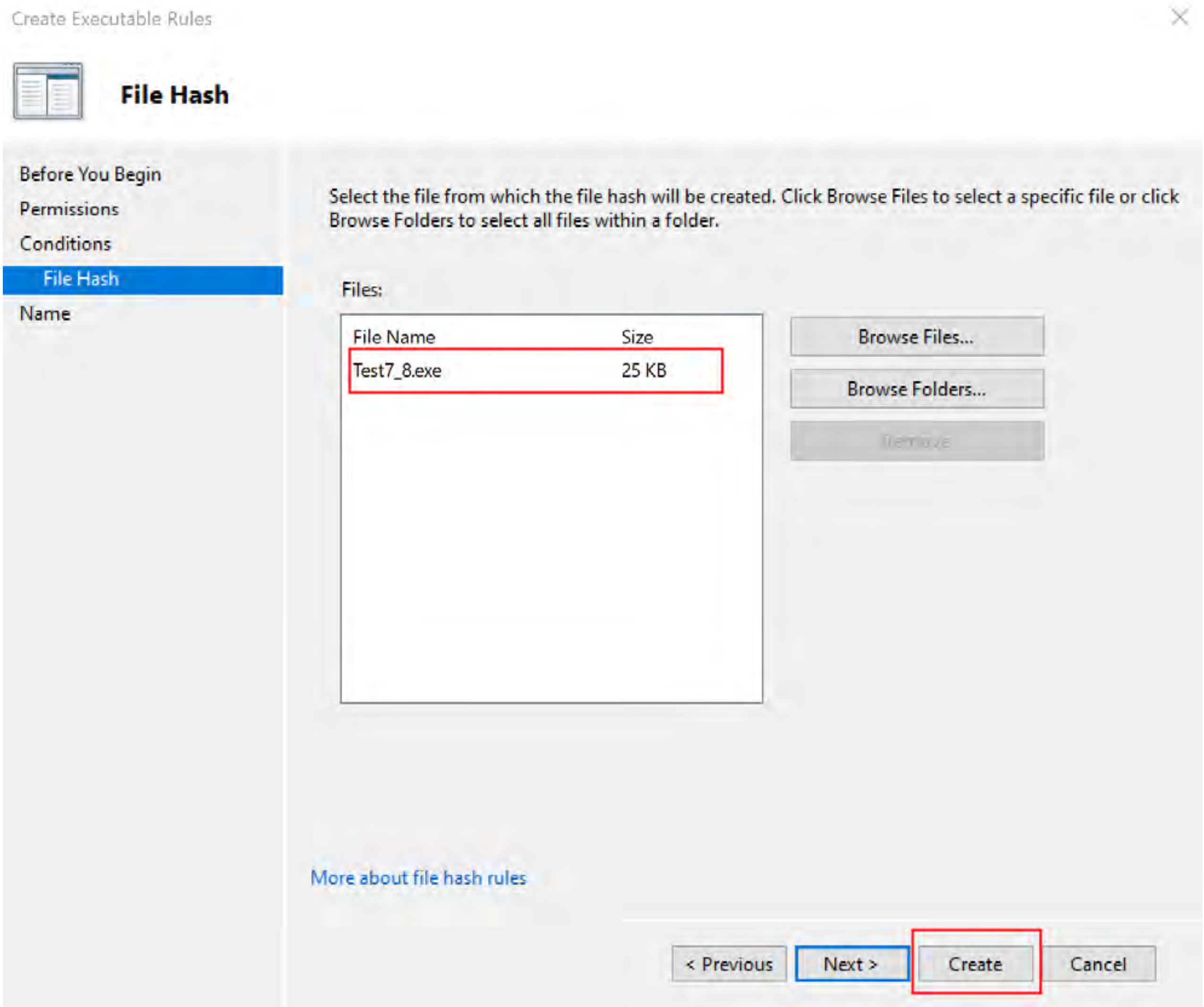
Select the type of primary condition that you would like to create.

○ Publisher
Select this option if the application you want to create the rule for is signed by the software publisher.

○ Path
Create a rule for a specific file or folder path. If you select a folder, all files in the folder will be affected by the rule.

● File hash
Select this option if you want to create a rule for an application that is not signed.

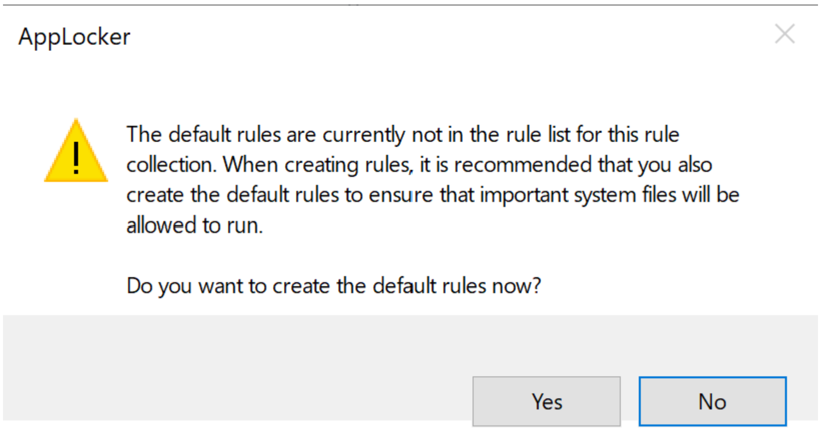
- Browse and select the file *Test7_8.exe*.



Select the file from which the file hash will be created. Click Browse Files to select a specific file or click Browse Folders to select all files within a folder.

File Name	Size
Test7_8.exe	25 KB

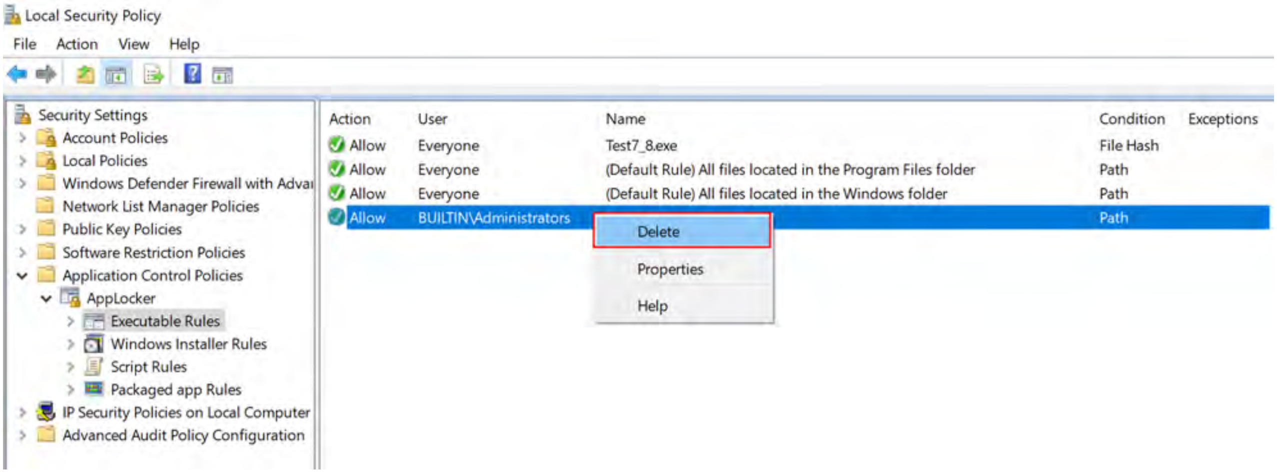
- Click over *Apply* button and select *Yes* to the warning message when prompted.



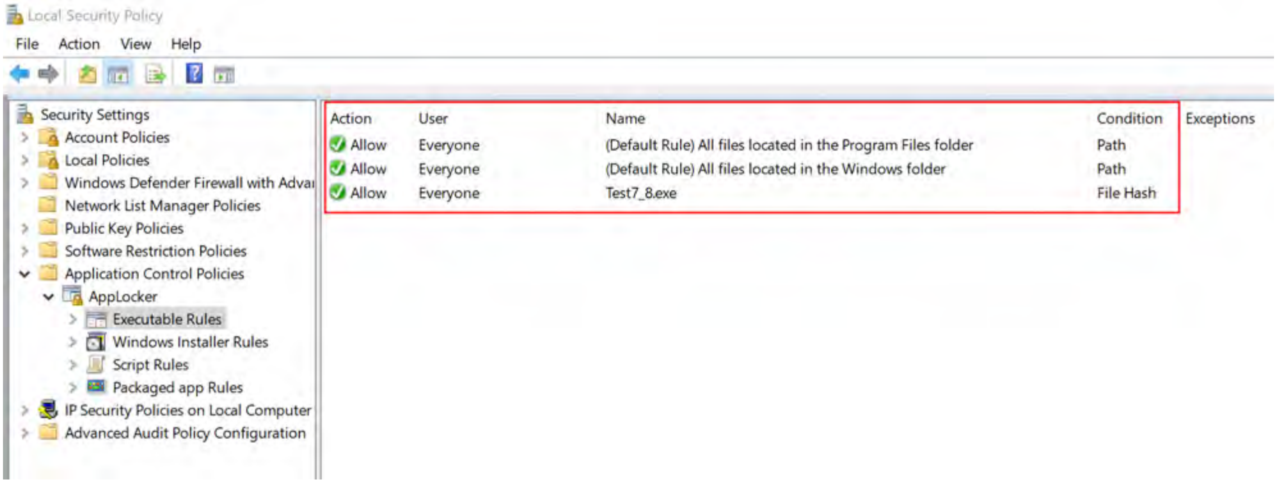
The default rules are currently not in the rule list for this rule collection. When creating rules, it is recommended that you also create the default rules to ensure that important system files will be allowed to run.

Do you want to create the default rules now?

- Go to *Security Settings* -> *Application Restriction Policies* -> *AppLocker* -> *Executable Rules*. Delete the default rule for *BUILTIN\Administrators* as shown below:



Action	User	Name	Condition	Exceptions
Allow	Everyone	Test7_8.exe	File Hash	
Allow	Everyone	(Default Rule) All files located in the Program Files folder	Path	
Allow	Everyone	(Default Rule) All files located in the Windows folder	Path	
Allow	BUILTIN\Administrators		Path	


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Windows Defender Firewall with Advai
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
AppLocker
Executable Rules
Windows Installer Rules
Script Rules
Packaged app Rules
IP Security Policies on Local Computer
Advanced Audit Policy Configuration

Action	User	Name	Condition	Exceptions
Allow	Everyone	(Default Rule) All files located in the Program Files folder	Path	
Allow	Everyone	(Default Rule) All files located in the Windows folder	Path	
Allow	Everyone	Test7_8.exe	File Hash	

- Restart to apply the changes.

42.2.4.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

42.2.4.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

42.2.4.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 7 and Test 8** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 7 and Test 8**.

42.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FPT_SRP_EXT.1.1.

43 FPT_TST_EXT.1.1

The assurance activity for the **FPT_TST_EXT.1.1** requirement is stated as follows:

> The evaluator will verify that the TSS section of the ST includes a comprehensive description of the boot procedures, including a description of the entire bootchain, for the TSF. The evaluator will ensure that the OS cryptographically verifies each piece of software it loads in the bootchain to include bootloaders and the kernel. Software loaded for execution directly by the platform (e.g. first-stage bootloaders) is out of scope. For each additional category of executable code verified before execution, the evaluator will verify that the description in the TSS describes how that software is cryptographically verified.
>
> The evaluator will verify that the TSS contains a description of the protection afforded to the mechanism performing the cryptographic verification.
>
> The evaluator will perform the following tests:
>
> - **Test 1:** The evaluator will perform actions to cause TSF software to load and observe that the integrity mechanism does not flag any executables as containing integrity errors and that the OS properly boots.
> - **Test 2:** The evaluator will modify a TSF executable that is part of the bootchain verified by the TSF (i.e. Not the first-stage bootloader) and attempt to boot. The evaluator will ensure that an integrity violation is triggered and the OS does not boot (Care must be taken so that the integrity violation is determined to be the cause of the failure to load the module, and not the fact that in such a way to invalidate the structure of the module.).
> - **Test 3[conditional]:** If the ST author indicates that the integrity verification is performed using a public key in an X509 certificate, the evaluator will verify that the boot integrity mechanism includes a certificate validation according to FIA_X509_EXT.1 for all certificates in the chain from the certificate used for boot integrity to a certificate in the trust store that are not themselves in the trust store. This means that, for each X509 certificate in this chain that is not a trust store element, the evaluator must ensure that revocation information is available to the TOE during the bootstrap mechanism (before the TOE becomes fully operational).

43.1 Documentation Review Activity

43.1.1 Findings

The evaluator has reviewed the section **6.6.4 Windows Platform Integrity and Code Integrity** of the ***Security Target*** document, which describes the different stages of the boot process, providing information about which are the main files loaded in each step of the boot chain.

This information has allowed the evaluator to design a testing plan, which will be used during the test activity. The evaluator has identified four different stages during the boot process:

- **First stage:** Secure boot checks the file integrity of early boot components, comparing them with the values stored in the TPM. Due to the fact that TPM is part of the external TOE environment, this stage will not be tested during the test activity.
- **Second stage:** After the preliminary components have been loaded, the UEFI firmware loads the OS Boot Manager. Once the integrity of OS Boot Manager has been checked, it attempts to load one of these boot applications:
  - OS Loader: *winload.exe* or *winload.efi*
  - OS Resume: *winresume.exe* or *winresume.efi (The administrative guidance states that the hibernation is disabled, so this boot application will not be used during the evaluation)*
  - A physical memory testing application: *memtest.exe (The* **Security Target** *document states that it is considered a non-operational mode for the evaluation).*

  In addition, a list with the critical loaded files during the bootchain when the *winload.exe* is selected has been included. These files are the following:

  - This text has been intentionally left blank.
- **Third stage:** Once the *winload.exe* or *winload.efi* file has been loaded and its integrity has been checked, the next step in the bootchain is loading the *ntoskrnl.exe* file. Additional critical drivers and libraries are loaded together with this file. The following information is also included regarding Code Integrity, which verifies the integrity of the kernel drivers loaded into the memory. For x64-based computers, all kernel-mode drivers must be digitally signed. If during the boot process an unsigned-driver is loaded, the operating system will not load. In addition, for a x86-based computer only the files listed above must be digitally signed. If any of these files are not signed, the operating system will not load. However, if another unsigned-driver is detected during the boot process, the operating system may be loaded normally.
- **Fourth stage:** After the critical device drivers and libraries have been loaded, the Windows kernel continues to boot the rest of the operating system.

The integrity validation mechanism is explained throughout this section, including information about how the TOE validates each piece of software using a hash based signature and an embedded public key.

Finally, this section provides the following information regarding the ability of the operating system to repair itself when a failure occurs during the boot process:

> *Should the Winload boot application be unable to validate the integrity of one of the Windows image files, the Winload boot application does not continue to load other Windows image files. Rather it displays an error message and fails into a non-operational mode. In limited circumstances the pre-boot environment will attempt to repair the boot environment, such as copying files from a repair partition to repair files with integrity errors. When repair is not possible, the boot manager will ask the user to reinstall Windows.*

43.1.2 Verdict

The evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfilment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

43.2 Test Activity

43.2.1 Test 1

The evaluator will observe that the integrity mechanism does not flag any executable with integrity errors and that the OS properly boots.

43.2.1.1 Setup

Before the test execution, the following setup conditions must be fulfilled:

- The platform to be tested shall count with a TPM or a virtual TPM.
- The *PcpTool* application should be available and executed on another computer (not the TOE).
- The boot measurements records need to be stored, to do that the following option related to the boot configuration should be applied via *Command Line Terminal*:

```
bcdedit /set {globalsettings} integrityservices enable
```

43.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

43.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

43.2.1.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

43.2.2 Test 2

An executable file which is part of the bootchain will be modified and then an attempt to boot the TOE will be performed.

43.2.2.1 Setup

Before the test execution, the following setup condition must be fulfilled:

- A hexadecimal editor (e.g. *HxD*) must be installed in the evaluated platforms to modify the binary files loaded during the boot process.
- A *WinPE* USB for both architectures must be available.

43.2.2.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

43.2.2.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

43.2.2.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 2** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 2**.

43.2.3 Test 3

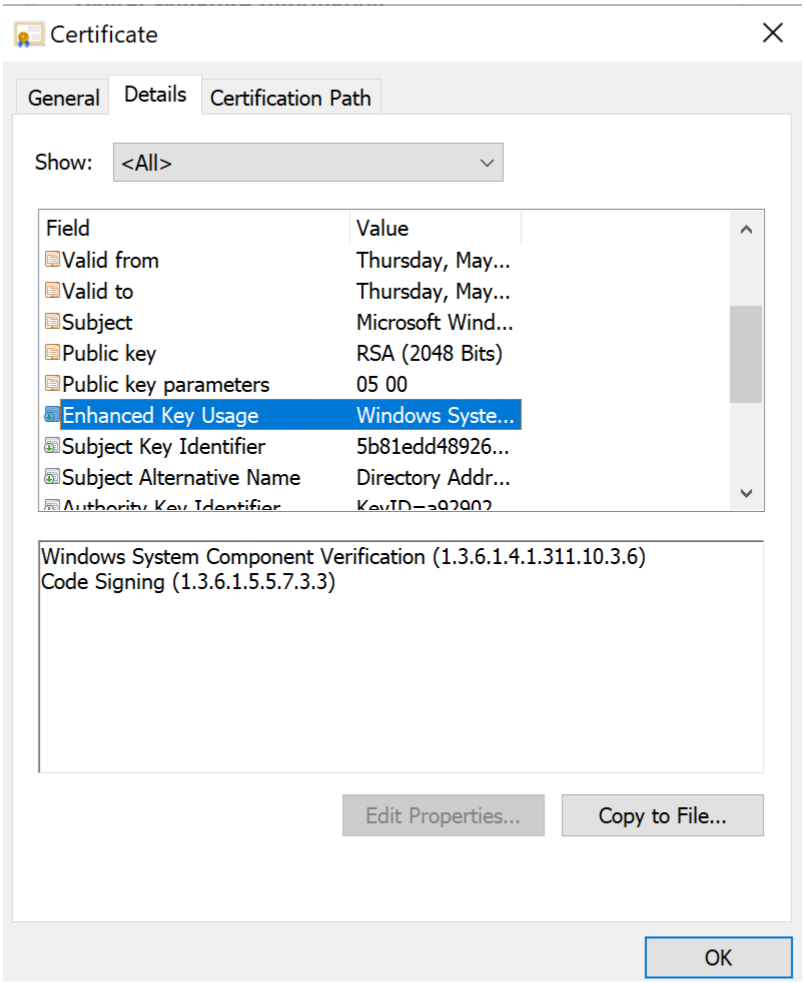
To do this test, the evaluator shall have access to the required binaries signed by the vendor CA.

The evaluator shall attempt to boot the TOE using an executable which has been signed with a certificate which does not have the *Code Signing* purpose. After that, the evaluator shall repeat the same procedure using an executable which has been signed with a certificate which has the *Code Signing* purpose.

43.2.3.1 Setup

To perform the test, the evaluator shall need a binary signed with a valid certificate and without *Code Signing* purpose in the *extendedKeyUsage* field. The vendor has provided the following binary files, which shall be used during the test execution.

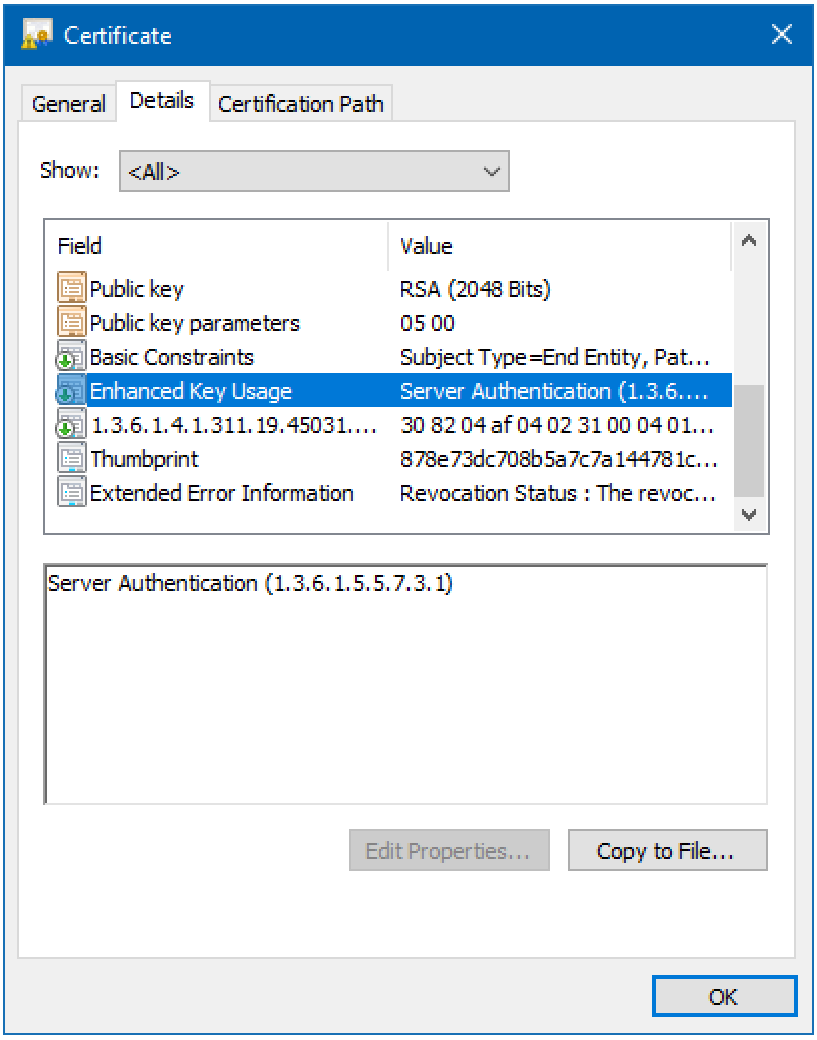
- *cng.sys.codesigned*: This file has been signed using a certificate with *Code Signing* purpose in the *extendedKeyUsage* field as it can be shown in the following picture:



Field	Value
Valid from	Thursday, May...
Valid to	Thursday, May...
Subject	Microsoft Wind...
Public key	RSA (2048 Bits)
Public key parameters	05 00
Enhanced Key Usage	Windows Syste...
Subject Key Identifier	5b81edd48926...
Subject Alternative Name	Directory Addr...
Authority Key Identifier	KeyID=a92902

Windows System Component Verification (1.3.6.1.4.1.311.10.3.6)
Code Signing (1.3.6.1.5.5.7.3.3)

- *cng.sys.serverauthsigned*: This file has been signed using a certificate with *Server Authentication* purpose in the *extendedKeyUsage* field as it can be shown in the following picture:



Show: <All>

Field	Value
Public key	RSA (2048 Bits)
Public key parameters	05 00
Basic Constraints	Subject Type=End Entity, Pat...
Enhanced Key Usage	Server Authentication (1.3.6....
1.3.6.1.4.1.311.19.45031....	30 82 04 af 04 02 31 00 04 01...
Thumbprint	878e73dc708b5a7c7a144781c...
Extended Error Information	Revocation Status : The revoc...

Server Authentication (1.3.6.1.5.5.7.3.1)

- Additionally, a *WinPE* USB for both architectures (x64 & x86) must be available.

43.2.3.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

43.2.3.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

43.2.3.4 Verdict

As the above results state, an integrity error is triggered if a binary file which has been signed using a certificate with an *extendedKeyUsage* value different from *Code Signing* is loaded during the boot process. Otherwise, the boot process is completed properly.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 3** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 3**.

43.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FPT_TST_EXT.1.1.

44 FPT_TUD_EXT.1.1

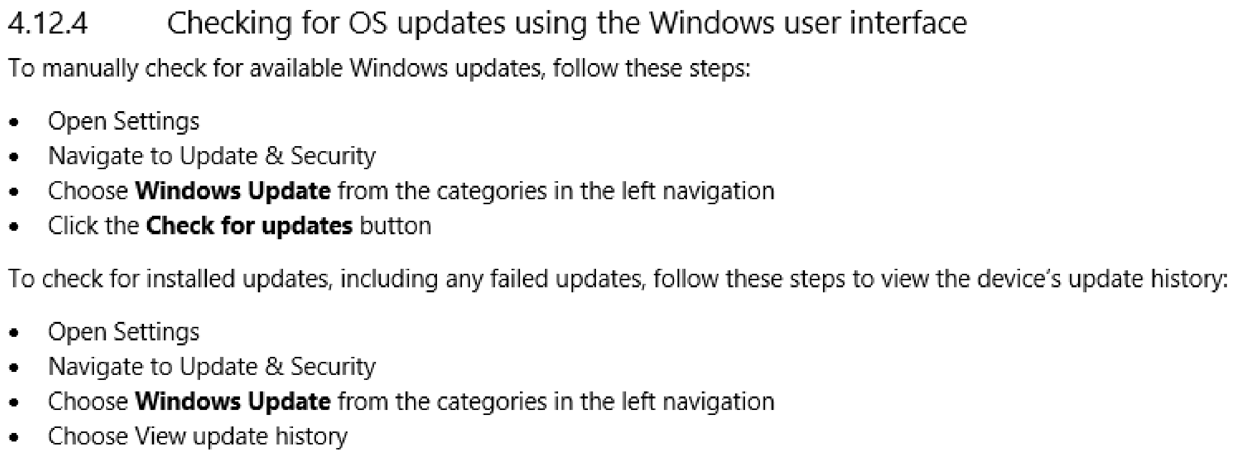
The assurance activity for the **FPT_TUD_EXT.1.1** requirement is stated as follows:

> The evaluator will check for an update using procedures described in the documentation and verify that the OS provides a list of available updates. Testing this capability may require installing and temporarily placing the system into a configuration in conflict with secure configuration guidance which specifies automatic update.
>
> The evaluator is also to ensure that the response to this query is authentic by using a digital signature scheme specified in FCS_COP.1(3). The digital signature verification may be performed as part of a network protocol as described in FTP_ITC_EXT.1. If the signature verification is not performed as part of a trusted channel, the evaluator shall send a query response with a bad signature and verify that the signature verification fails. The evaluator shall then send a query response with a good signature and verify that the signature verification is successful.

44.1 Documentation Review Activity

44.1.1 Findings

The evaluator has reviewed the section **4.12 Managing Updates** of the ***Operational Guidance*** document, which describes the steps which should be followed to check for updates.



4.12.4 Checking for OS updates using the Windows user interface

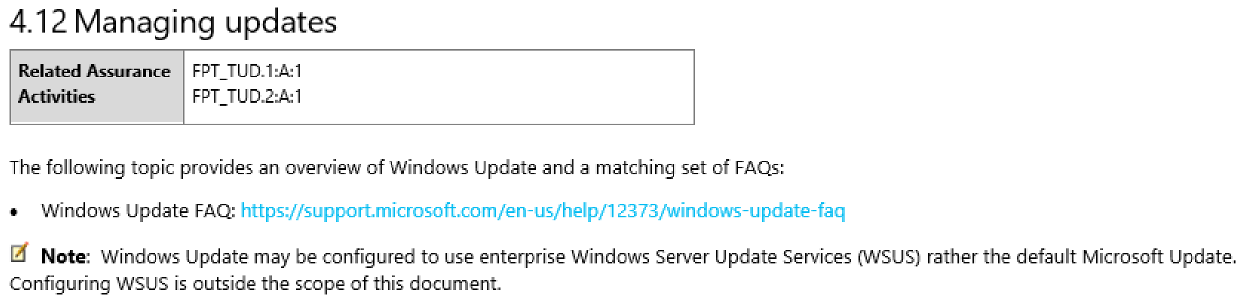
To manually check for available Windows updates, follow these steps:

- Open Settings
- Navigate to Update & Security
- Choose **Windows Update** from the categories in the left navigation
- Click the **Check for updates** button

To check for installed updates, including any failed updates, follow these steps to view the device's update history:

- Open Settings
- Navigate to Update & Security
- Choose **Windows Update** from the categories in the left navigation
- Choose View update history

In addition, there is a link to the Windows support website with a FAQ and instructions to keep the PC up to date. The following screenshot extracted from the ***Operational Guidance*** document, shows this information:



4.12 Managing updates

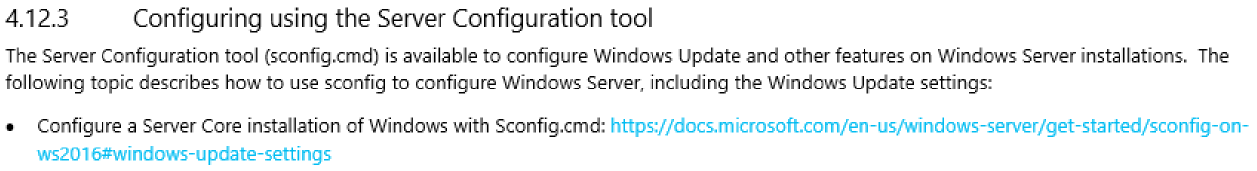
Related Assurance Activities	FPT_TUD.1:A:1 FPT_TUD.2:A:1

The following topic provides an overview of Windows Update and a matching set of FAQs:

- Windows Update FAQ: https://support.microsoft.com/en-us/help/12373/windows-update-faq

Note: Windows Update may be configured to use enterprise Windows Server Update Services (WSUS) rather the default Microsoft Update. Configuring WSUS is outside the scope of this document.

On the other hand, the same section provides a different link to the vendor website where the procedure about how to check for updates in Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions is provided. The following image shows the included link:

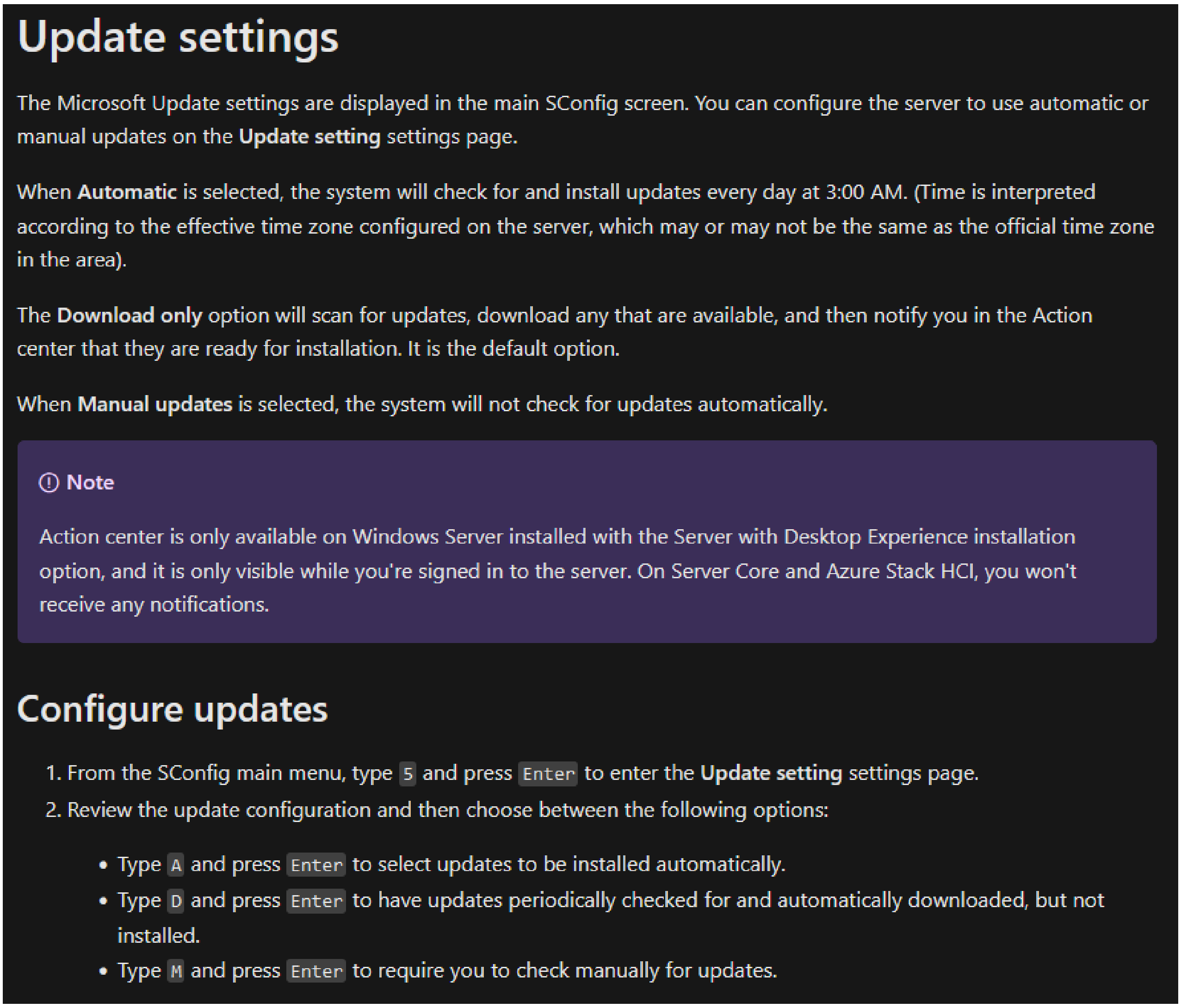


4.12.3 Configuring using the Server Configuration tool

The Server Configuration tool (sconfig.cmd) is available to configure Windows Update and other features on Windows Server installations. The following topic describes how to use sconfig to configure Windows Server, including the Windows Update settings:

- Configure a Server Core installation of Windows with Sconfig.cmd: https://docs.microsoft.com/en-us/windows-server/get-started/sconfig-on-ws2016#windows-update-settings

The vendor's information about managing the update settings provided through the vendor website is the following:



Update settings

The Microsoft Update settings are displayed in the main SConfig screen. You can configure the server to use automatic or manual updates on the **Update setting** settings page.

When **Automatic** is selected, the system will check for and install updates every day at 3:00 AM. (Time is interpreted according to the effective time zone configured on the server, which may or may not be the same as the official time zone in the area).

The **Download only** option will scan for updates, download any that are available, and then notify you in the Action center that they are ready for installation. It is the default option.

When **Manual updates** is selected, the system will not check for updates automatically.

> ⓘ **Note**
>
> Action center is only available on Windows Server installed with the Server with Desktop Experience installation option, and it is only visible while you're signed in to the server. On Server Core and Azure Stack HCI, you won't receive any notifications.

Configure updates

1. From the SConfig main menu, type `5` and press `Enter` to enter the **Update setting** settings page.
2. Review the update configuration and then choose between the following options:
   - Type `A` and press `Enter` to select updates to be installed automatically.
   - Type `D` and press `Enter` to have updates periodically checked for and automatically downloaded, but not installed.
   - Type `M` and press `Enter` to require you to check manually for updates.

44.1.2 Verdict

The ***Operational Guidance*** document includes in its section **4.12 Managing Updates** enough information to allow the evaluator to determine how to check for new updates for all the operating systems evaluated.

The evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfilment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

44.2 Test Activity

44.2.1 Test 1

The evaluator shall ensure that the OS has the ability to check for updates for the operating system and the query is performed over a trusted channel.

44.2.1.1 Setup

Before the test execution, the following setup condition must be fulfilled:

- A network protocol analyzer (e.g. *Wireshark*).

44.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

44.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

44.2.1.4 Verdict

The evaluator has verified that the connection between the client and the update server is performed over a trusted channel, which it has been established as described in *FTP_ITC_EXT.1* and *FCS_TLSC_EXT.1*.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

44.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FPT_TUD_EXT.1.1.

45 FPT_TUD_EXT.1.2

The assurance activity for the **FPT_TUD_EXT.1.2** requirement is stated as follows:

> For the following tests, the evaluator will initiate the download of an update and capture the update prior to installation. The download could originate from the vendor's website, an enterprise-hosted update repository, or another system (e.g. network peer). All supported origins for the update must be indicated in the TSS and evaluated.
>
> - **Test 1:** The evaluator will ensure that the update has a digital signature belonging to the vendor prior to its installation. The evaluator will modify the downloaded update in such a way that the digital signature is no longer valid. The evaluator will then attempt to install the modified update. The evaluator will ensure that the OS does not install the modified update.
> - **Test 2:** The evaluator will ensure that the update has a digital signature belonging to the vendor. The evaluator will then attempt to install the update (or permit installation to continue). The evaluator will ensure that the OS successfully installs the update.

45.1 Documentation Review Activity

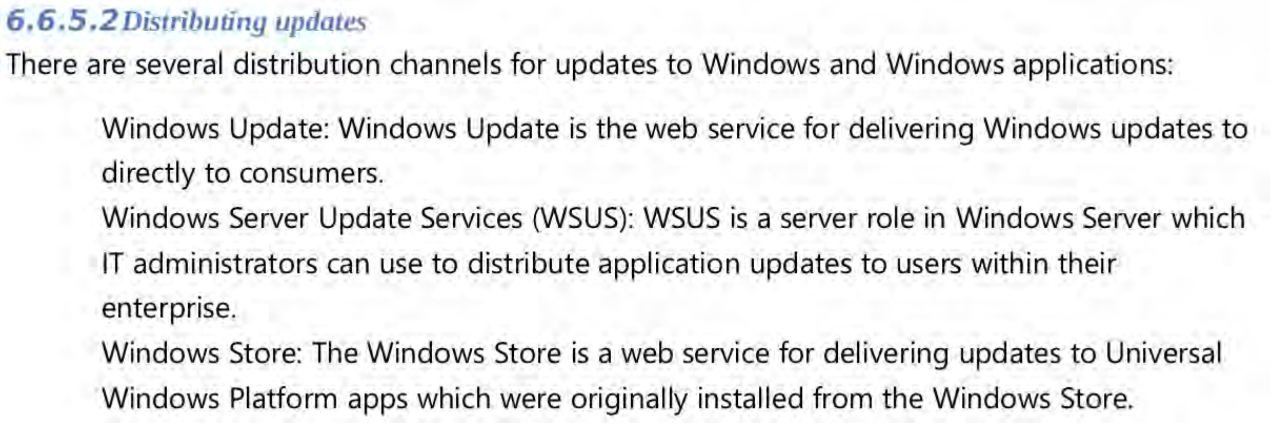
45.1.1 Findings

The evaluator has reviewed the section **6.6.5 Windows and Application Updates** of the ***Security Target*** document, which is related to how the updates are provided by the vendor.

This section states that the operating system updates are delivered through the *Windows Update* capability, which is enabled by default. Additionally, this section also states that the user can obtain update files by visiting the following vendor website:

- Windows Update Catalog

Moreover, the ***Security Target*** document, includes the following information in its section **6.6.5.2 Distributing updates**, pointing again that the origin supported by the OS for system updates is the Windows Update.



6.6.5.2 Distributing updates

There are several distribution channels for updates to Windows and Windows applications:

Windows Update: Windows Update is the web service for delivering Windows updates to directly to consumers.

Windows Server Update Services (WSUS): WSUS is a server role in Windows Server which IT administrators can use to distribute application updates to users within their enterprise.

Windows Store: The Windows Store is a web service for delivering updates to Universal Windows Platform apps which were originally installed from the Windows Store.

45.1.2 Verdict

The ***Security Target*** document includes enough information in its TSS section to allow the evaluator to know how the updates are provided by the vendor and how to obtain an update file from the vendor website.

The evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfilment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

45.2 Test Activity

45.2.1 Test 1

An attempt to install an update with a non-valid digital signature will be performed during this test case.

45.2.1.1 Setup

Before the test execution, the following setup conditions must be fulfilled:

- The *Wincab* tool provided by the OS vendor which allows the evaluator to pack and unpack the *MSU* update file and extract its content.
- The *PowerShell* execution policy shall be configured to allow the execution of *PowerShell* scripts.

45.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, en-

suring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

45.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

45.2.1.4 Verdict

After analysing the obtained results, the evaluator considers that the update file can not be installed properly, when the modified file is used and verified during the installation. In the cases where the modified file is not used during the installation or its integrity is not validated, the update can be applied successfully.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

45.2.2 Test 2

An installation of one update with a valid digital signature belonging to the vendor will be performed during this test case. The update shall be installed successfully.

45.2.2.1 Setup

Before the test execution, the following setup condition must be fulfilled:

- The original update file downloaded for *Test 1* is available.

45.2.2.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

45.2.2.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

45.2.2.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 2** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 2**.

45.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FPT_TUD_EXT.1.2.

46 FPT_TUD_EXT.2.1

The assurance activity for the **FPT_TUD_EXT.2.1** requirement is stated as follows:

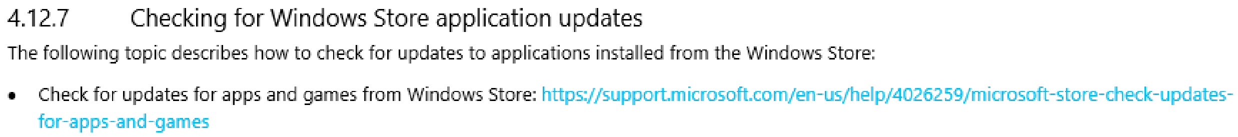
> The evaluator will check for updates to application software using procedures described in the documentation and verify that the OS provides a list of available updates. Testing this capability may require temporarily placing the system into a configuration in conflict with secure configuration guidance which specifies automatic update.
>
> The evaluator is also to ensure that the response to this query is authentic by using a digital signature scheme specified in FCS_COP.1(3). The digital signature verification may be performed as part of a network protocol as described in FTP_ITC_EXT.1. If the signature verification is not performed as part of a trusted channel, the evaluator shall send a query response with a bad signature and verify that the signature verification fails. The evaluator shall then send a query response with a good signature and verify that the signature verification is successful.

46.1 Documentation Review Activity

46.1.1 Findings

The evaluator has reviewed the section **4.12 Managing Updates** of the ***Operational Guidance*** document, which provides information regarding how to check for application updates in all the operating systems.

Regarding Windows and Windows 11 editions, the vendor provides the following link to the vendor support website, in which the procedure to check for application updates through the *Windows Store* is described.



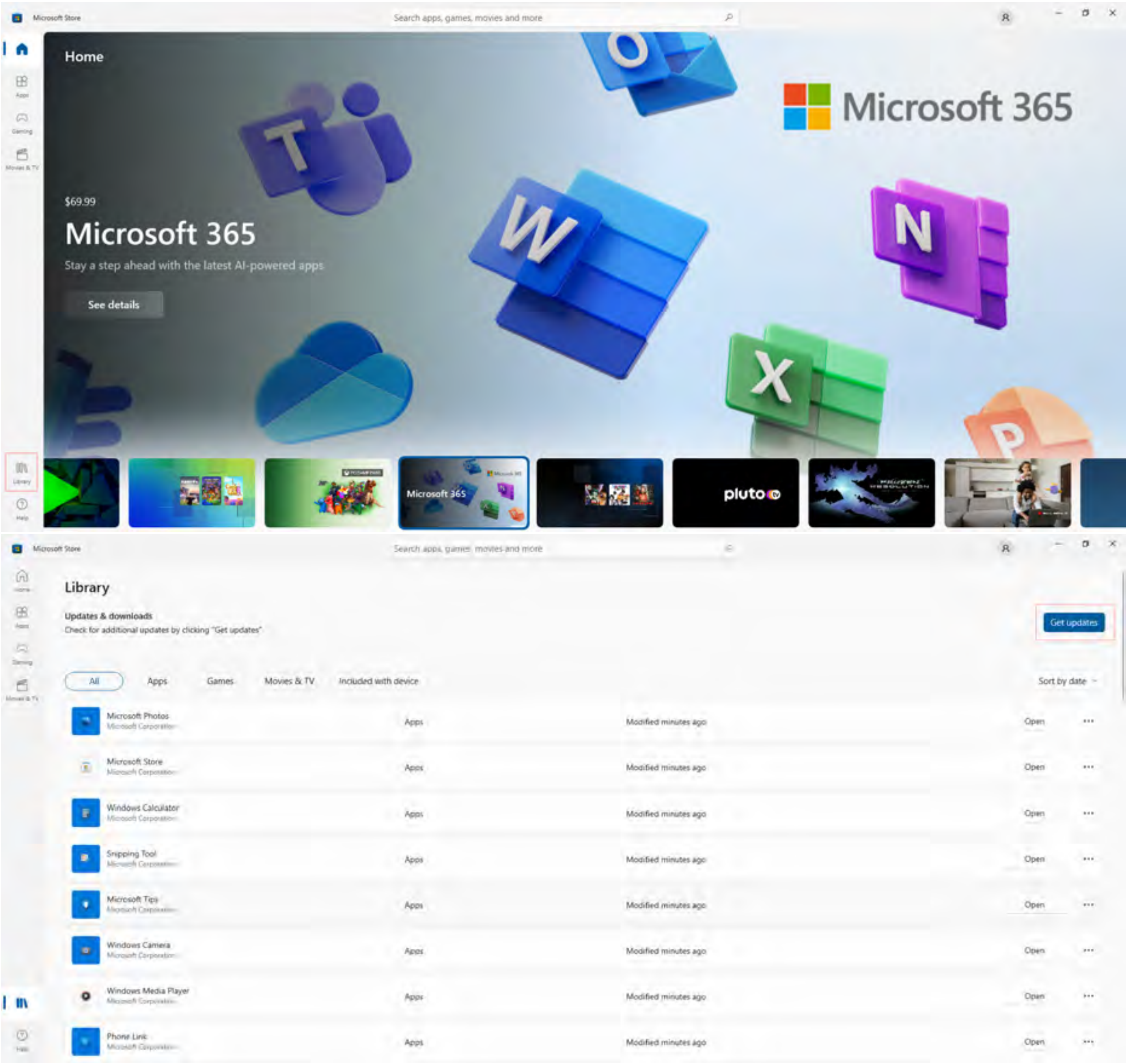
4.12.7 Checking for Windows Store application updates

The following topic describes how to check for updates to applications installed from the Windows Store:

- Check for updates for apps and games from Windows Store: https://support.microsoft.com/en-us/help/4026259/microsoft-store-check-updates-for-apps-and-games

The process, summarised, is the following:

- Go to *Start*, then open *Microsoft Store*. Click the *Library* menu in the left column. On the next page, click the *Get updates* button.



$69.99

Microsoft 365

Stay a step ahead with the latest AI-powered apps

See details

Library

Updates & downloads

Check for additional updates by clicking "Get updates"

Get updates

All | Apps | Games | Movies & TV | Included with device | Sort by date

Microsoft Photos Microsoft Corporation	Apps	Modified minutes ago	Open	···
Microsoft Store Microsoft Corporation	Apps	Modified minutes ago	Open	···
Windows Calculator Microsoft Corporation	Apps	Modified minutes ago	Open	···
Snipping Tool Microsoft Corporation	Apps	Modified minutes ago	Open	···
Microsoft Tips Microsoft Corporation	Apps	Modified minutes ago	Open	···
Windows Camera Microsoft Corporation	Apps	Modified minutes ago	Open	···
Windows Media Player Microsoft Corporation	Apps	Modified minutes ago	Open	···
Phone Link Microsoft Corporation	Apps	Modified minutes ago	Open	···

Regarding Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions, the vendor has provided the following link, describing also the necessary steps to check for application updates. This section also includes a link explaining the required infrastructure (*Windows Server Update Service*).

4.12.3 Configuring using the Server Configuration tool

The Server Configuration tool (sconfig.cmd) is available to configure Windows Update and other features on Windows Server installations. The following topic describes how to use sconfig to configure Windows Server, including the Windows Update settings:

- Configure a Server Core installation of Windows with Sconfig.cmd: https://docs.microsoft.com/en-us/windows-server/get-started/sconfig-on-ws2016#windows-update-settings

46.1.2 Verdict

The ***Operational Guidance*** document, includes in its section **4.12 Managing Updates** two pointers to the vendor support website.

The first one, provides enough information to allow the evaluator to determine how to check for application updates through *Windows Store* in Windows 10 and Windows 11.

The second one, explains the required infrastructure needed to check for updates of applications using *Windows Server Update Service*, since the *Windows Store* is not available in Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions.

The evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfilment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

46.2 Test Activity

46.2.1 Test 1

The evaluator shall ensure that the OS has the ability to check for application updates and the query is performed over a trusted channel.

46.2.1.1 Setup

Before the test execution, the following setup conditions must be fulfilled:

- A network protocol analyzer (e.g. *Wireshark*)
- (*Optional but recommended*) Microsoft Windows Store app must be configured with a Microsoft account before checking for updates.

A different approach was taken to test this requirement in Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions, since the Windows Store is not available for any edition of Windows Server.

46.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

46.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

46.2.1.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 1** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 1** activity.

46.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to this FPT_TUD_EXT.2.1.

47 FPT_TUD_EXT.2.2

The assurance activity for the **FPT_TUD_EXT.2.2** requirement is stated as follows:

> The evaluator will initiate an update to an application. This may vary depending on the application, but it could be through the application vendor's website, a commercial app store, or another system. All origins supported by the OS must be indicated in the TSS and evaluated. However, this only includes those mechanisms for which the OS is providing a trusted installation and update functionality. It does not include user or administrator-driven download and installation of arbitrary files.
>
> - **Test 1:** The evaluator will ensure that the update has a digital signature which chains to the OS vendor or another trusted root managed through the OS. The evaluator will modify the downloaded update in such a way that the digital signature is no longer valid. The evaluator will then attempt to install the modified update. The evaluator will ensure that the OS does not install the modified update.
> - **Test 2:** The evaluator will ensure that the update has a digital signature belonging to the OS vendor or another trusted root managed through the OS. The evaluator will then attempt to install the update. The evaluator will ensure that the OS successfully installs the update.

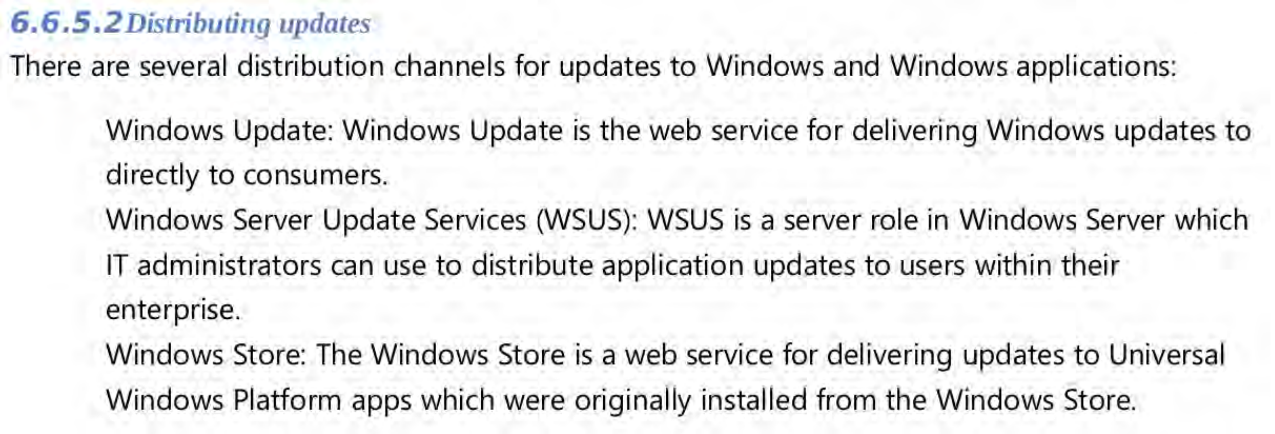
47.1 Documentation Review Activity

47.1.1 Findings

The evaluator has reviewed the section **6.6.5.1 Windows Store Applications** of the ***Security Target*** document. The information provided explains how the application packages are verified during its installation using a digital signature from the vendor with the *Code Signing* usage.

The applications are contained in *AppX* packages following the *OPC* standard, whose internal structure are explained in detail in the ***Security Target*** document within its section **10. Appendix B: AppX Package Implementation**.

In addition, the ***Security Target*** document, includes the following information in its section **6.6.5.2 Distributing updates** regarding the origins supported by the operating systems for application updates:



6.6.5.2 Distributing updates

There are several distribution channels for updates to Windows and Windows applications:

Windows Update: Windows Update is the web service for delivering Windows updates to directly to consumers.

Windows Server Update Services (WSUS): WSUS is a server role in Windows Server which IT administrators can use to distribute application updates to users within their enterprise.

Windows Store: The Windows Store is a web service for delivering updates to Universal Windows Platform apps which were originally installed from the Windows Store.

Summarizing, the application updates can be distributed through the following channel:

- Windows Store: this method supported by Windows 10 and Windows 11 operating systems, allows to get update of UWP apps previously installed from it.
- Windows Server Update Services: this method supported by Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge is used by IT administrators to distribute application updates.

47.1.2 Verdict

The evaluator has reviewed the information provided in the TSS section of the ***Security Target*** document. This information allows the evaluator to identify the origin supported by the TOEs for the application updates.

The evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfilment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

47.2 Test Activity

47.2.1 Test 1

The evaluator will ensure that the update has a digital signature which chains to the OS vendor or other trusted root managed by the OS. An application update shall be modified so its digital signature is no longer valid. Therefore the evaluator will ensure that the OS does not install the modified update.

47.2.1.1 Setup

Before the test execution, the following setup conditions must be fulfilled:

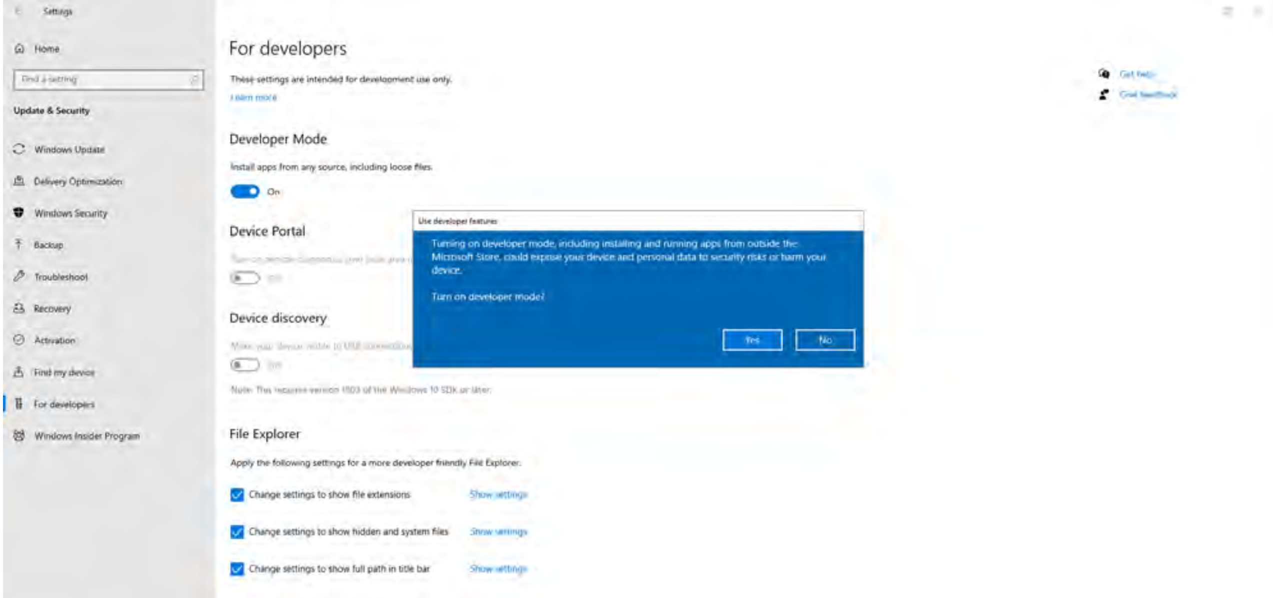
For Windows 10 & Windows 11 operating systems:

- *SignTool*, a command line tool that provides the ability to sign files and verify signatures in files. It is distributed with the *Windows Software Development Kit (SDK)*.
- A hexadecimal editor (e.g. *HxD*)
- A file archiver (e.g. *WinRar*).
- *AppInstallApp_1.0.0.0* and *AppInstallApp_1.1.0.0 .appxbundle* (or *.appx*) installer packages provided by the vendor. These packages require the following dependency packages:
  - *Microsoft.NET.Native.Framework.1.3.appx*
  - *Microsoft.NET.Native.Runtime.1.4.appx*
  - *Microsoft.VCLibs.x64.14.00.appx*

Since these applications are not signed by a trusted certification authority, the following steps must be executed to allow their installation:

- Enable the developer mode. To do that, go to *Settings->Update & Security-> For developers* in Windows 10 or *Settings->Privacy & Security-> For developers* in Windows 11 and select the *Developer mode* option.

47.2.1.1.1 Windows 10 platforms:



For developers

These settings are intended for development use only.

Developer Mode

Install apps from any source, including loose files.

On

Device Portal

Device discovery

Use developer features

Turning on developer mode, including installing and running apps from outside the Microsoft Store, could expose your device and personal data to security risks or harm your device.

Turn on developer mode?

File Explorer

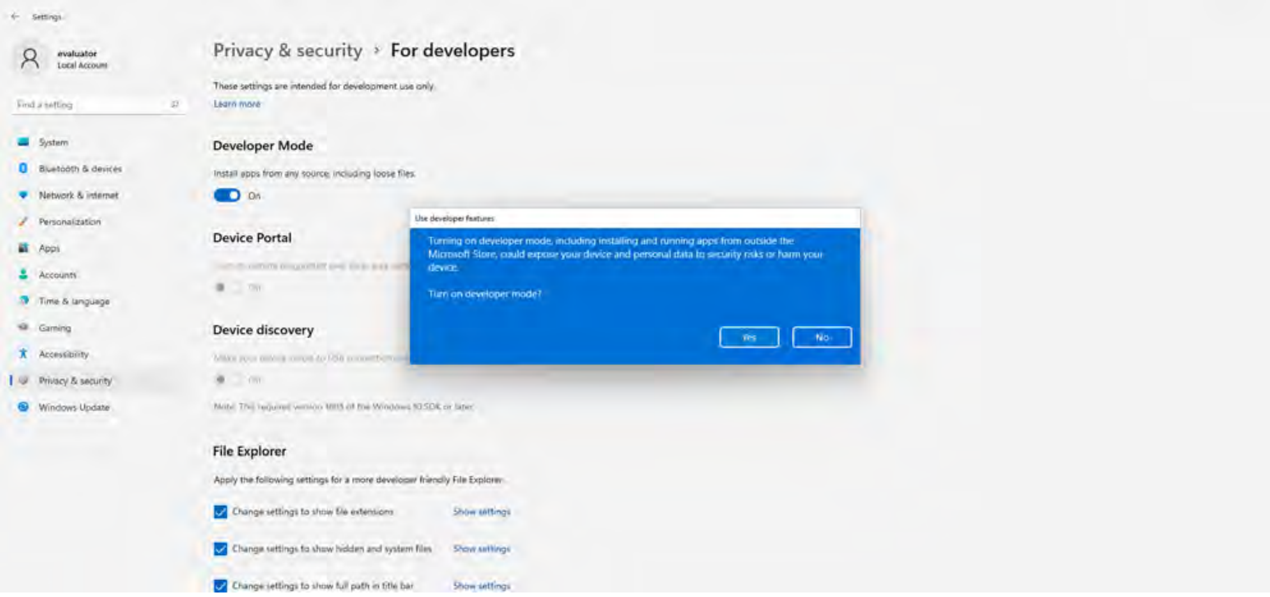
Apply the following settings for a more developer friendly File Explorer.

☑ Change settings to show file extensions

☑ Change settings to show hidden and system files

☑ Change settings to show full path in title bar

47.2.1.1.2 Windows 11 platforms:



Privacy & security > For developers

These settings are intended for development use only.
Learn more

Developer Mode

Install apps from any source, including loose files.
On

Device Portal

Off

Device discovery

Off

Note: This requires version 1803 of the Windows 10 SDK or later.

File Explorer

Apply the following settings for a more developer friendly File Explorer.

☑ Change settings to show file extensions Show settings

☑ Change settings to show hidden and system files Show settings

☑ Change settings to show full path in title bar Show settings

Use developer features

Turning on developer mode, including installing and running apps from outside the Microsoft Store, could expose your device and personal data to security risks or harm your device.

Turn on developer mode?

For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge operating systems:

- A hexadecimal editor (e.g. *HxD*)
- *TestConsole* applications *.msi* packages provided by the vendor.

47.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

47.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

47.2.1.4 Verdict

The evaluator has verified for both operating systems that the application updates are not installed if there is an integrity error in some file used during the update process.

Therefore, the evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 1** requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to **Test 1**.

47.2.2 Test 2

The evaluator will ensure that the update has a digital signature which chains to the OS vendor or other trusted root managed by the OS. The evaluator will ensure that the OS successfully installs the update.

47.2.2.1 Setup

The applicable setup for this test is the same as the one defined for *Test 1*.

47.2.2.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

47.2.2.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

47.2.2.4 Verdict

The evaluator has verified for both operating systems that the application updates are installed properly if the update file has a digital signature which chains to the OS vendor.

Therefore, the evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 2** requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to **Test 2**.

47.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FPT_TUD_EXT.2.2.

48 FTA_TAB.1.1

The assurance activity for the **FTA_TAB.1.1** requirement is stated as follows:

> The evaluator will configure the OS, per instructions in the OS manual, to display the advisory warning message "TEST TEST Warning Message TEST TEST". The evaluator will then log out and confirm that the advisory message is displayed before logging in can occur.

48.1 Documentation Review Activity

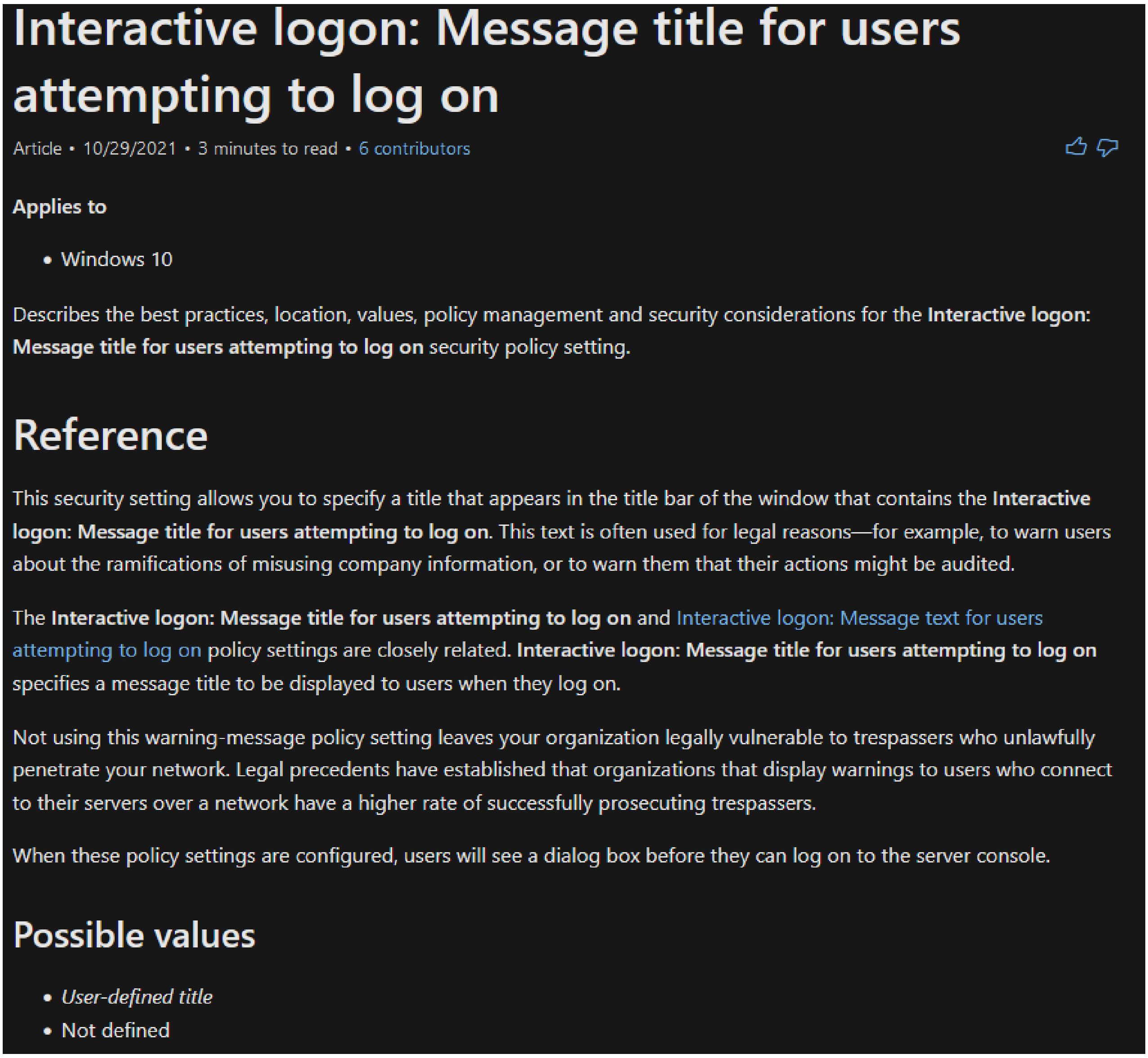
48.1.1 Findings

The evaluator has reviewed the ***Operational Guidance*** document, which explains the necessary steps to configure the OS to display the advisory warning message. This document includes in Section ***4.10 Managing the logon banner*** two links to the vendor support webpage.

These links had been checked and the evaluator has followed the described steps to configure the OS advisory message items:

- Message title for users attempting to log on.
- Message text for users attempting to log on.

The following screenshots show the information provided through the links included in the ***Operational Guidance*** document.



Interactive logon: Message title for users attempting to log on

Article • 10/29/2021 • 3 minutes to read • 6 contributors

Applies to

- Windows 10

Describes the best practices, location, values, policy management and security considerations for the **Interactive logon: Message title for users attempting to log on** security policy setting.

Reference

This security setting allows you to specify a title that appears in the title bar of the window that contains the **Interactive logon: Message title for users attempting to log on.** This text is often used for legal reasons—for example, to warn users about the ramifications of misusing company information, or to warn them that their actions might be audited.

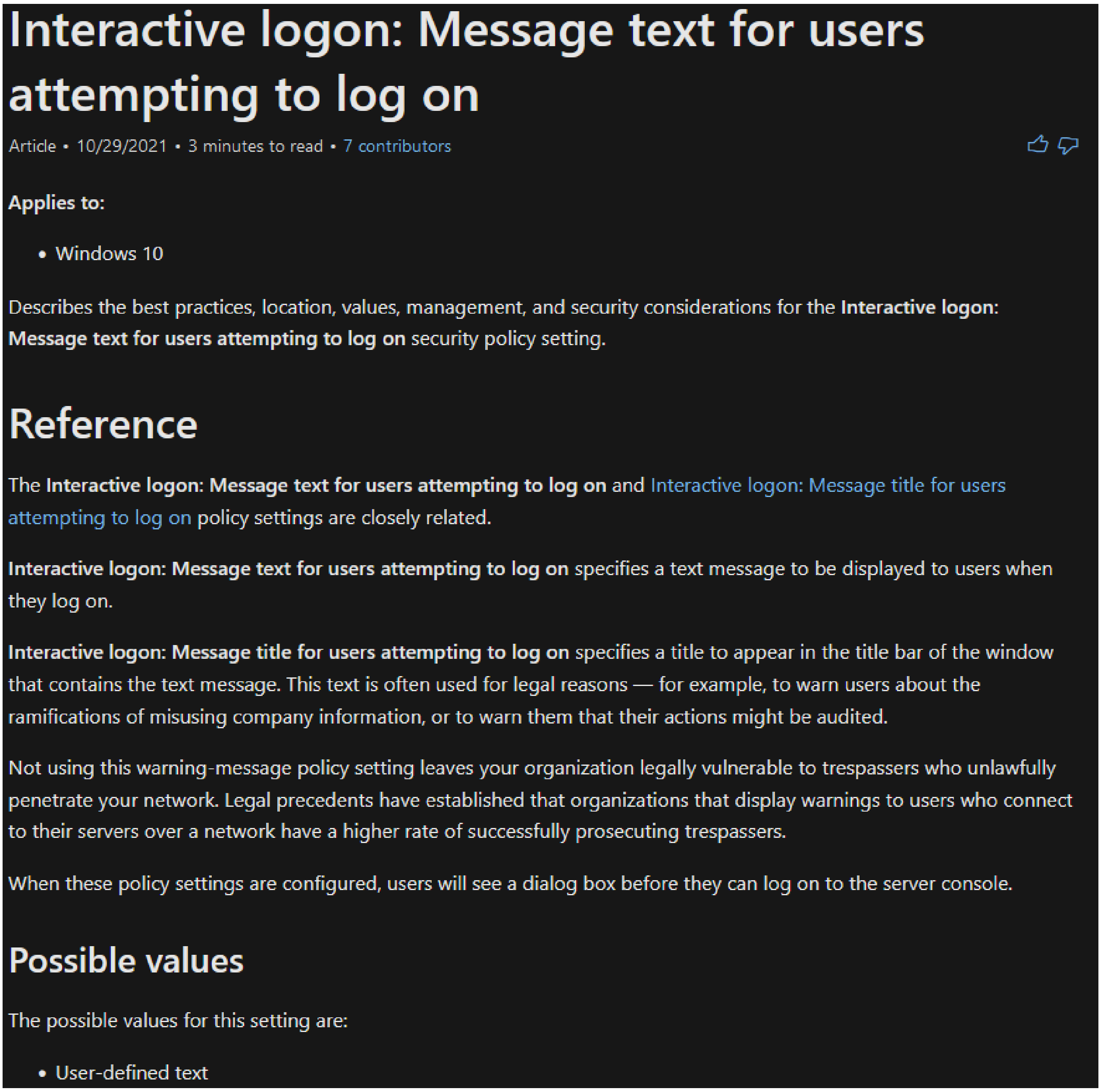
The **Interactive logon: Message title for users attempting to log on** and Interactive logon: Message text for users attempting to log on policy settings are closely related. **Interactive logon: Message title for users attempting to log on** specifies a message title to be displayed to users when they log on.

Not using this warning-message policy setting leaves your organization legally vulnerable to trespassers who unlawfully penetrate your network. Legal precedents have established that organizations that display warnings to users who connect to their servers over a network have a higher rate of successfully prosecuting trespassers.

When these policy settings are configured, users will see a dialog box before they can log on to the server console.

Possible values

- *User-defined title*
- Not defined



Interactive logon: Message text for users attempting to log on

Article • 10/29/2021 • 3 minutes to read • 7 contributors

Applies to:

- Windows 10

Describes the best practices, location, values, management, and security considerations for the **Interactive logon: Message text for users attempting to log on** security policy setting.

Reference

The **Interactive logon: Message text for users attempting to log on** and Interactive logon: Message title for users attempting to log on policy settings are closely related.

Interactive logon: Message text for users attempting to log on specifies a text message to be displayed to users when they log on.

Interactive logon: Message title for users attempting to log on specifies a title to appear in the title bar of the window that contains the text message. This text is often used for legal reasons — for example, to warn users about the ramifications of misusing company information, or to warn them that their actions might be audited.

Not using this warning-message policy setting leaves your organization legally vulnerable to trespassers who unlawfully penetrate your network. Legal precedents have established that organizations that display warnings to users who connect to their servers over a network have a higher rate of successfully prosecuting trespassers.

When these policy settings are configured, users will see a dialog box before they can log on to the server console.

Possible values

The possible values for this setting are:

- User-defined text

48.1.2 Verdict

The evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfilment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

48.2 Test Activity

48.2.1 Test 1

During this test, an advisory warning message will be configured and will be shown by the OS before establishing a user session.

48.2.1.1 Setup

Before the test execution, the following setup condition must be fulfilled:

- The *PowerShell* execution policy shall be configured to allow the execution of *PowerShell* scripts. To do it, execute in a *Powershell* terminal with administrator rights the command:

  ```
  Set-ExecutionPolicy Unrestricted -Force
  ```

- Script *FTA_TAB.ps1* shall be available.

