**Assurance Activity Report for**

# Arista Networks 7280 Series Switches Running EOS 4.28

Arista Networks 7280 Series Switches Running EOS 4.28 Common Criteria Security Target

Version 0.5

**collaborative Protection Profile for Network Devices Version 2.2e**

AAR Version 1.8, 07/24/2023

**Evaluated by:**

**2400 Research Blvd, Suite 395**
**Rockville, MD 20850**

**Prepared for:**

**National Information Assurance Partnership**
**Common Criteria Evaluation and Validation Scheme**

**The Developer of the TOE:**
Arista Networks, Inc.
5453 Great America Parkway
Santa Clara, CA 95054

**The Author of the Security Target:**
Acumen Security, LLC
2400 Research Blvd., Suite 395
Rockville, MD 20850

**The TOE Evaluation was Sponsored by:**
Arista Networks, Inc.
5453 Great America Parkway
Santa Clara, CA 95054

**Evaluation Personnel:**
FATHI NASRAOUI
MANOHAR NEGI
NISHAN SINGH
BRANDON J. SOLBERG

**Common Criteria Version**
Common Criteria Version 3.1 Revision 5

**Common Evaluation Methodology Version**
CEM Version 3.1 Revision 5

# Revision History

| VERSION | DATE | CHANGES |
|---|---|---|
| 1.0 | 04/03/2023 | Initial Release |
| 1.1 | 05/30/2023 | Conducted all assurance activities |
| 1.2 | 05/30/2023 | Applied TD0738 |
| 1.3 | 06/05/2023 | Updating section Testing |
| 1.4 | 06/07/2023 | QA Comments Addressed |
| 1.5 | 06/09/2023 | Release of new ST version |
| 1.6 | 07/04/2023 | Addressing validator comments |
| 1.7 | 07/14/2023 | Addressing Validators comments |
| 1.8 | 07/24/2023 | Addressing Validators comment |

# Contents

# 1 TOE Overview

## 1.1 TOE Type

The TOE is classified as a Network Device, that is, a device composed of both hardware and software that is connected to the network and has an infrastructure role within the network.

## 1.2 TOE Usage

The Arista Networks Data Center and Cloud Computing Switches are networking switches (Network Devices for CC purposes) that provide OSI model Layer 2, 3, and 4 Ethernet interconnectivity and network management services (Data Link, Network, and Transport Layers, respectively). Each model is manufactured with high performance electronics making it ideally suitable for demanding data center environments.

## 1.3 TOE Major Security Features Summary

- Security Audit
  - Generates audit records, storing them locally and transmitting them to a remote audit server.
  - Supports secure communication to remote syslog-compatible audit servers protected by the SSHv2 Trusted Channel.
- Cryptographic Support
  - Utilization of NIST-specified and CAVP validated cryptographic algorithms for asymmetric key generation, AES encryption/decryption, digital signature generation/verification, hashing, and keyed-hashing (Message Authentication Code).
  - Cryptographic-key Destruction using PP specified methods.
  - Deterministic Random Bit Generation (DRBG).
  - Assurance of seeding the DRBG with sufficient entropy (minimum of 256-bits of entropy).
- Identification and Authentication
  - Administrative password management.
  - Protected authentication data at the local and remote consoles.
  - Identification and authentication of the Security Administrative user.
  - X509 certificate-based authentication and validation.
  - X509 certificate request generation.
- Security Management
  - Trusted Update mechanism.
  - Restriction of TSF management to the Security Administrator.
  - Local and remote administration of the TOE by the Security Administrator.
- Protection of the TSF
  - Protection of stored passwords.
  - Prevention of disclosing passwords via normal management interfaces.
  - Prevention of disclosing private keys via normal management interfaces.
  - Automated self-testing upon boot-up.
  - Querying of the TOE firmware/software.
  - Reliable timestamps.
- TOE Access
  - Session termination (TSF initiated, and User initiated).
  - Display of a warning and consent banner on the local and remote management interfaces prior to authentication.
- Trusted Path/Channels
  - Cryptographically secure path between the TOE and the Security Administrative user for remote management.

- Cryptographically secure channels between the TOE and authorized IT entities in the Operational Environment to support the TSF.

## 1.4 Operational Environment

The TOE's Operational Environment must provide the following services to support the secure operation of the TOE:

- Local Console Administrative Access
  - RS-232 Serial Console.
  - VT-100 terminal emulation program.
- Remote Management
  - SSH client for remote interactive session utilizing SSH.
  - eAPI JSON-RPC Client capable of establishing a mutually authenticated TLS session.
- Audit Server
  - Syslog server capable of accepting an SSHv2 tunnel utilizing SSH Protocol Version 2 (SSHv2).
- Certificate Revocation List (CRL) Server
  - Server from where CRLs can be downloaded on TOE to check validity of X509v3 certificates.

## 1.5 References

In additional to TOE documentation, the following reference may also be valuable when understanding and controlling the TOE:

- Collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP]
- Arista Networks 7280 Switches Running EOS 4.28 Common Criteria Guidance Supplement Version: 2.0

# 2 Assurance Activities Identification

The Assurance Activities contained within this document include all those defined within the NDcPP 2.2e based upon the core SFRs and those implemented based on selections within the PP.

## 2.1 Technical Decisions

The following technical decisions were applied for this evaluation:

| Technical decisions | Applicability | Rational for not applicable |
|---|---|---|
| 0638 – NIT Technical Decision for Key Pair Generation for Authentication | **Yes** | |
| 0636 – NIT Technical Decision for Clarification of Public Key User Authentication for SSH | **Yes** | |
| 0635 – NIT Technical Decision for TLS Server and Key Agreement Parameters | **Yes** | |
| 0631 – NIT Technical Decision for Clarification of public key authentication for SSH Server | **Yes** | |
| 0592 – NIT Technical Decision for Local Storage of Audit Records | **Yes** | |
| 0581 – NIT Technical Decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3 | **Yes** | |
| 0580 – NIT Technical Decision for clarification about use of DH14 in NDcPPv2.2e | **Yes** | |
| 0572 – NiT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers | **Yes** | |
| 0571 – NiT Technical Decision for Guidance on how to handle FIA_AFL.1 | **Yes** | |
| 0570 – NiT Technical Decision for Clarification about FIA_AFL.1 | **Yes** | |
| 0569 – NIT Technical Decision for Session ID Usage Conflict in FCS_DTLSS_EXT.1.7 | **Yes** | |
| 0564 – NiT Technical Decision for Vulnerability Analysis Search Criteria | **Yes** | |
| 0563 – NiT Technical Decision for Clarification of audit date information | **Yes** | |
| 0556 – NIT Technical Decision for RFC 5077 question | **Yes** | |
| 0555 – NIT Technical Decision for RFC Reference incorrect in TLSS Test | **Yes** | |
| 0547 – NIT Technical Decision for Clarification on developer disclosure of AVA_VAN | **Yes** | |
| 0536 – NIT Technical Decision for Update Verification Inconsistency | **Yes** | |
| 0527 – NIT Technical Decision for Updates to Certificate Revocation Testing (FIA_X509_EXT.1) | **Yes** | |

| | | |
|---|---|---|
| 0528 – NIT Technical Decision for Missing EAs for FCS_NTP_EXT.1.4 | **No** | Not claimed in ST |
| 0537 – NIT Technical Decision for Incorrect reference to FCS_TLSC_EXT.2.3 | **No** | ST does not claim FCS_TLSC_EXT |
| 0546 – NIT Technical Decision for DTLS – clarification of Application Note 63 | **No** | Not claimed in ST |
| 0591 – NIT Technical Decision for Virtual TOEs and hypervisors | **No** | Not a Virtual TOE. |
| 0632 – NIT Technical Decision for Consistency with Time Data for vNDs | **No** | TOE does not receive time updates from an underlying virtual server |
| 0633 – NIT Technical Decision for IPsec IKE/SA Lifetimes Tolerance | **No** | TOE does not claim IPsec as a secure channel |
| 0634 – NIT Technical Decision for Clarification required for testing IPv6 | **No** | TOE does not claim FCS_TLSC_EXT or DTLSC |
| 0639 – NIT Technical Decision for Clarification for NTP MAC Keys | **No** | TOE does not claim NTP |
| 0670 – NIT Technical Decision for Mutual and Non-Mutual Auth TLSC Testing | **No** | TOE does not claim FCS_TLSC_EXT |
| 0738 – NIT Technical Decision for Link to Allowed-With List | **Yes** | |

# 3 Test Equivalency Justification

## 3.1 Introduction

This section provides a testing equivalency analysis for the Arista Networks 7280 Series Switches Running EOS 4.28 TOE. This analysis provides an explanation of the differences between each of the hardware models included within the TOE boundary and provides an analysis of the impact each of the differences have on the TSF functionality.

## 3.2 Architectural Description

The Arista 7280 series switches are fixed form factor switches. The 7280 series switches range in size between 1 and 2 RU. Models vary in total throughput, port count, port speeds, route table scales etc.

Each switch model runs Arista's Linux-based network operating system called Extensible Operating System (EOS). The same EOS binary image runs on all TOE hardware models. All EOS code is compiled to the same i686 assembly, making it such that no processor runs anything different from any other processor. All processors implement the i686 assembly language. All SFRs in this Security Target are implemented by EOS. Hence, they behave identically on every switch model.

The table below provides the list of appliances across different series:

**Table 1: Hardware Appliances**

| Series | Models | Interfaces | Host CPU |
|---|---|---|---|
| 7280CR | • SKN-7280CR3-3C2 | 3x100GbE (CFP2) + 2x100GbE | Intel Broadwell-DE D1519 |
| | • SKN-7280CR3-3C2-2 | 3x100GbE (CFP2) + 2x100GbE | Intel Broadwell-DE D1519 |
| | • SKN-7280CR3-3C2-2-DEV | 3x100GbE (CFP2) + 2x100GbE | Intel Broadwell-DE D1519 |
| | • SKN-7280CR3-3C2-2G | 3x100GbE (CFP2) + 2x100GbE | Intel Broadwell-DE D1519 |
| | • SKN-7280CR3-3C2-3 | 3x100GbE (CFP2) + 2x100GbE | Intel Broadwell-DE D1519 |
| | • SKN-7280CR3-3C2-3-DEV | 3x100GbE (CFP2) + 2x100GbE | Intel Broadwell-DE D1519 |
| | • SKN-7280CR3-3C2-3G | 3x100GbE (CFP2) + 2x100GbE | Intel Broadwell-DE D1519 |
| | • SKN-7280CR3-3C2-DEV | 3x100GbE (CFP2) + 2x100GbE | Intel Broadwell-DE D1519 |
| | • SKN-7280CR3-4C2 | 4x100GbE (CFP2) + 2x100GbE | Intel Broadwell-DE D1519 |
| | • SKN-7280CR3-4C2-DEV | 4x100GbE (CFP2) + 2x100GbE | Intel Broadwell-DE D1519 |
| | • SKN-7280CR3-4C2G | 4x100GbE (CFP2) + 2x100GbE | Intel Broadwell-DE D1519 |
| | • SKN-7280CR3-4C6 | 3x100GbE (CFP2) + (9 or 10)x100GbE | Intel Broadwell-DE D1519 |
| | • SKN-7280CR3-4C6-DEV | 3x100GbE (CFP2) + (9 or 10)x100GbE | Intel Broadwell-DE D1519 |
| | • SKN-7280CR3-4C6G | 3x100GbE (CFP2) + (9 or 10)x100GbE | Intel Broadwell-DE D1519 |
| | • SKN-7280CR3-5C2 | 5x100GbE (CFP2) + 2x100GbE | Intel Broadwell-DE D1519 |
| | • SKN-7280CR3-5C2-DEV | 5x100GbE (CFP2) + 2x100GbE | Intel Broadwell-DE D1519 |
| | • SKN-7280CR3-5C2G | 5x100GbE (CFP2) + 2x100GbE | Intel Broadwell-DE D1519 |
| 7280SR | • SKN-7280SR3-16YC8 | 4x CFP2 100G/200G + 4x 40/100G QSFP + 16x 25/10GbE SFP | Intel Broadwell-DE D1519 |

The TOE supports local administration via the local console port. Remote administration is performed over the Secure Shell v2 (SSHv2) protocol. Alternatively, the switch supports eAPI JSON-RPC interface over TLS for remote automation scripts to perform management functions on the switch.

The Arista Networks 7280 Series Switches Running EOS 4.28 Target of Evaluation (TOE) is a standalone TOE. Deployment of the TOE in its evaluated configuration consists of one CUCM server and the required IT Environment components in section 1.3.4 of the ST.

## 3.3 OS, Processor, and Firmware Analysis

The following table compares the Operating System, CPU, and firmware that runs on each of the included TOE platforms

**Table 2: TOE Comparison**

| TOE Models | Description | Analysis |
|---|---|---|
| **Operating system** | | |
| • SKN-7280CR3-3C2<br>• SKN-7280CR3-3C2-2<br>• SKN-7280CR3-3C2-2-DEV<br>• SKN-7280CR3-3C2-2G<br>• SKN-7280CR3-3C2-3<br>• SKN-7280CR3-3C2-3-DEV<br>• SKN-7280CR3-3C2-3G<br>• SKN-7280CR3-3C2-DEV<br>• SKN-7280CR3-4C2<br>• SKN-7280CR3-4C2-DEV<br>• SKN-7280CR3-4C2G<br>• SKN-7280CR3-4C6<br>• SKN-7280CR3-4C6-DEV<br>• SKN-7280CR3-4C6G<br>• SKN-7280CR3-5C2<br>• SKN-7280CR3-5C2-DEV<br>• SKN-7280CR3-5C2G<br>• SKN-7280SR3-16YC8 | Same EOS 4.28 software used in all the different hardware | OS is identical |
| **Base CPU** | | |
| • SKN-7280CR3-3C2<br>• SKN-7280CR3-3C2-2<br>• SKN-7280CR3-3C2-2-DEV<br>• SKN-7280CR3-3C2-2G<br>• SKN-7280CR3-3C2-3<br>• SKN-7280CR3-3C2-3-DEV<br>• SKN-7280CR3-3C2-3G<br>• SKN-7280CR3-3C2-DEV<br>• SKN-7280CR3-4C2<br>• SKN-7280CR3-4C2-DEV<br>• SKN-7280CR3-4C2G<br>• SKN-7280CR3-4C6<br>• SKN-7280CR3-4C6-DEV<br>• SKN-7280CR3-4C6G<br>• SKN-7280CR3-5C2<br>• SKN-7280CR3-5C2-DEV<br>• SKN-7280CR3-5C2G | Intel Broadwell-DE D1519 | CPU microarchitecture is identical |

| | | |
|---|---|---|
| • SKN-7280SR3-16YC8 | | |

## 3.4 Specification of Differences

The following tables provide a description of the physical differences between hardware models. None of the listed hardware differences have any impact of the security functionality provided by the TSF.

**Table 3: TOE's Hardware appliances**

| Series | Models | Interfaces | Host CPU |
|---|---|---|---|
| 7280CR | • SKN-7280CR3-3C2 | 3x100GbE (CFP2) + 2x100GbE | Intel Broadwell-DE D1519 |
| | • SKN-7280CR3-3C2-2 | 3x100GbE (CFP2) + 2x100GbE | Intel Broadwell-DE D1519 |
| | • SKN-7280CR3-3C2-2-DEV | 3x100GbE (CFP2) + 2x100GbE | Intel Broadwell-DE D1519 |
| | • SKN-7280CR3-3C2-2G | 3x100GbE (CFP2) + 2x100GbE | Intel Broadwell-DE D1519 |
| | • SKN-7280CR3-3C2-3 | 3x100GbE (CFP2) + 2x100GbE | Intel Broadwell-DE D1519 |
| | • SKN-7280CR3-3C2-3-DEV | 3x100GbE (CFP2) + 2x100GbE | Intel Broadwell-DE D1519 |
| | • SKN-7280CR3-3C2-3G | 3x100GbE (CFP2) + 2x100GbE | Intel Broadwell-DE D1519 |
| | • SKN-7280CR3-3C2-DEV | 3x100GbE (CFP2) + 2x100GbE | Intel Broadwell-DE D1519 |
| | • SKN-7280CR3-4C2 | 4x100GbE (CFP2) + 2x100GbE | Intel Broadwell-DE D1519 |
| | • SKN-7280CR3-4C2-DEV | 4x100GbE (CFP2) + 2x100GbE | Intel Broadwell-DE D1519 |
| | • SKN-7280CR3-4C2G | 4x100GbE (CFP2) + 2x100GbE | Intel Broadwell-DE D1519 |
| | • SKN-7280CR3-4C6 | 3x100GbE (CFP2) + (9 or 10)x100GbE | Intel Broadwell-DE D1519 |
| | • SKN-7280CR3-4C6-DEV | 3x100GbE (CFP2) + (9 or 10)x100GbE | Intel Broadwell-DE D1519 |
| | • SKN-7280CR3-4C6G | 3x100GbE (CFP2) + (9 or 10)x100GbE | Intel Broadwell-DE D1519 |
| | • SKN-7280CR3-5C2 | 5x100GbE (CFP2) + 2x100GbE | Intel Broadwell-DE D1519 |
| | • SKN-7280CR3-5C2-DEV | 5x100GbE (CFP2) + 2x100GbE | Intel Broadwell-DE D1519 |
| | • SKN-7280CR3-5C2G | 5x100GbE (CFP2) + 2x100GbE | Intel Broadwell-DE D1519 |
| 7280SR | • SKN-7280SR3-16YC8 | 4x CFP2 100G/200G + 4x 40/100G QSFP + 16x 25/10GbE SFP | Intel Broadwell-DE D1519 |

## 3.5 Equivalency Analysis

The following equivalency analysis provides a per category analysis of key areas of differentiation for each hardware model to determine the minimum subset to be used in testing. The areas examined will use the areas and analysis description provided in the supporting documentation for the NDcPP. Additionally, a comparison of the data presented in section 3 is provided to identify a testing subset that will exercise each of the differences in TOE models.

### 3.5.1 Platform/Hardware Dependencies

The TOE boundary is inclusive of all hardware required by the TOE. The hardware platforms do not provide any of the TSF functionality. All security functionality is implemented in Platform Independent code which is the same operating system EOS 4.28 across hardware models. The hardware within the TOE only differs by configuration and performance. There are no platform or hardware specific dependencies of the product.

Both models employ Linux Random Number Generator (LRNG), a software RNG in the Arista EOS operating system which takes inputs from an arbitrary number of software-based noise sources to seed the software DRBG implemented within the TOE.

**Result:** All TOE platforms are equivalent.

### 3.5.2 Software/OS Dependencies

All software including the OS is included in EOS 4.28 and within the TOE boundary. There are no specific dependencies on the OS since the TOE will not be installed with different OSs.

**Result:** All TOE platforms are equivalent.

### 3.5.3 Differences in Libraries Used to Provide TOE Functionality

All software binaries compiled in the TOE software are identical and have the same version numbers. There are no differences between the included libraries. A CAVP certificate has been provided for the cryptographic functionality as tested in the TOE's operational environment.

**Result:** CAVP algorithm testing provide valid coverage for both platforms. The libraries are identical.

### 3.5.4 TOE Management Interface Differences

The TOE is managed via either human user or eAPI JSON-RPC trusted IT entity client. The TOE allows human users with the Security Administrator role to administer the TOE over a remote console (SSH Trusted Path) and local CLI (Local Console). These management options are available on all hardware platforms regardless of the configuration. There is no difference in the management interface for any platform.

**Result:** All TOE platforms are equivalent.

### 3.5.5 TOE Functional Differences

Each hardware model within the TOE boundary provides identical functionality. There is no difference in the way the user interacts with each of the devices or the services that are available to the user in for each of these devices. Each device can be run with the same identical version of EOS software. For TOE software, differences in the provided functionality is denoted by a different version of the software. If there had been differences in the functionality provided by the software, the actual release version would have been different for the platform.

**Result:** All TOE platforms are equivalent

### 3.5.6 Difference Comparison

The following table provides a comparison of each of the categories with differences.

| Series | Models | Base Processor | Software | Crypto Library |
|---|---|---|---|---|
| 7280CR | SKN-7280CR3-3C2 | Intel Broadwell-DE D1519 | EOS 4.28 | EOS Crypto Module v2.0 |
| | SKN-7280CR3-3C2-2 | | | |
| | SKN-7280CR3-3C2-2-DEV | | | |
| | SKN-7280CR3-3C2-2G | | | |
| | SKN-7280CR3-3C2-3 | | | |
| | SKN-7280CR3-3C2-3-DEV | | | |
| | SKN-7280CR3-3C2-3G | | | |
| | SKN-7280CR3-3C2-DEV | | | |
| | SKN-7280CR3-4C2 | | | |
| | SKN-7280CR3-4C2-DEV | | | |
| | SKN-7280CR3-4C2G | | | |
| | SKN-7280CR3-4C6 | | | |
| | SKN-7280CR3-4C6-DEV | | | |
| | SKN-7280CR3-4C6G | | | |
| | SKN-7280CR3-5C2 | | | |
| | SKN-7280CR3-5C2-DEV | | | |
| | SKN-7280CR3-5C2G | | | |

| | | | | |
|---|---|---|---|---|
| 7280SR | SKN-7280SR3-16YC8 | | | |

**Table 4 TOE Difference Highlight**

The above table shows that the TOE models are equivalent.

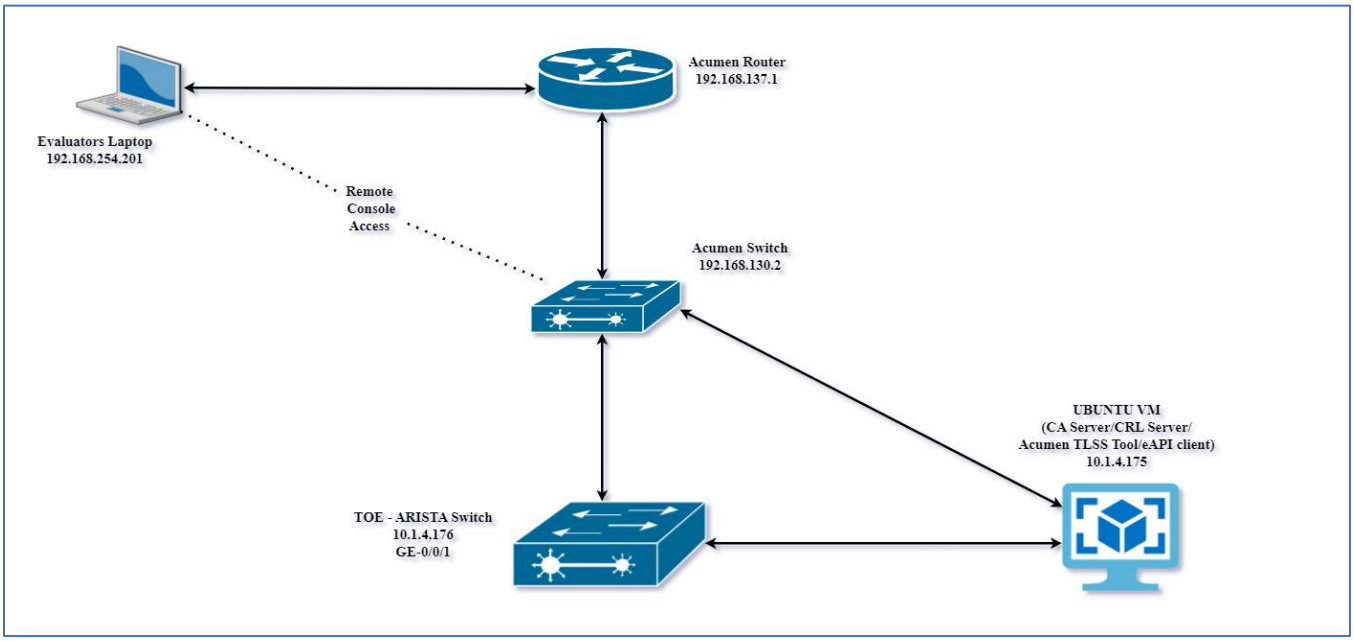
As also described in section “Cryptographic Support” of the ST, all cryptographic functionality for the TOE is implemented by the Arista Crypto Module v2.0. The evaluator has confirmed that the implementation used is identical between the hardware models. The CAVP certificate has been provided for the exact OE on which the TOE software executes.

### 3.5.7 Recommendations/Conclusions

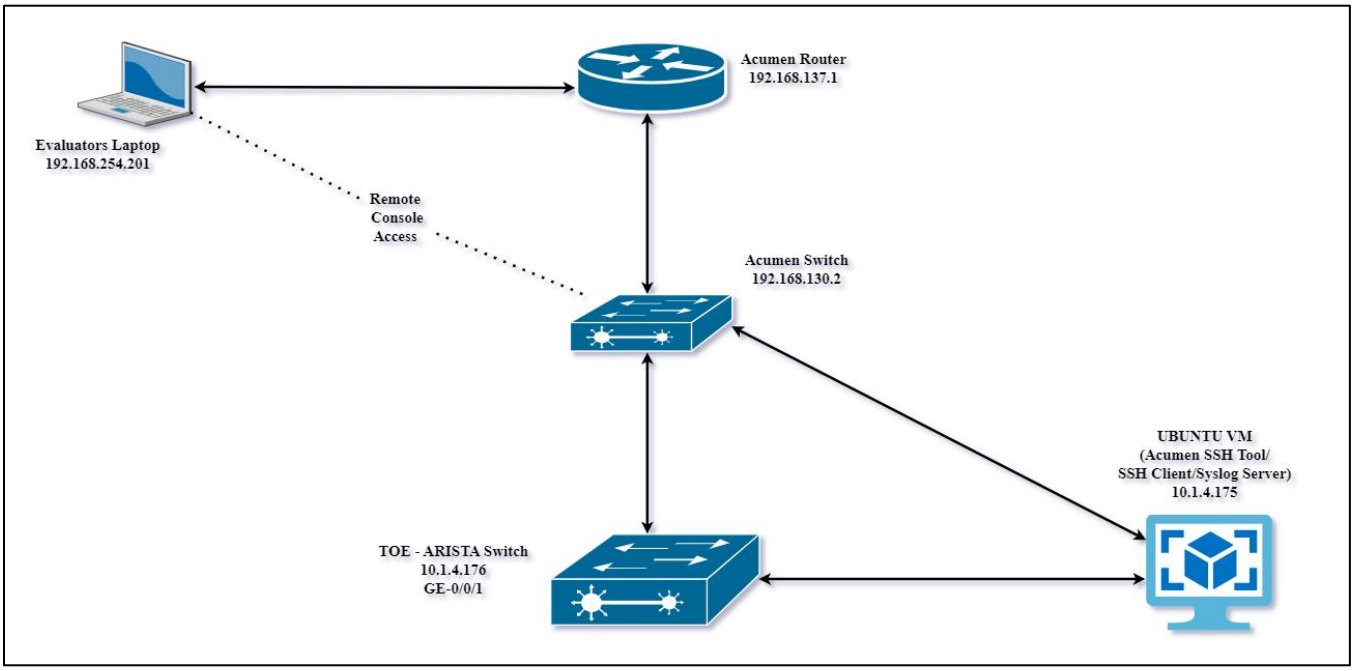
Based on the equivalency rationale listed above, testing will be performed in full on the TOE hardware model: SKN-7280SR3-16YC8.

# 4 Test Bed Descriptions

## 4.1 Test Bed Network Diagram for X509 and TLS Test Cases




## 4.2 Test Bed Network Diagram for Audit, Auth, SSH, update test cases




## 4.3 Test Bed Details

| Name | OS | Function | Protocols | MAC Address | Time | Tools (version) | IP Address |
|---|---|---|---|---|---|---|---|
| Arista Networks 7280 Series Switch | EOS 4.28 | TOE | SSH, TLS | 6e37.6da1.8070 | Manually set and verified | N/A | 10.1.4.176 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Ubuntu VM | Ubuntu 20.04.6 | Packet Capture/ Management workstation/CRL Server/eAPIclient/CA Server/Syslog server | SSH, TLS | 00:50:56:8B:59:92 | Manually set and verified | OpenSSL (1.1.1f), Rsyslog version (8.2210.0), tcpdump version (4.9.3), libpcap version (1.9.1), SSH (OpenSSH 8.2p1) CA Server, CRL Server, Acumen SSHS Tool, Acumen SSHC Tool, Acumen TLSS Tool, eAPI Client (Wget 1.20.3) | 10.1.4.175 |
| Evaluator's Laptop | Windows 10 pro | For TOE configuration and testing. | SSH, TLS | 54-14-F3-E8-BB-AB | Manually set and verified | MobaXterm (Version 21.3), WinSCP 5.19.6, Wireshark 3.4.8 | 192.168.254.201 |

## 4.4 Test Time and location

All testing was conducted on the TOE model SKN-7280SR3-16YC8 running software version 4.28, situated at the Acumen Security offices, specifically at 2400 Research Blvd Suite #395, Rockville, MD 20850. The testing took place between March 2022 and June 2023.

The TOE was located in a physically protected and access-controlled designated test lab, where unattended entry or exit was not permitted. Prior to the start of each testing day, the test bed underwent verification to ensure its integrity and security. All evaluation documentation was consistently stored in a secure folder accessible only to authorized evaluators

A regressing testing was also conducted on the TOE model SKN-7280SR3-16YC8, situated at the Acumen Security offices, specifically at 2400 Research Blvd Suite #395, Rockville, MD 20850. The regression testing took place between May 30, and June 2, 2023, on all SSHC SFR, 2 TLS and 2 x509 test cases.

# 5 Detailed Guidance Assurance Activities

## 5.1 Guidance Activities (Auditing)

### 5.1.1 FAU_GEN.1

#### 5.1.1.1 FAU_GEN.1 Guidance 1

<table>
<tr><td>Objective</td><td>The evaluator shall check the guidance documentation and ensure that it provides an example of each auditable event required by FAU_GEN.1 (i.e., at least one instance of each auditable event, comprising the mandatory, optional and selection-based SFR sections as applicable, shall be provided from the actual audit record).</td></tr>
<tr><td>Evaluator Findings</td><td>The evaluator examined the section titled 4.1 FAU_GEN.1.1 in the AGD to verify that it provides an example of each auditable event required by FAU_GEN.1. Upon investigation, the evaluator found that the AGD section 4.1 FAU_GEN.1.1 contains a listing and description of each of the fields in generated audit records that contain the information required in FAU_GEN.1.2.
<table>
<tr><th colspan="3">Table 7: Auditable Events (Table 2 of cPP)</th></tr>
<tr><th>SFR</th><th>Description</th><th>Additional Audit Record Contents</th></tr>
<tr><td>FAU_GEN.1</td><td>None.</td><td>None.</td></tr>
<tr><td>FAU_GEN.2</td><td>None.</td><td>None.</td></tr>
<tr><td>FAU_STG_EXT.1</td><td>None.</td><td>None.</td></tr>
<tr><td>FCS_CKM.1</td><td>None.</td><td>None.</td></tr>
<tr><td>FCS_CKM.2</td><td>None.</td><td>None.</td></tr>
<tr><td>FCS_CKM.4</td><td>None.</td><td>None.</td></tr>
<tr><td>FCS_COP.1/DataEncryption</td><td>None.</td><td>None.</td></tr>
<tr><td>FCS_COP.1/SigGen</td><td>None.</td><td>None.</td></tr>
<tr><td>FCS_COP.1/Hash</td><td>None.</td><td>None.</td></tr>
<tr><td>FCS_COP.1/KeyedHash</td><td>None.</td><td>None.</td></tr>
<tr><td>FCS_RBG_EXT.1</td><td>None.</td><td>None.</td></tr>
<tr><td>FCS_SSHC_EXT.1</td><td>Failure to establish an SSH session</td><td>Reason for failure.</td></tr>
<tr><td>FCS_SSHS_EXT.1</td><td>Failure to establish an SSH session</td><td>Reason for failure.</td></tr>
<tr><td>FCS_TLSS_EXT.1</td><td>Failure to establish a TLS session</td><td>Reason for failure.</td></tr>
<tr><td>FCS_TLSS_EXT.2</td><td>Failure to authenticate the client</td><td>Reason for failure</td></tr>
<tr><td>FIA_AFL.1</td><td>Unsuccessful login attempts limit is met or exceeded.</td><td>Origin of the attempt (e.g., IP address).</td></tr>
<tr><td>FIA_PMG_EXT.1</td><td>None.</td><td>None.</td></tr>
<tr><td>FIA_UIA_EXT.1</td><td>All use of the identification and authentication mechanism.</td><td>Origin of the attempt (e.g., IP address).</td></tr>
<tr><td>FIA_UAU_EXT.2</td><td>All use of the identification and authentication mechanism.</td><td>Origin of the attempt (e.g., IP address).</td></tr>
<tr><td>FIA_UAU.7</td><td>None.</td><td>None.</td></tr>
<tr><td>FIA_X509_EXT.1/Rev</td><td>Unsuccessful attempt to validate a certificate<br>Any addition, replacement or</td><td>Reason for failure of certificate validation.<br>Identification of certificates</td></tr>
</table>
</td></tr>
</table>

| | | |
|---|---|---|
| | removal of trust anchors in the TOE's trust store. | added, replaced or removed as trust anchor in the TOE's trust store. |
| FIA_X509_EXT.2 | None. | None. |
| FIA_X509_EXT.3 | None. | None. |
| FMT_MOF.1/Functions | None. | None. |
| FMT_MOF.1/ManualUpdate | Any attempt to initiate a manual update | None. |
| FMT_MTD.1/CoreData | None. | None. |
| FMT_MTD.1/CryptoKeys | None. | None. |
| FMT_SMF.1 | All management activities of TSF data. | None. |
| FMT_SMR.2 | None. | None. |
| FPT_SKP_EXT.1 | None. | None. |
| FPT_APW_EXT.1 | None. | None. |
| FPT_TST_EXT.1 | None. | None. |
| FPT_TUD_EXT.1 | Initiation of update; result of the update attempt (success or failure) | None. |
| FPT_STM_EXT.1 | Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1) | For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address). |
| FTA_SSL_EXT.1 | The termination of a local session by the session locking mechanism. | None. |
| FTA_SSL.3 | The termination of a remote session by the session locking mechanism. | None. |
| FTA_SSL.4 | The termination of an interactive session. | None. |
| FTA_TAB.1 | None. | None. |
| FTP_ITC.1 | Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions. | Identification of the initiator and target of failed trusted channels establishment attempt. |
| FTP_TRP.1/Admin | Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions. | None. |

Based on these findings, this assurance activity is considered satisfied.

| | |
|---|---|
| Verdict | Pass |

5.1.1.2 FAU_GEN.1 Guidance 2

<table>
<tr><td>Objective</td><td>The evaluator shall also make a determination of the administrative actions related to TSF data related to configuration changes. The evaluator shall examine the guidance documentation 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 cPP. The evaluator shall document the methodology or approach taken while determining which actions in the administrative guide are related to TSF data related to configuration changes. The evaluator may perform this activity as part of the activities associated with ensuring that the corresponding guidance documentation satisfies the requirements related to it.</td></tr>
<tr><td>Evaluator Findings</td><td>The evaluator examined the AGD to verify that it identifies administrative commands, including subcommands, scripts, and configuration files, which 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 cPP. The evaluator first examined the entirety of AGD to determine what administrative commands are associated with each administrative activity. Upon investigation, the evaluator found that the following are applicable:
<table>
<tr><th>Administrative Activity</th><th>Method (Command/GUI Configuration)</th><th>Section</th></tr>
<tr><td>Audit configuration</td><td>Command</td><td>3.10 Audit Logs Configuration</td></tr>
<tr><td>User Creation</td><td>Command</td><td>3.11 Named User Accounts</td></tr>
<tr><td>Software update</td><td>Command</td><td>3.1 Software Image</td></tr>
<tr><td>Setting time</td><td>Command</td><td>3.2 Hostname, DNS Server, Time Setting, Login Banner and Password Restrictions</td></tr>
<tr><td>Configuring banner</td><td>Command</td><td>3.2 Hostname, DNS Server, Time Setting, Login Banner and Password Restrictions</td></tr>
</table>
Next, the evaluator examined each of the test cases and identified test cases which exercised the above referenced functionality. The audit record associated with the configuration was captured. The following table identifies the test cases in which audit records for those configurations can be found.
<table>
<tr><th>Administrative Activity</th><th>Method (Command/GUI Configuration)</th><th>Test Case(s)</th></tr>
<tr><td>Audit configuration</td><td>Command</td><td>FAU_STG_EXT.1 Test#1</td></tr>
<tr><td>User Creation</td><td>Command</td><td>FIA_PMG_EXT.1 Test#1</td></tr>
<tr><td>Software update</td><td>Command</td><td>FPT_TUD_EXT.1 Test#1</td></tr>
</table></td></tr>
</table>

| | | | |
|---|---|---|---|
| | **Setting time** | Command | FPT_STM_EXT.1 Test#1 |
| | **Configuring banner** | Command | FTA_TAB.1 Test#1 |
| | Based on these findings, this assurance activity is considered satisfied. | | |
| Verdict | Pass | | |

### 5.1.2 FAU_STG_EXT.1

#### 5.1.2.1 FAU_STG_EXT.1 Guidance 1

| | |
|---|---|
| Objective | The evaluator shall also examine the guidance documentation to ensure it describes how to establish the trusted channel to the audit server, as well as describe any requirements on the audit server (particular audit server protocol, version of the protocol required, etc.), as well as configuration of the TOE needed to communicate with the audit server. |
| Evaluator Findings | The evaluator examined the section titled 3.9 SSH Tunnel in the AGD to verify that it describes how to establish the trusted channel to the audit server, as well as describe any requirements on the audit server (particular audit server protocol, version of the protocol required, etc.), as well as configuration of the TOE needed to communicate with the audit server. Upon investigation, the evaluator found that the AGD states that the guidance document consists of configurations necessary on both ends of the SSH Tunnel, including the Endpoint on the Syslog Server and the Endpoint on the Switch.<br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

#### 5.1.2.2 FAU_STG_EXT.1 Guidance 2

| | |
|---|---|
| Objective | The evaluator shall also examine the guidance documentation to determine that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. For example, when an audit event is generated, is it simultaneously sent to the external server and the local store, or is the local store used as a buffer and “cleared” periodically by sending the data to the audit server. |
| Evaluator Findings | The evaluator examined the section titled 3.10 Audit Logs Configuration in the AGD to verify that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. Upon investigation, the evaluator found that the AGD states that<br>By virtue of configuration of SSH Tunnel on this port as described before, log messages are securely tunneled inside SSH to remote Syslog server. Log is sent into the tunnel as soon as it is generated.<br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

#### 5.1.2.3 FAU_STG_EXT.1 Guidance 3

| | |
|---|---|
| Objective | The evaluator shall also ensure that the guidance documentation describes all possible configuration options for FAU_STG_EXT.1.3 and the resulting behavior of the TOE for each |

| | |
|---|---|
| | possible configuration. The description of possible configuration options and resulting behavior shall correspond to those described in the TSS. |
| Evaluator Findings | The evaluator examined the section title 3.10 Audit Logs Configuration in the AGD to verify that it describes all possible configuration options for FAU_STG_EXT.1.3 and the resulting behavior of the TOE for each possible configuration. Upon investigation, the evaluator found that the AGD states the configuration of the periodic audit log rotation for when the local storage space for audit data is full and this is consistent throughout the ST and Guidance Document.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

## 5.2 Guidance Activities (Cryptographic Support)

Note that Test activities in the SD that are typically addressed by referencing CAVP certs are addressed in this section and are identified as "Test/CAVP" activities.

### 5.2.1 FCS_CKM.1

#### 5.2.1.1 FCS_CKM.1 Guidance 1

| | |
|---|---|
| Objective | The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected key generation scheme(s) and key size(s) for all cryptographic protocols defined in the Security Target. |
| Evaluator Findings | The evaluator examined the sections titled 3.12 TLS Server and 4.1 FAU_GEN.1.1 in the AGD to verify that it instructs the administrator how to configure the TOE to use the selected key generation scheme(s) and key size(s) for all cryptographic protocols defined in the Security Target. Upon investigation, the evaluator found that the AGD states the configuration required for the key generation of the key sizes mentioned in the TSS.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 5.2.2 FCS_CKM.2

#### 5.2.2.1 FCS_CKM.2 Guidance 1

| | |
|---|---|
| Objective | The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected key establishment scheme(s). |
| Evaluator Findings | The evaluator examined the section titled 3.8 SSH configuration and 3.12.4 Define ciphersuites in the AGD to verify that they instruct the administrator how to configure the TOE to use the selected key establishment scheme(s).<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 5.2.3 FCS_CKM.4

#### 5.2.3.1 FCS_CKM.4 Guidance 1

| | |
|---|---|
| Objective | A TOE may be subject to situations that could prevent or delay key destruction in some cases. The evaluator shall 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 supporting |

| | |
|---|---|
| | information used). The evaluator shall check that the guidance documentation provides guidance on situations where key destruction may be delayed at the physical layer. |
| Evaluator Findings | The evaluator examined the section titled 3.12.8 cryptographic key destruction in the AGD to verify that it 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. Upon investigation, the evaluator found that there are no items that did not meet conformance to the key destruction requirement.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 5.2.4 FCS_COP.1/DataEncryption

#### 5.2.4.1 FCS_COP.1/DataEncryption Guidance 1

| | |
|---|---|
| Objective | The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected mode(s) and key size(s) defined in the Security Target supported by the TOE for data encryption/decryption. |
| Evaluator Findings | The evaluator examined the sections titled 3.12.4 Define ciphersuites and 3.8 SSH configuration in the AGD to verify that they provide guidance to the administrator on how to configure the TOE to use the selected mode(s) and key size(s) defined in the Security Target supported by the TOE for data encryption/decryption.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 5.2.5 FCS_COP.1/SigGen

#### 5.2.5.1 FCS_COP.1/SigGen Guidance 1

| | |
|---|---|
| Objective | The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected cryptographic algorithm and key size defined in the Security Target supported by the TOE for signature services. |
| Evaluator Findings | The evaluator examined the sections titled 3.9.2 Tunnel Endpoint on the Syslog Server, 3.9.1.2 Generate Public Host Key, 3.12.3 Generate CSR and obtain cert, and 4.1.4 Cryptographic Keys in the AGD to verify that they provide guidance instructs the administrator how to configure the TOE to use the selected cryptographic algorithm and key size defined in the Security Target supported by the TOE for signature services. Upon investigation, the evaluator found that the AGD states the configuration of the supported cipher suites and key size.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 5.2.6 FCS_COP.1/Hash

#### 5.2.6.1 FCS_COP.1/Hash Guidance 1

| | |
|---|---|
| Objective | The evaluator checks the AGD documents to determine that any configuration that is required to configure the required hash sizes is present. |
| Evaluator Findings | the evaluator reviewed sections 3.12.4 'Define cipher suites' and 3.8 'SSH Configuration' in the AGD to verify that they provide instructions on how to configure the required hash sizes. The purpose of this check is to ensure that the TOE operates securely and uses only the |

| | |
|---|---|
| | supported hash sizes. After examining the sections, the evaluator found that the AGD includes the necessary guidance to configure the required hash sizes as specified in the ST. Based on this analysis, the evaluator concluded that this assurance activity has been satisfactorily completed. |
| Verdict | Pass |

### 5.2.7 FCS_COP.1/KeyedHash

#### 5.2.7.1 FCS_COP.1/KeyedHash Guidance 1

| | |
|---|---|
| Objective | The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the values used by the HMAC function: key length, hash function used, block size, and output MAC length used defined in the Security Target supported by the TOE for keyed hash function. |
| Evaluator Findings | The evaluator reviewed section 3.8 titled 'SSH Configuration' in the AGD to verify how to configure the TOE to use the values specified by the Security Target (ST) for the HMAC function, such as key length, hash function, block size, and output MAC length. After examining the section, the evaluator found that the AGD provides the necessary instructions for configuring the HMAC functions:hmac-sha2-256 and hmac-sha2-512 for symmetric encryption, key exchange, and message authentication as required by the ST.<br><br>Based on this analysis, the evaluator concluded that this assurance activity has been satisfactorily completed. |
| Verdict | Pass |

### 5.2.8 FCS_RBG_EXT.1

#### 5.2.8.1 FCS_RBG_EXT.1 Guidance 1

| | |
|---|---|
| Objective | The evaluator shall confirm that the guidance documentation contains appropriate instructions for configuring the RNG functionality. |
| Evaluator Findings | The evaluator examined the section titled 3.7 entropy in the AGD to verify that it contains appropriate instructions for configuring the RNG functionality. Upon investigation, the evaluator found that the AGD states that the network interrupts entropy source is always running when the switch is running. Hardware-based entropy needs to be enabled as follows.<br>`switch(config)#management security`<br>`switch(config-mgmt-sec)#entropy source hardware`<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

## 5.3 Guidance Activities (SSH)

### 5.3.1 FCS_SSHC_EXT.1

#### 5.3.1.1 FCS_SSHC_EXT.1.2 Guidance [TD 0636]

| | |
|---|---|
| Objective | The evaluator shall check the Guidance documentation to ensure that it contains instructions to the administrator on how to ensure that only the allowed mechanisms are used in SSH connections initiated by the TOE. |

| | |
|---|---|
| Evaluator Findings | As part of the evaluation, the evaluator reviewed section 3.8 titled 'SSH Configuration' in the AGD to verify that it provides instructions to the administrator on how to restrict SSH connections initiated by the TOE to only allowed mechanisms. The purpose of this check is to ensure that the TOE operates securely and only uses approved mechanisms for its SSH connections. After examining the section, the evaluator confirmed that it includes the necessary guidance to configure the TOE accordingly. |
| Verdict | Pass |

5.3.1.2 FCS_SSHC_EXT.1.4 Guidance 1

| | |
|---|---|
| Objective | The evaluator shall also check the guidance documentation to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements). |
| Evaluator Findings | The evaluator reviewed section 3.8 titled 'SSH Configuration' in the AGD to verify that it provides instructions on configuring the TOE to conform to the description of SSH in the TSS. After examining the section, the evaluator found that the AGD includes the necessary instructions to configure the TOE with required algorithms to meet the TSS requirements.<br><br>Based on this analysis, the evaluator concluded that this assurance activity has been satisfactorily completed. |
| Verdict | Pass |

5.3.1.3 FCS_SSHC_EXT.1.5 Guidance 1

| | |
|---|---|
| Objective | The evaluator shall also check the guidance documentation to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements). |
| Evaluator Findings | The evaluator reviewed section 3.8 titled 'SSH Configuration' in the AGD to verify that it provides instructions on configuring the TOE to conform to the description of SSH in the TSS. After examining the section, the evaluator found that the AGD includes the necessary instructions to configure the required algorithms as specified in the TSS.<br><br>Based on this analysis, the evaluator concluded that this assurance activity has been satisfactorily completed. |
| Verdict | Pass |

5.3.1.4 FCS_SSHC_EXT.1.6 Guidance 1

| | |
|---|---|
| Objective | The evaluator shall also check the guidance documentation to ensure that it contains instructions to the Security Administrator on how to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE (specifically, that the “none” MAC algorithm is not allowed). |
| Evaluator Findings | The evaluator reviewed section 3.8 titled 'SSH Configuration' in the AGD to confirm that it provides instructions to the administrator on how to restrict SSH connections with the TOE to only allowed data integrity algorithms. After examining the section, the evaluator determined that the AGD includes the necessary guidance to configure the required data integrity algorithms as specified in the ST. |

| | |
|---|---|
| | Based on this analysis, the evaluator concluded that this assurance activity has been satisfactorily completed. |
| Verdict | Pass |

#### 5.3.1.5 FCS_SSHC_EXT.1.7 Guidance 1

| | |
|---|---|
| Objective | The evaluator shall also check the guidance documentation to ensure that it contains instructions to the Security Administrator on how to ensure that only the allowed key exchange algorithms are used in SSH connections with the TOE. |
| Evaluator Findings | The evaluator reviewed section 3.8 of the SSH Configuration in the AGD to verify if it contains instructions for the administrator to ensure that only the allowed key exchange algorithms are used in SSH connections with the TOE. Upon investigation, the evaluator found that the AGD indeed outlines the configuration required to enforce the allowed key exchange algorithms.<br><br>Based on these findings, the assurance activity is considered satisfied. |
| Verdict | Pass |

#### 5.3.1.6 FCS_SSHC_EXT.1.8 Guidance 1

| | |
|---|---|
| Objective | If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, then the evaluator shall check that the guidance documentation describes how to configure those thresholds. Either the allowed values are specified in the guidance documentation and must not exceed the limits specified in the SFR (one hour of session time, one gigabyte of transmitted traffic) or the TOE must not accept values beyond the limits specified in the SFR. The evaluator shall check that the guidance documentation describes that the TOE reacts to the first threshold reached. |
| Evaluator Findings | The evaluator reviewed section 3.8 of the SSH Configuration in the AGD to confirm whether it provides guidance on how to configure any configurable thresholds checked by the TOE to fulfill the SFR and whether the TOE reacts appropriately when the threshold is reached. Upon investigation, the evaluator found that the AGD does contain the necessary configuration instructions for the thresholds, including the frequency and interval, and outlines how the TOE reacts when a threshold is reached.<br><br>Based on these findings, the assurance activity is considered satisfied |
| Verdict | Pass |

### 5.3.2 FCS_SSHS_EXT.1

#### 5.3.2.1 FCS_SSHS_EXT.1.4 Guidance 1

| | |
|---|---|
| Objective | The evaluator shall also check the guidance documentation to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements). |
| Evaluator Findings | The evaluator examined the section titled 3.8 SSH Configuration in the AGD to verify that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS. Upon investigation, the evaluator found that the AGD states the instructions to configure the TOE with claimed algorithms mentioned in the TSS. |

| | |
|---|---|
| | Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

5.3.2.2 FCS_SSHS_EXT.1.5 Guidance 1

| | |
|---|---|
| Objective | The evaluator shall also check the guidance documentation to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements). |
| Evaluator Findings | The evaluator reviewed section 3.8 of the SSH Configuration in the AGD to confirm whether it provides instructions for configuring the TOE to ensure that SSH conforms to the description in the TSS. After examining the section, the evaluator found that the AGD does contain instructions on how to configure the TOE with the required algorithms as specified in the TSS. Based on these findings, the assurance activity is considered satisfied. |
| Verdict | Pass |

5.3.2.3 FCS_SSHS_EXT.1.6 Guidance 1

| | |
|---|---|
| Objective | The evaluator shall also check the guidance documentation to ensure that it contains instructions to the Security Administrator on how to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE (specifically, that the “none” MAC algorithm is not allowed). |
| Evaluator Findings | The evaluator reviewed section 3.8 of the SSH Configuration in the AGD to verify whether it includes instructions for the administrator to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE. After examining the section, the evaluator found that the AGD does provide instructions on how to configure the required algorithms as specified in the TSS. Based on these findings, the assurance activity is considered satisfied. |
| Verdict | Pass |

5.3.2.4 FCS_SSHS_EXT.1.7 Guidance 1

| | |
|---|---|
| Objective | The evaluator shall also check the guidance documentation to ensure that it contains instructions to the Security Administrator on how to ensure that only the allowed key exchange algorithms are used in SSH connections with the TOE. |
| Evaluator Findings | The evaluator examined the section titled 3.8 SSH Configuration in the AGD to verify that it contains instructions to the administrator on how to ensure that only the allowed key exchange algorithms are used in SSH connections with the TOE. Upon investigation, the evaluator found that the AGD states the configuration to enforce the allowed key exchange algorithm.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

5.3.2.5 FCS_SSHS_EXT.1.8 Guidance 1

| | |
|---|---|
| Objective | If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, then the evaluator shall check that the guidance documentation describes how to configure those thresholds. Either the allowed values are specified in the guidance documentation and must not exceed the limits specified in the SFR (one hour of session time, one gigabyte of |

| | |
|---|---|
| | transmitted traffic) or the TOE must not accept values beyond the limits specified in the SFR. The evaluator shall check that the guidance documentation describes that the TOE reacts to the first threshold reached. |
| Evaluator Findings | The evaluator conducted an examination of the section titled "3.8 SSH Configuration" in the AGD with the aim of verifying whether it provides instructions for configuring any configurable thresholds. Upon thorough investigation, it was determined that the AGD includes explicit configuration guidelines for the thresholds of the TOE, encompassing both the frequency and interval. Furthermore, the section emphasizes the importance of executing the SSH rekeying function with unwavering compliance to ensure strict adherence to the common criteria requirements<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

## 5.4 Guidance Activities (TLS)

### 5.4.1 FCS_TLSS_EXT.1

#### 5.4.1.1 FCS_TLSS_EXT.1.1 Guidance 1

| | |
|---|---|
| Objective | The evaluator shall check the guidance documentation 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). |
| Evaluator Findings | During the evaluation, the evaluator reviewed section 3.12.4 Define ciphersuites in the AGD to confirm that it includes instructions on configuring the TOE to ensure that TLS conforms to the description provided in the TSS. Upon investigation, the evaluator determined that the AGD contains instructions to configure the TLS cipher suites supported, which are listed as follows:<br>• AES256-SHA256<br>• AES128-SHA256<br>• DHE-RSA-AES128-SHA256<br>• DHE-RSA-AES256-SHA256<br>• AES256-GCM-SHA384<br>• DHE-RSA-AES256-GCM-SHA384<br><br>These ciphersuites are identical to those listed in the TSS.<br><br>Based on these findings, the assurance activity is considered satisfied. |
| Verdict | Pass |

#### 5.4.1.2 FCS_TLSS_EXT.1.2 Guidance 1

| | |
|---|---|
| Objective | The evaluator shall verify that any configuration necessary to meet the requirement must be contained in the AGD guidance. |
| Evaluator Findings | The evaluator examined the section titled 3.12 TLS Server in the AGD to verify that it contains any configuration necessary to meet the requirement must be contained in the AGD |

| | |
|---|---|
| | guidance. Upon investigation, the evaluator found that the AGD states the list of instructions required to configure the TOE with TLS version 1.2 and deny all other versions.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

#### 5.4.1.3 FCS_TLSS_EXT.1.3 Guidance 1

| | |
|---|---|
| Objective | The evaluator shall verify that any configuration necessary to meet the requirement must be contained in the AGD guidance. |
| Evaluator Findings | The evaluator examined the section titled 3.12 Define cipher suites in the AGD to verify that it contains any configuration necessary to meet the requirement. Upon investigation, the evaluator found that the AGD states the configuration required to use RSA 2048 as well as Diffie-Hellman groups (ffdhe2048, ffdhe3072, ffdhe4096) as claimed in the ST.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

#### 5.4.1.4 FCS_TLSS_EXT.1.4 Guidance 1 [TD0569]

| | |
|---|---|
| Objective | The evaluator shall verify that any configuration necessary to meet the requirement must be contained in the AGD guidance. |
| Evaluator Findings | The evaluator examined the section titled 3.12.4 Define cipher suites in the AGD to verify that it contains any configuration necessary to meet the requirement. Upon investigation, the evaluator found that the AGD states that The TOE implements session resumption using session IDs according to RFC 5246 (TLS 1.2).<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 5.4.2 FCS_TLSS_EXT.2

#### 5.4.2.1 FCS_TLSS_EXT.2.1 and FCS_TLSS_EXT.2.2 Guidance 1

| | |
|---|---|
| Objective | If the TSS indicates that mutual authentication using X.509v3 certificates is used, the evaluator shall verify that the AGD guidance includes instructions for configuring the client-side certificates for TLS mutual authentication. |
| Evaluator Findings | The evaluator thoroughly examined Section 3.14, titled "eAPI Client Operation," in the AGD to ensure that it provides instructions for configuring client-side certificates for TLS mutual authentication when the TSS specifies the use of X.509v3 certificates for mutual authentication. After a detailed investigation, the evaluator discovered that the AGD indeed includes the necessary instructions for configuring the client-side certificate for TLS mutual authentication.<br><br>Based on these conclusive findings, it can be confidently concluded that this assurance activity has been satisfactorily fulfilled |
| Verdict | Pass |

#### 5.4.2.2 FCS_TLSS_EXT.2.1 and FCS_TLSS_EXT.2.2 Guidance 2

| | |
|---|---|
| Objective | The evaluator shall verify the guidance describes how to configure the TLS client certificate authentication function. If the TSF supports fallback authentication functions, the evaluator |

| | |
|---|---|
| | shall verify the guidance provides instructions for configuring the fallback authentication functions. If fallback authentication functions can be disabled, the evaluator shall verify the guidance provides instructions for disabling the fallback authentication functions. |
| Evaluator Findings | The evaluator conducted a comprehensive examination of Section 3.13.1, titled "eAPI fallback authentication" within the AGD. Following an investigation, it was ascertained that the AGD explicitly states that the TOE does incorporate a fallback mechanism for x509 authentication when authenticating any eAPI client. Also, the mentioned section provides instructions for disabling and enabling the fallback authentication function.<br><br>Based on these conclusive findings, it can be concluded that this assurance activity has been satisfactorily fulfilled. |
| Verdict | Pass |

#### 5.4.2.3 FCS_TLSS_EXT.2.3 Guidance 1

| | |
|---|---|
| Objective | The evaluator shall ensure that the AGD guidance describes the configuration of expected identifier(s) for X.509 certificate-based authentication of TLS clients. The evaluator ensures this description includes all types of identifiers described in the TSS and, if claimed, configuration of the TOE to use a directory server. |
| Evaluator Findings | The evaluator examined the section titled 3.12 TLS Server and 3.14 eAPI Client Operation in the AGD to verify that it contains a configuration necessary to meet the requirement. Upon investigation, the evaluator found that the AGD states the instructions to the configuration of the X.509 certificates and CSR required for certificate-based authentication.<br><br>“Note that the certificate used to authenticate, <file2> in the above example, must have the username as the CN attribute in the Subject: of the x509 certificate.”<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

## 5.5 Guidance Activities (Identification and Authentication)

### 5.5.1 FIA_AFL.1

#### 5.5.1.1 FIA_AFL.1 Guidance 1

| | |
|---|---|
| Objective | The evaluator shall examine the guidance documentation to ensure that instructions for configuring the number of successive unsuccessful authentication attempts and time period (if implemented) are provided, and that the process of allowing the remote administrator to once again successfully log on is described for each “action” specified (if that option is chosen). If different actions or mechanisms are implemented depending on the secure protocol employed (e.g., TLS vs. SSH), all must be described. |
| Evaluator Findings | The evaluator examined the section titled 3.11 Named User Accounts in the AGD to verify that it provides instructions for configuring the number of successive unsuccessful authentication attempts and time period, and that the process of allowing the remote administrator to once again successfully log on is described for each “action” specified. Upon investigation, the evaluator found that the AGD states the instructions to configure the |

| | |
|---|---|
| | number of unsuccessful authentication attempts and time period for unlocking the user account.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

5.5.1.2 FIA_AFL.1 Guidance 2

| | |
|---|---|
| Objective | The evaluator shall examine the guidance documentation to confirm that it describes, and identifies the importance of, any actions that are required in order to ensure that administrator access will always be maintained, even if remote administration is made permanently or temporarily unavailable due to blocking of accounts as a result of FIA_AFL.1. |
| Evaluator Findings | The evaluator examined the section titled 3.11 Named User Accounts in the AGD to verify that it describes, and identifies the importance of, actions that are required in order to ensure that administrator access will always be maintained, even if remote administration is made permanently or temporarily unavailable due to blocking of accounts as a result of FIA_AFL.1. Upon investigation, the evaluator found that the AGD states that the RS-232/VT-100 local administrative interface is never locked out.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 5.5.2 FIA_PMG_EXT.1

5.5.2.1 FIA_PMG_EXT.1.1 Guidance 1

| | |
|---|---|
| Objective | The evaluator shall examine the guidance documentation to determine that it:<br><br>a) identifies the characters that may be used in passwords and provides guidance to security administrators on the composition of strong passwords, and<br><br>b) provides instructions on setting the minimum password length and describes the valid minimum password lengths supported. |
| Evaluator Findings | The evaluator examined the section titled 3.2 Hostname, DNS Server, Time Setting, Banner and Password Restrictions in the AGD to verify that it identifies the characters that may be used in passwords and provides guidance to security administrators on the composition of strong passwords and provides instructions on setting the minimum password length and describes the valid minimum password lengths supported. Upon investigation, the evaluator found that the AGD states the instructions to configure the minimum length of the password.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 5.5.3 FIA_UIA_EXT.1

5.5.3.1 FIA_UIA_EXT.1 Guidance 1

| | |
|---|---|
| Objective | The evaluator shall examine the guidance documentation to determine that any necessary preparatory steps (e.g., establishing credential material such as pre- shared keys, tunnels, certificates, etc.) to logging in are described. For each supported the login method, the evaluator shall ensure the guidance documentation provides clear instructions for successfully logging on. If configuration is necessary to ensure the services provided before |

| | |
|---|---|
| | login are limited, the evaluator shall determine that the guidance documentation provides sufficient instruction on limiting the allowed services. |
| Evaluator Findings | The evaluator examined the section titled 3.4 Default Accounts Protection in the AGD to verify that it describes any necessary preparatory steps (e.g., establishing credential material such as pre- shared keys, tunnels, certificates, etc.) to logging in. Upon investigation, the evaluator found that the AGD states that there are two authentication stages to access to switch. Instructions to configure the initial password of the admin, and configuration of the boot password are within the section.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 5.5.4 FIA_UAU.7

#### 5.5.4.1 FIA_UAU.7 Guidance 1

| | |
|---|---|
| Objective | The evaluator shall examine the guidance documentation to determine that any necessary preparatory steps to ensure authentication data is not revealed while entering for each local login allowed. |
| Evaluator Findings | The evaluator examined the section titled 3.4 Default Accounts Protection in the AGD to verify that it describes any necessary preparatory steps to ensure authentication data is not revealed while entering for each local login allowed. Upon investigation, the evaluator found that the AGD states the instructions to configure the authentication data is not revealed while entering the password for both logins supported to login to the TOE.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 5.5.5 FIA_X509_EXT.1/Rev

#### 5.5.5.1 FIA_X509_EXT.1/Rev Guidance 1

| | |
|---|---|
| Objective | The evaluator shall also ensure that the guidance documentation describes where the check of validity of the certificates takes place, describes any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied) and describes how certificate revocation checking is performed and on which certificate. |
| Evaluator Findings | The evaluator examined the section titled 3.12.9 x509 certificate validation in the AGD to verify that it contains describes where the check of validity of the certificates takes place, describes any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE and describes how certificate revocation checking is performed and on which certificate. Upon investigation, the evaluator found that the AGD states that extended key usage in server certificate must have Server Authentication purpose and in client presented certificate must have Client Authentication purpose. Also the evaluator found that theAGD states that the TOE does not provide support for code signing and OCSP signing attributes in the extendedKeyUsage field of the leaf certificate when presented by the e-API client or when included in an x509 certificate imported into its trusted store.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 5.5.6 FIA_X509_EXT.2

#### 5.5.6.1 FIA_X509_EXT.2 Guidance 1

| | |
|---|---|
| Objective | The evaluator shall check the administrative guidance to ensure that it includes any necessary instructions for configuring the operating environment so that the TOE can use the certificates. |
| Evaluator Findings | The evaluator reviewed the section titled 3.12 TLS Server in the AGD to verify the presence of instructions necessary for configuring the operating environment to enable the TOE to utilize the certificates. Upon investigation, it was discovered that the AGD includes the instructions of loading the certificate chain and CRL onto the TOE and configuring them so that they can be access from the TOE, the configuration required so the TOE can access the correct certificates from the SSL profile created, the configuration required on the TOE for the eAPI Server to use the correct SSL profile.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

#### 5.5.6.2 FIA_X509_EXT.2 Guidance 2

| | |
|---|---|
| Objective | If the requirement that the administrator is able to specify the default action, then the evaluator shall ensure that the guidance documentation contains instructions on how this configuration action is performed. |
| Evaluator Findings | The evaluator examined the section titled 3.12.9 X509 certificate validation in the AGD to verify that, if the requirement that the administrator is able to specify the default action, the guidance documentation contains instructions on how this configuration action is performed. Upon investigation, the evaluator found that the AGD states that the certificate will not be accepted if the validity of the certificate cannot be verified and states that this is the default action.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

#### 5.5.6.3 FIA_X509_EXT.2 Guidance 3

| | |
|---|---|
| Objective | The evaluator shall also ensure that the guidance documentation describes the configuration required in the operating environment so the TOE can use the certificates. The guidance documentation shall also include any required configuration on the TOE to use the certificates. The guidance document shall also describe the steps for the Security Administrator to follow if the connection cannot be established during the validity check of a certificate used in establishing a trusted channel. |
| Evaluator Findings | The evaluator examined the section titled 3.12 TLS Server in the AGD. Upon investigation, the evaluator found that the AGD states that if the certificate validation process fails, or if the CRL is deleted, the SSL profile becomes invalid and provide instructions on how to successfully reestablish the process, also the AGD states examples of failed logs as reference to unlikely events.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 5.5.7 FIA_X509_EXT.3

#### 5.5.7.1 FIA_X509_EXT.3 Guidance 1

| | |
|---|---|
| Objective | The evaluator shall check to ensure that the guidance documentation contains instructions on requesting certificates from a CA, including generation of a Certificate Request. If the ST author selects "Common Name", "Organization", "Organizational Unit", or "Country", the evaluator shall ensure that this guidance includes instructions for establishing these fields before creating the Certification Request. |
| Evaluator Findings | The evaluator examined the section titled 3.12.3 Generate CSR and obtain signed certificate in the AGD to verify that it contains instructions on requesting certificates from a CA, including generation of a Certification Request. Upon investigation, the evaluator found that the AGD states the instructions to configure the Common Name, Organization, Organizational Unit, and Country and establishing the field during the Certificate Request creation.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

## 5.6 Guidance Activities (Security Management)

### 5.6.1 FMT_MOF.1/ManualUpdate

#### 5.6.1.1 FMT_MOF.1/ManualUpdate Guidance 1

| | |
|---|---|
| Objective | The evaluator shall examine the guidance documentation to determine that any necessary steps to perform manual update are described.<br><br>The guidance documentation shall also provide warnings regarding functions that may cease to operate during the update (if applicable). |
| Evaluator Findings | The evaluator examined the section titled 3.1 Software Image in the AGD to verify that it describes any necessary steps to perform manual update. Upon investigation, the evaluator found that the AGD states the instructions to download an image from a usb and perform a manual update.<br><br>The evaluator examined the section titled 3.1 Software Image in the AGD to verify that it provides warnings regarding functions that may cease to operate during the update (if applicable). Upon investigation, the evaluator found that the AGD states that:" Note: As part of the update procedure, a reboot of the switch will be required to facilitate the loading of the new image. Consequently, there will be a brief window of disruption affecting all functions and features until the switch is successfully reinitialized with the updated image. Subsequently, upon completion of the reboot process, all functions and features will be restored to their normal operational state."<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 5.6.2 FMT_FMT_MOF.1/Functions

#### 5.6.2.1 FMT_MOF.1/Functions Guidance 2

| | |
|---|---|
| Objective | For non-distributed TOEs, the evaluator shall also ensure the Guidance Documentation describes how the Security Administrator determines or modifies the behaviour of (whichever |

| | |
|---|---|
| | is supported by the TOE) transmitting audit data to an external IT entity, handling of audit data, audit functionality when Local Audit Storage Space is full (whichever is supported by the TOE) are performed to include required configuration settings. |
| Evaluator Findings | The evaluator examined the section titled 3.10 Audit Logs Configuration and 3.9 SSH Tunnel in the AGD to verify that it describes how the Security Administrator determines or modifies the behavior of transmitting audit data to an external IT entity, handling of audit data, audit functionality when Local Audit Storage Space is full are performed to include required configuration settings. Upon investigation, the evaluator found that the AGD states that audit data is written to local persistent storage as soon as it is generated. When the file exceeds its size limit, it is trimmed to remove the oldest audit logs until the size drops below set length.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 5.6.3 FMT_MTD.1/CoreData

#### 5.6.3.1 FMT_MTD.1/CoreData Guidance 1

| | |
|---|---|
| Objective | The evaluator shall review the guidance documentation to determine that each of the TSF-data-manipulating functions implemented in response to the requirements of the cPP is identified, and that configuration information is provided to ensure that only administrators have access to the functions. |
| Evaluator Findings | The evaluator examined the section titled 4.2.9 FMT_SMF.1 in the AGD to verify that it identifies each of the TSF-data-manipulating functions implemented in response to the requirements of the cPP. Upon investigation, the evaluator found that the AGD states that all CLI commands run by users are logged and all management activities performed on TSF data are logged and can be viewed by the Security Administrators at all times.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

#### 5.6.3.2 FMT_MTD.1/CoreData Guidance 2

| | |
|---|---|
| Objective | If the TOE supports handling of X.509v3 certificates and provides a trust store, the evaluator shall review the guidance documentation to determine that it provides sufficient information for the administrator to configure and maintain the trust store in a secure way. If the TOE supports loading of CA certificates, the evaluator shall review the guidance documentation to determine that it provides sufficient information for the administrator to securely load CA certificates into the trust store. The evaluator shall also review the guidance documentation to determine that it explains how to designate a CA certificate a trust anchor. |
| Evaluator Findings | The evaluator conducted an examination of the section titled "3.12.5 Configure Certificate Check Restrictions" in the AGD (Administrator's Guide Document) to validate that, in case the TOE (Target of Evaluation) supports X.509v3 certificates and provides a trust store, it offers comprehensive instructions to the administrator for secure configuration and maintenance of the trust store. Upon investigation, it was determined that the AGD specifies the requisite configuration steps for importing and locating X.509v3 certificates into the trust store.<br><br>Additionally, the evaluator reviewed the section titled "3.12.6 Load Certificate Chain and CRLs" in the AGD to verify that, if the TOE supports loading of CA (Certificate Authority) certificates, it furnishes sufficient guidance to the administrator for secure loading of CA |

| | |
|---|---|
| | certificates into the trust store, as well as explaining the process of designating a CA certificate as a trust anchor. After investigation, it was ascertained that the AGD provides the necessary information to import the required CA certificates into the certificate folder of the TOE, along with supplementary details for managing the CA certificates.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 5.6.4 FMT_MTD.1/CryptoKeys