48.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

48.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Voyager Klaas Telecom with Azure Stack Hub (build 10.0.17784.1068)
- Panasonic CF-33 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R840 with Azure Stack Edge (build 10.0.17784.1068)
- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)

- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Voyager Klaas Telecom with Azure Stack Hub (build 10.0.17784.1068)
- HPE Edgeline EL8000 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

48.2.1.4 Verdict

The evaluator considers that, the results obtained during the test activity demonstrate the fulfilment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

48.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FTA_TAB.1.1.

49 FTP_ITC_EXT.1.1 (DTLS)

The assurance activity for the **FTP_ITC_EXT.1.1 (DTLS)** requirement is stated as follows:

> The evaluator will configure the OS to communicate with another trusted IT product as identified in the second selection. The evaluator will monitor network traffic while the OS performs communication with each of the servers identified in the second selection. The evaluator will ensure that for each session a trusted channel was established in conformance with the protocols identified in the first selection.

49.1 Documentation Review activity

49.1.1 Findings

Assurance activity does not state any documentation review activity for this requirement.

49.1.2 Verdict

Assurance activity does not state any documentation review activity for this requirement. Therefore, the **PASS** verdict is assigned to the documentation review activity.

49.2 Test Activity

The assurance activity states that the OS shall use DTLS 1.0 and 1.2 to support web traffic and datagram-based application protocols. These capabilities are tested in FCS_DTLS_EXT.1.1 and FCS_DTLS_EXT.1.2, where the tools *WebClient.exe* and *WebServer.exe* were used, effectively verifying that a trusted channel was established for UDP traffic with web contents. The documentation for FCS_DTLS_EXT.1.1 includes information about the suitability of these tools for this evaluation.

49.2.1 Test 1

49.2.1.1 Setup

The applicable setup for this test is covered in the Test Activity section for the FCS_DTLS_EXT.1.1 requirement.

49.2.1.2 Procedure

The procedure for this test is covered in the Test Activity section for the FCS_DTLS_EXT.1.1 requirement.

49.2.1.3 Results

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

49.2.1.4 Verdict

According to the obtained results for FCS_DTLS_EXT.1.1 and FCS_DTLS_EXT.1.2, the evaluator considers that the requirements established in the assurance activity section for FTP_ITC_EXT.1(DTLS) are fulfilled. Therefore, the **PASS** verdict is assigned to the **Test 1** activity.

49.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to this FTP_ITC_EXT.1.1(DTLS).

50 FTP_ITC_EXT.1.1 (TLS)

The assurance activity for the **FTP_ITC_EXT.1.1 (TLS)** requirement is stated as follows:

> The evaluator will configure the OS to communicate with another trusted IT product as identified in the second selection. The evaluator will monitor network traffic while the OS performs communication with each of the servers identified in the second selection. The evaluator will ensure that for each session a trusted channel was established in conformance with the protocols identified in the first selection.

50.1 Documentation Review activity

50.1.1 Findings

Assurance activity does not state any documentation review activity for this requirement.

50.1.2 Verdict

Assurance activity does not state any documentation review activity for this requirement. Therefore, the **PASS** verdict is assigned to the documentation review activity.

50.2 Test Activity

50.2.1 Test 1

50.2.1.1 Setup

The certificates used for this Assurance Activity are automatically generated by the Active Directory Certificate Services, and its configuration is explained below.

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Server Machine acting as Active Directory Domain Controller, Root Certificate Authority and Web Server (Windows Server 2022)
- Client Machine (Platforms listed in the ST)

These machines are all in the same network with the following configuration:

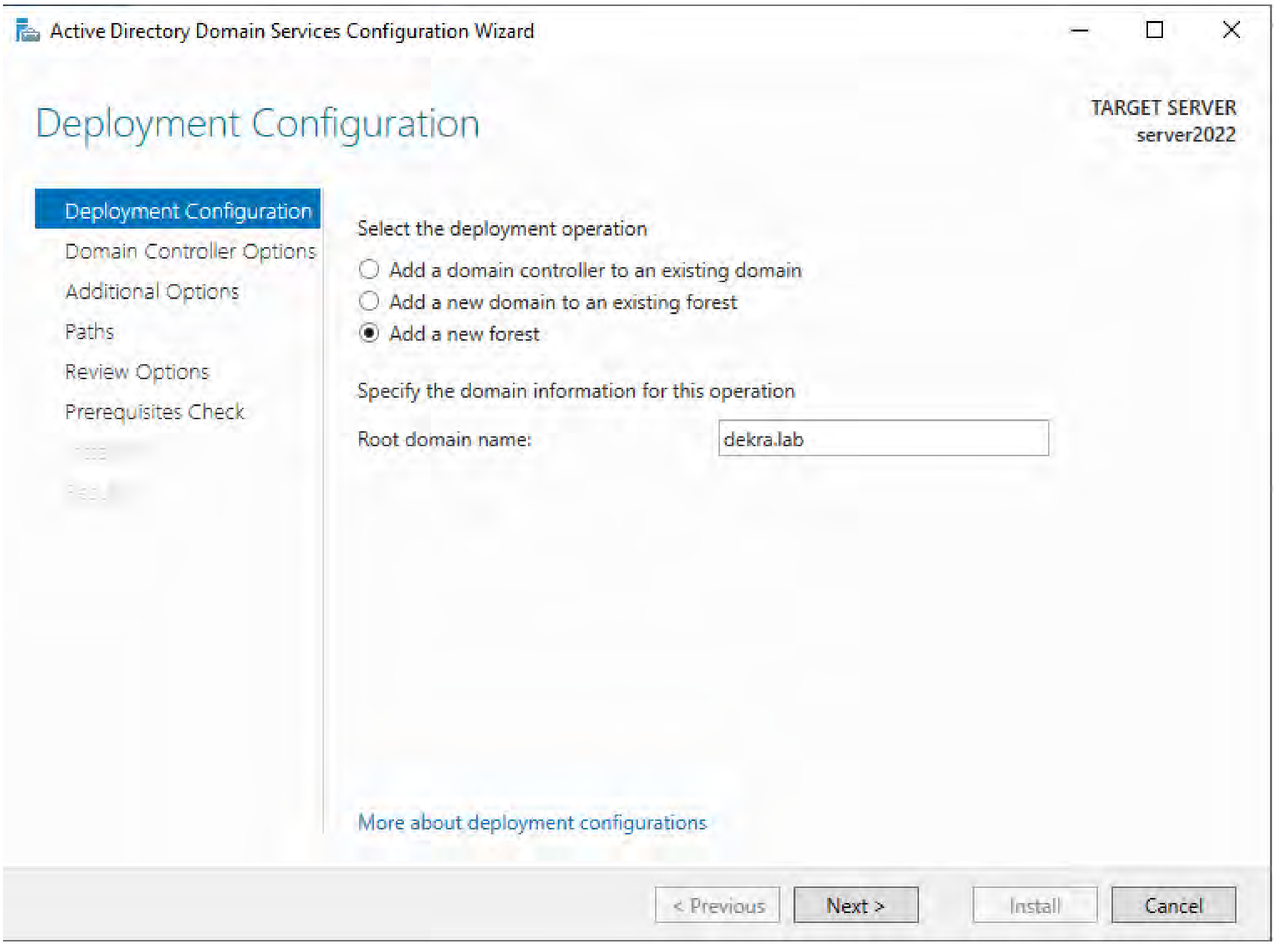
- Server Machine, IP = 192.168.3.22
- Client Machine, IP = 192.168.3.16

The client machine shall have the secure configuration enabled, according to the section **3.2 Operational prerequisites** of the ***Operational Guidance***. In addition, The *Wireshark* network analyzer is installed on the client machine.

The Server Machine shall have the following roles enabled: Active Directory Domain Services, Active Directory Certificate Services and Web Server (IIS). In order to configure the Server Machine the next steps are followed.

"Active Directory Domain Services" role needs to be installed first. It can be done following the next steps:

- Open the Server Manager form the task bar.
- From the Server Manager Dashboard select "Manage" and then "Add Roles and Features".
- Click next until the "Select server roles" screen, then select "Active Directory Domain Services" and then click "Next", accepting the suggested additional features.
- Click "Next" until the confirmation screen is reached, review the selections made and click "Install".
- When finished, click on the "Promote this server to a domain controller" option, in blue colour together with the results.
- From the Deployment Configuration tab select "Add a new forest". Insert your root domain name into the corresponding field and click next. For this evaluation, "dekra.lab" was introduced.



Select the deployment operation

○ Add a domain controller to an existing domain

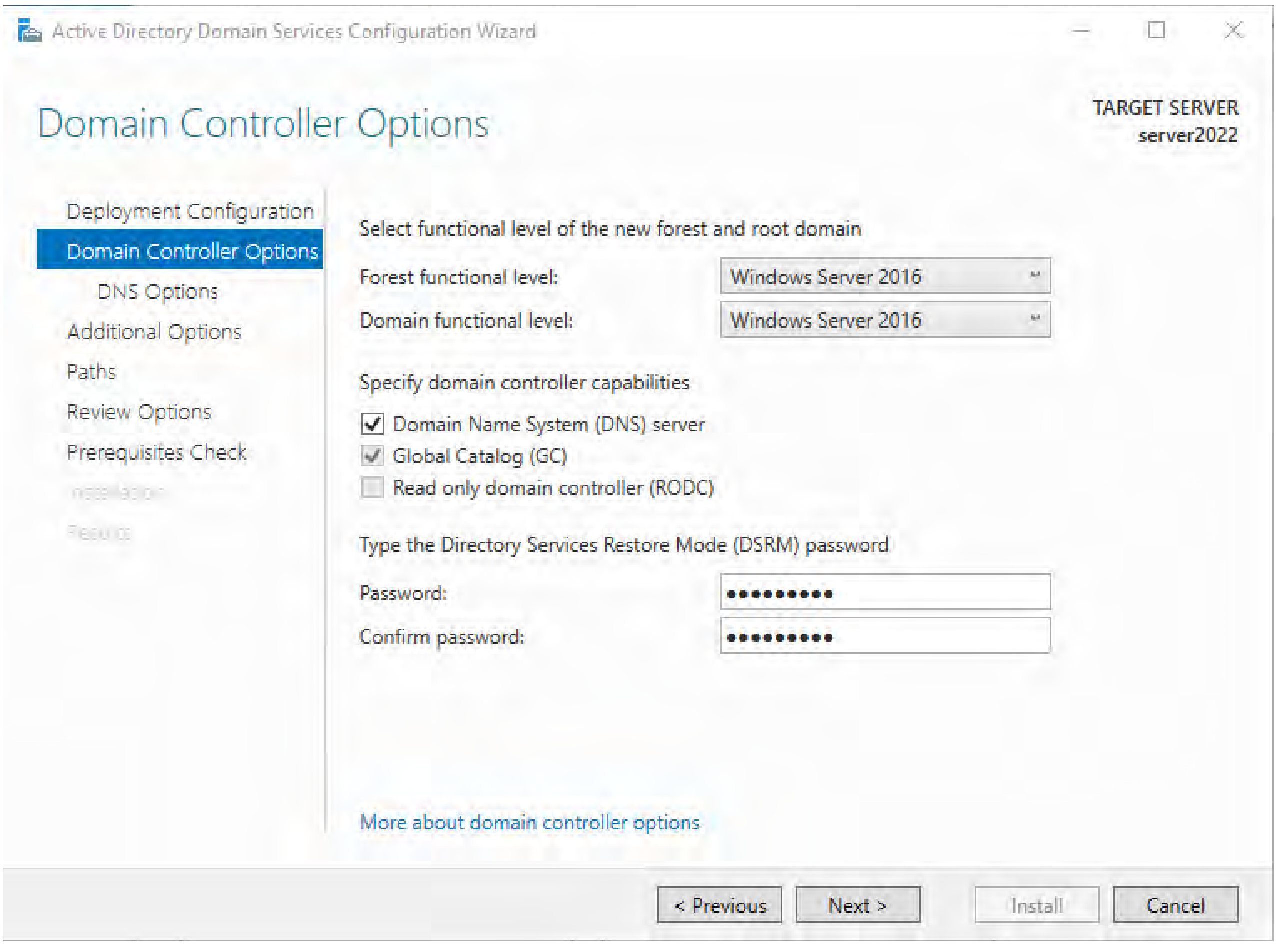
○ Add a new domain to an existing forest

● Add a new forest

Specify the domain information for this operation

Root domain name: dekra.lab

- Select Forest and Domain functional levels. In this case, both are set to "Windows Server 2016". Domain Name System (DNS) server is selected by default. Type a password in the DSRM password field and then click "Next".



Domain Controller Options

TARGET SERVER
server2022

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2016

Domain functional level: Windows Server 2016

Specify domain controller capabilities

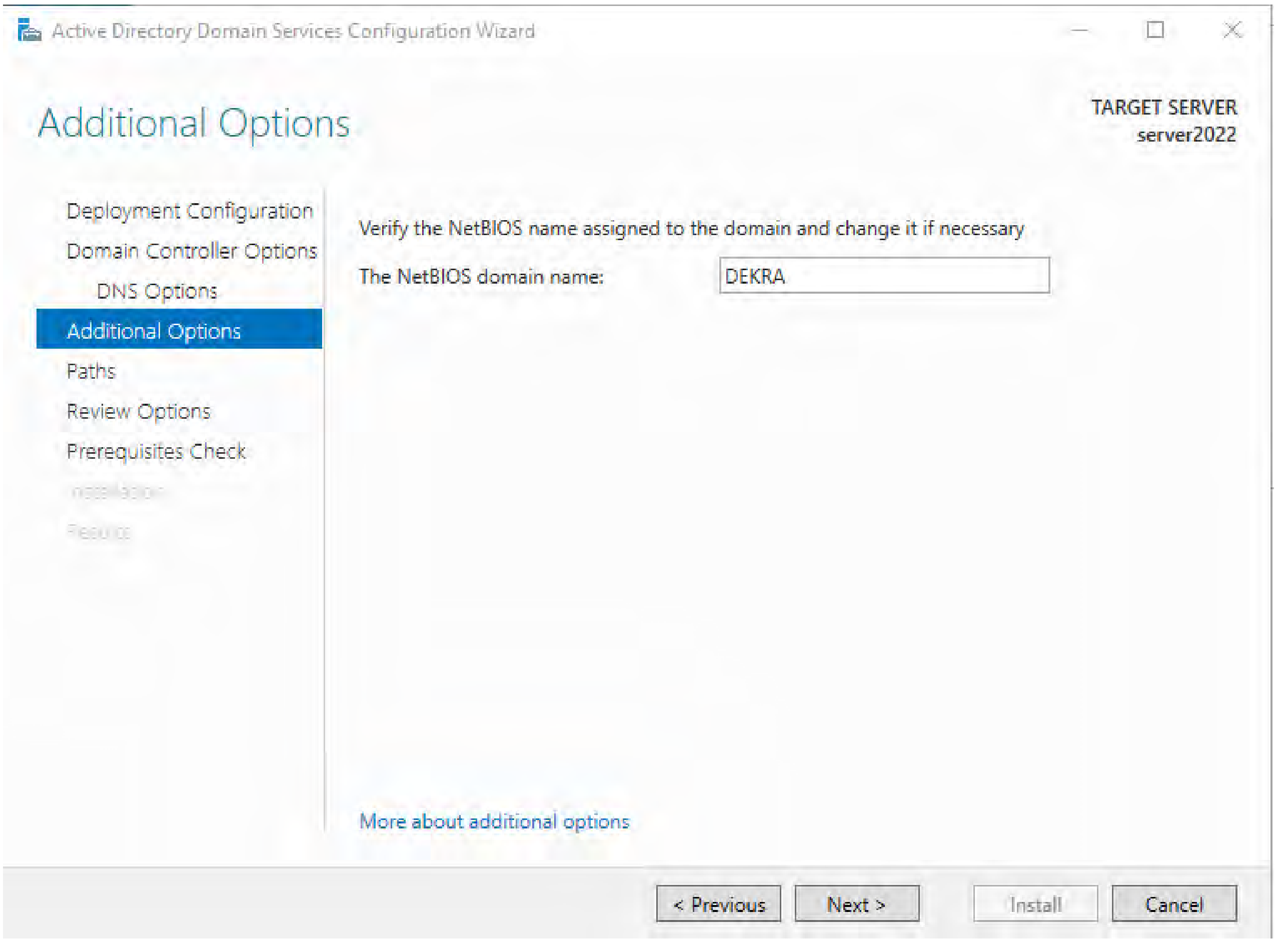
☑ Domain Name System (DNS) server
☑ Global Catalog (GC)
□ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password: ●●●●●●●●●

Confirm password: ●●●●●●●●●

- The next screen warns about DNS delegation unavailability. Click “Next”.
- Confirm the NetBIOS name (“DEKRA” for this evaluation), and then click “Next”.



Active Directory Domain Services Configuration Wizard

Additional Options

TARGET SERVER
server2022

Verify the NetBIOS name assigned to the domain and change it if necessary

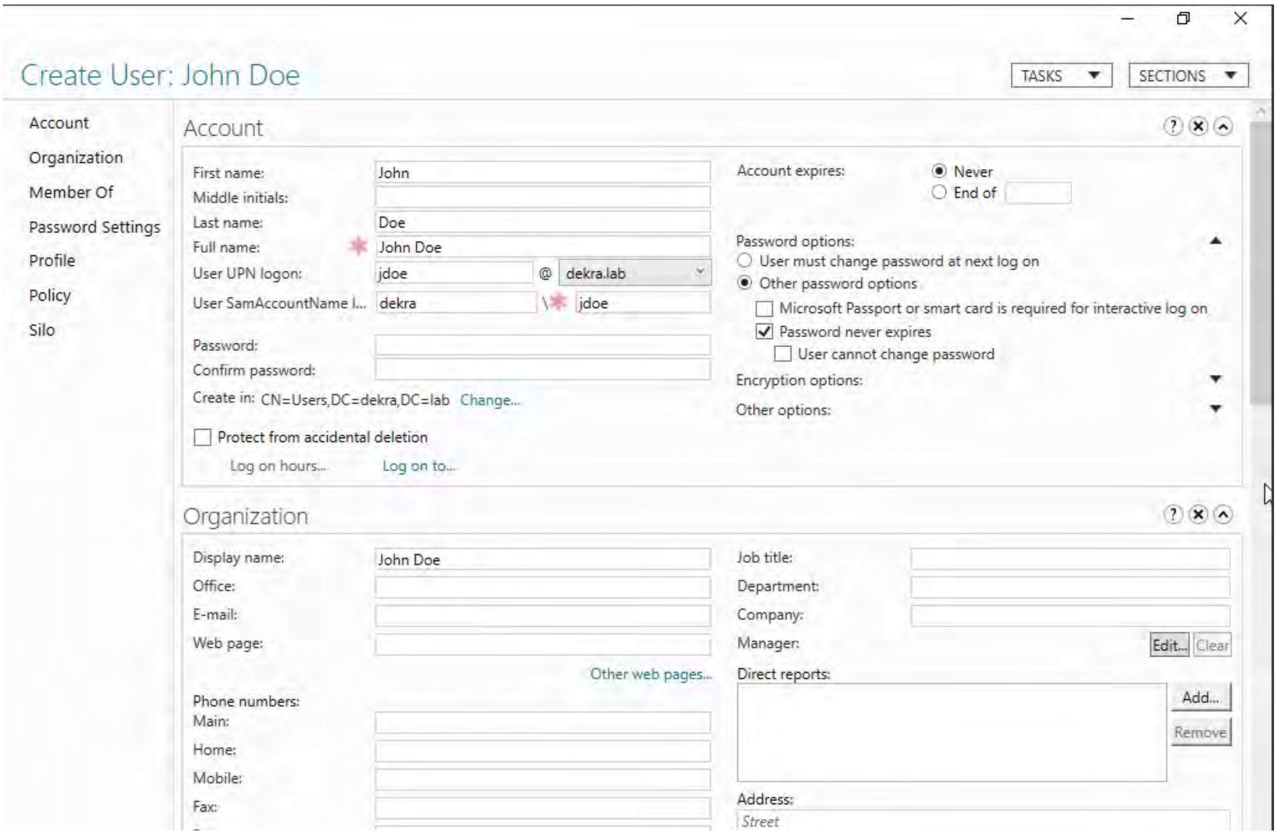
The NetBIOS domain name: DEKRA

More about additional options

- The location of SYSVOL, database folders and log files are selected by default. Click "Next".
- Click "Next" on the "Review Options" screen.
- The system will check to ensure all prerequisites are installed on the system for several minutes. If these tests pass, click "Install".

After the computer restarts, an LDAP user shall be created in the Active Directory Domain Services, following the next steps:

- Open the Server Manager from the task bar.
- Select "AD DS" form the left panel in the Server Manager Dashboard.
- Right click on the server and select "Active Directory Administrative Center".
- Select the section <Domain Name> (local) (Domain Name is set during the Active Directory installation).
- Double-click on the Users folder.
- On the right panel, click "New" in the "Users" section and then click "User".
- On the "Create User" screen, fill the fields: Full name "John Doe", user UPN logon "jdoe". Introduce a valid password and select "Other password options" to avoid the need to change it later and then click "OK".



Create User: John Doe

Account

First name: John
Middle initials:
Last name: Doe
Full name: John Doe
User UPN logon: jdoe @ dekra.lab
User SamAccountName l...: dekra \ jdoe
Password:
Confirm password:
Create in: CN=Users,DC=dekra,DC=lab Change...
□ Protect from accidental deletion
Log on hours... Log on to...

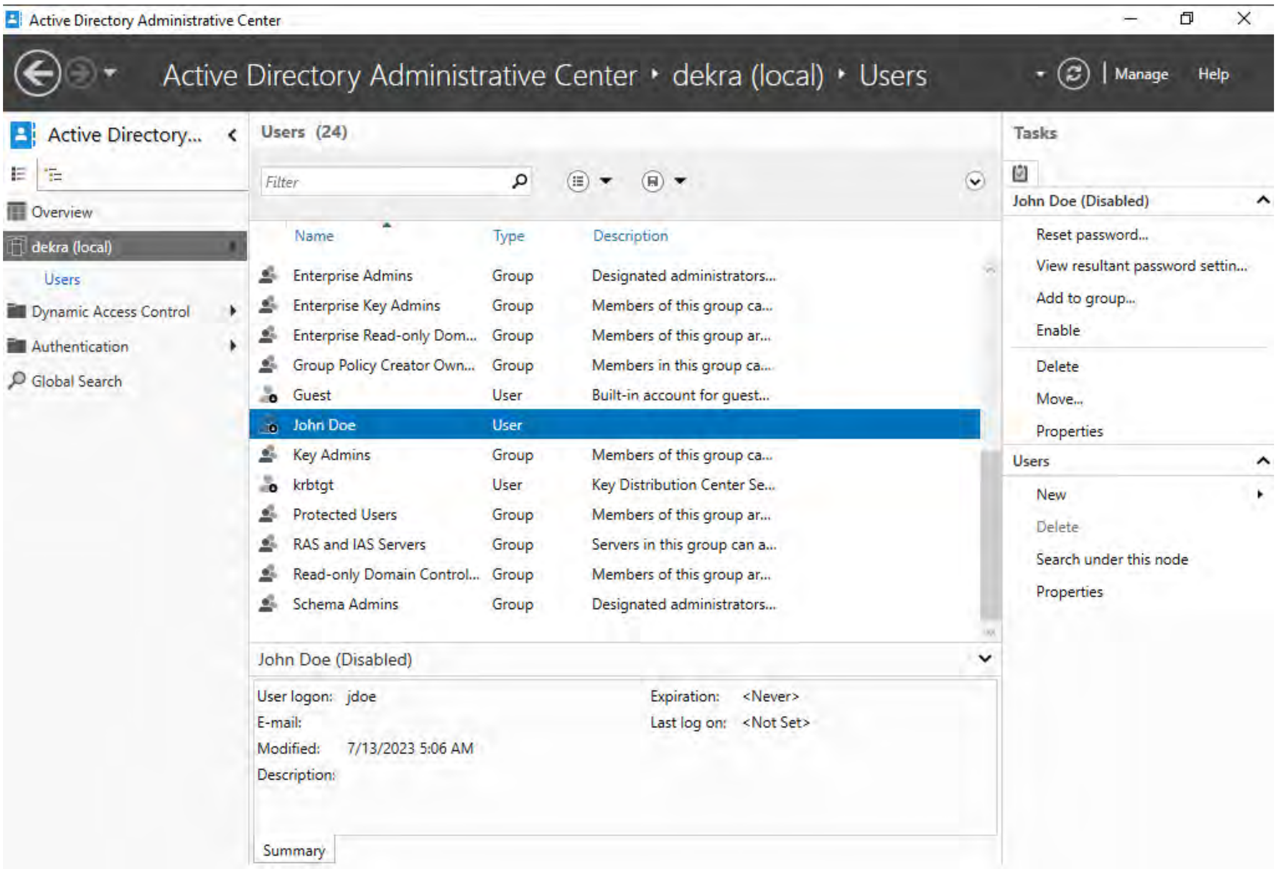
Account expires: ● Never ○ End of
Password options:
○ User must change password at next log on
● Other password options
□ Microsoft Passport or smart card is required for interactive log on
☑ Password never expires
□ User cannot change password
Encryption options:
Other options:

Organization

Display name: John Doe
Office:
E-mail:
Web page:
Other web pages...
Phone numbers:
Main:
Home:
Mobile:
Fax:

Job title:
Department:
Company:
Manager: Edit... Clear
Direct reports: Add... Remove
Address:
Street

- Verify the new user appears in the list of users of the domain.



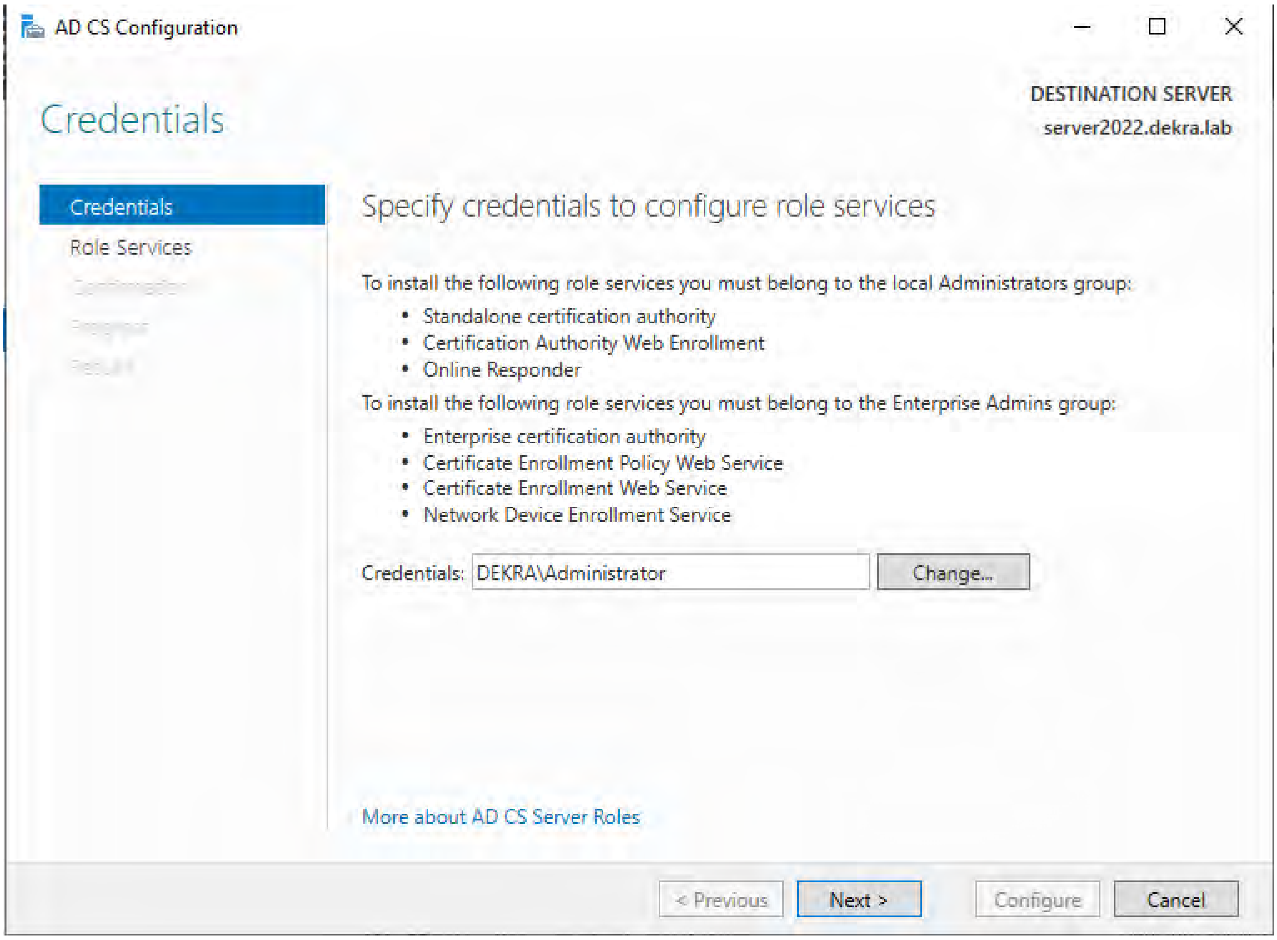
Name	Type	Description
Enterprise Admins	Group	Designated administrators...
Enterprise Key Admins	Group	Members of this group ca...
Enterprise Read-only Dom...	Group	Members of this group ar...
Group Policy Creator Own...	Group	Members in this group ca...
Guest	User	Built-in account for guest...
John Doe	User	
Key Admins	Group	Members of this group ca...
krbtgt	User	Key Distribution Center Se...
Protected Users	Group	Members of this group ar...
RAS and IAS Servers	Group	Servers in this group can a...
Read-only Domain Control...	Group	Members of this group ar...
Schema Admins	Group	Designated administrators...

John Doe (Disabled)

User logon: jdoe
E-mail:
Modified: 7/13/2023 5:06 AM
Description:
Expiration: <Never>
Last log on: <Not Set>

Next, Active Directory Certificate Services shall be installed and configured following the next steps:

- Open the Server Manager form the task bar.
- From the Server Manager Dashboard select “Manage” and then “Add Roles and Features”.
- Click next until the “Select server roles” screen, then select “Active Directory Certificate Services” and click “Next”, accepting the suggested additional features.
- Click “Next” until the “Select role services” screen is shown, and then check the option “Certification Authority” and click “Next”.
- Click “Install”.
- When the installation is finished, click “Configure Active Directory Certificate Services on the destination server”, in blue color together with the results.
- If not there already, write the name of the administrator (“DEKRA/Administrator” for this evaluation) in the “Credentials” field and click “Next”.



Specify credentials to configure role services

To install the following role services you must belong to the local Administrators group:

- Standalone certification authority
- Certification Authority Web Enrollment
- Online Responder

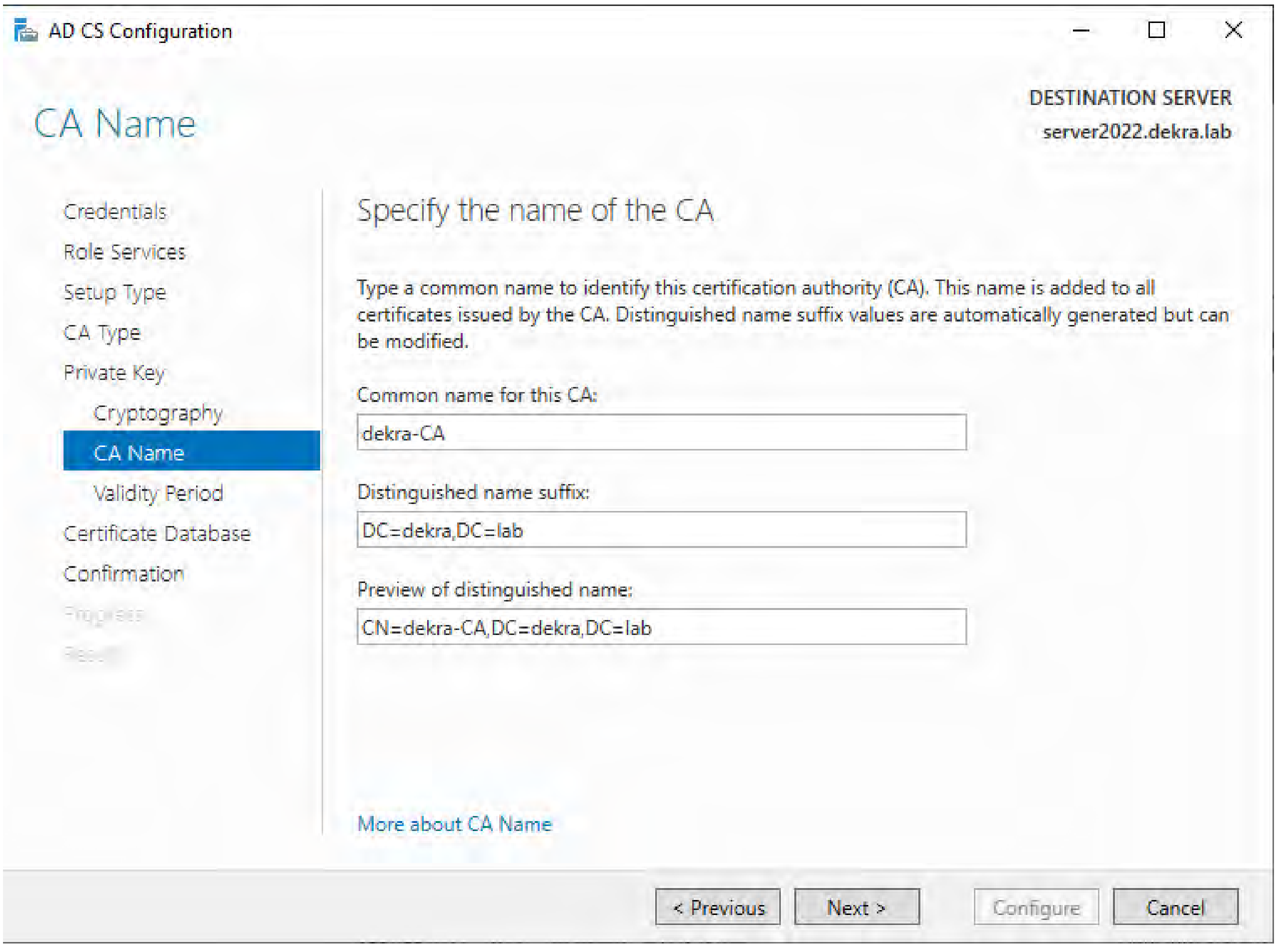
To install the following role services you must belong to the Enterprise Admins group:

- Enterprise certification authority
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Network Device Enrollment Service

Credentials: DEKRA\Administrator Change...

More about AD CS Server Roles

- On the "Role services" screen check the option "Certification Authority" and click "Next".
- On the "Setup Type" screen, select "Enterprise CA" and click "Next".
- On the "CA Type" screen, select "Root CA" and click "Next".
- On the "Private Key" screen, select "Create a new private key" and click "next".
- On the "Cryptography for CA" screen, select SHA256 and click "Next".
- On the "CA Name" screen, all fields are left to default. Click "Next".



Specify the name of the CA

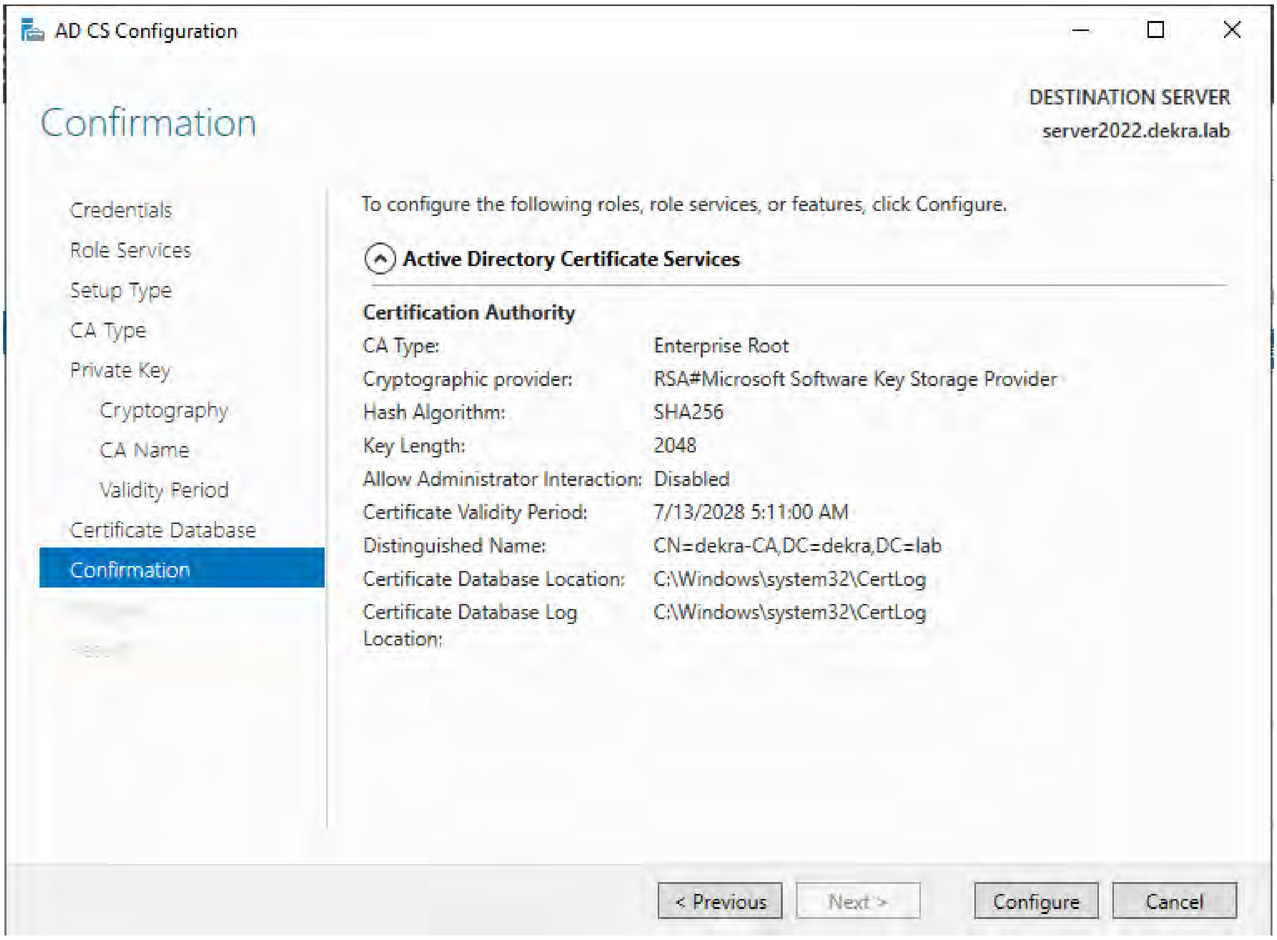
Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA: dekra-CA

Distinguished name suffix: DC=dekra,DC=lab

Preview of distinguished name: CN=dekra-CA,DC=dekra,DC=lab

- On the “Validity Period” screen, select 25 years and click “Next”.
- On the “CA Database” screen, the database locations are left to default. Click “Next”.
- Review the information on the “Confirmation” screen and click “Configure”.



Confirmation

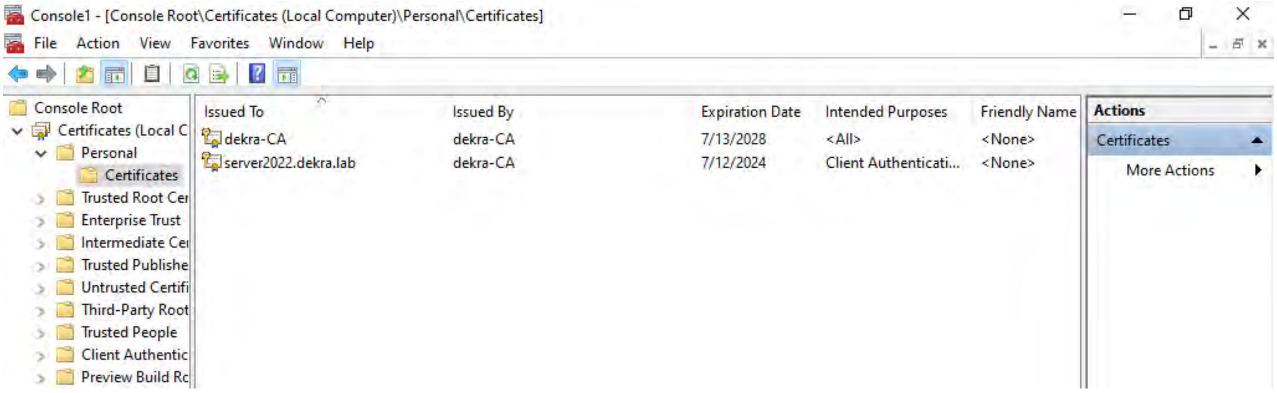
To configure the following roles, role services, or features, click Configure.

Active Directory Certificate Services

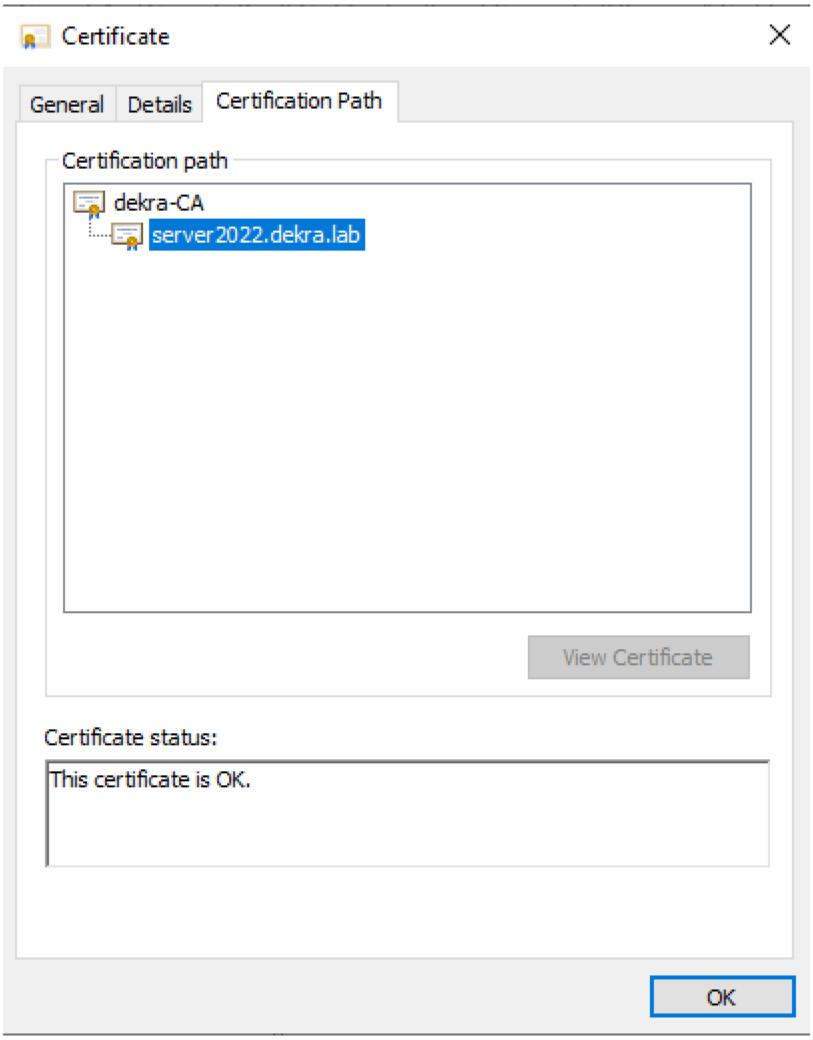
Certification Authority

CA Type:	Enterprise Root
Cryptographic provider:	RSA#Microsoft Software Key Storage Provider
Hash Algorithm:	SHA256
Key Length:	2048
Allow Administrator Interaction:	Disabled
Certificate Validity Period:	7/13/2028 5:11:00 AM
Distinguished Name:	CN=dekra-CA,DC=dekra,DC=lab
Certificate Database Location:	C:\Windows\system32\CertLog
Certificate Database Log Location:	C:\Windows\system32\CertLog

Once finished, reboot the Server Machine. This automatically creates a certificate with *server-Auth* key usage, with reference identifier set to <machine name>.<domain FQDN> (for this evaluation this was "server2022.dekra.lab") and issued by the root CA just created.



Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
dekra-CA	dekra-CA	7/13/2028	<All>	<None>
server2022.dekra.lab	dekra-CA	7/12/2024	Client Authenticati...	<None>



Certificate status:

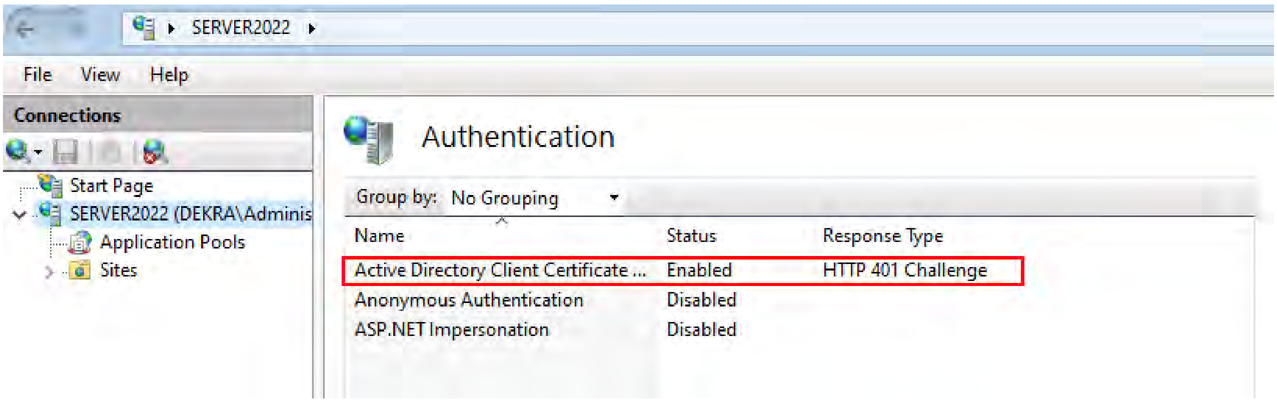
This certificate is OK.

The last role that needs to be installed is “Web Server (IIS)”. In order to do so next steps shall be followed:

- Open the Server Manager form the task bar.
- From the Server Manager Dashboard select “Manage” and then “Add Roles and Features”.
- Click next until the “Select server roles” screen.
- Select “Web Server (IIS)” and then click “Next”, accepting the suggested additional features.
- Click “Next” until the “Select role services” screen is shown, and then leave the options selected by default, additionally checking “Client Certificate Mapping Authentication” under “Web Server” -> “Security”. Then click “Next”.
- Click “Install” and restart the machine when finished.

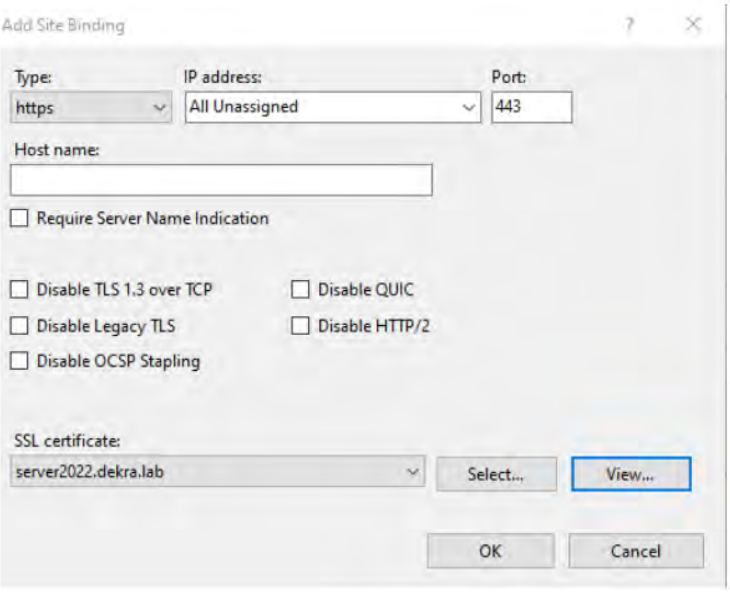
The IIS server shall be configured so that its contents can only be accessed authenticating with a valid client certificate belonging to a user present in the Active Directory, concretely the John Doe user just created. The next steps shall be followed to configure such a scenario:

- Open the Server Manager form the task bar.
- From the Server Manager Dashboard select "Tools" and then "Internet Information Services (IIS) Manager".
- On the left panel, click on <Computer name> (<NetBIOS name>\<Username>), which corresponds to "server2022 (DEKRA\Administrator)" for this evaluation.
- In the middle "Features View" panel, double-click on "Authentication". Disable "Anonymous Authentication" and enable "Active Directory Client Certificate Authentication".



Name	Status	Response Type
Active Directory Client Certificate ...	Enabled	HTTP 401 Challenge
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Disabled	

- On the left panel, click on "Default Web Site".
- On the right "Actions" panel, click "Bindings...".
- Click "Add..." and select "https" as "Type", and the <machine name>.<domain FQDN> certificate ("server2022.dekra.lab" in this evaluation) as "SSL certificate", leaving the other options by default. Then click "OK" and "Close".



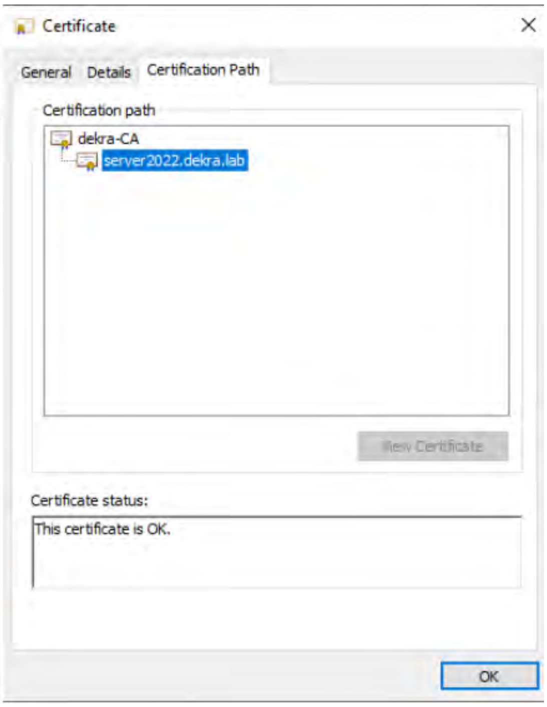
Add Site Binding

Type: https
IP address: All Unassigned
Port: 443
Host name:

□ Require Server Name Indication

□ Disable TLS 1.3 over TCP
□ Disable QUIC
□ Disable Legacy TLS
□ Disable HTTP/2
□ Disable OCSP Stapling

SSL certificate: server2022.dekra.lab



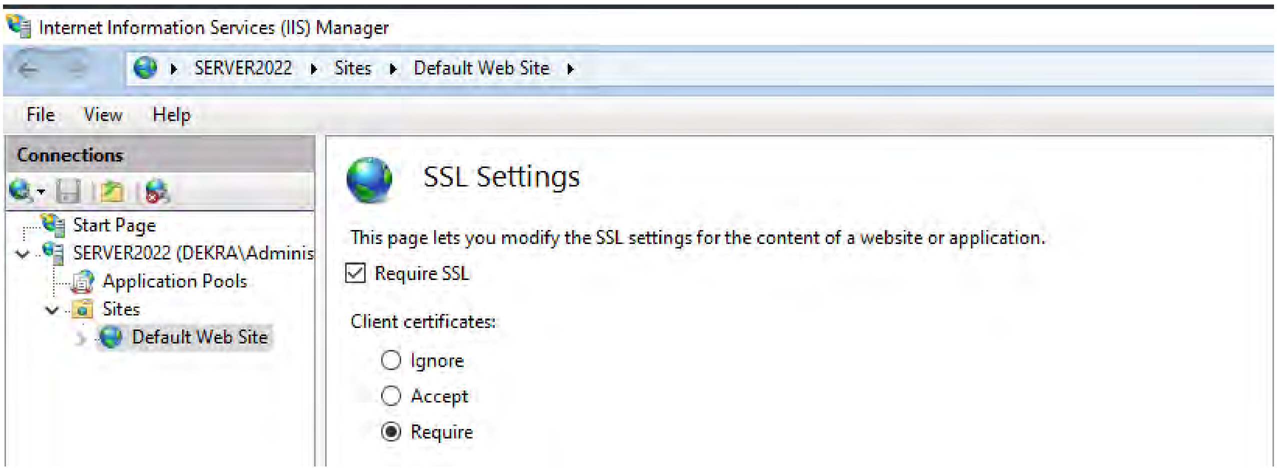
Certificate

General Details Certification Path

Certification path
dekra-CA
server2022.dekra.lab

Certificate status:
This certificate is OK.

- On the middle “Features View” panel, double-click “SSL Settings”.
- Check “Require SSL” and select “Require” client certificates. Then click “Apply” on the right panel.



Internet Information Services (IIS) Manager

SERVER2022 ▸ Sites ▸ Default Web Site ▸

SSL Settings

This page lets you modify the SSL settings for the content of a website or application.

☑ Require SSL

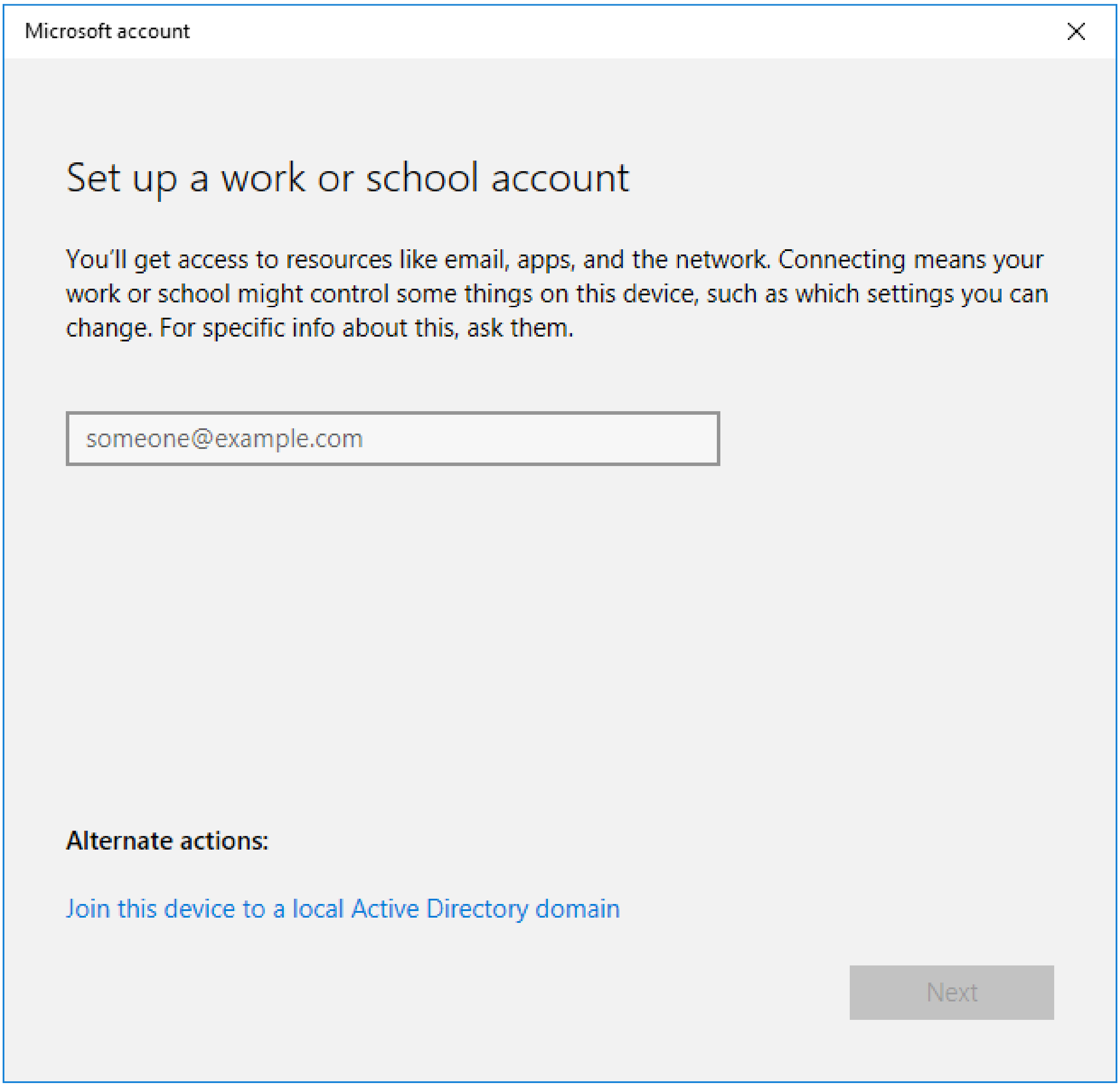
Client certificates:

○ Ignore
○ Accept
● Require

The Client Machine needs to belong to the domain just created so that it can get a client certificate for authentication. In order to do so, follow the next steps:

- Ensure the DNS of the network adapter are set to the Server Machine’s IP.
- Right click on the “Windows” icon and click “System”.
- On the displayed “About” screen, click on “Connect to work or school”.

- On the “Microsoft Account” popup screen, select “Join this device to a local Active Directory domain” under “Alternate actions”.



Microsoft account

Set up a work or school account

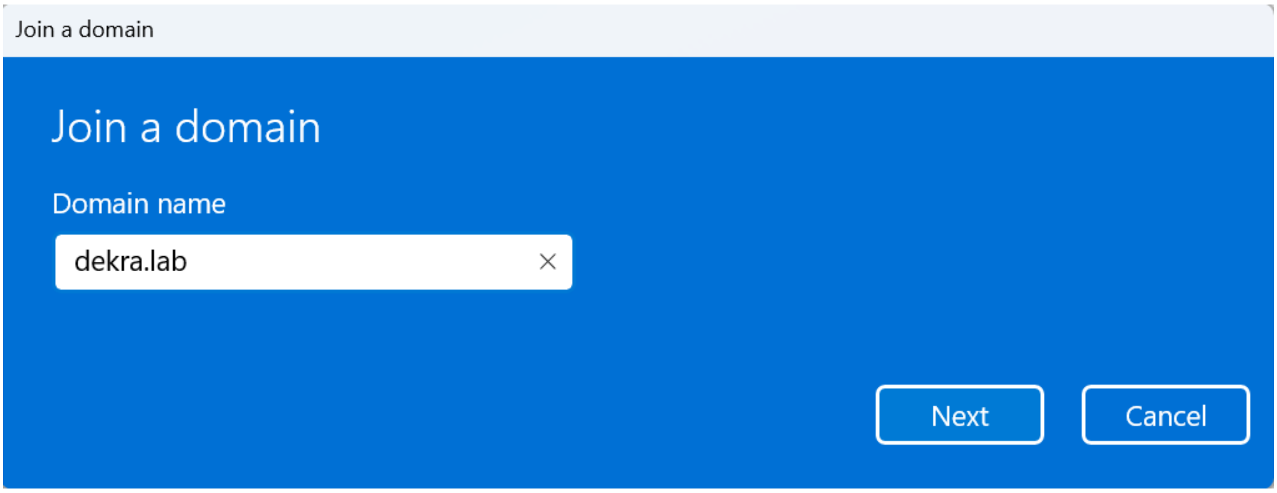
You’ll get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

someone@example.com

Alternate actions:

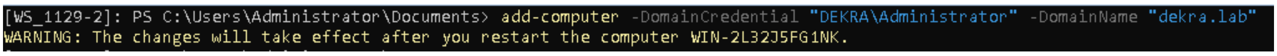
Join this device to a local Active Directory domain

- On the “Join a domain” popup screen, introduce the FQDN of the domain that was created (“dekra.lab” for this evaluation) and click next.



Domain name: dekra.lab

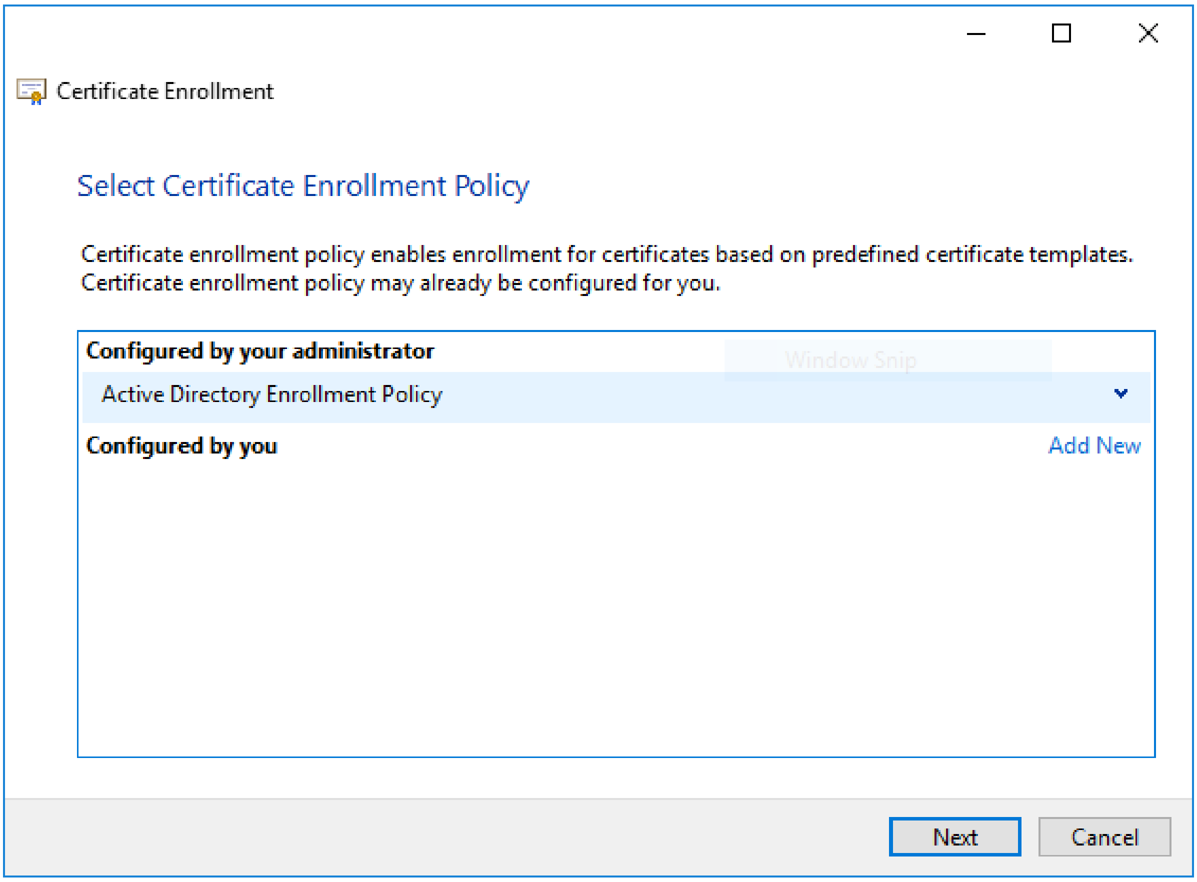
- Introduce the Administrator’s username and password.
- In the “Add an account” popup screen, click “Skip”.
- A system restart is required after the successful domain join.
- For Azure Stack HCIv2 run the following command in a PowerShell terminal.



```
[WS_1129-2]: PS C:\Users\Administrator\Documents> add-computer -DomainCredential "DEKRA\Administrator" -DomainName "dekra.lab"
WARNING: The changes will take effect after you restart the computer WIN-2L32J5FG1NK.
```

Once restarted, login as the domain user created previously (“DEKRA\jdoe” for this evaluation). The next steps shall be followed to request the client certificate from the certificate authority:

- Open “mmc.exe” (e.g. from WIN+R).
- Click on “File” -> “Add/Remove Snap-in...”.
- Select “Certificates” on the left panel and click “Add” and then “OK”.
- On the left panel, under “Certificates” right click on “Personal”, select “All Tasks” and then “Request new Certificate...”.
- Click “Next”.
- On the “Select Certificate Enrollment Policy” screen, select “Active Directory Enrollment Policy” and click “Next”.



Certificate Enrollment

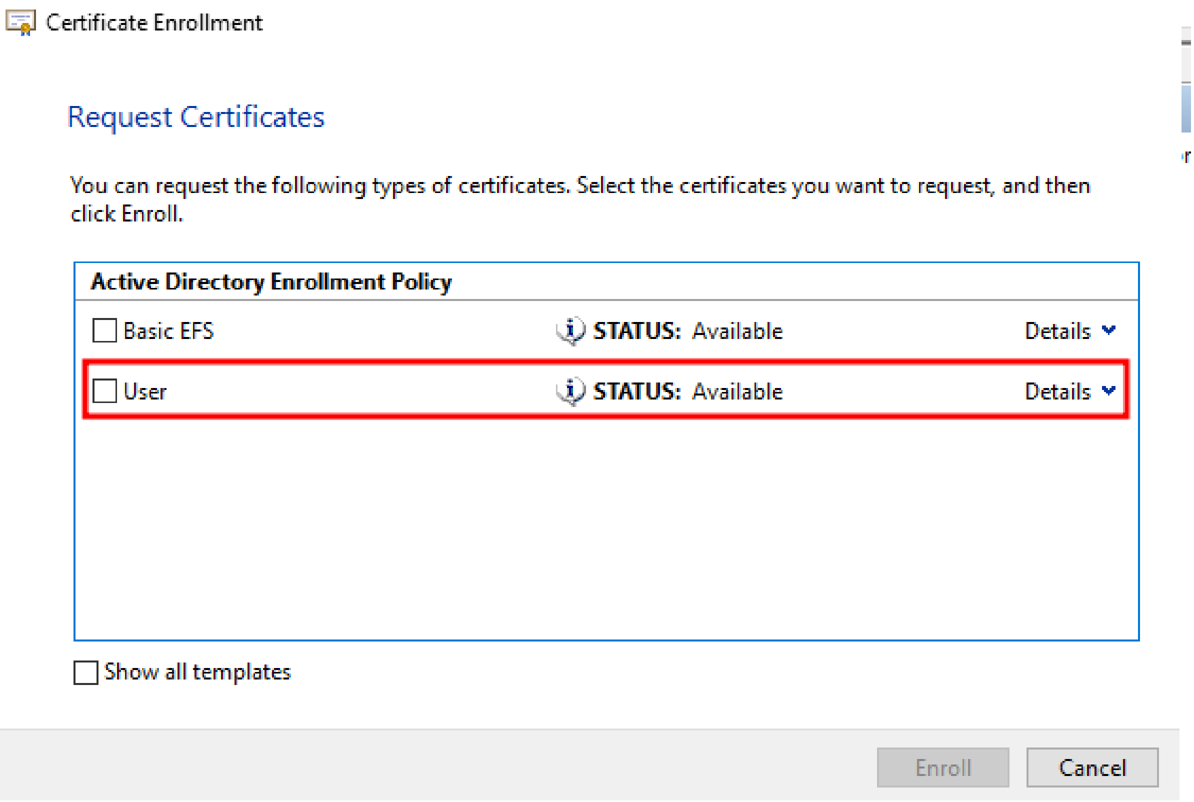
Select Certificate Enrollment Policy

Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

Configured by your administrator

Active Directory Enrollment Policy

Configured by you



Certificate Enrollment

Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

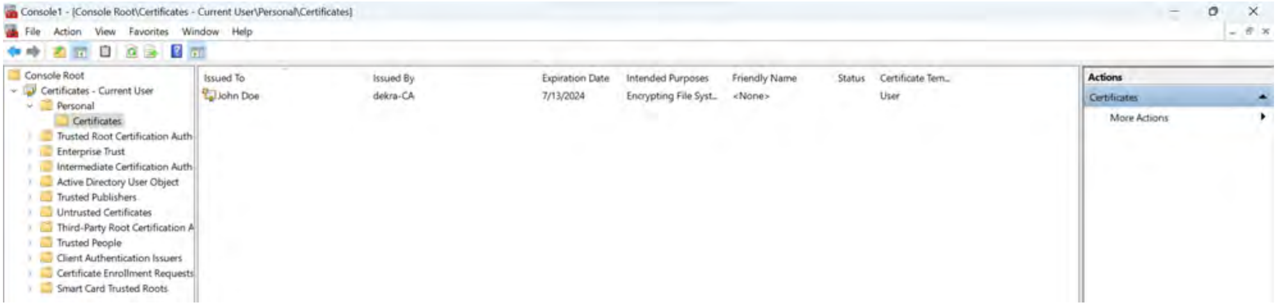
Active Directory Enrollment Policy

☐ Basic EFS **STATUS:** Available Details

☐ User **STATUS:** Available Details

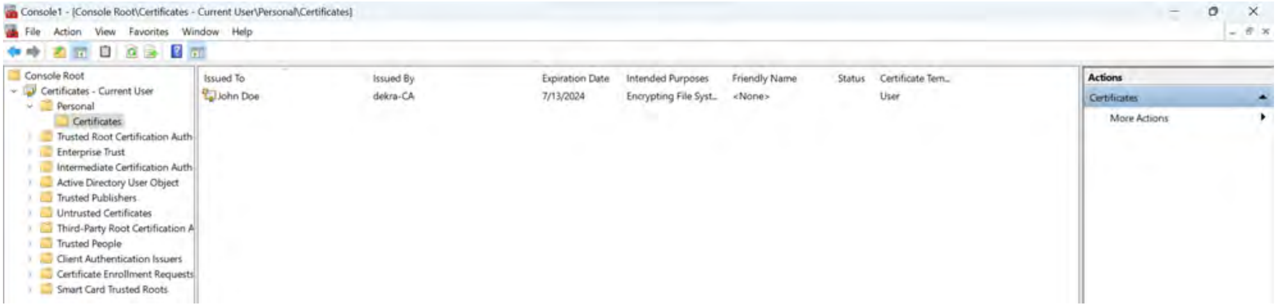
☐ Show all templates

- On the “Request Certificates” screen, check “User” and click “Enroll”.


Console1 - [Console Root\Certificates - Current User\Personal\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Auth
Enterprise Trust
Intermediate Certification Auth
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification A
Trusted People
Client Authentication Issuers
Certificate Enrollment Requests
Smart Card Trusted Roots
Actions
Certificates
More Actions

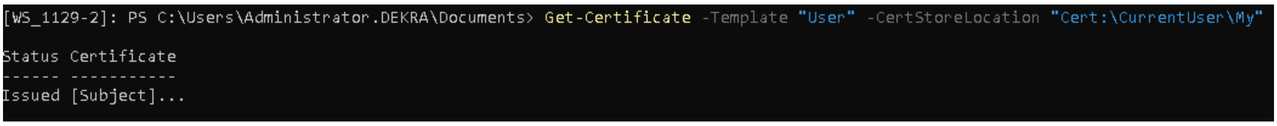
Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem...
John Doe	dekra-CA	7/13/2024	Encrypting File Syst...	<None>		User

- Once finished, the presence of the client certificate can be verified in “mmc.exe” if the “Certificates” section under “Personal” is refreshed.


Console1 - [Console Root\Certificates - Current User\Personal\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Certificates
Trusted Root Certification Auth
Enterprise Trust
Intermediate Certification Auth
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification A
Trusted People
Client Authentication Issuers
Certificate Enrollment Requests
Smart Card Trusted Roots
Actions
Certificates
More Actions

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem...
John Doe	dekra-CA	7/13/2024	Encrypting File Syst...	<None>		User

- For Azure Stack HCIv2 run the following command in a PowerShell terminal in order to perform the request of the user certificate.



```
[WS_1129-2]: PS C:\Users\Administrator.DEKRA\Documents> Get-Certificate -Template "User" -CertStoreLocation "Cert:\CurrentUser\My"

Status Certificate
------ -----------
Issued [Subject]...
```

50.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

50.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**.Additionally, the following supplementary platforms have been also tested:

- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)

- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)

- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

The evaluator has obtained the same results for all the tested platforms. (*Windows 10, Windows 11 and Windows Server and Azure platforms*.)

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

50.2.1.4 Verdict

According to the results presented in the previous section, the evaluator considers that the test results obtained during the **Test 1** activity demonstrate the fulfilment of the requirements established in the assurance activity section. Therefore, the **PASS** verdict is assigned to the **Test 1** activity.

50.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to this FTP_ITC_EXT.1.1(TLS).

51 FTP_TRP.1.1

The assurance activity for the **FTP_TRP.1.1** requirement is stated as follows:

> The evaluator will examine the TSS to determine that the methods of remote OS administration are indicated, along with how those communications are protected. The evaluator will also confirm that all protocols listed in the TSS in support of OS administration are consistent with those specified in the requirement, and are included in the requirements in the ST. The evaluator will confirm that the operational guidance contains instructions for establishing the remote administrative sessions for each supported method. The evaluator will also perform the following tests:
>
> - **Test 1:** The evaluator will ensure that communications using each remote administration method is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful.
> - **Test 2:** For each method of remote administration supported, the evaluator will follow the operational guidance to ensure that there is no available interface that can be used by a remote user to establish a remote administrative sessions without invoking the trusted path.
> - **Test 3:** The evaluator will ensure, for each method of remote administration, the channel data is not sent in plaintext.
> - **Test 4:** The evaluator will ensure, for each method of remote administration, modification of the channel data is detected by the OS.

51.1 Documentation Review Activity

51.1.1 Findings

Section **6.9 Trusted Channels** of the ***Security Target*** document describes the protections used for the *TLS* and *HTTPS* communications. Moreover, there is a pointer to the section **6.2.3.1 TLS, HTTPS, DTLS, EAP-TLS** where the description of how the communications are protected is located.

This section also describes the offered remote access methods, which are the following:

- Remote Desktop Services.
- Connect to another computer using Remote Desktop Connection.
- PowerShell Remoting for Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions.

Finally, the ***Operational Guidance*** document, includes in section **2.4 Remote Administration** the necessary steps to establish a *Remote Desktop Connection* and in section **2.4.4 Remote administration using PowerShell remoting** the steps to configure and secure the PowerShell Remoting communications.

51.1.2 Verdict

The evaluator has found in the TSS the methods used for the remote access and the protocols used to protect the connection.

In addition, the evaluator has checked the ***Operational Guidance*** document, includes information for establishing the remote administrative sessions for each supported method listed in the ***Security Target*** document.

The evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfilment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

51.2 Test Activity

51.2.1 Test 1 & Test 3

The evaluator will ensure that communications using Remote Administration methods are successful. In addition, for each method of remote administration, the data is not sent in plain text.

51.2.1.1 Setup

On all the platforms, except the ones with Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions as operating system, the Remote Administration method is the Remote Desktop Connection. The necessary scenario to perform the tests over this method is described in the assurance activity section and it is composed by the following elements:

- Server Machine (Windows Server 2019)
- Client Machine (Platforms listed in the ST)

These machines are in the same network.

On the platforms with Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions, the remote administration method is *PowerShell Remoting*.

For these platforms, the scenario needed to perform the tests is the following:

- Server Machine (Platforms listed in the ST)
- Client Machine (Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge)

51.2.1.1.1 Remote Desktop Administration (Windows 10 & 11)

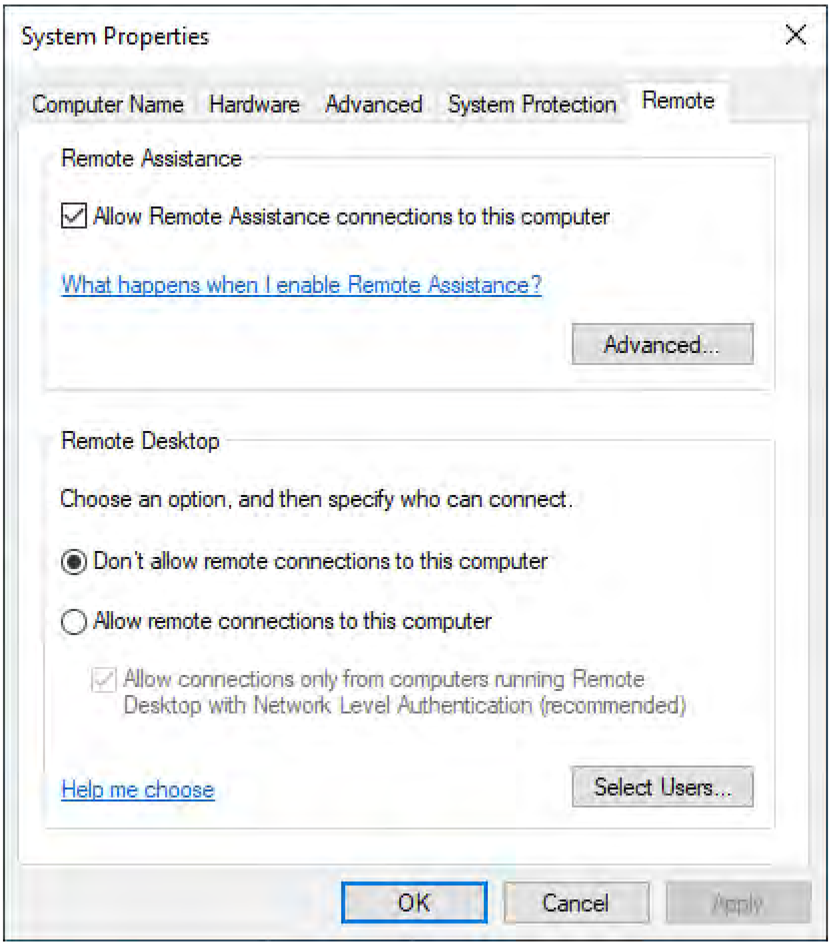
To be able to use the Remote Administration, the following steps shall be performed in the Server Machine.

- Go to Server Manager application, click *Manage* then, *Add Roles and Features*.
- Click on *Next*.
- Select *Role-based or feature-based installation* and click on *Next*.
- Mark the checkbox with the option: *Select a server from the server pool* and choose the server with the IP of the Server Machine and click on *Next*.
- Select *Remote Desktop Services*. Press *Add features* and click on *Next*.
- Click on *Next*.
- Press *Install*.

In the client machine, the remote administration shall be allowed.

- Go to *System Properties* (*WIN + r, then type 'sysdm.cpl'*).
- In the *Remote* tab, under the *RemoteDesktop* section, select the '*Allow remote connections to this computer*' checkbox.

51.2.1.1.2 Windows 10 platforms:



System Properties

Remote Assistance

☑ Allow Remote Assistance connections to this computer

What happens when I enable Remote Assistance?

Remote Desktop

Choose an option, and then specify who can connect.

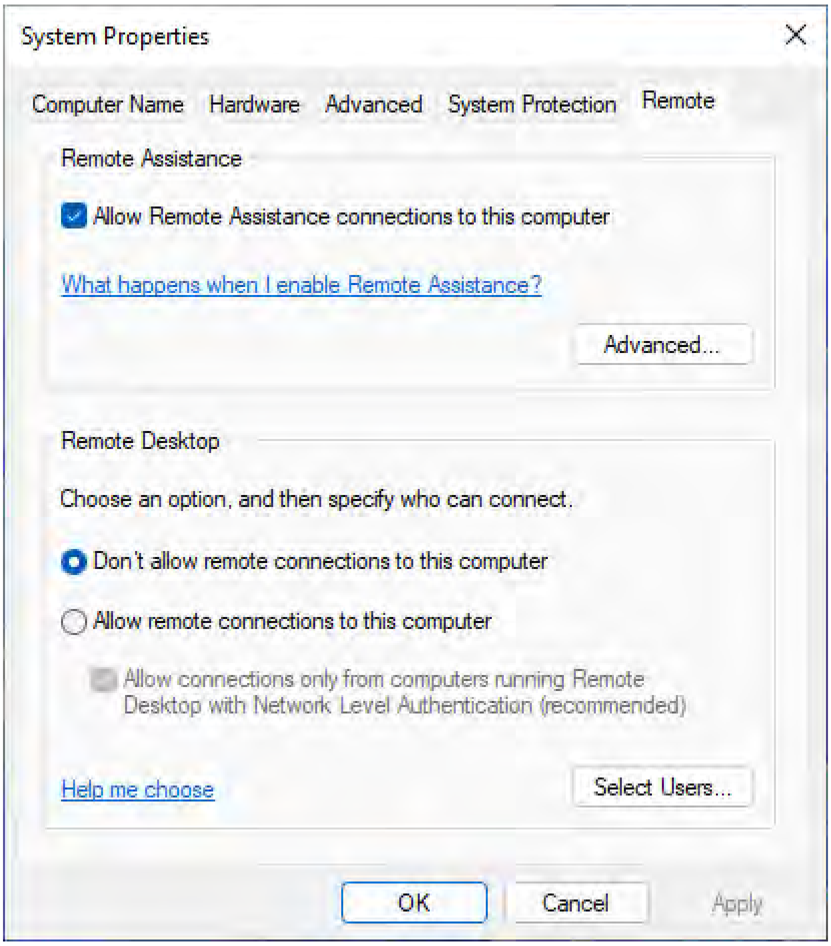
● Don't allow remote connections to this computer

○ Allow remote connections to this computer

☑ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)

Help me choose

51.2.1.1.3 Windows 11 platforms:



System Properties

Remote Assistance

☑ Allow Remote Assistance connections to this computer

What happens when I enable Remote Assistance?

Remote Desktop

Choose an option, and then specify who can connect.

● Don't allow remote connections to this computer

○ Allow remote connections to this computer

☑ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)

Help me choose

To record the establishment of the remote administration connection, the Server Machine shall have a network packet analyzer application installed (e.g. *Wireshark*).

The Client Machine shall have enabled the secure configuration according to the section 3 of the ***Operational Guidance***. In addition, a network packet analyzer application shall be also installed.

51.2.1.1.4 PowerShell Remoting (Windows Server & Azure)

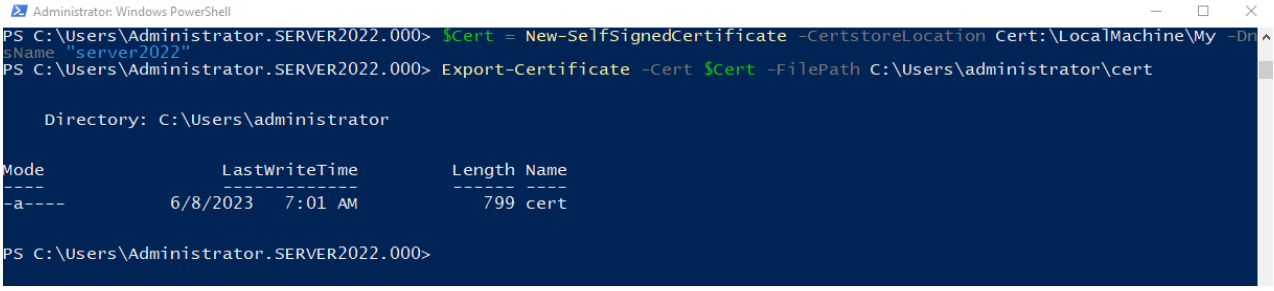
For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions, the setup scenario is the following:

To be able to use *PowerShell Remoting*, the following steps shall be performed in the Server Machine.

- Open a *PowerShell* terminal. A certificate should be generated in the server machine and then exported. Execute the following commands as shown in the image below:

```
$Cert = New-SelfSignedCertificate -CertstoreLocation Cert:\LocalMachine\My
-DnsName “<remote computer>”
```

Export-Certificate -Cert $Cert -FilePath C:\Users\administrator\cert



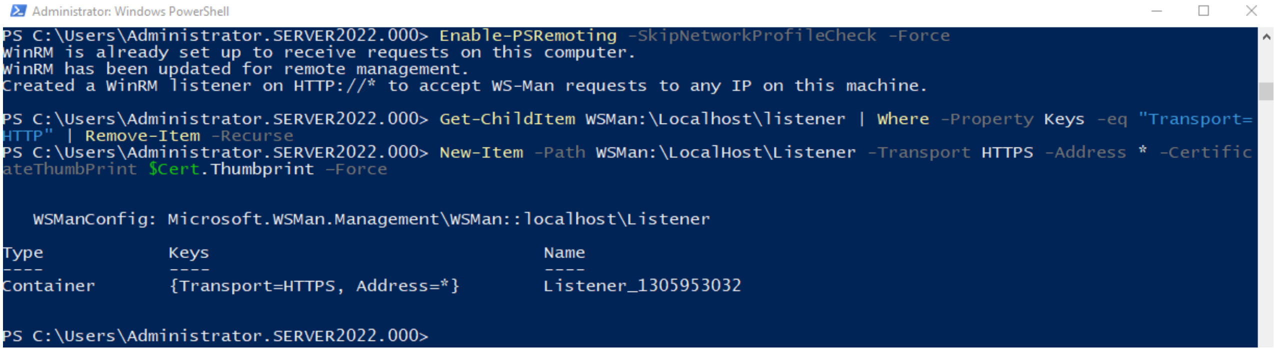
```
PS C:\Users\Administrator.SERVER2022.000> $Cert = New-SelfSignedCertificate -CertstoreLocation Cert:\LocalMachine\My -Dn
sName "server2022"
PS C:\Users\Administrator.SERVER2022.000> Export-Certificate -Cert $Cert -FilePath C:\Users\administrator\cert


    Directory: C:\Users\administrator


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          6/8/2023   7:01 AM            799 cert


PS C:\Users\Administrator.SERVER2022.000>
```

- Open a Command Line terminal (*cmd*), where a listener should be configured with the certificate signature and the local server machine IP. To ensure that *Powershell* does not use HTTP to connect to the computer and only uses HTTPS, the following commands shall be executed:

  Enable-PSRemoting -SkipNetworkProfileCheck -Force

  Get-ChildItem WSMan:\Localhost\listener | Where -Property Keys -eq “Transport=HTTP” | Remove-Item -Recurse

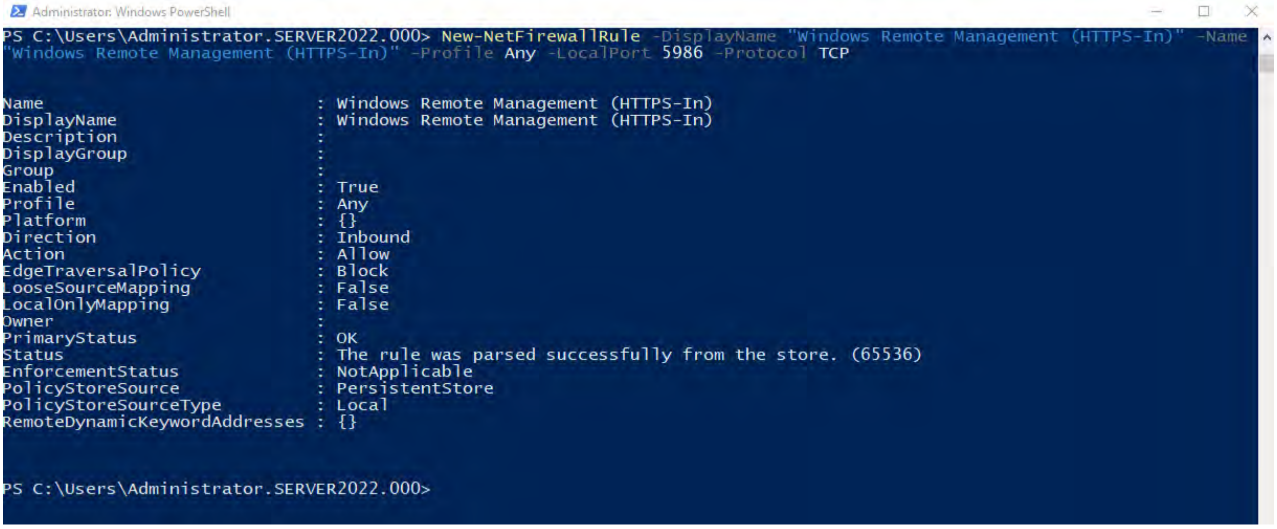
  New-Item -Path WSMan:\LocalHost\Listener -Transport HTTPS -Address * -CertificateThumbPrint $Cert.Thumbprint –Force



```
PS C:\Users\Administrator.SERVER2022.000> Enable-PSRemoting -SkipNetworkProfileCheck -Force
WinRM is already set up to receive requests on this computer.
WinRM has been updated for remote management.
Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.

PS C:\Users\Administrator.SERVER2022.000> Get-ChildItem WSMan:\Localhost\listener | Where -Property Keys -eq "Transport=
HTTP" | Remove-Item -Recurse
PS C:\Users\Administrator.SERVER2022.000> New-Item -Path WSMan:\LocalHost\Listener -Transport HTTPS -Address * -Certific
ateThumbPrint $Cert.Thumbprint -Force


   WSManConfig: Microsoft.WSMan.Management\WSMan::localhost\Listener

Type            Keys                                Name
----            ----                                ----
Container       {Transport=HTTPS, Address=*}        Listener_1305953032


PS C:\Users\Administrator.SERVER2022.000>
```

- Finally, create a firewall rule by executing the command shown in the following image. The firewall will be configured to accept the remote connections:

  New-NetFirewallRule -DisplayName “Windows Remote Management (HTTPS-In)” -Name “Windows Remote Management (HTTPS-In)” -Profile Any -LocalPort 5986 -Protocol TCP



```
PS C:\Users\Administrator.SERVER2022.000> New-NetFirewallRule -DisplayName "Windows Remote Management (HTTPS-In)" -Name
"Windows Remote Management (HTTPS-In)" -Profile Any -LocalPort 5986 -Protocol TCP


Name                          : Windows Remote Management (HTTPS-In)
DisplayName                   : Windows Remote Management (HTTPS-In)
Description                   :
DisplayGroup                  :
Group                         :
Enabled                       : True
Profile                       : Any
Platform                      : {}
Direction                     : Inbound
Action                        : Allow
EdgeTraversalPolicy           : Block
LooseSourceMapping            : False
LocalOnlyMapping              : False
Owner                         :
PrimaryStatus                 : OK
Status                        : The rule was parsed successfully from the store. (65536)
EnforcementStatus             : NotApplicable
PolicyStoreSource             : PersistentStore
PolicyStoreSourceType         : Local
RemoteDynamicKeywordAddresses : {}



PS C:\Users\Administrator.SERVER2022.000>
```

51.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

51.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)

- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)

- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

51.2.1.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 1** and **Test 3** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1** and **Test 3**.

51.2.2 Test 2

The evaluator will ensure that following the ***Operational Guidance*** document, there is no available interface that can be used by a remote user to establish a remote administrative sessions without invoking the trusted path.

51.2.2.1 Setup

The machines used to perform this test shall have enabled the secure configuration according to the section **3. Evaluated configuration** of the ***Operational Guidance*** document.

51.2.2.2 Procedure

The procedure for this test is identically the same as previously defined for test 1 & test 3.

51.2.2.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)

- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)

- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

51.2.2.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 2** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 2**.

51.2.3 Test 4

The evaluator will ensure that any modification done to the channel data is detected by the OS and the connection is refused.

51.2.3.1 Setup

The Remote Administration methods available are the *Remote Desktop Connection* and *PowerShell Remoting*. The necessary scenario to perform the tests described in the assurance activities of the Protection Profile is composed by the following elements:

- Server Machine (Windows Server 2022)
- Client Machine (Platforms listed in the ST)
- MITM Machine (Debian 9)

These machines are in the same network.

51.2.3.1.1 Remote Desktop Administration (Windows 10 & 11)

The applicable setup for this test is the same as the one defined for *Test 1 & 3*.

51.2.3.1.2 PowerShell Remoting (Windows Server & Azure)

The applicable setup for this test is the same as the one defined for *Test 1 & 3*.

To perform this test, a MITM Machine shall be used. This machine shall be between the Server Machine and the Client Machine, acting as a switch and modifying the packets that match with certain patterns (depending the remote administration method used).

- Remote Desktop Connection:

```
{
    "debuglevel":1,
    "patterns":[
        {
            "match":{
                "bpf":"tcp port 3389",
                "regex":".*\\x17\\x03\\x03.*"
            },
    "replacement":{
        "regex":"(\\x17\\x03\\x03.{2})(.{3})",
        "replacement":"$1\\x44\\x54\\x43"
        }
    }
    ]
}
```

- PowerShell remoting:

```
{
    "debuglevel":1,
    "patterns":[
        {
            "match":{
                "bpf":"tcp port 5986",
                "regex":".*\\x17\\x03\\x03.*"
            },
    "replacement":{
        "regex":"(\\x17\\x03\\x03.{2})(.{3})",
        "replacement":"$1\\x44\\x54\\x43"
        }
    }
]
}
```

51.2.3.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [GPOSPP421] instructions in order to collect the results as stipulated by the protection profile [GPOSPP421].

51.2.3.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)

- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)

- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

The evaluator has obtained the same results for all the tested platforms.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

51.2.3.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 4** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 4**.

51.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FPT_TRP.1.1.

52 FAU_GEN.1/WLAN

The assurance activity for the **FAU_GEN.1/WLAN** requirement is stated as follows:

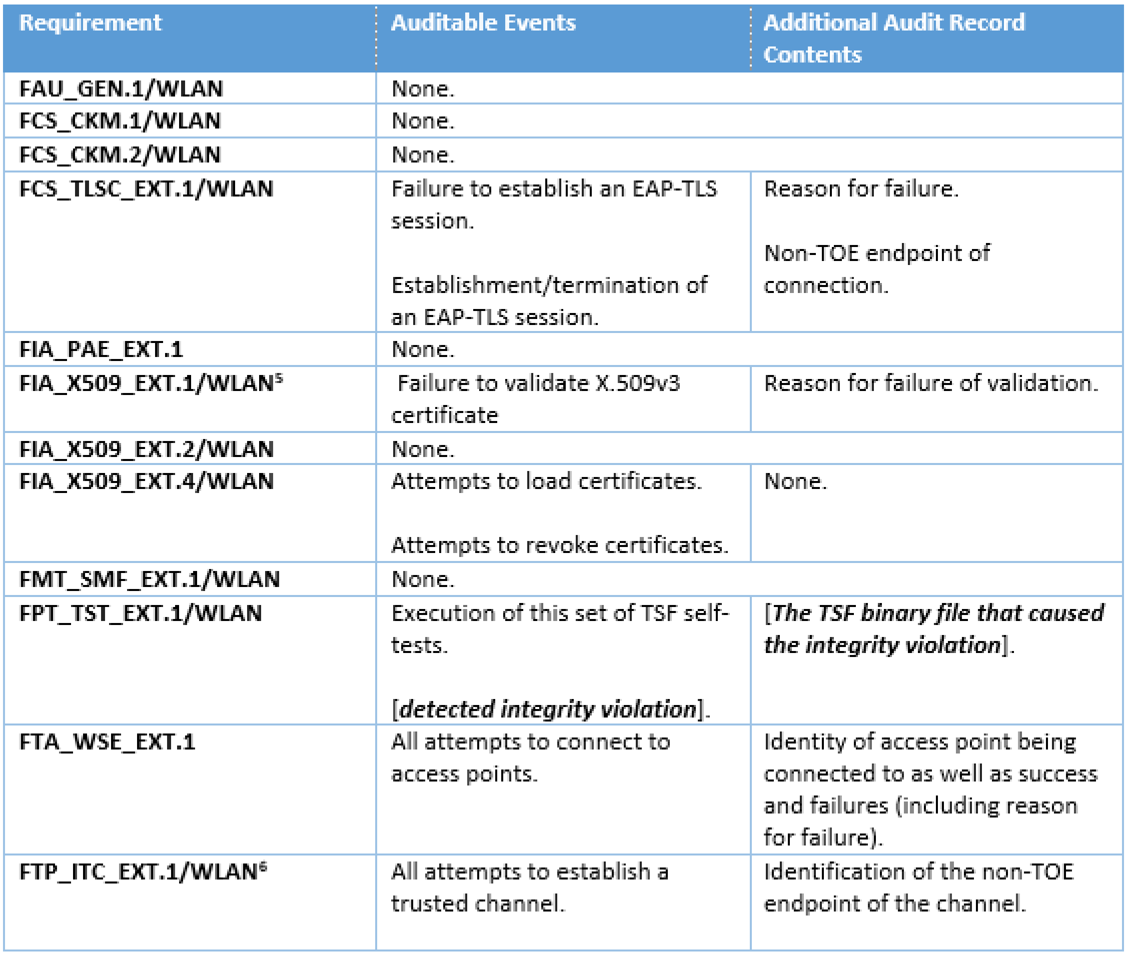
> The evaluator shall check the operational guidance and ensure that it lists all of the auditable events and provides a format for audit records. Each audit record format type must be covered, along with a brief description of each field. The evaluator shall check to make sure that every audit event type mandated by the EP is described and that the description of the fields contains the information required in FAU_GEN.1.2, and the additional information specified in Table 2.
>
> The evaluator shall in particular ensure that the operational guidance is clear in relation to the contents for failed cryptographic events. In Table 2, information detailing the cryptographic mode of operation and a name or identifier for the object being encrypted is required. The evaluator shall ensure that name or identifier is sufficient to allow an administrator reviewing the audit log to determine the context of the cryptographic operation (for example, performed during a key negotiation exchange, performed when encrypting data for transit) as well as the non-TOE endpoint of the connection for cryptographic failures relating to communications with other IT systems.
>
> The evaluator shall also make a determination of the administrative actions that are relevant in the context of this EP. The TOE may contain functionality that is not evaluated in the context of this EP because the functionality is not specified in an SFR. This functionality may have administrative aspects that are described in the operational guidance. Since such administrative actions will not be performed in an evaluated configuration of the TOE, the evaluator shall examine the operational guidance and make a determination of which administrative commands, including subcommands, scripts, and configuration files, are related to the configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the EP, which thus form the set of "all administrative actions". The evaluator may perform this activity as part of the activities associated with ensuring the AGD_OPE guidance satisfies the requirements.
>
> - **Test 1:** The evaluator shall test the TOE's ability to correctly generate audit records by having the TOE generate audit records in accordance with the assurance activities associated with the functional requirements in this EP. When verifying the test results, the evaluator shall ensure the audit records generated during testing match the format specified in the administrative guide, and that the fields in each audit record have the proper entries.
>
> Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly. For example, testing performed to ensure that the administrative guidance provided is correct verifies that AGD_OPE.1 is

satisfied and should address the invocation of the administrative actions that are needed to verify the audit records are generated as expected.

52.1 Documentation Review activity

52.1.1 Findings

The ***Security Target*** document, defines in its section **5.1.1.1 Audit Data Generation(FAU_GEN.1) and FAU_GEN.1(WLAN)**, the following auditable events:



Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1/WLAN	None.	
FCS_CKM.1/WLAN	None.	
FCS_CKM.2/WLAN	None.	
FCS_TLSC_EXT.1/WLAN	Failure to establish an EAP-TLS session. Establishment/termination of an EAP-TLS session.	Reason for failure. Non-TOE endpoint of connection.
FIA_PAE_EXT.1	None.	
FIA_X509_EXT.1/WLAN[5]	Failure to validate X.509v3 certificate	Reason for failure of validation.
FIA_X509_EXT.2/WLAN	None.	
FIA_X509_EXT.4/WLAN	Attempts to load certificates. Attempts to revoke certificates.	None.
FMT_SMF_EXT.1/WLAN	None.	
FPT_TST_EXT.1/WLAN	Execution of this set of TSF self-tests. [***detected integrity violation***].	[***The TSF binary file that caused the integrity violation***].
FTA_WSE_EXT.1	All attempts to connect to access points.	Identity of access point being connected to as well as success and failures (including reason for failure).
FTP_ITC_EXT.1/WLAN[6]	All attempts to establish a trusted channel.	Identification of the non-TOE endpoint of the channel.

Moreover, the evaluator has reviewed the section **5.1 Audit events by scenario** of the ***Operational Guidance***, where it is included a table with all the events related to the WLAN client extended package requirements implemented by the TOE. The content of this table matches with the selection performed by the vendor in the ***Security Target*** document as it can be seen in the image above.

52.1.2 Verdict

The evaluator has reviewed the ***Security Target*** document and has ensured that every auditable event type selected in the ***Security Target*** document is included in the ***Operational Guidance*** document.

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfilment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

52.2 Test Activity

52.2.1 Test 1

For this case, all the auditable events will be obtained during the test execution of each security functional requirement.

52.2.1.1 Setup

The necessary setup for obtaining each auditable event will be described in the *Setup* section of the requirements shown in the above table.

52.2.1.2 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)

For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions editions, the wireless extended profile has not been tested because is out of the scope.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

52.2.1.3 Verdict

As the result above states, the related events have been correctly generated and they include all the information defined in the ***Security Target*** document.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

52.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FAU_GEN.1/WLAN.

53 FCS_CKM.1/WPA & FCS_CKM.2/WLAN

The assurance activity for the **FCS_CKM.1/WPA & FCS_CKM.2/WLAN** requirement is stated as follows:

> The evaluator shall verify that the TSS describes how the primitives defined and implemented by this EP are used by the TOE in establishing and maintaining secure connectivity to the wireless clients.
>
> The TSS shall also provide a description of the developer's method(s) of assuring that their implementation conforms to the cryptographic standards; this includes not only testing done by the developing organization, but also any third-party testing that is performed.:
>
> - **Test 1:** The evaluator shall configure the access point so the cryptoperiod of the session key is 1 hour. The evaluator shall successfully connect the TOE to the access point and maintain the connection for a length of time that is greater than the configured cryptoperiod. The evaluator shall use a packet capture tool to determine that after the configured cryptoperiod, a re-negotiation is initiated to establish a new session key. Finally, the evaluator shall determine that the renegotiation has been successful and the client continues communication with the access point.
> - **Test 2:** The evaluator shall perform the following test using a packet sniffing tool to collect frames between the TOE and a wireless LAN access point:
>   - Step 1: The evaluator shall configure the access point to an unused channel and configure the WLAN sniffer to sniff only on that channel (i.e., lock the sniffer on the selected channel). The sniffer should also be configured to filter on the MAC address of the TOE and/or access point.
>   - Step 2: The evaluator shall configure the TOE to communicate with a WLAN access point using IEEE 802.11-2012 and a 256-bit (64 hex values 0-f) pre-shared key. The pre-shared key is only used for testing.
>   - Step 3: The evaluator shall start the sniffing tool, initiate a connection between the TOE and the access point, and allow the TOE to authenticate, associate, and successfully complete the 4 way handshake with the client.
>   - Step 4: The evaluator shall set a timer for 1 minute, at the end of which the evaluator shall disconnect the TOE from the wireless network and stop the sniffer.
>   - Step 5: The evaluator shall identify the 4-way handshake frames (denoted EAPOL-key in Wireshark captures) and derive the PTK from the 4-way handshake frames and pre-shared key as specified in IEEE 802.11-2012.

- Step 6: The evaluator shall select the first data frame from the captured packets that was sent between the TOE and access point after the 4-way handshake successfully completed, and without the frame control value 0x4208 (the first 2 bytes are 08 42). The evaluator shall use the PTK to decrypt the data portion of the packet as specified in IEEE 802.11-2012, and shall verify that the decrypted data contains ASCII-readable text.
- Step 7: The evaluator shall repeat Step 6 for the next 2 data frames between the TOE and access point and without frame control value 0x4208.

53.1 Documentation Review activity

53.1.1 Findings

The evaluator has reviewed the section **6.2.3.2 Wireless Networking** of the ***Security Target*** document. This section states that Windows can use PRF-384 to generate AES 128-bit keys or PRF-704 to generate AES 256-bit keys using Windows RBG. In addition to this, it states that Windows complies with the IEE 802.11-2012 and IEE 802.11ac-2013 standards and is able to interoperate with devices that implement the standard. All the evaluated platforms count with certificates from the Wi-Fi alliance that provides compliance for FIPS-Approved algorithms, like the *AES-CCMP*, *AES-CCMP-256* and *AES-GCMP-256*, as selected for the FCS_COP.1 requirement.

The “model number” shown in the Wi-Fi Alliance certificates is used to identify the product. This varies from vendor to vendor based on their business. Some vendors will have different label for product and model number while others use the same for both. Microsoft uses either the name of the device or the name of the adapter on the device for its certified devices.

As specified in the Wi-Fi Test Suite Version 10.9.0, document, which is a software platform developed by the Wi-Fi Alliance to support certification program development and device certification, the FIPS-Approved algorithms: *AES-CCMP*, *AES-CCMP-256* and *AES-GCMP-256* are thoroughly tested during the Wi-Fi Alliance certification process.

Finally, according to section **6.2.1 Cryptographic Algorithms and Operations** of the ***Security Target*** document, Windows shall be running in FIPS validated mode. In this mode, all used algorithms must be FIPS approved. The evaluator has followed instructions included in section **3.2.5 FIPS 140 Approved crip tography mode** of the ***Operational Guidance*** document for setting this mode.

53.1.2 Verdict

The evaluator considers that the TSS provides enough information related to what primitives are used to establishing and maintaining security in wireless connections. In addition to this, TSS provides information about FIPS and Wi-Fi certifications.

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfilment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

53.2 Test Activity

53.2.1 Test 1

The evaluator will attempt to verify that a re-negotiation to establish a new key exists after a defined cryptoperiod. In this case, a cryptoperiod of 1 minute for testing purposes will be used.

53.2.1.1 Setup

In this case, the evaluator has used the architecture defined for the *Setup* for *Test 1* in FMT_SMF_EXT.1/WLAN with the following elements and roles:

- Windows NPS Server (EAP-TLS)
- Windows Client using domain user (FIPS Enabled)
- AP WPA23/3-Enterprise mode
- Kali Linux (sniffing machine) using aircrack suite

53.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [PPMWLAN10] instructions in order to collect the results as stipulated by the protection profile [PPMWLAN10].

53.2.1.3 Results

The evaluator has performed this test in all the canonical platforms as defined in section: **8. Test environment definition**.

Additionally, the following supplementary platforms have been also tested:

- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)

The evaluator has obtained the same results for all the tested platforms.

For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions, the wireless extended profile has not been tested because is out of the scope.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

53.2.1.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

53.2.2 Test 2

The evaluator will attempt to capture data frames after after the 4-way handshake has been successfully completed. Using the PTK the evaluator will decrypt data frames in order to see ASCII-readable text.

53.2.2.1 Setup

In this case, an special configuration shall be configured as shown below:

- AP should be configured in WPA2 PSK mode.
- Client should connect to previously created network.
- Linux Sniffing machine with Aircrack suite installed.
- FCS_CKM_Test2.py python script shall be available.

53.2.2.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [PPMWLAN10] instructions in order to collect the results as stipulated by the protection profile [PPMWLAN10].

53.2.2.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

Additionally, the following supplementary platforms have been also tested:

- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)

The evaluator has obtained the same results for all the tested platforms.

For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions editions, the wireless extended profile has not been tested because is out of the scope.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

53.2.2.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 2** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 2**.

53.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FCS_CKM.1/WPA & FCS_CKM.2/WLAN.

54 FCS_TLSC_EXT.1/WLAN

The assurance activity for the **FCS_TLSC_EXT.1/WLAN** requirement is stated as follows:

> The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the ciphersuites supported are specified. The evaluator shall check the TSS to ensure that the ciphersuites specified include those listed for this component.
>
> The evaluator shall also check the operational guidance to ensure that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS.
>
> The evaluator shall also check the operational guidance to ensure that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS (for instance, the set of ciphersuites advertised by the TOE may have to be restricted to meet the requirements).
>
> The evaluator shall check that the OPE guidance contains instructions for the administrator to configure the list of Certificate Authorities that are allowed to sign certificates used by the authentication server that will be accepted by the TOE in the EAP-TLS exchange, and instructions on how to specify the algorithm suites that will be proposed and accepted by the TOE during the EAP-TLS exchange.
>
> The evaluator shall write, or the ST author shall provide, an application for the purposes of testing TLS.
>
> The evaluator shall also perform the following tests:
>
> - **Test 1**: The evaluator shall establish a TLS connection using each of the ciphersuites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of an EAP session. It is sufficient to observe the successful negotiation of a ciphersuite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic in an attempt to discern the ciphersuite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).
> - **Test 2**: The evaluator shall attempt to establish the connection using a server with a server certificate that contains the Server Authentication purpose in the extendedKeyUsage field and verify that a connection is established. The evaluator will then verify that the client rejects an otherwise valid server certificate that lacks the Server Authentication purpose in the extendedKeyUsage field and a connection is not established. Ideally, the two certificates should be identical except for the extendedKeyUsage field.
> - **Test 3**: The evaluator shall send a server certificate in the TLS connection that does not match the server-selected ciphersuite (for example, send

a ECDSA certificate while using the TLS_RSA_WITH_AES_128_CBC_SHA ciphersuite or send a RSA certificate while using one of the ECDSA ciphersuites.) The evaluator shall verify that the TOE disconnects after receiving the server's Certificate handshake message.

- **Test 4**: The evaluator shall configure the server to select the TLS_NULL_WITH_NULL_NULL ciphersuite and verify that the client denies the connection.
- **Test 5**: The evaluator shall perform the following modifications to the traffic:
  - Change the TLS version selected by the server in the Server Hello to a non- supported TLS version (for example 1.3 represented by the two bytes 03 04) and verify that the client rejects the connection.
  - Modify at least one byte in the server's nonce in the Server Hello handshake message, and verify that the client rejects the Server Key Exchange handshake message (if using a DHE or ECDHE ciphersuite) or that the server denies the client's Finished handshake message.
  - Modify the server's selected ciphersuite in the Server Hello handshake message to be a ciphersuite not presented in the Client Hello handshake message. The evaluator shall verify that the client rejects the connection after receiving the Server Hello.
  - **[conditional]** If DHE or ECDHE cipher suites are supported, modify the signature block in the Server's Key Exchange handshake message and verify that the client does not complete the handshake and no application data flows. This test does not apply to cipher suites using RSA key exchange. If a TOE only supports RSA key exchange in conjuction with TLS, then this test shall be omitted.
  - Modify a byte in the Server Finished handshake message, and verify that the client sends a fatal alert upon receipt and does not send any application data.
  - Send a garbled message from the Server after the Server has issued the ChangeCipherSpec message and verify that the client denies the connection.

54.1 Documentation Review activity

54.1.1 Findings

The evaluator has reviewed the section **4.3.3 Available EAP-TLS ciphersuites** of the ***Operational Guidance*** document. This section states that Windows can use different ciphersuites including among others those requested:

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246

- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5430

  Complete set of TLS cipher suites implemented can be found here: Cipher Suites in TLS/SSL (Schannel SSP)

These cipher suites match with the selected ones in the requirement definition. The cipher suites listed above are a subset of the ones implemented in the Schannel library, as it can be checked in the previous URL.

In addition, sections **4.3.4 Configuring with MDM**, **4.3.5 Configuring with PowerShell** and **4.3.6 Configuring with group policy** of the ***Operational Guidance*** document describes how to configure these TLS cipher suites. In addition to this, the information can be found in the following MSDN link included in the ***Operational Guidance***: How to restrict the use of certain cryptographic algorithms and protocols in Schannel.dll

Selection of TLS cipher suites in the TLS handshake process is performed according to the order defined which can be configured as described in the links listed above.

54.1.2 Verdict

The evaluator considers that the TSS provides enough information related to what cipher suites are available.

The ***Operational Guidance*** includes information regarding how to configure correctly the TOE for testing purposes including ciphersuite selection and associated restrictions.

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfilment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

54.2 Test Activity

54.2.1 Test 1

The evaluator will attempt to force the client to use the following ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5430

54.2.1.1 Setup

In this case, the evaluator will use the general NPS architecture composed by the following elements:

- Windows NPS Server (EAP-TLS)
- Windows Client using domain user (FIPS Enabled)
- AP WPA2/3-Enterprise mode
- Windows-EAP-TLS profile added in the TOE.
- FCS_TLSC_EXT.1_Server.ps1

54.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [PPMWLAN10] instructions in order to collect the results as stipulated by the protection profile [PPMWLAN10].

54.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Panasonic CF-33 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)

The evaluator has obtained the same results for all the tested platforms.

For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions editions, the wireless extended profile has not been tested because is out of the scope.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE’s behavior is as expected and detailed in the security target [ST004].

54.2.1.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

54.2.2 Test 2

The evaluator will attempt to establish a connection with a server providing a valid server certificate containing Server Authentication Purpose. Then, the evaluator will use a valid server certificate without Server Authentication purpose and will verify that the connection is not established.

54.2.2.1 Setup

In this case, the evaluator will use the general NPS architecture composed by the following elements:

- Windows NPS Server (EAP-TLS)
- CA Template with KeyPurposeId "email replication"
- Windows Client using domain user (FIPS Enabled)
- AP WPA2/3-Enterprise mode

54.2.2.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [PPMWLAN10] instructions in order to collect the results as stipulated by the protection profile [PPMWLAN10].

54.2.2.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Panasonic CF-33 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)

The evaluator has obtained the same results for all the tested platforms.

For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions editions, the wireless extended profile has not been tested because is out of the scope.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

54.2.2.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfillment of the **Test 2** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 2**.

54.2.3 Test 3

The evaluator will attempt to establish a server ciphersuite that does not match with the server certificate by modifying packets in real time.

54.2.3.1 Setup

In this case, the evaluator will use the general NPS architecture composed by the following elements:

- Windows NPS Server (EAP-TLS) with ADCS
- Windows Client using domain user (FIPS Enabled)
- AP WPA2/3-Enterprise mode

For modifying packets, the following Rehtse configuration file will be used:

```
{
    "debuglevel":1,
    "patterns":[
        {
            "match":{
                "bpf":"udp port 1812",
                "regex":".*\\xc0\\x23.*"
            },
            "replacement":{
                "regex":"\\xc0\\x24",
                "replacement":"\\x00\\x2f"
            }
        }
    ]
}
```

This snippet will change default server ciphersuite from TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc02) to TLS_RSA_WITH_AES_128_CBC_SHA (0x002f).

54.2.3.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [PPMWLAN10] instructions in order to collect the results as stipulated by the protection profile [PPMWLAN10].

54.2.3.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test envionment definition**.

Additionally, the following supplementary platforms have been also tested:

- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)

The evaluator has obtained the same results for all the tested platforms.

For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions editions, the wireless extended profile has not been tested because is out of the scope.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

54.2.3.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 3** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 3**.

54.2.4 Test 4

The evaluator will configure the server forcing it to use TLS_NULL_WITH_NULL_NULL ciphersuite and will verify that TOE rejects the connection.

54.2.4.1 Setup

In this case, the evaluator will use the general NPS architecture composed by the following elements:

- Windows NPS Server (EAP-TLS)
- Windows Client using domain user (FIPS Enabled)
- AP WPA2/3-Enterprise mode

For modifying packets, the following Rehtse configuration file will be used:

```
{
    "debuglevel":1,
    "patterns":[
        {
            "match":{
                "bpf":"udp port 1812",
                "regex":".*\\xc0\\x23.*"
            },
            "replacement":{
                "regex":"\\xc0\\x23",
                "replacement":"\\x00\\x00"
            }
        }
    ]
}
```

54.2.4.2 Procedure

The procedure is the same as defined in **Test 3**.

54.2.4.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test envionment definition**.

Additionally, the following supplementary platforms have been also tested:

- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)

The evaluator has obtained the same results for all the tested platforms.

For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions editions, the wireless extended profile has not been tested because is out of the scope.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

54.2.4.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 4** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 4**.

54.2.5 Test 5

The evaluator will perform the following modifications by using MITM tool:

- Change the TLS version to an unsupported version
- Modify server nonce in Server Hello
- Modify Server finished handshake
- Send a garbled message after ChangeCipherSpec Message

54.2.5.1 Setup

In this case, the evaluator will use the general NPS architecture composed by the following elements:

- Windows NPS Server (EAP-TLS) with ADCS
- Windows Client using domain user (FIPS Enabled)
- AP WPA2-Enterprise mode

In order to force the server to perform traffic modifications, the evaluator will use Rehtse tool with different configurations for each test.

54.2.5.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [PPMWLAN10] instructions in order to collect the results as stipulated by the protection profile [PPMWLAN10].

54.2.5.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

Additionally, the following supplementary platforms have been also tested:

- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)

The evaluator has obtained the same results for all the tested platforms.

For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions editions, the wireless extended profile has not been tested because is out of the scope.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

54.2.5.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 5** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 5**.

54.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FCS_TLSC_EXT.1/WLAN.

55 FCS_TLSC_EXT.2/WLAN

The assurance activity for the **FCS_TLSC_EXT.2/WLAN** requirement is stated as follows:

> The evaluator shall verify that the TSS describes the supported Elliptic Curves Extension and whether the required behavior is performed by default or may be configured.
>
> If the TSS indicates that the supported Elliptic Curves Extension must be configured to meet the requirement, the evaluator shall verify that the operational guidance includes instructions on configuration of the supported Elliptic Curves Extension.
>
> The evaluator shall perform the following test:
>
> **Test 1**: The evaluator shall configure a server to perform ECDHE key exchange using each of the TOE's supported curves and shall verify that the TOE successfully connects to the server.

55.1 Documentation Review activity

55.1.1 Findings

The evaluator has reviewed the section **4.3.3 Available EAP-TLS ciphersuites** of the ***Operational Guidance*** document. This section states that Windows can use different Elliptic Curves ciphersuites including among others those requested:

- secp256r1
- secp384r1
- secp521r1

Complete set of TLS cipher suites implemented can be found here: Cipher Suites in TLS/SSL (Schannel SSP)

These cipher suites match with the selected ones in the requirement definition. The Cipher suites listed above are a subset of the ones implemented in the Schannel library, as it can be checked in the previous URL.

55.1.2 Verdict

The evaluator considers that the TSS provides enough information related to what Elliptic Curves cipher suites are available.

The ***Operational Guidance*** document includes information regarding how to configure correctly the TOE for testing purposes including ciphersuite selection and associated restrictions.

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfilment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

55.2 Test Activity

55.2.1 Test 1

The evaluator will attempt to force the client to use the following ciphersuites:

- secp256r1
- secp384r1
- secp521r1

55.2.1.1 Setup

In this case, the general NPS architecture composed by the following elements is used:

- Windows NPS Server (EAP-TLS) with Active Directory Certificate Authority (ADCS)
- Windows Client using domain user (FIPS Enabled)
- AP WPA2-Enterprise mode
- W10WLANServerAutomator.ps1
- deploy_client.ps1
- client_out_domain.ps1

55.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [PPMWLAN10] instructions in order to collect the results as stipulated by the protection profile [PPMWLAN10].

55.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

Additionally, the following supplementary platforms have been also tested:

- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)

The evaluator has obtained the same results for all the tested platforms.

For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions editions, the wireless extended profile has not been tested because is out of the scope.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

55.2.1.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

55.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FCS_TLSC_EXT.2/WLAN.

56 FCS_WPA_EXT.1/WLAN

The assurance activity for the **FCS_WPA_EXT.1/WLAN** requirement is stated as follows:

> The evaluator shall examine the TSS to determine that it defines the TSF shall support WPA3 and WPA2 security type.
>
> The WLAN client can support connecting to networks of other security types (e.g., open); however, those will not be tested as part of this evaluation and FMT_SMF.1 will ensure that the client can be configured to only connect to WPA3 and, if selected WPA2, networks.
>
> - **Test 1:** The evaluator configures the AP to allow a connection to a wireless network with a specific SSID with the security type WPA3. The evaluator will attempt to connect to the network. Once the TOE is connected, the SSID security type shall be modified and the TOE could not connect.

56.1 Documentation Review activity

56.1.1 Findings

The evaluator has reviewed the section **6.7 TOE Access** of the ***Security Target*** document, which describes that administrator can specify which Wi-Fi networks (SSID) a TOE may be connected to.

Also, the ***Operational Guidance*** document includes in its section **4.5 Managing network connections** instructions for configuring allowed Wi-Fi networks.

This information has allowed the evaluator to design a testing plan, which will be used during the test activity.

56.1.2 Verdict

The evaluator considers that, the findings obtained during the documentation review activity demonstrate the fullfilment of the requirements established in the assurance activity section. Hence, the PASS verdict is assigned to the documentation review activity.

56.2 Test Activity

56.2.1 Test 1

The evaluator will use SSID: PSK and will block access to PSK modifying the security type into the AP. Then, the evaluator will check that it is not possible to connect to the PSK SSID.

56.2.1.1 Setup

In this case, the evaluator has used the general NPS architecture with the following elements and roles:

- Windows NPS Server (EAP-TLS)
- Windows Client using domain user (FIPS Enabled)
- AP WPA2/3-Enterprise mode
- Kali Linux (sniffing machine)
- PSK profile is loaded into the client.

56.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [PPMWLAN10] instructions in order to collect the results as stipulated by the protection profile [PPMWLAN10].

56.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8.Test environment definition**.

Additionally, the followings supplementary platforms have been also tested:

- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)

For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions editions, the wireless extended profile has not been tested because is out of the scope.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

56.2.1.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

56.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FCS_WPA_EXT.1/WLAN.

57 FIA_PAE_EXT.1/WLAN

The assurance activity for the **FIA_PAE_EXT.1/WLAN** requirement is stated as follows:

> The evaluator shall perform the following tests:
>
> - **Test 1:** The evaluator shall demonstrate that the TOE has no access to the test network. After successfully authenticating with an authentication server through a wireless access system, the evaluator shall demonstrate that the TOE does have access to the test network communication with the access point.
> - **Test 2:** The evaluator shall demonstrate that the TOE has no access to the test network. The evaluator shall attempt to authenticate using an invalid client certificate, such that the EAP-TLS negotiation fails. This should result in the TOE still being unable to access the test network.
> - **Test 3:** The evaluator shall demonstrate that the TOE has no access to the test network. The evaluator shall attempt to authenticate using an invalid authentication server certificate, such that the EAP-TLS negotiation fails. This should result in the TOE still being unable to access the test network.

57.1 Documentation Review activity

57.1.1 Findings

The related assurance activity does not define any action for this requirement.

57.1.2 Verdict

The related assurance activity does not define any action for this requirement. Therefore, the **PASS** verdict is assigned to the documentation review activity.

57.2 Test Activity

57.2.1 Test 1

The evaluator will attempt to verify that once connected, the TOE has access to the test network.

57.2.1.1 Setup

In this case, the evaluator has used the general NPS architecture with the following elements:

- Windows NPS Server (EAP-TLS)
- Windows Client using domain user (FIPS Enabled)
- AP WPA2/3-Enterprise mode
- Kali Linux (sniffing machine)

57.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [PPMWLAN10] instructions in order to collect the results as stipulated by the protection profile [PPMWLAN10].

57.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8.Test environment definition**.

Additionally, the followings supplementary platforms have been also tested:

- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions editions, the wireless extended profile has not been tested because is out of the scope.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

57.2.1.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

57.2.2 Test 2

The evaluator will attempt to connect to the test network using a revoked certificate.

57.2.2.1 Setup

In this case, the evaluator has used the general NPS architecture with the following elements:

- Windows NPS Server (EAP-TLS)
- Windows Client using domain user (FIPS Enabled)
- AP WPA2-Enterprise mode
- Kali Linux (sniffing machine)

57.2.2.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [PPMWLAN10] instructions in order to collect the results as stipulated by the protection profile [PPMWLAN10].

57.2.2.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**.

Additionally, the followings supplementary platforms have been also tested:

- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions editions, the wireless extended profile has not been tested because is out of the scope.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

57.2.2.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 2** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 2**.

57.2.3 Test 3

The evaluator will attempt to connect to the test network using an invalid CA server certificate.

57.2.3.1 Setup

In this case, the evaluator has used the general NPS architecture with the following elements:

- Windows NPS Server (EAP-TLS)
- Windows Client using domain user (FIPS Enabled)
- AP WPA2/3-Enterprise mode
- Debian 9 (sniffing machine)

57.2.3.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [PPMWLAN10] instructions in order to collect the results as stipulated by the protection profile [PPMWLAN10].

57.2.3.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8. Test environment definition**.

Additionally, the followings supplementary platforms have been also tested:

- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions editions, the wireless extended profile has not been tested because is out of the scope.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

57.2.3.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfillment of the **Test 3** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 3**.

57.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FIA_PAE_EXT.1/WLAN.

58 FIA_X509_EXT.1/WLAN

The assurance activity for the **FIA_X509_EXT.1/WLAN** requirement is stated as follows:

> The evaluator shall examine the TSS to determine that it describes all certificate stores implemented that contain certificates used to meet the requirements of this EP. This description shall contain information pertaining to how certificates are loaded into the store, and how the store is protected from unauthorized access.
>
> The tests described must be performed in conjunction with the other Certificate Services assurance activities. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. The evaluator shall create a chain of at least four certificates: the node certificate to be tested, two Intermediate CAs, and the self-signed Root CA.
>
> - **Test 1:** The evaluator shall then load a certificate or certificates to the Trust Anchor Database needed to validate the certificate to be used in the function (e.g. application validation), and demonstrate that the function succeeds. The evaluator then shall delete one of the certificates, and show that the function fails.
> - **Test 2:** The evaluator shall demonstrate that validating an expired certificate results in the function failing.
> - **Test 3:** The evaluator shall construct a certificate path, such that the certificate of the CA issuing the TOE's certificate does not contain the basicConstraints extension. The validation of the certificate path fails.
> - **Test 4:** The evaluator shall construct a certificate path, such that the certificate of the CA issuing the TOE's certificate has the CA flag in the basicConstraints extension not set. The validation of the certificate path fails.
> - **Test 5:** The evaluator shall modify version v3 of the certificate and demonstrate that the certificate fails to validate (the certificate will fail to parse correctly).
> - **Test 6:** The evaluator shall modify cA: True value of the certificate and demonstrate that the certificate fails to validate (the signature on the certificate will not validate).

58.1 Documentation Review activity

58.1.1 Findings

The evaluator has reviewed the section **6.4.2 Certificate Storage** of the ***Security Target***, where it is stated that each user has their own certificate store and there is a certificate store for computer account. Certificate store is managed by access control policy in Windows and only authorized administrator (like local administrator) can add or remove entries.

58.1.2 Verdict

The related assurance activity does not define any action for this requirement. Therefore, the **PASS** verdict is assigned to the documentation review activity.

58.2 Test Activity

58.2.1 Test 1

In this test, user certificates are derived from CA root certificate. The evaluator will load the generated certificate into Certificate Store in order to probe that authentication between client and NPS server success.

58.2.1.1 Setup

In this test, the evaluator will use the general NPS architecture composed by the following elements:

- Windows NPS Server (EAP-TLS)
- Windows Client using domain user (FIPS Enabled)
- AP WPA2-Enterprise mode
- W10WLANClientAutomator.ps1
- W10WLANServerAutomator.ps1

58.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [PPMWLAN10] instructions in order to collect the results as stipulated by the protection profile [PPMWLAN10].

58.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8.Test environment definition**.

Additionally, the following supplementary platforms have been also tested:

- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions editions, the wireless extended profile has not been tested because is out of the scope.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

58.2.1.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfillment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

58.2.2 Test 2

This test shall prove that a the connection fails when a expired certificate is used to authenticated against NPS server.

58.2.2.1 Setup

In this test, the evaluator will use the general NPS architecture composed by the following elements:

- Windows NPS Server (EAP-TLS)
- Windows Client using domain user (FIPS Enabled)
- AP WPA2-Enterprise mode

58.2.2.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [PPMWLAN10] instructions in order to collect the results as stipulated by the protection profile [PPMWLAN10].

58.2.2.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8.Test environment definition**.

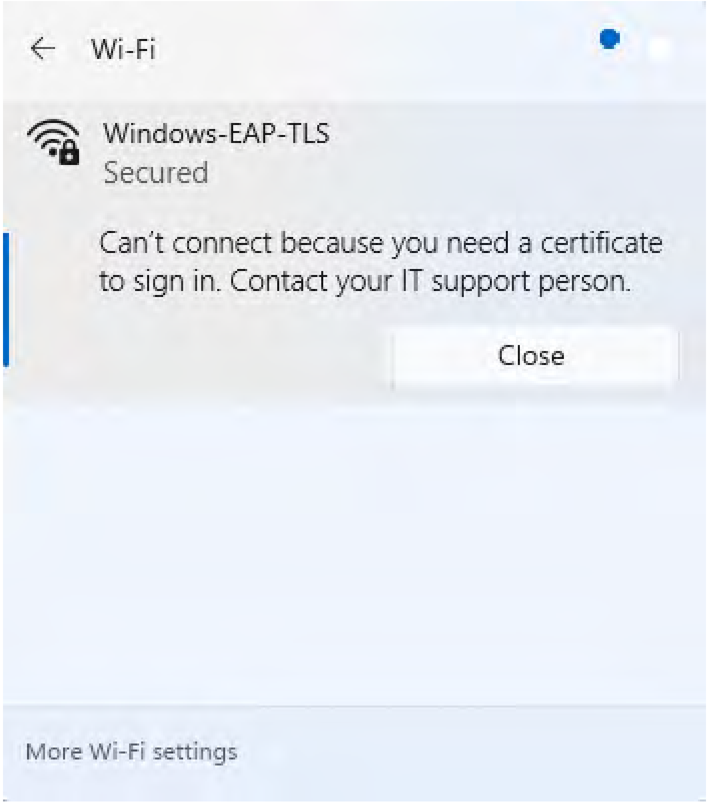
Additionally, the following supplementary platforms have been also tested:

- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions editions, the wireless extended profile has not been tested because is out of the scope.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

58.2.2.3.1 Windows 10 and 11 platforms:



Windows-EAP-TLS
Secured

Can't connect because you need a certificate to sign in. Contact your IT support person.

58.2.2.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfillment of the **Test 2** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 2**.

58.2.3 Test 3

This test prove that a connection against NPS server is not established when the Certification Authority, which issued the certificates, doesn't contain "basicConstraints" extension.

58.2.3.1 Setup

In this test, the evaluator will use the general NPS architecture composed by the following elements:

- Windows NPS Server (EAP-TLS)
- Windows Client using domain user (FIPS Enabled)
- AP WPA2/3-Enterprise mode

58.2.3.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [PPMWLAN10] instructions in order to collect the results as stipulated by the protection profile [PPMWLAN10].

58.2.3.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8.Test environment definition**.

Additionally, the following supplementary platforms have been also tested:

- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions editions, the wireless extended profile has not been tested because is out of the scope.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

58.2.3.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfillment of the **Test 3** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 3**.

58.2.4 Test 4

This test prove that a connection against NPS server is not established when the Certification Authority's "basicConstraints" extension, which issued the certificates, is not set.

58.2.4.1 Setup

In this test, the evaluator will use the general NPS architecture composed by the following elements:

- Windows NPS Server (EAP-TLS)
- Windows Client using domain user (FIPS Enabled)
- AP WPA2/3-Enterprise mode

58.2.4.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [PPMWLAN10] instructions in order to collect the results as stipulated by the protection profile [PPMWLAN10].

58.2.4.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8.Test environment definition**.

Additionally, the following supplementary platforms have been also tested:

- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions editions, the wireless extended profile has not been tested because is out of the scope.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

58.2.4.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfillment of the **Test 4** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 4**.

58.2.5 Test 5

This test proves that connection is not established against NPS server when some byte of the eight first bytes of the certificate is altered.

58.2.5.1 Setup

In this test, the evaluator will use the general NPS architecture composed by the following elements:

- Windows NPS Server (EAP-TLS)
- Windows Client using domain user (FIPS Enabled)
- AP WPA2/3-Enterprise mode

In addition, Rehtse tool will be used for modifying network traffic between NPS server and TOE.

58.2.5.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [PPMWLAN10] instructions in order to collect the results as stipulated by the protection profile [PPMWLAN10].

58.2.5.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8.Test environment definition**.

Additionally, the following supplementary platforms have been also tested:

- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions editions, the wireless extended profile has not been tested because is out of the scope.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

58.2.5.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 5** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 5**.

58.2.6 Test 6

This test proves that connection is not established against NPS server when some byte of certificate signature algorithm is altered.

58.2.6.1 Setup

In this test, the evaluator will use the general NPS architecture composed by the following elements:

- Windows NPS Server (EAP-TLS)
- Windows Client using domain user (FIPS Enabled)
- AP WPA2/3-Enterprise mode

In addition, Rehtse tool will be used for modifying network traffic between NPS server and TOE.

58.2.6.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [PPMWLAN10] instructions in order to collect the results as stipulated by the protection profile [PPMWLAN10].

58.2.6.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8.Test environment definition**.

Additionally, the following supplementary platforms have been also tested:

- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions editions, the wireless extended profile has not been tested because is out of the scope.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

58.2.6.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfillment of the **Test 6** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 6**.

58.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FIA_X509_EXT.1/WLAN.

59 FIA_X509_EXT.2/WLAN

The assurance activity for the **FIA_X509_EXT.2** requirement is stated as follows:

> The evaluator shall check the TSS to ensure that it describes how the TOE chooses which certificates to use, and any necessary instructions in the administrative guidance for configuring the operating environment so that the TOE can use the certificates. The evaluator shall examine the TSS to confirm that it describes the behavior of the TOE when a connection cannot be established during the validity check of a certificate used in establishing a trusted channel. The evaluator shall verify that any distinctions between trusted channels are described. If the requirement that the administrator is able to specify the default action, then the evaluator shall ensure that the operational guidance contains instructions on how this configuration action is performed.
>
> The evaluator shall check the administrative guidance to ensure that it describes how the TOE chooses which certificates to use, and any necessary instructions for configuring the operating environment so that the TOE can use the certificates.
>
> The evaluator shall perform the following test for each trusted channel:
>
> - **Test 1:** The evaluator shall demonstrate using a valid certificate that requires certificate validation checking to be performed in at least some part by communicating with a non-TOE IT entity. The evaluator shall then manipulate the environment so that the TOE is unable to verify the validity of the certificate, and observe that the action selected in FIA_X509_EXT.2.2 is performed. If the selected action is administrator-configurable, then the evaluator shall follow the operational guidance to determine that all supported administrator-configurable options behave in their documented manner.

59.1 Documentation Review activity

59.1.1 Findings

The evaluator has reviewed the section **6.4.1 X.509 Certificate Validation and Generation** of the ***Security Target*** document.

According to section **6.4.1 X.509 Certificate Validation and Generation** and following the ***Operational Guidance***, all windows components user a common system subcomponent for certificate validation a described in RFC 5280 including all applicable usage constraints such as Client and Server Authentication.

In addition to this, regarding certificate validation procedure, if certificate validation fails, or if TOE is not able to check the validation status for a certificate, TOE will not establish a trusted network channel and will inform the user and seek their consent before establishing secure connection.

The evaluator has reviewed the Windows Administrative Guide section **4.2.3 Certificate validation and revocations checks** and specifically section **4.2.3.2 Configuring certificate validation for EAP-TLS**.

Administrator can configure certificate validation as described in Extensible Authentication Protocol (EAP) Settings for network Access in section Smart Card or other certificate properties configuration items: Extensible Authentication Protocol (EAP) Settings for Network Access

59.1.2 Verdict

The evaluator considers that the TSS and AGD provides enough information related to which certificates are used, determines if certificate validation is needed and the appropriate actions related to its acceptance.

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfilment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

59.2 Test Activity

59.2.1 Test 1

The evaluator will attempt to verify that when the TOE cannot verify the validity of the certificate, it will ask the user to explicitly accept it.

59.2.1.1 Setup

In this case, the evaluator has used the general NPS architecture with the following elements:

- Windows NPS Server (EAP-TLS)
- Windows Client using domain user (FIPS Enabled)
- AP WPA2-Enterprise mode
- Kali Linux (sniffing machine)

59.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, en-

suring compliance with the protection profile [PPMWLAN10] instructions in order to collect the results as stipulated by the protection profile [PPMWLAN10].

59.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8.Test environment definition**.

Additionally, the following supplementary platforms have been also tested:

- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions editions, the wireless extended profile has not been tested because is out of the scope.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

59.2.1.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

59.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FIA_X509_EXT.2/WLAN.

60 FIA_X509_EXT.6/X.509

The assurance activity for the **FIA_X509_EXT.6/X.509** requirement is stated as follows:

> The evaluator shall examine the TSS to determine that it describes all certificate stores implemented that contain certificates used to meet the requirements of this EP. This description shall contain information pertaining to how certificates are loaded into the store, and how the store is protected from unauthorized access.
>
> The evaluator shall perform the following tests for each function in the system that requires the use of certificates:
>
> - **Test 1:** The evaluator then shall delete one of the certificates, and show that the function fails.
> - **Test 2:** The evaluator shall then load a certificate or certificates needed to validate the certificate to be used in the function, and demonstrate that the function succeeds.

60.1 Documentation Review activity

60.1.1 Findings

The evaluator has reviewed the section **6.4.2 Certificate Storage** of the ***Security Target***, where it is stated that each user has their own certificate store and there is a certificate store for computer account. Certificate store is managed by access control policy in Windows and only authorized administrator (like local administrator) can add or remove entries.

60.1.2 Verdict

The evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfillment of the requirements established in the assurance activity section. Hence, the PASS verdict is assigned to the documentation review activity.

60.2 Test Activity

60.2.1 Test 1

In this case, a user *cert* belongs to the domain is logged in for this test. The user *cert* with no privileges should try to delete a CA imported in *Cert:\LocalMachine\Root*.

60.2.1.1 Setup

- FIA_X509_EXT.6.ps1 script is available in the TOE.
- CA *ca.cer* is available in the TOE.

60.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [PPMWLAN10] instructions in order to collect the results as stipulated by the protection profile [PPMWLAN10].

60.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8.Test environment definition**.

Additionally, the following supplementary platforms have been also tested:

- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions editions, the wireless extended profile has not been tested because is out of the scope.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

60.2.1.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfillment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

60.2.2 Test 2

In this case, a user *cert* belongs to the domain is logged in for this test. The user *cert* with no privileges should try to import a CA *ca.cer* in *Cert:\LocalMachine\Root*.

60.2.2.1 Setup

- FIA_X509_EXT.6.ps1 script is available in the TOE.

- CA *ca.cer* is available in the TOE.

60.2.2.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [PPMWLAN10] instructions in order to collect the results as stipulated by the protection profile [PPMWLAN10].

60.2.2.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8.Test environment definition**.

Additionally, the following supplementary platforms have been also tested:

- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions editions, the wireless extended profile has not been tested because is out of the scope.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

60.2.2.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfillment of the **Test 2** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 2**.

60.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FIA_X509_EXT.6/X.509.

61 FMT_SMF.1/WLAN

The assurance activity for the **FMT_SMF.1/WLAN** requirement is stated as follows:

> The evaluator shall check to make sure that every management function mandated by the EP is described in the operational guidance and that the description contains the information required to perform the management duties associated with the management function.
>
> The evaluator shall test the TOE's ability to provide the management functions by configuring the TOE and testing each option listed in the requirement above.
>
> Note that the testing here may be accomplished in conjunction with the testing of other requirements, such as FCS_TLSC_EXT and FTA_WSE_EXT.

61.1 Documentation Review activity

61.1.1 Findings

The evaluator has reviewed the Windows ***Operational Guidance*** document sections **4.5 Managing network connections** and **4.6 Managing personal hotspots**.

The evaluator has verified that every management function required is included in Administrative Guide and it provides information about how to properly configure them.

61.1.2 Verdict

The evaluator considers that the ***Operational Guidance*** provides enough information related to managements functions included in the EP.

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfilment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

61.2 Test Activity

61.2.1 Test 1

The evaluator will attempt to verify supported management functions required by the EP as described in the operational guidance.

61.2.1.1 Setup

To perform tests related for this Assurance Activity, a full simulation environment for WPA2/WPA3 Enterprise based on Microsoft Radius Server Implementation (Network Policy Server) should be deployed.

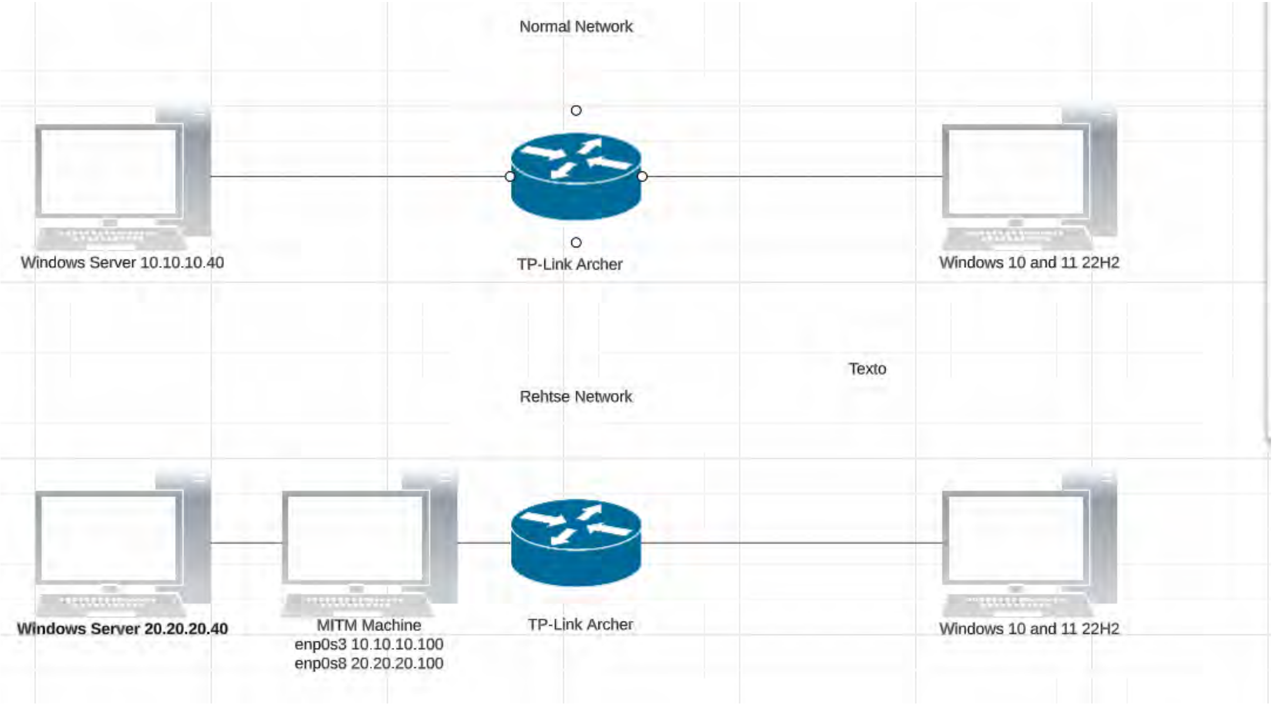
The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Server Machine acting as Active Directory Domain Controller, Root Certificate Authority, Web Server and Network Policy and Access Services.
- Wi-Fi Client Machine (Windows 10 and Windows 11 (22H2))
- MITM / Wi-Fi Sniffer with two physical network interfaces and a Wi-Fi interface.
- TP-Link Access Point
- TLS Debian server

All devices are in different networks with the following configuration:

- Server Machine, IP = 10.10.10.40 or 20.20.20.40 in Rehtse network.
- Client Machine, IP = 10.10.10.*
- Access Point, IP = 10.10.10.1
- TLS Debian server, IP = 10.10.10.12
- Sniffer Machine, IP-1 = 10.10.10.100 IP-2 = 20.20.20.100

Final configuration of full environment is as follows:



61.2.1.1.1 Server Machine Configuration

The server machine shall have at least the following roles enabled: Active Directory Domain Services, Active Directory Certificate Services and Network Policy and Access Services. These roles should be installed in correct order as described below.