#### 5.6.4.1 FMT_MTD.1/CryptoKeys Guidance 2

| | |
|---|---|
| Objective | For non-distributed TOEs, the evaluator shall also ensure the Guidance Documentation lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed. |
| Evaluator Findings | The evaluator examined the section titled 3.8 SSH Configuration and 3.12 TLS Server and 4.1.4 Cryptographic Keys in the AGD to verify that it lists the keys the Security Administrator is able to manage to include the options available (e.g., generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed. Upon investigation, the evaluator found that the AGD states that for each of the keys that the TOE supports and requires, SSH key and TLS key, there are instructions to manage, generate, import, modify, and delete the keys.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 5.6.5 FMT_SMF.1

#### 5.6.5.1 FMT_SMF.1 Guidance 1

| | |
|---|---|
| Objective | The evaluator shall examine the TSS and Guidance Documentation to verify they both describe the local administrative interface. The evaluator shall ensure the Guidance Documentation includes appropriate warnings for the administrator to ensure the interface is local. |
| Evaluator Findings | The evaluator examined the section titled 5.1 console CLI access in the AGD to verify that it describes the local administrative interface. Upon investigation, the evaluator found that the AGD states that the console port is a serial port located on the front of the switch. The TOE's administrator should use a serial or RS-232 cable to connect to the console port. The accessory kit also includes an RJ-45 to DB-9 adapter cable for connecting to the switch.<br><br>The evaluator examined the section titled 1.5 console CLI access in the AGD to verify that it includes appropriate warnings for the administrator to ensure the interface is local. Upon investigation, the evaluator found that the AGD describes the steps associated with connecting to the serial port of a computer. This sufficiently ensures that the interface is a local interface.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 5.6.6 FMT_SMR.2

#### 5.6.6.1 FMT_SMR.2 Guidance 1

| | |
|---|---|
| Objective | The evaluator shall review the guidance documentation to ensure that it contains instructions for administering the TOE both locally and remotely, including any configuration that needs to be performed on the client for remote administration. |
| Evaluator Findings | The evaluator examined the section titled 3.4 Default Accounts Protection and 3.11 Named User Accounts in the AGD to verify that it contains instructions for administering the TOE both locally and remotely, including any configuration that needs to be performed on the client for remote administration. Upon investigation, the evaluator found that the AGD states the initial setup required to locally access the administrative accounts, and also to configure the remote access of the admin accounts.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

## 5.7 Guidance Activities (Protection of the TSF)

### 5.7.1 FPT_STM_EXT.1

#### 5.7.1.1 FPT_STM_EXT.1 Guidance 1 [TD0632]

| | |
|---|---|
| Objective | The evaluator examines the guidance documentation to ensure it instructs the administrator how to set the time. If the TOE supports the use of an NTP server, the guidance documentation instructs how a communication path is established between the TOE and the NTP server, and any configuration of the NTP client on the TOE to support this communication.<br><br>If the TOE supports obtaining time from the underlying VS, the evaluator shall verify the Guidance Documentation specifies any configuration steps necessary. If no configuration is necessary, no statement is necessary in the Guidance Documentation. If there is a delay between updates to the time on the VS and updating the time on the TOE, the evaluator shall ensure the Guidance Documentation informs the administrator of the maximum possible delay. |
| Evaluator Findings | The evaluator examined the section titled 3.2 Hostname, DNS Server, Time Setting, Login Banner, and Password Restrictions in the AGD to verify that it describes the instructions on how the administrator can set and check time on the TOE.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass. |

### 5.7.2 FPT_TST_EXT.1.1

#### 5.7.2.1 FPT_TST_EXT.1.1 Guidance 1

| | |
|---|---|
| Objective | The evaluator shall also ensure that the guidance documentation describes the possible errors that may result from such tests, and actions the administrator should take in response; these possible errors shall correspond to those described in the TSS. |
| Evaluator Findings | The evaluator examined the section titled 4.2.18 Verifying Integrity of Software and FIPS self-tests on Startup in the AGD to verify that it describes the possible errors that may result from such tests, and actions the administrator should take in response. Upon investigation, the |

| | |
|---|---|
| | evaluator found that the AGD states the method of entering debug mode and viewing audit logs for checking the integrity and taking response to it.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 5.7.3 FPT_TUD_EXT.1

#### 5.7.3.1 FPT_TUD_EXT.1 Guidance 1

| | |
|---|---|
| Objective | The evaluator shall verify that the guidance documentation describes how to query the currently active version. If a trusted update can be installed on the TOE with a delayed activation, the guidance documentation needs to describe how to query the loaded but inactive version. |
| Evaluator Findings | The evaluator examined the section titled 3.1 Software Image in the AGD to verify that it describes how to query the currently active version and, if a trusted update can be installed on the TOE with a delayed activation, the loaded but inactive version. Upon investigation, the evaluator found that the AGD states the command to show the current software version of the TOE.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

#### 5.7.3.2 FPT_TUD_EXT.1 Guidance 2

| | |
|---|---|
| Objective | The evaluator shall verify that the guidance documentation describes how the verification of the authenticity of the update is performed (digital signature verification or verification of published hash). The description shall include the procedures for successful and unsuccessful verification. The description shall correspond to the description in the TSS. |
| Evaluator Findings | The evaluator examined the section titled 3.1 Software Image in the AGD to verify that it describes how the verification of the authenticity of the update is performed. Upon investigation, the evaluator found that the AGD states the command to verify the checksum of the image file and to check for the hash and verify with the published hash.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

#### 5.7.3.3 FPT_TUD_EXT.1 Guidance 3

| | |
|---|---|
| Objective | If a published hash is used to protect the trusted update mechanism, the evaluator shall verify that the guidance documentation describes how the Security Administrator can obtain authentic published hash values for the updates. |
| Evaluator Findings | The evaluator conducted an examination of the section titled "3.1 Software Image" in the AGD to verify whether it provides instructions on obtaining authentic published hash values for updates, specifically when a published hash is utilized to safeguard the trusted update mechanism. Upon investigation, it was discovered that the AGD explicitly mentions that the authentic published hash can be obtained from the Vendor's website.<br><br>Based on these findings, this assurance activity is considered satisfied . |
| Verdict | Pass |

#### 5.7.3.4 FPT_TUD_EXT.1 Guidance 4

| | |
|---|---|
| Objective | For distributed TOEs the evaluator shall verify that the guidance documentation describes how the versions of individual TOE components are determined for FPT_TUD_EXT.1, how all TOE components are updated, and the error conditions that may arise from checking or applying the update (e.g. failure of signature verification, or exceeding available storage space) along with appropriate recovery actions. . The guidance documentation only has to describe the procedures relevant for the Security Administrator; it does not need to give information about the internal communication that takes place when applying updates. |
| Evaluator Findings | Not applicable because the TOE is not a distributed TOE. |
| Verdict | N/A |

#### 5.7.3.5 FPT_TUD_EXT.1 Guidance 5

| | |
|---|---|
| Objective | If this was information was not provided in the TSS: For distributed TOEs, the evaluator shall examine the Guidance Documentation to ensure that it describes how all TOE components are updated, that it describes all mechanisms that support continuous proper functioning of the TOE during update (when applying updates separately to individual TOE components) and how verification of the signature or checksum is performed for each TOE component. |
| Evaluator Findings | Not applicable because the TOE is not a distributed TOE. |
| Verdict | N/A |

#### 5.7.3.6 FPT_TUD_EXT.1 Guidance 6

| | |
|---|---|
| Objective | If this was information was not provided in the TSS: If the ST author indicates that a certificate-based mechanism is used for software update digital signature verification, the evaluator shall verify that the Guidance Documentation contains a description of how the certificates are contained on the device. The evaluator also ensures that the Guidance Documentation describes how the certificates are installed/updated/selected, if necessary. |
| Evaluator Findings | The evaluator examined the TSS & AGD and confirmed that the certificate-based mechanism is not employed for digital signature verification of software updates to the TOE. |
| Verdict | Pass |

## 5.8 Guidance Activities (TOE Access)

### 5.8.1 FTA_SSL_EXT.1

#### 5.8.1.1 FTA_SSL_EXT.1 Guidance 1

| | |
|---|---|
| Objective | The evaluator shall confirm that the guidance documentation states whether local administrative session locking or termination is supported and instructions for configuring the inactivity time period. |
| Evaluator Findings | The evaluator examined the section titled 3.11 Named User Accounts in the AGD to verify whether it provides information regarding the support for local administrative session locking or termination, as well as instructions for configuring the inactivity time period. Upon investigation, it was determined that the AGD contains explicit instructions for configuring the lock on unsuccessful authentication attempts, along with the duration settings. These |

| | |
|---|---|
| | guidelines ensure that the system allows for appropriate management of local administrative sessions.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 5.8.2 FTA_SSL.3

#### 5.8.2.1 FTA_SSL.3 Guidance 1

| | |
|---|---|
| Objective | The evaluator shall confirm that the guidance documentation includes instructions for configuring the inactivity time period for remote administrative session termination. |
| Evaluator Findings | The evaluator conducted an examination of the section titled "3.8 SSH Configuration" in the AGD with the objective of verifying whether it encompasses instructions for configuring the inactivity time period to facilitate the termination of remote administrative sessions. Upon investigation, it was determined that the AGD provides explicit instructions for configuring the termination of a remote administrative session using the supported protocol. These instructions ensure that the system can effectively manage and terminate remote administrative sessions based on the specified inactivity time period.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 5.8.3 FTA_SSL.4

#### 5.8.3.1 FTA_SSL.4 Guidance 1

| | |
|---|---|
| Objective | The evaluator shall confirm that the guidance documentation states how to terminate a local or remote interactive session. |
| Evaluator Findings | The evaluator reviewed the sections titled "3.3 Console Idle Timeout" in the AGD to verify if it provides instructions on terminating local or remote interactive sessions. Upon investigation, it was found that the AGD does include instructions on how to terminate a local or remote interactive sessions.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 5.8.4 FTA_TAB.1

#### 5.8.4.1 FTA_TAB.1 Guidance 1

| | |
|---|---|
| Objective | The evaluator shall check the guidance documentation to ensure that it describes how to configure the banner message. |
| Evaluator Findings | The evaluator examined the section titled 3.2 Hostname, DNS Server, Time Setting, Login Banner and Password Restrictions in the AGD. The objective was to confirm whether it provides detailed instructions on configuring the banner message. Upon investigation, it was determined that the AGD includes precise guidelines for configuring the login banner, ensuring its proper display prior to establishing any connection.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

## 5.9 Guidance Activities (Trusted Path/Channels)

### 5.9.1 FTP_ITC.1

#### 5.9.1.1 FTP_ITC.1 Guidance 1

| | |
|---|---|
| Objective | The evaluator shall confirm that the guidance documentation contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken. |
| Evaluator Findings | The evaluator examined the AGD's "3.8 SSH Configuration" and "3.12 TLS Server" sections to verify the presence of instructions concerning the establishment of permitted protocols with authorized IT entities, as well as guidelines for recovering from unintended connection disruptions. Upon investigation, it was determined that the AGD does include explicit instructions for configuring and recovering established sessions with each authorized IT entity.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 5.9.2 FTP_TRP.1/Admin

#### 5.9.2.1 FTP_TRP.1/Admin Guidance 1

| | |
|---|---|
| Objective | The evaluator shall confirm that the guidance documentation contains instructions for establishing the remote administrative sessions for each supported method. |
| Evaluator Findings | The evaluator reviewed the "3.8 SSH Configuration" section in the AGD to validate the presence of instructions for setting up remote administrative sessions using each supported method. Upon investigation, it was determined that the AGD outlines the configuration requirements for establishing a remote connection to the TOE for remote administrative sessions using the supported method.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

# 6 Detailed TSS Assurance Activities

## 6.1 TSS Activities (Auditing)

### 6.1.1 FAU_GEN.1

#### 6.1.1.1 FAU_GEN.1 TSS 1

| | |
|---|---|
| Objective | For the administrative task of generating/import of, changing, or deleting of cryptographic keys as defined in FAU_GEN.1.1c, the TSS should identify what information is logged to identify the relevant key. |
| Evaluator Findings | The evaluator examined the section titled 7.1 Security Audit in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that within this section it identified the following information that was logged in order to identify the relevant key in relation to import/generation, changing, or deletion of cryptographic keys:<br>Changes to cryptographic keys performed by security administrators:<br>▪ Generating SSH key pair. The same key pair is used by both SSH server and client.<br>▪ Generating key pair for Certificate Signing Request (CSR).<br>▪ Importing of new TLS server certificate.<br>In each of the above cases, SHA-256 hash of the public key or the certificate file is included in the audit log to uniquely identify them.<br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 6.1.2 FAU_GEN.2

#### 6.1.2.1 FAU_GEN.2 TSS 1

| | |
|---|---|
| Objective | The TSS and Guidance Documentation requirements for FAU_GEN.2 are already covered by the TSS and Guidance Documentation requirements for FAU_GEN.1. |
| Verdict | N/A. The TOE is not distributed. |

### 6.1.3 FAU_STG_EXT.1

#### 6.1.3.1 FAU_STG_EXT.1 TSS 1

| | |
|---|---|
| Objective | The evaluator shall examine the TSS to ensure it describes the means by which the audit data are transferred to the external audit server, and how the trusted channel is provided. |
| Evaluator Findings | The evaluator examined the section titled 7.1 Security Audit in the Security Target to verify that the TSS describes the means by which the audit data are transferred to the external audit server, and how the trusted channel is provided. Upon investigation, the evaluator found that the TSS states the following:<br>"The logs can also be sent to configured remote audit server in syslog format as soon as they are generated. To protect the audit records in transit from the TOE to the remote audit server in the Operational Environment, the TOE establishes a Trusted Channel between itself and the external audit server using the SSHv2 protocol. The Trusted Channel is created when the |

| | |
|---|---|
| | TOE establishes an SSH session between itself and the remote audit server with TCP port forwarding enabled. After the SSH session is established, the TOE is configured by the Security Administrative user to forward all messages received by the syslog process to the listening TCP port created by the SSH connection. This ensures that all audit traffic is encapsulated and hence protected by the SSH connection."<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

6.1.3.2 FAU_STG_EXT.1 TSS 2

| | |
|---|---|
| Objective | The evaluator shall examine the TSS to ensure it describes the amount of audit data that are stored locally; what happens when the local audit data store is full; and how these records are protected against unauthorized access. |
| Evaluator Findings | The evaluator examined the section titled 7.1 Security Audit in the Security Target to verify that the TSS describes the amount of audit data that are stored locally; what happens when the local audit data store is full; and how these records are protected against unauthorized access. Upon investigation, the evaluator found that the TSS states the following:<br><br>"Audit logs generated by the TSF are stored locally in the persistent Flash memory. The maximum size for the file storing the local audit logs is configurable. When the file exceeds its size limit, it is trimmed to remove the oldest audit logs until the size drops below the configured threshold. Locally stored audit records are protected from unauthorized viewing, modification and deletion by the file system's read/write permissions and a restrictive CLI which only allows identified, authorized and authenticated administrative users read/write access. The Security Administrative user can delete the locally stored audit records. Modification of the audit records other than deleting them is not supported."<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

6.1.3.3 FAU_STG_EXT.1 TSS 3

| | |
|---|---|
| Objective | The evaluator shall examine the TSS to ensure it describes whether the TOE is a standalone TOE that stores audit data locally or a distributed TOE that stores audit data locally on each TOE component or a distributed TOE that contains TOE components that cannot store audit data locally on themselves but need to transfer audit data to other TOE components that can store audit data locally. The evaluator shall examine the TSS to ensure that for distributed TOEs it contains a list of TOE components that store audit data locally. The evaluator shall examine the TSS to ensure that for distributed TOEs that contain components which do not store audit data locally but transmit their generated audit data to other components it contains a mapping between the transmitting and storing TOE components. |
| Evaluator Findings | The evaluator examined the section titled 7. TOE Summary Specification in the Security Target to verify that the TSS describes whether the TOE is a standalone TOE that stores audit data locally or a distributed TOE that stores audit data locally on each TOE component or a distributed TOE that contains TOE components that cannot store audit data locally on themselves but need to transfer audit data to other TOE components that can store audit data locally. Upon investigation, the evaluator found that the TSS states the following procedure: |

| | |
|---|---|
| | “The TOE consist of a single standalone component that stores audit data locally. Audit logs generated by the TSF are stored locally in the persistent Flash memory.”<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

6.1.3.4 FAU_STG_EXT.1 TSS 4

| | |
|---|---|
| Objective | The evaluator shall examine the TSS to ensure that it details the behaviour of the TOE when the storage space for audit data is full. When the option ‘overwrite previous audit record’ is selected this description should include an outline of the rule for overwriting audit data. If ‘other actions’ are chosen such as sending the new audit data to an external IT entity, then the related behaviour of the TOE shall also be detailed in the TSS. |
| Evaluator Findings | The section on "Security Audit" in the Security Target was examined by the evaluator to ensure that the TSS section provides comprehensive information about the TOE's behavior when the storage space allocated for audit data reaches its maximum capacity. After examination, the evaluator found that the TSS explicitly outlines the following procedure:<br><br>"When the size of the audit file surpasses its predefined limit, a trimming mechanism is employed to eliminate the oldest audit logs until the file size decreases to a level below the configured threshold."<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

6.1.3.5 FAU_STG_EXT.1 TSS 5

| | |
|---|---|
| Objective | The evaluator shall examine the TSS to ensure that it details whether the transmission of audit information to an external IT entity can be done in realtime or periodically. In case the TOE does not perform transmission in realtime the evaluator needs to verify that the TSS provides details about what event stimulates the transmission to be made as well as the possible acceptable frequency for the transfer of audit data. |
| Evaluator Findings | The evaluator reviewed the "Security Audit" section within the Security Target to verify whether the TSS provides explicit information regarding the real-time or periodic transmission of audit information to an external IT entity. Upon investigation, the evaluator found the following details stated in the TSS:<br><br>“The logs can also be sent to configured remote audit server in syslog format as soon as they are generated. To protect the audit records in transit from the TOE to the remote audit server in the Operational Environment, the TOE establishes a Trusted Channel between itself and the external audit server using the SSHv2 protocol. The Trusted Channel is created when the TOE establishes an SSH session between itself and the remote audit server with TCP port forwarding enabled. After the SSH session is established, the TOE is configured by the Security Administrative user to forward all messages received by the syslog process to the listening TCP port created by the SSH connection. This ensures that all audit traffic is encapsulated and hence protected by the SSH connection.” |

| | |
|---|---|
| | Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

## 6.2 TSS Activities (Cryptographic Support)

Note that Test activities in the SD that are typically addressed by referencing CAVP certs are addressed in this section and are identified as “Test/CAVP” activities.

### 6.2.1 FCS_CKM.1

#### 6.2.1.1 FCS_CKM.1 TSS 1

| | |
|---|---|
| Objective | The evaluator shall ensure that the TSS identifies the key sizes supported by the TOE. If the ST specifies more than one scheme, the evaluator shall examine the TSS to verify that it identifies the usage for each scheme. |
| Evaluator Findings | the evaluator reviewed the "Cryptographic Support" section within the Security Target. The main objective was to verify whether the TSS clearly identifies the key sizes that are supported by the TOE. After investigation, the evaluator discovered that the TSS provides the following information:<br><br>“The TSF supports generation of 2048-bit RSA asymmetric keys for eAPI TLS server authentication and for SSH client and SSH server authentication. Additionally, ECDSA host keys may be used for SSH client and SSH server authentication. The supported RSA scheme meets the FIPS PUB 186-4, Digital Signature Standard (DSS), Appendix B.3 standard. The supported ECDSA scheme meets the FIPS PUB 186-4, Digital Signature Standard (DSS), Appendix B.4. The TSF generates Diffie-Hellman asymmetric keys for session key establishment in accordance with SP 800-56a Rev3 for SSH and TLS sessions according to RFC 3526 and RFC 7919.”<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

#### 6.2.1.2 FCS_CKM.1 Test/CAVP 1

| | |
|---|---|
| Objective | The evaluator shall verify the key generation mechanisms supported by the TOE. |
| Evaluator Findings | CAVP Certs: #A2946<br><br>Key Generation for FIPS PUB 186-4 RSA Schemes<br><br>For RSA key generation, the validation of this scheme was conducted and validated by #A2946 (RSA KeyGen (FIPS PUB 186-4) for the tested TOE model.<br><br>Key Generation for Elliptic Curve Cryptography (ECC)<br><br>For ECC (ECDSA) key generation, the validation of this scheme was conducted and validated by #A2946 (ECDSA KeyGen (FIPS PUB 186-4)) for the tested TOE model.<br><br>Key Generation for Finite-Field Cryptography (FFC)<br><br>FCC schemes are not claimed, hence not applicable to the TOE.<br><br>Safe Primes Key Generation<br><br>For FFC-Safe prime key generation, the validation of this scheme was conducted and validated by #A2946 (Safe Primes Key Generation) for the tested TOE model. |

| | |
|---|---|
| | Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 6.2.2 FCS_CKM.2

#### 6.2.2.1 FCS_CKM.2 TSS 1 [**TD0580]**

| | |
|---|---|
| Objective | The evaluator shall 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 shall examine the TSS to verify that it identifies the usage for each scheme. It is sufficient to provide the scheme, SFR, and service in the TSS. |
| Evaluator Findings | The evaluator examined the section titled 7.2 Cryptographic Support in the Security Target to verify that the TSS supported key establishment schemes correspond to the key generation schemes identified in FCS_CKM.1.1. Upon investigation, the evaluator found that the TSS states that<br><br>Session keys for both SSH and TLS are generated with Diffie Hellman (DH) key exchange. OpenSSL library is used to perform DH operations of key pair generation and common secret computation using values of DH prime and DH generator is as specified in SP 800-56a Rev3 and RFC 3526 and RFC 7919. Depending on the TLS cipher suite used during a TLS communication, session keys for TLS are also generated using RSA key establishment schemes that adhere to RSAES-PKCS1-v1_5, as specified in Section 7.2 of RFC 3447, “Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1”.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

#### 6.2.2.2 FCS_CKM.2 Test/CAVP 1

| | |
|---|---|
| Objective | The evaluator shall verify the key establishment mechanisms supported by the TOE. |
| Evaluator Findings | CAVP Certs: #A2946<br><br>RSA-based key establishment schemes<br><br>The evaluator conducted testing using an independent known-good implementation during test cases for FCS_TLSS_EXT.1.1 using RSA public/private keys. The connections were successful.<br><br>SP800-56A Key Establishment Schemes<br><br>TOE does not claim elliptic-key based key exchange scheme; therefore, this test requirement is not applicable.<br><br>FFC Schemes using “safe-prime” groups<br><br>The FFC Schemes using “safe-prime” scheme: the validation of this scheme was conducted and validated by #A2946 (KAS-FFC-SSC) for the tested TOE model.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 6.2.3 FCS_CKM.4

#### 6.2.3.1 FCS_CKM.4 TSS 1

| | |
|---|---|
| Objective | The evaluator shall examine the TSS to ensure it lists all relevant keys (describing the origin and storage location of each), all relevant key destruction situations (e.g., factory reset or device wipe function, disconnection of trusted channels, key change as part of a secure channel protocol), and the destruction method used in each case. For the purpose of this Evaluation Activity the relevant keys are those keys that are relied upon to support any of the SFRs in the Security Target. The evaluator confirms that the description of keys and storage locations is consistent with the functions carried out by the TOE (e.g., that all keys for the TOE-specific secure channels and protocols, or that support FPT_APW.EXT.1 and FPT_SKP_EXT.1, are accounted for2). In particular, if a TOE claims not to store plaintext keys in non-volatile memory, then the evaluator checks that this is consistent with the operation of the TOE. |
| Evaluator Findings | The evaluator examined the section titled 7.2 Cryptographic Support (FCS) in the Security Target to verify that the TSS lists all relevant keys (describing the origin and storage location of each), all relevant key destruction situations (e.g., factory reset or device wipe function, disconnection of trusted channels, key change as part of a secure channel protocol), and the destruction method used in each case. Upon investigation, the evaluator found that the TSS states that for plain keys in volatile storage, the destruction shall be executed by a single overwrite consisting of zeros.<br><br>The evaluator examined the section titled 7.2 Cryptographic Support (FCS) in the Security Target to verify that the TSS description of keys and storage locations is consistent with the functions carried out by the TOE. Upon investigation, the evaluator found that the TSS states that that for plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that logically addresses the storage location of the key and performs a single-pass overwrite consisting of zeros.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

#### 6.2.3.2 FCS_CKM.4 TSS 2

| | |
|---|---|
| Objective | The evaluator shall check to ensure the TSS identifies how the TOE destroys keys stored as plaintext in non-volatile memory, and that the description includes identification and description of the interfaces that the TOE uses to destroy keys (e.g., file system APIs, key store APIs). |
| Evaluator Findings | The evaluator examined the section titled 7.2 Cryptographic Support (FCS) in the Security Target to verify that the TSS identifies how the TOE destroys keys stored as plaintext in non-volatile memory, and that the description includes identification and description of the interfaces that the TOE uses to destroy keys. Upon investigation, the evaluator found that the TSS states that the programmatic destruction of keys is carried out by using a specialized algorithm that overwrites the file location with successive random and all-zero patterns and then ensures that the key is destroyed by reading it back. This is done before writing the new key to the file.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

6.2.3.3 FCS_CKM.4 TSS 3

<table>
<tr><td>Objective</td><td>Where the TSS identifies keys that are stored in a non-plaintext form, the evaluator shall check that the TSS identifies the encryption method and the key-encrypting-key used, and that the key-encrypting-key is either itself stored in an encrypted form or that it is destroyed by a method included under FCS_CKM.4.</td></tr>
<tr><td>Evaluator Findings</td><td>The evaluator examined the section titled 7.2 Cryptographic Support (FCS) in the Security Target to verify that the TSS identifies the encryption method and the key-encrypting-key used, and that the key-encrypting-key is either itself stored in an encrypted form or that it is destroyed by a method included under FCS_CKM.4. Upon investigation, the evaluator found that the TSS states that
<table>
<tr><th colspan="6">Table 18: CSPs</th></tr>
<tr><th>CSP</th><th>Purpose</th><th>Generation</th><th>Clearing Method</th><th>When cleared</th><th>Storage Location</th></tr>
<tr><td>TLS Server: RSA Private Key</td><td>“eAPI” server authentication</td><td>Generated internally when TLS server is first started or when new key pair is requested by Security Administrator</td><td>Single direct overwrite consisting of zeroes</td><td>When replaced by the Security Administrator</td><td>Flash</td></tr>
<tr><td>TLS Server: DH Private Key</td><td>Establish session keys for TLS session</td><td>Generated internally at the start of TLS session</td><td>Single direct overwrite consisting of zeroes</td><td>When TLS session keys are derived</td><td>RAM</td></tr>
<tr><td>TLS Server: Session Keys</td><td>Message authentication and encryption in TLS session</td><td>Generated internally at the start of TLS session</td><td>Single direct overwrite consisting of zeroes</td><td>When TLS session terminates</td><td>RAM</td></tr>
<tr><td>SSH Server: RSA Private Key</td><td>SSH host authentication for remote administrative session</td><td>Generated internally when SSH service on the TOE is first started or when new key pair is requested by Security Administrator.</td><td>Single direct overwrite consisting of zeroes</td><td>When replaced by the Security Administrator</td><td>Flash</td></tr>
</table>
</td></tr>
</table>

| | | | | | | |
|---|---|---|---|---|---|---|
| | SSH Server: DH Private Key | Establish session keys for SSH session | Generated internally at the start of SSH session | Single direct overwrite consisting of zeroes | When SSH session keys are derived | RAM |
| | SSH Server: Session Keys | Message authentication and encryption in SSH session | Generated internally at the start of SSH session | Single direct overwrite consisting of zeroes | When SSH session terminates | RAM |
| | SSH Client: RSA Private Key | SSH client authentication to audit server | Generated internally when SSH service on the TOE is first started or when new key pair is requested by Security Administrator. | Single direct overwrite consisting of zeroes | When replaced by the Security Administrator | Flash |
| | SSH Client: ECDSA Private Key | SSH client authentication to audit server | Generated internally when SSH service on the TOE is first started or when new key pair is requested by Security Administrator. | Single direct overwrite consisting of zeroes | When replaced by the Security Administrator | Flash |
| | SSH Client: DH Private Key | Establish session keys for SSH session | Generated internally at the start of SSH session | Single direct overwrite consisting of zeroes | When SSH session keys are derived | RAM |
| | SSH Client: Session Keys | Message authentication and encryption in SSH session | Generated internally at the start of SSH session | Single direct overwrite consisting of zeroes | When SSH session terminates | RAM |
| | Based on these findings, this assurance activity is considered satisfied. | | | | | |
| Verdict | Pass | | | | | |

#### 6.2.3.4 FCS_CKM.4 TSS 4

| | |
|---|---|
| Objective | The evaluator shall check that the TSS identifies any configurations or circumstances that may not conform to the key destruction requirement (see further discussion in the Guidance Documentation section below). Note that reference may be made to the Guidance Documentation for description of the detail of such cases where destruction may be prevented or delayed. |
| Evaluator Findings | The evaluator examined the section titled 7.2 Cryptographic Support (FCS) in the Security Target to verify that the TSS identifies any configurations or circumstances that may not conform to the key destruction requirement. Upon investigation, the evaluator found that the TSS states the following:" In the unlikely event that there is a write-failure the issue will be reported in the logging system. In such circumstances it is recommended to replace the media and physically destroy the faulty non-volatile memory device."<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

#### 6.2.3.5 FCS_CKM.4 TSS 5

| | |
|---|---|
| Objective | Where the ST specifies the use of "a value that does not contain any CSP" to overwrite keys, the evaluator shall examine the TSS to ensure that it describes how that pattern is obtained and used, and that this justifies the claim that the pattern does not contain any CSPs. |
| Evaluator Findings | The evaluator examined the section titled 7.2 Cryptographic Support (FCS) in the Security Target to verify that the TSS describes how that pattern is obtained and used, and that this justifies the claim that the pattern does not contain any CSPs. Upon investigation, the evaluator found that the TSS states that DH keys and session keys of TLS and SSH are ephemeral and stored in RAM. They are zeroized by a single direct overwrite consisting of zeroes, by the time the corresponding session terminates.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 6.2.4 FCS_COP.1/DataEncryption

#### 6.2.4.1 FCS_COP.1/DataEncryption TSS 1

| | |
|---|---|
| Objective | The evaluator shall examine the TSS to ensure it identifies the key size(s) and mode(s) supported by the TOE for data encryption/decryption. |
| Evaluator Findings | The evaluator examined the section titled 7.2 Cryptographic Support (FCS) in the Security Target to verify that the TSS to ensure it identifies the key size(s) and mode(s) supported by the TOE for data encryption/decryption. Upon investigation, the evaluator found that the TSS states that the TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in CBC, GCM mode and cryptographic key sizes 128 bits, 256 bits that meet the following: AES as specified in ISO 18033-3, CBC as specified in ISO 10116, GCM as specified in ISO 19772.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

#### 6.2.4.2 FCS_COP.1/DataEncryption Test/CAVP 1

| | |
|---|---|
| Objective | The evaluator shall verify the implementation of encryption supported by the TOE. |
| Evaluator Findings | CAVP AES Certs: # A2946 (AES-CBC)<br>CBC as specified in ISO 10116, GCM as specified in ISO 19772:<br>The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in CBC, GCM mode and cryptographic key sizes 128 bits, 256 bits that meet the following: AES as specified in ISO 18033-3<br>AES-GCM cryptographic operations are validated under CAVP A2946 (AES-GCM).<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 6.2.5 FCS_COP.1/SigGen

#### 6.2.5.1 FCS_COP.1/SigGen TSS 1

| | |
|---|---|
| Objective | The evaluator shall examine the TSS to determine that it specifies the cryptographic algorithm and key size supported by the TOE for signature services. |
| Evaluator Findings | The evaluator examined the section titled 7.2 Cryptographic Support (FCS) in the Security Target to verify that the TSS to ensure it specifies the cryptographic algorithm and key size supported by the TOE for signature services. Upon investigation, the evaluator found that the TSS states that:<br>RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSAPKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3<br><br>ECDSA schemes using curve P-384 that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D, Implementing “NIST curves” P-256, P-384, ISO/IEC 14888-3, Section 6.4<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

#### 6.2.5.2 FCS_COP.1/SigGen Test/CAVP 1

| | |
|---|---|
| Objective | The evaluator shall verify the implementation of signature generation and verification supported by the TOE. |
| Evaluator Findings | RSA Signature Algorithm Tests:<br>For the claimed TOE model, RSA SigGen operations for TLS are validated under CAVP A2946 (RSA SigGen (FIPS186-4)).<br>RSA SigVer operations for TLS for the claimed TOE model are validated under CAVP A2946 (RSA SigVer(FIPS186-4)).<br><br>ECDSA Algorithm Tests |

| | |
|---|---|
| | For the claimed TOE model, ECDSA SigGen operations for SSH are validated under CAVP A2946 (ECDSA SigGen(FIPS186-4)).<br>ECDSA SigVer operations for SSH for the claimed TOE model are validated under CAVP A2946 (ECDSA SigVer (FIPS186-4)).<br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 6.2.6 FCS_COP.1/Hash

#### 6.2.6.1 FCS_COP.1/Hash TSS 1

| | |
|---|---|
| Objective | The evaluator shall check that the association of the hash function with other TSF cryptographic functions (for example, the digital signature verification function) is documented in the TSS. |
| Evaluator Findings | The evaluator examined the section titled 7.2 Cryptographic Support (FCS) in the Security Target to verify that the TSS documents the association of the hash function with other TSF cryptographic functions. Upon investigation, the evaluator found that the TSS states<br>SHS that meets ISO/IEC 10118-3:2004.<br>SHA<br>Bit-oriented Mode<br>Byte-oriented Mode<br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

#### 6.2.6.2 FCS_COP.1/Hash Test/CAVP 1

| | |
|---|---|
| Objective | The evaluator shall verify the implementation of hashing supported by the TOE. |
| Evaluator Findings | TLS and SSH hashing services, and Password hashing services are validated under CAVP Certs: #A2946 (SHA2-256, SHA2-384, SHA2-512) for the claimed TOE model<br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 6.2.7 FCS_COP.1/KeyedHash

#### 6.2.7.1 FCS_COP.1/KeyedHash TSS 1

| | |
|---|---|
| Objective | The evaluator shall examine the TSS to ensure that it specifies the following values used by the HMAC function: key length, hash function used, block size, and output MAC length used. |
| Evaluator Findings | The evaluator examined the section titled 7.2 Cryptographic Support (FCS) in the Security Target to verify that the TSS specifies the following values used by the HMAC function: key length, hash function used, block size, and output MAC length used. Upon investigation, the evaluator found that the TSS states<br>HMAC-SHA2-256<br>HMAC-SHA2-384 |

| | |
|---|---|
| | HMAC-SHA2-512<br><br>Key Sizes < Block Size<br>Key Sizes > Block Size<br>Key Sizes = Block Size<br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

6.2.7.2 FCS_COP.1/KeyedHash Test/CAVP 1

| | |
|---|---|
| Objective | The evaluator shall verify the implementation of MACing supported by the TOE. |
| Evaluator Findings | TLS and SSH secure hashing services are validated under the CAVP HMAC Certs: #A2946 (HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512)<br>HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 and cryptographic key sizes **256, 384, and 512-bits** and **message digest sizes 256, 384, 512 bits** that meet the following: ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2".<br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

## 6.2.8 FCS_RBG_EXT.1

6.2.8.1 FCS_RBG_EXT.1 TSS 1

| | |
|---|---|
| Objective | The evaluator shall examine the TSS to determine that it specifies the DRBG type, identifies the entropy source(s) seeding the DRBG, and state the assumed or calculated min-entropy supplied either separately by each source or the min-entropy contained in the combined seed value. |
| Evaluator Findings | The evaluator examined the section titled 7.2 Cryptographic Support (FCS) in the Security Target to verify that the TSS specifies the DRBG type, identifies the entropy source(s) seeding the DRBG, and state the assumed or calculated min-entropy supplied either separately by each source or the min-entropy contained in the combined seed value. Upon investigation, the evaluator found that the TSS states that<br>The TOE uses a platform-based CTR_DRBG (AES-256) random bit generator (DRBG) that complies with NIST SP 800-90 for all cryptographic operations. Each DRBG instance is seeded with full 384 bits of entropy (256 bits for AES key and 128 bits for nonce) sourced from Linux Random Number Generator (LRNG) operating in a blocking mode (/dev/random). LRNG accumulates entropy from the Infineon SLB9670 Trusted Platform Module. The detailed entropy justification is provided in [ENT].<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

6.2.8.2 FCS_RBG_EXT.1.1 Test/CAVP 1

| | |
|---|---|
| Objective | The evaluator shall perform 15 trials for the RNG implementation. If the RNG is configurable, the evaluator shall perform 15 trials for each configuration. |

| | |
|---|---|
| | 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 shall 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<br><br>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 SP800-90A).<br><br>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 shall generate eight input values for each trial. The first is a count (0<br><br>– 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.<br><br>The following paragraphs contain more information on some of the input values to be generated/selected by the evaluator.<br><br>**Entropy input:** the length of the entropy input value must equal the seed length.<br><br>**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.<br><br>**Personalization string:** The length of the personalization string must be <= 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 shall use personalization strings of two different lengths. If the implementation does not use a personalization string, no value needs to be supplied.<br><br>**Additional input:** the additional input bit lengths have the same defaults and restrictions as the personalization string lengths. |
| Evaluator Findings | The implementation of SP 800-90A DRBG is validated under the CAVP DRBG Certs: #A2946 (Counter DRBG)<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

## 6.3 TSS Activities (SSH)

### 6.3.1 FCS_SSHC_EXT.1

#### 6.3.1.1 FCS_SSHC_EXT.1.2 TSS 1 **[TD0636]**

| | |
|---|---|
| Objective | The evaluator shall check to ensure that the TSS contains a list of the public key algorithms that are acceptable for use for user authentication and that this list is consistent with |

| | |
|---|---|
| | asymmetric key generation algorithms selected in FCS_CKM.1, hashing algorithms selected in FCS_COP.1/Hash, and signature generation algorithms selected in FCS_COP.1/SigGen. The evaluator shall confirm the TSS is unambiguous in declaring the TOE's ability to authenticate itself to a remote endpoint with a user-based public key.<br><br>If password-based authentication method has been selected in the FCS_SSHC_EXT.1.2, then the evaluator shall confirm it is also described in the TSS. |
| Evaluator Findings | The evaluator examined the section titled 7.2 Cryptographic Support (FCS) in the Security Target to verify that the TSS contains a description of the public key algorithms that are acceptable for use for authentication and that this list is consistent with asymmetric key generation algorithms elected in FCS_CKM.1, hashing algorithms selected in FCS_COP.1/Hash, and signature generation algorithms selected in FCS_COP.1/SigGen and ensure that if password-based authentication methods have been selected in FCS_SSHC_EXT1.2 then these are also described. Upon investigation, the evaluator found that the TSS states that<br><br>The following public key scheme is supported: rsa-sha2-256 that uses 2048-bit RSA key and SHA-256 digital signature or ecdsa-sha2-nistp384.<br><br>The SSH client session keys are established using DH key exchange. The scheme supported is: diffie-hellman-group14-sha1. It supports 2048-bit asymmetric keys (DH Group 14). It uses SHA-1 for exchange hash. Exchange hash is the hashing method used to generate session keys hierarchy from the shared secret derived from DH key establishment.<br><br>The encryption/decryption cipher supported is AES-CBC with 128 and 256 key lengths. The Message authentication code supported are hmac-sha2-256 and hmac-sha2-512.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

6.3.1.2 FCS_SSHC_EXT.1.3 TSS 1

| | |
|---|---|
| Objective | The evaluator shall check that the TSS describes how "large packets" in terms of RFC 4253 are detected and handled. |
| Evaluator Findings | The evaluator reviewed section 7.2 Cryptographic Support (FCS) in the Security Target to confirm whether the TSS provides details on the detection and handling of "large packets" as defined in RFC 4253. Upon investigation, it was discovered that the TOE utilizes OpenSSH as the software for SSH server capabilities. OpenSSH employs a default maximum packet size of 256 KB for SSH connections. Throughout the SSH connection establishment process, OpenSSH actively monitors and validates the size of incoming packets. Should a packet be identified as exceeding the specified maximum size, OpenSSH adheres to the requirements outlined in RFC 4253 and terminates the connection.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

6.3.1.3 FCS_SSHC_EXT.1.4 TSS 1

| | |
|---|---|
| Objective | The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics are specified, and the encryption algorithms supported |

| | |
|---|---|
| | are specified as well. The evaluator shall check the TSS to ensure that the encryption algorithms specified are identical to those listed for this component. |
| Evaluator Findings | The evaluator reviewed section 7.2 Cryptographic Support (FCS) in the Security Target to validate whether the TSS provides information on the optional features and supported encryption algorithms, ensuring that the specified encryption algorithms match those listed for this particular component. After examination, the evaluator determined that the TSS specifies the following:<br><br>Encryption/decryption cipher supported: AES-CBC with key lengths of 128 and 256. This means that the TOT supports the AES encryption algorithm in Cipher Block Chaining (CBC) mode, with key sizes of 128 bits and 256 bits.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

6.3.1.4 FCS_SSHC_EXT.1.5 TSS 1 **[TD 0636]**

| | |
|---|---|
| Objective | The evaluator shall confirm the TSS describes how a host-key public key (i.e., SSH server's public key) is associated with the server identity.<br><br>The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics are specified, and the host-key public key algorithms supported by the TOE are specified as well. The evaluator shall check the TSS to ensure that the host-key public key algorithms specified are identical to those listed for this component. |
| Evaluator Findings | The evaluator examined the section titled 7.2 Cryptographic Support (FCS) in the Security Target to verify that the TSS specifies the optional characteristics and the public key algorithms supported. The evaluator checked the TSS to ensure that the public key algorithms specified are identical to those listed for this component and that the public key algorithms specified are identical to those listed for this component. Upon investigation, the evaluator found that the TSS states that<br><br>The TOE performs the role of SSH client in Trusted Channel. The TSF ensures that the SSH client authenticates the identity of the audit server using the /etc/ssh/known_hosts file which associates each server host name with its corresponding public key as described in RFC 4251. For this, the TSF compares the received host key from the audit server during the SSH handshake and compares it to the keys configured in the known_hosts file. If there is a match, the connection establishment process proceeds. If there is no match found, the session is terminated. SSH client authenticates to the audit server using public key.<br><br>The following public key scheme is supported: rsa-sha2-256 that uses 2048-bit RSA key and SHA-256 digital signature or ecdsa-sha2-nistp384.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

6.3.1.5 FCS_SSHC_EXT.1.5 TSS 2

| | |
|---|---|
| Objective | If x509v3-based public key authentication algorithms are claimed, the evaluator shall confirm that the TSS includes the description of how the TOE establishes the server's identity and how this identity is confirmed with the one that is presented in the provided certificate. For |

| | |
|---|---|
| | example, the TOE could verify that a server's configured IP address matches the one presented in the server's x.509v3 certificate. |
| Evaluator Findings | The security target does not declare support for the x509v3-based public key authentication algorithm in SSH. As a result, this TSS assurance activity is not applicable. |
| Verdict | Pass |

6.3.1.6 FCS_SSHC_EXT.1.6 TSS 1

| | |
|---|---|
| Objective | The evaluator shall check the TSS to ensure that it lists the supported data integrity algorithms, and that the list corresponds to the list in this component. |
| Evaluator Findings | The evaluator examined the section titled 7.2 Cryptographic Support (FCS) in the Security Target to verify that the TSS lists the supported data integrity algorithms, and that that list corresponds to the list in this component. Upon investigation, the evaluator found that the TSS states that<br><br>SSH session keys are established using DH key exchange. The scheme supported is: diffie-hellman-group14-sha1. It supports 2048-bit asymmetric keys (DH Group 14). It uses SHA-1 for exchange hash. Exchange hash is the hashing method used to generate session keys hierarchy from the shared secret derived from DH key establishment.<br><br>Encryption/decryption cipher supported is AES-CBC with 128 and 256 key lengths. Message authentication code supported is hmac-sha2-256 and hmac-sha2-512.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

6.3.1.7 FCS_SSHC_EXT.1.7 TSS 1

| | |
|---|---|
| Objective | The evaluator shall check the TSS to ensure that it lists the supported key exchange algorithms, and that the list corresponds to the list in this component. |
| Evaluator Findings | The evaluator reviewed section 7.2 Cryptographic Support (FCS) in the Security Target to validate whether the TSS provides a comprehensive list of supported key exchange algorithms, ensuring that it aligns with the list specified for this component. After investigation, the evaluator discovered the following information in the TSS:<br><br>The TSS states that SSH session keys are established using the Diffie-Hellman (DH) key exchange. The specific scheme supported is diffie-hellman-group14-sha1. It utilizes 2048-bit asymmetric keys (DH Group 14) for the key exchange process. Additionally, SHA-1 is employed as the hashing method for the exchange hash, which generates the session keys hierarchy from the shared secret derived during the DH key establishment.<br><br>Based on these findings, the assurance activity is deemed satisfied, as the TSS accurately lists the supported key exchange algorithms and their corresponding parameters, aligning with the requirements specified for this component. |
| Verdict | Pass |

#### 6.3.1.8 FCS_SSHC_EXT.1.8 TSS 1

| | |
|---|---|
| Objective | The evaluator shall check that the TSS specifies the following:<br>a) Both thresholds are checked by the TOE.<br>b) Rekeying is performed upon reaching the threshold that is hit first. |
| Evaluator Findings | The evaluator examined the section titled 7.2 Cryptographic Support (FCS) in the Security Target to verify that the TSS specifies that both thresholds are checked by the TOE and rekeying is performed upon reaching the threshold that is hit first. Upon investigation, the evaluator found that the TSS states that<br><br>The SSH performs rekeying when 1 GB of SSH data has been sent, or after 1 hour of that session being open. A counter in the SSH code keeps track of the sent SSH data packets. If the data counter reaches 1 GB, or if the time counter reaches 1 hour, the TSF sends a 'Key Exchange Init' message to the peer to initiate a new key-exchange negotiation. If the new key-exchange fails to establish a new key for the session, the session is terminated by the TSF.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 6.3.2 FCS_SSHS_EXT.1

#### 6.3.2.1 FCS_SSHS_EXT.1.2 TSS 1 **[TD0631]**

| | |
|---|---|
| Objective | The evaluator shall check to ensure that the TSS contains a list of supported public key algorithms that are accepted for client authentication and that this list is consistent with signature verification algorithms selected in FCS_COP.1/SigGen (e.g., accepting EC keys requires corresponding Elliptic Curve Digital Signature algorithm claims).<br><br>The evaluator shall confirm that the TSS includes the description of how the TOE establishes a user identity when an SSH client presents a public key or X.509v3 certificate. For example, the TOE could verify that the SSH client's presented public key matches one that is stored within the SSH server's authorized_keys file.<br><br>If password-based authentication method has been selected in the FCS_SSHS_EXT.1.2, then the evaluator shall confirm its role in the authentication process is described in the TSS. |
| Evaluator Findings | The evaluator examined the section titled 7.2 Cryptographic Support (FCS) in the Security Target to verify that the TSS contains a description of the public key algorithms that are acceptable for use for authentication, that this list conforms to FCS_SSHS_EXT.1.5, and that if password-based authentication methods have been selected in the ST then these are also described. Upon investigation, the evaluator found that the TSS states that<br><br>TOE performs the role of SSH server in Trusted Path. SSH server in the TOE authenticates remote administrative user using public key or password. Following public key scheme is supported: rsa-sha2-256 that uses 2048-bit RSA key and SHA-256 digital signature or ecdsa-sha2-nistp384. Additional details of remote administrative user authentication are provided in FIA_UIA_EXT.1.<br><br>In password-based authentication, once a user initiates a connection to the administration interface, they are prompted to provide username and password credentials. After a user provides a username and password, the TOE invokes a PAM (Pluggable Authentication Modules) AAA plugin.<br><br>Based on these findings, this assurance activity is considered satisfied. |

| | |
|---|---|
| Verdict | Pass |

6.3.2.2 FCS_SSHS_EXT.1.3 TSS 1

| | |
|---|---|
| Objective | The evaluator shall check that the TSS describes how “large packets” in terms of RFC 4253 are detected and handled. |
| Evaluator Findings | The evaluator examined the section titled 7.2 Cryptographic Support (FCS) in the Security Target to verify that the TSS describes how “large packets” in terms of RFC 4253 are detected and handled. Upon investigation, the evaluator found that the TSS states that<br>In order to comply with RFC 4253, “large packets” received by the SSH client or server (packets greater than 262,144-bytes) in the SSH connection are dropped.<br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

6.3.2.3 FCS_SSHS_EXT.1.4 TSS 1

| | |
|---|---|
| Objective | The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics are specified, and the encryption algorithms supported are specified as well. The evaluator shall check the TSS to ensure that the encryption algorithms specified are identical to those listed for this component. |
| Evaluator Findings | The evaluator reviewed section 7.2 Cryptographic Support (FCS) in the Security Target to confirm whether the TSS specifies the supported encryption algorithms and optional characteristics. Upon investigation, it was found that the TSS states the following:<br>Encryption/decryption cipher supported: AES-CBC with key lengths of 128 and 256. This means that the TSS supports AES encryption in Cipher Block Chaining (CBC) mode with key sizes of 128 bits and 256 bits.<br>Based on these findings, the assurance activity is considered satisfied, as the TSS accurately specifies the supported encryption algorithms (AES-CBC with 128 and 256 key lengths). |
| Verdict | Pass |

6.3.2.4 FCS_SSHS_EXT.1.5 TSS 1 [TD0631]

| | |
|---|---|
| Objective | The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the SSH server’s host public key algorithms supported are specified and that they are identical to those listed for this component. |
| Evaluator Findings | The evaluator examined the section titled 7.2 Cryptographic Support (FCS) in the Security Target to verify that the TSS specifies the optional characteristics and the public key algorithms supported. Upon investigation, the evaluator found that the TSS states the following:<br>TOE performs the role of SSH server in Trusted Path. SSH server in the TOE authenticates remote administrative user using public key or password. Following public key scheme is supported: rsa-sha2-256 that uses 2048-bit RSA key and SHA-256 digital signature or ecdsa- |

| | |
|---|---|
| | sha2-nistp384. Additional details of remote administrative user authentication are provided in FIA_UIA_EXT.1.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

6.3.2.5 FCS_SSHS_EXT.1.5 TSS 2

| | |
|---|---|
| Objective | The evaluator shall confirm that the TSS includes the description of how the TOE establishes a user identity when an SSH client presents a public key or X.509v3 certificate. For example, the TOE could verify that the SSH client's presented public key matches one that is stored within the SSH server's authorized_keys file. |
| Evaluator Findings | The evaluator reviewed section 7.2 Cryptographic Support (FCS) in the Security Target to confirm whether the TSS specifies how the Target of Evaluation (TOE) establishes a user identity when an SSH client presents a public key or X.509v3 certificate. After investigation, the evaluator found the following information in the TSS:<br><br>If the TOE's SSH server authenticates the SSH client using the public key mechanism, the TSF ensures that the SSH server verifies the identity of the SSH client by utilizing the "/etc/ssh/known_hosts" file. This file associates each client host name with its corresponding public key, as defined in RFC 4251. The TSF achieves this by comparing the host key received from the SSH client during the SSH handshake with the keys configured in the known_hosts file. If a match is found, the connection establishment process proceeds. However, if no match is found, the session is terminated.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

6.3.2.6 FCS_SSHS_EXT.1.6 TSS 1

| | |
|---|---|
| Objective | The evaluator shall check the TSS to ensure that it lists the supported data integrity algorithms, and that the list corresponds to the list in this component. |
| Evaluator Findings | The evaluator reviewed section 7.2 Cryptographic Support (FCS) in the Security Target to validate whether the TSS specifies the supported data integrity algorithms and confirms that the list aligns with the requirements for this component. After thorough investigation, the evaluator found the following information in the TSS:<br>The message authentication code supported are hmac-sha2-256 and hmac-sha2-512.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

6.3.2.7 FCS_SSHS_EXT.1.7 TSS 1

| | |
|---|---|
| Objective | The evaluator shall check the TSS to ensure that it lists the supported key exchange algorithms, and that the list corresponds to the list in this component. |

| | |
|---|---|
| Evaluator Findings | The evaluator reviewed section 7.2 Cryptographic Support (FCS) in the Security Target to validate whether the TSS specifies the supported key exchange algorithms and confirms that the list aligns with the requirements for this component. After thorough investigation, the evaluator found the following information in the TSS:<br><br>• SSH session keys are established using DH (Diffie-Hellman) key exchange.<br>• The supported key exchange scheme is diffie-hellman-group14-sha1.<br>• The TSS supports 2048-bit asymmetric keys corresponding to DH Group 14.<br>• SHA-1 is used as the exchange hash algorithm.<br>• The exchange hash serves as the hashing method to generate a session keys hierarchy from the shared secret derived during the DH key establishment.<br><br>Based on these findings, the assurance activity is considered satisfied as the TSS accurately lists the supported key exchange algorithms, including the specific scheme (diffie-hellman-group14-sha1), the supported key sizes (2048-bit DH Group 14), and the use of SHA-1 as the exchange hash algorithm. The specified details align with the requirements for this component |
| Verdict | Pass |

6.3.2.8 FCS_SSHS_EXT.1.8 TSS 1

| | |
|---|---|
| Objective | The evaluator shall check that the TSS specifies the following:<br><br>a) Both thresholds are checked by the TOE.<br>b) Rekeying is performed upon reaching the threshold that is hit first. |
| Evaluator Findings | The evaluator examined the section titled 7.2 Cryptographic Support (FCS) in the Security Target to verify that the TSS specifies that both thresholds are checked, and that rekeying is performed upon reaching the threshold that is hit first. Upon investigation, the evaluator found that the TSS states that<br><br>The SSH performs rekeying when 1 GB of SSH data has been sent, or after 1 hour of that session being open. A counter in the SSH code keeps track of the sent SSH data packets. If the data counter reaches 1 GB, or if the time counter reaches 1 hour, the TSF sends a 'Key Exchange Init' message to the peer to initiate a new key-exchange negotiation. If the new key-exchange fails to establish a new key for the session, the session is terminated by the TSF.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

## 6.4 TSS Activities (TLS)

### 6.4.1 FCS_TLSS_EXT.1

6.4.1.1 FCS_TLSS_EXT.1.1 TSS 1

| | |
|---|---|
| Objective | 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 are identical to those listed for this component. |
| Evaluator Findings | The evaluator examined the section titled 7.2 Cryptographic Support (FCS) in the Security Target to verify that the TSS specifies the ciphersuites supported and that the ciphersuites |

| | |
|---|---|
| | specified are identical to those listed for this component. Upon investigation, the evaluator found that the TSS states that<br><br>The TOE allows for automated remote management of the TSF via the eAPI JSON-RPC (“eAPI”) interface. The communication channel is protected by TLS TLSv1.2 with mutual authentication. Any attempts to establish a session using any other TLS or SSL versions (SSL 1.0, SSL, 2.0, SSL 3.0, TLS 1.0, TLS 1.1) is denied by the TSF. Following TLS cipher suites are supported:<br>● TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246<br>● TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246<br>● TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246<br>● TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246<br>● TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288<br>● TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

6.4.1.2 FCS_TLSS_EXT.1.2 TSS 1

| | |
|---|---|
| Objective | The evaluator shall verify that the TSS contains a description of how the TOE technically prevents the use of old SSL and TLS versions. |
| Evaluator Findings | The evaluator reviewed section 7.2 Cryptographic Support (FCS) in the Security Target to confirm whether the TSS provides a description of the denial of old SSL and TLS versions. After conducting the investigation, the evaluator found the following information in the TSS:<br><br>The TOE allows for automated remote management of the TSF through the eAPI JSON-RPC ("eAPI") interface.<br><br>The communication channel utilized for the eAPI interface is protected by TLSv1.2 with mutual authentication, ensuring secure communication.<br><br>The TOE incorporates the nginx server to handle TLS connections. When configured to utilize the TLS version 1.2 option, the nginx server is explicitly set to exclusively accept TLS 1.2 protocols from the list of permitted protocols. As a result, any attempts to establish a session using other TLS or SSL versions, including SSL 1.0, SSL 2.0, SSL 3.0, TLS 1.0, and TLS 1.1, are categorically denied by the TSF.<br><br>Based on these findings, the assurance activity is considered satisfied as the TSS includes a description of the denial of old SSL and TLS versions. The TSF ensures that only TLSv1.2 is allowed for secure communication while rejecting attempts to use obsolete versions that may pose security risks. |
| Verdict | Pass |

6.4.1.3 FCS_TLSS_EXT.1.3 TSS 1 **[TD0635]**

| | |
|---|---|
| Objective | If using ECDHE and/or DHE ciphers, the evaluator shall verify that the TSS lists all EC Diffie-Hellman curves and/or Diffie-Hellman groups used in the key establishment by the TOE when acting as a TLS Server. For example, if the TOE supports |

| | |
|---|---|
| | TLS_DHE_RSA_WITH_AES_128_CBC_SHA cipher and Diffie-Hellman parameters with size 2048 bits, then list Diffie-Hellman Group 14. |
| Evaluator Findings | The evaluator examined the section titled 7.2 Cryptographic Support (FCS) in the Security Target to verify that, if using ECDHE or DHE ciphers, the TSS describes the key agreement parameters of the server Key Exchange message. Upon investigation, the evaluator found that the TSS states the following:<br><br>When the TSF is establishing a TLS session utilizing a cipher suite with DHE key establishment, the TSF supports ffdhe2048, ffdhe3072, and ffdhe4096 safe primes per RFC 7919. The TSF sends public key from the pair to the peer to facilitate pre-master secret establishment.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

6.4.1.4 FCS_TLSS_EXT.1.4 TSS 1

| | |
|---|---|
| Objective | The evaluator shall verify that the TSS describes if session resumption based on session IDs is supported (RFC 4346 and/or RFC 5246) and/or if session resumption based on session tickets is supported (RFC 5077). |
| Evaluator Findings | The evaluator examined the section titled 7.2 Cryptographic Support (FCS) in the Security Target. Upon investigation, the evaluator found that the TSS states that<br><br>The TLS server implements session resumption using session IDs according to RFC 5246 (TLS 1.2).<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

6.4.1.5 FCS_TLSS_EXT.1.4 TSS 2

| | |
|---|---|
| Objective | If session tickets are supported, the evaluator shall verify that the TSS describes that the session tickets are encrypted using symmetric algorithms consistent with FCS_COP.1/DataEncryption. The evaluator shall verify that the TSS identifies the key lengths and algorithms used to protect session tickets. |
| Evaluator Findings | Not applicable because the TOE does not support TLS session tickets. |
| Verdict | Pass |

6.4.1.6 FCS_TLSS_EXT.1.4 TSS 3

| | |
|---|---|
| Objective | If session tickets are supported, the evaluator shall verify that the TSS describes that session tickets adhere to the structural format provided in section 4 of RFC 5077 and if not, a justification shall be given of the actual session ticket format. |
| Evaluator Findings | Not applicable because the TOE does not support TLS session tickets. |
| Verdict | Pass |

#### 6.4.1.7 FCS_TLSS_EXT.1.4 TSS 4 **[TD0569]**

| | |
|---|---|
| Objective | If the TOE claims a (D)TLS server capable of session resumption (as a single context, or across multiple contexts), the evaluator verifies that the TSS describes how session resumption operates (i.e. what would trigger a full handshake, e.g. checking session status, checking Session ID, etc.). If multiple contexts are used the TSS describes how session resumption is coordinated across those contexts. In case session establishment and session resumption are always using a separate context, the TSS shall describe how the contexts interact with respect to session resumption (in particular regarding the session ID). It is acceptable for sessions established in one context to be resumable in another context. |
| Evaluator Findings | The evaluator examined the section titled 7.2 Cryptographic Support (FCS) in the Security Target to verify, if the TOE claims a (D)TLS server capable of session resumption, that the TSS describes how session resumption operates; if multiple contexts are used, the TSS describes how session resumption is coordinated across those contexts; and, in case session establishment and session resumption are always using a separate context, the TSS shall describe how the contexts interact. Upon investigation, the evaluator found that the TSS states that The TLS server implements session resumption using session IDs according to RFC 5246 (TLS 1.2) without any context.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 6.4.2 FCS_TLSS_EXT.2

#### 6.4.2.1 FCS_TLSS_EXT.2.1 and FCS_TLSS_EXT.2.2 TSS 1.

| | |
|---|---|
| Objective | The evaluator shall ensure that the TSS description required per FIA_X509_EXT.2.1 includes the use of client-side certificates for TLS mutual authentication. |
| Evaluator Findings | The evaluator examined the section titled 7.2 Cryptographic Support (FCS)in the Security Target to verify that the TSS description required per FIA_X509_EXT.2.1 includes the use of client-side certificates for TLS mutual authentication. Upon investigation, the evaluator found that the TSS states that<br><br>The communication channel is protected by TLS TLSv1.2 with mutual authentication.<br><br>The TLS server supports authentication of the eAPI TLS client. The Security Administrator configures TLS server with trusted CA certificate used to validate the eAPI TLS client certificate. The trusted CA certificate is then associated to a Security Administrative user account. This particular administrative account is only to be used by the eAPI. This is to ensure that there is no ambiguity when viewing the audit records as to whether a human user's action or the eAPI's action generated the audit record. When eAPI TLS client attempts to establish a session with the TSF, the TSF responds to the client by sending a Certificate_Request message immediately after the ServerKeyExchange message is sent during the TLS handshake. The client must send a Client_Certificate message containing an RSA 2048-bit public-key in the x.509v3 certificate to authenticate the client to the TSF. The TSF validates the client certificate according to FIA_X509_EXT.1.1, checks that it is signed by the trusted CA, checks the local CRL for the revocation status of the client certificate. If any of these validity checks fail, the session is terminated.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

6.4.2.2 FCS_TLSS_EXT.2.1 and FCS_TLSS_EXT.2.2 TSS 2

| | |
|---|---|
| Objective | The evaluator shall verify the TSS describes how the TSF uses certificates to authenticate the TLS client. The evaluator shall verify the TSS describes if the TSF supports any fallback authentication functions (e.g., username/password, challenge response) the TSF uses to authenticate TLS clients that do not present a certificate. If fallback authentication functions are supported, the evaluator shall verify the TSS describes whether the fallback authentication functions can be disabled. |
| Evaluator Findings | The evaluator examined the section titled 7.2 Cryptographic Support (FCS) in the Security Target to verify that the TSS describes how the TSF uses certificates to authenticate the TLS client. The evaluator verifies the TSS describes if the TSF supports any fallback authentication functions (e.g., username/password, challenge response) the TSF uses to authenticate TLS clients that do not present a certificate. If fallback authentication functions are supported and verify the TSS describes whether the fallback authentication functions can be disabled. Upon investigation, the evaluator found that the TSS states the following:<br><br>The TOE provides support for password-based authentication as a fallback option. The availability of fallback authentication depends on the configuration of the "secret" parameter in the "username" command. If the "secret" parameter is configured with a password, fallback authentication is enabled. In this case, the client can authenticate by providing their password instead of a client certificate. However, if the "secret" parameter is configured with the "*" (asterisk) character, the fallback authentication is disabled. In this scenario, the client will not be able to authenticate using their password.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

6.4.2.3 FCS_TLSS_EXT.2.3 TSS 1

| | |
|---|---|
| Objective | The evaluator shall verify that the TSS describes which types of identifiers are supported during client authentication (e.g. Fully Qualified Domain Name (FQDN)). If FQDNs are supported, the evaluator shall verify that the TSS describes that corresponding identifiers are matched according to RFC6125. For all other types of identifiers, the evaluator shall verify that the TSS describes how these identifiers are parsed from the certificate, what the expected identifiers are and how the parsed identifiers from the certificate are matched against the expected identifiers. |
| Evaluator Findings | The evaluator examined the section titled 7.2 Cryptographic Support (FCS) in the Security Target. Upon investigation, the evaluator found that the TSS states that<br><br>If the client certificate validity checks passes, the TSF checks to see if the CN value matches the username of the account specifically configured for the eAPI client. If no match is found, TSF will terminate the attempted session establishment. If a match is found, TSF allows the authentication process to complete and the session to successfully establish. The TSF does not process SAN value in the client certificate.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

## 6.5 TSS Activities (Identification and Authentication)

### 6.5.1 FIA_AFL.1

#### 6.5.1.1 FIA_AFL.1 TSS 1

| | |
|---|---|
| Objective | The evaluator shall examine the TSS to determine that it contains a description, for each supported method for remote administrative actions, of how successive unsuccessful authentication attempts are detected and tracked. The TSS shall also describe the method by which the remote administrator is prevented from successfully logging on to the TOE, and the actions necessary to restore this ability. |
| Evaluator Findings | The evaluator examined the section titled 7.3 Cryptographic Support (FCS) in the Security Target to verify that the TSS contains a description, for each supported method for remote administrative actions, of how successive unsuccessful authentication attempts are detected and tracked; the method by which the remote administrator is prevented from successfully logging on to the TOE; and the actions necessary to restore this ability. Upon investigation, the evaluator found that the TSS states that<br><br>Consecutive authentication failures result into temporary account lockout for remote administrative user. The threshold number of failures between 1 and 255 and subsequent lockout period are configured by Security Administrator when initializing the TOE. The RS-232/VT-100 local administrative interface is never locked out.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

#### 6.5.1.2 FIA_AFL.1 TSS 2

| | |
|---|---|
| Objective | The evaluator shall examine the TSS to confirm that the TOE ensures that authentication failures by remote administrators cannot lead to a situation where no administrator access is available, either permanently or temporarily (e.g., by providing local logon which is not subject to blocking). |
| Evaluator Findings | The evaluator examined the section titled 7.3 Identification and Authentication (FIA) in the Security Target to verify that the TSS ensures that authentication failures by remote administrators cannot lead to a situation where no administrator access is available. Upon investigation, the evaluator found that the TSS states that<br><br>Consecutive authentication failures result into temporary account lockout for remote administrative user. The threshold number of failures between 1 and 255 and subsequent lockout period are configured by Security Administrator when initializing the TOE. The RS-232/VT-100 local administrative interface is never locked out.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 6.5.2 FIA_PMG_EXT.1

#### 6.5.2.1 FIA_PMG_EXT.1.1 TSS 1

| | |
|---|---|
| Objective | The evaluator shall examine the TSS to determine that it contains the lists of the supported special character(s) and minimum and maximum number of charters supported for administrator passwords. |
| Evaluator Findings | The evaluator examined the section titled 7.3 Identification and Authentication (FIA)in the Security Target to verify that the TSS contains the lists of the supported special character(s) and minimum and maximum number of charters supported for administrator passwords. Upon investigation, the evaluator found that the TSS states that<br><br>The Security Administrator passwords are able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(”, “)”. Minimum length of the password is configurable by the Security Administrator between 1 and 32. It is recommended to configure minimum length as at least 8.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 6.5.3 FIA_UIA_EXT.1

#### 6.5.3.1 FIA_UIA_EXT.1 TSS 1

| | |
|---|---|
| Objective | The evaluator shall examine the TSS to determine that it describes the logon process for each logon method (local, remote (HTTPS, SSH, etc.)) supported for the product. This description shall contain information pertaining to the credentials allowed/used, any protocol transactions that take place, and what constitutes a “successful logon”. |
| Evaluator Findings | The evaluator examined the section titled 7.3 Identification and Authentication (FIA)in the Security Target to verify that the TSS describes the logon process for each logon method supported for the product. Upon investigation, the evaluator found that the TSS states that<br><br>The TSF provides a local administrative CLI interface over RS-232/VT-100 that supports password-based authentication. It also provides remote administrative CLI interface over SSH that supports password-based and public key-based authentication.<br><br>In password-based authentication, once a user initiates a connection to the administration interface they are prompted to provide username and password credentials. After a user provides a username and password, the TOE invokes a PAM (Pluggable Authentication Modules) AAA plugin. This plugin is configured to use the RBAC (Role Based Access Control) module. The AAA plugin passes the authentication credentials to the RBAC module. The RBAC module checks the credentials against its database and then responds with a SUCCESS or DENIED message. Based on the response from the RBAC module, the AAA plugin then returns a SUCCESS or DENIED message to the requesting program. If the requesting program receives a DENIED message, it prints an error message to the user and denies the login attempt. If the requesting program receives a SUCCESS message, it makes an EXEC authorization request to the RBAC module, which responds with the additional permissions for the CLI. At this point, authentication is successful, and the user is presented with the CLI.<br><br>When RSA public key authentication is used with a remote SSH session, the SSH daemon performs the initial authentication verification locally by comparing public key supplied by the |

| | |
|---|---|
| | client with /home/<account>/.ssh/authorized_keys. Once the public key matches, the daemon performs an EXEC authorization request to the RBAC module as detailed above.<br><br>The TSF also provides "eAPI" interface over TLS for remote automated configuration. The details of eAPI authentication process are provided above in FCS_TLSS_EXT.2. After the authentication is successful, EXEC authorization request is made to the RBAC module.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