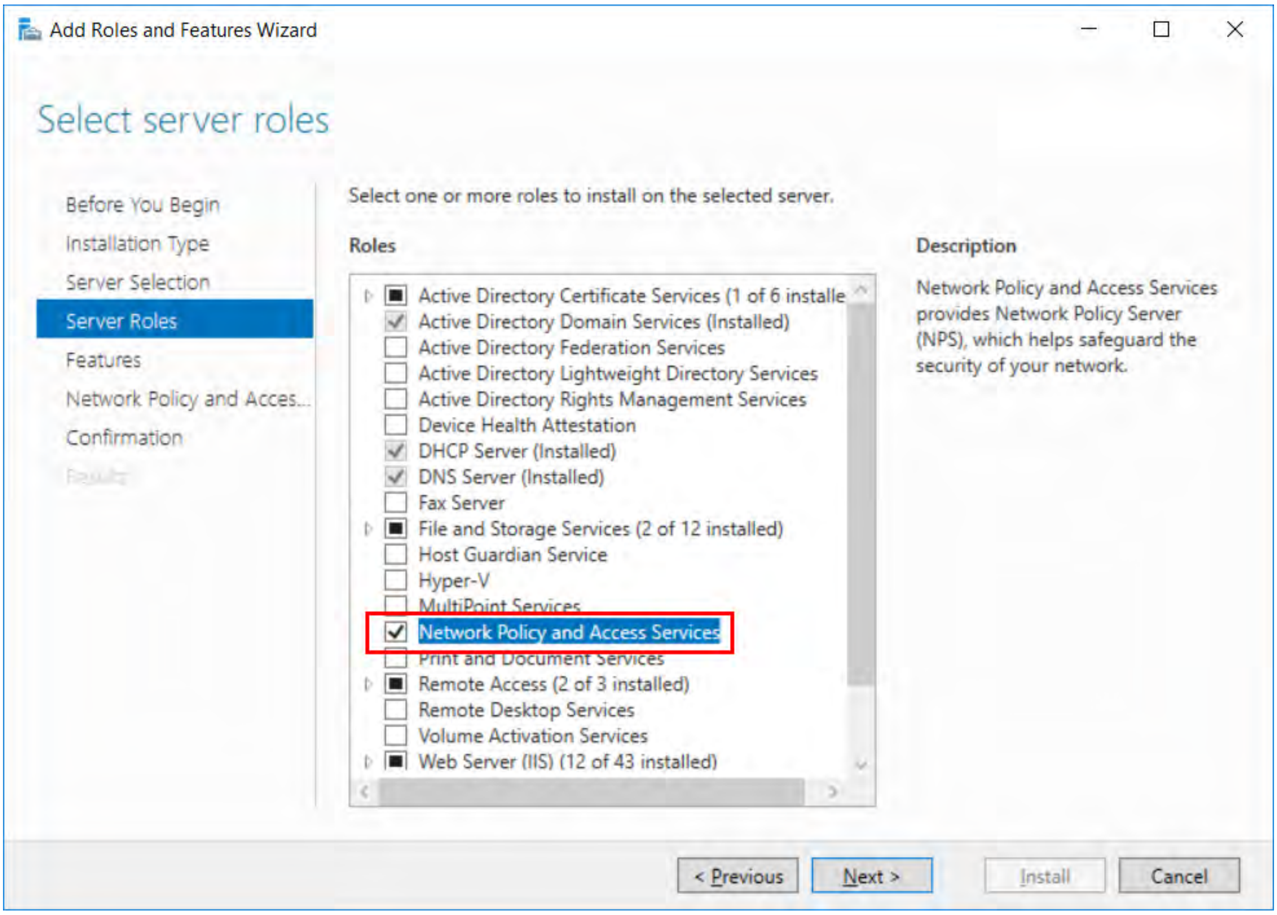
Active Directory Domain Services and Active Directory Certificate Services

The setup can be found in FTP_ITC_EXT .1.1(TLS).

Network Policy and Access Services

Network Policy and Access Services shall be installed and configured following the next steps:

- Open the Server Manager form the task bar.
- From the Server Manager Dashboard select "Manage" and then "Add Roles and Features".
- Click next until the "Select server roles" screen, then select "Network Policy and Access Services" and click "Next", accepting the suggested additional features.



Select server roles

Select one or more roles to install on the selected server.

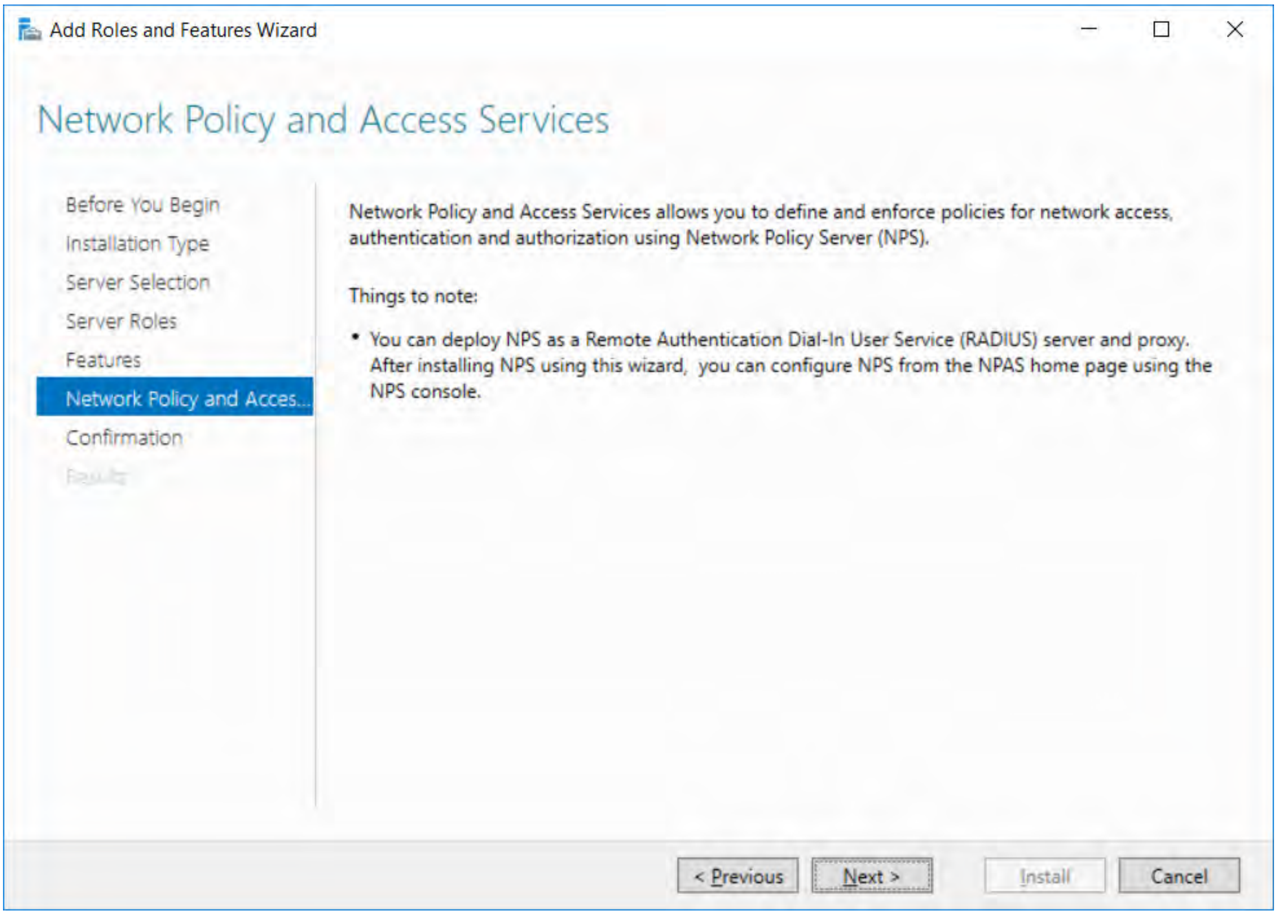
Roles

- ■ Active Directory Certificate Services (1 of 6 installe
- ☑ Active Directory Domain Services (Installed)
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- ☑ DHCP Server (Installed)
- ☑ DNS Server (Installed)
- □ Fax Server
- ■ File and Storage Services (2 of 12 installed)
- □ Host Guardian Service
- □ Hyper-V
- □ MultiPoint Services
- ☑ Network Policy and Access Services
- □ Print and Document Services
- ■ Remote Access (2 of 3 installed)
- □ Remote Desktop Services
- □ Volume Activation Services
- ■ Web Server (IIS) (12 of 43 installed)

Description

Network Policy and Access Services provides Network Policy Server (NPS), which helps safeguard the security of your network.

- Click next until option Network Policy and Access Services is selected:



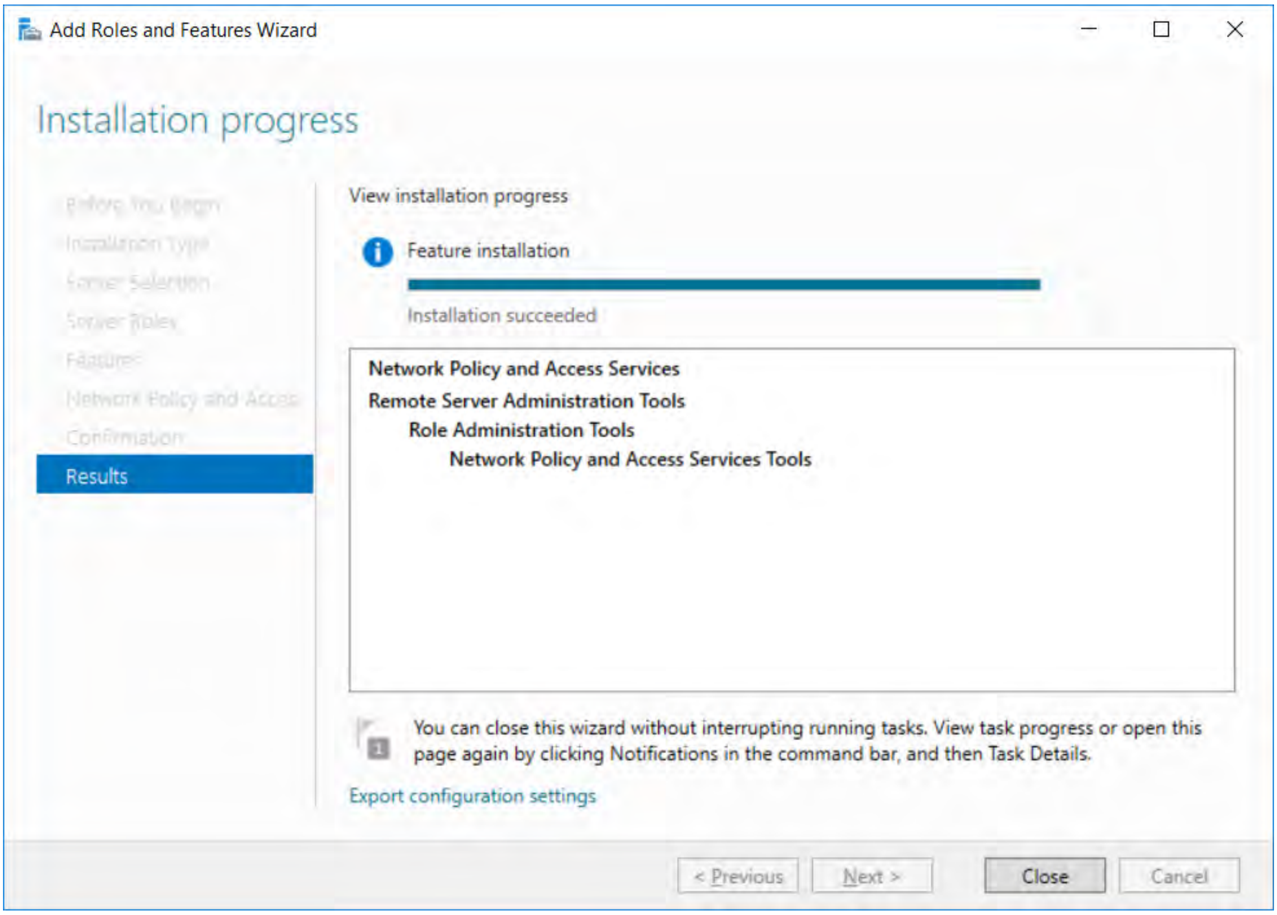
Network Policy and Access Services

Network Policy and Access Services allows you to define and enforce policies for network access, authentication and authorization using Network Policy Server (NPS).

Things to note:

- You can deploy NPS as a Remote Authentication Dial-In User Service (RADIUS) server and proxy. After installing NPS using this wizard, you can configure NPS from the NPAS home page using the NPS console.

- Click Next until Installation is completed and the Close.
- Once installed, in Server Manager => Tools, you should click in “Network Policy Server”use . You should select option “RADIUS server for 802.1X Wireless or Wired Connections” and then “Configure 802.1X”.



Installation progress

View installation progress

Feature installation

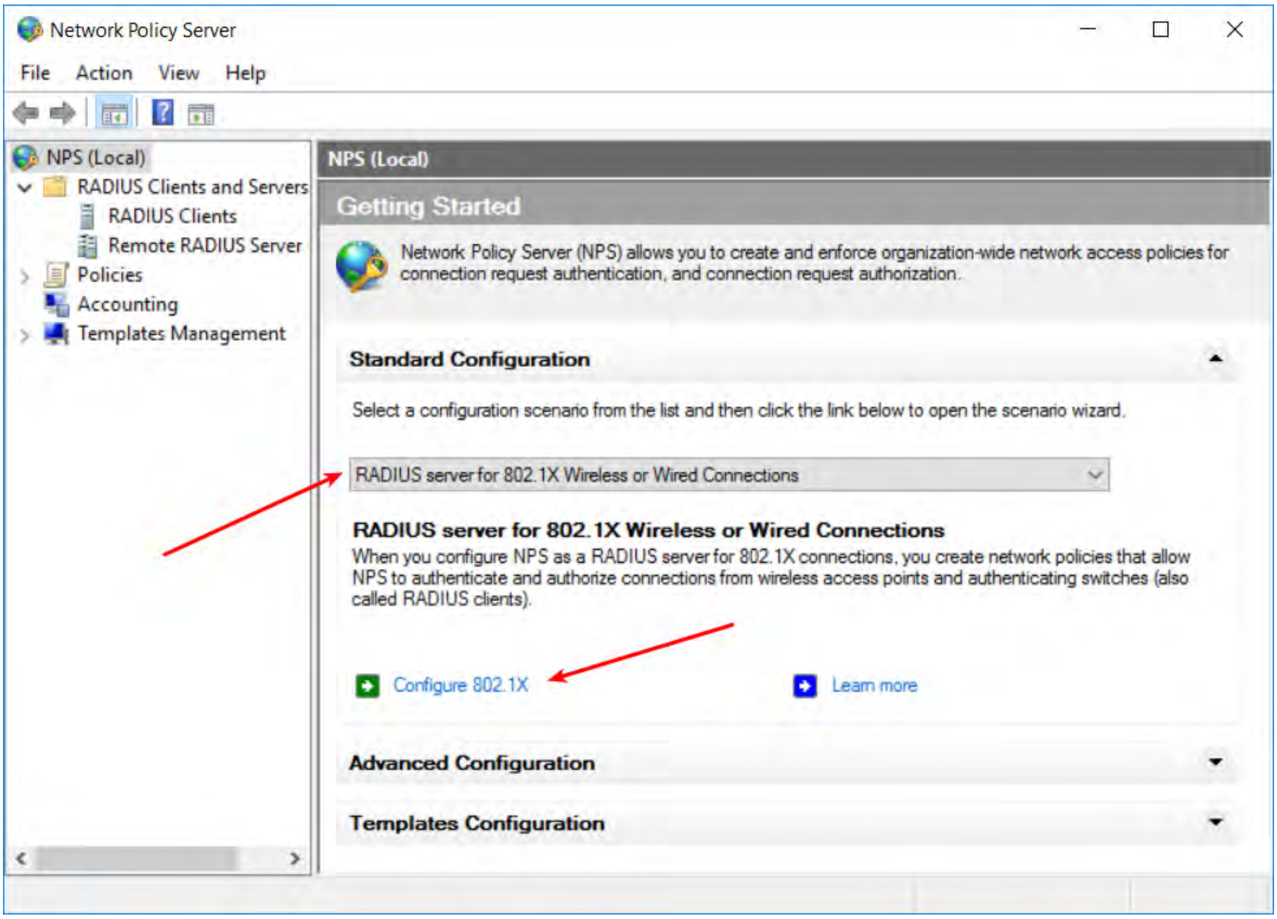
Installation succeeded

Network Policy and Access Services
Remote Server Administration Tools
Role Administration Tools
Network Policy and Access Services Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

- Select Secure Wireless connection and click Next.
- In Specify 802.1X Switches, Click Add.



Getting Started

Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for connection request authentication, and connection request authorization.

Standard Configuration

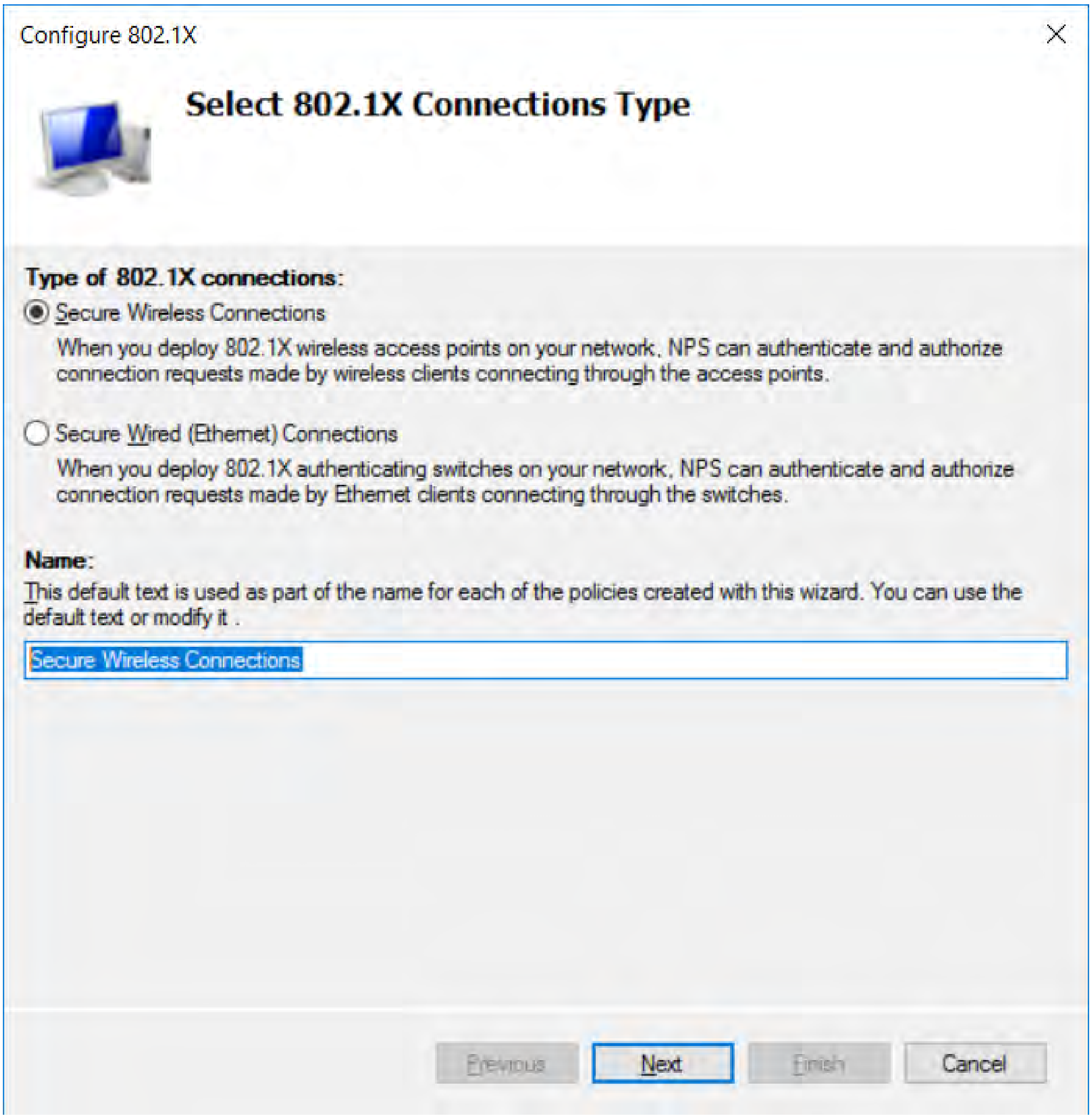
Select a configuration scenario from the list and then click the link below to open the scenario wizard.

RADIUS server for 802.1X Wireless or Wired Connections

RADIUS server for 802.1X Wireless or Wired Connections

When you configure NPS as a RADIUS server for 802.1X connections, you create network policies that allow NPS to authenticate and authorize connections from wireless access points and authenticating switches (also called RADIUS clients).

- Complete information related to the Access Point including:
  - Name
  - IP (10.10.10.1)
  - Shared secret (this is the password that we will use later in the AP configuration)



Configure 802.1X

Select 802.1X Connections Type

Type of 802.1X connections:

● Secure Wireless Connections

When you deploy 802.1X wireless access points on your network, NPS can authenticate and authorize connection requests made by wireless clients connecting through the access points.

○ Secure Wired (Ethernet) Connections

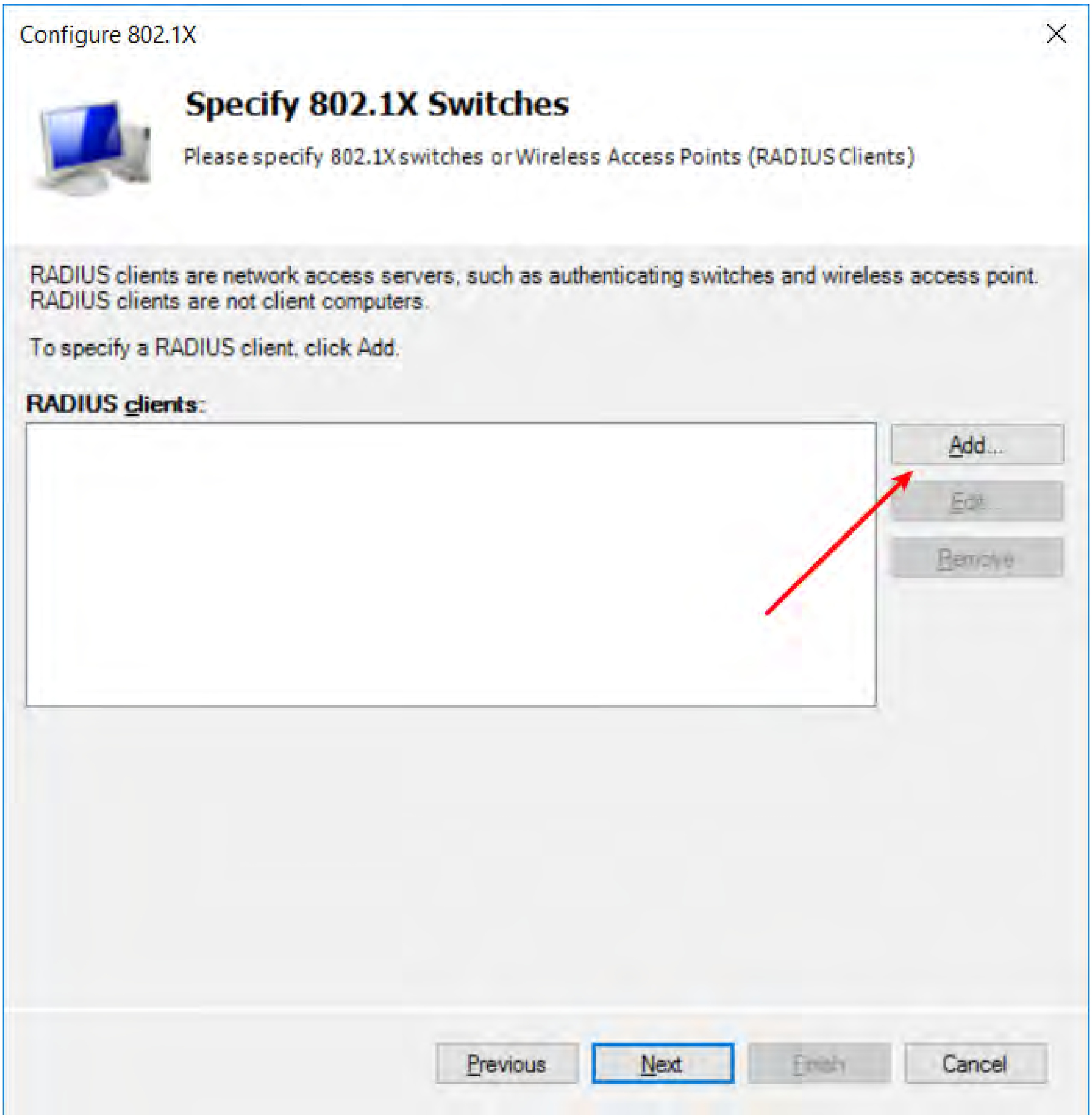
When you deploy 802.1X authenticating switches on your network, NPS can authenticate and authorize connection requests made by Ethernet clients connecting through the switches.

Name:

This default text is used as part of the name for each of the policies created with this wizard. You can use the default text or modify it .

Secure Wireless Connections

- In Specify 802.1X Switches, click Next.
- In Configure an Authentication Method, select Microsoft: Smart Card or other certificate.



Configure 802.1X

Specify 802.1X Switches

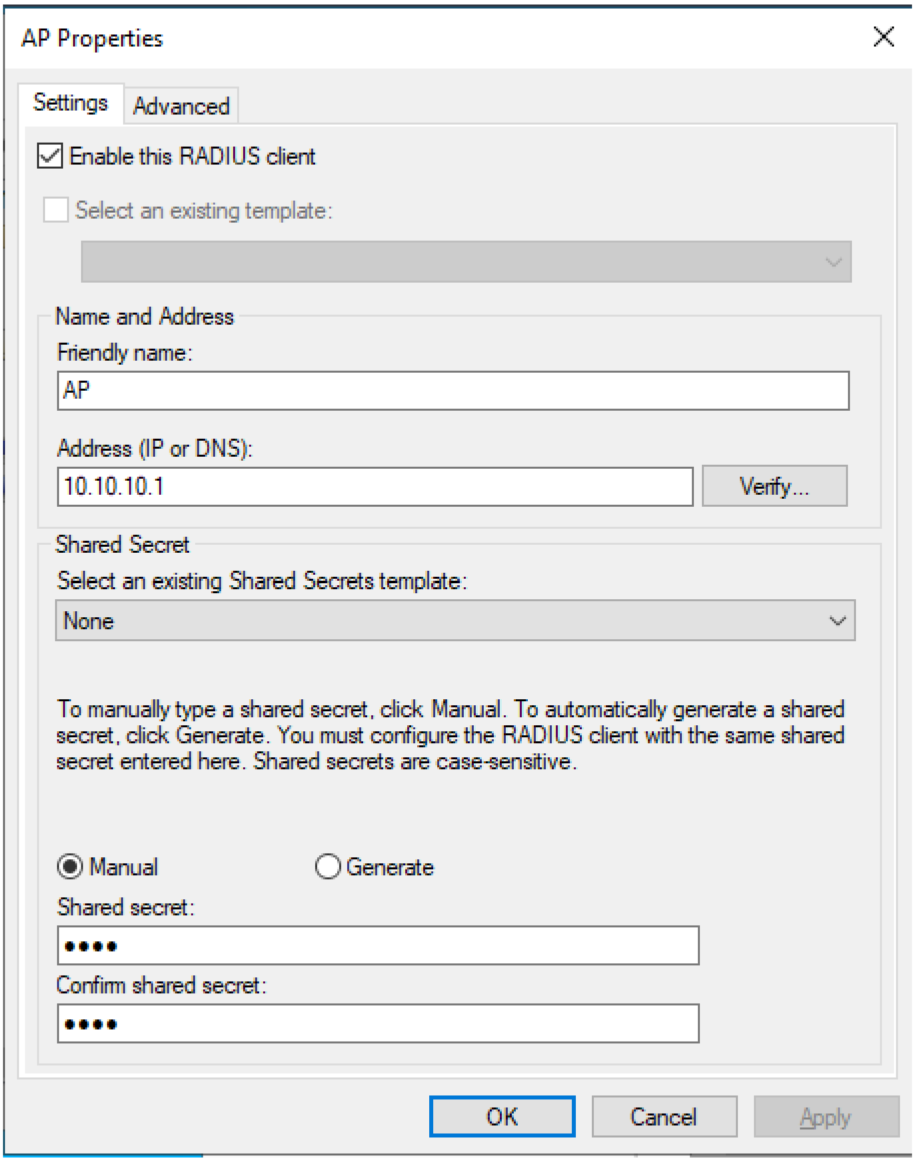
Please specify 802.1X switches or Wireless Access Points (RADIUS Clients)

RADIUS clients are network access servers, such as authenticating switches and wireless access point. RADIUS clients are not client computers.

To specify a RADIUS client, click Add.

RADIUS clients:

- Do not add any group in Specify User Groups and Click “Next”.



AP Properties

☑ Enable this RADIUS client

□ Select an existing template:

Name and Address

Friendly name: AP

Address (IP or DNS): 10.10.10.1

Shared Secret

Select an existing Shared Secrets template: None

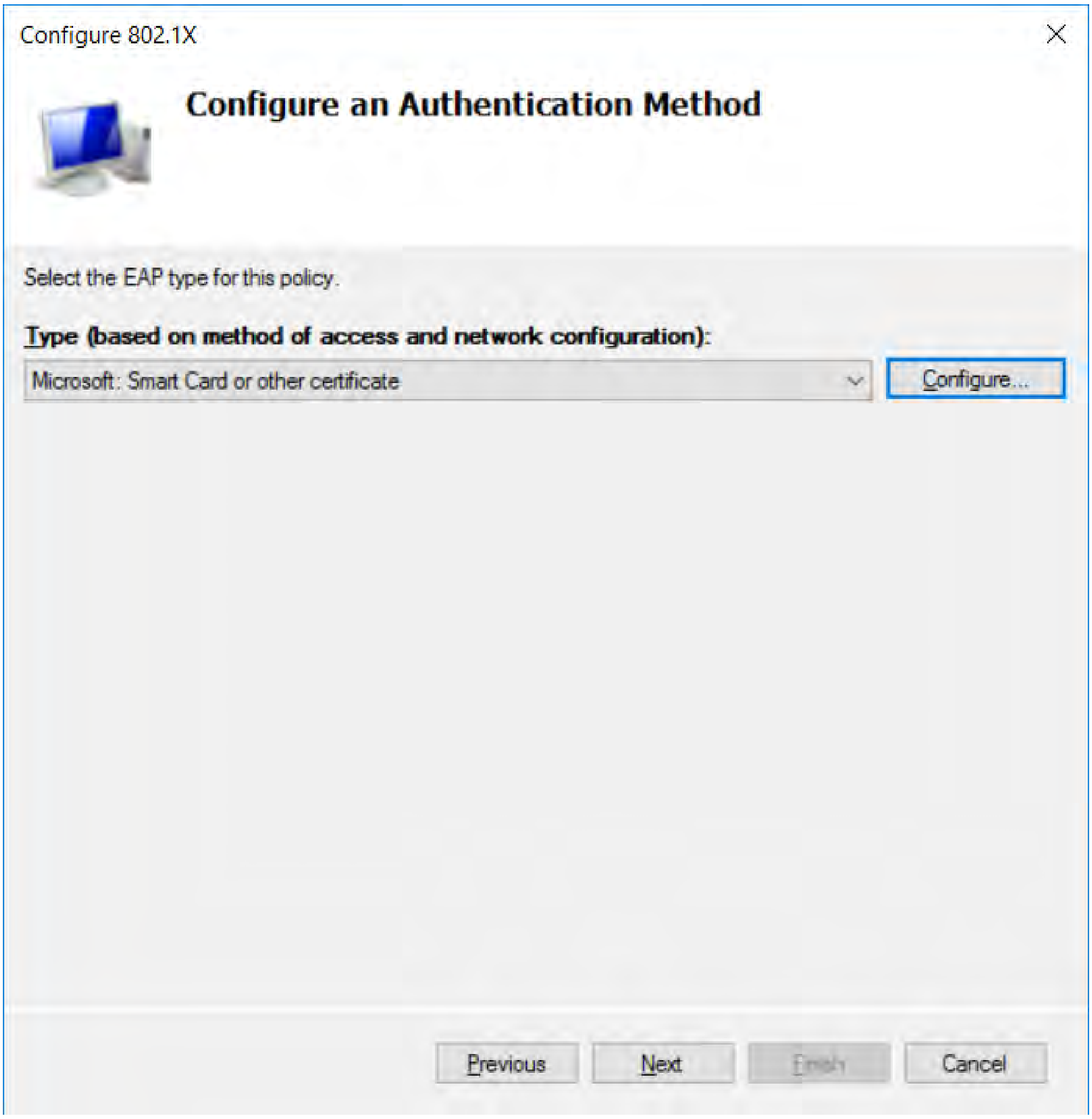
To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret: ••••

Confirm shared secret: ••••

- In Configure traffic controls screen, click Next.



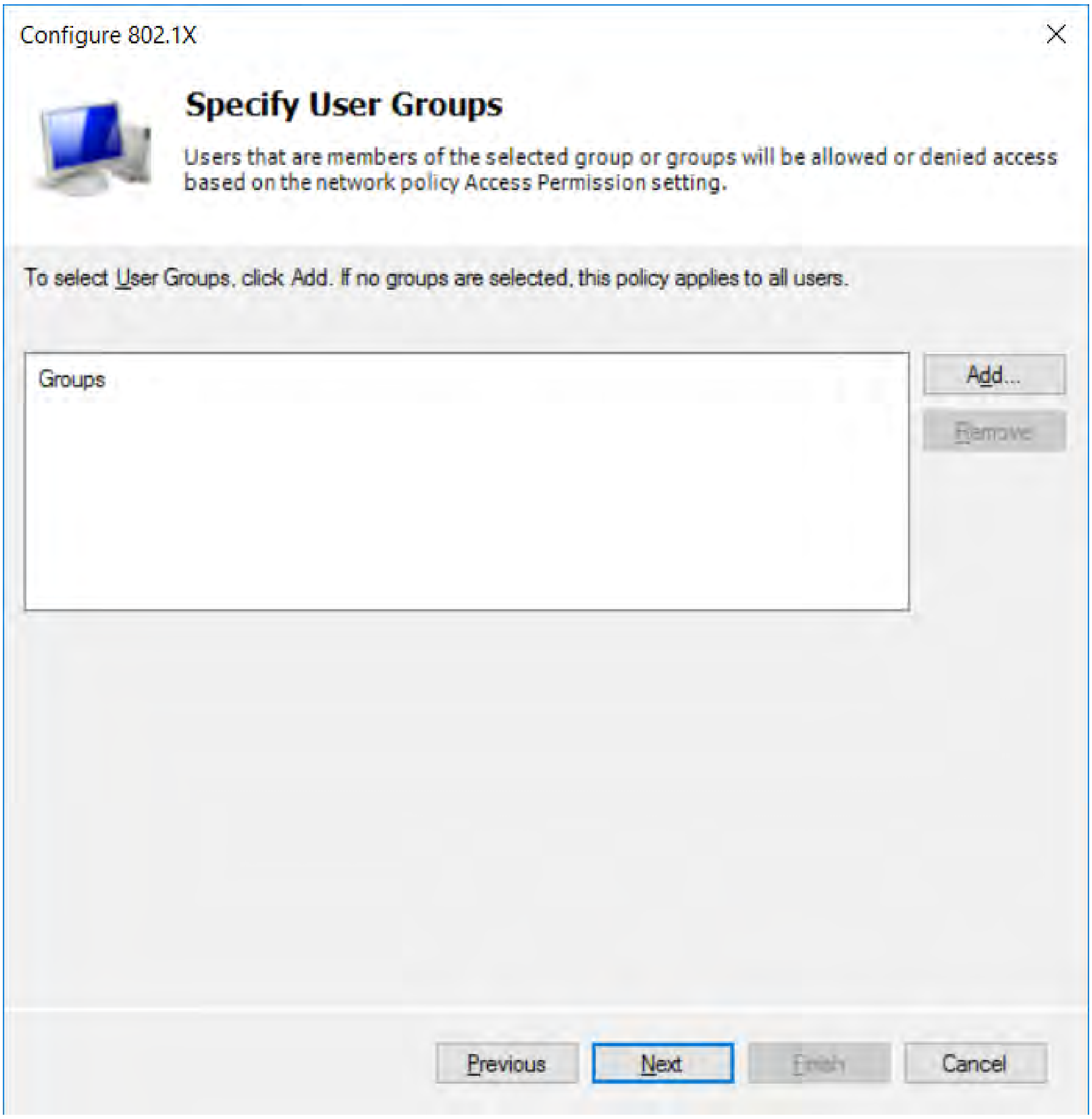
Configure 802.1X

Configure an Authentication Method

Select the EAP type for this policy.

Type (based on method of access and network configuration): Microsoft: Smart Card or other certificate

- And then click Finish.



Configure 802.1X

Specify User Groups

Users that are members of the selected group or groups will be allowed or denied access based on the network policy Access Permission setting.

To select User Groups, click Add. If no groups are selected, this policy applies to all users.

61.2.1.1.2 Access Point Configuration

Access point shall be configured in WPA2/WPA3 Enterprise Mode according to data obtained from previous configuration steps including Server IP, connection type and shared secret.

- Network name: Radius
- Shared key: whatever (configured previously in NPS in server)
- Radius server: 10.10.10.40 (Server IP)
- Radius port: 1812
- Channel: 8 (According to test procedures, you should choose a channel not occupied by other Wi-Fi networks)

- Enable Second Network with WPA2/WPA3 Personal as shown below because it will be used during testing procedures as well.
- For routing traffic using the MITM machine, an static route shall be created

61.2.1.1.3 Man in the Middle Machine Configuration

The evaluator has configured a machine with the following configuration:

- 1 Physical Ethernet interfaces
- 1 Virtual network interface
- 1 Wi-Fi network interface (Supporting Monitor Mode)

Software:

- Debian 9
- RehtSe: https://github.com/JmFoces/Rehtse
- Aircrack-ng Suite: https://www.aircrack-ng.org/
- Wireshark: https://www.wireshark.org/

Initial script for network configuration:

```
#!/bin/bash

ip addr add 10.10.10.100/24 dev enp0s3
ip addr add 20.20.20.100/24 dev enp0s8

if [ $(cat /proc/sys/net/ipv4/ip_forward) -eq 0 ]; then
    echo "1" > /proc/sys/net/ipv4/ip_forward
```

IP Tables configuration script for configuring MITM and allow RehtSe to modify packets can be seen below:

```
#!/bin/bash

iptables -A FORWARD -s 20.20.20.40 -d 10.10.10.1 -j NFQUEUE --queue-num 0
iptables -A FORWARD -s 10.10.10.1 -d 20.20.20.40 -j ACCEPT
```

61.2.1.1.4 Windows 10 and Windows 11 Client Configuration

Firstly the client connected to LAN for joining the Domain and obtaining certificates will be configured. Secondly, the client shall be disconnected from the LAN and has to use the Wi-Fi to connect to the domain using Radius services.

These steps can be found in FTP_ITC_EXT .1.1(TLS).

61.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [PPMWLAN10] instructions in order to collect the results as stipulated by the protection profile [PPMWLAN10].

61.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8.Test environment definition**.

Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)

For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions editions, the wireless extended profile has not been tested because is out of the scope.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE’s behavior is as expected and detailed in the security target [ST004].

61.2.1.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

61.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FMT_SMF.1/WLAN.

62 FPT_TST_EXT.3/WLAN

The assurance activity for the **FPT_TST_EXT.3/WLAN** requirement is stated as follows:

> The evaluator shall examine the TSS to ensure that it details the self tests that are run by the TSF on start-up; this description should include an outline of what the tests are actually doing (e.g., rather than saying "memory is tested", a description similar to "memory is tested by writing a value to each memory location and reading it back to ensure it is identical to what was written" shall be used). The evaluator shall ensure that the TSS makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly.
>
> The evaluator shall examine the TSS to ensure that it describes how to verify the integrity of stored TSF executable code when it is loaded for execution. The evaluator shall ensure that the TSS makes an argument that the tests are sufficient to demonstrate that the integrity of stored TSF executable code has not been compromised. The evaluator also ensures that the TSS (or the operational guidance) describes the actions that take place for successful (e.g. hash verified) and unsuccessful (e.g., hash not verified) cases.
>
> The evaluator shall ensure that the TSS (or the operational guidance) describes the actions that take place for successful (e.g. hash verified) and unsuccessful (e.g., hash not verified) cases.
>
> The evaluator shall perform the following tests:
>
> - **Test 1:** The evaluator performs the integrity check on a known good TSF executable and verifies that the check is successful.
> - **Test 2:** The evaluator modifies the TSF executable, performs the integrity check on the modified TSF executable and verifies that the check fails.

62.1 Documentation Review activity

62.1.1 Findings

The evaluator has reviewed the section **6.6.4 Windows Platform Integrity and Code Integrity** of the ***Security Target*** document, which describes the different stages of the boot process, providing information about which are the main files loaded in each step of the boot chain.

This information has allowed the evaluator to design a testing plan, which will be used during the test activity. The evaluator has identified four different stages during the boot process:

- **First stage:** Secure boot checks the file integrity of early boot components, comparing them with the values stored in the TPM. Due to the fact that TPM is part of the external TOE environment, this stage will not be tested during the test activity.

- **Second stage:** After the preliminary components have been loaded, the UEFI firmware loads the OS Boot Manager. Once the integrity of OS Boot Manager has been checked, it attempts to load one of these boot applications:
  - OS Loader: *winload.exe* or *winload.efi*
  - OS Resume: *winresume.exe* or *winresume.efi (The administrative guidance states that the hibernation is disabled, so this boot application will not be used during the evaluation)*
  - A physical memory testing application: *memtest.exe (The* **Security Target** *document states that it is considered a non-operational mode for the evaluation).*

  In addition, a list with the critical loaded files during the bootchain when the *winload.exe* is selected has been included. These files are the following:

  - Text intentionally left blank.
- **Third stage:** Once the *winload.exe* or *winload.efi* file has been loaded and its integrity has been checked, the next step in the bootchain is loading the *ntoskrnl.exe* file. Additional critical drivers and libraries are loaded together with this file. The following information is also included regarding Code Integrity, which verifies the integrity of the kernel drivers loaded into the memory. For x64-based computers, all kernel-mode drivers must be digitally signed. If during the boot process an unsigned-driver is loaded, the operating system will not load. On the other hand, for a x86-based computer only the files listed above must be digitally signed. If any of these files are not signed, the operating system will not load. However, if another unsigned-driver is detected during the boot process, the operating system may be loaded normally.
- **Fourth stage:** After the critical device drivers and libraries have been loaded, the Windows kernel continues to boot the rest of the operating system.

The integrity validation mechanism is explained throughout this section, including information about how the TOE validates each piece of software using a hash based signature and an embedded public key as shown in the following extract:

> *[...]After the initial device drivers have been loaded, the Windows kernel will continue to boot the rest of the operating system using the Code Integrity capability (ci.dll) to measure code integrity for (1) the remaining kernel-mode and user-mode programs which need to be loaded for the OS to complete its boot and (2) after booting, CI also verifies the integrity of applications launched by the user (applications from Microsoft are always signed by Microsoft, and third-party applications which may be signed by the developer) by checking the RSA signature for the binary and SHA-256 hashes of the binary which are compared to the catalog files described above.*

62.1.2 Verdict

The evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfilment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

62.2 Test Activity

62.2.1 Test 1

The evaluator will observe that the integrity mechanism does not flag any executable or internal library with integrity errors. Boot procedure has been described and tested in the *FPT_TST_EXT.1.1* requirement of the *General Purpose OS PP*.

62.2.1.1 Setup

Before the test execution, the following setup condition must be fulfilled:

- The SignTool application must be available. This application comes within the Windows 10 SDK and Windows 11 SDK.

62.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [PPMWLAN10] instructions in order to collect the results as stipulated by the protection profile [PPMWLAN10].

62.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8.Test environment definition**.

The evaluator has obtained the same results for all the tested platforms.

For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions editions, the wireless extended profile has not been tested because is out of the scope.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

62.2.1.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

62.2.2 Test 2

The evaluator will modify the selected file and will try to obtain the evidence in the system log.

62.2.2.1 Setup

Before the test execution, the following setup condition must be fulfilled:

- A hexadecimal editor (e.g. *HxD*) must be installed in the evaluated platforms to modify the binary files loaded during the WLAN connection process.
- A *WinPE* USB must be available.

62.2.2.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [PPMWLAN10] instructions in order to collect the results as stipulated by the protection profile [PPMWLAN10].

62.2.2.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8.Test environment definition**.

Additionally, the following supplementary platforms have been also tested:

- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)

For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions editions, the wireless extended profile has not been tested because is out of the scope.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

62.2.2.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 2** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 2**.

62.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FPT_TST_EXT.3/WLAN.

63 FTA_WSE_EXT.1/WLAN

The assurance activity for the **FTA_WSE_EXT.1/WLAN** requirement is stated as follows:

> The evaluator shall examine the TSS to determine that it defines SSIDs as the attribute to specify acceptable networks.
>
> The evaluator shall examine the operational guidance to determine that it contains guidance for configuring the list of SSID that the WLAN Client is able to connect to.
>
> The evaluator shall ensure that the TSS (or the operational guidance) describes the actions that take place for successful (e.g. hash verified) and unsuccessful (e.g., hash not verified) cases.
>
> The evaluator shall also perform the following test:
>
> - **Test 1:** The evaluator configures the TOE to allow a connection to a wireless network with a specific SSID. The evaluator also configures the test environment such that the allowed SSID and an SSID that is not allowed are both "visible" to the TOE. The evaluator shall demonstrate that they can successfully establish a session with the allowed SSID. The evaluator will then attempt to establish a session with the disallowed SSID, and observe that the attempt fails.

63.1 Documentation Review activity

63.1.1 Findings

The evaluator has reviewed the section **6.7 TOE Access** of the ***Security Target*** document, which describes that administrator can specify which Wi-Fi networks (SSID) a TOE may be connected to.

Also, the ***Operational Guidance*** document includes in its section **4.5 Managing network connections** instructions for configuring allowed Wi-Fi networks.

This information has allowed the evaluator to design a testing plan, which will be used during the test activity.

63.1.2 Verdict

The evaluator considers that, the findings obtained during the documentation review activity demonstrate the fullfilment of the requirements established in the assurance activity section. Hence, the PASS verdict is assigned to the documentation review activity.

63.2 Test Activity

63.2.1 Test 1

The evaluator will use two different Wi-Fi networks with different SSID: Radius and PSK and will block access to PSK. Then, the evaluator will check that it is not possible to connect to the PSK SSID.

63.2.1.1 Setup

In this case, the evaluator has used the general NPS architecture with the following elements and roles:

- Windows NPS Server (EAP-TLS)
- Windows Client using domain user (FIPS Enabled)
- AP WPA2-Enterprise mode
- Kali Linux (sniffing machine)

63.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [PPMWLAN10] instructions in order to collect the results as stipulated by the protection profile [PPMWLAN10].

63.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8.Test environment definition**.

Additionally, the following supplementary platforms have been also tested:

- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)

For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions editions, the wireless extended profile has not been tested because is out of the scope.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

63.2.1.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

63.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FTA_WSE_EXT.1/WLAN.

64 FTP_ITC.1/WLAN

The assurance activity for the **FTP_ITC_EXT.1/WLAN** requirement is stated as follows:

> The evaluator shall examine the TSS to determine that it describes the details of the TOE connecting to an access point in terms of the cryptographic protocols specified in the requirement, along with TOE-specific options or procedures that might not be reflected in the specification. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST.
>
> The evaluator shall confirm that the operational guidance contains instructions for establishing the connection to the access point, and that it contains recovery instructions should a connection be unintentionally broken.
>
> The evaluator shall perform the following tests:
>
> - **Test 1:** The evaluators shall ensure that the TOE is able to initiate communications with an access point using the protocols specified in the requirement, setting up the connections as described in the operational guidance and ensuring that communications are successful.
> - **Test 2:** The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.
> - **Test 3:** The evaluator shall ensure, for each communication channel with an authorized IT entity, modification of the channel data is detected by the TOE.
> - **Test 4:** The evaluators shall physically interrupt the connection from the TOE to the access point (e.g., moving the TOE host out of range of the access point, turning the access point off). The evaluators shall ensure that subsequent communications are appropriately protected, at a minimum in the case of any attempts to automatically resume the connection or connect to a new access point.
>
> Further assurance activities are associated with the specific protocols.

64.1 Documentation Review activity

64.1.1 Findings

The evaluator has reviewed the sections **6.2.3.1 TLS, HTTPS, EAP-TLS, DTLS** and **6.2.3.2 Wireless Networking** of the ***Security Target*** document, which describes the TLS RFCs implemented in the TOE as well as the supported ciphersuites and Wi-Fi standards compliance.

The TSS identifies the following cipher suites used during the evaluated configuration:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289

Full list of supported ciphersuites are described in the following document: Cipher Suites in TLS/SSL (Schannel SSP).

In addition to this, TSS describes how the TOE natively implements IEEE 802.11-2012 and IEEE 802.11ac-2013 for providing secure wireless local area networking (Wi-Fi). Additionally, in section **6.2.3.2 Wireless Networking**, it describes how the TOE can use PRF-384 in WPA2 Wi-Fi sessions and can generate AES 128-bit keys or PRF-704 to generate AES-256 bit keys both using the WIndows RBG. Key wrapping and unwrapping are performed according to the NIST SP 800-38F specification for securing GTK.

Moreover, the ***Operational Guidance*** document includes in its section **4.5.7 Configuring a Wi-Fi connection profile with the Windows UI** instructions about how to establish connection to an access point using EAP-TLS. In addition to this, section **4.5.6 Selecting a secure Wi-Fi connection with the Windows UI** states that when connection is unintentionally broken, TOE will automatically attempt to reconnect when it becomes available again.

This information has allowed the evaluator to design a testing plan, which will be used during the test activity.

64.1.2 Verdict

The evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfillment of the requirements established in the assurance activity section. Hence, the PASS verdict is assigned to the documentation review activity.

64.2 Test Activity

64.2.1 Test 1

The evaluator will try to successfully establish connection with AP using the protocols specified below.

64.2.1.1 Setup

The applicable setup for this test is the same as the one defined for *Test 1* in FCS_TLSC_EXT.1/WLAN.

64.2.1.2 Procedure

The evaluator shall carry out the same procedure as one defined for *Test 1* in FCS_TLSC_EXT.1/WLAN.

64.2.1.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8.Test environment definition**.

Additionally, the following supplementary platforms have been also tested:

- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)

For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions editions, the wireless extended profile has not been tested because is out of the scope.

This test was performed in conjunction with FCS_TLSC_EXT.1/WLAN. Results can be seen in *Test 1* in FCS_TLSC_EXT.1/WLAN

64.2.1.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

64.2.2 Test 2

The evaluator will review that no plaintext data is sent using authorized communication channels.

64.2.2.1 Setup

The applicable setup for this test is the same as the one defined for *Test 2* in FCS_CKM.1/WLAN.

64.2.2.2 Procedure

The evaluator shall carry out the same procedure as one defined for *Test 2* in FCS_CKM.1/WLAN.

64.2.2.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8.Test environment definition**.

Additionally, the following supplementary platforms have been also tested:

- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)

For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions editions, the wireless extended profile has not been tested because is out of the scope.

This test was performed in conjunction with FCS_CKM.1/WLAN. Results can be seen in *Test 2* in FCS_CKM.1/WLAN.

64.2.2.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 2** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 2**.

64.2.3 Test 3

The evaluator will review that modification of the channel data is detected by the TOE.

64.2.3.1 Setup

The applicable setup for this test is the same as the one defined for for *Test 5* in FCS_TLSC_EXT.1/WLAN.

64.2.3.2 Procedure

The evaluator shall carry out the same procedure as one defined for for *Test 5* in FCS_TLSC_EXT.1/WLAN.

64.2.3.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8.Test environment definition**.

Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)

For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions editions, the wireless extended profile has not been tested because is out of the scope.

This test was performed in conjunction with FCS_TLSC_EXT.1/WLAN. Results can be seen in for *Test 5* in FCS_TLSC_EXT.1/WLAN.

64.2.3.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 3** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 3**.

64.2.4 Test 4

The evaluator will physically disconnect the AP and will review that communications are appropriately protected.

64.2.4.1 Setup

In this case, we are going to use the general NPS architecture composed by the following elements:

- Windows NPS Server (EAP-TLS)
- Windows Client using domain user (FIPS Enabled)
- AP WPA2-Enterprise mode

64.2.4.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the protection profile [PPMWLAN10] instructions in order to collect the results as stipulated by the protection profile [PPMWLAN10].

64.2.4.3 Results

The evaluator has performed this test on all the canonical platforms as defined in section **8.Test environment definition**.

Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)

For Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge editions editions, the wireless extended profile has not been tested because is out of the scope.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

64.2.4.4 Verdict

The evaluator considers that, the results obtained from the test activity demonstrate the fulfilment of the **Test 4** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 4**.

64.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FTP_ITC.1/WLAN.

65 FAU_GEN.1(VPN)

The assurance activity for the **FAU_GEN.1(VPN)** requirement is stated as follows:

> The evaluator shall check the operational guidance and ensure that it lists all of the auditable events and provides a format for audit records. Each audit record format type must be covered, along with a brief description of each field. The evaluator shall check to make sure that every audit event type mandated by the VPN Client PP-Module is described and that the description of the fields contains the information required in FAU_GEN.1.2/VPN, and the additional information specified in the Auditable Events table of the VPN Client PP-PP-Module.
>
> In particular, the evaluator shall ensure that the operational guidance is clear in relation to the contents for failed cryptographic events. In the Auditable Events table of the VPN Client PP-Module, information detailing the cryptographic mode of operation and a name or identifier for the object being encrypted is required. The evaluator shall ensure that name or identifier is sufficient to allow an administrator reviewing the audit log to determine the context of the cryptographic operation (for example, performed during a key negotiation exchange, performed when encrypting data for transit) as well as the non-TOE endpoint of the connection for cryptographic failures relating to communications with other IT systems.
>
> The evaluator shall also make a determination of the administrative actions that are relevant in the context of the VPN Client PP-Module. The TOE may contain functionality that is not evaluated in the context of the VPN Client PP-Module because the functionality is not specified in an SFR. This functionality may have administrative aspects that are described in the operational guidance. Since such administrative actions will not be performed in an evaluated configuration of the TOE, the evaluator shall examine the operational guidance and make a determination of which administrative commands, including subcommands, scripts, and configuration files, are related to the configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the VPN Client PP- Module, which thus form the set of "all administrative actions". The evaluator may perform this activity as part of the activities associated with ensuring the AGD_OPE guidance satisfies the requirements.
>
> For each required auditable event, the evaluator shall examine the operational guidance to determine that it is clear to the reader where each event is generated (e.g. the TSF may generate its own audit logs in one location while the platform-provided auditable events are generated elsewhere).
>
> **Test:**

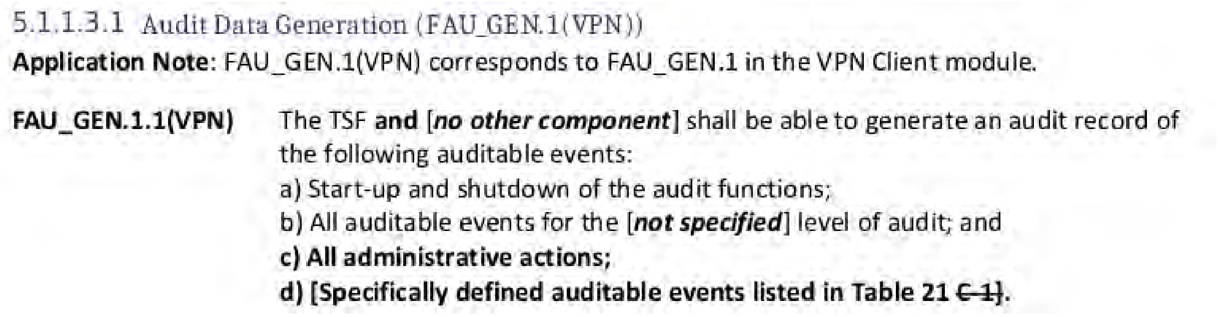
The evaluator shall test the TOE's ability to correctly generate audit records by having the TOE generate audit records in accordance with the EAs associated with the functional requirements in the VPN Client PP-Module. Additionally, the evaluator shall test that each administrative action applicable in the context of the VPN Client PP-Module is auditable. When verifying the test results, the evaluator shall ensure the audit records generated during testing match the format specified in the administrative guide, and that the fields in each audit record have the proper entries.

Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly. For example, testing performed to ensure that the administrative guidance provided is correct verifies that AGD_OPE.1 is satisfied and should address the invocation of the administrative actions that are needed to verify the audit records are generated as expected.

65.1 Documentation Review activity

65.1.1 Findings

The ***Security Target*** document, defines in its section **5.1.1.3.1 Audit Data Generation (FAU_GEN.1(VPN))**, the following auditable events:



5.1.1.3.1 Audit Data Generation (FAU_GEN.1(VPN))

Application Note: FAU_GEN.1(VPN) corresponds to FAU_GEN.1 in the VPN Client module.

FAU_GEN.1.1(VPN) The TSF **and** [***no other component***] shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events for the [***not specified***] level of audit; and
c) All administrative actions;
d) [Specifically defined auditable events listed in Table 21 ~~C-1~~].

The evaluator has reviewed the section **5.1.1.3 Security Audit for VPN Client Module** of the **Security Target** document, which determines the events to be audited for this requirement, specifically in table 21.

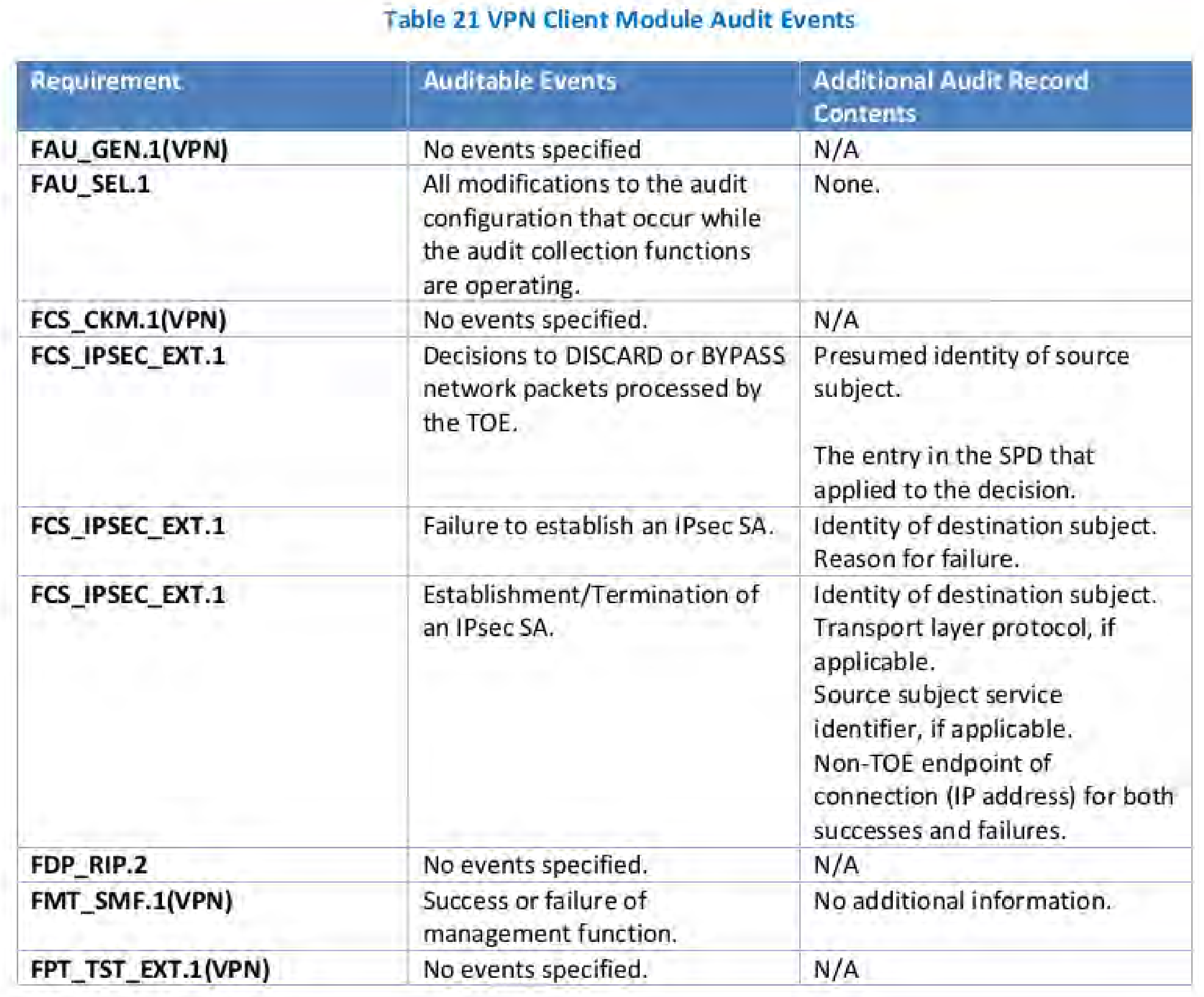


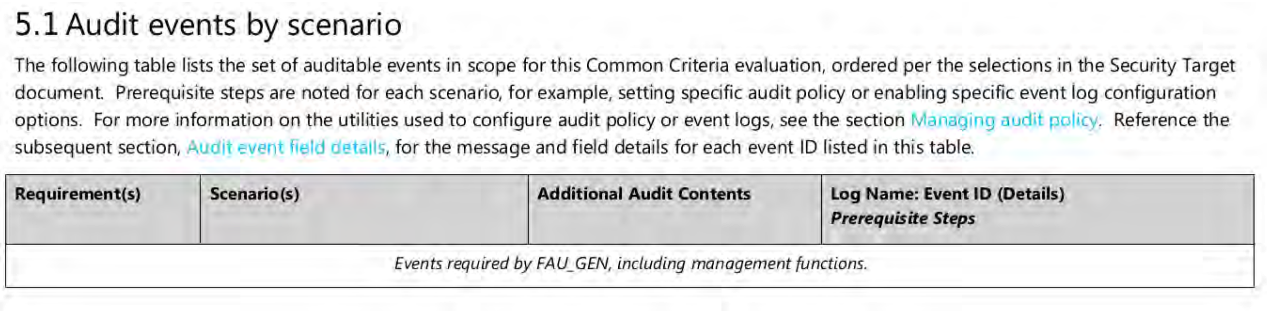
Table 21 VPN Client Module Audit Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1(VPN)	No events specified	N/A
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating.	None.
FCS_CKM.1(VPN)	No events specified.	N/A
FCS_IPSEC_EXT.1	Decisions to DISCARD or BYPASS network packets processed by the TOE.	Presumed identity of source subject. The entry in the SPD that applied to the decision.
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA.	Identity of destination subject. Reason for failure.
FCS_IPSEC_EXT.1	Establishment/Termination of an IPsec SA.	Identity of destination subject. Transport layer protocol, if applicable. Source subject service identifier, if applicable. Non-TOE endpoint of connection (IP address) for both successes and failures.
FDP_RIP.2	No events specified.	N/A
FMT_SMF.1(VPN)	Success or failure of management function.	No additional information.
FPT_TST_EXT.1(VPN)	No events specified.	N/A

This document also states the minimum information that each audit record should include. These fields are the following:

- Date and time of the event.
- Type of the event.
- Subject identity.
- Outcome (success or failure) of the event.
- For each audit event type, based on the auditable event definitions of the functional components included in the PP-Module/ST, information specified in column three of Table 21.

In addition, the ***Operational Guidance*** document, includes in its section **5.1 Audit Events by scenario** a table with all the auditable events generated by the TOE.

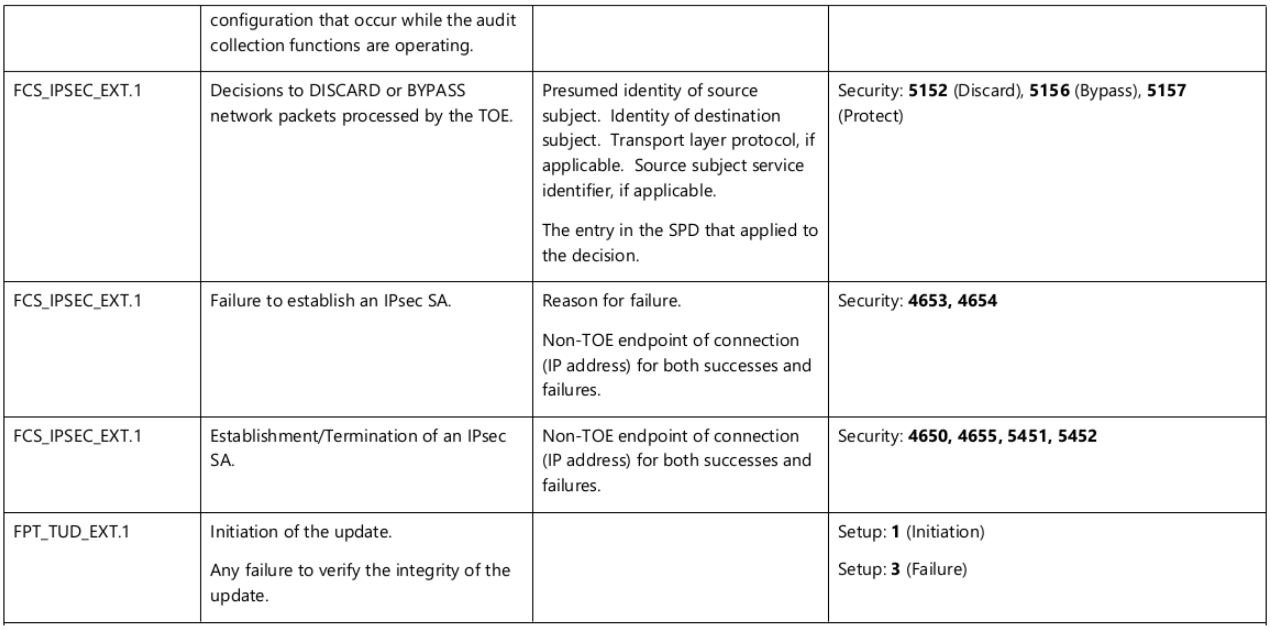


5.1 Audit events by scenario

The following table lists the set of auditable events in scope for this Common Criteria evaluation, ordered per the selections in the Security Target document. Prerequisite steps are noted for each scenario, for example, setting specific audit policy or enabling specific event log configuration options. For more information on the utilities used to configure audit policy or event logs, see the section Managing audit policy. Reference the subsequent section, Audit event field details, for the message and field details for each event ID listed in this table.

Requirement(s)	**Scenario(s)**	**Additional Audit Contents**	**Log Name: Event ID (Details)** ***Prerequisite Steps***
Events required by FAU_GEN, including management functions.			

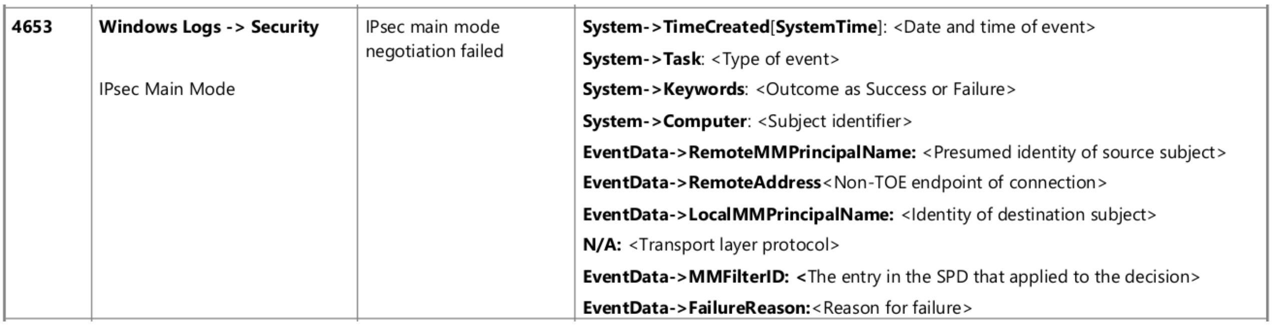
Events required by the IPsec extended package.			
FAU_GEN.1 (VPN) FMT_SMF.1 (VPN) (Function #1)	Specify VPN gateways to use for connections		Microsoft-Windows-VPN-Client/Operational: **10001** (Success) Microsoft-Windows-VPN-Client/Operational: **10002** (Failure)
FAU_GEN.1 (VPN) FMT_SMF.1 (VPN) (Function #2)	Specify IPsec VPN Clients to use for connections		Microsoft-Windows-VPN-Client/Operational: **10001** (Success) Microsoft-Windows-VPN-Client/Operational: **10002** (Failure)
FAU_GEN.1 (VPN) FMT_SMF.1 (VPN) (Function #3)	Specify IPsec-capable network devices to use for connections]		Microsoft-Windows-VPN-Client/Operational: **10001** (Success) Microsoft-Windows-VPN-Client/Operational: **10002** (Failure)
FAU_GEN.1 (VPN) FMT_SMF.1 (VPN) (Function #4)	Specify client credentials to be used for connections		Microsoft-Windows-VPN-Client/Operational: **10001** (Success) Microsoft-Windows-VPN-Client/Operational: **10002** (Failure)
FAU_GEN.1 (VPN) FMT_SMF.1 (VPN) (Function #5)	Configure the reference identifier of the peer		Microsoft-Windows-VPN-Client/Operational: **10001** (Success) Microsoft-Windows-VPN-Client/Operational: **10002** (Failure)
FAU_SEL.1	All modifications to the audit		Security: **4719**



	configuration that occur while the audit collection functions are operating.		
FCS_IPSEC_EXT.1	Decisions to DISCARD or BYPASS network packets processed by the TOE.	Presumed identity of source subject. Identity of destination subject. Transport layer protocol, if applicable. Source subject service identifier, if applicable. The entry in the SPD that applied to the decision.	Security: **5152** (Discard), **5156** (Bypass), **5157** (Protect)
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.	Security: **4653, 4654**
FCS_IPSEC_EXT.1	Establishment/Termination of an IPsec SA.	Non-TOE endpoint of connection (IP address) for both successes and failures.	Security: **4650, 4655, 5451, 5452**
FPT_TUD_EXT.1	Initiation of the update. Any failure to verify the integrity of the update.		Setup: **1** (Initiation) Setup: **3** (Failure)

The content of this table matches with the selection performed by the vendor in the ***Security Target*** document, as it can be seen in the image above.

Moreover, the ***Operational Guidance*** document also provides information related the main fields for each auditable event. This information includes the auditable events, the additional audit record contents and the event ID for each one. For example, the following image shows the main required fields for the auditable event 4653 (*IPsec main mode negotation failed*).



4653	**Windows Logs -> Security** IPsec Main Mode	IPsec main mode negotiation failed	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <Type of event> **System->Keywords**: <Outcome as Success or Failure> **System->Computer**: <Subject identifier> **EventData->RemoteMMPrincipalName:** <Presumed identity of source subject> **EventData->RemoteAddress**<Non-TOE endpoint of connection> **EventData->LocalMMPrincipalName:** <Identity of destination subject> **N/A:** <Transport layer protocol> **EventData->MMFilterID:** <The entry in the SPD that applied to the decision> **EventData->FailureReason:**<Reason for failure>

65.1.2 Verdict

The evaluator has reviewed the ***Security Target*** document and has ensured that every auditable event type selected in the ***Security Target*** document is included in the ***Operational Guidance*** document. Moreover, the evaluator has also ensured that the format of every auditable event is described, including at least the fields defined in the ***Security Target*** document (*date and time, type of the event, subject identity, outcome and information of column 3*).

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfilment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to this activity.

65.2 Test Activity

For this requirement, some of the auditable events will be obtained during the test execution of each security functional requirement.

65.2.1 Test 1

65.2.1.1 Setup

The scenario to perform the assurance Server activities according to the Protection Profile is composed of the following elements:

- Testing Machine (Debian 11 Bullseye, using Strongswan U5.9.1/K5.10)
- Windows Client Machine (Platforms listed in the ST)
- Script FAU_GEN.1.ps1 is available in TOE

Both machines are in the same network with the following configuration:

- Testing Machine, IP = 20.20.20.100
- Client Machine, IP = 20.20.20.50

This setup will be required to set the audit policy for the audit generation of the events listed in table 21.

The additional setup required for obtaining each auditable event listed in Table 21 will be described in the *Setup* section of the following requirements:

- FAU_SEL.1
- FCS_IPSEC_EXT.1
- FDP_RIP.2
- FCS_RBG_EXT.1
- FMT_SMF.1(VPN)
- FPT_TUD_EXT.1

All the audit events required will be obtained and described in each test defined in the previous list. In addition, the audit events will be shown in the results section for the sake of a better readability.

65.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMVPN24SD] instructions in order to collect the results as stipulated by the supporting document [PPMVPN24SD].

65.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)

Results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms*.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

65.2.1.4 Verdict

As the result above states, the related events have been correctly generated and they include all the information defined in the ***Security Target*** document.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

65.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FAU_GEN.1(VPN).

66 FAU_SEL.1

The assurance activity for the **FAU_SEL.1** requirement is stated as follows:

> The evaluator shall review the administrative guidance to ensure that the guidance itemizes all event types, as well as describes all attributes that are to be selectable in accordance with the requirement, to include those attributes listed in the assignment. The administrative guidance shall also contain instructions on how to set the pre-selection, or how the VPN gateway will configure the client, as well as explain the syntax (if present) for multi-value pre-selection. The administrative guidance shall also identify those audit records that are always recorded, regardless of the selection criteria currently being enforced.
>
> The evaluator shall perform the following tests:
>
> - **Test 1:** For each attribute listed in the requirement, the evaluator shall devise a test to show that selecting the attribute causes only audit events with that attribute (or those that are always recorded, as identified in the administrative guidance) to be recorded.
> - **Test 2 [conditional]:** If the TSF supports specification of more complex audit pre-selection criteria (e.g., multiple attributes, logical expressions using attributes) then the evaluator shall devise tests showing that this capability is correctly implemented. The evaluator shall also, in the test plan, provide a short narrative justifying the set of tests as representative and sufficient to exercise the capability.

66.1 Documentation Review activity

66.1.1 Findings

The evaluator has reviewed section **4.20 Managing audit policy and event logs** of the **Operational and Administrative Guidance** document. In these section, the events to be audited and the relationship with the codes to obtain them are defined.

66.1.2 Verdict

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfillment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

66.2 Test Activity

66.2.1 Test 1 and Test2

66.2.1.1 Setup

Before the test execution, the following setup condition must be fulfilled:

The scenario to perform the assurance activities according to the Protection Profile consists of the following elements:

- TOE (Platforms listed in the ST)
- Script *FAU_SEL.1.1.ps1* is available in TOE

66.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMVPN24SD] instructions in order to collect the results as stipulated by the supporting document [PPMVPN24SD].

66.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)

- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)

- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)

The results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms*.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

66.2.1.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 1 and Test 2** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1 and Test 2**.

66.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FAU_SEL.1.

67 FCS_CKM.1.1 (VPN)

The assurance activity for the **FCS_CKM.1.1 (VPN)** requirement is stated as follows:

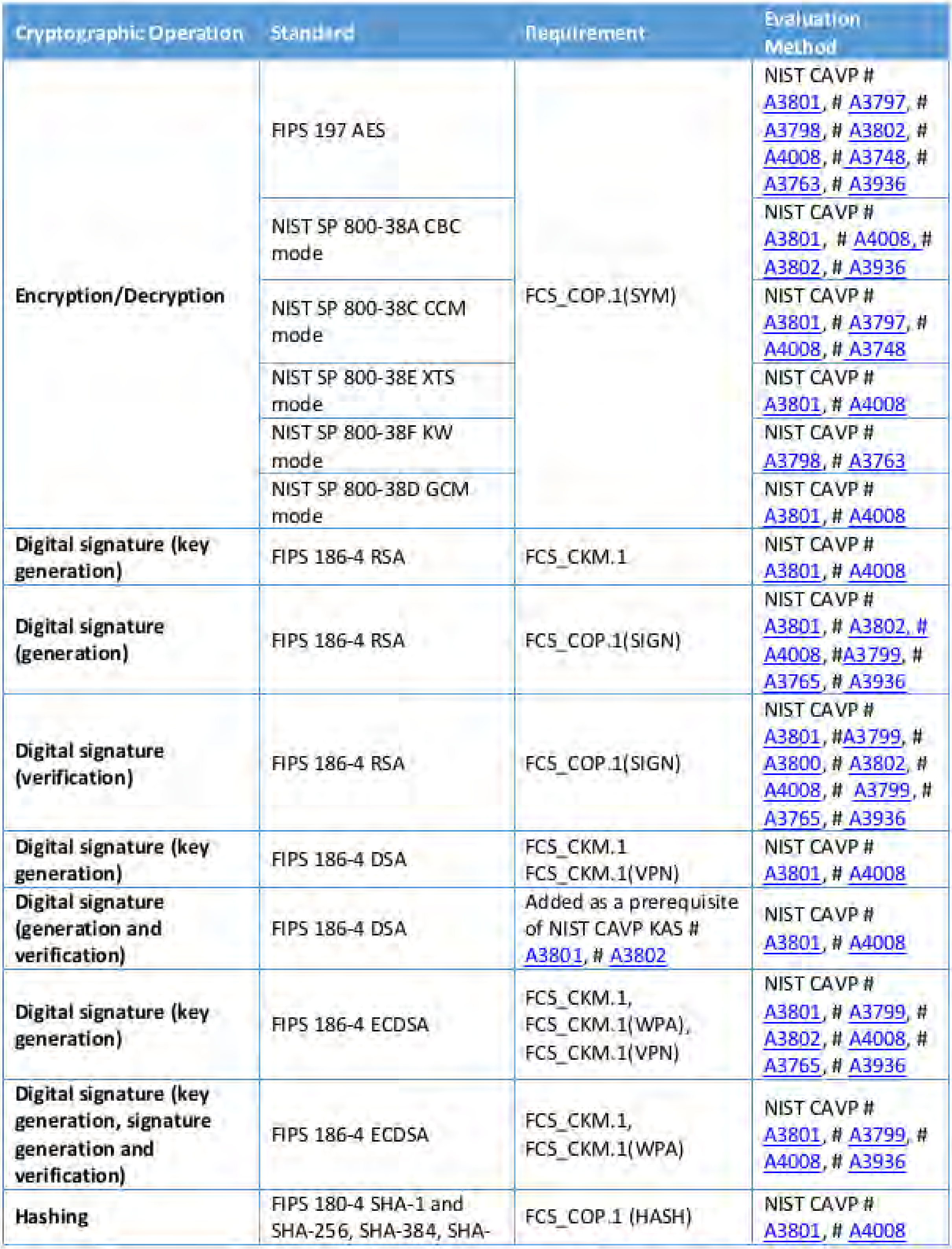
> **TSS**
>
> The evaluator shall examine the TSS to verify that it describes how the key generation functionality is invoked.
>
> **Operational Guidance**
>
> There are no AGD Assurance Activities for this requirement.
>
> **Test**
>
> There are no test Assurance Activities for this requirement.

67.1 Documentation Review activity

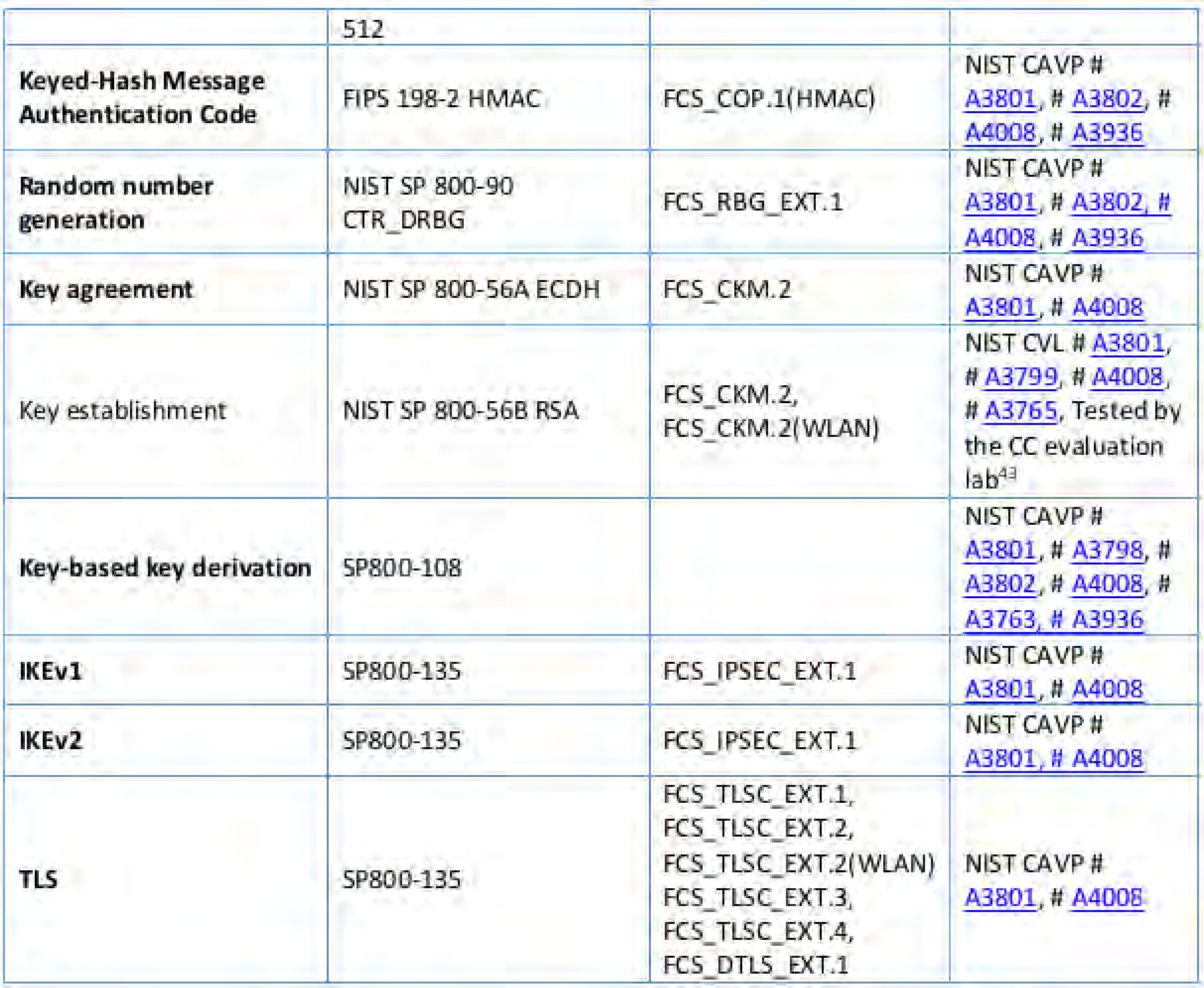
67.1.1 Findings

The evaluator has reviewed the ***Security Target*** document and the information provided in the TSS, section **6.2.1 Cryptographic Algorithms and Operations**. This section includes the following tables of the cryptographic algorithms supported by Windows 11, Windows 10, Windows Server 21H2, Windows Server 2022, Azure Stack HCIv2, Azure Stack Hub and Azure Stack Edge. These tables include the CAVP certificates associated for each TOE version.

67.1.1.1 Cryptographic Algorithm Standards and Evaluation Methods for Windows 11 (version 22H2)

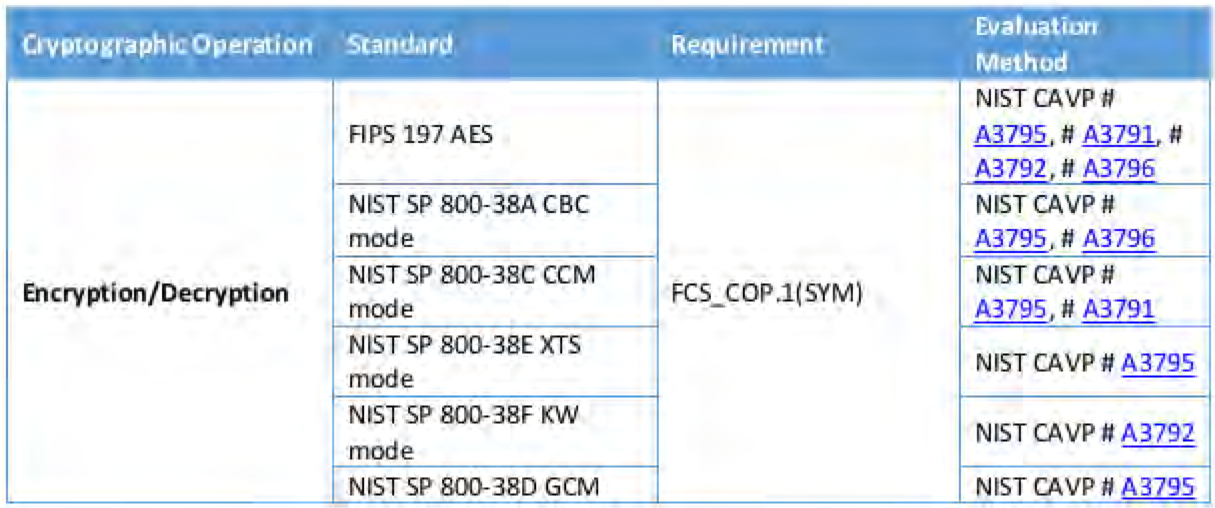


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3801, # A3797, # A3798, # A3802, # A4008, # A3748, # A3763, # A3936
	NIST SP 800-38A CBC mode		NIST CAVP # A3801, # A4008, # A3802, # A3936
	NIST SP 800-38C CCM mode		NIST CAVP # A3801, # A3797, # A4008, # A3748
	NIST SP 800-38E XTS mode		NIST CAVP # A3801, # A4008
	NIST SP 800-38F KW mode		NIST CAVP # A3798, # A3763
	NIST SP 800-38D GCM mode		NIST CAVP # A3801, # A4008
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP # A3801, # A4008
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3801, # A3802, # A4008, #A3799, # A3765, # A3936
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3801, #A3799, # A3800, # A3802, # A4008, # A3799, # A3765, # A3936
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3801, # A4008
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3801, # A3802	NIST CAVP # A3801, # A4008
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3801, # A3799, # A3802, # A4008, # A3765, # A3936
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3801, # A3799, # A4008, # A3936
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-	FCS_COP.1 (HASH)	NIST CAVP # A3801, # A4008

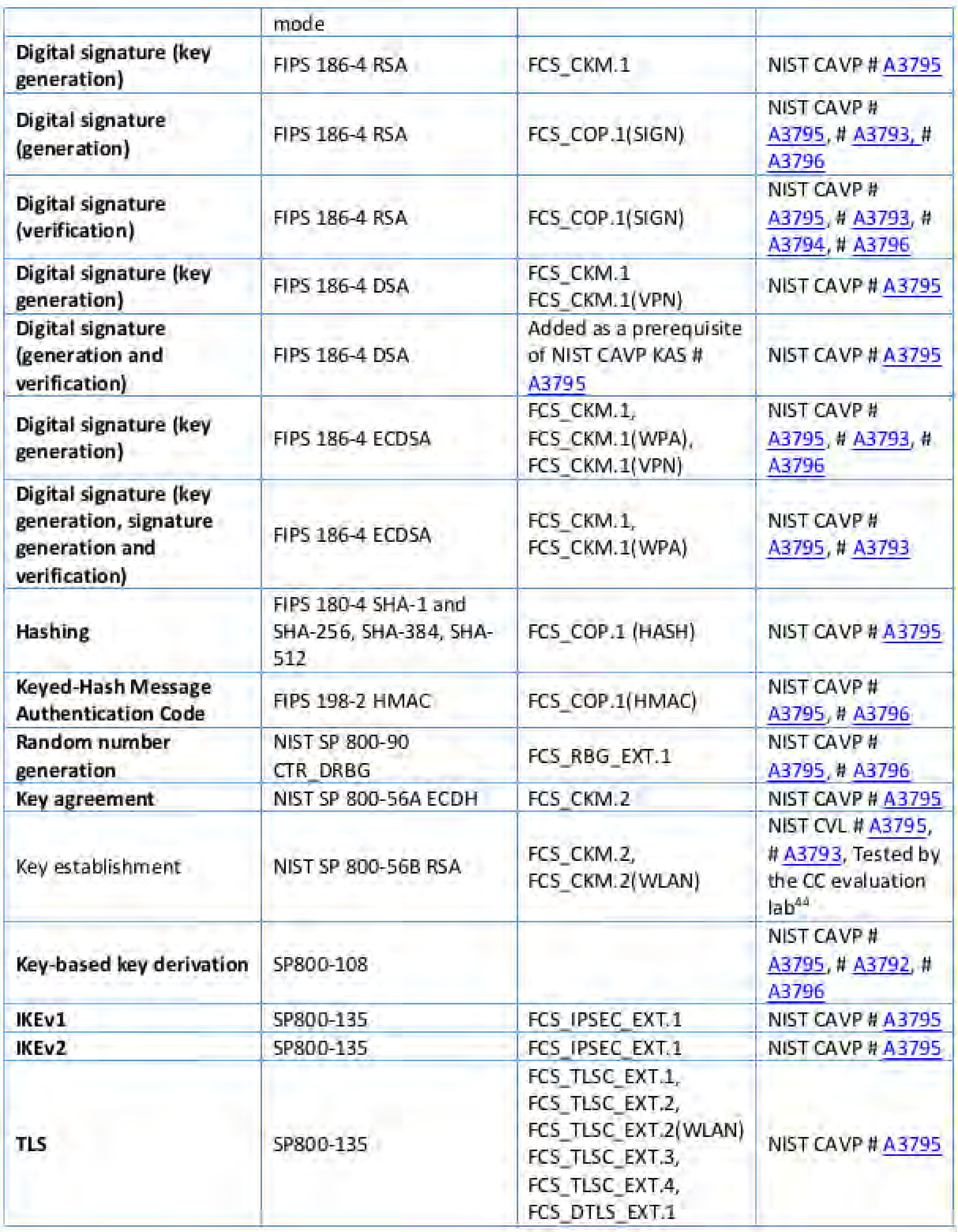


	512		
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3801, # A3802, # A4008, # A3936
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3801, # A3802, # A4008, # A3936
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3801, # A4008
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2, FCS_CKM.2(WLAN)	NIST CVL # A3801, # A3799, # A4008, # A3765, Tested by the CC evaluation lab[43]
Key-based key derivation	SP800-108		NIST CAVP # A3801, # A3798, # A3802, # A4008, # A3763, # A3936
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3801, # A4008
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3801, # A4008
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3801, # A4008

67.1.1.2 Cryptographic Algorithm Standards and Evaluation Methods for Windows 10 (version 22H2)

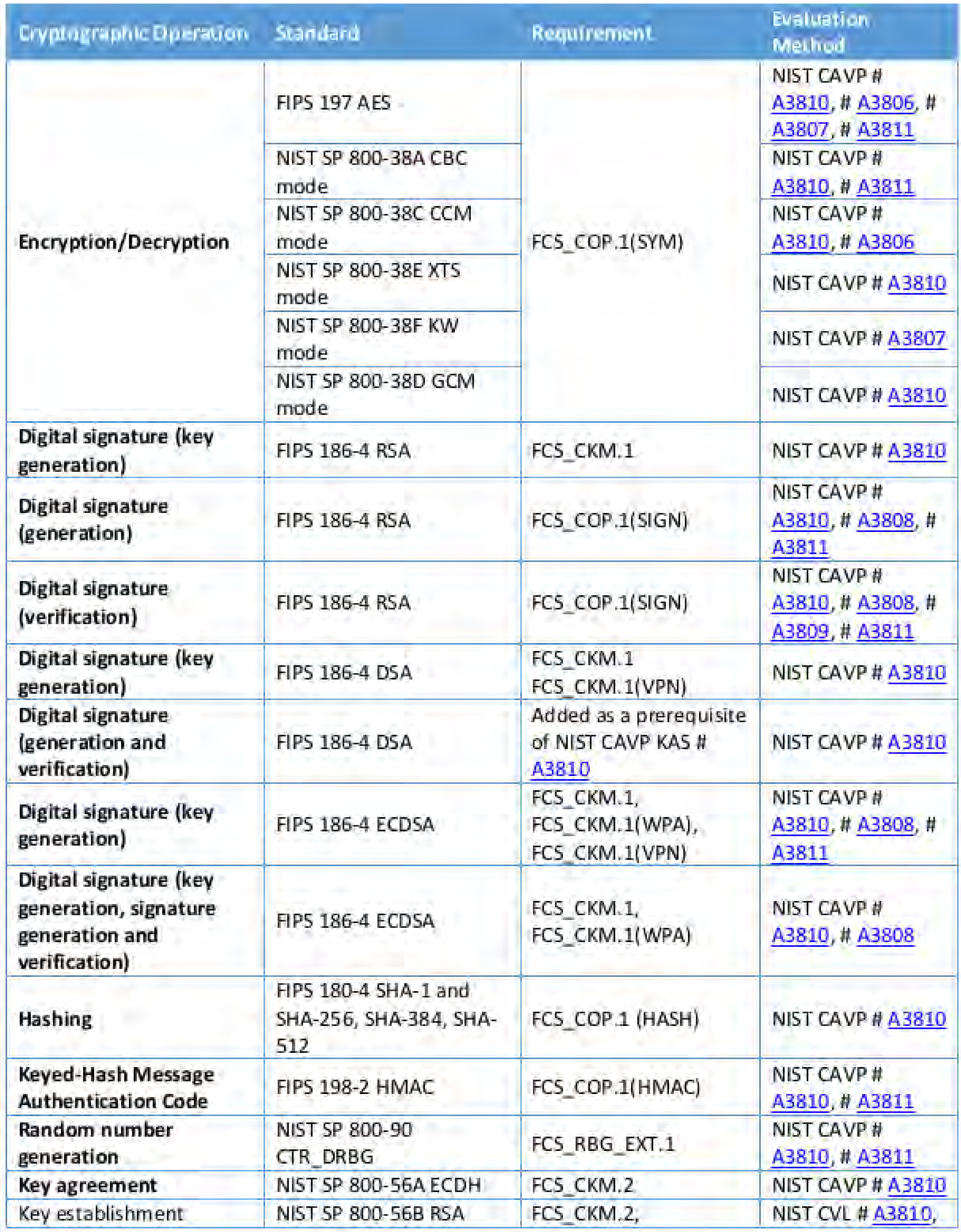


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3795, # A3791, # A3792, # A3796
	NIST SP 800-38A CBC mode		NIST CAVP # A3795, # A3796
	NIST SP 800-38C CCM mode		NIST CAVP # A3795, # A3791
	NIST SP 800-38E XTS mode		NIST CAVP # A3795
	NIST SP 800-38F KW mode		NIST CAVP # A3792
	NIST SP 800-38D GCM		NIST CAVP # A3795

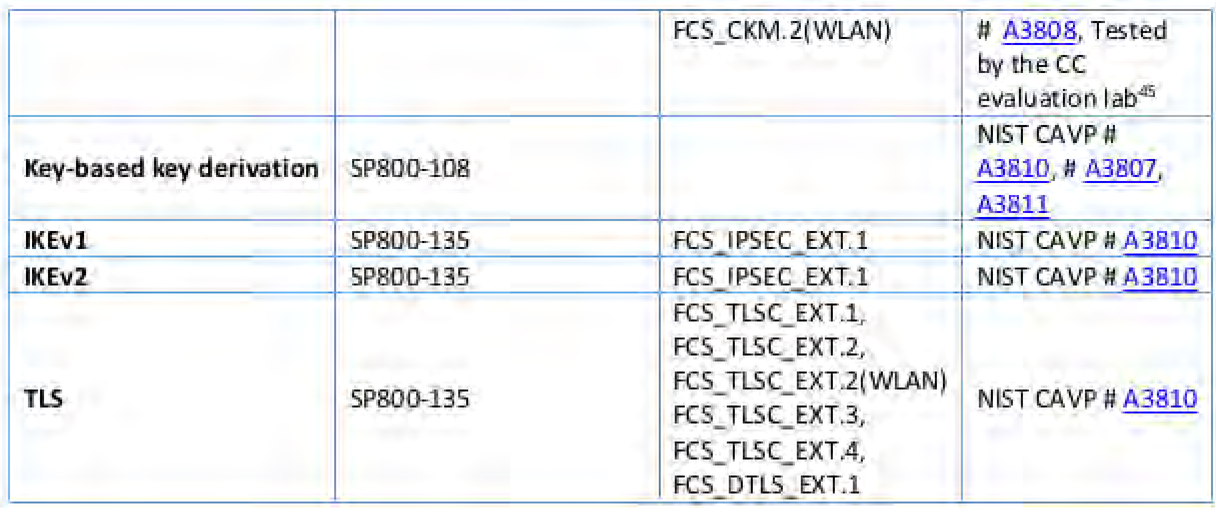


	mode		
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP # A3795
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3795, # A3793, # A3796
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3795, # A3793, # A3794, # A3796
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3795
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3795	NIST CAVP # A3795
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3795, # A3793, # A3796
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3795, # A3793
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3795
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3795, # A3796
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3795, # A3796
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3795
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2, FCS_CKM.2(WLAN)	NIST CVL # A3795, # A3793, Tested by the CC evaluation lab[44]
Key-based key derivation	SP800-108		NIST CAVP # A3795, # A3792, # A3796
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3795
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3795
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3795

67.1.1.3 Cryptographic Algorithm Standards and Evaluation Methods for Windows Server 2022 and Windows Server Datacenter: Azure Edition

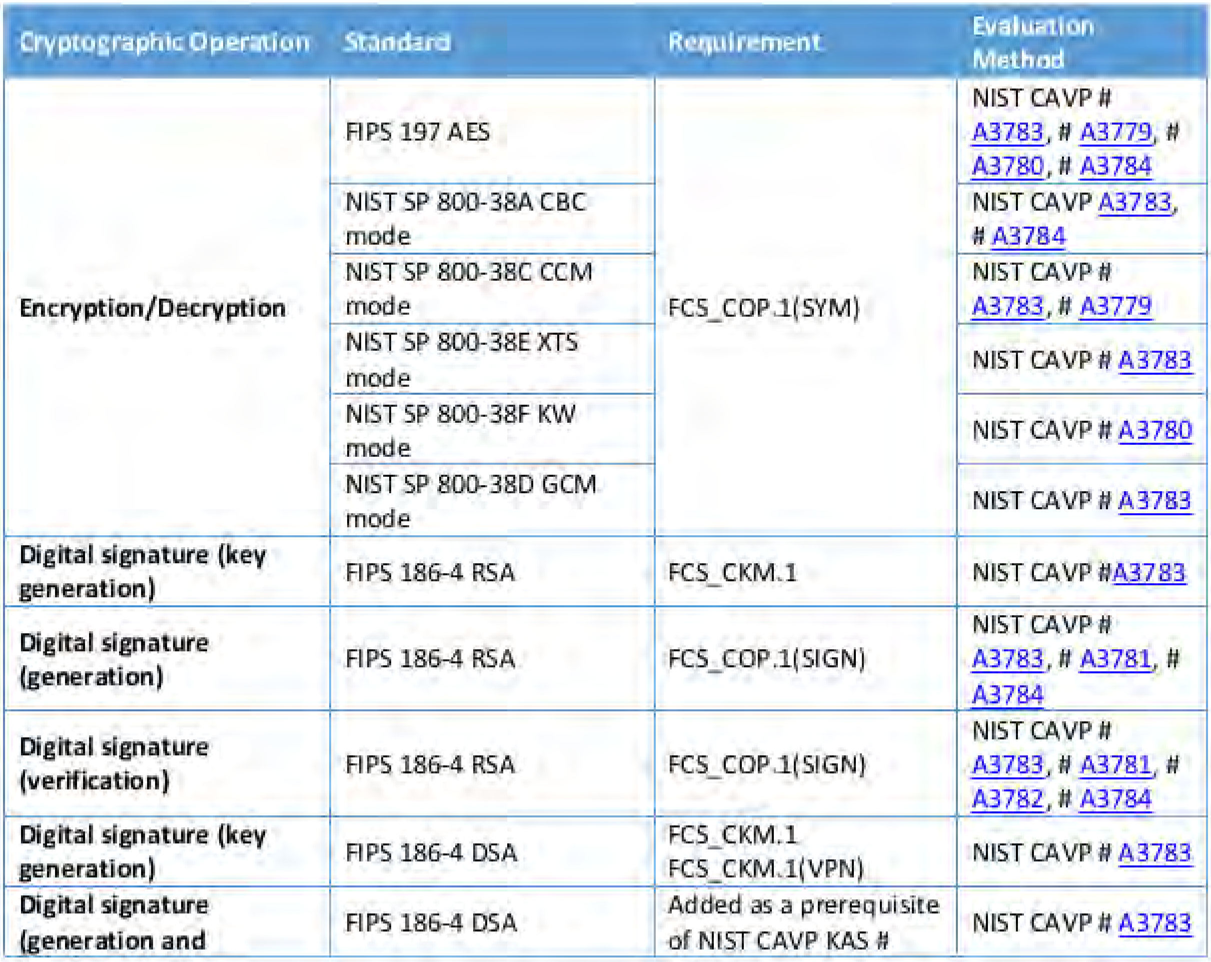


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3810, # A3806, # A3807, # A3811
	NIST SP 800-38A CBC mode		NIST CAVP # A3810, # A3811
	NIST SP 800-38C CCM mode		NIST CAVP # A3810, # A3806
	NIST SP 800-38E XTS mode		NIST CAVP # A3810
	NIST SP 800-38F KW mode		NIST CAVP # A3807
	NIST SP 800-38D GCM mode		NIST CAVP # A3810
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP # A3810
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3810, # A3808, # A3811
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3810, # A3808, # A3809, # A3811
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3810
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3810	NIST CAVP # A3810
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3810, # A3808, # A3811
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3810, # A3808
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3810
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3810, # A3811
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3810, # A3811
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3810
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2,	NIST CVL # A3810,

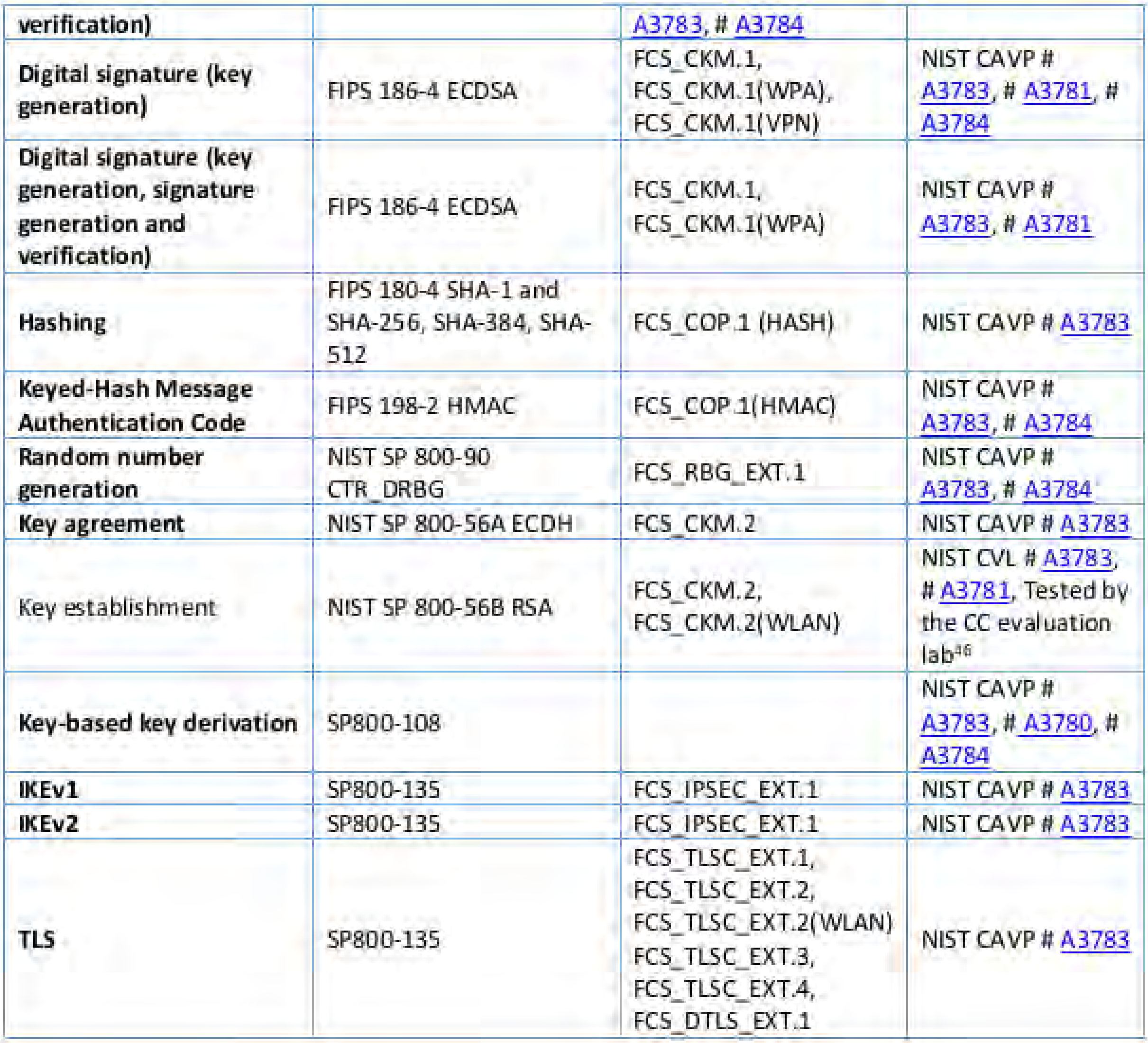


		FCS_CKM.2(WLAN)	# A3808, Tested by the CC evaluation lab[45]
Key-based key derivation	SP800-108		NIST CAVP # A3810, # A3807, A3811
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3810
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3810
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3810

67.1.1.4 Cryptographic Algorithm Standards and Evaluation Methods for Windows Server Azure Stack HCIv2 version 22H2

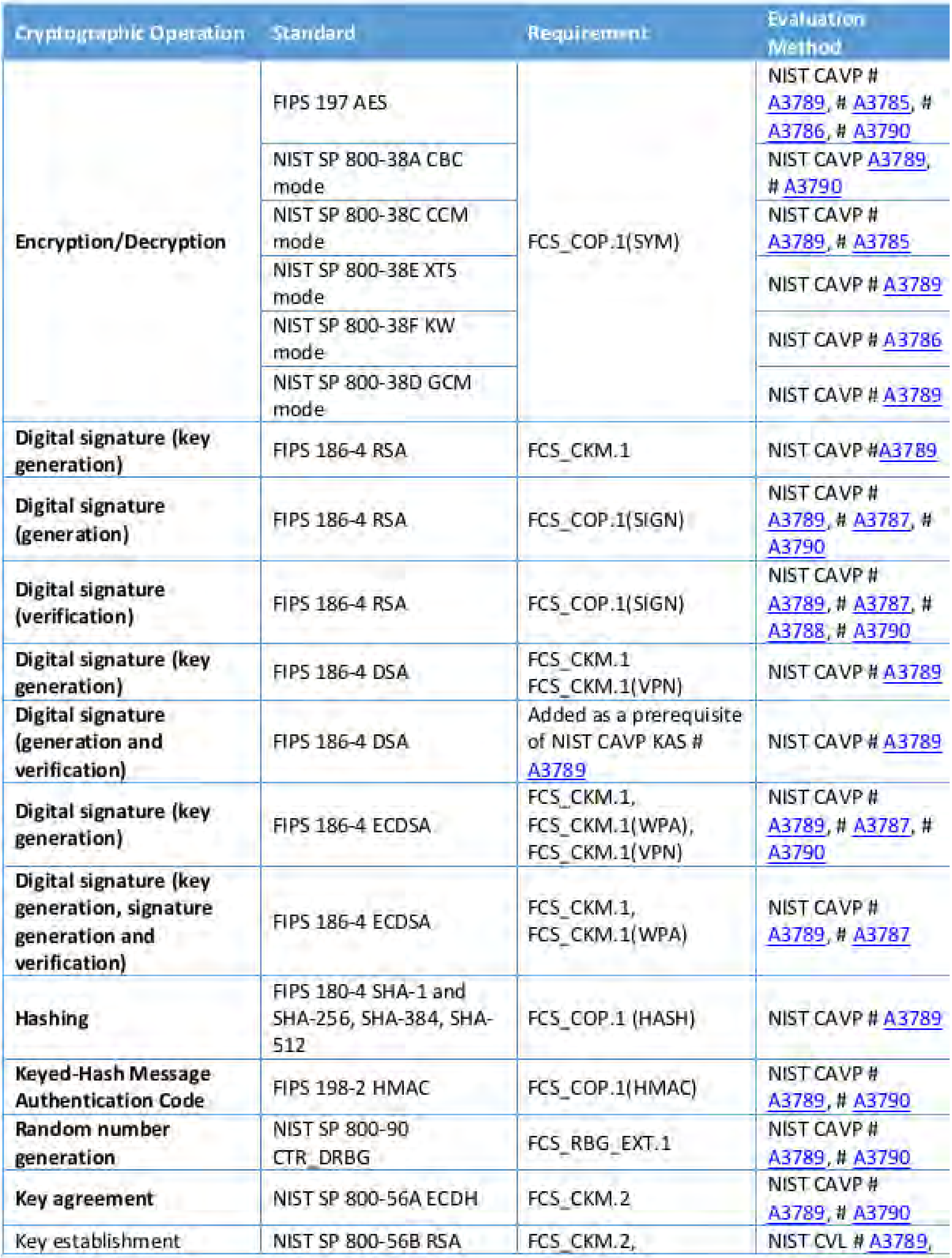


Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3783, # A3779, # A3780, # A3784
	NIST SP 800-38A CBC mode		NIST CAVP A3783, # A3784
	NIST SP 800-38C CCM mode		NIST CAVP # A3783, # A3779
	NIST SP 800-38E XTS mode		NIST CAVP # A3783
	NIST SP 800-38F KW mode		NIST CAVP # A3780
	NIST SP 800-38D GCM mode		NIST CAVP # A3783
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP #A3783
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3783, # A3781, # A3784
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3783, # A3781, # A3782, # A3784
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3783
Digital signature (generation and	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS #	NIST CAVP # A3783

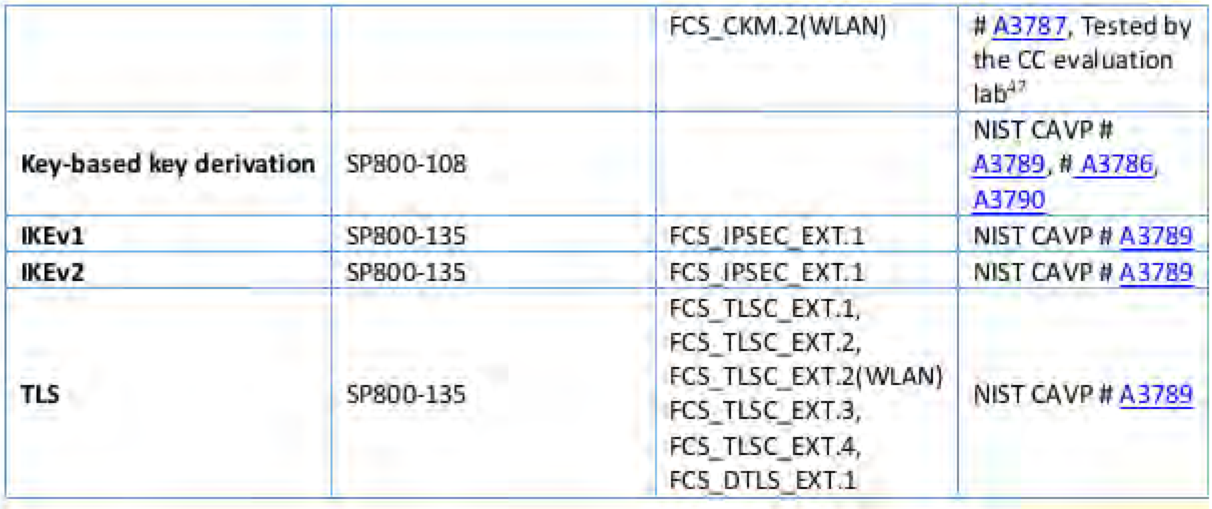


verification)		A3783, # A3784	
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3783, # A3781, # A3784
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3783, # A3781
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3783
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3783, # A3784
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3783, # A3784
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3783
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2, FCS_CKM.2(WLAN)	NIST CVL # A3783, # A3781, Tested by the CC evaluation lab[46]
Key-based key derivation	SP800-108		NIST CAVP # A3783, # A3780, # A3784
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3783
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3783
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3783

67.1.1.5 Cryptographic Algorithm Standards and Evaluation Methods for Azure Stack Hub and Azure Stack Edge



Cryptographic Operation	Standard	Requirement	Evaluation Method
Encryption/Decryption	FIPS 197 AES	FCS_COP.1(SYM)	NIST CAVP # A3789, # A3785, # A3786, # A3790
	NIST SP 800-38A CBC mode		NIST CAVP A3789, # A3790
	NIST SP 800-38C CCM mode		NIST CAVP # A3789, # A3785
	NIST SP 800-38E XTS mode		NIST CAVP # A3789
	NIST SP 800-38F KW mode		NIST CAVP # A3786
	NIST SP 800-38D GCM mode		NIST CAVP # A3789
Digital signature (key generation)	FIPS 186-4 RSA	FCS_CKM.1	NIST CAVP #A3789
Digital signature (generation)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3789, # A3787, # A3790
Digital signature (verification)	FIPS 186-4 RSA	FCS_COP.1(SIGN)	NIST CAVP # A3789, # A3787, # A3788, # A3790
Digital signature (key generation)	FIPS 186-4 DSA	FCS_CKM.1 FCS_CKM.1(VPN)	NIST CAVP # A3789
Digital signature (generation and verification)	FIPS 186-4 DSA	Added as a prerequisite of NIST CAVP KAS # A3789	NIST CAVP # A3789
Digital signature (key generation)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA), FCS_CKM.1(VPN)	NIST CAVP # A3789, # A3787, # A3790
Digital signature (key generation, signature generation and verification)	FIPS 186-4 ECDSA	FCS_CKM.1, FCS_CKM.1(WPA)	NIST CAVP # A3789, # A3787
Hashing	FIPS 180-4 SHA-1 and SHA-256, SHA-384, SHA-512	FCS_COP.1 (HASH)	NIST CAVP # A3789
Keyed-Hash Message Authentication Code	FIPS 198-2 HMAC	FCS_COP.1(HMAC)	NIST CAVP # A3789, # A3790
Random number generation	NIST SP 800-90 CTR_DRBG	FCS_RBG_EXT.1	NIST CAVP # A3789, # A3790
Key agreement	NIST SP 800-56A ECDH	FCS_CKM.2	NIST CAVP # A3789, # A3790
Key establishment	NIST SP 800-56B RSA	FCS_CKM.2,	NIST CVL # A3789,



		FCS_CKM.2(WLAN)	# A3787, Tested by the CC evaluation lab[47]
Key-based key derivation	SP800-108		NIST CAVP # A3789, # A3786, A3790
IKEv1	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3789
IKEv2	SP800-135	FCS_IPSEC_EXT.1	NIST CAVP # A3789
TLS	SP800-135	FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.2(WLAN) FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1	NIST CAVP # A3789

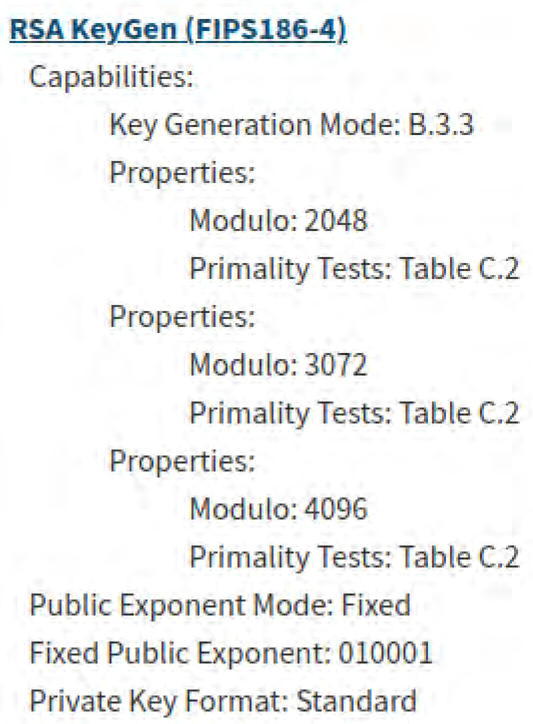
The ***Operational Guidance*** document, states that for the evaluated version the following security policy needs to be applied (Section 3.2.5):

- Local Policies \ Security Options\System cryptography: Use FIPS 140 compliant cryptographic algorithms, including encryption, hashing and signing algorithm.

After applying this policy, only FIPS certified algorithms can be used, including the key generation algorithms defined in the table above.

As part of the testing activity described below, the correctness of the cryptographic functionality has been demonstrated against the BOTAN tool. However, ffdhe groups are not available in BOTAN, and the laboratory has verified the implementation against the CAVP tool. Below, the CAVP certificates granted for this functionality are listed (extracted from the tables above)

67.1.1.6 Windows 11 version 22H2 (CAVP Cert. #A4008)



RSA KeyGen (FIPS186-4)

Capabilities:

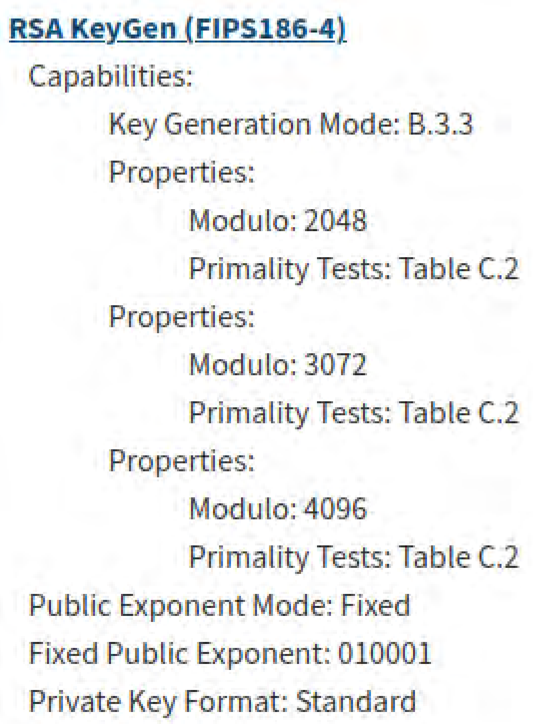
- Key Generation Mode: B.3.3
- Properties:
  - Modulo: 2048
  - Primality Tests: Table C.2
- Properties:
  - Modulo: 3072
  - Primality Tests: Table C.2
- Properties:
  - Modulo: 4096
  - Primality Tests: Table C.2

Public Exponent Mode: Fixed

Fixed Public Exponent: 010001

Private Key Format: Standard

67.1.1.7 Windows 10 version 22H2(CAVP Cert. #A3795)



RSA KeyGen (FIPS186-4)

Capabilities:

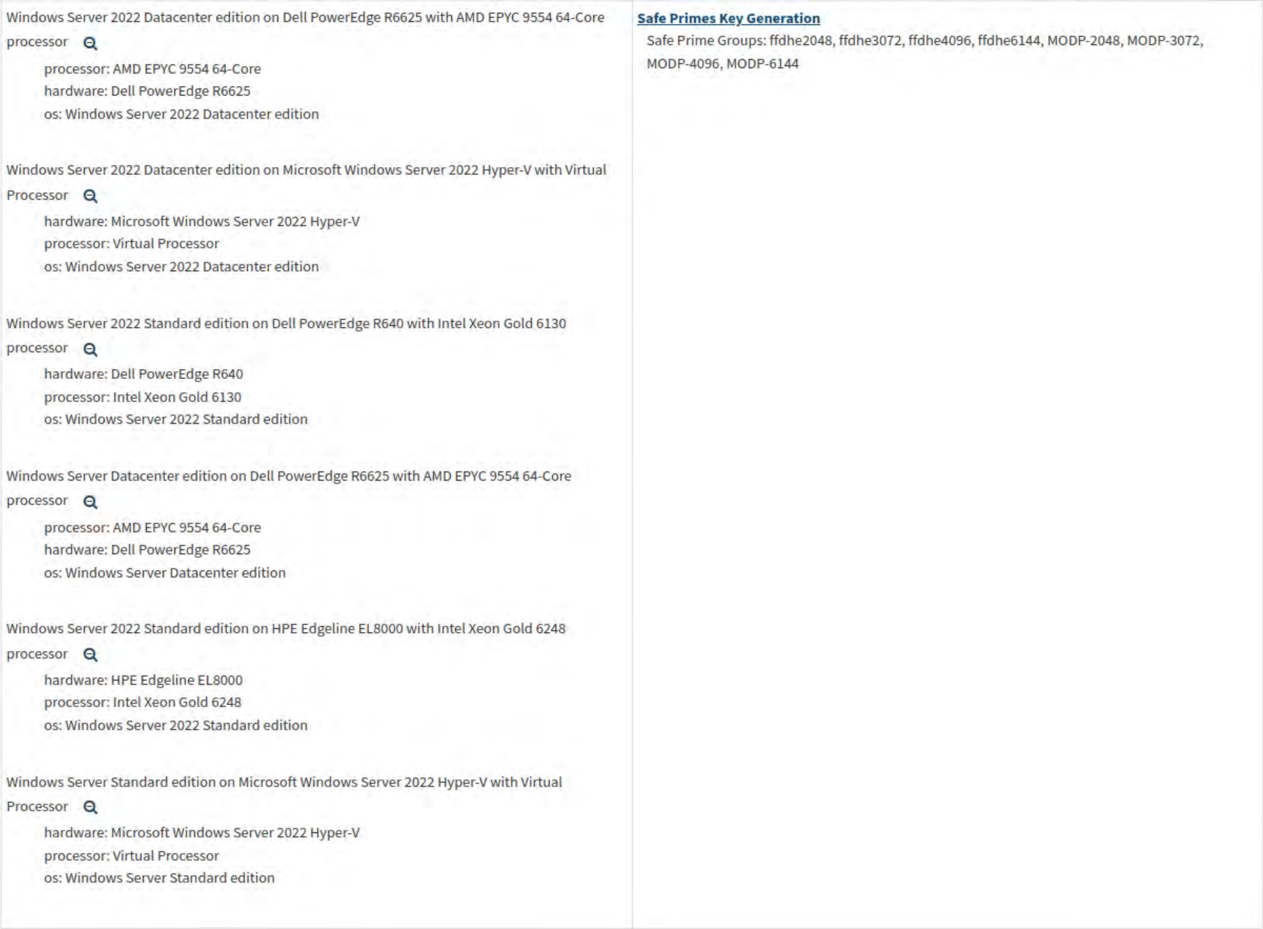
- Key Generation Mode: B.3.3
- Properties:
  - Modulo: 2048
  - Primality Tests: Table C.2
- Properties:
  - Modulo: 3072
  - Primality Tests: Table C.2
- Properties:
  - Modulo: 4096
  - Primality Tests: Table C.2

Public Exponent Mode: Fixed

Fixed Public Exponent: 010001

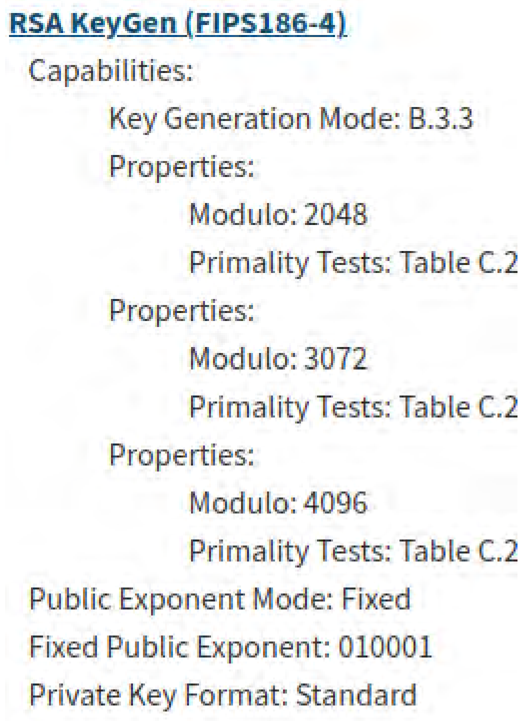
Private Key Format: Standard

67.1.1.8 Windows Server 2022 and Windows Server Datacenter: Azure Edition (CAVP Cert. #A4009)



Windows Server 2022 Datacenter edition on Dell PowerEdge R6625 with AMD EPYC 9554 64-Core processor processor: AMD EPYC 9554 64-Core hardware: Dell PowerEdge R6625 os: Windows Server 2022 Datacenter edition Windows Server 2022 Datacenter edition on Microsoft Windows Server 2022 Hyper-V with Virtual Processor hardware: Microsoft Windows Server 2022 Hyper-V processor: Virtual Processor os: Windows Server 2022 Datacenter edition Windows Server 2022 Standard edition on Dell PowerEdge R640 with Intel Xeon Gold 6130 processor hardware: Dell PowerEdge R640 processor: Intel Xeon Gold 6130 os: Windows Server 2022 Standard edition Windows Server Datacenter edition on Dell PowerEdge R6625 with AMD EPYC 9554 64-Core processor processor: AMD EPYC 9554 64-Core hardware: Dell PowerEdge R6625 os: Windows Server Datacenter edition Windows Server 2022 Standard edition on HPE Edgeline EL8000 with Intel Xeon Gold 6248 processor hardware: HPE Edgeline EL8000 processor: Intel Xeon Gold 6248 os: Windows Server 2022 Standard edition Windows Server Standard edition on Microsoft Windows Server 2022 Hyper-V with Virtual Processor hardware: Microsoft Windows Server 2022 Hyper-V processor: Virtual Processor os: Windows Server Standard edition	**Safe Primes Key Generation** Safe Prime Groups: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, MODP-2048, MODP-3072, MODP-4096, MODP-6144

67.1.1.9 Windows Server Azure Stack HCIv2 version 22H2 (CAVP Cert. #A3783)



RSA KeyGen (FIPS186-4)

Capabilities:

Key Generation Mode: B.3.3

Properties:

Modulo: 2048

Primality Tests: Table C.2

Properties:

Modulo: 3072

Primality Tests: Table C.2

Properties:

Modulo: 4096

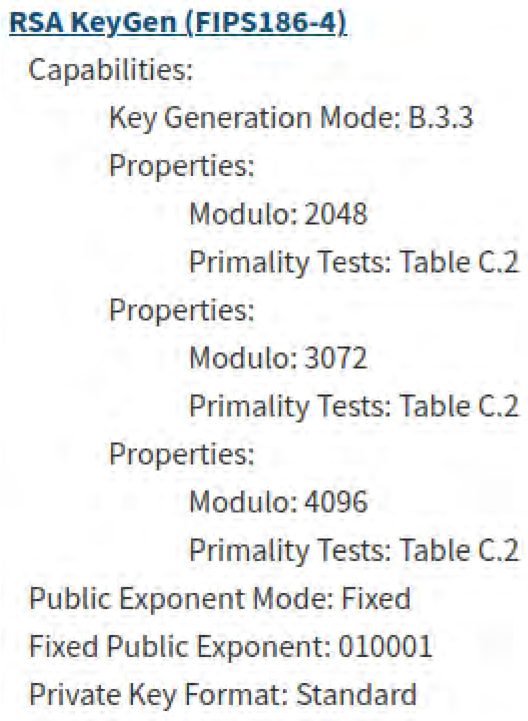
Primality Tests: Table C.2

Public Exponent Mode: Fixed

Fixed Public Exponent: 010001

Private Key Format: Standard

67.1.1.10 Azure Stack Hub and Azure Stack Edge (CAVP Cert. #A3789)



RSA KeyGen (FIPS186-4)

Capabilities:

Key Generation Mode: B.3.3

Properties:

Modulo: 2048

Primality Tests: Table C.2

Properties:

Modulo: 3072

Primality Tests: Table C.2

Properties:

Modulo: 4096

Primality Tests: Table C.2

Public Exponent Mode: Fixed

Fixed Public Exponent: 010001

Private Key Format: Standard

67.1.2 Verdict

The evaluator considers that the TSS identifies the key sizes supported by the OS for every algorithm through its NIST certificates. Moreover, all the key generation algorithms (whose purpose is to be used as part of digital signatures processes) follow the same standard (*FIPS 186-4*).

The ***Operational Guidance*** document, defines the FIPS security policy to be applied. Once this policy is applied, only the approved key generation method described above can be used. No further configuration is needed to generate keys following the *Appendix B.1*, *B.3* and *B.4* of the *FIPS-PUB 186-4* standard.

Hence, the **PASS** verdict is assigned to the documentation review activity.

67.2 Test Activity

The assurance activity does not require any testing activities for this requirement.

67.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FCS_CKM.1.1 (VPN).

68 FCS_CKM.2.1

The assurance activity for the **FCS_CKM.2.1** requirement is stated as follows:

> **TSS**
>
> Regardless of whether this requirement is met by the VPN client or the OS, the evaluator will check the TSS to ensure that it lists each persistent secret (credential, secret key) and private key needed to meet the requirements in the ST. For each of these items, the evaluator will confirm that the TSS lists for what purpose it is used, and how it is stored.
>
> The evaluator shall review the TSS for to determine that it makes a case that, for each item listed as being manipulated by the VPN client, it is not written unencrypted to persistent memory, and that the item is stored by the OS.
>
> **Operational Guidance**
>
> There are no AGD Assurance Activities for this requirement.
>
> **Test**
>
> There are no test Assurance Activities for this requirement.

68.1 Documentation Review activity

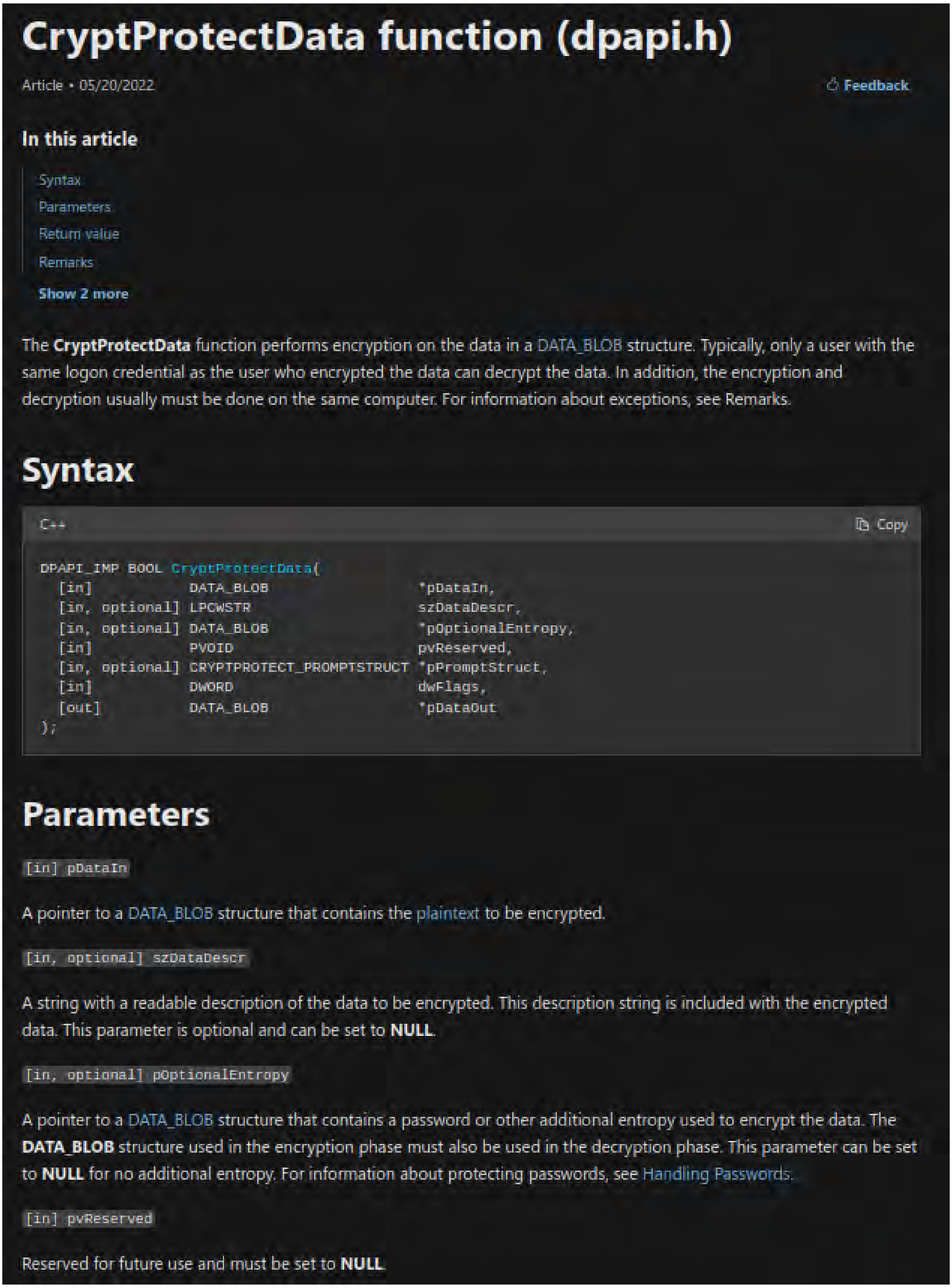
68.1.1 Findings

The evaluator has reviewed the section **6.2.4. Protecting Data with DPAPI** of the ***Security Target*** document. This section states that Windows provides the *Data Protection API*, CNG DPAPI, which can be used to protect any persistent secret and private keys which the developer deems to be sensitive.

DPAPI uses the *AES-CBC* algorithm to encrypt and decrypt the sensitive information. Once the sensitive information has been encrypted, it is stored in a directory which is part of the user's profile.

DPAPI provides two functions to encrypt (*CryptProtectData* function) and decrypt (*CryptUnprotectData* function) data. This section of the TSS also includes a link to the Microsoft Developer Network (*MSDN*) where detailed information about the usage of these API functions is provided. The following images, which have been obtained from the *MSDN* website, describe the syntax of these API functions:

CryptProtectData:



CryptProtectData function (dpapi.h)

Article • 05/20/2022

In this article

- Syntax
- Parameters
- Return value
- Remarks

Show 2 more

The **CryptProtectData** function performs encryption on the data in a DATA_BLOB structure. Typically, only a user with the same logon credential as the user who encrypted the data can decrypt the data. In addition, the encryption and decryption usually must be done on the same computer. For information about exceptions, see Remarks.

Syntax

```
DPAPI_IMP BOOL CryptProtectData(
  [in]           DATA_BLOB                 *pDataIn,
  [in, optional] LPCWSTR                   szDataDescr,
  [in, optional] DATA_BLOB                 *pOptionalEntropy,
  [in]           PVOID                     pvReserved,
  [in, optional] CRYPTPROTECT_PROMPTSTRUCT *pPromptStruct,
  [in]           DWORD                     dwFlags,
  [out]          DATA_BLOB                 *pDataOut
);
```

Parameters

`[in] pDataIn`

A pointer to a DATA_BLOB structure that contains the plaintext to be encrypted.

`[in, optional] szDataDescr`

A string with a readable description of the data to be encrypted. This description string is included with the encrypted data. This parameter is optional and can be set to **NULL**.

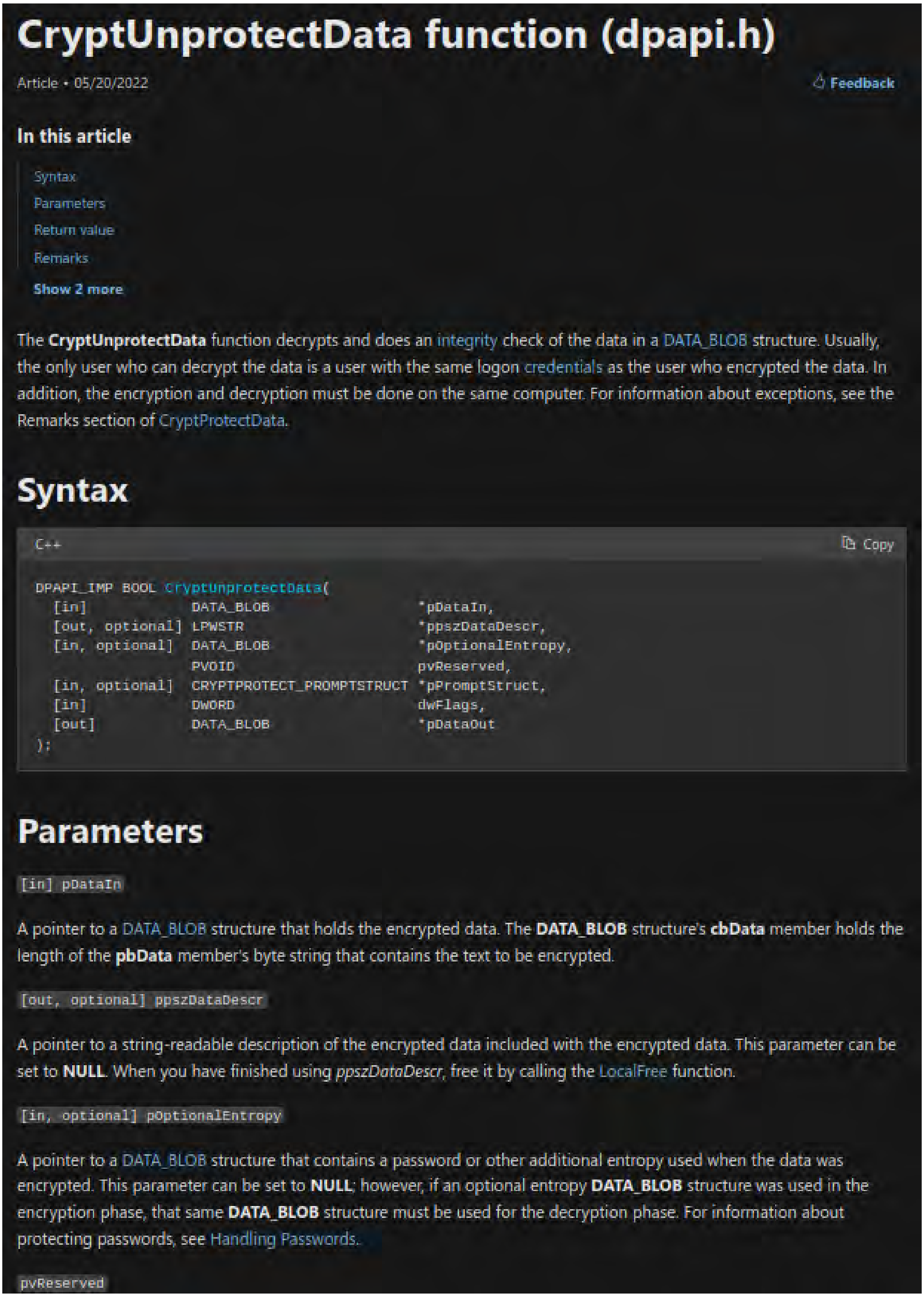
`[in, optional] pOptionalEntropy`

A pointer to a DATA_BLOB structure that contains a password or other additional entropy used to encrypt the data. The **DATA_BLOB** structure used in the encryption phase must also be used in the decryption phase. This parameter can be set to **NULL** for no additional entropy. For information about protecting passwords, see Handling Passwords.

`[in] pvReserved`

Reserved for future use and must be set to **NULL**.

CryptUnprotectData:



CryptUnprotectData function (dpapi.h)

Article • 05/20/2022

In this article

- Syntax
- Parameters
- Return value
- Remarks

Show 2 more

The **CryptUnprotectData** function decrypts and does an integrity check of the data in a DATA_BLOB structure. Usually, the only user who can decrypt the data is a user with the same logon credentials as the user who encrypted the data. In addition, the encryption and decryption must be done on the same computer. For information about exceptions, see the Remarks section of CryptProtectData.

Syntax

C++

```
DPAPI_IMP BOOL CryptUnprotectData(
  [in]            DATA_BLOB                 *pDataIn,
  [out, optional] LPWSTR                    *ppszDataDescr,
  [in, optional]  DATA_BLOB                 *pOptionalEntropy,
                  PVOID                     pvReserved,
  [in, optional]  CRYPTPROTECT_PROMPTSTRUCT *pPromptStruct,
  [in]            DWORD                     dwFlags,
  [out]           DATA_BLOB                 *pDataOut
);
```

Parameters

`[in] pDataIn`

A pointer to a DATA_BLOB structure that holds the encrypted data. The **DATA_BLOB** structure's **cbData** member holds the length of the **pbData** member's byte string that contains the text to be encrypted.

`[out, optional] ppszDataDescr`

A pointer to a string-readable description of the encrypted data included with the encrypted data. This parameter can be set to **NULL**. When you have finished using *ppszDataDescr*, free it by calling the LocalFree function.

`[in, optional] pOptionalEntropy`

A pointer to a DATA_BLOB structure that contains a password or other additional entropy used when the data was encrypted. This parameter can be set to **NULL**; however, if an optional entropy **DATA_BLOB** structure was used in the encryption phase, that same **DATA_BLOB** structure must be used for the decryption phase. For information about protecting passwords, see Handling Passwords.

`pvReserved`

68.1.2 Verdict

The evaluator considers that the TSS provides enough information related to the method used for persistent secrets and private keys storage. The vendor states that any persistent data which the developer deems to be sensitive can be protected using DPAPI. After protecting the data, the information is stored in a directory inside the user's profile.

The vendor has also identified the available interfaces for data protection (*CryptProtectData* and *CryptUnprotectData*), as well as the cryptographic algorithm used, AES-256-CBC, which is one of the selected in the FCS_COP.1(SYM) requirement.

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfilment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

68.2 Test Activity

The assurance activity does not require any testing activities for this requirement.

68.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FCS_CKM.2.1.

69 FCS_EAP_EXT.1

The assurance activity for the **FCS_EAP_EXT.1** requirement is stated as follows:

> The evaluator shall verify that the guidance documents describe any configurable features of the EAP or TLS functionality, including instructions for configuration of the authenticators and registration processes for clients.
>
> The evaluator shall perform the following test(s) based on the selections chosen:
>
> - **Test 1:** The evaluator shall follow AGD guidance to configure the TSF to use the EAP method claimed. The evaluator shall follow AGD guidance to configure the TSF to use the authentication method claimed and, for EAP-TTLS, register a client with the appropriate key material required for the authentication method. The evaluator shall establish an VPN session using a test client with a valid certificate and, for EAP-TTLS, configured to provide a correct value for the configured authenticator. The evaluator shall observe the the VPN session is successful.
> - **Test 2 (conditional for EAP-TTLS support):** The evaluator shall cause the test client with a valid certificate to send an invalid authenticator for the claimed authentication method: For HOTP, replay the HOTP value sent previously, For TOTP or PSK, modify a byte of the properly constructed value, and observe that the TSF aborts the session.
> - **Test 3:** The evaluator shall establish a new, valid certificate for a test client using an identifier not corresponding to a registered user. For EAP-TTLS, the evaluator shall cause the test client using this certificate to send a correct authenticator value for the registered user. The evaluator shall initiate a VPN session from the test client to the TSF and observe that the TSF aborts the session.
> - **Test 4:** The evaluator shall follow AGD guidance to configure the TSF to use a supported EAP method and register the user with the key material required for a supported authentication method. The evaluator shall configure a test client to respond to an IKEv2 exchange with EAP-request, providing valid phase 1 handshake and valid TLS handshake, but computing the phase 2 shared key using standard (non-EAP) methods. The evaluator shall initiate a VPN session between the test client and the TSF, and observe that the TSF aborts the session.