#### 6.5.3.2 FIA_UIA_EXT.1 TSS 2

| | |
|---|---|
| Objective | The evaluator shall examine the TSS to determine that it describes which actions are allowed before user identification and authentication. The description shall cover authentication and identification for local and remote TOE administration. |
| Evaluator Findings | The evaluator examined the section titled 7.3 Identification and Authentication (FIA)in the Security Target to verify that the TSS describes which actions are allowed before user identification and authentication. Upon investigation, the evaluator found that the TSS states that<br><br>The TSF displays a warning banner (in accordance with FTA_TAB.1) on CLI prior to requiring identification and authentication. This banner is not required to be, nor is it, presented to the eAPI JSON-RPC client prior to it authenticating to the TSF.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 6.5.4 FIA_X509_EXT.1/Rev

#### 6.5.4.1 FIA_X509_EXT.1/Rev TSS 1

| | |
|---|---|
| Objective | The evaluator shall ensure the TSS describes where the check of validity of the certificates takes place, and that the TSS identifies any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied). It is expected that revocation checking is performed when a certificate is used in an authentication step and when performing trusted updates (if selected). It is not necessary to verify the revocation status of X.509 certificates during power-up self-tests (if the option for using X.509 certificates for self-testing is selected). |
| Evaluator Findings | The evaluator examined the section titled 7.3 Identification and Authentication (FIA)in the Security Target to verify that the TSS describes where the check of validity of the certificates takes place, and that the TSS identifies any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e., where the ST is therefore claiming that they are trivially satisfied). Upon investigation, the evaluator found that the TSS states that<br><br>Following conditions are checked at the time of import and the import is rejected if any of the following conditions do not check:<br>● That the entire chain of certificates is imported. That is, the leaf TLS server certificate, any intermediate certificates leading from the leaf up to the root and the root certificate are imported. |

| | |
|---|---|
| | • That the current date and time lies between the “Valid from” and “Valid to” for each certificate.<br>• That the basicConstraints extension is included with CA flag is set to TRUE for all CA certificates in the chain<br>• That the extendedKeyUsage field in the leaf certificate has the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1)<br>• That the digital signatures are correct in all certificates<br>• That none of the certificates from the leaf up to the root is revoked.<br><br>Also the evaluator found that the Section 7.3 in the ST states that the TOE does not provide support for code signing and OCSP signing attributes in the extendedKeyUsage field of the leaf certificate when presented by the e-API client or when included in an x509 certificate imported into its trusted store.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

6.5.4.2 FIA_X509_EXT.1/Rev TSS 2

| | |
|---|---|
| Objective | The TSS shall describe when revocation checking is performed and on what certificates. If the revocation checking during authentication is handled differently depending on whether a full certificate chain or only a leaf certificate is being presented, any differences must be summarized in the TSS section and explained in the Guidance. |
| Evaluator Findings | The evaluator examined the section titled 7.3 Identification and Authentication (FIA)in the Security Target to verify that the TSS describes when revocation checking is performed and on what certificates. Upon investigation, the evaluator found that the TSS states that<br><br>In order to facilitate revocation checking, Security Administrator specifies Certificate Distribution Points (CDPs) during initial configuration of the TOE. Security Administrator is required to specify CDPs for the CRLs published by the trust anchor and every CA certificate between the trust anchor and the leaf certificate of the eAPI client. The TOE downloads CRLs from the specified CDPs every 24 hours and stores the most recently fetched CRLs locally. Digital signatures on downloaded CRLs are validated and in case of failure of signature verification, CRL is not added to the local copy. The local copies of the CRLs are used for certificate revocation checking. At the time of revocation checking, the TOE ensures that the current time lies within the validity period of the CRL, that is between the effective date and the next update date mentioned in the CRL. The certification revocation checking can fail either because the certificate is revoked as per the CRL or because the recent CRL for the CA that issued the certificate is not present in the local copy to perform the revocation checking.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

## 6.5.5 FIA_X509_EXT.2

6.5.5.1 FIA_X509_EXT.2 TSS 1

| | |
|---|---|
| Objective | The evaluator shall check the TSS to ensure that it describes how the TOE chooses which certificates to use. |

| | |
|---|---|
| Evaluator Findings | The evaluator examined the section titled 7.3 Identification and Authentication (FIA) in the Security Target to verify that the TSS describes how the TOE chooses which certificates to use. Upon investigation, the evaluator found that the TSS states that<br><br>The above certificate chain is presented to the eAPI client at the beginning of TLS connection. This facilitates the eAPI client to validate identity of the server.<br>At the time of establishing TLS connection, the eAPI client presents its x.509v3 certificate to the TLS server in the TOE. This certificate is used by the TOE to authenticate the eAPI client.<br>The TOE performs following checks on the certificate presented by the eAPI client:<br>● That the certificate chain presented by the eAPI client can be traced to the CA certificate that is lowest in the hierarchy of certificates imported into the TOE as described above. That is, this lowest CA certificate acts as the trust anchor. Note that the trust anchor can be an intermediate CA certificate or the root CA certificate.<br>● That the current date and time lies between the "Valid from" and "Valid to" for each certificate from the leaf certificate in the chain presented by eAPI client upto and including the trust anchor.<br>● That the basicConstraints extension is included with CA flag is set to TRUE for all CA certificates in the chain.<br>● That the extendedKeyUsage field in the leaf certificate in the chain presented by eAPI client has the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2).<br>● That the digital signatures are correct in all certificates.<br>That none of the certificates from the leaf up to the trust anchor is revoked. It is not necessary to check revocation status of the trust anchor and other CA certificates upstream of the trust anchor.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

6.5.5.2 FIA_X509_EXT.2 TSS 2

| | |
|---|---|
| Objective | The evaluator shall examine the TSS to confirm that it describes the behaviour 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 guidance documentation contains instructions on how this configuration action is performed. |
| Evaluator Findings | The evaluator examined the section titled 7.3 Identification and Authentication (FIA)in the Security Target to verify that the TSS describes the behaviour of the TOE when a connection cannot be established during the validity check of a certificate used in establishing a trusted channel. Upon investigation, the evaluator found that the TSS states that<br><br>Digital signatures on downloaded CRLs are validated and in case of failure of signature verification, CRL is not added to the local copy. The local copies of the CRLs are used for certificate revocation checking. At the time of revocation checking, the TOE ensures that the current time lies within the validity period of the CRL, that is between the effective date and the next update date mentioned in the CRL. The certification revocation checking can fail either because the certificate is revoked as per the CRL or because the recent CRL for the CA that issued the certificate is not present in the local copy to perform the revocation checking.<br><br>Based on these findings, this assurance activity is considered satisfied. |

| | |
|---|---|
| Verdict | Pass |

### 6.5.6 FIA_X509_EXT.3

#### 6.5.6.1 FIA_X509_EXT.3 TSS 1

| | |
|---|---|
| Objective | If the ST author selects "device-specific information", the evaluator shall verify that the TSS contains a description of the device-specific fields used in certificate requests. |
| Evaluator Findings | The ST does not claim “device-specific information” hence this assurance activity is considered not applicable to the TOE. |
| Verdict | N/A |

## 6.6 TSS Activities (Security Management)

#### 6.6.1.1 FMT_MOF.1/ Functions TSS 1

| | |
|---|---|
| Objective | For distributed TOEs it is required to verify the TSS to ensure that it describes how every function related to security management is realized for every TOE component and shared between different TOE components. The evaluator shall confirm that all relevant aspects of each TOE component are covered by the FMT SFRs |
| Evaluator Findings | Not applicable because the TOE is not a distributed TOE. |
| Verdict | N/A |

#### 6.6.1.2 FMT_MOF.1/Functions TSS 2

| | |
|---|---|
| Objective | For non-distributed TOEs, the evaluator shall ensure the TSS for each administrative function identified the TSS details how the Security Administrator determines or modifies the behaviour of (whichever is supported by the TOE) transmitting audit data to an external IT entity, handling of audit data, audit functionality when Local Audit Storage Space is full (whichever is supported by the TOE). |
| Evaluator Findings | The evaluator examined the section titled 7.1 Security Audit (FAU) in the Security Target to verify that the TSS identifies each administrative function identified the TSS details how the Security Administrator determines or modifies the behaviour of (whichever is supported by the TOE) transmitting audit data to an external IT entity, handling of audit data, audit functionality when Local Audit Storage Space is full (whichever is supported by the TOE). Upon investigation, the evaluator found that the TSS states that<br><br>Audit logs generated by the TSF are stored locally in the persistent Flash memory. The maximum size for the file storing the local audit logs is configurable. When the file exceeds its size limit, it is trimmed to remove the oldest audit logs until the size drops below the configured threshold. Locally stored audit records are protected from unauthorized viewing, modification and deletion by the file system’s read/write permissions and a restrictive CLI which only allows identified, authorized and authenticated administrative users read/write access. The Security Administrative user can delete the locally stored audit records. Modification of the audit records other than deleting them is not supported.<br><br>The logs can also be sent to configured remote audit server in syslog format as soon as they are generated. To protect the audit records in transit from the TOE to the remote audit server in the Operational Environment, the TOE establishes a Trusted Channel between itself and |

| | |
|---|---|
| | the external audit server using the SSHv2 protocol. The Trusted Channel is created when the TOE establishes an SSH session between itself and the remote audit server with TCP port forwarding enabled. After the SSH session is established, the TOE is configured by the Security Administrative user to forward all messages received by the syslog process to the listening TCP port created by the SSH connection. This ensures that all audit traffic is encapsulated and hence protected by the SSH connection.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 6.6.2 FMT_MTD.1/CoreData

#### 6.6.2.1 FMT_MTD.1/CoreData TSS 1

| | |
|---|---|
| Objective | The evaluator shall examine the TSS to determine that, for each administrative function identified in the guidance documentation; those that are accessible through an interface prior to administrator log-in are identified. For each of these functions, the evaluator shall also confirm that the TSS details how the ability to manipulate the TSF data through these interfaces is disallowed for non-administrative users. |
| Evaluator Findings | The evaluator examined the section titled 7.4 Security Management (FMT) in the Security Target to verify that the TSS identifies administrative functions that are accessible through an interface prior to administrator log-in. Upon investigation, the evaluator found that the TSS states that<br><br>The TSF maintains the 'Security Administrator' role and allows that role to be associated to users of the TOE. The Security Administrator role is enforced via the permission features of the base Linux kernel of the EOS operating system. Users are associated with credentials for identification and role for authorization to the TOE.<br><br>The local console and remote management interfaces allow the Security Administrator to perform the following TSF management functions:<br>● Administer the TOE locally and remotely<br>● Create the TOE access banner<br>● Set the session inactivity timeout values<br>● Verify and manually install firmware updates (verification using published hash)<br>● Configure failed login threshold and lockout period<br>● Generate, import, delete and configure cryptographic keys required by SSH and TLS<br>● Specify ciphersuites for SSH and TLS<br>● Configure syslog forwarding<br>● Set system time<br>● Import x.509v3 certificates in trust store<br><br>The evaluator examined the section titled 7.4 Security Management (FMT) in the Security Target to verify that the TSS details how the ability to manipulate the TSF data through these interfaces is disallowed for non-administrative users. Upon investigation, the evaluator found that the TSS states that<br><br>In addition, users' permissions are assigned and enforced by the base Linux kernel filesystem of EOS via read/write/execute permissions and group policies that ensure that only Security Administrative users can manage the TSF data. The TSF restricts the ability to manage (i.e. |

| | |
|---|---|
| | create, view, initialize, modify/append, delete/clear, and change the default setting) of the TSF data to only identified, authenticated and authorized Security Administrators.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

6.6.2.2 FMT_MTD.1/CoreData TSS 2

| | |
|---|---|
| Objective | If the TOE supports handling of X.509v3 certificates and implements a trust store, the evaluator shall examine the TSS to determine that it contains sufficient information to describe how the ability to manage the TOE's trust store is restricted. |
| Evaluator Findings | The evaluator examined the section titled 7.4 Security Management (FMT)in the Security Target to verify that, if the TOE supports handling of X.509v3 certificates and implements a trust store, the TSS contains sufficient information to describe how the ability to manage the TOE's trust store is restricted. Upon investigation, the evaluator found that the TSS states that<br><br>users' permissions are assigned and enforced by the base Linux kernel filesystem of EOS via read/write/execute permissions and group policies that ensure that only Security Administrative users can manage the TSF data. The TSF restricts the ability to manage (i.e. create, view, initialize, modify/append, delete/clear, and change the default setting) of the TSF data to only identified, authenticated and authorized Security Administrators.<br><br>The local console and remote management interfaces allow the Security Administrator to perform the following TSF management functions:<br>● Administer the TOE locally and remotely<br>● Create the TOE access banner<br>● Set the session inactivity timeout values<br>● Verify and manually install firmware updates (verification using published hash)<br>● Configure failed login threshold and lockout period<br>● Generate, import, delete and configure cryptographic keys required by SSH and TLS<br>● Specify ciphersuites for SSH and TLS<br>● Configure syslog forwarding<br>● Set system time<br>● Import x.509v3 certificates in trust store<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

6.6.2.3 FMT_MTD.1/CryptoKeys TSS 2

| | |
|---|---|
| Objective | For non-distributed TOEs, the evaluator shall ensure the TSS lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed. |
| Evaluator Findings | The evaluator examined the section titled 7.2 Cryptographic Support (FCS) and 7.4 Security Management (FMT) in the Security Target to verify that the TSS lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed. Upon investigation, the evaluator found that the TSS states that<br><br>**Table 18: CSPs** |

| CSP | Purpose | Generation | Clearing Method | When cleared | Storage Location |
|---|---|---|---|---|---|
| TLS Server: RSA Private Key | "eAPI" server authentication | Generated internally when TLS server is first started or when new key pair is requested by Security Administrator | Single direct overwrite consisting of zeroes | When replaced by the Security Administrator | Flash |
| TLS Server: DH Private Key | Establish session keys for TLS session | Generated internally at the start of TLS session | Single direct overwrite consisting of zeroes | When TLS session keys are derived | RAM |
| TLS Server: Session Keys | Message authentication and encryption in TLS session | Generated internally at the start of TLS session | Single direct overwrite consisting of zeroes | When TLS session terminates | RAM |
| SSH Server: RSA Private Key | SSH host authentication for remote administrative session | Generated internally when SSH service on the TOE is first started or when new key pair is requested by Security Administrator. | Single direct overwrite consisting of zeroes | When replaced by the Security Administrator | Flash |
| SSH Server: DH Private Key | Establish session keys for SSH session | Generated internally at the start of SSH session | Single direct overwrite consisting of zeroes | When SSH session keys are derived | RAM |
| SSH Server: Session Keys | Message authentication and encryption in SSH session | Generated internally at the start of SSH session | Single direct overwrite consisting of zeroes | When SSH session terminates | RAM |
| SSH Client: RSA Private Key | SSH client authentication to audit server | Generated internally when SSH service on the TOE is first started or | Single direct overwrite consisting of zeroes | When replaced by the Security Administrator | Flash |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | when new key pair is requested by Security Administrator. | | | |
| | SSH Client: ECDSA Private Key | SSH client authentication to audit server | Generated internally when SSH service on the TOE is first started or when new key pair is requested by Security Administrator. | Single direct overwrite consisting of zeroes | When replaced by the Security Administrator | Flash |
| | SSH Client: DH Private Key | Establish session keys for SSH session | Generated internally at the start of SSH session | Single direct overwrite consisting of zeroes | When SSH session keys are derived | RAM |
| | SSH Client: Session Keys | Message authentication and encryption in SSH session | Generated internally at the start of SSH session | Single direct overwrite consisting of zeroes | When SSH session terminates | RAM |

The TSF maintains the 'Security Administrator' role and allows that role to be associated to users of the TOE. The Security Administrator role is enforced via the permission features of the base Linux kernel of the EOS operating system. Users are associated with credentials for identification and role for authorization to the TOE. In addition, users' permissions are assigned and enforced by the base Linux kernel filesystem of EOS via read/write/execute permissions and group policies that ensure that only Security Administrative users can manage the TSF data. The TSF restricts the ability to manage (i.e. create, view, initialize, modify/append, delete/clear, and change the default setting) of the TSF data to only identified, authenticated and authorized Security Administrators.

The local console and remote management interfaces allow the Security Administrator to perform the following TSF management functions:

- Administer the TOE locally and remotely
- Create the TOE access banner
- Set the session inactivity timeout values
- Verify and manually install firmware updates (verification using published hash)
- Configure failed login threshold and lockout period
- Generate, import, delete and configure cryptographic keys required by SSH and TLS
- Specify ciphersuites for SSH and TLS
- Configure syslog forwarding
- Set system time
- Import x.509v3 certificates in trust store

| | |
|---|---|
| | Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 6.6.3 FMT_SMF.1

#### 6.6.3.1 FMT_SMF.1 TSS 1

| | |
|---|---|
| Objective | The evaluator shall confirm that the TSS details which security management functions are available through which interface(s) (local administration interface, remote administration interface).<br><br>The evaluator shall examine the TSS Documentation to verify they both describe the local administrative interface. |
| Evaluator Findings | The evaluator examined the section titled 7.7 Trust Path/Channels (FTP) in the TSS to verify that it details which security management functions are available through which interface(s). Upon investigation, the evaluator found that the AGD states that<br><br>Trusted Path connection protects communication between TSF and human user (Security Administrator) performing management of the TSF. It is protected by SSH. TOE acts as SSH Server in the Trusted Path connection<br><br>The evaluator examined the section titled 7.3 Identification and Authentication (FIA) in the TSS to verify that it describes the local administrative interface. Upon investigation, the evaluator found that the AGD states that<br><br>The TSF provides a local administrative CLI interface over RS-232/VT-100 that supports password-based authentication. It also provides remote administrative CLI interface over SSH that supports password-based and public key-based authentication.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 6.6.4 FMT_SMR.2

#### 6.6.4.1 FMT_SMR.2 TSS 1

| | |
|---|---|
| Objective | The evaluator shall examine the TSS to determine that it details the TOE supported roles and any restrictions of the roles involving administration of the TOE. |
| Evaluator Findings | The evaluator examined the section titled 7.4 Security Management (FMT)in the TSS and the section titled 3.11 Named User Roles in the AGD to verify that the TOE supported roles and any restrictions of the roles involving administration of the TOE. Upon investigation, the evaluator found that the TSS and AGD state that<br><br>The TSF maintains the 'Security Administrator' role and allows that role to be associated to users of the TOE. The Security Administrator role is enforced via the permission features of the base Linux kernel of the EOS operating system. Users are associated with credentials for identification and role for authorization to the TOE. In addition, users' permissions are assigned and enforced by the base Linux kernel filesystem of EOS via read/write/execute permissions and group policies that ensure that only Security Administrative users can manage the TSF data. The TSF restricts the ability to manage (i.e. create, view, initialize, |

| | |
|---|---|
| | modify/append, delete/clear, and change the default setting) of the TSF data to only identified, authenticated and authorized Security Administrators.<br>The local console and remote management interfaces allow the Security Administrator to perform the following TSF management functions:<br>● Administer the TOE locally and remotely<br>● Create the TOE access banner<br>● Set the session inactivity timeout values<br>● Verify and manually install firmware updates (verification using published hash)<br>● Configure failed login threshold and lockout period<br>● Generate, import, delete and configure cryptographic keys required by SSH and TLS<br>● Specify ciphersuites for SSH and TLS<br>● Configure syslog forwarding<br>● Set system time<br>● Import x.509v3 certificates in trust store<br><br>The AGD supports the above claim of the TSS with the necessary instructions to enforce a role-based structure to manage the TSF data.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

## 6.7 TSS Activities (Protection of the TSF)

### 6.7.1 FPT_APW_EXT.1

#### 6.7.1.1 FPT_APW_EXT.1 TSS 1

| | |
|---|---|
| Objective | The evaluator shall examine the TSS to determine that it details all authentication data that are subject to this requirement, and the method used to obscure the plaintext password data when stored. The TSS shall also detail passwords are stored in such a way that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. |
| Evaluator Findings | The evaluator examined the section titled 7.5 Protection of the TSF (FPT) in the Security Target to verify that the TSS details all authentication data that are subject to this requirement and the method used to obscure the plaintext password data when stored. Upon investigation, the evaluator found that the TSS states that<br><br>The TSF does not store passwords in plaintext. The TSF uses SHA-512 hash (with a salt) protection to ensure that any users' password is not stored in plaintext.<br><br>The evaluator also examined the section titled 7.5 Protection of the TSF (FPT) in the Security Target to verify that the TSS details that passwords are stored in such a way that they are unable to be viewed through an interface designed specifically for that purpose. Upon investigation, the evaluator found that the TSS states that<br><br>When a user authenticates to the TSF (local or remote), the system generates a hash of the entered password and compares it against the stored hash value of the password associated to the username provided to ensure that the plaintext password is not disclosed.<br><br>Based on these findings, this assurance activity is considered satisfied. |

| Verdict | Pass |
|---|---|

### 6.7.2 FPT_SKP_EXT.1

#### 6.7.2.1 FPT_SKP_EXT.1 TSS 1

| Objective | The evaluator shall examine the TSS to determine that it details how any preshared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. If these values are not stored in plaintext, the TSS shall describe how they are protected/obscured. |
|---|---|

**Evaluator Findings**

The evaluator examined the section titled 7.2 Cryptographic Support (FCS) in the Security Target to verify that the TSS details how any pre-shared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose. Upon investigation, the evaluator found that the TSS states that

Administrative interface does not provide a documented command for any user to view any of the private or session keys. There are no pre-shared keys.

**Table 18: CSPs**

| CSP | Purpose | Generation | Clearing Method | When cleared | Storage Location |
|---|---|---|---|---|---|
| TLS Server: RSA Private Key | "eAPI" server authentication | Generated internally when TLS server is first started or when new key pair is requested by Security Administrator | Single direct overwrite consisting of zeroes | When replaced by the Security Administrator | Flash |
| TLS Server: DH Private Key | Establish session keys for TLS session | Generated internally at the start of TLS session | Single direct overwrite consisting of zeroes | When TLS session keys are derived | RAM |
| TLS Server: Session Keys | Message authentication and encryption in TLS session | Generated internally at the start of TLS session | Single direct overwrite consisting of zeroes | When TLS session terminates | RAM |
| SSH Server: RSA Private Key | SSH host authentication for remote administrative session | Generated internally when SSH service on the TOE is first started or when new key pair is requested by | Single direct overwrite consisting of zeroes | When replaced by the Security Administrator | Flash |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | Security Administrator. | | | |
| | SSH Server: DH Private Key | Establish session keys for SSH session | Generated internally at the start of SSH session | Single direct overwrite consisting of zeroes | When SSH session keys are derived | RAM |
| | SSH Server: Session Keys | Message authentication and encryption in SSH session | Generated internally at the start of SSH session | Single direct overwrite consisting of zeroes | When SSH session terminates | RAM |
| | SSH Client: RSA Private Key | SSH client authentication to audit server | Generated internally when SSH service on the TOE is first started or when new key pair is requested by Security Administrator. | Single direct overwrite consisting of zeroes | When replaced by the Security Administrator | Flash |
| | SSH Client: ECDSA Private Key | SSH client authentication to audit server | Generated internally when SSH service on the TOE is first started or when new key pair is requested by Security Administrator. | Single direct overwrite consisting of zeroes | When replaced by the Security Administrator | Flash |
| | SSH Client: DH Private Key | Establish session keys for SSH session | Generated internally at the start of SSH session | Single direct overwrite consisting of zeroes | When SSH session keys are derived | RAM |
| | SSH Client: Session Keys | Message authentication and encryption in SSH session | Generated internally at the start of SSH session | Single direct overwrite consisting of zeroes | When SSH session terminates | RAM |
| | Based on these findings, this assurance activity is considered satisfied. | | | | | |
| Verdict | Pass | | | | | |

### 6.7.3 FPT_STM_EXT.1

#### 6.7.3.1 FPT_STM_EXT.1 TSS 1 [TD0632]

| | |
|---|---|
| Objective | a) The evaluator shall examine the TSS to ensure that it lists each security function that makes use of time, and that it provides a description of how the time is maintained and considered reliable in the context of each of the time related functions.<br><br>b) If “obtain time from the underlying virtualization system” is selected, the evaluator shall examine the TSS to ensure that it identifies the VS interface the TOE uses to obtain time. If there is a delay between updates to the time on the VS and updating the time on the TOE, the TSS shall identify the maximum possible delay. |
| Evaluator Findings | a) The evaluator examined the subsection FPT_STM_EXT.1 in section titled 7.5 protection of the TSF (FPT) in the Security Target to verify that the TSS lists each security function that makes use of time and provides a description of how the time is maintained and considered reliable in the context of each of the time related functions. Upon investigation, the evaluator found that the TSS states that the initial system time is manually configured by the Security Administrator using the CLI interface. After that, two components are responsible to keep the system time, namely, the Real Time Clock (RTC) and the “system clock”.in addition, it states that the following TSFs make use of the system time:<br>• Time stamping of TSF generated audit records<br>• Refetching of the new CRL at the end of validity period of the previous CRL and to check that the time when the certificate is presented to the TOE lies within the validity period of the CRL<br>• Time keeping of interactive sessions between the Security Administrator and the TSF (local console, remote SSH console interfaces) for the purpose of TSF termination of the interactive sessions due to inactivity.<br><br>b) The toe does not obtain time from the underlying virtualization system.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 6.7.4 FPT_TST_EXT.1.1

#### 6.7.4.1 FPT_TST_EXT.1.1 TSS 1

| | |
|---|---|
| Objective | The evaluator shall examine the TSS to ensure that it details the self-tests that are run by the TSF; 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. |
| Evaluator Findings | The evaluator examined the section titled 7.5 Protection of the TSF (FPT) in the Security Target to verify that the TSS makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly. Upon investigation, the evaluator found that the TSS states that: “These four distinct tests provide ample evidence to conclude that the TSF operates correctly. They comprehensively |

| | |
|---|---|
| | assess all the cryptographic functions performed by the TSF through cryptographic self-tests, pairwise consistency tests, and CRNGT (Cryptographic Random Number Generator Tests). Additionally, the software integrity test safeguards against any modifications to the tests themselves. By continuously covering all the cryptographic functions within the TSF and ensuring their integrity, these tests effectively fulfill the requirements for evaluating the TSF's correct operation. Therefore, it can be confidently asserted that no additional tests are necessary."<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 6.7.5 FPT_TUD_EXT.1

#### 6.7.5.1 FPT_TUD_EXT.1 TSS 1

| | |
|---|---|
| Objective | The evaluator shall verify that the TSS describe how to query the currently active version. If a trusted update can be installed on the TOE with a delayed activation, the TSS needs to describe how and when the inactive version becomes active. The evaluator shall verify this description. |
| Evaluator Findings | The evaluator examined the section titled 7.5 Protection of the TSF (FPT) in the Security Target to verify that the TSS describes how to query the currently active version. Upon investigation, the evaluator found that the TSS states that the security Administrator can verify the version of currently running EOS with "show version" CLI command.<br><br>The evaluator examined subsection FPT_TUD_EXT.1 within section 7.5 titled "Protection of the TSF (FPT)" in the Security Target. The objective was to validate whether the TSS section adequately addresses the process for activating the inactive version in the event of a trusted update with delayed activation. Upon investigation, the evaluator ascertained that the TSS stipulates the involvement of the TOE administrator, who is responsible for modifying the boot-config file to specify the precise location of the new image in the flash folder. Subsequently, the configuration changes are saved to the startup-config file, and the TOE undergoes a reboot to implement the installation of the new file.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

#### 6.7.5.2 FPT_TUD_EXT.1 TSS 2

| | |
|---|---|
| Objective | The evaluator shall verify that the TSS describes all TSF software update mechanisms for updating the system firmware and software (for simplicity the term 'software' will be used in the following although the requirements apply to firmware and software). The evaluator shall verify that the description includes a digital signature verification of the software before installation and that installation fails if the verification fails. Alternatively, an approach using a published hash can be used. In this case the TSS shall detail this mechanism instead of the digital signature verification mechanism. The evaluator shall verify that the TSS describes the method by which the digital signature or published hash is verified to include how the candidate updates are obtained, the processing associated with verifying the digital signature or published hash of the update, and the actions that take place for both successful and unsuccessful signature verification or published hash verification. |
| Evaluator Findings | The evaluator examined the section titled 7.5 Protection of the TSF (FPT) in the Security Target to verify that the TSS describes the method by which the published hash is verified to include how the candidate updates are obtained, the processing associated with verifying the published hash of the update, and the actions that take place for both successful and |

| | |
|---|---|
| | unsuccessful published hash verification. Upon investigation, the evaluator found that the TSS states:<br><br>"Software updates are verified using SHA-512 published hash values. The update is performed by Security Administrator and only on the management console. The candidate update package is downloaded from the Arista's customer portal. Arista customers require a valid credential to login to this portal to obtain the candidate updates<br><br>The Security Administrator is required to transfer the downloaded candidate package from a trusted terminal to the TOE using secure means; typically SCP (secure copy) is utilized. The SHA-512 checksum of the candidate file is to be generated on the candidate update package that was securely copied to the TOE. This is done by issuing the following command: *sha512sum <update-package>*. The Security Administrator must verify that the on-screen output of the checksum of the candidate update package matches the published hash of the candidate update package before initiating the installation of the candidate update package. The Security Administrator accomplishes this by visually comparing the published checksum to the checksum of the candidate update package that was generated by the Security Administrator. If the hash generated does not match the published hash for the candidate update, the Security Administrator is instructed not to proceed further."<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

6.7.5.3 FPT_TUD_EXT.1 TSS 3

| | |
|---|---|
| Objective | If the options 'support automatic checking for updates' or 'support automatic updates' are chosen from the selection in FPT_TUD_EXT.1.2, the evaluator shall verify that the TSS explains what actions are involved in automatic checking or automatic updating by the TOE, respectively. |
| Evaluator Findings | Not Applicable. The Security Target (ST) explicitly states that it does not assert support for "automatic checking for updates" or "automatic updates" as selectable features. |
| Verdict | Pass |

6.7.5.4 FPT_TUD_EXT.1 TSS 5

| | |
|---|---|
| Objective | If a published hash is used to protect the trusted update mechanism, then the evaluator shall verify that the trusted update mechanism does involve an active authorization step of the Security Administrator, and that download of the published hash value, hash comparison and update is not a fully automated process involving no active authorization by the Security Administrator. In particular, authentication as Security Administration according to FMT_MOF.1/ManualUpdate needs to be part of the update process when using published hashes. |
| Evaluator Findings | The evaluator examined the section titled 7.5 Protection of the TSF (FPT) in the Security Target to verify that the TSS, if a published hash is used to protect the trusted update mechanism, contains a description of how the trusted update mechanism involves an active authorization step of the Security Administrator, and that download of the published hash value, hash comparison and update is not a fully automated process involving no active authorization by the Security Administrator. Upon investigation, the evaluator found that the TSS states that |

| | |
|---|---|
| | Software updates are verified using SHA-512 published hash values. The update is performed by Security Administrator and only on the SSH remote management console. The candidate update package is downloaded from the Arista's customer portal. Arista customers require a valid credential to login to this portal to obtain the candidate updates. The candidate updates are provided with a separate download of the SHA-512 hashed value of the update package. The Security Administrator is required to transfer the downloaded candidate package from a trusted terminal to the TOE using secure means; typically SCP (secure copy) is utilized. The SHA-512 checksum of the candidate file is to be generated on the candidate update package that was securely copied to the TOE. This is done by issuing the following command: sha512sum <update-package>. The Security Administrator must verify that the on-screen output of the checksum of the candidate update package matches the published hash of the candidate update package before initiating the installation of the candidate update package. The Security Administrator accomplishes this by visually comparing the published checksum to the checksum of the candidate update package that was generated by the Security Administrator. If the hash generated does not match the published hash for the candidate update, the Security Administrator is instructed not to proceed further.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

## 6.8 TSS Activities (TOE Access)

### 6.8.1 FTA_SSL_EXT.1

#### 6.8.1.1 FTA_SSL_EXT.1 TSS 1

| | |
|---|---|
| Objective | The evaluator shall examine the TSS to determine that it details whether local administrative session locking or termination is supported and the related inactivity time period settings. |
| Evaluator Findings | The evaluator examined the section titled 7.6 TOE Access (FTA) in the Security Target to verify that the TSS identifies whether local administrative session locking, or termination is supported and the related inactivity time period settings. Upon investigation, the evaluator found that the TSS states that<br><br>Security Administrator can configure a time period to be used to automatically terminate administrative session after inactivity. For local and remote administrative session, the TSF terminates the session after this period of inactivity.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 6.8.2 FTA_SSL.3

#### 6.8.2.1 FTA_SSL.3 TSS 1

| | |
|---|---|
| Objective | The evaluator shall examine the TSS to determine that it details the administrative remote session termination and the related inactivity time period. |
| Evaluator Findings | The evaluator examined the section titled 7.6 TOE Access (FTA) in the Security Target to verify that the TSS identifies administrative remote session termination and the related inactivity time period. Upon investigation, the evaluator found that the TSS states that |

| | |
|---|---|
| | For local and remote administrative session, the TSF terminates the session after this period of inactivity. To facilitate this, a timer is started for the session after successful authentication of Security Administrator. The timer is reset each time the Security Administrator provides input. If the Security Administrator does not provide input for a duration of configured inactivity period, the TSF terminates the administrative session.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 6.8.3 FTA_SSL.4

#### 6.8.3.1 FTA_SSL.4 TSS 1

| | |
|---|---|
| Objective | The evaluator shall examine the TSS to determine that it details how the local and remote administrative sessions are terminated. |
| Evaluator Findings | The evaluator examined the section titled 7.6 TOE Access (FTA) in the Security Target to verify that the TSS identifies details how the local and remote administrative sessions are terminated. Upon investigation, the evaluator found that the TSS states that<br><br>Security Administrator can configure a time period to be used to automatically terminate administrative session after inactivity. For local and remote administrative session, the TSF terminates the session after this period of inactivity. To facilitate this, a timer is started for the session after successful authentication of Security Administrator. The timer is reset each time the Security Administrator provides input. If the Security Administrator does not provide input for a duration of configured inactivity period, the TSF terminates the administrative session.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 6.8.4 FTA_TAB.1

#### 6.8.4.1 FTA_TAB.1 TSS 1

| | |
|---|---|
| Objective | The evaluator shall check the TSS to ensure that it details each administrative method of access (local and remote) available to the Security Administrator (e.g., serial port, SSH, HTTPS). The evaluator shall check the TSS to ensure that all administrative methods of access available to the Security Administrator are listed and that the TSS states that the TOE is displaying an advisory notice and a consent warning message for each administrative method of access. The advisory notice and the consent warning message might be different for different administrative methods of access and might be configured during initial configuration (e.g., via configuration file). |
| Evaluator Findings | The evaluator examined the section titled 7.7 Trusted Path/Channels (FTP) in the Security Target to verify that the TSS details each administrative method of access available to the Security Administrator and states that the TOE is displaying an advisory notice and consent warning message for each administrative method of access. Upon investigation, the evaluator found that the TSS states that<br><br>Before establishing an administrative user session to the TSF, the TSF displays a Security Administrator-specified advisory notice and consent warning message (banner). The banner is presented prior to human user authentication on each of the TOE's administrative interfaces. This banner is not required to be, nor is it, presented to the eAPI JSON-RPC client prior to it |

| | |
|---|---|
| | authenticating to the TSF. The banner can be configured via any one of the following administrative interfaces: Local console (serial port), remote console (SSH), remote management (eAPI JSON-RPC client).<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