69.1 Documentation Review activity

69.1.1 Findings

The ***Operational Guidance*** document, defines in its section **4.2.3.2 Configuring certificate validation for EAP-TLS**, that Windows supports EAP-TLS and how to configure it using *rasphone.exe*

Moreover, section **4.3.3 Available EAP-TLS ciphersuites** shows a table with the ciphersuites available.

69.1.2 Verdict

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfillment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

69.2 Test Activity

For this case, all the auditable events will be obtained during the test execution of each security functional requirement.

69.2.1 Test 1, Test 2, Test 3 and Test 4

69.2.1.1 Setup

- The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:
  - Testing Machine (Debian 11 Bullseye, using Strongswan U5.9.1/K5.10)
  - Client Machine (Platforms listed in the ST)
  - Scripts FCS_EAP_EXT.1.1.ps1 and deploy_vpn.sh are available in TOE

  Both machines are in the same network with the following configuration:

  - Testing Machine, IP = 20.20.20.100
  - Windows Client Machine, IP = 20.20.20.50

69.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, en-

suring compliance with the supporting document [PPMVPN24SD] instructions in order to collect the results as stipulated by the supporting document [PPMVPN24SD].

69.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)
- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- HPE Edgeline EL8000 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

The results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms*.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE’s behavior is as expected and detailed in the security target [ST004].

69.2.1.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 1, Test 2, Test 3 and Test4** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1, Test 2, Test 3 & Test 4**.

69.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FCS_EAP_EXT.1

70 FCS_IPSEC_EXT.1.1

The assurance activity for the **FCS_IPSEC_EXT.1.1** requirement is stated as follows:

> The evaluator shall examine the TSS and determine that it describes how the IPsec capabilities are implemented.
>
> If the TOE is a standalone software application, the evaluator shall ensure that the TSS asserts that all IPsec functionality is implemented by the TSF. The evaluator shall also ensure that the TSS identifies what platform functionality the TSF relies upon to support its IPsec implementation, if any (e.g. does it invoke cryptographic primitive functions from the platform's cryptographic library, enforcement of packet routing decisions by low- level network drivers).
>
> If the TOE is part of a general-purpose desktop or mobile OS, the evaluator shall ensure that the TSS describes at a high level the architectural relationship between the VPN client portion of the TOE and the rest of the TOE (e.g. is the VPN client an integrated part of the OS or is it a standalone executable that is bundled into the OS package). If the SPD is implemented by the underlying platform in this case, then the TSS describes how the client interacts with the platform to establish and populate the SPD, including the identification of the platform's interfaces that are used by the client.
>
> In all cases, the evaluator shall also ensure that the TSS describes how the client interacts with the network stack of the platforms on which it can run (e.g., does the client insert itself within the stack via kernel mods, does the client simply invoke APIs to gain access to network services).
>
> The evaluator shall ensure that the TSS describes how the SPD is implemented and the rules for processing both inbound and outbound packets in terms of the IPsec policy. The TSS describes the rules that are available and the resulting actions available after matching a rule. The TSS describes how the available rules and actions form the SPD using terms defined in RFC 4301 such as BYPASS (e.g., no encryption), DISCARD (e.g., drop the packet), and PROTECT (e.g., encrypt the packet) actions defined in RFC 4301. As noted in section 4.4.1 of RFC 4301, the processing of entries in the SPD is non-trivial and the evaluator shall determine that the description in the TSS is sufficient to determine which rules will be applied given the rule structure implemented by the TOE. For example, if the TOE allows specification of ranges, conditional rules, etc., the evaluator shall determine that the description of rule processing (for both inbound and outbound packets) is sufficient to determine the action that will be applied, especially in the case where two different rules may apply. This description shall cover both the initial packets (that is, no SA is established on the interface or for that particular packet) as well as packets that are part of an established SA.
>
> **Operational Guidance**

The evaluator shall examine the operational guidance to verify it describes how the SPD is created and configured. If there is an administrative interface to the client, then the guidance describes how the administrator specifies rules for processing a packet. The description includes all three cases - a rule that ensures packets are encrypted/decrypted, dropped, and allowing a packet to flow in plaintext. The evaluator shall determine that the description in the operational guidance is consistent with the description in the TSS, and that the level of detail in the operational guidance is sufficient to allow the administrator to set up the SPD in an unambiguous fashion. This includes a discussion of how ordering of rules impacts the processing of an IP packet.

If the client is configured by an external application, such as the VPN gateway, then the operational guidance should indicate this and provide a description of how the client is configured by the external application. The description should contain information as to how the SPD is established and set up in an unambiguous fashion. The description should also include what is configurable via the external application, how ordering of entries may be expressed, as well as the impacts that ordering of entries may have on the packet processing.

In either case, the evaluator ensures the description provided In the TSS is consistent with the capabilities and description provided in the operational guidance.

Test

Depending on the implementation, the evaluator may be required to use a VPN gateway or some form of application to configure the client and platform. For Test 2, the evaluator is required to choose an application that allows for the configuration of the full set of capabilities of the VPN client (in conjunction with the platform). For example, if the client provides a robust interface that allows for specification of wildcards, subnets, etc., it is unacceptable for the evaluator to choose a VPN Gateway that only allows for specifying a single fully qualified IP addresses in the rule.

The evaluator shall perform the following tests:

- **Test 1:** The evaluator shall configure an SPD on the client that is capable of the following: dropping a packet, encrypting a packet, and allowing a packet to flow in plaintext. The selectors used in the construction of the rule shall be different such that the evaluator can generate a packet and send packets to the client with the appropriate fields (fields that are used by the rule - e.g., the IP addresses, TCP/UDP ports) in the packet header. The evaluator performs both positive and negative test cases for each type of rule. The evaluator observes via the audit trail, and packet captures that the TOE exhibited the expected behavior: appropriate packets were dropped, allowed through without modification, was encrypted by the IPsec implementation.

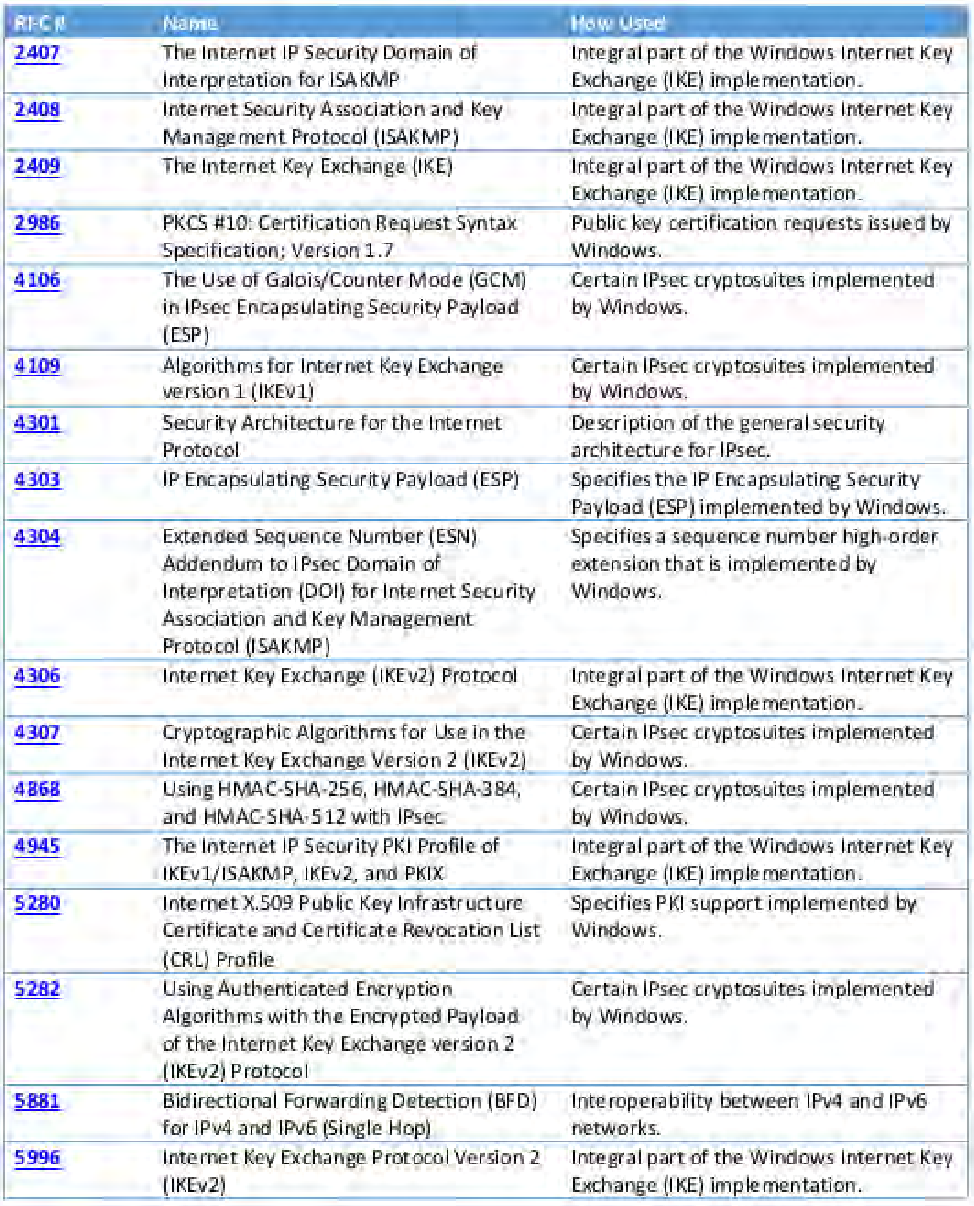
- **Test 2:** The evaluator shall devise several tests that cover a variety of scenarios for packet processing. These scenarios must exercise the range of possibilities for SPD entries and processing modes as outlined in the TSS and operational guidance. Potential areas to cover include rules with overlapping ranges and conflicting entries, inbound and outbound packets, and packets that establish SAs as well as packets that belong to established SAs. The evaluator shall verify, via the audit trail and packet captures, for each scenario that the expected behavior is exhibited, and is consistent with both the TSS and the operational guidance.

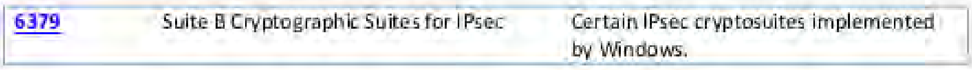
70.1 Documentation Review activity

70.1.1 Findings

The ***Security Target*** document, defines in its section **6.2.3.3 IPsec**, how the IPSec protocol and its capabilities are implemented by Windows. To protect IP communications, Windows implements the IPSec protocol as defined in RFC 4301. An explanation about how the network packets are processed and the relationship between the VPN client and the platform is provided via links to the vendor website and the respective RFCs documents. For instance, the following link, provided in the TSS, explains the IPSec architecture implemented by Windows, as well as, a description of the protocols. In addition, the TSS includes a table of all the RFCs used by windows for its IPSec implementation and how it is used.

Table 34 Windows Implementation of IPsec RFCs

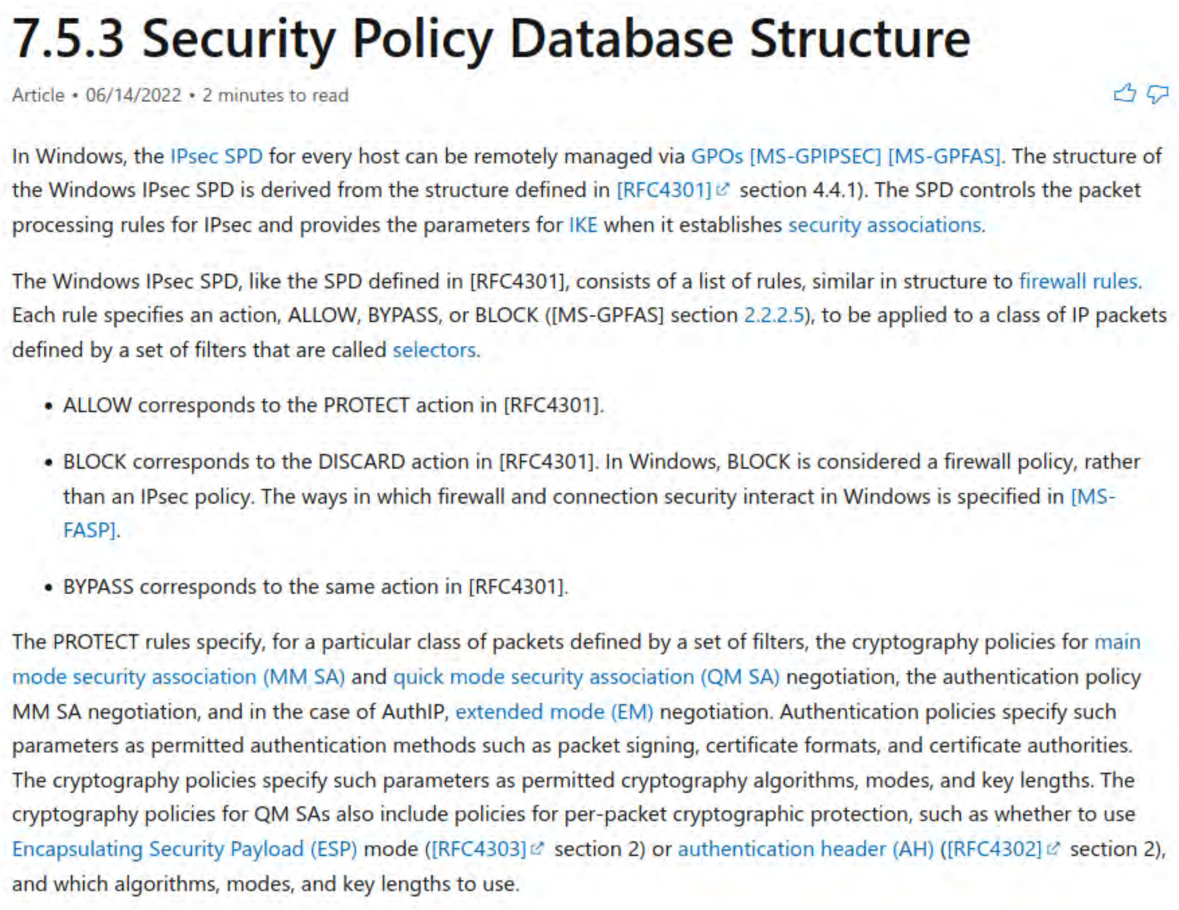




RFC #	Name	How Used
2407	The Internet IP Security Domain of Interpretation for ISAKMP	Integral part of the Windows Internet Key Exchange (IKE) implementation.
2408	Internet Security Association and Key Management Protocol (ISAKMP)	Integral part of the Windows Internet Key Exchange (IKE) implementation.
2409	The Internet Key Exchange (IKE)	Integral part of the Windows Internet Key Exchange (IKE) implementation.
2986	PKCS #10: Certification Request Syntax Specification; Version 1.7	Public key certification requests issued by Windows.
4106	The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)	Certain IPsec cryptosuites implemented by Windows.
4109	Algorithms for Internet Key Exchange version 1 (IKEv1)	Certain IPsec cryptosuites implemented by Windows.
4301	Security Architecture for the Internet Protocol	Description of the general security architecture for IPsec.
4303	IP Encapsulating Security Payload (ESP)	Specifies the IP Encapsulating Security Payload (ESP) implemented by Windows.
4304	Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)	Specifies a sequence number high-order extension that is implemented by Windows.
4306	Internet Key Exchange (IKEv2) Protocol	Integral part of the Windows Internet Key Exchange (IKE) implementation.
4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)	Certain IPsec cryptosuites implemented by Windows.
4868	Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec	Certain IPsec cryptosuites implemented by Windows.
4945	The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX	Integral part of the Windows Internet Key Exchange (IKE) implementation.
5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	Specifies PKI support implemented by Windows.
5282	Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol	Certain IPsec cryptosuites implemented by Windows.
5881	Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)	Interoperability between IPv4 and IPv6 networks.
5996	Internet Key Exchange Protocol Version 2 (IKEv2)	Integral part of the Windows Internet Key Exchange (IKE) implementation.
6379	Suite B Cryptographic Suites for IPsec	Certain IPsec cryptosuites implemented by Windows.

Additionally, within this section of the TSS, it is explained the way the TOE processes the network packets through a SPD. The SPD uses the traffic source, destination and transport protocol to determine if a packet should be transmitted or received, blocked, or protected with IPsec, based on firewall processing rules. In order to prevent unsolicited inbound traffic, an authorized administrator does not need to define a final catch-all rule which will discard a network packet when no other rules in the SPD apply because Windows will discard the packet.

In the provided link, the available rules and actions are explained in the terms defined for the RFC 4301:



7.5.3 Security Policy Database Structure

Article • 06/14/2022 • 2 minutes to read

In Windows, the IPsec SPD for every host can be remotely managed via GPOs [MS-GPIPSEC] [MS-GPFAS]. The structure of the Windows IPsec SPD is derived from the structure defined in [RFC4301] section 4.4.1). The SPD controls the packet processing rules for IPsec and provides the parameters for IKE when it establishes security associations.

The Windows IPsec SPD, like the SPD defined in [RFC4301], consists of a list of rules, similar in structure to firewall rules. Each rule specifies an action, ALLOW, BYPASS, or BLOCK ([MS-GPFAS] section 2.2.2.5), to be applied to a class of IP packets defined by a set of filters that are called selectors.

- ALLOW corresponds to the PROTECT action in [RFC4301].
- BLOCK corresponds to the DISCARD action in [RFC4301]. In Windows, BLOCK is considered a firewall policy, rather than an IPsec policy. The ways in which firewall and connection security interact in Windows is specified in [MS-FASP].
- BYPASS corresponds to the same action in [RFC4301].

The PROTECT rules specify, for a particular class of packets defined by a set of filters, the cryptography policies for main mode security association (MM SA) and quick mode security association (QM SA) negotiation, the authentication policy MM SA negotiation, and in the case of AuthIP, extended mode (EM) negotiation. Authentication policies specify such parameters as permitted authentication methods such as packet signing, certificate formats, and certificate authorities. The cryptography policies specify such parameters as permitted cryptography algorithms, modes, and key lengths. The cryptography policies for QM SAs also include policies for per-packet cryptographic protection, such as whether to use Encapsulating Security Payload (ESP) mode ([RFC4303] section 2) or authentication header (AH) ([RFC4302] section 2), and which algorithms, modes, and key lengths to use.

The ***Operational Guidance*** document, defines in its section **4.4.1 Configuring IPsec firewall rules using Windows Defender Firewall with Advance Security**, the way the SPD policy is created and managed. In Windows, the SPD policy is known as WFP (Windows Filtering Platform). The way WFP works, how the rules are processed and how ordering of rules impact the processing of the packets is explained in the provided links to the vendor website:

- WFP Operation

- IPsec Configuration

Finally, the instructions about configuring the SPD policy are provided based on the interface used for managing the policy (using the Windows user interface, a Group Policy, PowerShell, ora MDM).

70.1.2 Verdict

The evaluator has reviewed the ***Security Target*** document and has ensured that it describes how the IPSec capabilities are implemented and how the network packets are processed. Moreover, the ***Operational Guidance*** document includes instructions about how the SPD policies are created and configured. The information provided is consistent with the one provided in the TSS section of the ***Security Target*** document.

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfillment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

70.2 Test Activity

For this case, all the auditable events will be obtained during the test execution of each security functional requirement.

70.2.1 Test 1, Test 2 and Test 4 (FCS_IPSEC_EXT.1.2)

Bypass and Discard

70.2.1.1 Setup

Before the test execution, the following setup condition must be fulfilled:

- A user account with administrator rights shall exist.
- *Netcat* tool is available on testing machine.
- Firewall audit logs are available and enabled for all profiles in Windows Defender Firewall.
- Following scripts are available:
  - setup.sh
  - deploy_vpn.sh
  - Send-UdpDatagram.ps1

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Testing Machine (Debian 11 Bullseye, using Strongswan U5.9.1/K5.10)
- Windows Client Machine (Platforms listed in the ST)

Both machines are in the same network with the following configuration:

- Testing Machine, IP = 20.20.20.50
- Wiindows Client Machine, IP = 20.20.20.100

70.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMVPN24SD] instructions in order to collect the results as stipulated by the supporting document [PPMVPN24SD].

70.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- HPE Edgeline EL8000 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Panasonic CF-33 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

Results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms*.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

70.2.1.4 Setup

Before the test execution, the following setup condition must be fulfilled:

- The TOE is configured properly and it is available;

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Testing Machine (Debian 11 Bullseye, using Strongswan U5.9.1/K5.10)
- Windows Client Machine (Platforms listed in the ST)

Both machines are in the same network with the following configuration:

- Testing Machine, IP = 20.20.20.100
- Windows Client Machine, IP = 20.20.20.50

70.2.1.5 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMVPN24SD] instructions in order to collect the results as stipulated by the supporting document [PPMVPN24SD].

70.2.1.6 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- HPE Edgeline EL8000 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Panasonic CF-33 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

Results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms*.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

70.2.1.7 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 1** and **Test 2** requirements established in the assurance activity section.

70.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FCS_IPSEC_EXT.1.1.

71 FCS_IPSEC_EXT.1.2

The assurance activity for the **FCS_IPSEC_EXT.1.2** requirement is stated as follows:

> If both transport mode and tunnel mode are implemented, the evaluator shall review the operational guidance to determine how the use of a given mode is specified.
>
> The evaluator shall perform the following test(s) based on the selections chosen:
>
> - **Test 1 [conditional]:** If tunnel mode is selected, the evaluator uses the operational guidance to configure the TOE to operate in tunnel mode and also configures a VPN gateway to operate in tunnel mode. The evaluator configures the TOE and the VPN gateway to use any of the allowable cryptographic algorithms, authentication methods, etc. to ensure an allowable SA can be negotiated. The evaluator shall then initiate a connection from the client to connect to the VPN GW peer. The evaluator observes (for example, in the audit trail and the captured packets) that a successful connection was established using the tunnel mode.
> - **Test 2 [conditional]:** If transport mode is selected, the evaluator uses the operational guidance to configure the TOE to operate in transport mode and also configures an IPsec peer to accept IPsec connections using transport mode. The evaluator configures the TOE and the endpoint device to use any of the allowed cryptographic algorithms, authentication methods, etc. to ensure an allowable SA can be negotiated. The evaluator then initiates a connection from the TOE to connect to the remote endpoint. The evaluator observes (for example, in the audit trail and the captured packets) that a successful connection was established using the transport mode.
> - **Test 3 [conditional]:** If both tunnel mode and transport mode are selected, the evaluator shall perform both Test 1 and Test 2 above, demonstrating that the TOE can be configured to support both modes.
> - **Test 4 [conditional]:** If both tunnel mode and transport mode are selected, the evaluator shall modify the testing for FCS_IPSEC_EXT.1 to include the supported mode for SPD PROTECT entries to show that they only apply to traffic that is transmitted or received using the indicated mode.

71.1 Documentation Review activity

71.1.1 Findings

The ***Security Target*** document, defines in its section **6.2.3.3 IPsec**, that Windows implements both RFCS 2409, Internet Key Exchange (IKEv1), and RFC 4306, Internet Key Exchange version 2, (IKEv2). Windows IPsec supports both tunnel mode and transport mode and provides an option for NAT transversal. The RAS VPN interface uses tunnel mode only.

The ***Operational Guidance*** document, defines in its section **4.4.2 Configuring and using VPN connections and the VPN client**, that Windows supports Network Address Translation (NAT) traversal automatically as part of the IKEv1 and IKEv2 protocols. No configuration is needed or possible. Security association lifetime settings for IKEv2 may only be configured on the VPN gateway. No client configuration is needed or possible in the VPN client. For IKEv1 connections, Windows supports only main mode. It is not possible to configure IKEv1 to use aggressive mode. For IKEv1 connections, XAUTH is not supported.

IKEv1 and L2PT/IPSec does not support Tunnel Mode and IKEv2 only supports Tunnel Mode.

71.1.2 Verdict

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfillment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

71.2 Test Activity

For this case, all the auditable events will be obtained during the test execution of each security functional requirement.

71.2.1 Test 1, Test 2 & Test 3

71.2.1.1 Setup

Before the test execution, the following setup condition must be fulfilled:

- Firewall audit logs are enabled for all the profiles in Windows's firewall.
- A network packet analyzer application shall be installed on client machine (e.g. *Wireshark*).

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Testing Machine (Debian 11 Bullseye, using Strongswan U5.9.1/K5.10)
- Windows Client Machine (Platforms listed in the ST)
- Script *FCS_IPSEC_EXT.1.2.ps1* is available in TOE
- Script *deploy_vpn.sh* is available in server

Both machines are in the same network with the following configuration:

- Testing Machine, IP = 20.20.20.100
- Windows Client Machine, IP = 20.20.20.50

71.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMVPN24SD] instructions in order to collect the results as stipulated by the supporting document [PPMVPN24SD].

71.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

71.2.1.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 1 & Test 2 & Test 3** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1, Test 2 & Test 3**.

71.2.2 Test 4

This test was performed together with the tests associated for the *FCS_IPSEC_EXT.1.1* requirement. The required setup, procedure, results and verdict will be described there.

71.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FCS_IPSEC_EXT.1.2.

72 FCS_IPSEC_EXT.1.3

The assurance activity for the **FCS_IPSEC_EXT.1.3** requirement is stated as follows:

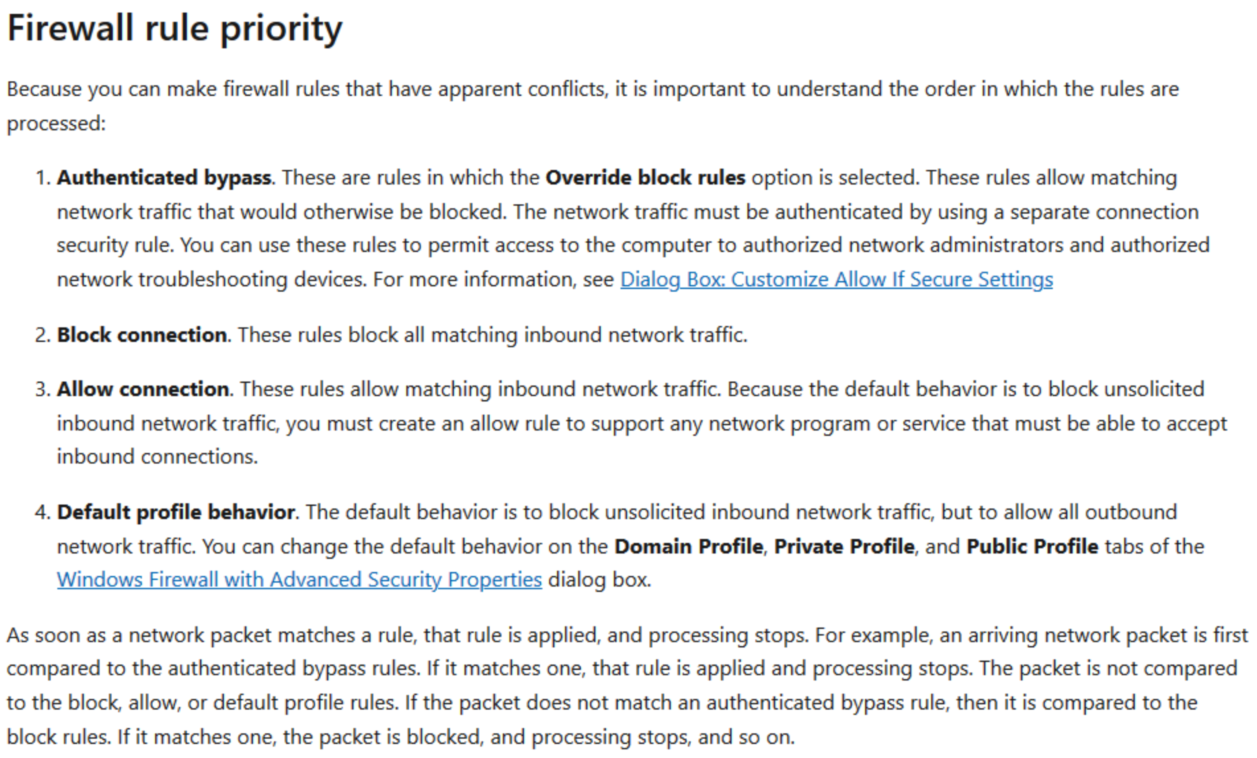
> The evaluator shall check that the operational guidance provides instructions on how to construct or acquire the SPD and uses the guidance to configure the TOE for the following test.
>
> **Operational Guidance**
>
> The evaluator checks that the operational guidance provides instructions on how to construct or acquire the SPD and uses the guidance to configure the TOE/-platform for the following test.
>
> **Test**
>
> The evaluator shall perform the following test:
>
> - **Test 1:** The evaluator shall configure the SPD such that it has entries that contain operations that DISCARD, PROTECT, and (if applicable) BYPASS network packets. The evaluator may use the SPD that was created for verification of FCS_IPSEC_EXT.1.1. The evaluator shall construct a network packet that matches a BYPASS entry and send that packet. The evaluator should observe that the network packet is passed to the proper destination interface with no modification. The evaluator shall then modify a field in the packet header; such that it no longer matches the evaluator-created entries (there may be a “TOE-created” final entry that discards packets that do not match any previous entries). The evaluator sends the packet, and observes that the packet was not permitted to flow to any of the TOE’s interfaces.

72.1 Documentation Review activity

72.1.1 Findings

The ***Security Target*** document, defines in its section **6.2.3.3 IPsec**, the way the TOE processes the network packets through a SPD. The SPD uses the traffic source, destination and transport protocol to determine if a packet should be transmitted or received, blocked, or protected with IPsec, based on firewall processing rules. In order to prevent unsolicited inbound traffic, an authorized administrator does not need to define a final catch-all rule which will discard a network packet when no other rules in the SPD apply because Windows will discard the packet.

In addition, there is a link to the vendor website where it is explained the SPD default behaviour when no rules are defined:



Firewall rule priority

Because you can make firewall rules that have apparent conflicts, it is important to understand the order in which the rules are processed:

1. **Authenticated bypass**. These are rules in which the **Override block rules** option is selected. These rules allow matching network traffic that would otherwise be blocked. The network traffic must be authenticated by using a separate connection security rule. You can use these rules to permit access to the computer to authorized network administrators and authorized network troubleshooting devices. For more information, see Dialog Box: Customize Allow If Secure Settings
2. **Block connection**. These rules block all matching inbound network traffic.
3. **Allow connection**. These rules allow matching inbound network traffic. Because the default behavior is to block unsolicited inbound network traffic, you must create an allow rule to support any network program or service that must be able to accept inbound connections.
4. **Default profile behavior**. The default behavior is to block unsolicited inbound network traffic, but to allow all outbound network traffic. You can change the default behavior on the **Domain Profile**, **Private Profile**, and **Public Profile** tabs of the Windows Firewall with Advanced Security Properties dialog box.

As soon as a network packet matches a rule, that rule is applied, and processing stops. For example, an arriving network packet is first compared to the authenticated bypass rules. If it matches one, that rule is applied and processing stops. The packet is not compared to the block, allow, or default profile rules. If the packet does not match an authenticated bypass rule, then it is compared to the block rules. If it matches one, the packet is blocked, and processing stops, and so on.

The ***Operational Guidance*** document, defines in its section **4.4.1 Configuring IPsec firewall rules using Windows Defender Firewall with Advance Security**, the way the SPD policy is created and managed. In Windows, the SPD policy is known as WFP (Windows Filtering Platform). The way WFP works, how the rules are processed and how ordering of rules impact the processing of the packets is explained in the provided links to the vendor website:

- WFP Operation
- IPsec Configuration

Finally, the instructions about configuring the SPD policy are provided based on the interface used for managing the policy (using the Windows user interface, a Group Policy, PowerShell, ora MDM).

72.1.2 Verdict

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfillment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

72.2 Test Activity

72.2.1 Test 1

72.2.1.1 Setup

Before the test execution, the following setup condition must be fulfilled:

- TOE is configured properly and it is available;
- Firewall audit logs are available and enabled for all profiles in Windows Defender Firewall;

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Testing Machine (Debian 11 Bullseye, using Strongswan U5.9.1/K5.10)
- Windows Client Machine (Platforms listed in the ST)

Both machines are in the same network with the following configuration:

- Testing Machine, IP = 20.20.20.100
- Windows Client Machine, IP = 20.20.20.50

72.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMVPN24SD] instructions in order to collect the results as stipulated by the supporting document [PPMVPN24SD].

72.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- HPE Edgeline EL8000 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Panasonic CF-33 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)

- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

Results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms*.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

72.2.1.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

72.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FCS_IPSEC_EXT.1.3.

73 FCS_IPSEC_EXT.1.4

The assurance activity for the **FCS_IPSEC_EXT.1.4** requirement is stated as follows:

> The evaluator shall examine the TSS to verify that the algorithms AES-GCM-128 and AES-GCM-256 are implemented. If the ST author has selected either AES-CBC-128 or AES-CBC-256 in the requirement, then the evaluator verifies the TSS describes these as well. In addition, the evaluator ensures that the SHA-based HMAC algorithm conforms to the algorithms specified in FCS_COP.1(4) Cryptographic Operations (for keyed-hash message authentication).
>
> The evaluator checks the operational guidance to ensure it provides instructions on how the TOE is configured to use the algorithms selected in this component and whether this is performed through direct configuration, defined during initial installation, or defined by acquiring configuration settings from an environmental component.
>
> - **Test 1:** The evaluator shall configure the TOE/platform as indicated in the operational guidance configuring the TOE/platform to using each of the AES-GCM-128, and AES-GCM-256 algorithms, and attempt to establish a connection using ESP. If the ST Author has selected either AES-CBC-128 or AES-CBC-256, the TOE/platform is configured to use those algorithms and the evaluator attempts to establish a connection using ESP for those algorithms selected.

73.1 Documentation Review activity

73.1.1 Findings

The ***Security Target*** document, defines in its section **6.2.3.4 IPsec**, that Windows 10, Windows 11 and Windows Server implements AES-GCM-128, AES-GCM-256, AES-CBC-128, and AES-CBC-256 as encryption algorithms for the encapsulating security payload (ESP). However only AES-CBC-128 and AES-CBC-256 can be used for IKEv1 and IKEv2 to protect the encrypted payload. The resulting potential strength of the symmetric key will be 128 or 256 bits of security depending on whether the IPsec VPN client and IPsec VPN server agreed to use a 128 or 256 AES symmetric key to protect the network traffic. Windows implements HMAC-SHA1, HMAC-SHA-256 and HMAC-SHA-384 as authentication algorithms for key exchange as well as Diffie-Hellman Groups 14, 19, and 20 . The IPsec VPN client will propose a cryptosuite to the IPsec VPN server; if the server responds with a cryptosuite that the client supports, the client will use the server's proposed cryptosuite instead. If the IPsec VPN client and server cannot agree on a cryptosuite, either side may terminate the connection attempt.

The ***Operational Guidance*** document, defines in its section **4.4.2.2 Configuring VPN using PowerShell**, with Set-VpnConnectionIPsecConfiguration cmdlet may be used to specify additional IPsec parameters, including the encryption algorithm, e.g. AES128 or AES 256. The following article provides more information on Set-VpnConnectionIPsecConfiguration:

- Set-VpnConnectionIPsecConfiguration

73.1.2 Verdict

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfillment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

73.2 Test Activity

For this case, all the auditable events will be obtained during the test execution of each security functional requirement.

73.2.1 Test 1

73.2.1.1 Setup

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Testing Machine (Debian 11 Bullseye, using Strongswan U5.9.1/K5.10)
- Windows Client Machine (Platforms listed in the ST)
- Script FCS_IPSEC_EXT.1.4.ps1 is available in TOE
- Script deploy_server.sh is available in Testing Machine

Both machines are in the same network with the following configuration:

- Testing Machine, IP = 20.20.20.100
- Windows Client Machine, IP = 20.20.20.50

73.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMVPN24SD] instructions in order to collect the results as stipulated by the supporting document [PPMVPN24SD].

73.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Voyager Klaas Telecom with Azure Stack Hub (build 10.0.17784.1068)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

73.2.1.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

73.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FCS_IPSEC_EXT.1.4.

74 FCS_IPSEC_EXT.1.5

The assurance activity for the **FCS_IPSEC_EXT.1.5** requirement is stated as follows:

> The evaluator shall examine the TSS to verify that IKEv1, IKEv2, or both IKEv1 and IKEv2 are implemented. If IKEv1 is implemented, the evaluator shall verify that the TSS indicates whether or not XAUTH is supported, and that aggressive mode is not used for IKEv1 Phase 1 exchanges (i.e. only main mode is used). It may be that these are configurable options.
>
> The evaluator shall check the operational guidance to ensure it instructs the administrator how to configure the TOE to use IKEv1, IKEv2, or both (as selected), and uses the guidance to configure the TOE to perform NAT traversal for the test below. If XAUTH is implemented, the evaluator shall verify that the operational guidance provides instructions on how it is enabled or disabled.
>
> If the TOE supports IKEv1, the evaluator shall verify that the operational guidance either asserts that only main mode is used for Phase 1 exchanges, or provides instructions for disabling aggressive mode.
>
> - **Test 1:** The evaluator shall configure the TOE so that it will perform NAT traversal processing as described in the TSS and RFC 7296, section 2.23. The evaluator shall initiate an IPsec connection and determine that the NAT is successfully traversed. If the TOE supports IKEv1 with or without XAUTH, the evaluator shall verify that this test can be successfully repeated with XAUTH enabled and disabled in the manner specified by the operational guidance. If the TOE only supports IKEv1 with XAUTH, the evaluator shall verify that connections not using XAUTH are unsuccessful. If the TOE only supports IKEv1 without XAUTH, the evaluator shall verify that connections using XAUTH are unsuccessful.
> - **Test 2 [conditional]:** If the TOE supports IKEv1, the evaluator shall perform any applicable operational guidance steps to disable the use of aggressive mode and then attempt to establish a connection using an IKEv1 Phase 1 connection in aggressive mode. This attempt should fail. The evaluator shall show that the TOE will reject a VPN gateway from initiating an IKEv1 Phase 1 connection in aggressive mode. The evaluator should then show that main mode exchanges are supported.

74.1 Documentation Review activity

74.1.1 Findings

The ***Security Target*** document, defines in its section **6.2.3.3 IPsec**, that Windows implements both RFCS 2409, Internet Key Exchange (IKEv1), and RFC 4306, Internet Key Exchange version 2, (IKEv2). Windows IPsec supports both tunnel mode and transport mode and provides an option for NAT transversal. The RAS VPN interface uses tunnel mode only. In this section the evaluator can find a whole list of RFCs implementation on Windows. In this section the evaluator can find a whole list of RFC implementation on Windows. In this list there isn't a RFC of IKEv1 protocol which has the implementation of XAUTH.

The ***Operational Guidance*** document, defines in its section **4.4.2 Configuring and using VPN connections and the VPN client**, that Windows supports Network Address Translation (NAT) traversal automatically as part of the IKEv1 and IKEv2 protocols. No configuration is needed or possible. Client security association lifetime settings for IKEv1 and IKEv2 in tunnel mode are configured on the VPN gateway. No client configuration is needed or possible in the VPN client. For IKEv1 connections, Windows supports only main mode. It is not possible to configure IKEv1 to use aggressive mode. For IKEv1 connections, XAUTH is not supported. Also states the different ways to configure this properties through the different interfaces.

74.1.2 Verdict

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfillment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

74.2 Test Activity

For this case, all the auditable events will be obtained during the test execution of each security functional requirement.

74.2.1 Test 1

74.2.1.1 Setup

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Testing Machine (Debian 11 Bullseye, using Strongswan U5.9.1/K5.10)
- Windows Client Machine (Platforms listed in the ST)
- Scripts FCS_IPSEC_EXT.1.5.ps1 and deploy_vpn.sh are available in TOE

Both machines are in the same network with the following configuration:

- Testing Machine, IP = 20.20.20.100
- Windows Client Machine, IP = 20.20.20.50

74.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMVPN24SD] instructions in order to collect the results as stipulated by the supporting document [PPMVPN24SD].

74.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Voyager Klaas Telecom with Azure Stack Hub (build 10.0.17784.1068)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

74.2.1.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

74.2.2 Test 2

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Testing Machine (Debian 11 Bullseye, using Strongswan U5.9.1/K5.10)
- Windows Client Machine (Platforms listed in the ST)
- Script FCS_IPSEC_EXT.1.5.ps1 is available in TOE

Both machines are in the same network with the following configuration:

- Server Machine, IP = 20.20.20.100
- Client Machine, IP = 20.20.20.50

74.2.2.1 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMVPN24SD] instructions in order to collect the results as stipulated by the supporting document [PPMVPN24SD].

74.2.2.2 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Voyager Klaas Telecom with Azure Stack Hub (build 10.0.17784.1068)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

74.2.2.3 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 2** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 2**.

74.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FCS_IPSEC_EXT.1.5.

75 FCS_IPSEC_EXT.1.6

The assurance activity for the **FCS_IPSEC_EXT.1.6** requirement is stated as follows:

> The evaluator shall ensure the TSS identifies the algorithms used for encrypting the IKEv1 and/or IKEv2 payload, and that the algorithms AES-CBC-128, AES-CBC-256 are specified, and if others are chosen in the selection of the requirement, those are included in the TSS discussion.
>
> The evaluator checks the operational guidance to ensure it provides instructions on how the TOE is configured to use the algorithms selected in this component and whether this is performed through direct configuration, defined during initial installation, or defined by acquiring configuration settings from an environmental component.
>
> The evaluator shall use the operational guidance to configure the TOE/platform (or to configure the Operational Environment to have the TOE receive configuration) to perform the following test for each cipher suite selected:
>
> - **Test 1:** The evaluator shall configure the TOE to use the ciphersuite under test to encrypt the IKE payload for each supported IKE version and establish a connection with a peer device, which is configured to only accept the payload encrypted using the indicated ciphersuite. The evaluator will confirm the algorithm was that used in the negotiation. The evaluator will confirm that the connection is successful by confirming that data can be passed through the connection once it is established. For example, the evaluator may connect to a webpage on the remote network and verify that it can be reached.

75.1 Documentation Review activity

75.1.1 Findings

The ***Security Target*** document, defines in its section **6.2.1 Cryptographic Algorithms and operations**, that the Cryptography API, Next Generation (CNG) API, is designed to be extensible at many levels and agnostic to cryptographic algorithm suites. Windows uses CNG exclusively for its own encryption needs and provides public APIs for external developers. An important feature of CNG is its native implementation of the Suite B algorithms, including algorithms for AES (128, 192, 256 key sizes)[Note that the 192-bit key size is not used by Windows but is available to developers.], the SHA-1 and SHA-2 family (SHA-256, SHA-384 and SHA-512) of hashing algorithms, elliptic curve Diffie Hellman (ECDH), and elliptical curve DSA (ECDSA) over the NIST-standard prime curves P-256, P-384, and P-521.

The ***Operational Guidance*** document, defines in its section **4.4.2.2 Configuring VPN using PowerShell**, with Set-VpnConnectionIPsecConfiguration cmdlet may be used to specify additional IPsec parameters, including the encryption algorithm, e.g. AES128 or AES 256. The following article provides more information on Set-VpnConnectionIPsecConfiguration:

- Set-VpnConnectionIPsecConfiguration

75.1.2 Verdict

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfillment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

75.2 Test Activity

For this case, all the auditable events will be obtained during the test execution of each security functional requirement.

75.2.1 Test 1

75.2.1.1 Setup

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Testing Machine (Debian 11 Bullseye, using Strongswan U5.9.1/K5.10)
- Windows Client Machine (Platforms listed in the ST)
- Script FCS_IPSEC_EXT.1.6.ps1 is available in TOE
- Script deploy_server.sh is available in Testing Machine

Both machines are in the same network with the following configuration:

- Testing Machine, IP = 20.20.20.100
- Windows Client Machine, IP = 20.20.20.50

75.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMVPN24SD] instructions in order to collect the results as stipulated by the supporting document [PPMVPN24SD].

75.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop Go 2
- Dell PowerEdge R640
- Microsoft Surface Go 3
- Dell PowerEdge R640
- Zebra L10ax / RTL 10C1
- Dell Latitude 9520
- Zebra ET80A Tablet
- Voyager Klaas Telecom
- Microsoft Windows Server 2019 Hyper-V
- Dell PowerEdge R760xp
- Surface Studio 2+

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

75.2.1.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

75.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FCS_IPSEC_EXT.1.6.

76 FCS_IPSEC_EXT.1.7

The assurance activity for the **FCS_IPSEC_EXT.1.7** requirement is stated as follows:

> **TSS**
>
> There are no TSS Assurance Activities for this requirement.
>
> **Operational Guidance**
>
> The evaluator shall check the operational guidance to ensure it provides instructions on how the TOE configures the values for SA lifetimes. In addition, the evaluator shall check that the guidance has the option for either the Administrator or VPN Gateway to configure Phase 1 SAs if time-based limits are supported. Currently there are no values mandated for the number of packets or number of bytes, the evaluator shall simply check the operational guidance to ensure that this can be configured if selected in the requirement.
>
> **Test**
>
> When testing this functionality, the evaluator needs to ensure that both sides are configured appropriately. From the RFC "A difference between IKEv1 and IKEv2 is that in IKEv1 SA lifetimes were negotiated. In IKEv2, each end of the SA is responsible for enforcing its own lifetime policy on the SA and rekeying the SA when necessary. If the two ends have different lifetime policies, the end with the shorter lifetime will end up always being the one to request the rekeying. If the two ends have the same lifetime policies, it is possible that both will initiate a rekeying at the same time (which will result in redundant SAs). To reduce the probability of this happening, the timing of rekeying requests SHOULD be jittered." Each of the following tests shall be performed for each version of IKE selected in the FCS_IPSEC_EXT.1.5 protocol selection:
>
> - **Test 1 [conditional]:** The evaluator shall configure a maximum lifetime in terms of the # of packets (or bytes) allowed following the operational guidance. The evaluator shall establish an SA and determine that once the allowed # of packets (or bytes) through this SA is exceeded, the connection is closed.
> - **Test 2 [conditional]:** The evaluator shall construct a test where a Phase 1 SA is established and attempted to be maintained for more than 24 hours before it is renegotiated. The evaluator shall observe that this SA is closed or renegotiated in 24 hours or less. If such an action requires that the TOE be configured in a specific way, the evaluator shall implement tests demonstrating that the configuration capability of the TOE works as documented in the operational guidance.
> - **Test 3 [conditional]:** The evaluator shall perform a test similar to Test 2 for Phase 2 SAs, except that the lifetime will be 8 hours or less instead of 24 hours or less.

- **Test 4 [conditional]:** If a fixed limit for IKEv1 SAs is supported, the evaluator shall establish an SA and observe that the connection is closed after the fixed traffic or time value is reached.

76.1 Documentation Review activity

76.1.1 Findings

The ***Operational Guidance*** document, defines in its section **6.4.2.5 VPN client security association lifetime**, that SA lifetime settings for tunnel mode using the RAS IPsec VPN interface for IKEv1 and IKEv2 are configured on the VPN gateway. The default values used for lifetimes by the RAS IPsec VPN Client are shown below:

- Main Mode
  - Lifetime in Seconds: 28800
- Quick Mode
  - Lifetime in Seconds: 3600
  - Lifetime in Packets: 2147483647
  - Lifetime in Kilobytes: 250000
  - Idle Duration in Seconds: 300

If the connection is broken due to network interruption, then the established SA remains in use until the SA lifetime limits are reached.

Moreover, section **6.4.3.2 Configuring IPsec security association lifetime using PowerShell** states that security association (SA) lifetimes for IKEv1 are configured locally when using transport mode. When using tunnel mode, SA lifetimes are configured on the VPN gateway. To configure SA lifetimes, it can be used Windows PowerShell *cmdlets* or Group Policy objects, however, *cmdlets* are the preferred solution for configuring IKEv1 SA lifetime, among other parameters, for both main mode (phase 1) and quick mode (phase 2).

There are several links to the vendor website with instructions for configuring both modes:

PowerShell configuration of main mode:

- New-NetIPsecMainModeCryptoSet

PowerShell configuration of quick mode:

- New-NetIPsecQuickModeCryptoProposal

Group policy configuration:

- Configure Key Exchange

76.1.2 Verdict

The evaluator has reviewed the ***Operational Guidance*** document and has ensured that it includes instructions about how to configures the values for SA lifetimes.

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfilment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

76.2 Test Activity

76.2.1 Test 1, Test 2 and Test 3

76.2.1.1 Setup

Before the test execution, the following setup condition must be fulfilled:

- A user account with administrator rights shall exist.
- The *PowerShell* execution policy shall be configured to allow the execution of *PowerShell* scripts. To do it, execute in a *Powershell* terminal with administrator rights the command:

  ```
  Set-ExecutionPolicy Unrestricted -Force
  ```

- Script *FCS_IPSEC_EXT.1.7.ps1* shall be available in the Windows Client Machine.
- deploy_vpn.sh_ shall be available in the Testing Machine.
- *PSTools* are available in the Windows Client Machine.
- A network packet analyzer application shall be installed on client machine (e.g. *Wireshark*).

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Testing Machine (Debian 11 Bullseye, using Strongswan 5.9.1)
- Testing Machine 2 (Windows Server 2019)
- Windows Client Machine (Platforms listed in the ST)

Both machines are in the same network with the following configuration:

- Testing Machine, IP = 20.20.20.100
- Windows Testing Machine, IP = 20.20.20.101
- Windows Client Machine, IP = 20.20.20.50

76.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMVPN24SD] instructions in order to collect the results as stipulated by the supporting document [PPMVPN24SD].

76.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

76.2.1.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 1, Test 2 and Test 3** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1, Test 2 and Test 3**.

76.2.2 Test 4

76.2.2.1 Setup

The applicable setup for this test is the same as the one defined in the previous test cases.

76.2.2.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMVPN24SD] instructions in order to collect the results as stipulated by the supporting document [PPMVPN24SD].

76.2.2.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

76.2.2.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 4** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 4**.

76.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FCS_IPSEC_EXT.1.7.

77 FCS_IPSEC_EXT.1.8

The assurance activity for the **FCS_IPSEC_EXT.1.8** requirement is stated as follows:

> The evaluator shall check to ensure that the DH groups specified in the requirement are listed as being supported in the TSS. If there is more than one DH group supported, the evaluator checks to ensure the TSS describes how a particular DH group is specified/negotiated with a peer.
>
> There are no AGD Assurance Activities for this requirement.
>
> The evaluator shall perform the following test:
>
> - **Test 1:** For each supported DH group, the evaluator shall test to ensure that all supported IKE protocols can be successfully completed using that particular DH group.

77.1 Documentation Review activity

77.1.1 Findings

The ***Security Target*** document, defines in its section **6.2.3.3 IPsec**, that Windows 10, Windows 11 and Windowes Server implement AES-GCM-128, AES-GCM-256, AES-CBC-128, and AES-CBC-256 as encryption algorithms for the encapsulating security payload (ESP). However only AES-CBC-128 and AES-CBC-256 can be used for IKEv1 and IKEv2 to protect the encrypted payload. The resulting potential strength of the symmetric key will be 128 or 256 bits of security depending on whether the IPsec VPN client and IPsec VPN server agreed to use a 128 or 256 AES symmetric key to protect the network traffic. Windows implements HMAC-SHA1, HMAC-SHA-256 and HMAC-SHA-384 as authentication algorithms for key exchange as well as Diffie-Hellman Groups 14, 19, 20 and 24 . The IPsec VPN client will propose a cryptosuite to the IPsec VPN server; if the server responds with a cryptosuite that the client supports, the client will use the server's proposed cryptosuite instead. If the IPsec VPN client and server cannot agree on a cryptosuite, either side may terminate the connection attempt.

77.1.2 Verdict

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfillment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

77.2 Test Activity

For this case, all the auditable events will be obtained during the test execution of each security functional requirement.

77.2.1 Test 1

77.2.1.1 Setup

Before the test execution, the following setup condition must be fulfilled:

- Testing Machine (Debian 11 Bullseye, using Strongswan U5.9.1/K5.10)
- Windows Client Machine (Platforms listed in the ST)
- Script *FCS_IPSEC_EXT.1.8.ps* is available in TOE
- Script *deploy_vpn.sh* is avalaible in VPN server
- Script *generate_certs.sh* is avalaible in VPN server
- Script *FCS_IPSEC_EXT.1.8.sh* is avalaible in VPN server

Both machines are in the same network with the following configuration:

- Testing Machine, IP = 20.20.20.100
- Windows Client Machine, IP = 20.20.20.50

77.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMVPN24SD] instructions in order to collect the results as stipulated by the supporting document [PPMVPN24SD].

77.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)

- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Voyager Klaas Telecom with Azure Stack Hub (build 10.0.17784.1068)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)

- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

77.2.1.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

77.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FCS_IPSEC_EXT.1.8.

78 FCS_IPSEC_EXT.1.9

The assurance activity for the **FCS_IPSEC_EXT.1.9** requirement is stated as follows:

> The TSF shall generate the secret value x used in the IKE DH key exchange ("x" in g^x mod p) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least [224,256,384] bits.

78.1 Documentation Review activity

78.1.1 Findings

The ***Security Target*** document, defines in its section **6.2.1 Cryptographic Algorithms and Operations**, that that deterministic random bit generation (DRBG) is implemented in accordance with NIST Special Publication 800-90. Windows generates random bits by taking the output of a cascade of two SP800-90 AES-256 counter mode based DRBGs in kernel-mode and four cascaded SP800-90 AES-256 DRBGs in user-mode; programmatic callers can choose to obtain either 128 or 256 bits from the RBG which is seeded from the Windows entropy pool. Windows has different entropy sources (deterministic and nondeterministic) which produce entropy data that is used for random numbers generation. In particular, this entropy data together with other data (such as the nonce) seed the DRBG algorithm. The entropy pool is populated using the following values:

- An initial entropy value from a seed file provided to the Windows OS Loader at boot time (512 bits of entropy).
- A calculated value based on the high-resolution CPU cycle counter which fires after every 1024 interrupts (a continuous source providing 16384 bits of entropy).
- Random values gathered periodically from the Trusted Platform Module (TPM), (320 bits of entropy on boot, 384 bits thereafter on demand based on an OS timer).
- Random values gathered periodically by calling the RDRAND CPU instruction, (256 bits of entropy on demand based on an OS timer).

Finally, according to section **6.2.1 Cryptographic Algorithms and Operations** of the ***Security Target*** document, Windows shall be running in FIPS validated mode. In this mode, all used algorithms must be FIPS approved. The evaluator has followed instructions in section **3.2.5 FIPS 140 Approved cryptography mode** of the ***Operational Guidance*** document for setting this mode.

There are no AGD Assurance Activities for this requirement.

78.1.2 Verdict

The evaluator considers that the TSS provides enough information related to DRBG and related to nonces length.

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfillment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

78.2 Test Activity

There are no test Assurance Activities for this requirement.

78.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FCS_IPSEC_EXT.1.9.

79 FCS_IPSEC_EXT.1.10

The assurance activity for the **FCS_IPSEC_EXT.1.10** requirement is stated as follows:

> The TSF shall generate nonces used in IKE exchanges in a manner such that the probability that a specific nonce value will be repeated during the life a specific IPsec SA is less than 1 in 2^256.

79.1 Documentation Review activity

Assurance Activities for this element are tested through Assurance Activities for FCS_IPSEC_EXT.1.9.

79.2 Test Activity

Assurance Activities for this element are tested through Assurance Activities for FCS_IPSEC_EXT.1.9.

79.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FCS_IPSEC_EXT.1.10.

80 FCS_IPSEC_EXT.1.11

The assurance activity for the **FCS_IPSEC_EXT.1.11** requirement is stated as follows:

> The evaluator shall ensures that the TSS whether peer authentication is performed using RSA, ECDSA, or both.
>
> If any selection with pre-shared keys is chosen in the selection, the evaluator shall check to ensure that the TSS describes how those selections work in conjunction with authentication of IPsec connections.
>
> The evaluator shall ensure that the TSS describes how the TOE compares the peer's presented identifier to the reference identifier. This description shall include whether the certificate presented identifier is compared to the ID payload presented identifier, which fields of the certificate are used as the presented identifier (DN, Common Name, or SAN) and, if multiple fields are supported, the logical order comparison. If the ST author assigned an additional identifier type, the TSS description shall also include a description of that type and the method by which that type is compared to the peer's presented certificate.
>
> The evaluator shall check that the operational guidance describes how pre-shared keys are to be generated and established.
>
> The evaluator ensures the operational guidance describes how to set up the TOE/platform to use the cryptographic algorithms RSA and/or ECDSA.
>
> In order to construct the environment and configure the TOE/platform for the following tests, the evaluator will ensure that the operational guidance also describes how to configure the TOE/platform to connect to a trusted CA, and ensure a valid certificate for that CA is loaded into the TOE/platform as a trusted CA.
>
> The evaluator shall also ensure that the operational guidance includes the configuration of the reference identifier(s) for the peer.
>
> For efficiency's sake, the testing that is performed here has been combined with the testing for **FIA_X509_EXT.2.1**(for IPsec connections), **FCS_IPSEC_EXT.1.12**, **FCS_IPSEC_EXT.1.13** and **FIA_X509_EXT.2.3**. The following tests shall be repeated for each peer authentication protocol selected in the **FCS_IPSEC_EXT.1.11** selection above:
>
> - **Test 1:** The evaluator shall have the TOE generate a public-private key pair, and submit a CSR (Certificate Signing Request) to a CA (trusted by both the TOE and the peer VPN used to establish a connection) for its signature. The values for the DN (Common Name, Organization, Organizational Unit, and Country) will also be passed in the request. Alternatively, the evaluator may import to the TOE a previously generated private key and corresponding certificate.

- **Test 2:** The evaluator shall configure the TOE to use a private key and associated certificate signed by a trusted CA and shall establish an IPsec connection with the peer.
- **Test 3:** The evaluator shall test that the TOE can properly handle revoked certificates - conditional on whether CRL or OCSP is selected; if both are selected, and then a test is performed for each method. For this current version of the PP-Module, the evaluator has to only test one up in the trust chain (future drafts may require to ensure the validation is done up the entire chain). The evaluator shall ensure that a valid certificate is used, and that the SA is established. The evaluator then attempts the test with a certificate that will be revoked (for each method chosen in the selection) to ensure when the certificate is no longer valid that the TOE will not establish an SA.
- **Test 4 [conditional]**: For each selection made, the evaluator shall verify factors are required, as indicated in the operational guidance, to establish an IPsec connection with the server.

For each supported identifier type (excluding DNs), the evaluator shall repeat the following tests:

- **Test 5:** For each field of the certificate supported for comparison, the evaluator shall configure the peer's reference identifier on the TOE (per the administrative guidance) to match the field in the peer's presented certificate and shall verify that the IKE authentication succeeds.
- **Test 6:** For each field of the certificate support for comparison, the evaluator shall configure the peer's reference identifier on the TOE (per the administrative guidance) to not match the field in the peer's presented certificate and shall verify that the IKE authentication fails.

The following tests are conditional

- **Test 7 [conditional]:** If, according to the TSS, the TOE supports both Common Name and SAN certificate fields and uses the preferred logic outlined in the Application Note, the tests above with the Common Name field shall be performed using peer certificates with no SAN extension. Additionally, the evaluator shall configure the peer's reference identifier on the TOE to not match the SAN in the peer's presented certificate but to match the Common Name in the peer's presented certificate, and verify that the IKE authentication fails.
- **Test 8 [conditional]:** If the TOE supports DN identifier types, the evaluator shall configure the peer's reference identifier on the TOE (per the administrative guidance) to match the subject DN in the peer's presented certificate and shall verify that the IKE authentication succeeds. To demonstrate a bitwise comparison of the DN, the evaluator shall change a single bit in the

DN (preferably, in an Object Identifier (OID) in the DN) and verify that the IKE authentication fails. To demonstrate a comparison of DN values, the evaluator shall change any one of the four DN values and verify that the IKE authentication fails.

- **Test 9 [conditional]:** If the TOE supports both IPv4 and IPv6 and supports IP address identifier types, the evaluator must repeat test 1 and 2 with both IPv4 address identifiers and IPv6 identifiers. Additionally, the evaluator shall verify that the TOE verifies that the IP header matches the identifiers by setting the presented identifiers and the reference identifier with the same IP address that differs from the actual IP address of the peer in the IP headers and verifying that the IKE authentication fails.
- **Test 10 [conditional]:** If, according to the TSS, the TOE performs comparisons between the peer's ID payload and the peer's certificate, the evaluator shall repeat the following test for each combination of supported identifier types and supported certificate fields (as above). The evaluator shall configure the peer to present a different ID payload than the field in the peer's presented certificate and verify that the TOE fails to authenticate the IKE peer.

80.1 Documentation Review activity

80.1.1 Findings

The ***Operational Guidance*** document, defines in its section **4.4.3.5 Using pre-shared keys**, that Windows supports the use of pre-shared keys for IKEv1 / L2TP connections. The secret value for the pre-shared key must be a text-based value manually entered in the input field for a pre-shared key. The secret value must match the secret value configured on the VPN server. While the secret can be any length, it should include at least 22 characters and up to 10000 characters as determined at the discretion of the administrator. For example organizational policies can enforce the use of strong passwords containing a minimum number of characters using at least one upper and one lower case letter, one number, and one special character from among the following: ! @ # $ % ^ & * ().

The ***Operational Guidance*** document, defines in its section **4.4.3.3 Configuring authentication signature algorithms**, that Windows supports the following signature algorithms for IPsec authentication with certificates:

- RSA
- ECDSA P256
- ECDSA P384

There is a official documentation where the configuration could be consulted New-NetIPsecAuthProposal.

The ***Operational Guidance*** document, details in its section **4.2 Managing X.509 certificates**, the processes for configuring the TOE platform to connect using trusted CA, and ensuring that these CA are correctly loaded on the TOE platform.

80.1.2 Verdict

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfillment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

80.2 Test Activity

80.2.1 Test 1

80.2.1.1 Setup

Before the test execution, the following setup condition must be fulfilled:

- Windows Client Machine (Platforms listed in the ST)
- Platforms listed in the ST
- Script FCS_IPSEC_EXT.1.11.ps1 is available in TOE

80.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMVPN24SD] instructions in order to collect the results as stipulated by the supporting document [PPMVPN24SD].

80.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)

- HPE Edgeline EL8000 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)

Results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms*.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

80.2.1.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

80.2.2 Test 2

80.2.2.1 Setup

Before the test execution, the following setup condition must be fulfilled:

- Testing Machine (Debian 11 Bullseye, using Strongswan 5.9.1)
- Windows Client Machine (Platforms listed in the ST)
- Script FCS_IPSEC_EXT.1.11.ps1 is available in TOE
- Script FCS_IPSEC_EXT.1.11.sh is available in Testing Machine
- Script FCS_IPSEC_EXT.1.11_test2.sh is available in Testing Machine
- generateCerts.sh and deploy_vpn.sh are available in Testing Machine

80.2.2.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMVPN24SD] instructions in order to collect the results as stipulated by the supporting document [PPMVPN24SD].

80.2.2.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- HPE Edgeline EL8000 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)

Results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms*.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

80.2.2.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 2** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 2**.

80.2.3 Test 3

80.2.3.1 Setup

Before the test execution, the following setup condition must be fulfilled:

- Testing Machine (Debian 11 Bullseye, using Strongswan 5.9.1)
- Windows Client Machine (Platforms listed in the ST)
- Script FCS_IPSEC_EXT.1.11.ps1 is available in TOE
- Script deploy_vpn.sh is available in testing machine
- Script FCS_IPSEC_EXT.1.11_test3.sh is available in testing machine

80.2.3.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMVPN24SD] instructions in order to collect the results as stipulated by the supporting document [PPMVPN24SD].

80.2.3.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- HPE Edgeline EL8000 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)

Results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms*.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

80.2.3.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 3** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 3**.

80.2.4 Test 4, 5, 6, 8, 10

80.2.4.1 Setup

Before the test execution, the following setup condition must be fulfilled:

- Testing Machine (Debian 11 Bullseye, using Strongswan 5.9.1)

- Windows Client Machine (Platforms listed in the ST)
- Domain test.com added to Windows Client's host file
- Script FCS_IPSEC_EXT.1.11.ps1 is available in TOE
- Script deploy_vpn.sh is available in testing machine
- Script FCS_IPSEC_EXT.1.11_auxialiary.sh is available in testing machine

80.2.4.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMVPN24SD] instructions in order to collect the results as stipulated by the supporting document [PPMVPN24SD].

80.2.4.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- HPE Edgeline EL8000 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)

Results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms*.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

80.2.4.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 4, Test 5, Test 6, Test 8 and Test 10** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 4, Test 5, Test 6, Test 8 and Test 10**.

80.2.5 Test 7 and Test 9

These tests are conditional and as stated in the section **6.2.3.3 IPsec** of the ***Security Target***:

> "Windows will validate certificates as described in section 6.4.1 by comparing the Common Name of the certificate presented by the VPN gateway to the expected values for the IP address or Fully Qualified Domain Name of the VPN gateway."

For **test 7** also, the TOE does not met the Application Note:

> *"Excluding the DN identifier type (which is necessarily the Subject DN in the peer certificate), the TOE may support the identifier in either the Common Name or Subject Alternative Name (SAN) or both.If both are supported, the preferred logic is to compare the reference identifier to a presented SAN, and only if the peer's certificate does not contain a SAN, to fall back to a comparison against the Common Name. In the future, the TOE will be required to compare the reference identifier to the presented identifier in the SAN only, ignoring the Common Name."*

Therefore, this test not applicable in this evaluation since the condition is not met.

80.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FCS_IPSEC_EXT.1.11.

81 FCS_IPSEC_EXT.1.12

The assurance activity for the **FCS_IPSEC_EXT.1.12** requirement is stated as follows:

> The TSF shall not establish an SA if the IP address, Fully Qualified Domain Name (FQDN), Distinguished Name (DN) and no other reference identifier type contained in a certificate does not match the expected value(s) for the entity attempting to establish a connection.

81.1 Documentation Review activity

Assurance Activities for this element are tested through Assurance Activities for FCS_IPSEC_EXT.1.11.

81.2 Test Activity

Assurance Activities for this element are tested through Assurance Activities for FCS_IPSEC_EXT.1.11.

81.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FCS_IPSEC_EXT.1.12.

82 FCS_IPSEC_EXT.1.13

The assurance activity for the **FCS_IPSEC_EXT.1.13** requirement is stated as follows:

> The TSF shall not establish an SA if the presented identifier does not match the configured reference identifier of the peer.

82.1 Documentation Review activity

Assurance Activities for this element are tested through Assurance Activities for FCS_IPSEC_EXT.1.11.

82.2 Test Activity

Assurance Activities for this element are tested through Assurance Activities for FCS_IPSEC_EXT.1.11.

82.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FCS_IPSEC_EXT.1.13.

83 FCS_IPSEC_EXT.1.14

The assurance activity for the **FCS_IPSEC_EXT.1.14** requirement is stated as follows:

> The evaluator shall check that the TSS describes the potential strengths (in terms of the number of bits in the symmetric key) of the algorithms that are allowed for the IKE and ESP exchanges. The TSS shall also describe the checks that are done when negotiating IKEv1 Phase 2 and/or IKEv2 CHILD_SA suites to ensure that the strength (in terms of the number of bits of key in the symmetric algorithm) of the negotiated algorithm is less than or equal to that of the IKE SA this is protecting the negotiation.
>
> There are no AGD Assurance Activities for this requirement.
>
> The evaluator follows the guidance to configure the TOE/platform to perform the following tests.
>
> - **Test 1:** This test shall be performed for each version of IKE supported. The evaluator shall successfully negotiate an IPsec connection using each of the supported algorithms and hash functions identified in the requirements.
> - **Test 2 [conditional]:** This test shall be performed for each version of IKE supported. The evaluator shall attempt to establish an SA for ESP that selects an encryption algorithm with more strength than that being used for the IKE SA (i.e., symmetric algorithm with a key size larger than that being used for the IKE SA). Such attempts should fail.
> - **Test 3:** This test shall be performed for each version of IKE supported. The evaluator shall attempt to establish an IKE SA using an algorithm that is not one of the supported algorithms and hash functions identified in the requirements. Such an attempt should fail.
> - **Test 4:** This test shall be performed for each version of IKE supported. The evaluator shall attempt to establish an SA for ESP (assumes the proper parameters where used to establish the IKE SA) that selects an encryption algorithm that is not identified in FCS_IPSEC_EXT.1.4. Such an attempt should fail.

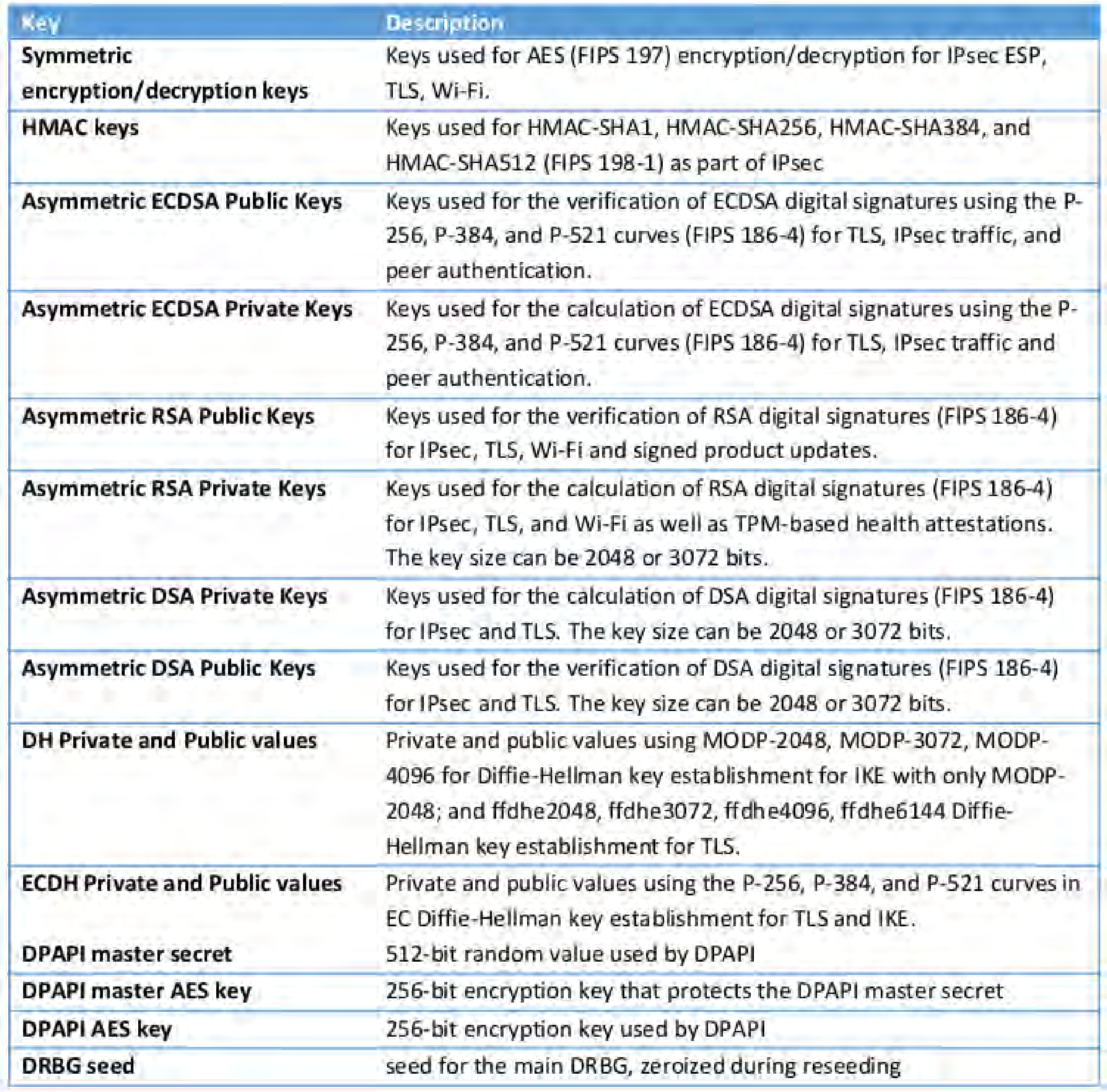
83.1 Documentation Review activity

83.1.1 Findings

The ***Security Target*** document, defines in its section **6.2.1 Cryptographic Algorithms and Operations**, that the Cryptography API: Next Generation (CNG) API is designed to be extensible at many levels and agnostic to cryptographic algorithm suites. The CNG provider for random number generation is the AES_CTR_DRBG, when Windows requires the use of a salt it uses the Windows RBG. The encryption and decryption operations are performed by independent modules, known as Cryptographic Service Providers (CSPs). Windows generates symmetric keys (AES keys) using the FIPS Approved random number generator.