## 6.9 TSS Activities (Trusted Path/Channels)

### 6.9.1 FTP_ITC.1

#### 6.9.1.1 FTP_ITC.1 TSS 1

| | |
|---|---|
| Objective | The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each secure communication mechanism is identified in terms of the allowed protocols for that IT entity, whether the TOE acts as a server or a client, and the method of assured identification of the non-TSF endpoint. The evaluator shall also confirm that all secure communication mechanisms are described in sufficient detail to allow the evaluator to match them to the cryptographic protocol Security Functional Requirements listed in the ST. |
| Evaluator Findings | The evaluator examined the section titled 7.7 Trusted Path/Channels (FTP) in the Security Target to verify that the TSS, for all communications with authorized IT entities identified in the requirement, each secure communication mechanism is identified in terms of the allowed protocols for that IT entity, whether the TOE acts as a server or a client, and the method of assured identification of the non-TSF endpoint. Upon investigation, the evaluator found that the TSS states the following:<br>• A Trusted Channel connection is created between TSF and the audit server, which is protected by SSH. The TOE acts as an SSH client in the Trusted Channel connection to the audit server. The operation of SSH is described above in FCS_SSHC_EXT.1.<br>• A Trusted Channel connection is created between TSF and the eAPI JSON-RPC Client, which is protected by TLS. The TOE acts as a TLS server in the Trusted Channel connection to the eAPI JSON-RPC Client. The operation of TLS is described above in FCS_TLSS_EXT.2.<br><br>The evaluator examined the section titled 7.2 Cryptographic Support (FCS) in the Security Target to verify that the TSS describes all secure communication mechanisms in sufficient detail to allow the evaluator to match them to the cryptographic protocol Security Functional Requirements listed in the ST. Upon investigation, the evaluator found that the TSS states that all the information mentioned about SSH and TLS in the TSS matches with the cryptographic protocols mentioned in the SFRs.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 6.9.2 FTP_TRP.1/Admin

#### 6.9.2.1 FTP_TRP.1/Admin TSS 1

| | |
|---|---|
| Objective | The evaluator shall examine the TSS to determine that the methods of remote TOE administration are indicated, along with how those communications are protected. The evaluator shall also confirm that all protocols listed in the TSS in support of TOE administration are consistent with those specified in the requirement, and are included in the requirements in the ST. |
| Evaluator Findings | The evaluator examined the section titled 7.7 Trusted Path/Channels (FTP) in the Security Target to verify that the TSS indicates the methods of remote TOE administration and how those communications are protected. Upon investigation, the evaluator found that the TSS states that<br><br>Trusted Path connection protects communication between TSF and human user (Security Administrator) performing management of the TSF. It is protected by SSH. TOE acts as SSH Server in the Trusted Path connection. Operation of SSH is described above in FCS_SSHS_EXT.1.<br><br>The evaluator examined the section titled 7.2 Cryptographic Support (FCS) in the Security Target to verify that the TSS protocols are consistent with those specified in the requirement. Upon investigation, the evaluator found that the TSS states that<br><br>TOE performs the role of SSH client in Trusted Channel. The TSF ensures that the SSH client authenticates the identity of the audit server using the /etc/ssh/known_hosts file which associates each server host name with its corresponding public key as described in RFC 4251<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

# 7 Detailed Testing Assurance Activities

## 7.1 Audit

## 7.2 FAU_GEN.1 Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 1: The evaluator shall test the TOE's ability to correctly generate audit records by having the TOE generate audit records for the events listed in the table of audit events and administrative actions listed above. This should include all instances of an event: for instance, if there are several different I&A mechanisms for a system, the FIA_UIA_EXT.1 events must be generated for each mechanism. The evaluator shall test that audit records are generated for the establishment and termination of a channel for each of the cryptographic protocols contained in the ST. If HTTPS is implemented, the test demonstrating the establishment and termination of a TLS session can be combined with the test for an HTTPS session. When verifying the test results, the evaluator shall ensure the audit records generated during testing match the format specified in the guidance documentation, and that the fields in each audit record have the proper entries.<br>Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly. |
| **Test Steps** | 1. Trigger each auditable event on the TOE.<br>2. Verify that each audit record is generated and contains the appropriate audit record details. |
| **Expected Test Results** | 1. The TOE should be able to generate audit records for each of the events described in the ST under the FAU_GEN.1.1, FAU_GEN.1.2.<br>2. The audit records generated should match the proper format as specified in the guidance documentation. |
| **Pass/Fail with Explanation** | Pass. The audit records associated with each test case are recorded with each test case. A comparison of required audit records to the presented audit records was additionally performed. This analysis shows that each required audit record is generated by the TOE, meeting the test requirements. |

## 7.3 FAU_STG_EXT.1 Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 1: The evaluator shall establish a session between the TOE and the audit server according to the configuration guidance provided. The evaluator shall then examine the traffic that passes between the audit server and the TOE during several activities of the evaluator's choice designed to generate audit data to be transferred to the audit server. The evaluator shall observe that these data are not able to be viewed in the clear during this transfer, and that they are successfully received by the audit server. The evaluator shall record the particular software (name, version) used on the audit server during testing. The evaluator shall verify that the TOE is capable of transferring audit data to an external audit server automatically without administrator intervention. |

| | |
|---|---|
| **Test Steps** | 1. Add the switch's public key for authentication to the Syslog Server by logging into the Syslog server with the username "admin2".<br>2. Copy the switch's entire public key from the USB to the ~/.ssh/authorized_keys file in the home directory of the "admin2".<br>3. Give the correct permissions to the SSH files and restart the SSH daemon.<br>4. Configure the TOE to communicate with the Syslog server by generating an RSA public key on the Syslog server.<br>5. Configure "admin2" user with the RSA public key authentication.<br>6. Confirm that the SSH tunnel is configured on the endpoints on the switch and the Syslog server.<br>7. Verify that the traffic between the TOE and the Syslog server is not sent in plain text.<br>8. Show version of the software that audit server is using. |
| **Expected Test Results** | 1. The switch's public key is added to the Syslog server using the "admin2" account.<br>2. The switch's public key will be copied to the authorized keys file in the home directory of "admin2".<br>3. The correct permissions will be granted to the SSH files and SSH daemon will be restarted.<br>4. An RSA public key on the Syslog server will be generated.<br>5. The "admin2" user will be configured on the TOE with the RSA public key authentication.<br>6. The SSH tunnel is configured on the endpoints on the switch and Syslog server.<br>7. The traffic between the TOE and Syslog server is not sent in plain text. |
| **Pass/Fail with Explanation** | Pass – Audit data from the TOE is sent automatically and received by the audit server; data is not sent in cleartext. This satisfies the constraints of this test case. |

### 7.4 FAU_STG_EXT.1 Test #2 (a)

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 2: The evaluator shall perform operations that generate audit data and verify that this data is stored locally. The evaluator shall perform operations that generate audit data until the local storage space is exceeded and verifies that the TOE complies with the behavior defined in FAU_STG_EXT.1.3. Depending on the configuration this means that the evaluator has to check the content of the audit data when the audit data is just filled to the maximum and then verifies that: The audit data remains unchanged with every new auditable event that should be tracked but that the audit data is recorded again after the local storage for audit data is cleared (for the option '**drop new audit data**' in FAU_STG_EXT.1.3). |
| **Pass/Fail with Explanation** | The [ST] states in FAU_STG_EXT.1 that "The TSF shall overwrite previous audit records according to the following rule: **periodic audit log rotation (delete the oldest log file)** when the local storage space for audit data is full."<br>Therefore, this test is non-applicable. |

### 7.5 FAU_STG_EXT.1 Test #2 (b)

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 2: The evaluator shall perform operations that generate audit data and verify that this data is stored locally. The evaluator shall perform operations that generate audit data until the local storage space is exceeded and verifies that the TOE complies with the behavior defined in FAU_STG_EXT.1.3. Depending on the configuration this means that the evaluator has to check the content of the audit data when the audit data is just filled to the maximum and then verifies that: The existing audit data is overwritten with every new auditable event that should be tracked according to the specified rule (for the option '**overwrite previous audit records**' in FAU_STG_EXT.1.3) |
| **Test Steps** | 1. Setup the syslog server on the TOE and configure syslog to log all the messages on the TOE and verify the log status by checking the contents of the audit log and recording the timestamp of the audit log.<br>2. Run a suite of self-test to create logs for the audit system to record.<br>3. Verify that the logs are locally stored and when the audit log data is full, the oldest log entry will be overwritten. |
| **Expected Test Results** | 1. The syslog server on the TOE is setup correctly and will log all audit log messages. The audit log status will be recorded with time and date.<br>2. The self-testing will create audit logs on the TOE, overwriting what was in the audit log file.<br>3. The local audit logs will be overwritten as per the TOE's "delete the oldest log file" functionality. |
| **Pass/Fail with Explanation** | Pass - When audit data is filled to the max, the existing audit data is overwritten. |

### 7.6 FAU_STG_EXT.1 Test #2 (c)

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 2c: The evaluator shall perform operations that generate audit data and verify that this data is stored locally. The evaluator shall perform operations that generate audit data until the local storage space is exceeded and verifies that the TOE complies with the behavior defined in FAU_STG_EXT.1.3. Depending on the configuration this means that the evaluator has to check the content of the audit data when the audit data is just filled to the maximum and then verifies that: The TOE behaves as specified (for the option '**other action**' in FAU_STG_EXT.1.3). |
| **Pass/Fail with Explanation** | The [ST] states in FAU_STG_EXT.1 that "The TSF shall overwrite previous audit records according to the following rule: **periodic audit log rotation (delete the oldest log file)** when the local storage space for audit data is full." Therefore, this test is non-applicable. |

### 7.7 FAU_STG_EXT.1 Test #4

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 4: For distributed TOEs, Test 1 defined above should be applicable to all TOE components that forward audit data to an external audit server. For the local storage according to FAU_STG_EXT.1.2 and FAU_STG_EXT.1.3 the Test 2 |

| | |
|---|---|
| | specified above shall be applied to all TOE components that store audit data locally. For all TOE components that store audit data locally and comply with FAU_STG_EXT.2/LocSpace Test 3 specified above shall be applied. The evaluator shall verify that the transfer of audit data to an external audit server is implemented. |
| **Pass/Fail with Explanation** | N/A. This test is not applicable since the TOE is not a distributed TOE |

### 7.8 FPT_STM_EXT.1 Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 1: If the TOE supports direct **setting of the time by the Security Administrator,** then the evaluator uses the guidance documentation to set the time. The evaluator shall then use an available interface to observe that the time was set correctly. |
| **Test Steps** | 1. Confirm the current time on the TOE.<br>2. Set a new time on the TOE using the guidance documentation.<br>3. Verify the TOE's audit logs logged the new time change. |
| **Expected Test Results** | 1. The current time on the TOE will be displayed.<br>2. A new time is set on the TOE.<br>3. The TOE's audit log will reflect the new time change implementation. |
| **Pass/Fail with Explanation** | Pass – The administrator was able to successfully configure the time on the TOE using the guidance documentation. |

### 7.9 FPT_STM_EXT.1 Test #2 [TD0632]

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 2: If the TOE supports the **use of an NTP server**; the evaluator shall use the guidance documentation to configure the NTP client on the TOE, and set up a communication path with the NTP server. The evaluator will observe that the NTP server has set the time to what is expected. If the TOE supports multiple protocols for establishing a connection with the NTP server, the evaluator shall perform this test using each supported protocol claimed in the guidance documentation. |
| **Pass/Fail with Explanation** | N/A – As per the [ST], the TOE uses a local clock for time stamps. It does not implement NTP. |

### 7.10 FPT_STM_EXT.1 Test #3

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 3: [conditional] If the TOE obtains time from the underlying VS, the evaluator shall record the time on the TOE, modify the time on the underlying VS, and verify the modified time is reflected by the TOE. If there is a delay between the setting |

| | |
|---|---|
| | the time on the VS and when the time is reflected on the TOE, the evaluator shall ensure this delay is consistent with the TSS and Guidance. |
| **Pass/Fail with Explanation** | N/A – As per the [ST], the TOE does not obtain time from the underlying VS. |

### 7.11 FPT_STM_EXT.1 Test #4

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 4: If **the audit component of the TOE consists of several parts with independent time information**, then the evaluator shall verify that the time information between the different parts are either synchronized or that it is possible for all audit information to relate the time information of the different part to one base information unambiguously. |
| **Pass/Fail with Explanation** | N/A – As per the [ST], the TOE's does not consist of several parts with independent time information. |

### 7.12 FTP_ITC.1 Test #1 (TD0572)

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 1: The evaluators shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful. |
| **Pass/Fail with Explanation** | Pass. This testing is covered by the requirements in FAU_STG_EXT.1 Test #1 for SSH to the syslog server and FCS_SSHC_EXT.1.2 Test#1 for SSH client and in FCS_TLSS_EXT.1 Test#1 for TLS from the client to the TOE. |

### 7.13 FTP_ITC.1 Test #2 (TD0572)

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 2: For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the guidance documentation to ensure that in fact the communication channel can be initiated from the TOE. |
| **Pass/Fail with Explanation** | Pass. This testing is covered by the requirements in FAU_STG_EXT.1 Test #1 for SSH to the syslog server and FCS_SSHC_EXT.1.2 Test#1 for SSH client and in FCS_TLSS_EXT.1 Test#1 for TLS from the client to the TOE. |

### 7.14 FTP_ITC.1 Test #3 (TD0572)

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 3: The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext. |

| | |
|---|---|
| **Pass/Fail with Explanation** | Pass. This testing is covered by the requirements in FAU_STG_EXT.1 Test #1 for SSH to the syslog server and FCS_SSHC_EXT.1.2 Test#1 for SSH client and in FCS_TLSS_EXT.1 Test#1 for TLS from the client to the TOE. |

### 7.15 FTP_ITC.1 Test #4 (TD0572)

| Item | Data |
|---|---|
| **Test Assurance Activity** | Objective: The objective of this test is to ensure that the TOE reacts appropriately to any connection outage or interruption of the route to the external IT entities.<br>The evaluator shall, for each instance where the TOE acts as a client utilizing a secure communication mechanism with a distinct IT entity, physically interrupt the connection of that IT entity for the following durations:<br>1. A duration that exceeds the TOE's application layer timeout setting,<br>2. A duration shorter than the application layer timeout but of sufficient length to interrupt the network link layer.<br>The evaluator shall ensure that, when the physical connectivity is restored, communications are appropriately protected and no TSF data is sent in plaintext.<br>In the case where the TOE is able to detect when the cable is removed from the device, another physical network device (e.g. a core switch) shall be used to interrupt the connection between the TOE and the distinct IT entity. The interruption shall not be performed at the virtual node (e.g. virtual switch) and must be physical in nature. |
| **Test Steps** | 1. Connect to the TOE via SSH and unplug the network cable for 10 seconds. The evaluator will ensure the connection is interrupted.<br>2. Reconnect to the TOE via SSH and ensure that no data is sent in plain text.<br>3. Connect to the TOE via SSH and unplug the network cable for 15 minutes. The evaluator will ensure that the connection is interrupted.<br>4. Reconnect to the TOE via SSH and ensure that no data is sent in plain text.<br>5. Connect to the TOE via TLS and unplug the network cable for 10 seconds. The evaluator will ensure the connection is interrupted.<br>6. Reconnect to the TOE via TLS and ensure that no data is sent in plain text.<br>7. Connect to the TOE via TLS and unplug the network cable for 15 minutes. The evaluator will ensure that the connection is interrupted.<br>8. Reconnect to the TOE via TLS and ensure that no data is sent in plain text. |
| **Expected Test Results** | 1. Connection is interrupted.<br>2. No data is sent in plain text.<br>3. Connection is interrupted.<br>4. No data is sent in plain text.<br>5. Connection being interrupted.<br>6. No data is sent in plain text.<br>7. Connection is interrupted.<br>8. No data is sent in plain text. |

| | |
|---|---|
| **Pass/Fail with Explanation** | Pass - The TOE does not send plaintext traffic when disconnected from the external entity. This meets the testing requirements. |

### 7.16 FCS_CKM.2 RSA (TD0581)

| Item | Data |
|---|---|
| **Test Assurance Activity** | **Key Establishment Schemes**<br>The evaluator shall verify the correctness of the TSF's implementation of RSAES-PKCS1-v1_5 by using a known good implementation for each protocol selected in FTP_TRP.1/Admin, FTP_TRP.1/Join, FTP_ITC.1 and FPT_ITT.1 that uses RSAES-PKCS1-v1_5. |
| **Pass/Fail with Explanation** | Pass. The evaluator tested all uses of each protocol selected in FTP_TRP.1/Admin, FTP_TRP.1/Join, FTP_ITC.1 and FPT_ITT.1 that uses RSAES-PKCS1-v1_5 using a known good implementation. |

### 7.17 FIA_AFL.1 Test #1 (TD0570)

| Item | Data |
|---|---|
| **Test Assurance Activity** | The evaluator shall perform the following tests for each method by which remote administrators access the TOE (e.g. any passwords entered as part of establishing the connection protocol or the remote administrator application):<br>Test 1: The evaluator shall use the operational guidance to configure the number of successive unsuccessful authentication attempts allowed by the TOE (and, if the time period selection in FIA_AFL.1.2 is included in the ST, then the evaluator shall also use the operational guidance to configure the time period after which access is re-enabled). The evaluator shall test that once the authentication attempts limit is reached, authentication attempts with valid credentials are no longer successful. |
| **Test Steps** | 1. Configure the TOE for several successive unsuccessful authentication attempts as well as lockout time period.<br>2. Initiate an SSH session and will attempt to login with the wrong password to lockout the user.<br>3. Ensure the user is locked out by examining the audit logs.<br>4. Attempt to login with the same user with a valid password before the lockout period has ended.<br>5. Verify that the attempt failed by examining the audit logs. |
| **Expected Test Results** | 1. The TOE is configured for authentication attempts and lockout time.<br>2. An SSH session is initiated and lockout the user.<br>3. Audit logs indicate the user is locked out.<br>4. Login is not possible due to the lockout period still being in effect.<br>5. Audit logs indicate the user failed to login. |
| **Pass/Fail with Explanation** | PASS – The authentication limit can be set by the user and the TOE does not allow access once the authentication attempt limit has been reached. This meets the testing requirements. |

### 7.18 FIA_AFL.1 Test #2a (TD0570)

| Item | Data |
|---|---|
| **Test Assurance Activity** | The evaluator shall perform the following tests for each method by which remote administrators access the TOE (e.g. any passwords entered as part of establishing the connection protocol or the remote administrator application):<br>Test 2: After reaching the limit for unsuccessful authentication attempts as in Test 1 above, the evaluator shall proceed as follows:<br>If the **administrator action** selection in FIA_AFL.1.2 is included in the ST, then the evaluator shall confirm by testing that following the operational guidance and performing each action specified in the ST to re-enable the remote administrator's access results in successful access (when using valid credentials for that administrator). |
| **Test Steps** | 1. Test the defined time period (lockout time) factor of the TOE; lockout the administrator account by providing the incorrect password 3 times (causing a lockout period of 2 minutes).<br>2. Test the authentication session before the lockout period has expired, resulting in an unsuccessfully login attempt.<br>3. Confirm after 2 minutes the successful login of the administrator is once again accepted.<br>4. Check the audit logs to ensure successful user lockout. |
| **Expected Test Results** | 1. An account lockout of the admin account will occur.<br>2. An attempt is made to connect to the TOE using the admin account before the lockout period has expired.<br>3. Waited 2 minutes, then will be able to login again to the TOE.<br>4. The audit logs verified the admin account was locked out. |
| **Pass/Fail with Explanation** | Pass – The TOE allowed authentication after the locked-out user was manually unlocked. This meets the testing requirements. |

### 7.19 FIA_AFL.1 Test #2b

| Item | Data |
|---|---|
| **Test Assurance Activity** | The evaluator shall perform the following tests for each method by which remote administrators access the TOE (e.g. any passwords entered as part of establishing the connection protocol or the remote administrator application):<br>Test 2: After reaching the limit for unsuccessful authentication attempts as in Test 1 above, the evaluator shall proceed as follows:<br>If the **time period** selection in FIA_AFL.1.2 is included in the ST, then the evaluator shall wait for just less than the time period configured in Test 1 and show that an authorization attempt using valid credentials does not result in successful access. The evaluator shall then wait until just after the time period configured in Test 1 and show that an authorization attempt using valid credentials results in successful access. |
| **Test Steps** | 1. Test the defined time period (lockout time) factor of the TOE by using the same lockout time previously set in FIA_AFL.1 Test#1.<br>2. Lockout the administrator account by providing the incorrect password 3 times (causing a lockout period of 2 minutes).<br>3. Test the authentication session before the lockout period has expired, resulting in an unsuccessfully login attempt.<br>4. Confirm after 2 minutes the successful login of the administrator is once again accepted. |

| | |
|---|---|
| | 5. Check the audit logs to ensure successful user lockout. |
| **Expected Test Results** | 1. Use the same settings from the previous test (FIA_AFL.1 Test 1)<br>2. Admin account will be locked out.<br>3. An attempt will be made to connect to the TOE using the admin account before the lockout period has expired.<br>4. Login will occur after 2 minutes, then be able to login again to the TOE.<br>5. The audit logs verify the admin account was locked out. |
| **Pass/Fail with Explanation** | Pass - The TOE allowed authentication after the TOE completed its locked-out threshold. This meets the testing requirements. |

### 7.20 FIA_PMG_EXT.1 Test #1 (TD0571)

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 1: The evaluator shall compose passwords that meet the requirements in some way. For each password, the evaluator shall verify that the TOE supports the password. While the evaluator is not required (nor is it feasible) to test all possible compositions of passwords, the evaluator shall ensure that all characters, and a minimum length listed in the requirement are supported and justify the subset of those characters chosen for testing. |
| **Test Steps** | 1. The evaluator will configure the TOE to accept the following password parameters: minimum password length = 10 in accordance with the [ST].<br>2. The evaluator will attempt to create three users whose passwords meet the security requirements, using step #1's support password metrics.<br>Username: Josh1 Password: Gola#98456<br>Username: Josh2 Password: G0l@$*358567<br>Username: Josh3 Password: Gg0!@^%26790<br>3. The evaluator will attempt to authenticate to the TOE using the three created users plus created passwords. |
| **Expected Test Results** | 1. Configure the TOE successfully to implement strong password complexity.<br>2. Create the three users and accompanying passwords.<br>3. Successfully authentication to the TOE will result using the provided passwords. |
| **Pass/Fail with Explanation** | Pass - The TOE was able to create users with passwords that meet the TOE's password complexity requirement. This meets the requirement. |

### 7.21 FIA_PMG_EXT.1 Test #2 (TD0571)

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 2: The evaluator shall compose passwords that do not meet the requirements in some way. For each password, the evaluator shall verify that the TOE does not support the password. While the evaluator is not required (nor is it feasible) to test all possible compositions of passwords, the evaluator shall ensure that the TOE enforces the allowed characters and the minimum length listed in the requirement and justify the subset of those characters chosen for testing. |

| | |
|---|---|
| **Test Steps** | 1. Configure a policy to only allow a minimum password length of 8 characters for newly configured users.<br>2. The evaluator will attempt to create a user whose password complexity does not meet the minimum requirements of having minimum 8 characters. |
| **Expected Test Results** | 1. The TOE will not allow the creation of the user due to the password complexity requirement not being met. |
| **Pass/Fail with Explanation** | Pass - The TOE was able to reject users with bad passwords. This meets the requirement. |

### 7.22 **FIA_UIA_EXT.1. Test #1**

| Item | Data |
|---|---|
| **Test Assurance Activity** | The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by what is claimed in FIA_UIA_EXT.1.2.<br>Test 1: The evaluator shall use the guidance documentation to configure the appropriate credential supported for the login method. For that credential/login method, the evaluator shall show that providing correct I&A information results in the ability to access the system, while providing incorrect information results in denial of access. |
| **Test Steps** | Local<br>1. Log into the TOE via console with bad credentials. This should fail with logs supporting this action on the TOE.<br>2. Log into the TOE via console with good credentials. This should succeed with the TOE Logs supporting this action.<br>3. Verify the audit logs reflect both attempts.<br>Remote (password-based)<br>1. Log into the TOE via SSH with bad credentials; this should fail with TOE audit logs supporting this action.<br>2. Log into the TOE via SSH with good credentials; this should succeed with TOE audit logs supporting this action.<br>3. Verify audit logs reflect both attempts.<br>Remote (public key-based)<br>1. Log into the TOE via SSH with bad credentials; this should fail.<br>2. Log into the TOE via SSH with good credentials; this should succeed.<br>3. Verify audit logs reflect both success and failure attempts. |
| **TExpected Test Results** | Local<br>1. Log into the TOE via console will not be possible with bad credentials.<br>2. Log into the TOE via console will be possible with good credentials.<br>3. Both login attempts will be recorded in the audit logs. |

| | |
|---|---|
| | Remote (password-based)<br>1. Log into the TOE via console will not be possible with bad credentials.<br>2. Log into the TOE via console will be possible with good credentials.<br>3. Both login attempts will be recorded in the audit logs.<br>Remote (public key-based)<br>1. Log into the TOE via console will not be possible with bad credentials.<br>2. Log into the TOE via console will be possible with good credentials.<br>3. Both login attempts will be recorded in the audit logs. |
| **Pass/Fail with Explanation** | Pass - Presenting incorrect authentication credentials results in denied access to the TOE. Presenting correct authentication credentials results in access being allowed to the TOE. This meets the testing requirements. |

### 7.23 FIA_UIA_EXT.1 Test #2

| Item | Data |
|---|---|
| **Test Assurance Activity** | The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by the login method:<br>Test 2: The evaluator shall configure the services allowed (if any) according to the guidance documentation, and then determine the services available to an external remote entity. The evaluator shall determine that the list of services available is limited to those specified in the requirement. |
| **Test Steps** | Key-Based<br>1. Log into the TOE.<br>2. Verify only a login banner is displayed prior to the user authenticating.<br>3. Verify that commands are not available to the user prior to user authentication.<br>4. Login to the TOE successfully and verify that commands are now available to the user.<br>5. Verify the failure of requests before user authentication and the success of requests after user authentication on the TOE via audit logs.<br><br>Password-Based<br>1. Log into the TOE.<br>2. Verify only a login banner is displayed prior to the user authenticating.<br>3. Verify that commands are not available to the user prior to user authentication.<br>4. Login to the TOE successfully and verify that commands are now available to the user.<br>5. Verify the failure of requests before user authentication and the success of requests after user authentication on the TOE via audit logs. |

| | |
|---|---|
| **Expected Test Results** | Password-Based & Key-Based<br>1. Log into the TOE.<br>2. Verify only a login banner is displayed prior to the user authenticating.<br>3. Verify that commands are not available to the user prior to user authentication.<br>4. Login to the TOE successfully and verify that commands are now available to the user.<br>5. Verify the failure of requests before user authentication and the success of requests after user authentication on the TOE via audit logs. |
| **Pass/Fail with Explanation** | Pass - No system services are available to an unauthenticated user connecting remotely. It is seen that only the login banner is displayed prior to authentication. This meets the testing requirements. |

### 7.24 FIA_UIA_EXT.1 Test #3

| Item | Data |
|---|---|
| **Test Assurance Activity** | The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by the login method:<br>Test 3: For local access, the evaluator shall determine what services are available to a local administrator prior to logging in, and make sure this list is consistent with the requirement. |
| **Test Steps** | Password-Based<br>1. Log into the TOE.<br>2. Verify only a login banner is displayed prior to the user authentication.<br>3. Show that a ping request is available to the user prior to user authentication.<br>4. Verify that commands are not available to the user prior to user authentication.<br>5. Login to the TOE successfully and verify that commands are now available to the user.<br>6. Verify the failure of requests before user authentication and the success of requests after user authentication on the TOE via audit logs. |
| **Expected Test Results** | 1. The TOE is logged into.<br>2. A login banner is displayed prior to authentication.<br>3. A ping request is available to the user prior to authentication.<br>4. Commands are not available to the user prior to authentication.<br>5. The TOE has been logged into successfully.<br>6. The audit logs show the failure of requests before user authentication and the success request after authentication on the TOE. |

| | |
|---|---|
| **Pass/Fail with Explanation** | Pass - No system services are available to an unauthenticated user via the directly connected console. It is seen that only the login banner is displayed prior to authentication. This meets the testing requirements. |

### 7.25 FIA_UIA_EXT.1 Test #4

| Item | Data |
|---|---|
| **Test Assurance Activity** | The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by the login method:<br>Test 4: For distributed TOEs where not all TOE components support the authentication of Security Administrators according to FIA_UIA_EXT.1 and FIA_UAU_EXT.2, the evaluator shall test that the components authenticate Security Administrators as described in the TSS. |
| **Pass/Fail with Explanation** | N/A – The TOE is not a distributed TOE; therefore, this test is non-applicable. |

### 7.26 FIA_UAU.7 Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 1: The evaluator shall perform the following test for each method of local login allowed:<br>The evaluator shall locally authenticate to the TOE. While making this attempt, the evaluator shall verify that at most obscured feedback is provided while entering the authentication information. |
| **Test Steps** | 1. Connect to the TOE via console with correct authentication credentials and verify that at most obscured feedback is provided.<br>2. Verify authentication logs reflect success. |
| **Expected Test Results** | 1. The TOE should not provide anything other than obscured feedback at the directly connected login prompt.<br>2. Evidence (screenshot or CLI output) showing no output from the password being entered.<br>3. Logs show successful/unsuccessful login attempts. |
| **Pass/Fail with Explanation** | Pass – While logging into the TOE, the TOE does not provide anything more than obscured feedback. This meets the testing requirements. |

### 7.27 FMT_MOF.1/ManualUpdate Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 1: The evaluator shall try to perform the update using a legitimate update image without prior authentication as Security Administrator (either by authentication as a user with no administrator privileges or without user authentication at all – depending on the configuration of the TOE). The attempt to update the TOE shall fail. |
| **Test Steps** | 1. Create a read-only user in which this test shall be performed as.<br>2. Attempt to update the TOE using an authorized user with no administrator privileges. |

| | |
|---|---|
| | 3. Verify the audit logs reflect this attempt. |
| **Expected Test Results** | 1. A read only user will be created on the TOE.<br>2. The authorized user with no administrator privileges will not be able to update the TOE. |
| **Pass/Fail with Explanation** | Pass - Unprivileged user cannot perform a software update on the TOE. These meets the testing requirements. |

### 7.28 FMT_MOF.1/ManualUpdate Test #2

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 2: The evaluator shall try to perform the update with prior authentication as Security Administrator using a legitimate update image. This attempt should be successful. This test case should be covered by the tests for FPT_TUD_EXT.1 already. |
| **Test Steps** | This testing is covered by the requirements in FPT_TUD_EXT.1 Test #1. |
| **Expected Test Results** | **This testing is covered by the requirements in FPT_TUD_EXT.1 Test #1.** |
| **Pass/Fail with Explanation** | This testing is covered by the requirements in FPT_TUD_EXT.1 Test #1. |

### 7.29 FMT_MOF.1/Functions (1) Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 1 (if **'transmission of audit data to external IT entity'** is selected from the second selection together with **'modify the behaviour of'** in the first selection): The evaluator shall try to modify all security related parameters for configuration of the transmission protocol for transmission of audit data to an external IT entity without prior authentication as Security Administrator (by authentication as a user with no administrator privileges or without user authentication at all). Attempts to modify parameters without prior authentication should fail. According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt to modify the security related parameters can be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator. |
| **Test Steps** | 1. Login as a user without Security Administrator privileges<br>2. Attempt to modify transmission protocol for the transmission of audit data to an external IT entity. This will fail as the options are unavailable |
| **Expected Test Results** | 1. The TOE should not allow users without administrative access to perform high privilege operations |

| | |
|---|---|
| | 2. Evidence - screenshot showing options are disabled |
| **Pass/Fail with Explanation** | Pass. Unauthorized users cannot alter the protocol because they cannot access the management interface for audit transmission. |

### 7.30 FMT_MOF.1/Functions (1) Test #2

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 2 (if **'transmission of audit data to external IT entity'** is selected from the second selection together with **'modify the behaviour of'** in the first selection): The evaluator shall try to modify all security related parameters for configuration of the transmission protocol for transmission of audit data to an external IT entity with prior authentication as Security Administrator. The effects of the modifications should be confirmed.<br>The evaluator does not have to test all possible values of the security related parameters for configuration of the transmission protocol for transmission of audit data to an external IT entity but at least one allowed value per parameter. |
| **Test Steps** | 1. Login as a user with Security Administrator privileges<br>2. Attempt to modify transmission protocol for the transmission of audit data to an external IT entity. |
| **Expected Test Results** | 1. The TOE will allow user with administrative privileges to modify data. |
| **Pass/Fail with Explanation** | Pass, the TOE allows the Security Administrator to modify Audit data. |

### 7.31 FMT_MTD.1/CryptoKeys Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 1: The evaluator shall try to perform at least one of the related actions (modify, delete, generate/import) without prior authentication as Security Administrator (either by authentication as a non-administrative user, if supported, or without authentication at all). Attempts to perform related actions without prior authentication should fail. According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt to manage cryptographic keys can be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator. |
| **Test Steps** | 1. Login to the TOE as a non-administrative user and attempt to modify cryptographic key functionality. This will fail as the user does not have sufficient privileges to do so. |
| **Expected Test Results** | The TOE should not allow a non-administrative user to modify cryptographic keys. |
| **Pass/Fail with Explanation** | Pass - Unprivileged user cannot perform security related configurations on the TOE. This meets the testing requirements. |

### 7.32 FMT_MTD.1/CryptoKeys Test #2

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 2: The evaluator shall try to perform at least one of the related actions with prior authentication as Security Administrator. This attempt should be successful. |
| **Test Steps** | 1. Login to the TOE as an administrative user and attempt to modify cryptographic key functionality. This will succeed as the user has sufficient privileges.<br>2. The audit logs will reflect this attempt. |
| **Expected Test Results** | 1. The TOE allows security administrator to modify any cryptographic key parameters.<br>2. The audit logs will reflect the failed attempt to modify cryptographic key parameters on the TOE. |
| **Pass/Fail with Explanation** | Pass - Security Administrator can perform security related configurations on the TOE. This meets the testing requirements. |