The ***Security Target*** document, defines in its section **6.2.2 Cryptographic Algorithm Validation**, that CNG performs a key error detection check on each transfer of key (internal and intermediate transfers). CNG prevents archiving of expired (private) signature keys and destroys non-persistent cryptographic keys. In this section the different keys used its shown in table 32 **Types of Keys Used by Windows**, as shown below.

Table 32 Types of Keys Used by Windows



Key	Description
Symmetric encryption/decryption keys	Keys used for AES (FIPS 197) encryption/decryption for IPsec ESP, TLS, Wi-Fi.
HMAC keys	Keys used for HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, and HMAC-SHA512 (FIPS 198-1) as part of IPsec
Asymmetric ECDSA Public Keys	Keys used for the verification of ECDSA digital signatures using the P-256, P-384, and P-521 curves (FIPS 186-4) for TLS, IPsec traffic, and peer authentication.
Asymmetric ECDSA Private Keys	Keys used for the calculation of ECDSA digital signatures using the P-256, P-384, and P-521 curves (FIPS 186-4) for TLS, IPsec traffic and peer authentication.
Asymmetric RSA Public Keys	Keys used for the verification of RSA digital signatures (FIPS 186-4) for IPsec, TLS, Wi-Fi and signed product updates.
Asymmetric RSA Private Keys	Keys used for the calculation of RSA digital signatures (FIPS 186-4) for IPsec, TLS, and Wi-Fi as well as TPM-based health attestations. The key size can be 2048 or 3072 bits.
Asymmetric DSA Private Keys	Keys used for the calculation of DSA digital signatures (FIPS 186-4) for IPsec and TLS. The key size can be 2048 or 3072 bits.
Asymmetric DSA Public Keys	Keys used for the verification of DSA digital signatures (FIPS 186-4) for IPsec and TLS. The key size can be 2048 or 3072 bits.
DH Private and Public values	Private and public values using MODP-2048, MODP-3072, MODP-4096 for Diffie-Hellman key establishment for IKE with only MODP-2048; and ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144 Diffie-Hellman key establishment for TLS.
ECDH Private and Public values	Private and public values using the P-256, P-384, and P-521 curves in EC Diffie-Hellman key establishment for TLS and IKE.
DPAPI master secret	512-bit random value used by DPAPI
DPAPI master AES key	256-bit encryption key that protects the DPAPI master secret
DPAPI AES key	256-bit encryption key used by DPAPI
DRBG seed	seed for the main DRBG, zeroized during reseeding

83.1.2 Verdict

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfillment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

83.2 Test Activity

83.2.1 Test 1, Test 2, Test 3 and Test 4

83.2.1.1 Setup

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Testing Machine (Debian 11 Bullseye, using Strongswan U5.9.1/K5.10)
- Windows Client Machine (Platforms listed in the ST)
- Script FCS_IPSEC_EXT.1.14.ps1 is available in TOE
- Script deplot_vpn.sh is available in testing machine

Both machines are in the same network with the following configuration:

- Testing Machine, IP = 20.20.20.100
- Windows Client Machine, IP = 20.20.20.50

83.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMVPN24SD] instructions in order to collect the results as stipulated by the supporting document [PPMVPN24SD].

83.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)

- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006) Gen3

- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)

- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)

- Voyager Klaas Telecom with Azure Stack Hub (build 10.0.17784.1068)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

83.2.1.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 1, Test 2, Test 3 and Test 4** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1, Test 2, Test 3 and Test 4**.

83.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FCS_IPSEC_EXT.1.14.

84 FDP_IFC_EXT.1(VPN)

The assurance activity for the **FDP_IFC_EXT.1(VPN)** requirement is stated as follows:

> The evaluator shall verify that the following is addressed by the documentation:
>
> - The description above indicates that if a VPN client is enabled, all configurations route all IP traffic (other than IP traffic required to establish the VPN connection) through the VPN client.
> - The AGD guidance describes how the user and/or administrator can configure the TSF to meet this requirement.
>
> The evaluator shall perform the following test:
>
> Step 1 -The evaluator shall use the platform to enable a network connection without using IPsec. The evaluator shall use a packet sniffing tool between the platform and an Internet-connected network. The evaluator shall turn on the sniffing tool and perform actions with the device such as navigating to websites, using provided applications, accessing other Internet resources (Use Case 1), accessing another VPN client (Use Case 2), or accessing an IPsec-capable network device (Use Case 3). The evaluator shall verify that the sniffing tool captures the traffic generated by these actions, turn off the sniffing tool, and save the session data.
>
> Step 2 -The evaluator shall configure an IPsec VPN client that supports the routing specified in this requirement, and if necessary, configure the device to perform the routing specified as described in the AGD guidance. The evaluator shall turn on the sniffing tool, establish the VPN connection, and perform the same actions with the device as performed in the first step. The evaluator shall verify that the sniffing tool captures traffic generated by these actions, turn off the sniffing tool, and save the session data.
>
> Step 3 - The evaluator shall examine the traffic from both step one and step two to verify that all IP traffic, aside from and after traffic necessary for establishing the VPN (such as IKE, DNS, and possibly HTTPS), is encapsulated by IPsec.
>
> Step 4 -The evaluator shall attempt to send packets to the TOE outside the VPN connection and shall verify that the TOE discards them.

84.1 Documentation Review activity

84.1.1 Findings

The evaluator has reviewed the section **6.3.2 VPN Client** of the **Security target** doument. It states that all IP traffic is routed through the IPsec tunnel except for:

- IKE traffic used to establish the VPN tunnel.
- IPv4 ARP traffic for resolution of local network layer addresses and to establish a local address.
- IPv6 NDP traffic for resolution of local network layer addresses and to establish a local address.

The evaluator has reviewed the section **6.4.2.3 Configuring a new VPN connection with the Windows UI** of the **Operational and Administrative Guidance** document. It states the following steps outline how to create and configure a new connection in the Windows RAS IPSec VPN client, including choosing options for IKEv1, IKEv1 with a pre-shared key, and IKEv2.

- Open the Settings app;
- Navigate to Network & Internet and choose VPN;
- Choose Add a VPN connection;
- From VPN provider, choose the option for Windows (built in) ;
- Enter the Connection name as a text string ;
- Enter the Server name or address as a DNS name or an IP address. Note that the Subject name of the server's certificate must match the DNS name or IP address entered;
- (Optional) to specify the connection type, choose one of the following:
  - For IKEv1, from VPN type choose L2TP/IPsec with certificate
  - For IKEv1 with a pre-shared key, from VPN type choose L2TP/IPsec with pre-shared key and enter the text of the key
  - For IKEv2, from VPN type choose the IKEv2 option and choose Certificate as the type of sign-in info

- Choose the authentication method from Type of sign-in inf;
- Configure the user credentials as appropriate; *and*
- Save the connection

84.1.2 Verdict

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfillment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

84.2 Test Activity

For this case, all the auditable events will be obtained during the test execution of each security functional requirement.

84.2.1 Test 1

84.2.1.1 Setup

The scenario that is set up is Use Case 3, specified in section **1.4 Use Cases** of document **PP-Module for Virtual Private Networks(VPN) Clients**. Is composed of the following elements:

- Testing Machine (Debian 11 Bullseye, using Strongswan U5.9.1/K5.10)
- Windows Client Machine (Platforms listed in the ST)
- A network packet analyzer application shall be installed on client machine (e.g. *Wireshark*).
- Testing machine must be configured with four network interfaces, one of then with an ip address from network configured in VPN server as leftsubnet, the other with an ip address from network not configured in VPN server
- Following scripts are available:
  - setup.sh
  - deploy_vpn.sh

Both machines are in the same network with the following configuration:

- Testing Machine, IP = 20.20.20.100, 192.168.56.1, 192.168.42.1, 192.168.1.49
- Windows Client Machine, IP = 20.20.20.50

84.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMVPN24SD] instructions in order to collect the results as stipulated by the supporting document [PPMVPN24SD].

84.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- HPE Edgeline EL8000 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Voyager Klaas Telecom with Azure Stack Hub (build 10.0.17784.1068)

- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Panasonic CF-33 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

Results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms*.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

84.2.1.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

84.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FDP_IFC_EXT.1(VPN).

85 FDP_RIP.2

The assurance activity for the **FDP_RIP.2** requirement is stated as follows:

> **TSS**
>
> **Requirement met by the platform**
>
> The evaluator shall examine the TSS to verify that it describes (for each supported platform) the extent to which the client processes network packets and addresses the FDP_RIP.2 requirement.
>
> **Requirement met by the TOE**
>
> "Resources" in the context of this requirement are network packets being sent through (as opposed to "to", as is the case when a security administrator connects to the TOE) the TOE. The concern is that once a network packet is sent, the buffer or memory area used by the packet still contains data from that packet, and that if that buffer is re-used, those data might remain and make their way into a new packet. The evaluator shall check to ensure that the TSS describes packet processing to the extent that they can determine that no data will be reused when processing network packets. The evaluator shall ensure that this description at a minimum describes how the previous data are zeroized/overwritten, and at what point in the buffer processing this occurs.
>
> **Operational Guidance**
>
> There are no guidance EAs for this requirement.
>
> **Test**
>
> There are no test EAs for this requirement.

85.1 Documentation Review activity

85.1.1 Findings

The evaluator has reviewed the section **6.3.3 Memory Management and Object Reuse** of the **Security target** doument. On it, it is described how the client process the network packets and how its content it is not reused.

The following extract from the TSS explains how the memory is managed by the OS to prevent object reuse of network packets:

> *"Windows ensures that any previous information content is unavailable upon allocation to subjects and objects. The TSF ensures that resources processed by the kernel or are exported to user-mode processes do not have residual information in the following ways:*

- *All objects are based on memory and disk storage. Memory allocated for objects, which includes memory allocated for network packets, is either overwritten with all zeros or overwritten with the provided data before being assigned to an object. Read/write pointers prevent reading beyond the space used by the object. Only the exact value of what is most recently written can be read and no more. For varying length objects, subsequent reads only return the exact value that was set, even though the actual allocated size of the object may be greater than this. Objects stored on disk are restricted to only disk space used for that object.*

- *Subject processes using the IPsec client have associated memory and an execution context. The TSF ensures that the memory associated with subjects is either overwritten with all zeros or overwritten with user data before allocation as described in the previous point for memory allocated to objects. In addition, the execution context (processor registers) is initialized when new threads within a process are created and restored when a thread context switch occurs.*
- *Network packets processed by IPsec are encrypted in place. In other words, the data to be encrypted is not copied to a separate buffer and then encrypted. The encrypted network packet is encrypted into the same buffer and overwrites the plaintext network packet. The buffers allocated to hold network packets are allocated with enough space to accommodate padding required for encryption. Each network packet is held in its own buffer. There is a list of buffers, one for each packet. A buffer that holds a network packet is not reused for another network packet. After a buffer holding a network packet is no longer in use the memory allocated for the buffer is freed and released back to the TSF.*

The above, in combination, will ensure that the memory used for inbound and outbound network packets does not contain data from previous use."

85.1.2 Verdict

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfillment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

85.2 Test Activity

There are no test Assurance Activities for this requirement.

85.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FDP_RIP.2.

86 FDP_VPN_EXT.1/VPN

The assurance activity for the **FDP_VPN_EXT.1/VPN** requirement is stated as follows:

> The evaluator shall verify that the following is addressed by the documentation:
>
> - The description above indicates that if a VPN client is enabled, all configurations route all IP traffic (other than IP traffic required to establish the VPN connection) through the VPN client.
> - The AGD guidance describes how the user and/or administrator can configure the TSF to meet this requirement.
>
> The evaluator shall perform the following test:
>
> Step 1 -The evaluator shall use the platform to enable a network connection without using IPsec. The evaluator shall use a packet sniffing tool between the platform and an Internet-connected network. The evaluator shall turn on the sniffing tool and perform actions with the device such as navigating to websites, using provided applications, accessing other Internet resources (Use Case 1), accessing another VPN client (Use Case 2), or accessing an IPsec-capable network device (Use Case 3). The evaluator shall verify that the sniffing tool captures the traffic generated by these actions, turn off the sniffing tool, and save the session data.
>
> Step 2 -The evaluator shall configure an IPsec VPN client that supports the routing specified in this requirement, and if necessary, configure the device to perform the routing specified as described in the AGD guidance. The evaluator shall turn on the sniffing tool, establish the VPN connection, and perform the same actions with the device as performed in the first step. The evaluator shall verify that the sniffing tool captures traffic generated by these actions, turn off the sniffing tool, and save the session data.
>
> Step 3 - The evaluator shall examine the traffic from both step one and step two to verify that all IP traffic, aside from and after traffic necessary for establishing the VPN (such as IKE, DNS, and possibly HTTPS), is encapsulated by IPsec.
>
> Step 4 -The evaluator shall attempt to send packets to the TOE outside the VPN connection and shall verify that the TOE discards them.

86.1 Documentation Review activity

86.1.1 Findings

The evaluator has reviewed the section **6.3.2 VPN Client** of the **Security target** doument. It states that all IP traffic is routed through the IPsec tunnel except for:

- IKE traffic used to establish the VPN tunnel.
- IPv4 ARP traffic for resolution of local network layer addresses and to establish a local address.
- IPv6 NDP traffic for resolution of local network layer addresses and to establish a local address.

The evaluator has reviewed the section **4.4.2.3 Configuring a new VPN connection with the Windows UI** of the ***Operational Guidance*** document. It states the following steps outline how to create and configure a new connection in the Windows RAS IPSec VPN client, including choosing options for IKEv1, IKEv1 with a pre-shared key, and IKEv2.

- Open the Settings app;
- Navigate to Network & Internet and choose VPN;
- Choose Add a VPN connection;
- From VPN provider, choose the option for Windows (built in) ;
- Enter the Connection name as a text string ;
- Enter the Server name or address as a DNS name or an IP address. Note that the Subject name of the server's certificate must match the DNS name or IP address entered;
- (Optional) to specify the connection type, choose one of the following:
  - For IKEv1, from VPN type choose L2TP/IPsec with certificate
  - For IKEv1 with a pre-shared key, from VPN type choose L2TP/IPsec with pre-shared key and enter the text of the key
  - For IKEv2, from VPN type choose the IKEv2 option and choose Certificate as the type of sign-in info
- Choose the authentication method from Type of sign-in inf;
- Configure the user credentials as appropriate; *and*
- Save the connection

86.1.2 Verdict

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfillment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

86.2 Test Activity

For this case, all the auditable events will be obtained during the test execution of each security functional requirement.

86.2.1 Test 1

86.2.1.1 Setup

The scenario that is set up is Use Case 3, specified in section **1.4 Use Cases** of document **PP-Module for Virtual Private Networks(VPN) Clients**. Is composed of the following elements:

- Testing Machine (Debian 11 Bullseye, using Strongswan U5.9.1/K5.10)
- Windows Client Machine (Platforms listed in the ST)
- A network packet analyzer application shall be installed on client machine (e.g. *Wireshark*).
- Testing machine must be configured with four network interfaces, one of then with an ip address from network configured in VPN server as leftsubnet, the other with an ip address from network not configured in VPN server
- Apache2 must be installed in testing machine
- Following scripts are available:
    - setup.sh
    - deploy_vpn.sh

Both machines are in the same network with the following configuration:

- Testing Machine, IP = 20.20.20.100, 192.168.56.1, 192.168.42.1, 192.168.1.49
- Windows Client Machine, IP = 20.20.20.50

86.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMVPN24SD] instructions in order to collect the results as stipulated by the supporting document [PPMVPN24SD].

86.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- HPE Edgeline EL8000 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)

- Voyager Klaas Telecom with Azure Stack Hub (build 10.0.17784.1068)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Panasonic CF-33 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

Results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms*.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE’s behavior is as expected and detailed in the security target [ST004].

86.2.1.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

86.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FDP_VPN_EXT.1/VPN.

87 FIA_PSK_EXT.1

The assurance activity for the **FIA_PSK_EXT.1** requirement is stated as follows:

> The evaluator shall examine the TSS to ensure that it identifies all protocols that allow pre-shared keys. For each protocol identified by the requirement, the evaluator shall confirm that the TSS states which pre-shared key selections are supported.
>
> **Operational Guidance**
>
> The evaluator shall examine the operational guidance to determine that it provides guidance to administrators on how to configure all selected pre-shared key options if any configuration is required.
>
> **Test**
>
> The evaluator shall also perform the following tests for each protocol (or instantiation of a protocol, if performed by a different implementation on the TOE).
>
> - Test 1: For each mechanism selected in FIA_PSK_EXT.1.2, the evaluator shall attempt to establish a connection and confirm that the connection requires the selected factors in the PSK to establish the connection.

87.1 Documentation Review activity

87.1.1 Findings

The ***Security Target*** document, defines in its section **6.4.3 IPSec and Pre-shared Keys**, that IIPsec is the only protocol in this evaluation which supports the use of pre-shared keys. These keys can range from a-z, A-Z, the numbers 0 - 9, and any special character entered from the keyboard. The length of the pre-shared key can range from 1 to 256 characters, and so the specific length of 22 characters which the protection profile requires is supported. And that IPsec pre-shared key is used as-is without modification by Windows and so the pre-shared key does not use the Windows random number generator. The reasoning for this is that if the user needs to supply a particular key, that specific key should be used. If the user desires a randomized bit string, then the solution is to use a X.509 certificate which will contain a bit string of suitable length and randomness.

The evaluator has reviewed section **4.4.3.5 Using pre-shared keys** of the ***Operational Guidance*** document. It states that Windows supports the use of pre-shared keys for IKEv1 / L2TP connections. The secret value for the pre-shared key must be a text-based value manually entered in the input field for a pre-shared key. The secret value input into the client must match the secret value configured on the VPN server. The key must be at least 22 characters in length, but less than 256 characters. The key may be composed of any combination of upper- and lower-case letters, numbers, and the following special characters: "!", "@", "#", "$", "%", "^", "&", "*","(", and")".

87.1.2 Verdict

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfillment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

87.2 Test Activity

For this case, all the auditable events will be obtained during the test execution of each security functional requirement.

87.2.1 Test 1

87.2.1.1 Setup

- The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:
    - Testing Machine (Debian 11 Bullseye, using Strongswan U5.9.1/K5.10)
    - Windows Client Machine (Platforms listed in the ST)
    - Script FIA_PSK_EXT_1.ps1 is available in TOE
    - Script deploy_vpn.sh is available in testing machine

  Both machines are in the same network with the following configuration:

    - Testing Machine, IP = 20.20.20.100
    - Windows Client Machine, IP = 20.20.20.50

87.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMVPN24SD] instructions in order to collect the results as stipulated by the supporting document [PPMVPN24SD].

87.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)

Results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms*.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

87.2.1.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**

87.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FIA_PSK_EXT.1.

88 FIA_PSK_EXT.2

The assurance activity for the **FIA_PSK_EXT.2** requirement is stated as follows:

> If “generate” is selected, the evaluator shall confirm that this process uses the RBG specified in FCS_RBG_EXT.1 and the output matches the size selected in FIA_PSK_EXT.2.1.
>
> **Operational Guidance**
>
> The evaluator shall confirm the operational guidance contains instructions for entering generated pre-shared keys for each protocol identified in the FIA_PSK_EXT.1.1.
>
> **Test**
>
> The evaluator shall also perform the following tests:
>
> - **Test 1 [conditional]**: If generate was selected the evaluator shall generate a pre-shared key and confirm the output matches the size selected in FIA_PSK_EXT.2.1.

88.1 Documentation Review activity

88.1.1 Findings

The ***Security Target*** document, defines in its section **6.4.3 IPSec and Pre-shared Keys**, that IPsec is the only protocol in this evaluation which supports the use of pre-shared keys. And that IPsec pre-shared key is used as-is without modification by Windows and so the pre-shared key does not use the Windows random number generator. The reasoning for this is that if the user needs to supply a particular key, that specific key should be used. If the user desires a randomized bit string, then the solution is to use a X.509 certificate which will contain a bit string of suitable length and randomness.

The evaluator has reviewed section **4.4.3.5 Using pre-shared keys** of the ***Operational Guidance*** document. It states that Windows supports the use of pre-shared keys for IKEv1 / L2TP connections. The secret value for the pre-shared key must be a text-based value manually entered in the input field for a pre-shared key. The secret value input into the client must match the secret value configured on the VPN server. The key must be at least 22 characters in length, but less than 256 characters. The key may be composed of any combination of upper and lower case letters, numbers, and the following special characters: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(” and “)”.

88.1.2 Verdict

Therefore, the evaluator considers that, the findings obtained during the documentation review activity and the selection chosen which has no testing demonstrate the fulfillment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

88.2 Test Activity

There are no test Assurance Activities for this requirement.

88.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FIA_PSK_EXT.2

89 FIA_X509_EXT.3

The assurance activity for the **FIA_X509_EXT.3** requirement is stated as follows:

> The evaluator shall check the TSS to ensure that it describes whether the VPN client or the OS implements the certificate validation functionality, how the VPN client/OS chooses which certificates to use, and any necessary instructions in the administrative guidance for configuring the OS so that desired certificates can be used.
>
> The evaluator shall examine the TSS to confirm that it describes the behavior of the client/OS when a connection cannot be established during the validity check of a certificate used in establishing a trusted channel.
>
> If the requirement indicates that the administrator is able to specify the default action, then the evaluator shall ensure that the operational guidance contains instructions on how this configuration action is performed.
>
> The evaluator shall perform the following test regardless of whether the certificate validation functionality is implemented by the VPN client or by the OS:
>
> - **Test 1:** The evaluator shall demonstrate that using a valid certificate that requires certificate validation checking to be performed in at least some part by communicating with a non-TOE IT entity. The evaluator shall then manipulate the environment so that the TOE is unable to verify the validity of the certificate, and observe that the action selected in FIA_X509_EXT.3.2 is performed. If the selected action is administrator-configurable, then the evaluator shall follow the operational guidance to determine that all supported administrator-configurable options behave in their documented manner.

89.1 Documentation Review activity

89.1.1 Findings

The evaluator has reviews section **6.4.1 X.509 Certificate Validation and Generation** of **Security Target**. This section exposes that every Windows component that uses X.509 certificates is responsible for performing certificate validation, however all components use a common system subcomponent,[See https://learn.microsoft.com/en-us/windows/win32/seccrypto/cryptography-functions?redirectedfrom=MSDN for the win32 interface description for this component.] which validates certificates as described in RFC 5280, and particular, the specific validation listed in section 5.1.4.1.3, including all applicable usage constraints such as Server Authentication for networking sessions and Code Signing when installing product updates. Every component that uses X.509 certificates will have a repository for public certificates and will select a certificate based on criteria such as entity name for the communication partner, any extended key usage constraints, and cryptographic algorithms associated with the certificate. The Windows component will use the same kinds of information along with a certification path and certificate trust lists as part of deciding to accept the certificate.

If certificate validation fails, or if Windows is not able to check the validation status for a certificate, Windows will not establish a trusted network channel, e.g. IPsec, however it will inform the user and seek their consent before establishing a HTTPS web browsing session. Certification validation for updates to Windows, mobile applications, and integrity verification is mandatory, neither the administrator nor the user have the option to bypass the results of a failed certificate validation; software installation and updates is further described in Windows and Application Updates.

When Windows needs to generate a certificate enrollment request it will include a distinguished name, information about the cryptographic algorithms used for the request, any certification extensions, and information about the client requesting the certificate.

The evaluator has reviewed section **4.2.3 Certificate validation and revocation check** of the **Operational and Administrative Guidance** document. It states that Windows automatically compares the distinguished name (DN) in the certificate to the expected distinguished name and does not require additional configuration. The reference identifiers for TLS are the DNS name or IP address of the remote server (ID payload), which is compared against the DNS name as the presented identifier in either the Common Name or the Subject Alternative Name (SAN) of the certificate.

89.1.2 Verdict

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfillment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

89.2 Test Activity

For this case, all the auditable events will be obtained during the test execution of each security functional requirement.

89.2.1 Test 1

89.2.1.1 Setup

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Testing Machine (Debian 11 Bullseye, using Strongswan U5.9.1/K5.10)
- Client Machine (Platforms listed in the ST)

- Scripts FIA_X509_EXT_3.sh, FIA_X509_EXT_3.ps1 and deploy_vpn.sh are available in server

Both machines are in the same network with the following configuration:

- Testing Machine, IP = 20.20.20.100
- Windows Client Machine, IP = 20.20.20.50

89.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMVPN24SD] instructions in order to collect the results as stipulated by the supporting document [PPMVPN24SD].

89.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Windows Server 2019 Hyper-V with Azure Stack HCIv2 version 22H2 (build 10.0.20349.1129)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)

The results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms*.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

89.2.1.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

89.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FIA_X509_EXT.3.

90 FMT_SMF_EXT.1/VPN

The assurance activity for the **FMT_SMF_EXT.1/VPN** requirement is stated as follows:

> The evaluator shall check to ensure the TSS describes the client credentials and how they are used by the TOE.
>
> The evaluator shall check to make sure that every management function mandated in the ST for this requirement is described in the operational guidance and that the description contains the information required to perform the management duties associated with each management function.
>
> The evaluator shall test the TOE's ability to provide the management functions by configuring the TOE according to the operational guidance and testing each management activity listed in the ST.
>
> The evaluator shall ensure that all management functions claimed in the ST can be performed by completing activities described in the AGD. Note that this may be performed in the course of completing other testing.

90.1 Documentation Review activity

90.1.1 Findings

The ***Security Target*** document, defines in its section **6.2.3.3 IPsec**, that Windows implements peer authentication using 2048 bit RSA certificates, or ECDSA certificates using the P-256 and P-384 curves for both IKEv1 and IKEv2. While Windows supports pre-shared keys, it is not recommended due to the potential weak pre-shared keys. Windows simply uses the pre-shared key that was entered by the authorized administrator,there is no additional processing on the input data.

The evaluator has reviewed section **4.4.2.2 Configuring VPN using PowerShell** and **4.4.2.3 Configuring a new VPN connection with the Windows UI** of the **Operational and Administrative Guidance** document. It states the different ways to configure and use a VPN connection, using the different interfaces Windows provides.

90.1.2 Verdict

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfilment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

90.2 Test Activity

For this case, all the auditable events will be obtained during the test execution of each security functional requirement.

90.2.1 Test 1

90.2.1.1 Setup

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Testing Machine (Debian 11 Bullseye, using Strongswan U5.9.1/K5.10)
- Windows Client Machine (Platforms listed in the ST)

Both machines are in the same network with the following configuration:

- Testing Machine, IP = 20.20.20.100
- Windows Client Machine, IP = 20.20.20.50

90.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMVPN24SD] instructions in order to collect the results as stipulated by the supporting document [PPMVPN24SD].

90.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)

- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)

- HPE Edgeline EL8000 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)

Results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms*.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

90.2.1.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

90.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FMT_SMF_EXT.1/VPN.

91 FPT_TST_EXT.1(VPN)

The assurance activity for the **FPT_TST_EXT.1/VPN** requirement is stated as follows:

TSS

The evaluator shall examine the TSS to ensure that it details the self-tests that are run by the TSF on startup; this description should include an outline of what the tests are actually doing (e.g., rather than saying "memory is tested," a description similar to "memory is tested by writing a value to each memory location and reading it back to ensure it is identical to what was written" shall be used). The evaluator shall ensure that the TSS makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly. If some of the tests are performed by the TOE platform, the evaluator shall check the TSS to ensure that those tests are identified, and that the ST for each platform contains a description of those tests. Note that the tests that are required by this component are those that support security functionality in the VPN Client PP-Module, which may not correspond to the set of all self-tests contained in the platform STs.

The evaluator shall examine the TSS to ensure that it describes how the integrity of stored TSF executable code is cryptographically verified when it is loaded for execution. The evaluator shall ensure that the TSS makes an argument that the tests are sufficient to demonstrate that the integrity of stored TSF executable code has not been compromised. The evaluator shall check to ensure that the cryptographic requirements listed are consistent with the description of the integrity verification process.

The evaluator also ensures that the TSS (or the operational guidance) describes the actions that take place for successful (e.g. hash verified) and unsuccessful (e.g., hash not verified) cases. For checks implemented entirely by the platform, the evaluator ensures that the operational guidance for the TOE references or includes the platform-specific guidance for each platform listed in the ST.

Operational Guidance

If not present in the TSS, the evaluator ensures that the operational guidance describes the actions that take place for successful (e.g. hash verified) and unsuccessful (e.g., hash not verified) cases. For checks implemented entirely by the platform, the evaluator ensures that the operational guidance for the TOE references or includes the platform-specific guidance for each platform listed in the ST.

Test

The evaluator shall perform the following tests:

Test 1: The evaluator performs the integrity check on a known good TSF executable and verifies that the check is successful.

Test 2: The evaluator modifies the TSF executable, performs the integrity check on the modified TSF executable and verifies that the check fails.

91.1 Documentation Review activity

91.1.1 Findings

The evaluator has reviewed the section **6.6.4 Windows Platform Integrity and Code Integrity** of the ***Security Target*** document, which describes the different stages of the boot process, providing information about which are the main files loaded in each step of the boot chain.

This information has allowed the evaluator to design a testing plan, which will be used during the test activity. The evaluator has identified four different stages during the boot process:

- **First stage:** Secure boot checks the file integrity of early boot components, comparing them with the values stored in the TPM. Due to the fact that TPM is part of the external TOE environment, this stage will not be tested during the test activity.
- **Second stage:** After the preliminary components have been loaded, the UEFI firmware loads the OS Boot Manager. Once the integrity of OS Boot Manager has been checked, it attempts to load one of these boot applications:
  - OS Loader: *winload.exe* or *winload.efi*
  - OS Resume: *winresume.exe* or *winresume.efi (The administrative guidance states that the hibernation is disabled, so this boot application will not be used during the evaluation)*
  - A physical memory testing application: *memtest.exe (The* **Security Target** *document states that it is considered a non-operational mode for the evaluation).*

  In addition, a list with the critical loaded files during the bootchain when the *winload.exe* is selected has been included. These files are the following:

  - Text intentionally left blank.
- **Third stage:** Once the *winload.exe* or *winload.efi* file has been loaded and its integrity has been checked, the next step in the bootchain is loading the *ntoskrnl.exe* file. Additional critical drivers and libraries are loaded together with this file. The following information is also included regarding Code Integrity, which verifies the integrity of the kernel drivers loaded into the memory. For x64-based computers, all kernel-mode drivers must be digitally signed. If during the boot process an unsigned-driver is loaded, the operating system will not load. On the other hand, for a x86-based computer only the files listed above must be digitally signed. If any of these files are not signed, the operating system will not load. However, if another unsigned-driver is detected during the boot process, the operating system may be loaded normally.

- **Fourth stage:** After the critical device drivers and libraries have been loaded, the Windows kernel continues to boot the rest of the operating system.

The integrity validation mechanism is explained throughout this section, including information about how the TOE validates each piece of software using a hash based signature and an embedded public key as shown in the following extract:

> *[...]After the initial device drivers have been loaded, the Windows kernel will continue to boot the rest of the operating system using the Code Integrity capability (ci.dll) to measure code integrity for (1) the remaining kernel-mode and user-mode programs which need to be loaded for the OS to complete its boot and (2) after booting, CI also verifies the integrity of applications launched by the user (applications from Microsoft are always signed by Microsoft, and third-party applications which may be signed by the developer) by checking the RSA signature for the binary and SHA-256 hashes of the binary which are compared to the catalog files described above.*

The evaluator has reviewed also the section **3.2.7 Code integrity configuration** of the ***Operational Guidance*** document. This section describes the WDAC policy applied during the evaluated configuration process. This policy, which is included with Windows, helps to protect the integrity of executable code that will be recorded in the audit log when this integrity verification fails.

91.1.2 Verdict

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfillment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

91.2 Test Activity

91.2.1 Test 1

91.2.1.1 Setup

Before the test execution, the following setup condition must be fulfilled:

- The SignTool application must be available.

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Testing Machine (Debian 11 Bullseye, using Strongswan 5.9.1)
- Windows Client Machine (Platforms listed in the ST)

Both machines are in the same network with the following configuration:

- Testing Machine, IP = 20.20.20.100
- Windows Client Machine, IP = 20.20.20.50

91.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMVPN24SD] instructions in order to collect the results as stipulated by the supporting document [PPMVPN24SD].

91.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)

- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- HPE Edgeline EL8000 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Voyager Klaas Telecom with Azure Stack Hub (build 10.0.17784.1068)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

Results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms*.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

91.2.1.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

91.2.2 Test 2

91.2.2.1 Setup

Before the test execution, the following setup condition must be fulfilled:

- The SignTool application must be available.
- A hexadecimal editor (e.g. HxD) must be installed in the evaluated platforms to modify the binary files loaded during the VPN connection process; or use *dd* in Testing Machine.

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Testing Machine (Debian 11 Bullseye, using Strongswan 5.9.1)
- Windows Client Machine (Platforms listed in the ST)

Both machines are in the same network with the following configuration:

- Server Machine, IP = 20.20.20.100
- Client Machine, IP = 20.20.20.50

91.2.2.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMVPN24SD] instructions in order to collect the results as stipulated by the supporting document [PPMVPN24SD].

91.2.2.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- HPE Edgeline EL8000 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Voyager Klaas Telecom with Azure Stack Hub (build 10.0.17784.1068)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)

- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

Results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms*.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

91.2.2.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 2** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 2**.

91.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FPT_TST_EXT.1(VPN).

92 FPT_ITC.1(VPN)

The assurance activity for the **FPT_ITC.1(VPN)** requirement is stated as follows:

TSS

The evaluator shall examine the TSS to determine that it describes the details of the TOE connecting to a VPN gateway and/or VPN client and/or IPsec-capable network device in terms of the cryptographic protocols specified in the requirement, along with TOE-specific options or procedures that might not be reflected in the specification. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST.

Operational Guidance

The evaluator shall confirm that the operational guidance contains instructions for establishing the connection to a VPN gateway and/or VPN client and/or IPsec-capable network device, and that it contains recovery instructions should a connection be unintentionally broken.

Test

The evaluator shall perform the following tests:

Test 1: The evaluators shall ensure that the TOE is able to initiate communications with a VPN gateway and/or VPN client and/or IPsec-capable network device using the protocols specified in the requirement, setting up the connections as described in the operational guidance and ensuring that communication is successful.

Test 2: The evaluator shall ensure, for each communication channel with an IPsec peer, the channel data is not sent in plaintext.

Test 3: The evaluator shall ensure, for each communication channel with an IPsec peer, modification of the channel data is detected by the TOE.

Test 4: The evaluators shall physically interrupt the connection from the TOE to the IPsec peer. The evaluators shall ensure that subsequent communications are appropriately protected, at a minimum in the case of any attempts to automatically resume the connection or connect to a new access point.

Further Assurance Activities are associated with requirements for FCS_IPSEC_EXT.1

92.1 Documentation Review activity

92.1.1 Findings

The evaluator has reviewed section **6.3.2 VPN Client** of the ***Security Target*** document. This section states the following:

> The Windows IPsec VPN client can be configured by the device local administrator. The administrator can configure the IPsec VPN client that all IP traffic is routed through the IPsec tunnel except for:
>
> - IKE traffic used to establish the VPN tunnel
> - IPv4 ARP traffic for resolution of local network layer addresses and to establish a local address
> - IPv6 NDP traffic for resolution of local network layer addresses and to establish a local address
>
> The IPsec VPN is an end-to-end internetworking technology and so VPN sessions can be established over physical network protocols such as wireless LAN (Wi-Fi) or local area network.
>
> The components responsible for routing IP traffic through the VPN client:
>
> - The **IPv4/IPv6 network stack** in the kernel processes ingoing and outgoing network traffic.
> - The **IPsec** and **IKE and AuthIP Keying Modules** service which hosts the IKE and Authenticated Internet Protocol (AuthIP) keying modules. These keying modules are used for authentication and key exchange in Internet Protocol security (IPsec).
> - The **Remote Access Service** device driver in the kernel, which is used primarily for VPN connections; known as the “RAS IPsec VPN” or “RAS VPN”.
> - The **IPsec Policy Agent** service which enforces IPsec policies.
>
> Universal Windows App developers can implement their own VPN client if authorized by Microsoft to use the networkingVpnProvider capability, which includes setting the policy to lockdown networking traffic as described above.

The evaluator has reviewed section **4.4 Managing IPsec and VPN connections** of the ***Operational Guidance*** document, where it is described how to establish VPN connections with the VPN client.Test3

This section is composed by the following main subsections:

- 4.4.1 Configuring IPsec firewall rules using Windows Defender Firewall with Advanced Security
- 4.4.2 Configuring and using VPN connections and the VPN client
- 4.4.3 Configuring security association (SA) parameters for IPsec connections

The first subsection describes the different methods available for configuring the firewall rules for IPsec. In addition, there is an explanation about the different rule types: protect, bypass and discard.

The second subsection explains how to configure the VPN client to create a connection profile and establish a VPN connection. There is also information about how to configure the profile to automatically reconnect in case of a network failure. In addition, there are notes about the VPN client limitations and bevahiours of the configurable parameters.

Finally, the third subsection describes how to manage the (Security Associations) between devices. It covers all the range of security configurations like transport mode, lifetimes, signature algorithms, certificate validation/revocation checks and pre-shared keys.

92.1.2 Verdict

The evaluator considers that the information provided in the TSS describes in detail how the VPN client establishes a VPN channel taking into account its different phases and providing the set of available interfaces required for doing that.

Moreover, the operational guidance covers all the managements operations when creating VPN connections with the VPN client, from the available firewall rules to the configuration parameters.

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfillment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

92.2 Test Activity

92.2.1 Test 1

92.2.1.1 Setup

Before the test execution, the following setup condition must be fulfilled:

- A user account with administrator rights shall exist.
- A network packet analyzer application shall be installed on client machine (e.g. *Wireshark*).

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Testing Machine (Debian 11 Bullseye, using Strongswan 5.9.1)
- Windows Client Machine (Platforms listed in the ST)

Both machines are in the same network with the following configuration:

- Testing Machine, IP = 20.20.20.100
- Windows Client Machine, IP = 20.20.20.50

92.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMVPN24SD] instructions in order to collect the results as stipulated by the supporting document [PPMVPN24SD].

92.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)

- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

- Voyager Klaas Telecom with Azure Stack Hub (build 10.0.17784.1068)

- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

92.2.1.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

92.2.2 Test 2

92.2.2.1 Setup

The applicable setup for this test is the same as the one defined in the previous test case.

92.2.2.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMVPN24SD] instructions in order to collect the results as stipulated by the supporting document [PPMVPN24SD].

92.2.2.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)
- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Voyager Klaas Telecom with Azure Stack Hub (build 10.0.17784.1068)
- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

92.2.2.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 2** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 2**.

92.2.3 Test 3

92.2.3.1 Setup

Before the test execution, the following setup condition must be fulfilled:

- A user account with administrator rights shall exist.
- A network packet analyzer application shall be installed on client machine (e.g. *Wireshark*).

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Testing Machine (Debian 11 Bullseye, using Strongswan 5.9.1/K5.10)
- Man in the middle machine (Debian 11, with dsniff package installed)
- Windows Client Machine (Platforms listed in the ST)

Also Corruptor tool must be availabe on the man in the middle machine:

- *Corruptor*: A proprietary application developed by the laboratory that allows to capture and modify packets, according to the protocol. It works by queueing network traffic based on its protocol and modifying the packet in the queue.

The three machines are in the same network with the following configuration:

- Testing Machine, IP = 20.20.20.100
- Client Machine, IP = 20.20.20.50

92.2.3.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMVPN24SD] instructions in order to collect the results as stipulated by the supporting document [PPMVPN24SD].

92.2.3.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)

- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Voyager Klaas Telecom with Azure Stack Hub (build 10.0.17784.1068)
- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)

The results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms*.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

92.2.3.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 3** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 3**.

92.2.4 Test 4

92.2.4.1 Setup

The applicable setup for this test is the same as the one defined in the first test case.

92.2.4.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMVPN24SD] instructions in order to collect the results as stipulated by the supporting document [PPMVPN24SD].

92.2.4.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Windows Server 2022 Hyper-V Windows Server 2022 Datacenter edition (22H2, build 10.0.20348.587)
- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Voyager Klaas Telecom with Azure Stack Hub (build 10.0.17784.1068)
- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)

The results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms*.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

92.2.4.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 4** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 4**.

92.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FPT_ITC.1(VPN).

93 FAU_GEN.1(BT)

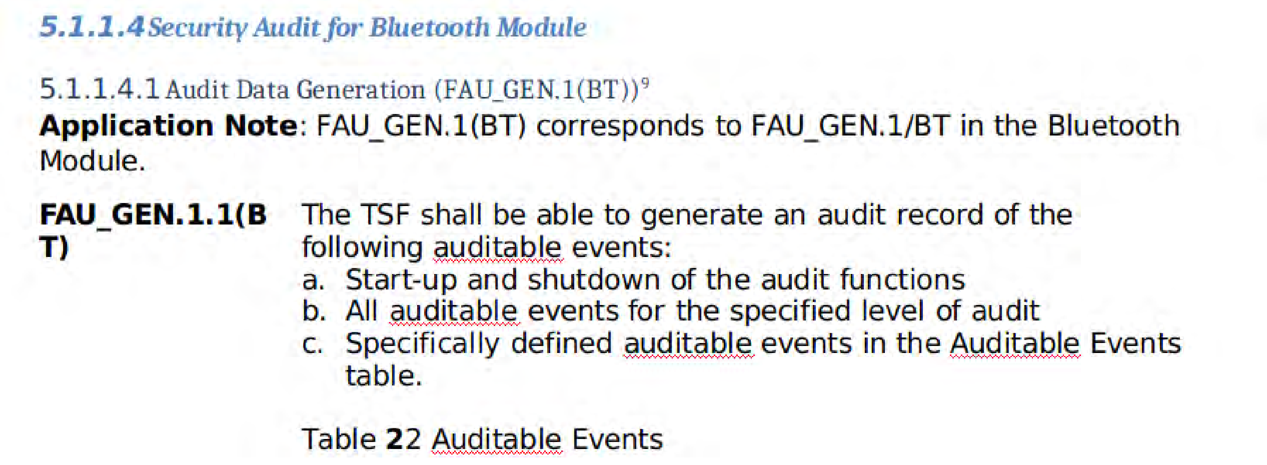
The assurance activity for the **FAU_GEN.1(BT)** requirement is stated as follows:

> There are additional auditable events that serve to extend the FAU_GEN.1 SFR found in each Base-PP.
>
> This SFR is evaluated in the same manner as defined by the Evaluation Activities for the claimed Base-PP.
>
> The only difference is that the evaluator shall also assess the auditable events required for this PP-Module in addition to those defined in the claimed Base-PP.

93.1 Documentation Review activity

93.1.1 Findings

The ***Security Target*** document, defines in its section **5.1.1.4.1 Audit Data Generation (FAU_GEN.1(BT))**, the following auditable events:



5.1.1.4 Security Audit for Bluetooth Module

5.1.1.4.1 Audit Data Generation (FAU_GEN.1(BT))[9]

Application Note: FAU_GEN.1(BT) corresponds to FAU_GEN.1/BT in the Bluetooth Module.

FAU_GEN.1.1(BT) The TSF shall be able to generate an audit record of the following auditable events:

a. Start-up and shutdown of the audit functions
b. All auditable events for the specified level of audit
c. Specifically defined auditable events in the Auditable Events table.

Table **2**2 Auditable Events

The evaluator has reviewed the section **5.1.1.4 Security Audit for Bluetooth Module** of the **Security Target** document, which determines the events to be audited for this requirement, specifically in table 22.

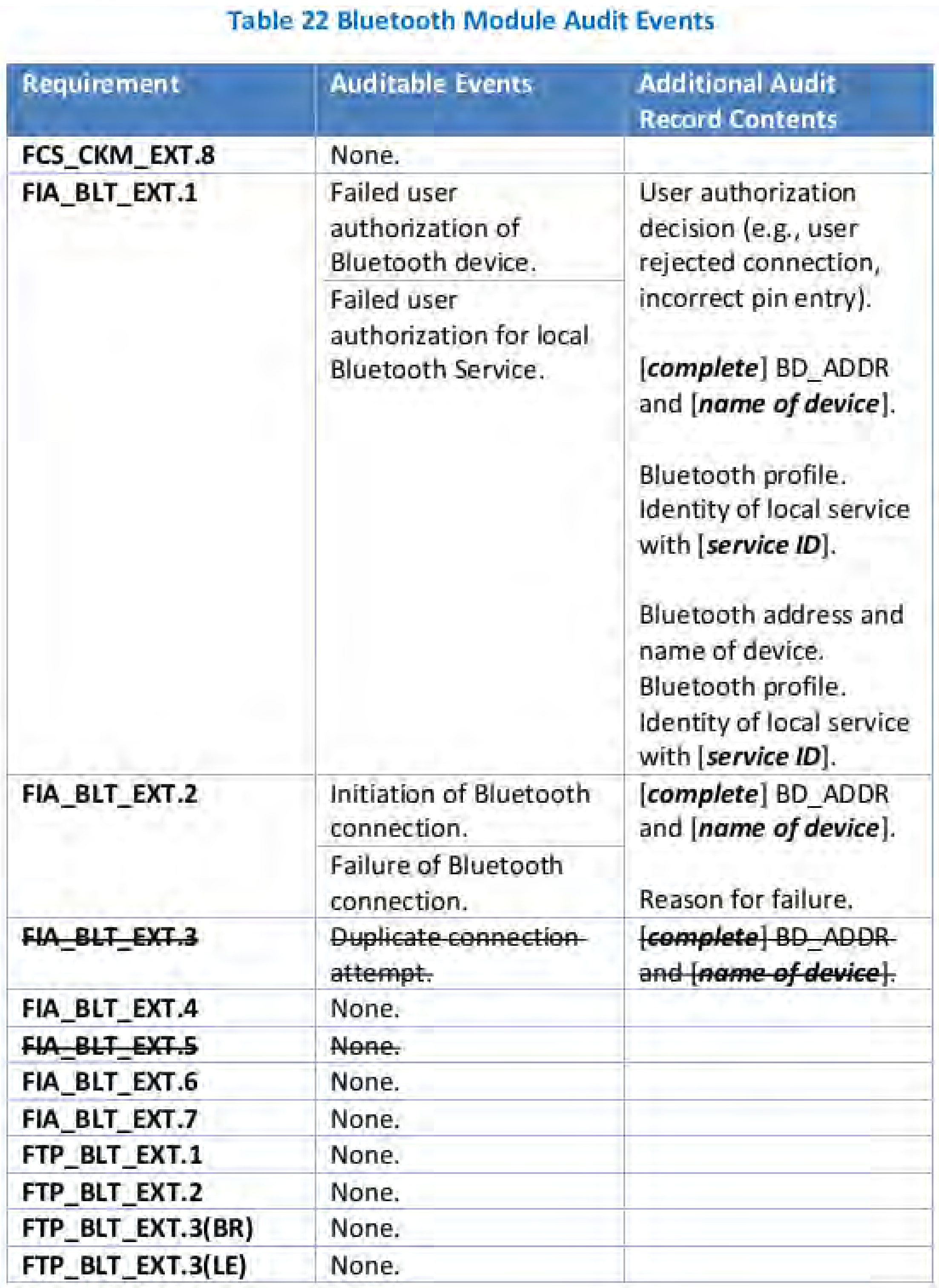


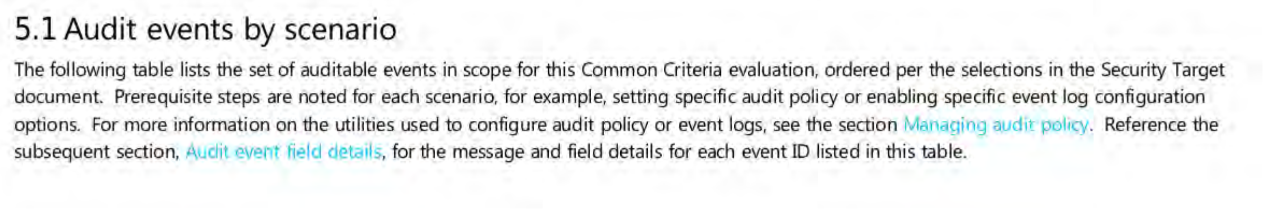
Table 22 Bluetooth Module Audit Events

Requirement	Auditable Events	Additional Audit Record Contents
FCS_CKM_EXT.8	None.	
FIA_BLT_EXT.1	Failed user authorization of Bluetooth device. Failed user authorization for local Bluetooth Service.	User authorization decision (e.g., user rejected connection, incorrect pin entry). [***complete***] BD_ADDR and [***name of device***]. Bluetooth profile. Identity of local service with [***service ID***]. Bluetooth address and name of device. Bluetooth profile. Identity of local service with [***service ID***].
FIA_BLT_EXT.2	Initiation of Bluetooth connection. Failure of Bluetooth connection.	[***complete***] BD_ADDR and [***name of device***]. Reason for failure.
~~**FIA_BLT_EXT.3**~~	~~Duplicate connection attempt.~~	~~[***complete***] BD_ADDR and [***name of device***].~~
FIA_BLT_EXT.4	None.	
~~**FIA_BLT_EXT.5**~~	~~None.~~	
FIA_BLT_EXT.6	None.	
FIA_BLT_EXT.7	None.	
FTP_BLT_EXT.1	None.	
FTP_BLT_EXT.2	None.	
FTP_BLT_EXT.3(BR)	None.	
FTP_BLT_EXT.3(LE)	None.	

This document also states the minimum information that each audit record should include. These fields are the following:

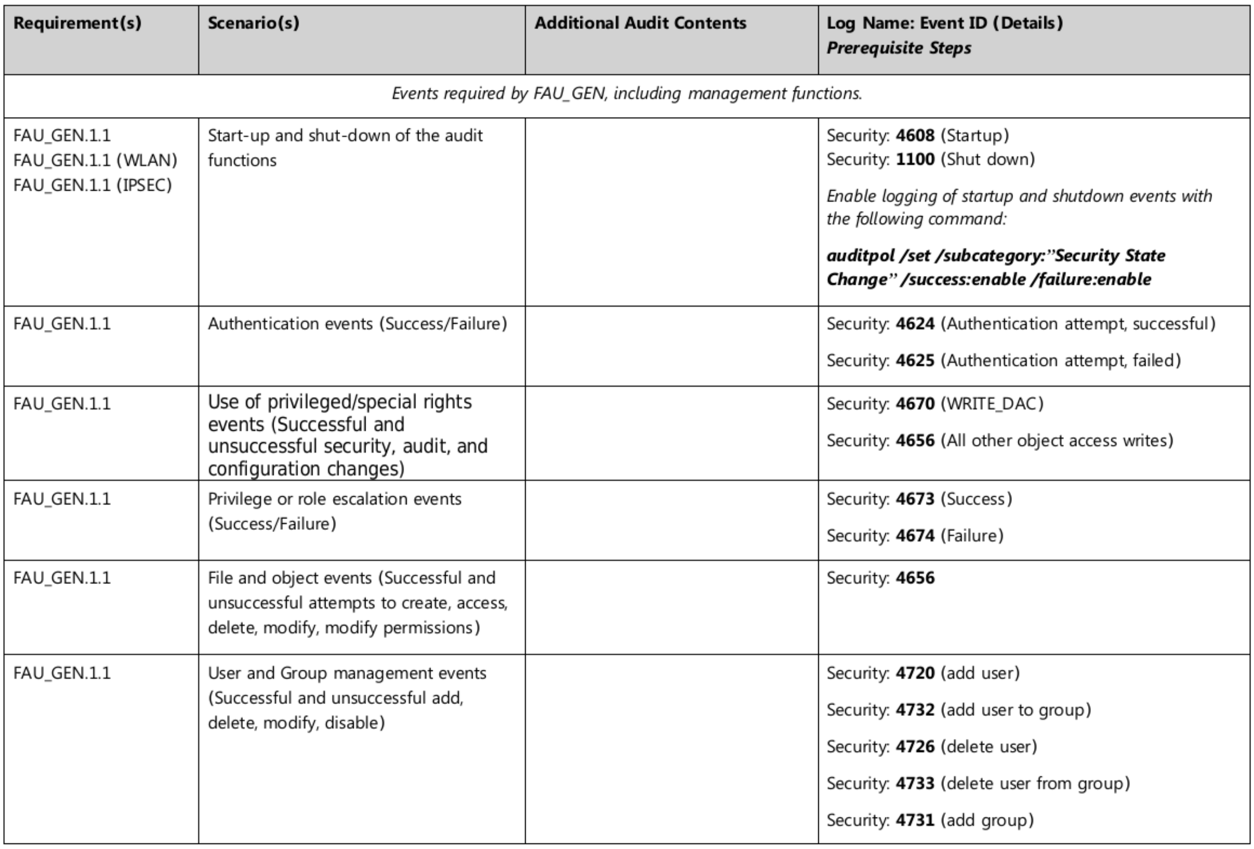
- Date and time of the event.
- Type of the event.
- Subject identity.
- Outcome (success or failure) of the event.
- For each audit event type, based on the auditable event definitions of the functional components included in the PP-Module/ST, information specified in column three of Table 22.

In addition, the ***Operational Guidance*** document, includes in its section **5.1 Audit Events by scenario** a table with all the auditable events generated by the TOE.

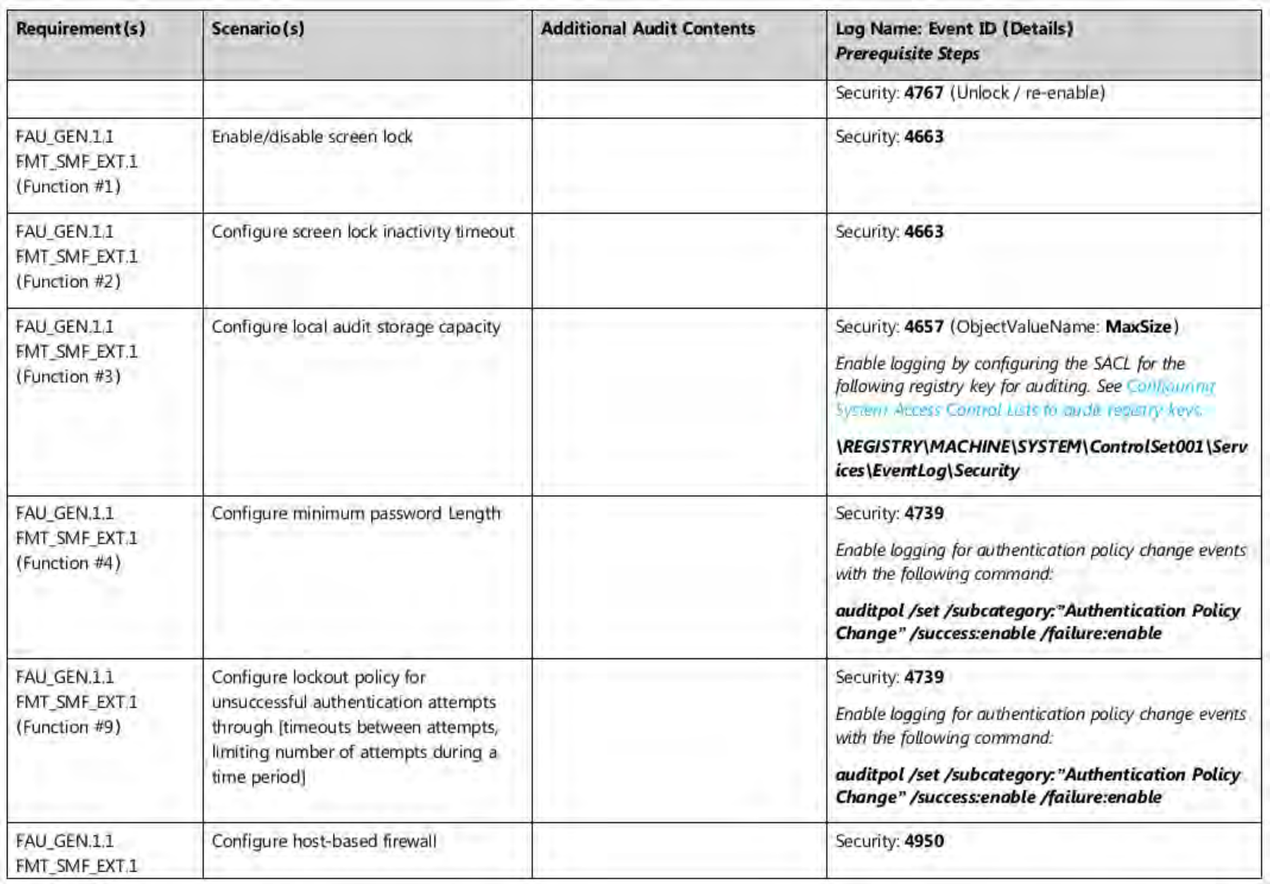


5.1 Audit events by scenario

The following table lists the set of auditable events in scope for this Common Criteria evaluation, ordered per the selections in the Security Target document. Prerequisite steps are noted for each scenario, for example, setting specific audit policy or enabling specific event log configuration options. For more information on the utilities used to configure audit policy or event logs, see the section Managing audit policy. Reference the subsequent section, Audit event field details, for the message and field details for each event ID listed in this table.



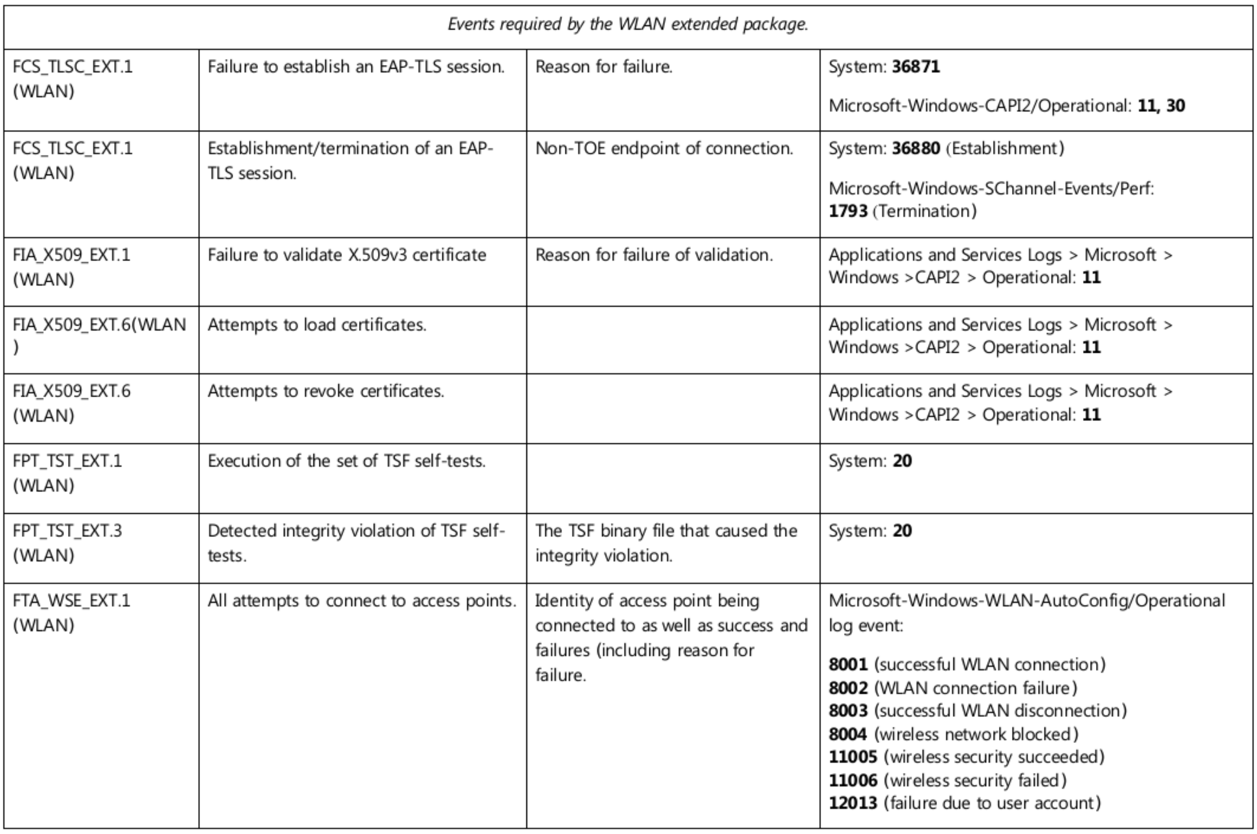
Requirement(s)	**Scenario(s)**	**Additional Audit Contents**	**Log Name: Event ID (Details)** ***Prerequisite Steps***
	Events required by FAU_GEN, including management functions.		
FAU_GEN.1.1 FAU_GEN.1.1 (WLAN) FAU_GEN.1.1 (IPSEC)	Start-up and shut-down of the audit functions		Security: **4608** (Startup) Security: **1100** (Shut down) *Enable logging of startup and shutdown events with the following command:* ***auditpol /set /subcategory:"Security State Change" /success:enable /failure:enable***
FAU_GEN.1.1	Authentication events (Success/Failure)		Security: **4624** (Authentication attempt, successful) Security: **4625** (Authentication attempt, failed)
FAU_GEN.1.1	Use of privileged/special rights events (Successful and unsuccessful security, audit, and configuration changes)		Security: **4670** (WRITE_DAC) Security: **4656** (All other object access writes)
FAU_GEN.1.1	Privilege or role escalation events (Success/Failure)		Security: **4673** (Success) Security: **4674** (Failure)
FAU_GEN.1.1	File and object events (Successful and unsuccessful attempts to create, access, delete, modify, modify permissions)		Security: **4656**
FAU_GEN.1.1	User and Group management events (Successful and unsuccessful add, delete, modify, disable)		Security: **4720** (add user) Security: **4732** (add user to group) Security: **4726** (delete user) Security: **4733** (delete user from group) Security: **4731** (add group)



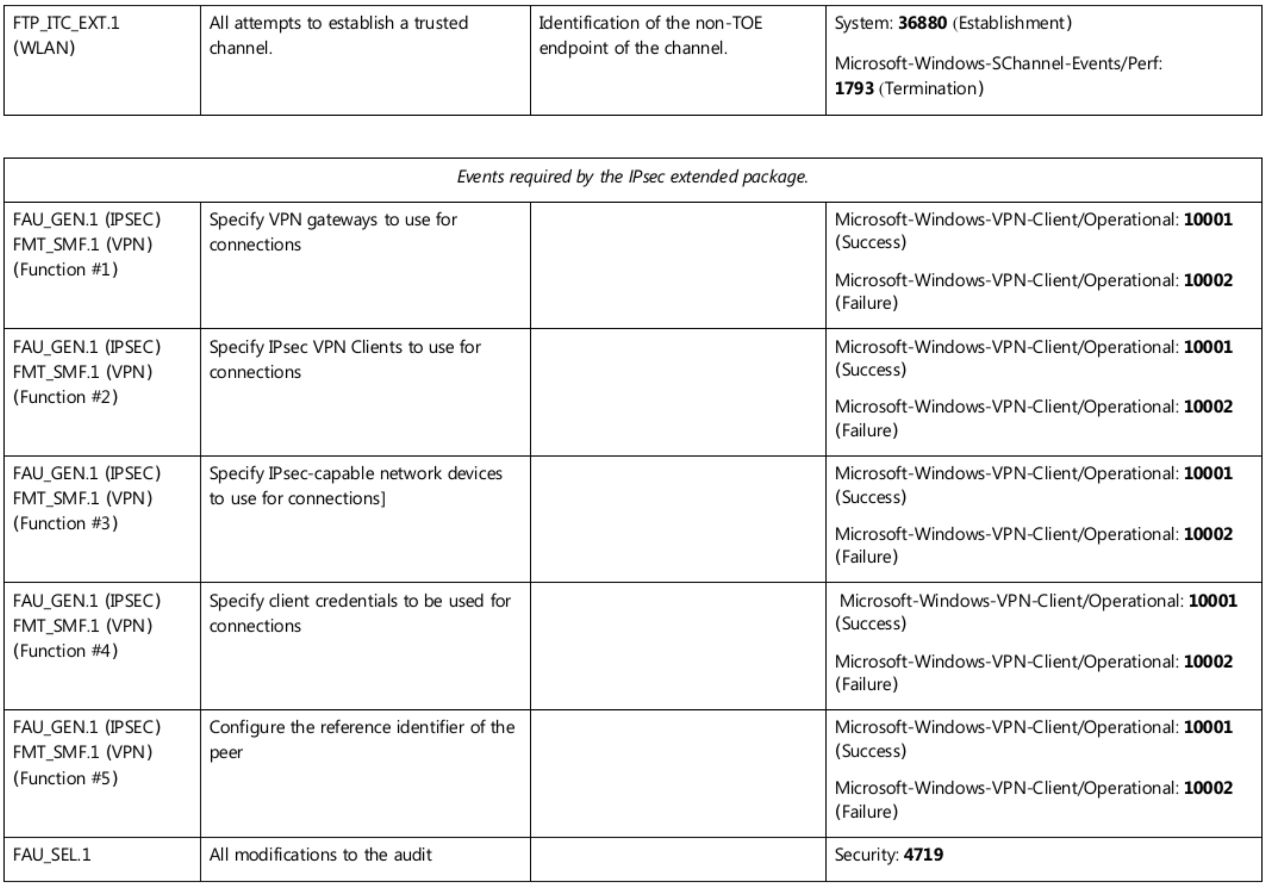
Requirement(s)	**Scenario(s)**	**Additional Audit Contents**	**Log Name: Event ID (Details)** ***Prerequisite Steps***
			Security: **4767** (Unlock / re-enable)
FAU_GEN.1.1 FMT_SMF_EXT.1 (Function #1)	Enable/disable screen lock		Security: **4663**
FAU_GEN.1.1 FMT_SMF_EXT.1 (Function #2)	Configure screen lock inactivity timeout		Security: **4663**
FAU_GEN.1.1 FMT_SMF_EXT.1 (Function #3)	Configure local audit storage capacity		Security: **4657** (ObjectValueName: **MaxSize**) *Enable logging by configuring the SACL for the following registry key for auditing. See Configuring System Access Control Lists to audit registry keys.* ***\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\EventLog\Security***
FAU_GEN.1.1 FMT_SMF_EXT.1 (Function #4)	Configure minimum password Length		Security: **4739** *Enable logging for authentication policy change events with the following command:* ***auditpol /set /subcategory:"Authentication Policy Change" /success:enable /failure:enable***
FAU_GEN.1.1 FMT_SMF_EXT.1 (Function #9)	Configure lockout policy for unsuccessful authentication attempts through [timeouts between attempts, limiting number of attempts during a time period]		Security: **4739** *Enable logging for authentication policy change events with the following command:* ***auditpol /set /subcategory:"Authentication Policy Change" /success:enable /failure:enable***
FAU_GEN.1.1 FMT_SMF_EXT.1	Configure host-based firewall		Security: **4950**

Requirement(s)	**Scenario(s)**	**Additional Audit Contents**	**Log Name: Event ID (Details)** ***Prerequisite Steps***
(Function #10)			
FAU_GEN.1.1 FMT_SMF_EXT.1 (Function #11)	Configure name/address of directory server to bind with		System: **3260** (non-virtual device) System: **4096** (virtual device)
FAU_GEN.1.1 FMT_SMF_EXT.1 (Function #12)	Configure name/address of remote management server from which to receive management settings		System: **3260** (non-virtual device) System: **4096** (virtual device)
FAU_GEN.1.1 FMT_SMF_EXT.1 (Function #14)	Configure audit rules		Security: **4719** *Enable events for audit policy changes with the following command:* ***auditpol /set /subcategory:"Audit Policy Change" /success:enable /failure:enable***
FAU_GEN.1.1 FMT_SMF_EXT.1 (Function #15)	Configure name/address of network time server		System: **37**
FAU_GEN.1.1 FMT_SMF_EXT.1 (Function #16)	Enable/disable automatic software update		Security: **4657** (ObjectValueName: **NoAutoUpdate**) *Enable logging by configuring the SACL for the following registry key for auditing. See Configuring System Access Control Lists to audit registry keys.* ***\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU***
FAU_GEN.1.1 FMT_SMF_EXT.1 (Function #17)	Configure Wi-Fi interface		Security: **6420** (enable) Security: **6422** (disable)

Requirement(s)	**Scenario(s)**	**Additional Audit Contents**	**Log Name: Event ID (Details)** ***Prerequisite Steps***
FAU_GEN.1.1 FMT_SMF_EXT.1 (Function #18)	Enable/disable Bluetooth interface		Security: **6420** (enable) Security: **6422** (disable)
FAU_GEN.1.1 FMT_SMF_EXT.1 (Function #19)	Enable/disable local area network interface		Security: **6420** (enable) Security: **6422** (disable)
FAU_GEN.1.1 FMT_SMF_EXT.1 (Function #19)	Configure USB interfaces		Security: **6420** (enable) Security: **6422** (disable)
FAU_GEN.1.1 FMT_SMF_EXT.1 (Function #20)	Manage Windows Diagnostics settings		
FAU_GEN.1.1 FMT_SMF_EXT.1 (Function #20)	Configure remote connection inactivity timeout		Security: **4657** (ObjectValueName: **MaxIdleTime**) *Enable logging by configuring the SACL for the following registry key for auditing. See Configuring System Access Control Lists to audit registry keys.* ***\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\Terminal Services***

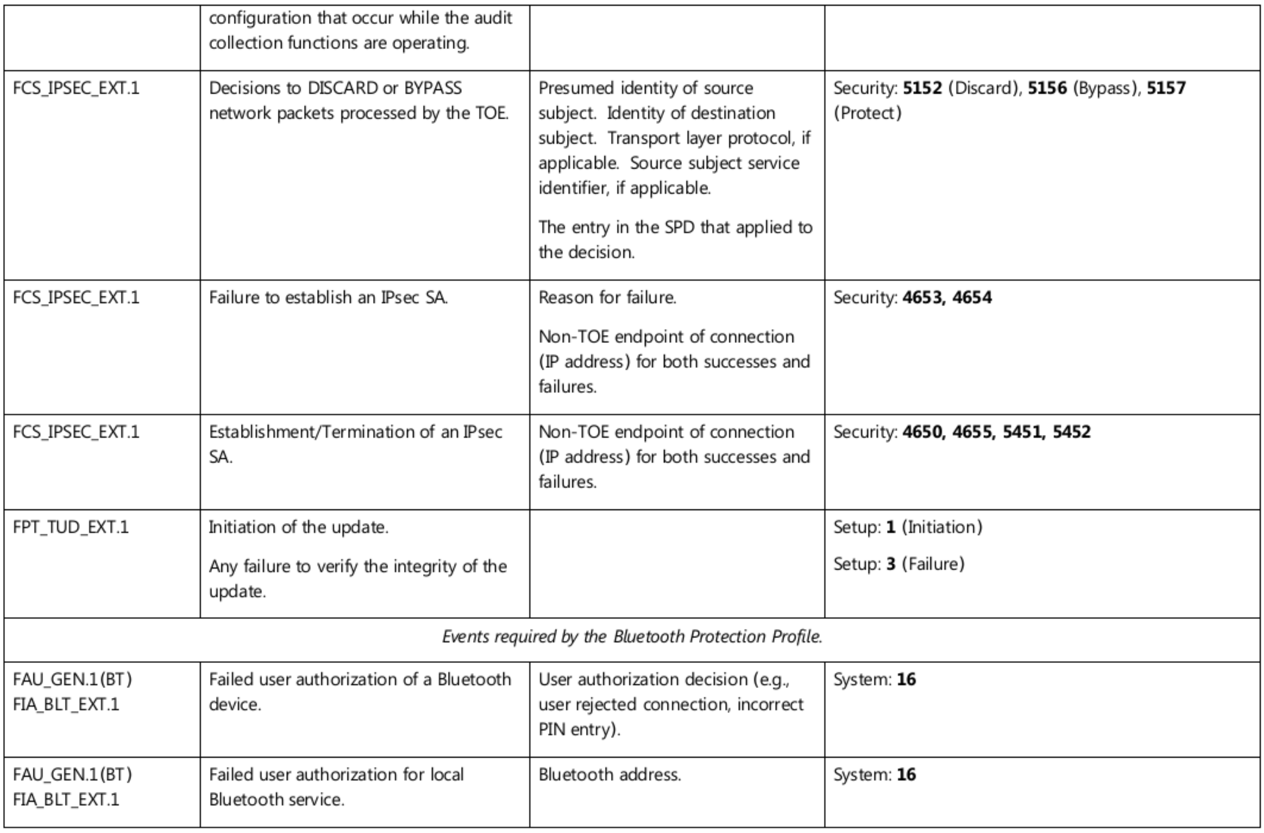


Events required by the WLAN extended package.			
FCS_TLSC_EXT.1 (WLAN)	Failure to establish an EAP-TLS session.	Reason for failure.	System: **36871** Microsoft-Windows-CAPI2/Operational: **11, 30**
FCS_TLSC_EXT.1 (WLAN)	Establishment/termination of an EAP-TLS session.	Non-TOE endpoint of connection.	System: **36880** (Establishment) Microsoft-Windows-SChannel-Events/Perf: **1793** (Termination)
FIA_X509_EXT.1 (WLAN)	Failure to validate X.509v3 certificate	Reason for failure of validation.	Applications and Services Logs > Microsoft > Windows >CAPI2 > Operational: **11**
FIA_X509_EXT.6(WLAN)	Attempts to load certificates.		Applications and Services Logs > Microsoft > Windows >CAPI2 > Operational: **11**
FIA_X509_EXT.6 (WLAN)	Attempts to revoke certificates.		Applications and Services Logs > Microsoft > Windows >CAPI2 > Operational: **11**
FPT_TST_EXT.1 (WLAN)	Execution of the set of TSF self-tests.		System: **20**
FPT_TST_EXT.3 (WLAN)	Detected integrity violation of TSF self-tests.	The TSF binary file that caused the integrity violation.	System: **20**
FTA_WSE_EXT.1 (WLAN)	All attempts to connect to access points.	Identity of access point being connected to as well as success and failures (including reason for failure.	Microsoft-Windows-WLAN-AutoConfig/Operational log event: **8001** (successful WLAN connection) **8002** (WLAN connection failure) **8003** (successful WLAN disconnection) **8004** (wireless network blocked) **11005** (wireless security succeeded) **11006** (wireless security failed) **12013** (failure due to user account)

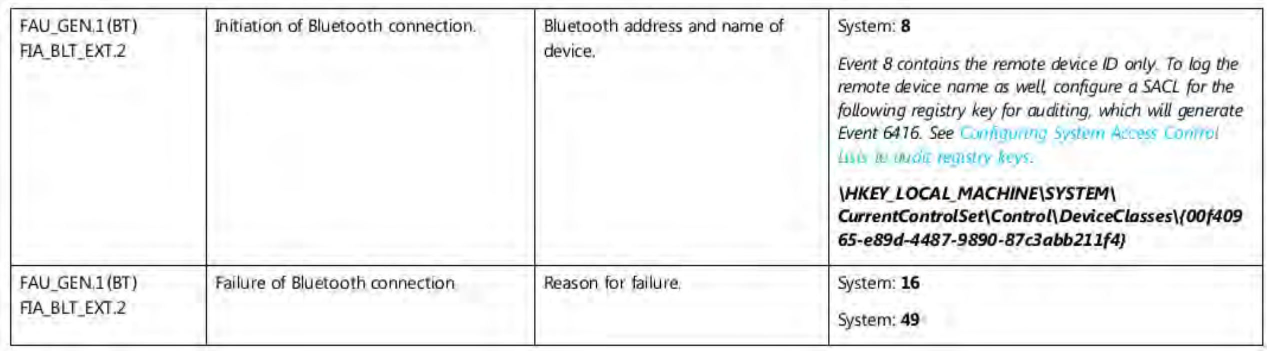


FTP_ITC_EXT.1 (WLAN)	All attempts to establish a trusted channel.	Identification of the non-TOE endpoint of the channel.	System: **36880** (Establishment) Microsoft-Windows-SChannel-Events/Perf: **1793** (Termination)

Events required by the IPsec extended package.			
FAU_GEN.1 (IPSEC) FMT_SMF.1 (VPN) (Function #1)	Specify VPN gateways to use for connections		Microsoft-Windows-VPN-Client/Operational: **10001** (Success) Microsoft-Windows-VPN-Client/Operational: **10002** (Failure)
FAU_GEN.1 (IPSEC) FMT_SMF.1 (VPN) (Function #2)	Specify IPsec VPN Clients to use for connections		Microsoft-Windows-VPN-Client/Operational: **10001** (Success) Microsoft-Windows-VPN-Client/Operational: **10002** (Failure)
FAU_GEN.1 (IPSEC) FMT_SMF.1 (VPN) (Function #3)	Specify IPsec-capable network devices to use for connections]		Microsoft-Windows-VPN-Client/Operational: **10001** (Success) Microsoft-Windows-VPN-Client/Operational: **10002** (Failure)
FAU_GEN.1 (IPSEC) FMT_SMF.1 (VPN) (Function #4)	Specify client credentials to be used for connections		Microsoft-Windows-VPN-Client/Operational: **10001** (Success) Microsoft-Windows-VPN-Client/Operational: **10002** (Failure)
FAU_GEN.1 (IPSEC) FMT_SMF.1 (VPN) (Function #5)	Configure the reference identifier of the peer		Microsoft-Windows-VPN-Client/Operational: **10001** (Success) Microsoft-Windows-VPN-Client/Operational: **10002** (Failure)
FAU_SEL.1	All modifications to the audit		Security: **4719**



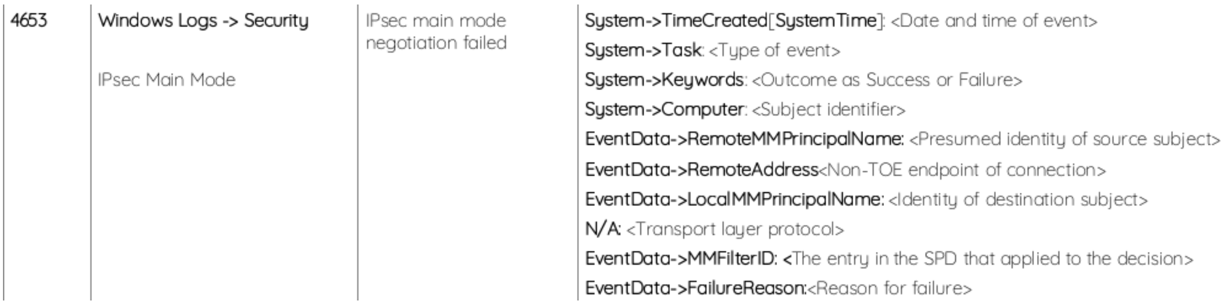
	configuration that occur while the audit collection functions are operating.		
FCS_IPSEC_EXT.1	Decisions to DISCARD or BYPASS network packets processed by the TOE.	Presumed identity of source subject. Identity of destination subject. Transport layer protocol, if applicable. Source subject service identifier, if applicable. The entry in the SPD that applied to the decision.	Security: **5152** (Discard), **5156** (Bypass), **5157** (Protect)
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.	Security: **4653, 4654**
FCS_IPSEC_EXT.1	Establishment/Termination of an IPsec SA.	Non-TOE endpoint of connection (IP address) for both successes and failures.	Security: **4650, 4655, 5451, 5452**
FPT_TUD_EXT.1	Initiation of the update. Any failure to verify the integrity of the update.		Setup: **1** (Initiation) Setup: **3** (Failure)
Events required by the Bluetooth Protection Profile.			
FAU_GEN.1(BT) FIA_BLT_EXT.1	Failed user authorization of a Bluetooth device.	User authorization decision (e.g., user rejected connection, incorrect PIN entry).	System: **16**
FAU_GEN.1(BT) FIA_BLT_EXT.1	Failed user authorization for local Bluetooth service.	Bluetooth address.	System: **16**



FAU_GEN.1(BT) FIA_BLT_EXT.2	Initiation of Bluetooth connection.	Bluetooth address and name of device.	System: **8** *Event 8 contains the remote device ID only. To log the remote device name as well, configure a SACL for the following registry key for auditing, which will generate Event 6416. See Configuring System Access Control Lists to audit registry keys.* ***\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\{00f40965-e89d-4487-9890-87c3abb211f4}***
FAU_GEN.1(BT) FIA_BLT_EXT.2	Failure of Bluetooth connection.	Reason for failure.	System: **16** System: **49**

The content of this table matches with the selection performed by the vendor in the ***Security Target*** document, as it can be seen in the image above.