### 7.33 FMT_SMF.1 Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 1: The evaluator tests management functions as part of testing the SFRs identified in section 2.4.4. No separate testing for FMT_SMF.1 is required unless one of the management functions in FMT_SMF.1.1 has not already been exercised under any other SFR. |
| **Test Steps** | Pass – The management functions outlined in FMT_SMF.1.1 including their associated SFR's have been tested within other SFR's and are outlined below; there is no ability that has not bed tested within another test case/SFR:<br><br>The TSF shall be capable of performing the following management functions:<br>● Ability to administer the TOE locally and remotely; covered by **FMT_SMR.2.3**<br>● Ability to configure the access banner; covered by **FTA_TAB.1.1**<br>● Ability to configure the session inactivity time before session termination or locking; covered by **FTA_SSL.3**<br>● Ability to update the TOE, and to verify the updates using hash comparison capability prior to installing those updates; covered by **FPT_TST_EXT.1**<br>● Ability to configure the authentication failure parameters for FIA_AFL.1;<br>o Ability to manage the cryptographic keys; covered by **FMT_MTD.1**<br>○ Ability to configure the cryptographic functionality; covered by **FMT_MTD.1.1/CryptoKeys**<br>○ Ability to set the time which is used for time-stamps; covered by **FMT_MTD.1.1/CryptoKeys**<br>○ Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors; covered by **FIA_X509_EXT.1/Rev**<br>○ Ability to import X.509v3 certificates to the TOE's trust store; covered by **FIA_X509_EXT.1/Rev** |

| | |
|---|---|
| **Expected Test Results** | All management functions identified in section 2.4.4 have been tested throughout the evaluation. Thus, this requirement has been met. |
| **Pass/Fail with Explanation** | Pass. This test is performed in conjunction with other tests. |

### 7.34 FMT_SMR.2 Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 1: In the course of performing the testing activities for the evaluation, the evaluator shall use all supported interfaces, although it is not necessary to repeat each test involving an administrative action with each interface. The evaluator shall ensure, however, that each supported method of administering the TOE that conforms to the requirements of this cPP be tested; for instance, if the TOE can be administered through a local hardware interface; SSH; and TLS/HTTPS; then all three methods of administration must be exercised during the evaluation team's test activities. |
| **Test Steps** | This test is covered in below tests:<br>FIA_UIA_EXT.1 Test #2, FIA_UIA_EXT.1 Test #3, FTA_SSL_EXT.1.1 Test #1, FTA_SSL.3 Test #1, FTA_SSL.4 Test #1 and FTA_TAB.1 Test #1 |
| **Expected Test Results** | This test is covered in below tests:<br>FIA_UIA_EXT.1 Test #2, FIA_UIA_EXT.1 Test #3, FTA_SSL_EXT.1.1 Test #1, FTA_SSL.3 Test #1, FTA_SSL.4 Test #1 and FTA_TAB.1 Test #1 |
| **Pass/Fail with Explanation** | Pass: This test requirement has been performed in conjunction with other tests. |

### 7.35 FTA_SSL.3 Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 1: The evaluator follows the guidance documentation to configure several different values for the inactivity time period referenced in the component. For each period configured, the evaluator establishes a remote interactive session with the TOE. The evaluator then observes that the session is terminated after the configured time period. |
| **Test Steps** | 1. Log onto the TOE and configure a new idle time for one minute.<br>2. Log out of the TOE, then Log back into the TOE and wait one minute with no session activity.<br>3. Log out due to inactivity occurs and the evaluator will verify via audit logs.<br>4. Configure a new idle time for 5 minutes.<br>5. Log out of the TOE, then log back into the TOE and wait two minutes with no session activity.<br>6. Log out due to inactivity will occur and verified via audit logs.<br>7. Configure a new idle time for 20 minutes.<br>8. Log out of the TOE, then log back into the TOE and wait two minutes with no session activity. |

| | |
|---|---|
| | 9. Log out due to inactivity will occur and verified via audit logs. |
| **Expected Test Results** | 1. A new idle timeout period will be configured on the TOE.<br>2. The session will be inactive for 1 minutes.<br>3. The user will be logged out and an audit log will be created.<br>4. a new idle timeout period will be configured on the TOE.<br>5. The session will be inactive for 5 minutes.<br>6. The user will be logged out and an audit log will be created.<br>7. a new idle timeout period will be configured on the TOE.<br>8. The session will be inactive for 20 minutes.<br>9. The user will be logged out and an audit log will be created. |
| **Pass/Fail with Explanation** | Pass - The remote administrative time out periods can be set by the administrative user. The TOE enforces the configured inactivity period in each instance. This meets the testing requirements. |

### 7.36 FTA_SSL.4 Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 1: The evaluator initiates an interactive local session with the TOE. The evaluator then follows the guidance documentation to exit or log off the session and observes that the session has been terminated. |
| **Test Steps** | 1. Log onto the TOE through an administrative interface.<br>2. Log out of the TOE.<br>3. Verify that the audit logs reflect the login and logout activity. |
| **Expected Test Results** | 1. The evaluator will login to the TOE via console access.<br>2. The evaluator will log out of the TOE.<br>3. The appropriate audit logs will be created. |
| **Pass/Fail with Explanation** | Pass – Upon exiting the terminal after logging in, audit logs are generated indicating that the session has been terminated. |

### 7.37 FTA_SSL.4 Test #2

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 1: The evaluator initiates an interactive remote session with the TOE. The evaluator then follows the guidance documentation to exit or log off the session and observes that the session has been terminated. |
| **Test Steps** | 1. Log onto the TOE through an administrative interface.<br>2. Log out of the TOE.<br>3. Verify that the audit logs reflect the login and logout activity. |
| **Expected Test Results** | 1. The evaluator will login to the TOE.<br>2. The evaluator will log out of the TOE. |

| | |
|---|---|
| | 3. The appropriate audit logs will be created. |
| **Pass/Fail with Explanation** | Pass - Upon exiting the terminal after logging in, audit logs are generated indicating that the session has been terminated. |

### 7.38 FTA_SSL_EXT.1.1 Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 1: The evaluator follows the guidance documentation to configure several different values for the inactivity time period referenced in the component. For each period configured, the evaluator establishes a local interactive session with the TOE. The evaluator then observes that the session is either locked or terminated after the configured time period. If locking was selected from the component, the evaluator then ensures that reauthentication is needed when trying to unlock the session. |
| **Test Steps** | 1. Log onto the TOE locally and configure a new idle time for one minute.<br>2. Log out of the TOE, then Log back into the TOE and wait one minute with no session activity.<br>3. The user will be logged out due to inactivity and the evaluator will verify via audit logs.<br>4. Configure a new idle time for 2 minutes.<br>5. Log out of the TOE, then log back into the TOE and wait two minutes with no session activity.<br>6. Log out will be automatic due to inactivity and the evaluator will verify via audit logs.<br>7. Configure a new idle time for 20 minutes.<br>8. Log out of the TOE, then log back into the TOE and wait 20 minutes with no session activity.<br>9. Log out will be automatic due to inactivity and the evaluator will verify via audit logs. |
| **Expected Test Results** | 1. A new idle timeout period will be configured on the TOE while logged in locally.<br>2. The session will be inactive for 1 minutes.<br>3. The user will be logged out and an audit log will be created.<br>4. a new idle timeout period will be configured on the TOE.<br>5. The session will be inactive for 2 minutes.<br>6. The user will be logged out and an audit log will be created.<br>7. a new idle timeout period will be configured on the TOE.<br>8. The session will be inactive for 20 minutes.<br>9. The user will be logged out and an audit log will be created. |
| **Pass/Fail with Explanation** | Pass - The local administrative inactivity was able to be set to multiple values. In each instance, the TOE logged the user out after the configured time. This meets the testing requirements. |

### 7.39 FTA_TAB.1 Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 1: The evaluator follows the guidance documentation to configure a notice and consent warning message. The evaluator shall then, for each method of access specified in the TSS, establish a session with the TOE. The evaluator shall verify that the notice and consent warning message is displayed in each instance. |
| **Test Steps** | 1. Configure an access banner on the TOE.<br>2. Verify that the audit logs reflect the configuration of the access banner.<br>3. Log onto the TOE via SSH and ensure the access banner is present.<br>4. Log onto the TOE via console and ensure the access banner is present. |
| **Expected Test Results** | 1. The access banners will be configured properly.<br>2. The audit logs will show the configuration of the access banner.<br>3. The access banner will be displayed to the user when logging in via SSH.<br>4. The access banner will be displayed to the user when logging in via console. |
| **Pass/Fail with Explanation** | Pass - An access banner can be set for all the methods that can be used to access the device. This meets the testing requirements. |

### 7.40 FTP_TRP.1/Admin Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 1: The evaluators shall ensure that communications using each specified (in the guidance documentation) remote administration method is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful. |
| **Test Steps** | 1. Connect to the TOE as admin via SSH.<br>2. Verify connection supports claimed ciphers via Wireshark. |
| **Expected Test Results** | 1. The TOE will allow the session to connect.<br>2. The Wireshark capture will demonstrate a successful session capture of the claimed ciphers. |
| **Pass/Fail with Explanation** | Pass – The traffic capture demonstrates proper connectivity between the TOE and the SSH terminal window. |

### 7.41 FTP_TRP.1/Admin Test #2

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 2: The evaluator shall ensure, for each communication channel, the channel data is not sent in plaintext. |
| **Test Steps** | 1. Connect to the TOE via SSH.<br>2. Have Wireshark running, the capture will show a successful setup of the connection.<br>3. Verify that the TOE demonstrates that data is not sent in plaintext. |

| | |
|---|---|
| **Expected Test Results** | 1. The TOE will allow the session to connect.<br>2. The Wireshark capture will demonstrate a successful session capture.<br>3. The TOE will demonstrate that no data is sent in plain text. |
| **Pass/Fail with Explanation** | Pass – The traffic capture demonstrates proper connectivity between the TOE and the SSH terminal window. |

## 7.42 SSHC

### 7.43 FCS_SSHC_EXT.1.2 Test #1 (TD0636)

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 1: For each claimed public-key authentication method, the evaluator shall configure the TOE to present a public key corresponding to that authentication method (e.g., 2048-bit RSA key when using ssh-rsa public key). The evaluator shall establish sufficient separate SSH connections with an appropriately configured remote non-TOE SSH server to demonstrate the use of all claimed public key algorithms. It is sufficient to observe the successful completion of the SSH Authentication Protocol to satisfy the intent of this test. |
| **Test Steps** | **RSA-SHA2-256**<br>• Show the RSA-SHA2-256 public key generated on the TOE.<br>• Configure the TOE for RSA-SHA2-256.<br>• Reload the SSH tunnel so that it connects using RSA-SHA2-256.<br>• Verify the successful connection using TOE logs.<br>• A packet capture depicting that encrypted packets were sent after a successful session is established.<br><br>**ECDSA-SHA2-NISTP384**<br>• Show the ECDSA-SHA2-NISTP384 public key generated on the TOE.<br>• Configure the TOE for ECDSA-SHA2-NISTP384.<br>• Reload the SSH tunnel so that it connects using ECDSA-SHA2-NISTP384.<br>• Verify the successful connection using TOE logs.<br>• A packet capture depicting that encrypted packets were sent after a successful session is established. |

| | |
|---|---|
| **Expected Test Results** | • The TOE will successfully establish a connection with the SSH Server using the supported public key algorithms.<br>• Logs showing each successful authentication.<br>• Packet capture of **RSA-SHA2-256** session being established.<br>• Packet capture of **ECDSA-SHA2-NISTP384** session being established. |
| **Pass/Fail with Explanation** | Pass. The TOE can establish a successful SSH connection using the supported public key algorithm. This meets the testing requirements. |

### 7.44 FCS_SSHC_EXT.1.2 Test #2 (TD0636)

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 2: [Conditional] If password-based authentication method has been selected in the FCS_SSHC_EXT.1.2, then following the guidance documentation the evaluator shall configure the TOE to perform password-based authentication with a remote SSH server to demonstrate that the TOE can successfully authenticate using a password as an authentication method. |
| **Pass/Fail with Explanation** | N/A. The TOE only supports public-key based authentication. |

### 7.45 FCS_SSHC_EXT.1.3 Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 1: The evaluator shall demonstrate that if the TOE receives a packet larger than that specified in this component, that packet is dropped. |
| **Test Steps** | • Run the Acumen-tool to send a large packet.<br>• Attempt a connection from the TOE to the server via SSH and verify large packet being sent to the TOE by the server.<br>• Verify using packet capture that the packet is dropped. |
| **Expected Test Results** | • The TOE should drop a larger packet than the allowed range.<br>• Packet capture shows TOE closes the connection when packet sent is larger than allowed range. |
| **Pass/Fail with Explanation** | Pass. The TOE drops large packets that are received within an SSH session. This meets the testing requirements. |

### 7.46 FCS_SSHC_EXT.1.4 Test #1

| Item | Data |
|---|---|

| | |
|---|---|
| **Test Assurance Activity** | The evaluator must ensure that **only claimed ciphers and cryptographic primitives** are used to establish an SSH connection.<br>Test 1: To verify this, the evaluator shall start session establishment for an SSH connection **with a remote server** (referred to as 'remote endpoint' below). The evaluator shall capture the traffic exchanged between the TOE and the remote endpoint during protocol negotiation (e.g. using a packet capture tool or information provided by the endpoint, respectively). **The evaluator shall verify from the captured traffic that the TOE offers all the ciphers defined in the TSS for the TOE for SSH sessions, but no additional ones compared to the definition in the TSS.**<br>The evaluator shall perform one successful negotiation of an SSH session to verify that the TOE behaves as expected. It is sufficient to observe the successful negotiation of the session to satisfy the intent of the test. If the evaluator detects that not all ciphers defined in the TSS for SSH are supported by the TOE and/or the TOE supports one or more additional ciphers not defined in the TSS for SSH, the test shall be regarded as failed. |
| **Test Steps** | • Configure the TOE to use only claimed ciphers and cryptographic primitives to establish a SSH connection.<br>• Reload the SSH tunnel so that it connects using only claimed ciphers and cryptographic primitives.<br>• Verify the successful connection using device logs.<br>• Verify the successful connection using Packet capture. |
| **Expected Test Results** | • The TOE should support successful negotiations when using the claimed ciphersuites.<br>• Packet capture of a successful session being established using the claimed ciphersuites. |
| **Pass/Fail with Explanation** | Pass. The TOE is able to use each of the claimed algorithms for SSH connections. This meets the testing requirements. |

### 7.47 FCS_SSHC_EXT.1.5 Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 1: **The evaluator shall establish an SSH connection using each of the public key algorithms specified by the requirement to authenticate an SSH server to the TOE.**<br>It is sufficient to observe (on the wire) the **successful negotiation of the algorithm to satisfy the intent of the test**.<br>Test objective: The purpose of this positive test is to check the authentication of the server by the client (when establishing the transport layer connection), and not for checking generation of the authentication message from the client (in the User Authentication Protocol). The evaluator shall therefore establish sufficient separate SSH connections (with an appropriately configured server) to cause the TOE to demonstrate use of all public key algorithms claimed in FCS_SSHC_EXT.1.5 in the ST. |
| **Test Steps** | **RSA-SHA2-256:**<br>• Configure the SSH Server for the Host Key Algorithm as RSA-SHA2-256.<br>• Verify that RSA-SHA2-256 is configured as one of the supported Host Key Algorithms on the TOE.<br>• Reload the SSH tunnel so that it connects using RSA-SHA2-256.<br>• Verify the successful connection using TOE logs.<br>• Verify the successful connection using Packet capture. |

| | |
|---|---|
| | **ECDSA-SHA2-NISTP384:**<br>• Configure the SSH Server for the Host Key Algorithm as ECDSA-SHA2-NISTP384.<br>• Verify that ECDSA-SHA2-NISTP384 is configured as one of the supported Host Key Algorithms on the TOE.<br>• Reload the SSH tunnel so that it connects using ECDSA-SHA2-NISTP384.<br>• Verify the successful connection using TOE logs.<br>• Verify the successful connection using Packet capture. |
| **Expected Test Results** | • Evidence (screenshot or CLI output) of each type of key-based authentication being configured on the SSH server.<br>• Logs showing successful connection.<br>• Packet capture showing successful connection. |
| **Pass/Fail with Explanation** | Pass. The TOE establishes a successful SSH connection to authenticate the SSH server using each of the public key algorithms specified. This meets the testing requirements. |

### 7.48 FCS_SSHC_EXT.1.5 Test #2

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 2: The evaluator shall configure an SSH server to only allow a public key algorithm that is not included in the ST selection. The evaluator shall attempt to establish an SSH connection from the TOE to the SSH server and observe that the connection is rejected. |
| **Test Steps** | • Configure the SSH Server for the unsupported Public Key Algorithm.<br>• Verify the SSH configuration on the TOE.<br>• Reload the SSH tunnel on the TOE and verify the SSH tunnel fails to re-establish.<br>• Verify the unsuccessful connection using TOE logs.<br>• Verify the unsuccessful connection using Packet capture. |
| **Expected Test Results** | • Evidence (screenshot or CLI output) of the unsupported key-based authentication being configured on the SSH server.<br>• Logs showing unsuccessful connection.<br>• Packet capture showing unsuccessful connection. |
| **Pass/Fail with Explanation** | Pass. The TOE rejects the connection when an unsupported host key algorithm is configured on the Server. This meets the testing requirements. |

### 7.49 FCS_SSHC_EXT.1.6 Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | [conditional, if an **HMAC or AEAD_AES_*_GCM** algorithm is selected in the ST] Test 1: The evaluator shall establish an SSH connection using each of the algorithms, except “implicit”, specified by the requirement. |

| | |
|---|---|
| | It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.<br>Note: To ensure the observed algorithm is used, the evaluator shall ensure a non-aes*-gcm@openssh.com encryption algorithm is negotiated while performing this test. |
| **Test Steps** | **HMAC-SHA2-256**<br>• Configure the SSH Server to use HMAC-SHA2-256 as the supported algorithm.<br>• Verify that HMAC-SHA2-256 is configured as one of the supported algorithms on the TOE.<br>• Reload the SSH tunnel so that it connects using HMAC-SHA2-256.<br>• Verify the successful connection using TOE logs.<br>• Verify the successful connection using Packet capture.<br><br>**HMAC-SHA2-512**<br>• Configure the SSH Server to use HMAC-SHA2-512 as the supported algorithm.<br>• Verify that HMAC-SHA2-512 is configured as one of the supported algorithms on the TOE.<br>• Reload the SSH tunnel so that it connects using HMAC-SHA2-512.<br>• Verify the successful connection using TOE logs.<br>• Verify the successful connection using Packet capture. |
| **Expected Test Results** | • The TOE successfully establishes a SSH connection with the Server using the claimed MAC algorithms.<br>• Logs showing successful connection.<br>• Packet capture showing successful connection. |
| **Pass/Fail with Explanation** | Pass. The TOE is able to make SSH connections with each claimed data integrity algorithm. This meets the testing requirements. |

### 7.50 FCS_SSHC_EXT.1.6 Test #2

| Item | Data |
|---|---|
| **Test Assurance Activity** | [conditional, if an **HMAC or AEAD_AES_*_GCM** algorithm is selected in the ST] Test 2: The evaluator shall configure an SSH server to only allow a MAC algorithm that is not included in the ST selection. The evaluator shall attempt to connect from the TOE to the SSH server and observe that the attempt fails<br>Note: To ensure the proposed MAC algorithm is used, the evaluator shall ensure a non-aes*- gcm@openssh.com encryption algorithm is negotiated while performing this test. |
| **Test Steps** | • Configure TOE to use the supported HMAC algorithms as claimed by the ST.<br>• Configure the SSH Server to use the unsupported HMAC algorithm.<br>• Reload the SSH tunnel on the TOE and verify the SSH tunnel fails to re-establish.<br>• Verify the unsuccessful connection using TOE logs.<br>• Verify the unsuccessful connection using Packet capture. |
| **Expected Test Results** | • Evidence (screenshot or CLI output) of the unsupported HMCA algorithm being configured on the SSH server. |

| | |
|---|---|
| | • Logs showing unsuccessful connection.<br>• Packet capture showing unsuccessful connection. |
| **Pass/Fail with Explanation** | Pass. The TOE rejects a connection made to a Server that is configured to support an unsupported MAC algorithm. This meets the testing requirements. |

### 7.51 FCS_SSHC_EXT.1.7 Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 1: The evaluator shall configure an SSH server to permit all allowed key exchange methods. The evaluator shall attempt to connect from the TOE to the SSH server using each allowed key exchange method and observe that each attempt succeeds. |
| **Test Steps** | • Configure the SSH Server for the allowed key exchange method diffie-hellman-group14-sha1.<br>• Configure the TOE for the allowed key exchange method diffie-hellman-group14-sha1.<br>• Reload the SSH tunnel so that it connects using diffie-hellman-group14-sha1.<br>• Verify the successful connection using TOE logs.<br>• Verify the successful connection using Packet capture. |
| **Expected Test Results** | • Evidence (screenshot or CLI output) of allowed key exchange method being configured on the SSH server.<br>• Logs showing successful connection.<br>• Packet capture showing successful connection. |
| **Pass/Fail with Explanation** | Pass. The TOE is able to make SSH connections with the claimed data key exchange method. This meets the testing requirements. |

### 7.52 FCS_SSHC_EXT.1.8 Test #1t

| Item | Data |
|---|---|
| **Test Assurance Activity** | The evaluator needs to perform testing that rekeying is performed according to the description in the TSS. The evaluator shall test both, the time-based threshold and the traffic-based threshold.<br><br>For testing of the time-based threshold, the evaluator shall use the TOE to connect to an SSH server and keep the session open until the threshold is reached. The evaluator shall verify that the SSH session has been active longer than the threshold value and shall verify that the TOE initiated a rekey (the method of verification shall be reported by the evaluator).<br><br>Testing does not necessarily have to be performed with the threshold configured at the maximum allowed value of one hour of session time, but the value used for testing shall not exceed one hour. The evaluator needs to ensure that the rekeying has been initiated by the TOE and not by the SSH server the TOE is connected to. |

| | |
|---|---|
| | If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, the evaluator needs to verify that the threshold(s) can be configured as described in the guidance documentation and the evaluator needs to test that modification of the thresholds is restricted to Security Administrators (as required by FMT_MOF.1/Functions). |
| **Test Steps** | • Verify the configured rekey interval on the TOE.<br>• Run the Acumen-tool to for time based Rekey.<br>• Initiate a connection from the TOE and verify the rekey via debug logs. |
| **Expected Test Results** | • The TOE issues a rekey after the specified time as configured on the TOE.<br>• Audit logs show the Session rekey request been sent after time-based threshold has been reached. |
| **Pass/Fail with Explanation** | Pass. The TOE initiates a rekey every 1 hr. This meets the testing requirements. |

### 7.53 FCS_SSHC_EXT.1.8 Test #1b

| Item | Data |
|---|---|
| **Test Assurance Activity** | The evaluator needs to perform testing that rekeying is performed according to the description in the TSS. The evaluator shall test both, the time-based threshold and the **traffic-based** threshold.<br><br>For testing of the traffic-based threshold the evaluator shall use the TOE to connect to an SSH server and shall transmit data to and/or receive data from the TOE within the active SSH session until the threshold for data protected by either encryption key is reached. It is acceptable if the rekey occurs before the threshold is reached (e.g. because the traffic is counted according to one of the alternatives given in the Application Note for FCS_SSHC_EXT.1.8).<br><br>The evaluator shall verify that more data has been transmitted within the SSH session than the threshold allows and shall verify that the TOE initiated a rekey (the method of verification shall be reported by the evaluator).<br><br>Testing does not necessarily have to be performed with the threshold configured at the maximum allowed value of one gigabyte of transferred traffic, but the value used for testing shall not exceed one gigabyte. The evaluator needs to ensure that the rekeying has been initiated by the TOE and not by the SSH server the TOE is connected to.<br><br>If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, the evaluator needs to verify that the threshold(s) can be configured as described in the guidance documentation and the evaluator needs to test that modification of the thresholds is restricted to Security Administrators (as required by FMT_MOF.1/Functions).<br><br>In cases where data transfer threshold could not be reached due to hardware limitations it is acceptable to omit testing of this (SSH rekeying based on data transfer threshold) threshold if both the following conditions are met: |

| | |
|---|---|
| | a. An argument is present in the TSS section describing this hardware- based limitation and<br>b. All hardware components that are the basis of such argument are definitively identified in the ST. For example, if specific Ethernet Controller or WiFi radio chip is the root cause of such limitation, these chips must be identified. |
| **Test Steps** | • Verify the configured rekey frequency on the TOE.<br>• Run the Acumen-tool to generate 1GB data.<br>• Initiate a connection from the TOE and verify the rekey via debug logs. |
| **Expected Test Results** | • The traffic based/data transfer threshold limit for rekeying is set to 1GB.<br>• The rekeying will occur after the traffic threshold is met. |
| **Pass/Fail with Explanation** | Pass. The TOE initiates a rekey in every 1GB of data. This meets the testing requirements. |

### 7.54 FCS_SSHC_EXT.1.9 Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 1: The evaluator shall delete all entries in the TOE's list of recognized SSH server host keys and, if selected, all entries in the TOE's list of trusted certification authorities. The evaluator shall initiate a connection from the TOE to an SSH server. The evaluator shall ensure that the TOE either rejects the connection or displays the SSH server's public key (either the key bytes themselves or a hash of the key using any allowed hash algorithm) and prompts the Security Administrator to accept or deny the key before continuing the connection. |
| **Test Steps** | • Verify the SSH configuration on the TOE.<br>• Delete all know-host entries in the TOE's SSH configuration.<br>• Reload the SSH tunnel on the TOE and verify the SSH tunnel fails to re-establish.<br>• Verify the unsuccessful connection using TOE logs.<br>• Verify the unsuccessful connection using Packet capture. |
| **Expected Test Results** | • Remove all entries Know host entries from SSH configuration of the TOE.<br>• SSH connection attempt from TOE would be rejected. |
| **Pass/Fail with Explanation** | Pass. The TOE rejects the SSH connection when the host key of Server is not present. This meets the testing requirements. |

### 7.55 FCS_SSHC_EXT.1.9 Test #2

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 2: The evaluator shall add an entry associating a host name with a public key into the TOE's local database. The evaluator shall replace, on the corresponding SSH server, the server's host key with a different host key. |

| | |
|---|---|
| | If 'password-based' is selected for the TOE in FCS_SSHC_EXT.1.2, the evaluator shall initiate a connection from the TOE to the SSH server using password-based authentication, shall ensure that the TOE rejects the connection, and shall ensure that the password was not transmitted to the SSH server (for example, by instrumenting the SSH server with a debugging capability to output received passwords).<br>If 'password-based' is not selected for the TOE in FCS_SSHC_EXT.1.2, the evaluator shall initiate a connection from the TOE to the SSH server using public key-based authentication and shall ensure that the TOE rejects the connection. |
| **Test Steps** | • Verify the SSH configuration on the TOE.<br>• Verify the public key on the SSH server.<br>• Generate a new public key on the SSH server and do not import it over to the TOE.<br>• Reload the SSH tunnel on the TOE and verify the SSH tunnel fails to re-establish<br>• Verify the unsuccessful connection using TOE logs. |
| **Expected Test Results** | • The TOE should reject the connection to SSH server when there is a mismatch in the public key.<br>• Verify the failed connection using TOE logs. |
| **Pass/Fail with Explanation** | Pass. The TOE rejects the connection to the SSH server when there is a mismatch in the public key. This meets the testing requirements. |

### 7.56 SSHS

### 7.57 FCS_SSHS_EXT.1.2 Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 1: For each supported client public-key authentication algorithm, the evaluator shall configure a remote client to present a public key corresponding to that authentication method (e.g., 2048-bit RSA key when using ssh-rsa public key). The evaluator shall establish sufficient separate SSH connections with an appropriately configured remote non-TOE SSH client to demonstrate the use of all applicable public key algorithms. It is sufficient to observe the successful completion of the SSH Authentication Protocol to satisfy the intent of this test. |
| **Test Steps** | **RSA-SHA2-256**<br>• Generate the RSA key on the VM.<br>• Configure the TOE to support RSA based SSH authentication method.<br>• Log into the TOE SSH with RSA-based authentication.<br>• Verify the successful connection using logs on TOE. |

| | |
|---|---|
| | • Verify the successful connection using packet capture.<br><br>**ECDSA-SHA2-NISTP384**<br>• Generate the ECDSA key on the VM.<br>• Configure the TOE to support ECDSA based SSH authentication method.<br>• Log into the TOE SSH with ECDSA-based authentication.<br>• Verify the successful connection using logs on TOE.<br>• Verify the successful connection using packet capture. |
| **Expected Test Results** | • The TOE should support successful negotiations when using the claimed public key algorithms. |
| **Pass/Fail with Explanation** | Pass. The TOE accepts SSH connections with the claimed public key algorithm. This meets the testing requirements. |

### 7.58 FCS_SSHS_EXT.1.2 Test #2

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 2: The evaluator shall choose one client public key authentication algorithm supported by the TOE. The evaluator shall generate a new client key pair for that supported algorithm without configuring the TOE to recognize the associated public key for authentication. The evaluator shall use an SSH client to attempt to connect to the TOE with the new key pair and demonstrate that authentication fails. |
| **Test Steps** | • Configure the SSH client with a new RSA keypair for SSH without configuring the TOE and attempt to login using ssh-rsa key.<br>• Log into the TOE via SSH using RSA-based authentication.<br>• Verify authentication logs on TOE.<br>• Verify authentication failure via packet capture. |
| **Expected Test Results** | • The TOE should reject SSH connections when incorrect/unknown public keys are presented.<br>• Evidence (screenshot or CLI output) of attempting to authenticate the TOE.<br>• Packet capture of unsuccessful authentication.<br>• Log showing unsuccessful authentication. |

| | |
|---|---|
| **Pass/Fail with Explanation** | Pass. The TOE denied a connection with a remote SSH user when incorrect authentication credentials are presented. This meets the testing requirements. |

### 7.59 FCS_SSHS_EXT.1.2 Test #3

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 3: If password-based authentication method has been selected in the FCS_SSHS_EXT.1.2, the evaluator shall configure the TOE to accept password-based authentication and demonstrate that user authentication succeeds when the correct password is provided by the connecting SSH client. |
| **Test Steps** | • Ensure the TOE supports password-based authentication.<br>• Log into the TOE via SSH with password authentication.<br>• Verify using authentication logs on TOE.<br>• Verify wire capture that SSH session was established. |
| **Expected Test Results** | • The TOE should set up a user with password-based authentication.<br>• User authentication succeeds when the correct password is provided by the user. |
| **Pass/Fail with Explanation** | Pass. The TOE accepts Password authentication from a remote SSH client. This meets the testing requirements. |

### 7.60 FCS_SSHS_EXT.1.2 Test #4

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 4: If password-based authentication method has been selected in the FCS_SSHS_EXT.1.2, the evaluator shall configure the TOE to accept password-based authentication and demonstrate that user authentication fails when the incorrect password is provided by the connecting SSH client. |
| **Test Steps** | • Ensure the TOE supports password-based authentication.<br>• Attempt to Log into the TOE via SSH with correct username incorrect password-based authentication parameters (will fail).<br>• Verify authentication via logs that reflect failures.<br>• Verify authentication via packet captures that reflect failures. |
| **Expected Test Results** | • The TOE should set up a user with password-based authentication. |

| | |
|---|---|
| | • User authentication fails when the incorrect password is provided by the user. |
| **Pass/Fail with Explanation** | Pass. The TOE does not establish a connection with a remote SSH user when incorrect authentication credentials are presented. This meets the testing requirements. |

### 7.61 FCS_SSHS_EXT.1.3 Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | The evaluator shall demonstrate that if the TOE receives a packet larger than that specified in this component, that packet is dropped. |
| **Test Steps** | • Use SSHS tool to send bad length packet.<br>• Verify authentication logs reflect failures.<br>• Verify via packet capture. |
| **Expected Test Results** | • The TOE should drop packets larger than the allowed range.<br>• Log showing the reason for closing the connection.<br>• Packet capture showing TOE closes the connection when packet sent is larger than allowed range. |
| **Pass/Fail with Explanation** | Pass. The TOE drops large packets that are received within an SSH session. This meets the testing requirements. |

### 7.62 FCS_SSHS_EXT.1.4 Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | The evaluator must ensure that only claimed ciphers and cryptographic primitives are used to establish an SSH connection.<br>To verify this, the evaluator shall start session establishment for an SSH connection from a remote client (referred to as 'remote endpoint' below). The evaluator shall capture the traffic exchanged between the TOE and the remote endpoint during protocol negotiation (e.g. using a packet capture tool or information provided by the endpoint, respectively). The evaluator shall verify from the captured traffic that the TOE offers all the ciphers defined in the TSS for the TOE for SSH sessions, but no additional ones compared to the definition in the TSS. The evaluator shall perform one successful negotiation of an SSH session to verify that the TOE behaves as expected. It is sufficient to observe the successful negotiation of the session to satisfy the intent of the test. |

| | |
|---|---|
| | If the evaluator detects that not all ciphers defined in the TSS for SSH are supported by the TOE and/or the TOE supports one or more additional ciphers not defined in the TSS for SSH, the test shall be regarded as failed. |
| **Test Steps** | • Configure the TOE for SSH login using the aes-128-cbc & aes256-cbc encryption algorithm.<br>• Login to the TOE using the aes-128-cbc encryption algorithm.<br>• Verify the login via logs.<br>• Verify that the SSH session was encrypted using aes-128-cbc via packet capture.<br>• Login to the TOE using the aes-256-cbc encryption algorithm.<br>• Verify the login via logs.<br>• Verify that the SSH session was encrypted using aes-256-cbc via packet capture.<br>• Establish a SSH session with the unclaimed algorithms.<br>• Verify the failure via device log.<br>• Verify the failure via packet capture. |
| **Expected Test Results** | • The TOE should support successful negotiations when using the claimed ciphersuites (aes-128-cbc & aes256-cbc) and reject SSH connections when using a non-approved algorithm. |
| **Pass/Fail with Explanation** | Pass. The TOE accepts SSH connections with each claimed algorithm and The TOE rejects SSH connections using a non-approved algorithm. This meets the testing requirements. |

### 7.63 FCS_SSHS_EXT.1.5 Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 1: The evaluator shall configure (only if required by the TOE) the TOE to use each of the claimed host public key algorithms. The evaluator will then use an SSH client to confirm that the client can authenticate the TOE server public key using the claimed algorithm. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.<br><br>**TD0631 has been applied.** |
| **Test Steps** | • Login to the TOE using the host public key (rsa-sha2-256) and verify that the session is established.<br>• Verify via logs that the session was established. |

| | |
|---|---|
| | • Verify via packet capture that the configured host key algorithm was used.<br>• Login to the TOE using the host public key (ecdsa-sha2-nistp384) and verify that the session is established.<br>• Verify via logs that the session was established.<br>• Verify via packet capture that the configured host key algorithm was used. |
| **Expected Test Results** | • TOE logs show successful establishment of the SSH connection.<br>• Packet capture shows session establishment with the configured host key algorithm. |
| **Pass/Fail with Explanation** | Pass. The TOE establishes a successful SSH connection using each one of the claimed host public key algorithms. |