Moreover, the ***Operational Guidance*** document also provides information related the main fields for each auditable event. This information includes the auditable events, the additional audit record contents and the event ID for each one. For example, the following image shows the main required fields for the auditable event 4653 (*IPsec main mode negotation failed*).



4653	Windows Logs -> Security IPsec Main Mode	IPsec main mode negotiation failed	System->TimeCreated[SystemTime]: <Date and time of event> System->Task: <Type of event> System->Keywords: <Outcome as Success or Failure> System->Computer: <Subject identifier> EventData->RemoteMMPrincipalName: <Presumed identity of source subject> EventData->RemoteAddress<Non-TOE endpoint of connection> EventData->LocalMMPrincipalName: <Identity of destination subject> N/A: <Transport layer protocol> EventData->MMFilterID: <The entry in the SPD that applied to the decision> EventData->FailureReason:<Reason for failure>

93.1.2 Verdict

The evaluator has reviewed the ***Security Target*** document and has ensured that every auditable event type selected in the ***Security Target*** document is included in the ***Operational Guidance*** document. Moreover, the evaluator has also ensured that the format of every auditable event is described, including at least the fields defined in the ***Security Target*** document (*date and time, type of the event, subject identity, outcome and information of column 3*).

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfilment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to this activity.

93.2 Test Activity

For this requirement, some of the auditable events will be obtained during the test execution of each security functional requirement.

93.2.1 Test 1

93.2.1.1 Setup

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Testing Machine (Debian 11 Bullseye, using bluez and bluetooth adapter)
- Windows Client Machine (Platforms listed in the ST)
- Wireshark

The additional setup required for obtaining each auditable event listed in Table 22 will be described in the *Setup* section of the following requirements:

- FIA_BLT_EXT.1
- FIA_BLT_EXT.2

All the audit events required will be obtained and described in each test defined in the previous list. In addition, the audit events will be shown in the results section for the sake of a better readability.

93.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMBT10SD] instructions in order to collect the results as stipulated by the supporting document [PPMBT10SD].

93.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Voyager Klaas Telecom with Azure Stack Hub (build 10.0.17784.1068)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)

Results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms*.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

93.2.1.4 Verdict

As the result above states, the related events have been correctly generated and they include all the information defined in the ***Security Target*** document.

Due to this, the evaluator considers that the results obtained from the test activity demonstrate the fulfilment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

93.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FAU_GEN.1(BT).

94 FCS_CKM.8 (BT)

The assurance activity for the **FCS_CKM.8 (BT)** requirement is stated as follows:

> **TSS**
>
> The evaluator shall ensure that the TSS describes the criteria used to determine the frequency of generating new ECDH public/private key pairs. In particular, the evaluator shall ensure that the implementation does not permit the use of static ECDH key pairs.
>
> **Guidance**
>
> There are no guidance evaluation activities for this component.
>
> **Tests**
>
> The evaluator shall perform the following steps:
>
> Step 1: Pair the TOE to a remote Bluetooth device and record the public key currently in use by the TOE. (This public key can be obtained using a Bluetooth protocol analyzer to inspect packets exchanged during pairing.)
>
> Step 2: Perform necessary actions to generate new ECDH public/private key pairs. (Note that this test step depends on how the TSS describes the criteria used to determine the frequency of generating new ECDH public/private key pairs.)
>
> Step 3: Pair the TOE to a remote Bluetooth device and again record the public key currently in use by the TOE.
>
> Step 4: Verify that the public key in Step 1 differs from the public key in Step 3.

94.1 Documentation Review activity

94.1.1 Findings

The ***Security Target*** document, defines in its section **6.2.1 Cryptographic Algorithms and Operations**, that Windows 10, Windows 11 and Windows Server implements elliptic curve Diffie Hellman (ECDH).

The **Bluetooth® Core Specification Version 5.2** in Vol 2. BR/EDR Controller, Part H: Security Specification, section 1 Security Overview shown how the Key Generation using ECDH is performed and Vol 2. BR/EDR Controller, Part H: Security Specification, section7 Security Simple Pairing explains how works ECDH when Secure Simple Pairing. In Vol 3. Host, Part H: Security Manager Specification, Section 2.3.5.6 LE Secure Connections pairing phase 2 shown how the Public key exchange using ECDH is performed.

94.1.2 Verdict

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfillment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

94.2 Test Activity

For this case, all the auditable events will be obtained during the test execution of each security functional requirement.

94.2.1 Test 1

94.2.1.1 Setup

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Testing Machine (Debian 11 Bullseye, using bluez and bluetooth adapter)
- Windows Client Machine (Platforms listed in the ST)
- Wireshark

94.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMBT10SD] instructions in order to collect the results as stipulated by the supporting document [PPMBT10SD].

94.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

94.2.1.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

94.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FCS_CKM.8 (BT).

95 FIA_BLT_EXT.1

The assurance activity for the **FIA_BLT_EXT.1** requirement is stated as follows:

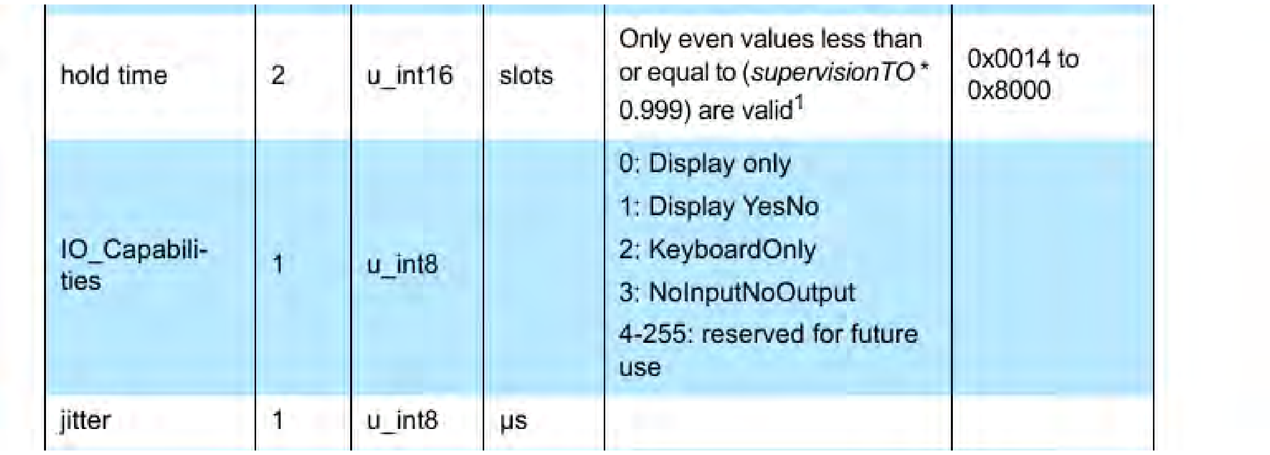
> **TSS**
>
> The evaluator shall examine the TSS to ensure that it contains a description of when user permission is required for Bluetooth pairing; and that this description mandates explicit user authorization via manual input for all Bluetooth pairing; including application use of the Bluetooth trusted channel and situations where temporary (non-bonded) connections are formed.
>
> **Operational Guidance**
>
> The evaluator shall examine the API documentation provided as a means of satisfying the requirements for the ADV assurance class (see section 5.2.2 in the MDF PP and GPOS PP) and verify that this API documentation does not include any API for programmatic entering of pairing information (e.g. PINs; numeric codes; or “yes/no” responses) intended to bypass manual user input during pairing.
>
> The evaluator shall examine the guidance to verify that these user authorization screens are clearly identified and instructions are given for authorizing Bluetooth pairings.
>
> **Test**
>
> The evaluator shall perform the following steps:
>
> Step 1: Initiate pairing with the TOE from a remote Bluetooth device that requests no man-in-the-middle protection; no bonding; and claims to have NoInput/NoOutput (IO) capability. Such a device will attempt to evoke behavior from the TOE that represents the minimal level of user interaction that the TOE supports during pairing.
>
> Step 2: Verify that the TOE does not permit any Bluetooth pairing without explicit authorization from the user (e.g. the user must have to minimally answer “yes” or “allow” in a prompt).

95.1 Documentation Review activity

95.1.1 Findings

The ***Security Target*** document, defines in its section **5.1.4.4 identification and Authentication for Bluetooth Module**, that Windows 10, Windows 11 and Windows Server implement the required mechanisms to ensure that the TOE requires explicit user authorization for Bluetooth pairing when required.

The **Bluetooth® Core Specification Version 5.2** defines the parameters definition in Vol 2. BR/EDR Controller section 5.2 PARAMETER DEFINITIONS, in Table 5.2 Parameters in LM PDUs, row "IO_Capabilities".



hold time	2	u_int16	slots	Only even values less than or equal to (*supervisionTO* * 0.999) are valid[1]	0x0014 to 0x8000
IO_Capabilities	1	u_int8		0: Display only 1: Display YesNo 2: KeyboardOnly 3: NoInputNoOutput 4-255: reserved for future use	
jitter	1	u_int8	µs		

95.1.2 Verdict

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfillment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

95.2 Test Activity

For this case, all the auditable events will be obtained during the test execution of each security functional requirement.

95.2.1 Test 1

95.2.1.1 Setup

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Testing Machine (Debian 11 Bullseye, using bluez and bluetooth adapter)
- Windows Client Machine (Platforms listed in the ST)
- Bluetooth Virtual Sniffer (btvs.exe)

95.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMBT10SD] instructions in order to collect the results as stipulated by the supporting document [PPMBT10SD].

95.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Voyager Klaas Telecom with Azure Stack Hub (build 10.0.17784.1068)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)

Results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms*.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

95.2.1.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 1** requirements established in the assurance activity section.

95.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FIA_BLT_EXT.1

96 FIA_BLT_EXT.2

The assurance activity for the **FIA_BLT_EXT.2** requirement is stated as follows:

> **TSS**
>
> The evaluator shall ensure that the TSS describes how data transfer of any type is prevented before the Bluetooth pairing is completed. The TSS shall specifically call out any supported RFCOMM and L2CAP data transfer mechanisms. The evaluator shall ensure that the data transfers are only completed after the Bluetooth devices are paired and mutually authenticated.
>
> **Operational Guidance**
>
> There are no guidance evaluation activities for this component.
>
> **Test**
>
> The evaluator shall use a Bluetooth tool to attempt to access TOE files using the OBEX Object Push service (OBEX Push) and verify that pairing and mutual authentication are required by the TOE before allowing access. If the OBEX Object Push service is unsupported on the TOE; a different service that transfers data over Bluetooth L2CAP and/or RFCOMM may be used in this test.

96.1 Documentation Review activity

96.1.1 Findings

The ***Security Target*** document, defines in its section **5.1.4.4 Identification and Authentication for Bluetooth Module**, that Windows 10, Windows 11 and Windows Server implements the required mechanisms to prevent data from any kind to be transfered before the Bluetooth pairing is completed.

96.1.2 Verdict

The evaluator has reviewed the ***Security Target*** document and has ensured that it describes how the IPSec capabilities are implemented and how the network packets are processed. Moreover, the ***Operational Guidance*** document includes instructions about how the SPD policies are created and configured. The information provided is consistent with the one provided in the TSS section of the ***Security Target*** document.

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfillment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

96.2 Test Activity

For this case, all the auditable events will be obtained during the test execution of each security functional requirement.

96.2.1 Test 1

96.2.1.1 Setup

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Testing Machine (Debian 11 Bullseye, using bluez and bluetooth adapter)
- Windows Client Machine (Platforms listed in the ST)

96.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMBT10SD] instructions in order to collect the results as stipulated by the supporting document [PPMBT10SD].

96.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Voyager Klaas Telecom with Azure Stack Hub (build 10.0.17784.1068)
- Panasonic CF-33 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

Results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms*.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

96.2.1.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 1** requirements established in the assurance activity section.

96.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FIA_BLT_EXT.2

97 FIA_BLT_EXT.3

The assurance activity for the **FIA_BLT_EXT.3** requirement is stated as follows:

> **TSS**
>
> The evaluator shall ensure that the TSS describes how Bluetooth sessions are maintained such that at least two devices with the same Bluetooth device address are not simultaneously connected and such that the initial session is not superseded by any following session initialization attempts.
>
> **Operational Guidance**
>
> There are no guidance evaluation activities for this component.
>
> **Test**
>
> The evaluator shall perform the following steps:
>
> Step 1: Pair the TOE with a remote Bluetooth device (DEV1) with a known address BD_ADDR. Establish an active session between the TOE and DEV1 with the known address BD_ADDR.
>
> Step 2: Attempt to pair a second remote Bluetooth device (DEV2) claiming to have a Bluetooth device address matching DEV1 BD_ADDR to the TOE. Using a Bluetooth protocol analyzer, verify that the pairing attempt by DEV2 is not completed by the TOE and that the active session to DEV1 is unaffected.
>
> Step 3: Attempt to initialize a session to the TOE from DEV2 containing address DEV1 BD_ADDR. Using a Bluetooth protocol analyzer, verify that the session initialization attempt by DEV2 is ignored by the TOE and that the initial session to DEV1 is unaffected.

97.1 Documentation Review activity

97.1.1 Findings

The ***Security Target*** document, defines in its section **5.1.4.4 identification and Authentication for Bluetooth Module**, that Windows 10, Windows 11 and Windows Server implements the required mechanisms to prevent attempts from pairings when the TOE is already paired with some other device.

97.1.2 Verdict

The evaluator has reviewed the ***Security Target*** document and has ensured that it describes how the Bluetooth capabilities are implemented and how Bluetooth is handled. Moreover, the ***Operational Guidance*** document includes instructions about how the SPD policies are created and configured. The information provided is consistent with the one provided in the TSS section of the ***Security Target*** document.

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfillment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

97.2 Test Activity

For this case, all the auditable events will be obtained during the test execution of each security functional requirement.

97.2.1 Test 1

97.2.1.1 Setup

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Testing Machine I (DEV1) (Debian 11 Bullseye, using Strongswan U5.9.1/K5.10)
- Testing Machine II (DEV2) (Debian 11 Bullseye, using Strongswan U5.9.1/K5.10)
- Windows Client Machine (Platforms listed in the ST)

97.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMBT10SD] instructions in order to collect the results as stipulated by the supporting document [PPMBT10SD].

97.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

Results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms*.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

97.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FIA_BLT_EXT.3

98 FIA_BLT_EXT.4

The assurance activity for the **FIA_BLT_EXT.4** requirement is stated as follows:

> **TSS**
>
> The evaluator shall verify that the TSS describes the secure simple pairing process.
>
> **Operational Guidance**
>
> There are no guidance evaluation activities for this component.
>
> **Test**
>
> The evaluator shall perform the following steps:
>
> Step 1: Initiate pairing with the TOE from a remote Bluetooth device that supports Secure Simple Pairing.
>
> Step 2: During the pairing process; observe the packets in a Bluetooth protocol analyzer and verify that the TOE claims support for both “Secure Simple Pairing (Host Support)” and “Secure Simple Pairing (Controller Support)” during the LMP Features Exchange.
>
> Step 3: Verify that Secure Simple Pairing is used during the pairing process.

98.1 Documentation Review activity

98.1.1 Findings

The ***Security Target*** document, defines in its section **5.1.4.4 identification and Authentication for Bluetooth Module**, that Windows 10, Windows 11 and Windows Server implements correctly the secure simple pairing process.

The **Bluetooth® Core Specification Version 5.2** in Vol 2. BR/EDR Controller, Part H: Security Specification, section 7 Security Simple Pairing explains Secure Simple Pairing security functions and procedures are described in this section. In addition, a cryptographic analysis of each procedure is provided.

98.1.2 Verdict

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfillment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

98.2 Test Activity

For this case, all the auditable events will be obtained during the test execution of each security functional requirement.

98.2.1 Test 1

98.2.1.1 Setup

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Testing Machine (Debian 11 Bullseye, using bluez and bluetooth adapter)
- Windows Client Machine (Platforms listed in the ST)
- Wireshark
- Bluetooth Virtual Sniffer (btvs.exe)

98.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMBT10SD] instructions in order to collect the results as stipulated by the supporting document [PPMBT10SD].

98.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Dell PowerEdge R640 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Voyager Klaas Telecom with Azure Stack Hub (build 10.0.17784.1068)
- Panasonic CF-33 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)

- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)

Results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms*.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

98.2.1.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

98.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FIA_BLT_EXT.4.

99 FIA_BLT_EXT.6

The assurance activity for the **FIA_BLT_EXT.6** requirement is stated as follows:

> **TSS**
>
> The evaluator shall verify that the TSS describes all Bluetooth profiles and associated services for which explicit user authorization is required before a remote device can gain access. The evaluator shall also verify that the TSS describes any difference in behavior based on whether or not the device has a trusted relationship with the TOE for that service (i.e. whether there are any services that require explicit user authorization for untrusted devices that do not require such authorization for trusted devices). The evaluator shall also verify that the TSS describes the method by which a device can become 'trusted'.
>
> **Operational Guidance**
>
> There are no guidance evaluation activities for this component.
>
> **Test**
>
> The evaluator shall perform the following tests:
>
> - **Test 1:** While the service is in active use by an application on the TOE, the evaluator shall attempt to gain access to a "protected" Bluetooth service (as specified in the assignment in FIA_BLT_EXT.6.1) from a "trusted" remote device. The evaluator shall verify that the user is explicitly asked for authorization by the TOE to allow access to the service for the particular remote device. The evaluator shall deny the authorization on the TOE and verify that the remote attempt to access the service fails due to lack of authorization.
> - **Test 2:** The evaluator shall repeat Test 1, this time allowing the authorization and verifying that the remote device successfully accesses the service.

99.1 Documentation Review activity

99.1.1 Findings

The ***Security Target*** document, defines in its section **5.1.4.4 identification and Authentication for Bluetooth Module**, that Windows 10, Windows 11 and Windows Server implements the mechanisms to prevent a remote device from gaining remote access without prior user explicit authorization.

99.1.2 Verdict

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfillment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

99.2 Test Activity

For this case, all the auditable events will be obtained during the test execution of each security functional requirement.

99.2.1 Test 1 and Test 2

99.2.1.1 Setup

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Testing Machine (Debian 11 Bullseye, using bluez and bluetooth adapter)
- Windows Client Machine (Platforms listed in the ST)

99.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMBT10SD] instructions in order to collect the results as stipulated by the supporting document [PPMBT10SD].

99.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop Studio with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Zebra L10ax / RTL 10C1 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)

- HPE Edgeline EL8000 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Voyager Klaas Telecom with Azure Stack Hub (build 10.0.17784.1068)
- Panasonic CF-33 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)

Results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms*.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

99.2.1.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1** and **Test 2**.

99.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FIA_BLT_EXT.6

100 FIA_BLT_EXT.7

The assurance activity for the **FIA_BLT_EXT.7** requirement is stated as follows:

TSS

The TSS evaluation activities for this component are addressed by FIA_BLT_EXT.6.

Operational Guidance

There are no guidance evaluation activities for this component.

Test

The evaluator shall perform the following tests if the TSF differentiates between "trusted" and "untrusted" devices for the purpose of granting access to services. If it does not, then the test evaluation activities for FIA_BLT_EXT.6 are sufficient to satisfy this component.

- **Test 1:** While the service is in active use by an application on the TOE, the evaluator shall attempt to gain access to a "protected" Bluetooth service (as specified in the assignment in FIA_BLT_EXT.7.1) from an "untrusted" remote device. The evaluator shall verify that the user is explicitly asked for authorization by the TOE to allow access to the service for the particular remote device. The evaluator shall deny the authorization on the TOE and verify that the remote attempt to access the service fails due to lack of authorization.
- **Test 2:** The evaluator shall repeat Test 1, this time allowing the authorization and verifying that the remote device successfully accesses the service.
- **Test 3 [conditional]:** If there exist any services that require explicit user authorization for access by untrusted devices but not by trusted devices (i.e. a service that is listed in FIA_BLT_EXT.7.1 but not FIA_BLT_EXT.6.1), the evaluator shall repeat Test 1 for these services and observe that the results are identical. That is, the evaluator shall use these results to verify that explicit user approval is required for an untrusted device to access these services, and failure to grant this approval will result in the device being unable to access them.
- **Test 4 [conditional]:** If test 3 applies, the evaluator shall repeat Test 2 using any services chosen in Test 3 and observe that the results are identical. That is, the evaluator shall use these results to verify that explicit user approval is required for an untrusted device to access these services, and granting this approval will result in the device being able to access them.
- **Test 5 [conditional]:** If test 3 applies, the evaluator shall repeat Test 3 except this time designating the device as "trusted" prior to attempting to access the service. The evaluator shall verify that access to the service is granted without explicit user authorization (because the device is now trusted and therefore FIA_BLT_EXT.7.1 no longer applies to it). That is, the

evaluator shall use these results to demonstrate that the TSF will grant a device access to different services depending on whether or not the device is trusted.

100.1 Documentation Review activity

100.1.1 Findings

The ***Security Target*** document, defines defines in its section 5.1.4.4 identification and Authentication for Bluetooth Module, that Windows 10, Windows 11 and Windows Server implements the mechanisms to prevent an untrusted remote device from gaining remote access without prior user explicit authorization.

100.1.2 Verdict

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfillment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

100.2 Test Activity

TOEs does not differentiate between “trusted” and “untrusted” devices, just paired or not, for the purpose of granting access services. Therefore, the test evaluation activities for FIA_BLT_EXT.6 are sufficient to satisfy this component.

100.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FIA_BLT_EXT.7

101 FMT_MOF_EXT.1/BT

The assurance activity for the **FMT_MOF_EXT.1/BT** requirement is stated as follows:

> **TSS**
>
> The evaluator shall examine the TSS to ensure that it identifies the Bluetooth-related management functions that are supported by the TOE and the roles that are authorized to perform each function.
>
> **Guidance**
>
> The evaluator shall examine the operational guidance to ensure that it provides sufficient guidance on each supported Bluetooth management function to describe how the function is performed and any role restrictions on the subjects that are authorized to perform the function.
>
> **Test**
>
> For each function that is indicated as restricted to the administrator, the evaluation shall perform the function as an administrator, as specified in the Operational Guidance, and determine that it has the expected effect as outlined by the Operational Guidance and the SFR. The evaluator will then perform the function (or otherwise attempt to access the function) as a non-administrator and observe that they are unable to invoke that functionality.

101.1 Documentation Review activity

101.1.1 Findings

The ***Security Target*** document, defines in its section **5.1.4.4 identification and Authentication for Bluetooth Module**, that Windows 10, Windows 11 and Windows Server implements the management functions to support roles and enforce the required policies to allow or deny to perform some operations depending on the role attempting to perform the given operation.

101.1.2 Verdict

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfilment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

101.2 Test Activity

For this case, all the auditable events will be obtained during the test execution of each security functional requirement.

101.2.1 Test 1

101.2.1.1 Setup

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Testing Machine (Debian 11 Bullseye, using bluez and bluetooth controller)
- Windows Client Machine (Platforms listed in the ST)

101.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMBT10SD] instructions in order to collect the results as stipulated by the supporting document [PPMBT10SD].

101.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**.

Results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms*.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

101.2.1.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

101.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FMT_MOF_EXT.1/VPN.

102 FMT_SMF_EXT.1/BT

The assurance activity for the **FMT_SMF_EXT.1/BT** requirement is stated as follows:

> **TSS**
>
> The evaluator shall ensure that the TSS includes a description of the Bluetooth profiles and services supported and the Bluetooth security modes and levels supported by the TOE.
>
> If function BT-4, "Allow/disallow additional wireless technologies to be used with Bluetooth," is selected, the evaluator shall verify that the TSS describes any additional wireless technologies that may be used with Bluetooth, which may include Wi-Fi with Bluetooth High Speed and/or NFC as an Out of Band pairing mechanism.
>
> If function BT-5, "Configure allowable methods of Out of Band pairing (for BR/EDR and LE)," is selected, the evaluator shall verify that the TSS describes when Out of Band pairing methods are allowed and which ones are configurable.
>
> If function BT-8, "Disable/enable the Bluetooth services and/or profiles available on the OS (for BR/EDR and LE)," is selected, the evaluator shall verify that all supported Bluetooth services are listed in the TSS as manageable and, if the TOE allows disabling by application rather than by service name, that a list of services for each application is also listed.
>
> If function BT-9, "Specify minimum level of security for each pairing (for BR/EDR and LE)," is selected, the evaluator shall verify that the TSS describes the method by which the level of security for pairings are managed, including whether the setting is performed for each pairing or is a global setting.
>
> **Guidance**
>
> The evaluator shall ensure that the management functions defined in the PP-Module are described in the guidance to the same extent required for the Base-PP management functions.
>
> **Test**
>
> The evaluator shall use a Bluetooth-specific protocol analyzer to perform the following tests:
>
> - **Test 1:** The evaluator shall disable the Discoverable mode and shall verify that other Bluetooth BR/EDR devices cannot detect the TOE. The evaluator shall use the protocol analyzer to verify that the TOE does not respond to inquiries from other devices searching for Bluetooth devices. The evaluator shall enable Discoverable mode and verify that other devices can detect the TOE and that the TOE sends response packets to inquiries from searching devices.

The following tests are conditional on if the corresponding function is included in the ST:

- **Test 2 (conditional):** The evaluator shall examine Bluetooth traffic from the TOE to determine the current Bluetooth device name, change the Bluetooth device name, and verify that the Bluetooth traffic from the TOE lists the new name. The evaluator shall examine Bluetooth traffic from the TOE to determine the current Bluetooth device name for BR/EDR and LE. The evaluator shall change the Bluetooth device name for LE independently of the device name for BR/EDR. The evaluator shall verify that the Bluetooth traffic from the TOE lists the new name.
- **Test 3 (conditional):** The evaluator shall disable Bluetooth BR/EDR and enable Bluetooth LE. The evaluator shall examine Bluetooth traffic from the TOE to confirm that only Bluetooth LE traffic is present. The evaluator shall repeat the test with Bluetooth BR/EDR enabled and Bluetooth LE disabled, confirming that only Bluetooth BR/EDR is present.
- **Test 4 (conditional):** For each additional wireless technology that can be used with Bluetooth as claimed in the ST, the evaluator shall revoke Bluetooth permissions from that technology. If the set of supported wireless technologies includes Wi-Fi, the evaluator shall verify that Bluetooth High Speed is not able to send Bluetooth traffic over Wi-Fi when disabled. If the set of supported wireless technologies includes NFC, the evaluator shall verify that NFC cannot be used for pairing when disabled. For any other supported wireless technology, the evaluator shall verify that it cannot be used with Bluetooth in the specified manner when disabled. The evaluator shall then re-enable all supported wireless technologies and verify that all functionality that was previously unavailable has been restored.
- **Test 5 (conditional):** The evaluator shall attempt to pair using each of the Out of Band pairing methods, verify that the pairing method works, iteratively disable each pairing method, and verify that the pairing method fails.
- **Test 6 (conditional):** The evaluator shall enable Advertising for Bluetooth LE, verify that the advertisements are captured by the protocol analyzer, disable Advertising, and verify that no advertisements from the device are captured by the protocol analyzer.
- **Test 7 (conditional):** The evaluator shall enable Connectable mode and verify that other Bluetooth devices may pair with the TOE and (if the devices were bonded) re-connect after pairing and disconnection. For BR/EDR devices: The evaluator shall use the protocol analyzer to verify that the TOE responds to pages from the other devices and permits pairing and re-connection. The evaluator shall disable Connectable mode and verify that the TOE does not respond to pages from remote Bluetooth devices,

thereby not permitting pairing or re-connection. For LE: The evaluator shall use the protocol analyzer to verify that the TOE sends connectable advertising events and responds to connection requests. The evaluator shall disable Connectable mode and verify that the TOE stops sending connectable advertising events and stops responding to connection requests from remote Bluetooth devices.

- **Test 8 (conditional):** For each supported Bluetooth service and/or profile listed in the TSS, the evaluator shall verify that the service or profile is manageable. If this is configurable by application rather than by service and/or profile name, the evaluator shall verify that a list of services and/or profiles for each application is also listed.
- **Test 9 (conditional):** The evaluator shall allow low security modes/levels on the TOE and shall initiate pairing with the TOE from a remote device that allows only something other than Security Mode 4/Level 3 or Security Mode 4/Level 4 (for BR/EDR), or Security Mode 1/Level 3 (for LE). (For example, a remote BR/EDR device may claim Input/Output capability "NoInputNoOutput" and state that man-in-the-middle (MiTM) protection is not required. A remote LE device may not support encryption.) The evaluator shall verify that this pairing attempt succeeds due to the TOE falling back to the low security mode/level. The evaluator shall then remove the pairing of the two devices, prohibit the use of low security modes/levels on the TOE, then attempt the connection again. The evaluator shall verify that the pairing attempt fails. With the low security modes/levels disabled, the evaluator shall initiate pairing from the TOE to a remote device that supports Security Mode 4/Level 3 or Security Mode 4/Level 4 (for BR/EDR) or Security Mode 1/Level 3 (for LE). The evaluator shall verify that this pairing is successful and uses the high security mode/level.

102.1 Documentation Review activity

102.1.1 Findings

The ***Security Target*** document, defines in its section **5.1.5.4 Security Management for Bluetooth Module**, that Windows 10, Windows 11 and Windows Server implements correctly the Bluetooth management functions.

102.1.2 Verdict

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfilment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

102.2 Test Activity

For this case, all the auditable events will be obtained during the test execution of each security functional requirement.

102.2.1 Test 1, Test 6 and Test 8

102.2.1.1 Setup

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Evaluator Machine
- Windows Client Machine (TOE)
- Windows Client Machine and Testing machine are not bonded
- Windows Client Machine and Testing machine have access to internet
- Ellysis Explorer is available
- A Faraday cage to isolate the TOE from external traffic noise for LE
- Two MDM accounts are available, one to administer the MDM settings and the other for the TOE to be enroled with it.

102.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMBT10SD] instructions in order to collect the results as stipulated by the supporting document [PPMBT10SD].

102.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

102.2.1.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Tests 1, 6 and 8** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1, 6 and 8**.

102.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FMT_SMF_EXT.1/BT.

103 FTP_BLT_EXT.1

The assurance activity for the **FTP_BLT_EXT.1** requirement is stated as follows:

> **TSS**
>
> The evaluator shall verify that the TSS describes the use of encryption, the specific Bluetooth protocol(s) it applies to, and whether it is enabled by default.
>
> The evaluator shall verify that the TSS includes the protocol used for encryption of the transmitted data and the key generation mechanism used.
>
> **Guidance**
>
> The evaluator shall verify that the operational guidance includes instructions on how to configure the TOE to require the use of encryption during data transmission (unless this behavior is enforced by default).
>
> **Test**
>
> There are no test EAs for this component. Testing for this SFR is addressed through the evaluation of FTP_BLT_EXT.3/BR and, if claimed, FTP_BLT_EXT.3/LE.

103.1 Documentation Review activity

Assurance Activities for this element are tested through Assurance Activities for FTP_BLT_EXT.3/BR, FTP_BLT_EXT.3/LE and FCS_CKM_EXT.8

103.2 Test Activity

Assurance Activities for this element are tested through Assurance Activities for FTP_BLT_EXT.3/BR, FTP_BLT_EXT.3/LE and FCS_CKM_EXT.8

103.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FTP_BLT_EXT.1

104 FPT_BLT_EXT.2

The assurance activity for the **FPT_BLT_EXT.2** requirement is stated as follows:

TSS

The evaluator shall verify that the TSS describes the TSF's behavior if a remote device stops encryption while connected to the TOE.

Guidance

The evaluator shall verify that the operational guidance describes how to enable/disable encryption (if configurable).

Test

The evaluator shall perform the following steps using a Bluetooth protocol analyzer to observe packets pertaining to the encryption key size:

Step 1: Initiate pairing with the TOE from a remote Bluetooth device that has been configured to have a minimum encryption key size that is equal to or greater than that of the TOE.

Step 2: After pairing has successfully finished and while a connection exists between the TOE and the remote device; turn off encryption on the remote device. This can be done using commercially-available tools.

Step 3: Verify that the TOE either restarts encryption with the remote device or terminates the connection with the remote device.

104.1 Documentation Review activity

104.1.1 Findings

The ***Security Target*** document, defines in its section **5.1.8.4 Trusted Path / Channels for Bluetooth Module**, that Windows 10, Windows 11 and Windows Server implements the correct behaviour when a remote device interrupts the encryption process.

The **Bluetooth® Core Specification Version 5.2** in Vol 2. BR/EDR Controller, Part C: Link Manager Protocol Specification, section 4.2.5 Encryption and Vol 6. Low Energy Controller, Part E: Encryption and authentication overview define how the encryption may be used, even for both BR/EDR and LE.

104.1.2 Verdict

The evaluator considers that the information provided in the TSS describes in detail how the VPN client establishes a VPN channel taking into account its different phases and providing the set of available interfaces required for doing that.

Moreover, the operational guidance covers all the managements operations when creating VPN connections with the VPN client, from the available firewall rules to the configuration parameters.

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfillment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

104.2 Test Activity

104.2.1 Test 1

104.2.1.1 Setup

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Testing Machine (Debian 11 Bullseye, using bluez and bluetooth adapter)
- Windows Client Machine (Platforms listed in the ST)
- Wireshark
- Bluetooth Virtual Sniffer (btvs.exe)

104.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMBT10SD] instructions in order to collect the results as stipulated by the supporting document [PPMBT10SD].

104.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Lenovo ThinkPad Z13 Gen3 with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006)
- Panasonic CF-33 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Microsoft Surface Pro 9 5G with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)

Results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms*.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

104.2.1.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

104.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FPT_BLT_EXT.2

105 FPT_BLT_EXT.3/BR

The assurance activity for the **FPT_BLT_EXT.3/BR** requirement is stated as follows:

TSS

The evaluator shall examine the TSS and verify that it specifies the minimum key size for BR/EDR encryption, whether this value is configurable, and the mechanism by which the TOE will not negotiate keys sizes smaller than the minimum.

Guidance

The evaluator shall verify that the guidance includes instructions on how to configure the minimum encryption key size for BR/EDR encryption, if configurable.

Test

The evaluator shall perform the following tests:

Test 1: The evaluator shall perform the following steps using a Bluetooth protocol analyzer to observe packets pertaining to the encryption key size:

Step 1: Initiate BR/EDR pairing with the TOE from a remote Bluetooth device that has been configured to have a minimum encryption key size that is equal to or greater than that of the TOE. This can be done using certain commercially-available tools that can send the appropriate command to certain commercially-available Bluetooth controllers.

Step 2: Use a Bluetooth packet sniffer to verify that the encryption key size negotiated for the connection is at least as large as the minimum encryption key size defined for the TOE.

Test 2 (conditional): If the encryption key size is configurable, configure the TOE to support a different minimum key size, then repeat Test 1 and verify that the negotiated key size is at least as large as the new minimum value.

Test 3: The evaluator shall perform the following steps using a Bluetooth protocol analyzer to observe packets pertaining to the encryption key size:

Step 1: Initiate BR/EDR pairing with the TOE from a remote Bluetooth device that has been configured to have a maximum encryption key size of 1 byte. This can be done using certain commercially-available tools that can send the appropriate command to certain commercially-available Bluetooth controllers.

Step 2: Verify that the encryption key size suggested by the remote device is not accepted by the TOE and that the connection is not completed.

105.1 Documentation Review activity

105.1.1 Findings

The ***Security Target*** document, defines in its section **5.1.8.4 Trusted Path / Channels for Bluetooth Module**, that Windows 10, Windows 11 and Windows Server implements correctly the negotiation process depending on the key sizes used.

The **Bluetooth® Core Specification Version 5.2** in Vol 2. BR/EDR Controller, Part C: Link Manager Protocol Specification, section 4.2.5 Encryption defines how the encryption may be used. Defines two mechanisms E0 Encryption (legacy) and AES-CCM encryption, and in Vol 2. BR/EDR Controller, Part H: Security Specification, section 4 Encryption (E0) and Vol 2. BR/EDR Controller, Part H: Security Specification, section 9 AES-CCM encryption for BR/EDR explain how the encryption and the encryption key size works.

In addition Vol 3: Host, Part H: Security Manager Specification, section 2.3.4 Encryption key size explains how works the maximum and minimum encryption key length parameters which defines the maximum and the minimum size of encryption key allowed in octets. The maximum and minimum encryption key length parameters shall be between 7 octets (56 bits) and 16 octets (128 bits), in 1 octet (8 bit) steps. This is defined by a profile or device application.

The smaller value of the initiating and responding devices maximum encryption key length parameters shall be used as the encryption key size.

This SFR is depending of Bluetooth controller because it need to have the HCI command "HCI_Read_Encryption_Key_Size". and the host should check the encryption key size using it.

105.1.2 Verdict

The evaluator considers that the information provided in the TSS describes in detail how the VPN client establishes a VPN channel taking into account its different phases and providing the set of available interfaces required for doing that.

Moreover, the operational guidance covers all the managements operations when creating VPN connections with the VPN client, from the available firewall rules to the configuration parameters.

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfillment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

105.2 Test Activity

105.2.1 Test 1

105.2.1.1 Setup

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Testing Machine (Debian 11 Bullseye, using bluez and bluetooth adapter)
- Windows Client Machine (Platforms listed in the ST)
- Wireshark
- Bluetooth Virtual Sniffer (btvs.exe)

105.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMBT10SD] instructions in order to collect the results as stipulated by the supporting document [PPMBT10SD].

105.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006) 30
- Panasonic CF-33 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)

Results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms*.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

105.2.1.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

105.2.2 Test 2

105.2.2.1 Setup

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Ellisys Explorer is available
- Testing Machine (Windows 10 with Ellisys Software)
- Raspberry Pi 3 Model B V1.2 with firmware BCM43430A1
  - Firmware version without patches and vulnerable to InternalBlue: http://github.com/RPi-
    Distro
  - InternalBlue is available
    - Modified Rpi3 KNOB POC is available
  - Pwntools is available
  - Wireshak is available
- Windows Client Machine (Platforms listed in the ST)
- Bluetooth Virtual Sniffer (btvs.exe)

105.2.2.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMBT10SD] instructions in order to collect the results as stipulated by the supporting document [PPMBT10SD].

105.2.2.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006) 30

- Panasonic CF-33 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)

Results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms*.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

105.2.2.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 2** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 2**.

105.2.3 Test 3

105.2.3.1 Setup

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Ellisys Explorer is available
- Testing Machine (Windows 10 with Ellisys Software)
- Raspberry Pi 3 Model B V1.2 with firmware BCM43430A1
  - Firmware version without patches and vulnerable to InternalBlue: http://github.com/RPi-Distro
  - InternalBlue is available
    - Rpi3 KNOB POC is available
  - Pwntools is available
  - Wireshak is available
- Windows Client Machine (Platforms listed in the ST)
- Bluetooth Virtual Sniffer (btvs.exe)

105.2.3.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMBT10SD] instructions in order to collect the results as stipulated by the supporting document [PPMBT10SD].

105.2.3.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Dell Latitude 7420 with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Zebra ET80Z Tablet with Windows 10 version 22H2 Enterprise edition (build 10.0.19045.2006) 30
- Panasonic CF-33 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Dell PowerEdge R760xp with Azure Stack Hub (build 10.0.17784.1068)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)
- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)

Results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms*.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

105.2.3.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 3** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 3**.

105.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FPT_BLT_EXT.3/BR

106 FPT_BLT_EXT.3/LE

The assurance activity for the **FPT_BLT_EXT.3/LE** requirement is stated as follows:

> **TSS**
>
> The evaluator shall examine the TSS and verify that it specifies the minimum key size for LE encryption, whether this value is configurable, and the mechanism by which the TOE will not negotiate keys sizes smaller than the minimum.
>
> **Guidance**
>
> The evaluator shall verify that the guidance includes instructions on how to configure the minimum encryption key size for LE encryption, if configurable.
>
> **Test**
>
> The evaluator shall perform the following tests:
>
> **Test 1:** The evaluator shall perform the following steps using a Bluetooth protocol analyzer to observe packets pertaining to the encryption key size:
>
> Step 1: Initiate LE pairing with the TOE from a remote Bluetooth device that has been configured to have a minimum encryption key size that is equal to or greater than that of the TOE. This can be done using certain commercially-available tools that can send the appropriate command to certain commercially-available Bluetooth controllers.
>
> Step 2: Use a Bluetooth packet sniffer to verify that the encryption key size negotiated for the connection is at least as large as the minimum encryption key size defined for the TOE.
>
> **Test 2 (conditional):** If the encryption key size is configurable, configure the TOE to support a different minimum key size, then repeat Test 1 and verify that the negotiated key size is at least as large as the new minimum value.
>
> **Test 3:** The evaluator shall perform the following steps using a Bluetooth protocol analyzer to observe packets pertaining to the encryption key size:
>
> Step 1: Initiate LE pairing with the TOE from a remote Bluetooth device that has been configured to have a maximum encryption key size of 1 byte. This can be done using certain commercially-available tools that can send the appropriate command to certain commercially-available Bluetooth controllers.
>
> Step 2: Verify that the encryption key size suggested by the remote device is not accepted by the TOE and that the connection is not completed.

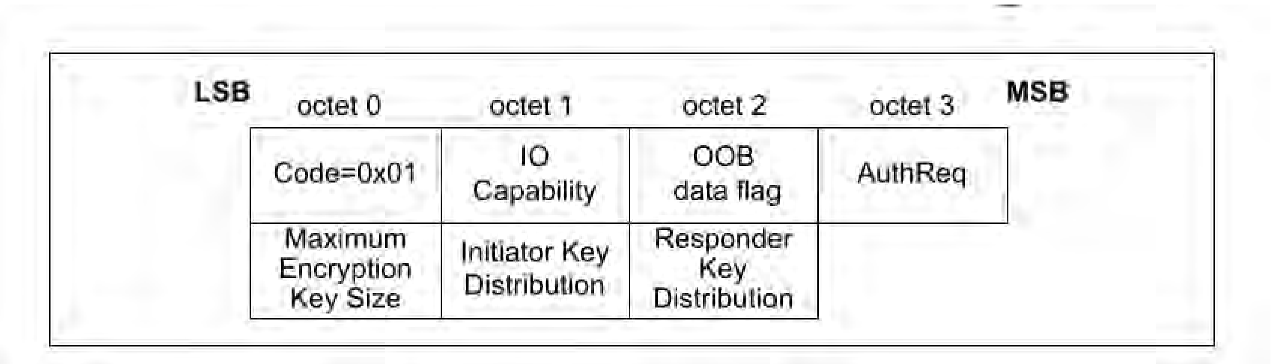
106.1 Documentation Review activity

106.1.1 Findings

The ***Security Target*** document, defines in its section **5.1.8.4 Trusted Path / Channels for Bluetooth Module**, that Windows 10, Windows 11 and Windows Server implements correctly the negotiation process depending on the key sizes used.

The **Bluetooth® Core Specification Version 5.2** in Vol 2. BR/EDR Controller, Part C: Link Manager Protocol Specification, section 4.2.5 Encryption defines how the encryption may be used. Defines two mechanisms E0 Encryption (legacy) and AES-CCM encryption, and in Vol 2. BR/EDR Controller, Part H: Security Specification, section 4 Encryption (E0) and Vol 2. BR/EDR Controller, Part H: Security Specification, section 9 AES-CCM encryption for BR/EDR explain how the encryption and the encryption key size works.

In addition Vol 3: Host, Part H: Security Manager Specification, section 3.5 Pairing methods defines the Pairing Feature Exchange and key generation, and the Pairing Request Packet which contains the "Maximum Encryption Key Size"



LSB	octet 0	octet 1	octet 2	octet 3	MSB
	Code=0x01	IO Capability	OOB data flag	AuthReq	
	Maximum Encryption Key Size	Initiator Key Distribution	Responder Key Distribution		

This value defines the maximum encryption key size in octets that the device can support. The maximum key size shall be in the range 7 to 16 octets.

106.1.2 Verdict

The evaluator considers that the information provided in the TSS describes in detail how the VPN client establishes a VPN channel taking into account its different phases and providing the set of available interfaces required for doing that.

Moreover, the operational guidance covers all the managements operations when creating VPN connections with the VPN client, from the available firewall rules to the configuration parameters.

Therefore, the evaluator considers that, the findings obtained during the documentation review activity demonstrate the fulfillment of the requirements established in the assurance activity section. Hence, the **PASS** verdict is assigned to the documentation review activity.

106.2 Test Activity

106.2.1 Test 1

106.2.1.1 Setup

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Testing Machine (Debian 10 Buster, using bluez and bluetooth adapter)
- Windows Client Machine (Platforms listed in the ST)
- Wireshark

106.2.1.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMBT10SD] instructions in order to collect the results as stipulated by the supporting document [PPMBT10SD].

106.2.1.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- HPE Edgeline EL8000 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

Results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms.*

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

106.2.1.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 1** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 1**.

106.2.2 Test 2

106.2.2.1 Setup

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Testing Machine (Debian 10 Buster with custom kernel, using bluez and bluetooth adapter)
- Windows Client Machine (Platforms listed in the ST)
- Wireshark

106.2.2.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMBT10SD] instructions in order to collect the results as stipulated by the supporting document [PPMBT10SD].

106.2.2.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)

- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- HPE Edgeline EL8000 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

Results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms*.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

106.2.2.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 3** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 2**.

106.2.3 Test 3

106.2.3.1 Setup

The scenario to perform the assurance activities according to the Protection Profile is composed of the following elements:

- Testing Machine (Debian 10 Buster with custom kernel, using bluez and bluetooth adapter)
- Windows Client Machine (Platforms listed in the ST)
- Wireshark

106.2.3.2 Procedure

The evaluator has followed the previous specified preparatory actions, including setup, configuration, and prerequisites. The evaluator has conducted the actions and test steps, ensuring compliance with the supporting document [PPMBT10SD] instructions in order to collect the results as stipulated by the supporting document [PPMBT10SD].

106.2.3.3 Results

The evaluator has performed this test on all canonical platforms as defined in section **8. Test environment definition**. Additionally, the following supplementary platforms have been also tested:

- Microsoft Surface Laptop 4 (AMD) with Windows 10 version 22H2 Pro edition (build 10.0.19045.2006)
- Microsoft Surface Laptop Go 2 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- HP 840 G10 with Windows 11 version 22H2 Education edition (build 10.0.22621.1)
- Microsoft Surface Go 3 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Dell Latitude 9520 with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- Microsoft Surface Laptop 4 (Intel) with Windows 11 version 22H2 Pro edition (build 10.0.22621.1)
- HPE Edgeline EL8000 with Windows Server 2022 Standard edition (22H2, build 10.0.20348.587)
- Panasonic FZ-55 with Windows 11 version 22H2 IoT edition (build 10.0.22621.1)
- Surface Studio 2+ with Windows 11 version 22H2 Enterprise edition (build 10.0.22621.1)

Results have obtained the same output in *Windows 10 platforms, Windows 11 platforms and Windows Server platforms*.

The evaluator has provided a detailed list of finding and results that are relevant to fulfill the security functional requirement. Therefore, the evaluator concludes that the TOE's behavior is as expected and detailed in the security target [ST004].

106.2.3.4 Verdict

The evaluator considers that the results obtained from the test activity demonstrate the fulfillment of the **Test 3** requirements established in the assurance activity section.

Therefore, the **PASS** verdict is assigned to **Test 3**.

106.3 Final Verdict

Since all activities have been assigned a **PASS** verdict, the evaluator considers that the requirements established in the assurance activity are properly fulfilled. Therefore, the **PASS** verdict is assigned to FTP_BLT_EXT.3/LE.

107 Final results

The following table summarizes the results obtained for each security requirement defined in the ***Security Target*** document, taking into account the information provided in the ***Operational Guidance*** document:

Security Functional Requirement - Coming from [GPOSPP421]:

SFRs	TSS Analysis	AGD Analysis	Testing Activity
FCS_CKM.1.1	PASS	PASS	PASS
FCS_CKM.2.1	PASS	PASS	PASS
FCS_CKM_EXT.4.1	PASS	PASS	PASS
FCS_COP.1.1(SYM)	PASS	PASS	PASS
FCS_COP.1.1(HASH)	PASS	PASS	PASS
FCS_COP.1.1(SIGN)	PASS	PASS	PASS
FCS_COP.1.1(HMAC)	PASS	PASS	PASS
FCS_RBG_EXT.1.1	PASS	PASS	PASS
FCS_RBG_EXT.1.2	PASS	PASS	PASS
FCS_STO_EXT.1.1	PASS	PASS	PASS
FCS_TLSC_EXT.1.1	PASS	PASS	PASS
FCS_TLSC_EXT.1.2	PASS	PASS	PASS
FCS_TLSC_EXT.1.3	PASS	PASS	PASS
FCS_TLSC_EXT.2.1	PASS	PASS	PASS
FCS_TLSC_EXT.3.1	PASS	PASS	PASS
FCS_TLSC_EXT.4.1	PASS	PASS	PASS
FCS_DTLS_EXT.1.1	PASS	PASS	PASS
FCS_DTLS_EXT.1.2	PASS	PASS	PASS
FDP_ACF_EXT.1.1	PASS	PASS	PASS
FDP_IFC_EXT.1.1	PASS	PASS	PASS
FAU_GEN.1.1	PASS	PASS	PASS
FAU_GEN.1.2	PASS	PASS	PASS
FIA_AFL.1.1	PASS	PASS	PASS
FIA_AFL.1.2	PASS	PASS	PASS
FIA_UAU.5.1	PASS	PASS	PASS
FIA_UAU.5.2	PASS	PASS	PASS
FIA_X509_EXT.1.1	PASS	PASS	PASS
FIA_X509_EXT.1.2	PASS	PASS	PASS
FIA_X509_EXT.2.1	PASS	PASS	PASS
FMT_MOF_EXT.1.1	PASS	PASS	PASS
FMT_SMF_EXT.1.1	PASS	PASS	PASS
FPT_ACF_EXT.1.1	PASS	PASS	PASS
FPT_ACF_EXT.1.2	PASS	PASS	PASS

SFRs	TSS Analysis	AGD Analysis	Testing Activity
FPT_ASLR_EXT.1.1	PASS	PASS	PASS
FPT_SBOP_EXT.1.1	PASS	PASS	PASS
FPT_SRP_EXT.1.1	PASS	PASS	PASS
FPT_TST_EXT.1.1	PASS	PASS	PASS
FPT_TUD_EXT.1.1	PASS	PASS	PASS
FPT_TUD_EXT.1.2	PASS	PASS	PASS
FPT_TUD_EXT.2.1	PASS	PASS	PASS
FPT_TUD_EXT.2.2	PASS	PASS	PASS
FTA_TAB.1.1	PASS	PASS	PASS
FTP_ITC_EXT.1.1(TLS)	PASS	PASS	PASS
FTP_ITC_EXT.1.1(DTLS)	PASS	PASS	PASS
FTP_TRP.1.1	PASS	PASS	PASS
FTP_TRP.1.2	PASS	PASS	PASS
FTP_TRP.1.3	PASS	PASS	PASS

Security Functional Requirement - Coming from [PPMWLAN10]:

SFRs	TSS Analysis	AGD Analysis	Testing Activity
FAU_GEN.1 (WLAN)	PASS	PASS	PASS
FCS_CKM.1 (WPA)	PASS	PASS	PASS
FCS_CKM.2 (WLAN)	PASS	PASS	PASS
FCS_TLSC_EXT.1 (WLAN)	PASS	PASS	PASS
FCS_TLSC_EXT.2 (WLAN)	PASS	PASS	PASS
FCS_WPA_EXT.1	PASS	PASS	PASS
FIA_PAE_EXT.1	PASS	PASS	PASS
FIA_X509_EXT.1 (WLAN)	PASS	PASS	PASS
FIA_X509_EXT.2 (WLAN)	PASS	PASS	PASS
FIA_X509_EXT.6 (WLAN)	PASS	PASS	PASS
FMT_SMF.1 (WLAN)	PASS	PASS	PASS
FPT_TST_EXT.3 (WLAN)	PASS	PASS	PASS
FTA_WSE_EXT.1	PASS	PASS	PASS
FPT_ITC.1 (WLAN)	PASS	PASS	PASS

Security Functional Requirement - Coming from [PPMVPN24]:

SFRs	TSS Analysis	AGD Analysis	Testing Activity
FAU_GEN.1 (VPN)	PASS	PASS	PASS
FAU_SEL.1.1	PASS	PASS	PASS

SFRs	TSS Analysis	AGD Analysis	Testing Activity
FCS_CKM.1.1 (VPN)	PASS	PASS	PASS
FCS_CKM_EXT.2.1	PASS	PASS	PASS
FCS_EAP_EXT.1.1	PASS	PASS	PASS
FCS_EAP_EXT.1.2	PASS	PASS	PASS
FCS_EAP_EXT.1.3	PASS	PASS	PASS
FCS_EAP_EXT.1.4	PASS	PASS	PASS
FCS_IPSEC_EXT.1.1	PASS	PASS	PASS
FCS_IPSEC_EXT.1.2	PASS	PASS	PASS
FCS_IPSEC_EXT.1.3	PASS	PASS	PASS
FCS_IPSEC_EXT.1.4	PASS	PASS	PASS
FCS_IPSEC_EXT.1.5	PASS	PASS	PASS
FCS_IPSEC_EXT.1.6	PASS	PASS	PASS
FCS_IPSEC_EXT.1.7	PASS	PASS	PASS
FCS_IPSEC_EXT.1.8	PASS	PASS	PASS
FCS_IPSEC_EXT.1.9	PASS	PASS	PASS
FCS_IPSEC_EXT.1.10	PASS	PASS	PASS
FCS_IPSEC_EXT.1.11	PASS	PASS	PASS
FCS_IPSEC_EXT.1.12	PASS	PASS	PASS
FCS_IPSEC_EXT.1.13	PASS	PASS	PASS
FCS_IPSEC_EXT.1.14	PASS	PASS	PASS
FDP_IFC_EXT.1.1 (VPN)	PASS	PASS	PASS
FDP_VPN_EXT.1.1	PASS	PASS	PASS
FDP_RIP.2.1	PASS	PASS	PASS
FIA_PSK_EXT.1.1	PASS	PASS	PASS
FIA_PSK_EXT.1.2	PASS	PASS	PASS
FIA_PSK_EXT.2.1	PASS	PASS	PASS
FIA_X509_EXT.3.1	PASS	PASS	PASS
FIA_X509_EXT.3.2	PASS	PASS	PASS
FIA_X509_EXT.3.3	PASS	PASS	PASS
FMT_SMF.1.1 (VPN)	PASS	PASS	PASS
FPT_TST_EXT.1.1 (VPN)	PASS	PASS	PASS
FPT_TST_EXT.1.2 (VPN)	PASS	PASS	PASS
FPT_ITC.1 (VPN)	PASS	PASS	PASS
FPT_ITC.1.2 (VPN)	PASS	PASS	PASS
FPT_ITC.1.3 (VPN)	PASS	PASS	PASS

Security Functional Requirement - Coming from [PPMBT10]:

SFRs	TSS Analysis	AGD Analysis	Testing Activity
FAU_GEN.1 (BT)	PASS	PASS	PASS
FCS_CKM_EXT.8	PASS	PASS	PASS
FIA_BLT_EXT.1	PASS	PASS	PASS
FIA_BLT_EXT.2	PASS	PASS	PASS
FIA_BLT_EXT.3	PASS	PASS	PASS
FIA_BLT_EXT.4	PASS	PASS	PASS
FIA_BLT_EXT.6	PASS	PASS	PASS
FIA_BLT_EXT.7	PASS	PASS	PASS
FMT_MOF_EXT.1 (BT)	PASS	PASS	PASS
FMT_SMF_EXT.1 (BT)	PASS	PASS	PASS
FTP_BLT_EXT.1	PASS	PASS	PASS
FTP_BLT_EXT.2	PASS	PASS	PASS
FTP_BLT_EXT.3 (BR/EDR)	PASS	PASS	PASS
FTP_BLT_EXT.3 (LE)	PASS	PASS	PASS

108 Evidence List

The evidences are listed in the document [MS-W11-22H2-I-000].

109 Evaluation Tools

- **BinSkim**, a verification tool which allows analysing binaries to ensure that they have been built in compliance with Microsoft's Security Development Lifecycle (SDL).
- **BOTAN-CCN**. Tool used to test the cryptographic algorithm included in the TOE.
- **Certutil(Inlcuded in libnss3-tools)**. Utility to manipulate NSS certificate databases.
- **Corruptor**. Tool for check integrity on network communications.
- **ee-tls-tool**. Test suite for TLS and X509 Common Criteria evaluations. It acts as an OpenSSL TLS server configured according to each test. A modified version based on tls-cc-tools has been used.
- **hping3**. Tool for sending TCP, IP, and UDP packets.
- **HxD**. Freeware Hex Editor and Disk Editor.
- **libreswan**. A free software implementation of the most widely supported and standarized VPN protocol usin "IPsec" and the Internet Key Exhange ("IKE").
- **strongswan**. A multiplatform IPsec implementation. The focus of the project is on strong authentication mechanisms using X.509 public key certificates and optional secure storage of private keys and certificates on smartcards through a standardized PKCS#11 interface and on TPM 2.0.
- **MITM Tool**. This software is a set of tools based on: br_netfiler + Iptables + NFQueue + BPF + Regex that allows modifying network packets on the fly. It is used to work as a MITM to modify the content of the network packages. More info at: Rehtse
- **PCPTool**. An utility which allows using TPM-related functionality.
- **PsTools**. Command-line tools to administer your Windows system.
- **SignTool**. A command line tool that provides the ability to sign files and verify signatures in files. It is distributed with the Windows 10 Software Development Kit (SDK).
- **Visual Studio 2022**. An integrated development environment from Microsoft.
- **VMMap**. VMMap is a process virtual and physical memory analysis utility.
- **WebClient** and **WebServer**. Internal tools that work as DTLS server and client.
- **Windows 10 & 11 Assessment and Deployment Kit (ADK)**. To create a WinPE USB.
- **Wireshark**. A network protocol analyser for macOS, Unix and Windows.

110 Acronyms

- **AGD**. Administrative Guidance Document
- **API**. Application Programming Interface
- **CAVP**. Cryptographic Algorithm Validation Program
- **CC**. Common Criteria
- **CVE**. Common Vulnerabilities and Exposures
- **FIPS**. Federal Information Processing Standard
- **HTTPS**. HyperText Transfer Protocol Secure
- **HW**. Hardware
- **IKE**. Internet Key Exchange
- **IPSec**. Internet Protocol Security
- **ISAKMP**. Internet Security Association and Key Management Protocol
- **IT**. Information Technology
- **MITM**. Man In The Middle
- **OCSP**. Online Certificate Status Protocol
- **OS**. Operative System
- **PP**. Protection Profile
- **SA**. Security association.
- **SFR**. Security Functional Requirement
- **SHA**. Secure Hash Algorithm
- **SSH**. Secure Shell
- **ST**. Security Target
- **SW**. Software
- **SSL**. Secure Socket Layer
- **TLS**. Transport Layer Security
- **TOE**. Target of Evaluation
- **TPM**. Trusted Platform Module
- **TSF**. TOE Security Functions
- **TSFI**. TOE Security Function Interface
- **TSS**. TOE Summary Specification
- **USB**. Universal Serial Bus
- **VPN**. Virtual Private Network

111 Glossary

111.1 Common Criteria Terms

- **Common Criteria (CC)**. Common Criteria for Information Technology Security Evaluation.
- **Common Evaluation Methodology (CEM)**. Common Evaluation Methodology for Information Technology Security Evaluation.
- **Protection Profile (PP)**. An implementation-independent set of security requirements for a category of products.
- **Security Target (ST)**. A set of implementation-dependent security requirements for a specific product.
- **Target of Evaluation (TOE)**. The product under evaluation. In this case, the Operating System as described in section and its supporting documentation.
- **TOE Security Functionality (TSF)**. The security functionality of the product under evaluation.
- **TOE Summary Specification (TSS)**. A description of how a TOE satisfies the SFRs in a ST
- **Security Functional Requirement (SFR)**. A requirement for security enforcement by the TOE.
- **Security Assurance Requirement (SAR)**. A requirement to assure the security of the TOE
- **Extended Package (EP)**. An implementation-independent set of security requirements for a category of products, which extends those in a Protection Profile.

111.2 Technology Terms

- **Address Space Layout Randomization (ASLR)**. An anti-exploitation feature, which loads memory mappings into unpredictable locations. ASLR makes it more difficult for an attacker to redirect control to code that they have introduced into the address space of a process.
- **Administrator**. An administrator is responsible for management activities, including setting policies that are applied by the enterprise on the operating system. This administrator could be acting remotely through a management server, from which the system receives configuration policies. An administrator can enforce settings on the system, which cannot be overridden by non-administrator users.
- **Application (app)**. Software that runs on a platform and performs tasks on behalf of the user or owner of the platform, as well as its supporting documentation.
- **Application Programming Interface (API)**. A specification of routines, data structures, object classes, and variables that allows an application to make use of services provided by another software component, such as a library. APIs are often provided for a set of libraries included with the platform.

- **Credential**. Data that establishes the identity of a user, e.g. a cryptographic key or password.
- **Critical Security Parameters (CSP)**. Information that is either user or system defined and is used to operate a cryptographic module in processing encryption functions including cryptographic keys and authentication data, such as passwords, the disclosure or modification of which can compromise the security of a cryptographic module or the security of the information protected by the module.
- **Data At Rest (DAR) Protection**. Countermeasures that prevent attackers, even those with physical access, from extracting data from non-volatile storage. Common techniques include data encryption and wiping.
- **Data Execution Prevention (DEP)**. An anti-exploitation feature of modern operating systems executing on modern computer hardware, which enforces a non-execute permission on pages of memory. DEP prevents pages of memory from containing both data and instructions, which makes it more difficult for an attacker to introduce and execute code.
- **Developer**. An entity that writes OS software. For the purposes of this document, vendors and developers are the same.
- **Host-based Firewall**. A software-based firewall implementation running on the OS for filtering inbound and outbound network traffic to and from processes running on the OS.
- **Operating System (OS)**. Software that manages physical and logical resources and provides services for applications. The terms *TOE* and *OS* are interchangeable in this document.
- **Personally Identifiable Information (PII)**. Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.
- **Sensitive Data**. Sensitive data may include all user or enterprise data or may be specific application data such as PII, emails, messaging, documents, calendar items, and contacts. Sensitive data must minimally include credentials and keys. Sensitive data shall be identified in the OS's TSS by the ST author.
- **User**. A user is subject to configuration policies applied to the operating system by administrators. On some systems under certain configurations, a normal user can temporarily elevate privileges to that of an administrator. At that time, such a user should be considered an administrator.
- **Secure Shell (SSH)**. Cryptographic network protocol for initiating text-based shell sessions on remote systems.