### 7.64 FCS_SSHS_EXT.1.5 Test #2

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 2: The evaluator shall configure a non-TOE SSH client to only allow it to authenticate an SSH server host public key algorithm that is not included in the ST selection. The evaluator shall attempt to establish an SSH connection from the non-TOE SSH client to the TOE SSH server and observe that the connection is rejected.<br><br>**TD0631 has been applied.** |
| **Test Steps** | • Attempt to establish a SSH session using the ssh-dss host public key algorithm.<br>• Verify that the SSH session was refused using ssh-dss via log.<br>• Verify that the connection is refused via packet capture. |
| **Expected Test Results** | • TOE logs verify connection establishment using an unsupported public key algorithm(ssh-dss) is denied by TOE.<br>• Packet Capture verifies connection establishment using an unsupported public key algorithm(ssh-dss) is denied by TOE. |
| **Pass/Fail with Explanation** | Pass. Toe rejects the connection if the session is established using a non-supported host key algorithm. This meets the testing requirement. |

### 7.65 FCS_SSHS_EXT.1.6 Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 1: [conditional, if an **HMAC or AEAD_AES_*_GCM** algorithm is selected in the ST] The evaluator shall establish an SSH connection using each of the algorithms, except "implicit", specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.<br><br>Note: To ensure the observed algorithm is used, the evaluator shall ensure a non-aes*-gcm@openssh.com encryption algorithm is negotiated while performing this test. |
| **Test Steps** | • Configure the TOE for SSH login using the configured supported algorithms hmac-sha2-256 & hmac-sha2-512.<br>• Attempt to establish an SSH session using hmac-sha2-256.<br>• Verify logs.<br>• Verify via packet capture.<br>• Attempt to establish an SSH session using hmac-sha2-512.<br>• Verify via logs.<br>• Verify via packet capture. |
| **Expected Test Results** | • The TOE must be able to make SSH connections with each claimed data integrity algorithm. |
| **Pass/Fail with Explanation** | Pass. The TOE makes SSH connections with each claimed data integrity algorithm. This meets the testing requirements. |

### 7.66 FCS_SSHS_EXT.1.6 Test #2

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 2: [conditional, if an **HMAC or AEAD_AES_*_GCM** algorithm is selected in the ST] The evaluator shall configure an SSH client to only allow a MAC algorithm that is not included in the ST selection. The evaluator shall attempt to connect from the SSH client to the TOE and observe that the attempt fails.<br><br>Note: To ensure the proposed MAC algorithm is used, the evaluator shall ensure a non-aes*-gcm@openssh.com encryption algorithm is negotiated while performing this test. |
| **Test Steps** | • Attempt to establish an SSH session using hmac-md5-96 mac. |

| | |
|---|---|
| | • Verify via logs on TOE.<br>• Verify via packet capture that the TOE does not continue negotiation. |
| **Expected Test Results** | • The TOE should reject unsupported mac algorithm while establishing SSH connection. |
| **Pass/Fail with Explanation** | Pass. The TOE rejects SSH connections using the unsupported MAC for data integrity. This meets the testing requirements. |

### 7.67 FCS_SSHS_EXT.1.7 Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | The evaluator shall configure an SSH client to only allow the diffie-hellman-group1-sha1 key exchange. The evaluator shall attempt to connect from the SSH client to the TOE and observe that the attempt fails. |
| **Test Steps** | • Attempt to establish an SSH session using diffiehellman-group1-sha1.<br>• Verify that the SSH session was refused via log.<br>• Verify the connection is refused via packet capture. |
| **Expected Test Results** | • The TOE should reject SSH connections when using a non-approved method. |
| **Pass/Fail with Explanation** | Pass. The TOE rejects SSH connections using diffiehellman-group1-sha1 (a non-approved algorithm) for key exchange. This meets the testing requirements. |

### 7.68 FCS_SSHS_EXT.1.7 Test #2

| Item | Data |
|---|---|
| **Test Assurance Activity** | For each allowed key exchange method, the evaluator shall configure an SSH client to only allow that method for key exchange, attempt to connect from the client to the TOE, and observe that the attempt succeeds. |
| **Test Steps** | • Establish an SSH session with the configured diffie-hellman-group14-sha1 key algorithms.<br>• Verify via the logs on TOE.<br>• Verify via the packet capture. |
| **Expected Test Results** | • The TOE should support successful negotiations when using the claimed key exchange method (diffiehellman-group14-sha1).<br>• Packet capture showing successful connection of each method. |

| | |
|---|---|
| **Pass/Fail with Explanation** | Pass. The TOE can use the claimed algorithm "diffie-hellman-group14-sha1" for SSH connection. This meets the testing requirements. |

### 7.69 FCS_SSHS_EXT.1.8 Test #1t

| Item | Data |
|---|---|
| **Test Assurance Activity** | The evaluator needs to perform testing that rekeying is performed according to the description in the TSS. The evaluator shall test both, the **time-based threshold** and the traffic-based threshold.<br><br>For testing of the time-based threshold, the evaluator shall use an SSH client to connect to the TOE and keep the session open until the threshold is reached. The evaluator shall verify that the SSH session has been active longer than the threshold value and shall verify that the TOE initiated a rekey (the method of verification shall be reported by the evaluator).<br><br>Testing does not necessarily have to be performed with the threshold configured at the maximum allowed value of one hour of session time but the value used for testing shall not exceed one hour. The evaluator needs to ensure that the rekeying has been initiated by the TOE and not by the SSH client that is connected to the TOE.<br><br>If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, the evaluator needs to verify that the threshold(s) can be configured as described in the guidance documentation and the evaluator needs to test that modification of the thresholds is restricted to Security Administrators (as required by FMT_MOF.1/Functions). |
| **Test Steps** | • Configure the TOE for SSH rekey with the time 10 minutes.<br>• Establish a SSH session with the TOE and keep it idle for 10 MINs<br>• Refer rekey logs on the TOE. |
| **Expected Test Results** | The TOE should issue a rekey after the specified time as configured on the TOE. |
| **Pass/Fail with Explanation** | Pass. TOE successfully rekeyed when the time limit was reached. This meets the testing requirements. |

### 7.70 FCS_SSHS_EXT.1.8 Test #1b

| Item | Data |
|---|---|
| **Test Assurance Activity** | The evaluator needs to perform testing that rekeying is performed according to the description in the TSS. The evaluator shall test both, the time-based threshold and the **traffic-based** threshold. |

| | |
|---|---|
| | For testing of the traffic-based threshold the evaluator shall use the TOE to connect to an SSH client and shall transmit data to and/or receive data from the TOE within the active SSH session until the threshold for data protected by either encryption key is reached. It is acceptable if the rekey occurs before the threshold is reached (e.g. because the traffic is counted according to one of the alternatives given in the Application Note for FCS_SSHS_EXT.1.8).<br><br>The evaluator shall verify that more data has been transmitted within the SSH session than the threshold allows and shall verify that the TOE initiated a rekey (the method of verification shall be reported by the evaluator).<br><br>Testing does not necessarily have to be performed with the threshold configured at the maximum allowed value of one gigabyte of transferred traffic but the value used for testing shall not exceed one gigabyte. The evaluator needs to ensure that the rekeying has been initiated by the TOE and not by the SSH client that is connected to the TOE.<br><br>If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, the evaluator needs to verify that the threshold(s) can be configured as described in the guidance documentation and the evaluator needs to test that modification of the thresholds is restricted to Security Administrators (as required by FMT_MOF.1/Functions).<br><br>In cases where data transfer threshold could not be reached due to hardware limitations it is acceptable to omit testing of this (SSH rekeying based on data transfer threshold) threshold if both the following conditions are met:<br><br>a. An argument is present in the TSS section describing this hardware- based limitation and<br>b. All hardware components that are the basis of such argument are definitively identified in the ST. For example, if specific Ethernet Controller or WiFi radio chip is the root cause of such limitation, these chips must be identified. |
| **Test Steps** | • Configuring the SSH REKEY with the Time 10 MIN and volume 100 KB.<br>• Establish a SSH session with the TOE and continually send traffic.<br>• Logging Details for Rekey based on volume. |
| **Expected Test Results** | • Evidence (screenshot or CLI output) showing configuration of rekey for time and volume threshold.<br>• Log showing session rekey request being sent after time-based and volume-based threshold has been reached. |
| **Pass/Fail with Explanation** | Pass. The TOE initiates a rekey after 100 KB data traffic. This meets the testing requirements. |

### 7.71 TLSS

### 7.72 FCS_TLSS_EXT.1.1 Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | **Test 1:** The evaluator shall 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 HTTPS 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 to discern the cipher suite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES). |
| **Test Steps** | • Show the configuration on the TOE for the list of available ciphers for TLS connection.<br>• Establish a connection with the TOE over TLS using the cipher suite TLS_RSA_WITH_AES_128_CBC_SHA256.<br>• Verify the required cipher suite with packet capture.<br>• Establish a connection with the TOE over TLS using the cipher suite TLS_RSA_WITH_AES_256_CBC_SHA256.<br>• Verify the required cipher suite with packet capture.<br>• Establish a connection with the TOE over TLS using the cipher suite TLS_DHE_RSA_WITH_AES_128_CBC_SHA256.<br>• Verify the required cipher suite with packet capture.<br>• Establish a connection with the TOE over TLS using the cipher suite TLS_DHE_RSA_WITH_AES_256_CBC_SHA256.<br>• Verify the required cipher suite with packet capture.<br>• Establish a connection with the TOE over TLS using the cipher suite TLS_RSA_WITH_AES_256_GCM_SHA384.<br>• Verify the required cipher suite with packet capture.<br>• Establish a connection with the TOE over TLS using the cipher suite TLS_DHE_RSA_WITH_AES_256_GCM_SHA348.<br>• Verify the required cipher suite with packet capture. |
| **Expected Test Results** | • Connection should be successfully established when supported cipher suite is used.<br>• Packet capture showing successful negotiation with supported cipher suites. |
| **Pass/Fail with Explanation** | Pass. The TOE successfully established each connection using all supported cipher suites, thereby meeting the testing requirements. |

### 7.73 FCS_TLSS_EXT.1.1 Test #2

| Item | Data |
|---|---|

| | |
|---|---|
| **Test Assurance Activity** | Test 2: The evaluator shall send a Client Hello to the server with a list of cipher suites that does not contain any of the cipher suites in the server's ST and verify that the server denies the connection. Additionally, the evaluator shall send a Client Hello to the server containing only the TLS_NULL_WITH_NULL_NULL cipher suite and verify that the server denies the connection. |
| **Test Steps** | • Attempt to establish a connection to the TOE using the Acumen-TLSS tool and verify that the connection fails with the non-supported cipher suite TLS_RSA_WITH_NULL_MD5.<br>• Verify the unsuccessful connection by checking the TOE's event logs.<br>• Verify the unsuccessful connection via packet capture.<br>• Attempt to establish a connection to the TOE using the Acumen-TLSS tool and verify that the connection fails with the non-supported cipher suite TLS_NULL_WITH_NULL_NULL.<br>• Verify the unsuccessful connection by checking the TOE's event logs.<br>• Verify the unsuccessful connection via packet capture. |
| **Expected Test Results** | • Connection should be rejected when the unsupported cipher suite is present.<br>• Packet capture shows handshake failure with unsupported cipher suites.<br>• Failure logs on TOE showing failure due to no shared cipher. |
| **Pass/Fail with Explanation** | Pass. The TOE successfully rejects TLS connections with unsupported cipher suites, thereby fulfilling the testing requirement. |

### 7.74 FCS_TLSS_EXT.1.1 Test #3a

| Item | Data |
|---|---|
| **Test Assurance Activity** | Modify a byte in the Client Finished handshake message and verify that the server rejects the connection and does not send any application data. |
| **Test Steps** | • Run the Acumen-TLSS tool with a modified client finished message and wait for the connection to establish. The connection should fail.<br>• Verify the failure logs on the device, which should indicate that the failure was due to a failed digest check.<br>• Verify the packet capture to identify the unsuccessful connection. |
| **Expected Test Results** | • TOE should reject a connection when byte in client finished handshake message is modified.<br>• Packet capture should show connection failure when message is modified.<br>• TOE logs show digest check error during handshake. |

| | |
|---|---|
| **Pass/Fail with Explanation** | Pass. The TOE rejects the connection after receiving the modified Client Handshake message. This meets the test requirements |

### 7.75 FCS_TLSS_EXT.1.1 Test #3b

| Item | Data |
|---|---|
| **Test Assurance Activity** | (Test Intent: The intent of this test is to ensure that the server's TLS implementation immediately makes use of the key exchange and authentication algorithms to: a) Correctly encrypt (D)TLS Finished message and b) Encrypt every (D)TLS message after session keys are negotiated.)<br><br>The evaluator shall use one of the claimed cipher suites to complete a successful handshake and observe transmission of properly encrypted application data.<br>The evaluator shall verify that no Alert with alert level Fatal (2) messages were sent.<br>The evaluator shall verify that the Finished message (Content type hexadecimal 16 and handshake message type hexadecimal 14) is sent immediately after the server's ChangeCipherSpec (Content type hexadecimal 14) message.<br>The evaluator shall examine the Finished message (encrypted example in hexadecimal of a TLS record containing a Finished message, 16 03 03 00 40 11 22 33 44 55...) and confirm that it does not contain unencrypted data (unencrypted example in hexadecimal of a TLS record containing a Finished message, 16 03 03 00 40 14 00 00 0c...), by verifying that the first byte of the encrypted Finished message does not equal hexadecimal 14 for at least one of three test messages.<br><br>There is a chance that an encrypted Finished message contains a hexadecimal value of '14' at the position where a plaintext Finished message would contain the message type code '14'. If the observed Finished message contains a hexadecimal value of '14' at the position where the plaintext Finished message would contain the message type code, the test shall be repeated three times in total. In case the value of '14' can be observed in all three tests it can be assumed that the Finished message has indeed been sent in plaintext and the test has to be regarded as 'failed'. Otherwise it has to be assumed that the observation of the value '14' has been due to chance and that the Finished message has indeed been sent encrypted. In that latter case the test shall be regarded as 'passed'. |
| **Test Steps** | • Initiate a connection to the TOE via Acumen-TLSS from the evaluator machine.<br>• Verify the connection using device logs.<br>• Verify via packet capture that the Finished message was sent after the ChangeCipherSpec message. |
| **Expected Test Results** | • Evidence (Packet capture) showing message is encrypted hence the connection is successful. |
| **Pass/Fail with Explanation** | Pass. the TLS server's implementation immediately makes use of the key exchange and authentication algorithms to correctly encrypt TLS Finished message and encrypt every LS message after session keys are negotiated. This meets the testing requirement. |

| | |
|---|---|
| | |

### 7.76 FCS_TLSS_EXT.1.2 Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | The evaluator shall send a Client Hello requesting a connection for all mandatory and selected protocol versions in the SFR (e.g. by enumeration of protocol versions in a test client) and verify that the server denies the connection for each attempt. |
| **Test Steps** | • Use the Acumen-TLSS tool to initiate a connection to the TOE and verify the connections fails for all the unsupported SSL and TLS versions.<br>• Verify the connection fails with SSLv2.0 via device logs.<br>• Verify failure using packet capture.<br>• Verify the connection fails with SSLv3.0 via device logs.<br>• Verify failure using packet capture.<br>• Verify the connection fails with TLSv1.0 via device logs.<br>• Verify failure using packet capture.<br>• Verify the connection fails with TLSv1.1 via device logs.<br>• Verify failure using packet capture. |
| **Expected Test Results** | • Server should reject a connection when a client requests a connection with unsupported TLS/SSL versions.<br>• TOE logs should show connection failure due to an unknown protocol.<br>• Packet capture should show connection reset for unsupported TLS/SSL versions. |
| **Pass/Fail with Explanation** | Pass. The TOE rejects all SSLv2, SSLv3, TLS v1.0 and TLS v1.1 connection attempts. This meets the testing requirement. |

### 7.77 FCS_TLSS_EXT.1.3 Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 1: [conditional] If ECDHE ciphersuites are supported:<br>a) The evaluator shall repeat this test for each supported elliptic curve. The evaluator shall attempt a connection using a supported ECDHE ciphersuite and a single supported elliptic curve specified in the Elliptic Curves Extension. The Evaluator shall verify |

| | |
|---|---|
| | (though a packet capture or instrumented client) that the TOE selects the same curve in the Server Key Exchange message and successfully establishes the connection.<br>b) The evaluator shall attempt a connection using a supported ECDHE ciphersuite and a single unsupported elliptic curve (e.g. secp192r1 (0x13)) specified in RFC4492, chap. 5.1.1. The evaluator shall verify that the TOE does not send a Serv |
| **Pass/Fail with Explanation** | N/A. The toe does not support ECDHE ciphersuites. |

### 7.78 FCS_TLSS_EXT.1.3 Test #2

| Item | Data |
|---|---|
| **Test Assurance Activity** | If **DHE cipher suites** are supported, the evaluator shall repeat the following test for each supported parameter size. If any configuration is necessary, the evaluator shall configure the TOE to use a supported Diffie-Hellman parameter size. The evaluator shall attempt a connection using a supported DHE cipher suite. The evaluator shall verify (through a packet capture or instrumented client) that the TOE sends a Server Key Exchange Message where p Length is consistent with the message are the ones configured Diffie-Hellman parameter size(s). |
| **Test Steps** | • Configure the TOE for using DHE 2048 for connectivity.<br>• Connect to the TOE using DHE 2048 bits and verify that it is successful.<br>• Packet capture depicts the successful connection.<br>• Configure the TOE for using DHE 3072 for connectivity.<br>• Connect to the TOE using DHE 3072 bits and verify that it is successful.<br>• Packet capture depicts the successful connection.<br>• Configure the TOE for using DHE 4096 for connectivity.<br>• Connect to the TOE using DHE 4096 bits and verify that it is successful.<br>• Packet capture depicts the successful connection. |
| **Expected Test Results** | • The TOE will be configured to allow or deny encrypted traffic to a client using a supported DHE cipher suite.<br>• Evidence (screenshot or CLI output) showing initiation of encrypted traffic.<br>• Packet capture showing the encrypted traffic and Client Hello details while attempting to make connection. |
| **Pass/Fail with Explanation** | Pass. The TOE was able to establish the connection using each supported Diffie-Hellman parameter size. This meets the testing requirements. |

### 7.79 FCS_TLSS_EXT.1.3 Test #3

| Item | Data |
|---|---|
| **Test Assurance Activity** | If **RSA key establishment cipher suites** are supported, the evaluator shall repeat this test for each RSA key establishment key size. If any configuration is necessary, the evaluator shall configure the TOE to perform RSA key establishment using a supported key size (e.g. by loading a certificate with the appropriate key size). The evaluator shall attempt a connection using a supported RSA key establishment cipher suite. The evaluator shall verify (through a packet capture or instrumented client) that the TOE sends a certificate whose modulus is consistent with the configured RSA key size. |
| **Test Steps** | • Connect to the TOE using RSA 2048 bit key and verify that it is successful.<br>• Verify that a connection is established with packet capture. |
| **Expected Test Results** | • The RSA key size used should match with the configured size and the connection should be established successfully.<br>• Evidence (Packet capture) showing RSA key size in modulus format. |
| **Pass/Fail with Explanation** | Pass. The TOE was able to establish the connection using the supported RSA key size of 2048 bits. This meets the testing requirements. |

### 7.80 FCS_TLSS_EXT.1.4 Test #1 (TD0569)

| Item | Data |
|---|---|
| **Test Assurance Activity** | If the **TOE does not support session resumption based on session IDs according to RFC4346 (TLS1.1) or RFC5246 (TLS1.2) or session tickets according to RFC5077**, the evaluator shall perform the following test:<br>a) The client sends a Client Hello with a zero-length session identifier and with a SessionTicket extension containing a zero-length ticket.<br>b) The client verifies the server does not send a NewSessionTicket handshake message (at any point in the handshake).<br>c) The client verifies the Server Hello message contains a zero-length session identifier or passes the following steps:<br><br>Note: The following steps are only performed if the ServerHello message contains a non-zero length SessionID.<br>d) The client completes the TLS handshake and captures the SessionID from the ServerHello.<br>e) The client sends a ClientHello containing the SessionID captured in step d). This can be done by keeping the TLS session in step d) open or start a new TLS session using the SessionID captured in step d).<br>f) The client verifies the TOE:<br>a. implicitly rejects the SessionID by sending a ServerHello containing a different SessionID and by performing a full handshake (as shown in Figure 1 of RFC 4346 or RFC 5246), or<br>b. terminates the connection in some way that prevents the flow of application data. |

| | |
|---|---|
| | Remark: If multiple contexts are supported for session resumption, the session ID or session ticket may be obtained in one context for resumption in another context. It is possible that one or more contexts may only permit the construction of sessions to be reused in other contexts but not actually permit resumption themselves. For contexts which do not permit resumption, the evaluator is required to verify this behaviour subject to the description provided in the TSS. It is not mandated that the session establishment and session resumption share context. For example, it is acceptable for a control channel to establish and application channel to resume the session. |
| **Test Steps** | N/A, TOE supports session resumption based on session IDs according to RFC5246 (TLS1.2) |
| **Pass/Fail with Explanation** | Pass |

### 7.81 FCS_TLSS_EXT.1.4 Test #2a (TD0569)

| Item | Data |
|---|---|
| **Test Assurance Activity** | If the **TOE supports session resumption using session IDs according to RFC4346 (TLS1.1) or RFC5246 (TLS1.2)**, the evaluator shall carry out the following steps (note that for each of these tests, it is not necessary to perform the test case for each supported version of TLS):<br>The evaluator shall conduct a successful handshake and capture the TOE-generated session ID in the Server Hello message. The evaluator shall then initiate a new TLS connection and send the previously captured session ID to show that the TOE resumed the previous session by responding with ServerHello containing the same SessionID immediately followed by ChangeCipherSpec and Finished messages (as shown in Figure 2 of RFC 4346 or RFC 5246). |
| **Test Steps** | • Use Acumen-TLSS tool to connect to the TOE<br>• Verify a successful connection using packet capture. |
| **Expected Test Results** | • Packet capture screenshot showing initial connection with session ID<br>• Packet capture screenshot showing re-connection using same session ID.<br>• The toe will initial a complete handshake |
| **Pass/Fail with Explanation** | Pass - The TOE supports session resumption using session IDs according to RFC5246 (TLS1.2) by responding with ServerHello containing the same SessionID immediately followed by ChangeCipherSpec and Finished messages. |

### 7.82 FCS_TLSS_EXT.1.4 Test #2b (TD0569)

| Item | Data |
|---|---|
| **Test Assurance Activity** | If the **TOE supports session resumption using session IDs according to RFC4346 (TLS1.1) or RFC5246 (TLS1.2)**, the evaluator shall carry out the following steps (note that for each of these tests, it is not necessary to perform the test case for each supported version of TLS): |

| | |
|---|---|
| | The evaluator shall initiate a handshake and capture the TOE-generated session ID in the Server Hello message. The evaluator shall then, within the same handshake, generate or force an unencrypted fatal Alert message immediately before the client would otherwise send its ChangeCipherSpec message thereby disrupting the handshake.<br>The evaluator shall then initiate a new Client Hello using the previously captured session ID, and verify that the server (1) implicitly rejects the session ID by sending a ServerHello containing a different SessionID and performing a full handshake (as shown in figure 1 of RFC 4346 or RFC 5246), or (2) terminates the connection in some way that prevents the flow of application data. |
| **Test Steps** | • Use the Acumen-TLSS tool to connect to the TOE.<br>• Verify the session connection using the device logs.<br>• Verify the session connection using the packet capture. |
| **Expected Test Results** | • Packet capture screenshot of New Session ID sent by the server during the first handshake.<br>• Packet capture screenshot shows Fatal Handshake Failure message error.<br>• Packet capture screenshot shows that client has chosen the previously captured session ID for re-connection.<br>• Packet capture Screenshot shows that the server has implicitly rejected the session ID by sending a ServerHello containing a different SessionID and performing a full handshake. |
| **Pass/Fail with Explanation** | Pass - The TOE supports session resumption using session IDs according to RFC5246 (TLS1.2) by verifying that the TOE implicitly rejects the session ID by sending a ServerHello containing a different SessionID and performing a full handshake. |

### 7.83 FCS_TLSS_EXT.1.4 Test #3 (TD0569)

| Item | Data |
|---|---|
| **Test Assurance Activity** | If the **TOE supports session tickets according to RFC5077**, the evaluator shall carry out the following steps (note that for each of these tests, it is not necessary to perform the test case for each supported version of TLS):<br><br>a) The evaluator shall permit a successful TLS handshake to occur in which a session ticket is exchanged with the non-TOE client. The evaluator shall then attempt to correctly reuse the previous session by sending the session ticket in the ClientHello. The evaluator shall confirm that the TOE responds with an abbreviated handshake described in section 3.1 of RFC 5077 and illustrated with an example in figure 2. Of particular note: if the server successfully verifies the client's ticket, then it may renew the ticket by including a NewSessionTicket handshake message after the ServerHello in the abbreviated handshake (which is shown in figure 2). This is not required, however as further clarified in section 3.3 of RFC 5077. |

| | |
|---|---|
| | b) The evaluator shall permit a successful TLS handshake to occur in which a session ticket is exchanged with the non-TOE client. The evaluator will then modify the session ticket and send it as part of a new Client Hello message. The evaluator shall confirm that the TOE either (1) implicitly rejects the session ticket by performing a full handshake (as shown in figure 3 or 4 of RFC 5077), or (2) terminates the connection in some way that prevents the flow of application data.<br><br>Remark: If multiple contexts are supported for session resumption, for each of the above test cases, the session ticket may be obtained in one context for resumption in another context. There is no requirement that the session ticket be obtained and replayed within the same context subject to the description provided in the TSS. All contexts that can reuse a session ticket constructed in another context must be tested. It is not mandated that the session establishment and session resumption share context. For example, it is acceptable for a control channel to establish and application channel to resume the session. |
| **Test Steps** | N/A, TOE supports session resumption based on session IDs according to RFC5246 (TLS1.2) |
| **Pass/Fail with Explanation** | Pass |

### 7.84 TLSS-MA

### 7.85 FCS_TLSS_EXT.2.1&2 Test #1a

| Item | Data |
|---|---|
| **Test Assurance Activity** | If the **TOE requires or can be configured to require a client certificate**, the evaluator shall configure the TOE to require a client certificate and send a Certificate Request to the client. The evaluator shall attempt a connection while sending a certificate_list structure with a length of zero in the Client Certificate message. The evaluator shall verify that the handshake is not finished successfully and no application data flows. |
| **Test Steps** | • Configure the TOE for a valid ssl profile.<br>• Using AcumenTLSS tool, attempt a connection between the TOE and eAPI Client using an empty certificate_list.<br>• Verify the unsuccessful connection using device logs.<br>• Verify the unsuccessful connection using Packet capture. |
| **Expected Test Results** | • Logs showing unsuccessful connection.<br>• Packet capture showing unsuccessful connection. |

| | |
|---|---|
| **Pass/Fail with Explanation** | Pass. The TOE rejects the connection when the client tries to connect with a certificate list structure of zero length. This satisfies the testing requirement. |

### 7.86 FCS_TLSS_EXT.2.1&2 Test #1b

| Item | Data |
|---|---|
| **Test Assurance Activity** | If the TOE supports fallback authentication functions and these functions cannot be disabled. The evaluator shall configure the fallback authentication functions on the TOE and configure the TOE to send a Certificate Request to the client. The evaluator shall attempt a connection while sending a certificate_list structure with a length of zero in the Client Certificate message. The evaluator shall verify the TOE authenticates the connection using the fallback authentication functions as described in the TSS. |
| **Test Steps** | • Configure the TOE for a valid ssl profile.<br>• Configure a new user (eAPIAdmin1) along with password on the TOE.<br>• Attempt to establish a connection between the TOE and eAPI Client using above created user eAPIAdmin1 credentials.<br>• Verify the successful connection using device logs.<br>• Verify the successful connection using Packet capture. |
| **Expected Test Results** | • Initiate a connection using username and password instead of the certificates.<br>• Logs showing successful connection.<br>• Packet capture showing successful connection. |
| **Pass/Fail with Explanation** | Pass. The TOE authenticates the connection using the fallback authentication function. This satisfies the testing requirement. |

### 7.87 FCS_TLSS_EXT.2.1&2 Test #2

| Item | Data |
|---|---|
| **Test Assurance Activity** | [conditional] If **TLS 1.2 is claimed for the TOE**, the evaluator shall configure the server to send a certificate request to the client without the supported_signature_algorithm used by the client's certificate. The evaluator shall attempt a connection using the client certificate and verify that the connection is denied. |
| **Test Steps** | • Create an eAPIclient Certificate without the supported_signature_algorithm.<br>• Using AcumenTLSS tool, attempt a connection between the TOE and eAPI Client using the above created certificate.<br>• Verify the unsuccessful connection using device logs.<br>• Verify the unsuccessful connection using Packet capture. |

| | |
|---|---|
| **Expected Test Results** | • TOE should reject a connection when supplied with an eAPIclient Certificate without the supported_signature_algorithm .<br>• Logs showing unsuccessful connection.<br>• Packet capture showing unsuccessful connection. |
| **Pass/Fail with Explanation** | Pass. The TOE rejects mutually authenticated TLS connection attempt from a client containing an unsupported signature algorithm. This meets testing requirements. |

### 7.88 FCS_TLSS_EXT.2.1&2 Test #3

| Item | Data |
|---|---|
| **Test Assurance Activity** | The aim of this test is to check the response of the server when it receives a client identity certificate that is signed by an impostor CA (either Root CA or intermediate CA).<br>To carry out this test the evaluator shall configure the client to send a client identity certificate with an issuer field that identifies a CA recognised by the TOE as a trusted CA, but where the key used for the signature on the client certificate does not correspond to the CA certificate trusted by the TOE (meaning that the client certificate is invalid because its certification path does not terminate in the claimed CA certificate).<br>The evaluator shall verify that the attempted connection is denied. |
| **Test Steps** | • Create an eAPIclient certificate using cert signed by an Imposter ICA.<br>• Establish a connection between the TOE and eAPI Client using the above created client certificate.<br>• Verify the unsuccessful connection using device logs.<br>• Verify the unsuccessful connection using Packet capture. |
| **Expected Test Results** | • TOE should reject a connection when supplied with an eAPIclient certificate using cert signed by an Imposter ICA.<br>• Log showing unsuccessful connection.<br>• Packet capture showing unsuccessful connection. |
| **Pass/Fail with Explanation** | Pass. TOE rejects the connection with the client certificate that is signed with wrong key. This meets the testing requirements. |

### 7.89 FCS_TLSS_EXT.2.1&2 Test #4

| Item | Data |
|---|---|
| **Test Assurance Activity** | The evaluator shall configure the client to send a certificate with the Client Authentication purpose in the extendedKeyUsage field and verify that the server accepts the attempted connection. The evaluator shall repeat this test |

| | |
|---|---|
| | without the Client Authentication purpose and shall verify that the server denies the connection. Ideally, the two certificates should be identical except for the Client Authentication purpose. |
| **Test Steps** | • Create an eAPIclient certificate with Client authentication purpose.<br>• Establish a connection between the TOE and eAPI Client using the above created client certificate.<br>• Verify the successful connection using device logs.<br>• Verify the successful connection using Packet capture.<br>• Create an eAPIclient certificate without the Client Authentication purpose in the extendedKeyUsage extension.<br>• Establish a connection between the TOE and eAPI Client using the above created client certificate.<br>• Verify the unsuccessful connection using device logs.<br>• Verify the unsuccessful connection using Packet capture. |
| **Expected Test Results** | • Connection establishes successfully when eAPIclient certificate is supplied with Client authentication purpose.<br>• Log showing successful connection.<br>• Packet capture showing successful connection.<br>• Connection fails when eAPIclient certificate is supplied without the Client authentication purpose.<br>• Log showing unsuccessful connection.<br>• Packet capture showing unsuccessful connection. |
| **Pass/Fail with Explanation** | Pass. The TOE does not make the connection because the evaluation of the extendedkeyusage field fails. This meets the testing requirements. |

### 7.90 FCS_TLSS_EXT.2.1&2 Test #5a

| Item | Data |
|---|---|
| **Test Assurance Activity** | Configure the server to require mutual authentication and then connect to the server with a client configured to send a client certificate that is signed by a Certificate Authority trusted by the TOE. The evaluator shall verify that the server accepts the connection. |
| **Test Steps** | • Configure the TOE for a valid ssl profile.<br>• Establish connection between the TOE and eAPI Client.<br>• Verify the successful connection using device logs.<br>• Verify the successful connection using Packet capture. |
| **Expected Test Results** | • The TOE accept connection using the server certificate which is signed by the trusted CA. |

| | |
|---|---|
| | • Log showing successful connection.<br>• Packet capture showing successful connection. |
| **Pass/Fail with Explanation** | Pass. The TOE accept connection using the server certificate which is signed by the trusted CA of the TOE. This meets the testing requirements. |

### 7.91 FCS_TLSS_EXT.2.1&2 Test #5b

| Item | Data |
|---|---|
| **Test Assurance Activity** | Configure the server to require mutual authentication and then modify a byte in the signature block of the client's Certificate Verify handshake message (see RFC5246 Sec 7.4.8). The evaluator shall verify that the server rejects the connection. |
| **Test Steps** | • Run the AcumenTLSS tool to attempt a TLS connection with the TOE and Modify a byte in the signature block of the client's Certificate.<br>• Verify the unsuccessful connection using device logs.<br>• Verify the unsuccessful connection using Packet capture. |
| **Expected Test Results** | • TOE should reject a connection when a byte in the signature block of the client's Certificate is modified.<br>• Logs showing unsuccessful connection.<br>• Packet capture showing unsuccessful connection. |
| **Pass/Fail with Explanation** | Pass. The evaluator verified that the server rejects the connection to the client that has a byte modified in the signature block of the client's Certificate Verify handshake message. This meets the testing requirements. |

### 7.92 FCS_TLSS_EXT.2.1&2 Test #6

| Item | Data |
|---|---|
| **Test Assurance Activity** | Using the administrative guidance, the evaluator shall load a CA certificate or certificates needed to validate the presented certificate used to authenticate an external entity and demonstrate that the function succeeds, and a trusted channel can be established. |
| **Pass/Fail with Explanation** | Pass. This test is performed in conjunction with the FIA_X509_EXT.1.1/Rev Test #1a Tests. This meets the testing requirements. |

### 7.93 FCS_TLSS_EXT.2.1&2 Test #7

| Item | Data |
|---|---|
| **Test Assurance Activity** | The evaluator shall then change the presented certificate(s) so that validation fails and show that the certificate is not automatically accepted. The evaluator shall repeat this test to cover the selected types of failure defined in the SFR (i.e. the selected ones from failed matching of the reference identifier, failed validation of the certificate path, failed validation of |

| | |
|---|---|
| | the expiration date, failed determination of the revocation status). The evaluator performs the action indicated in the SFR selection observing the TSF resulting in the expected state for the trusted channel (e.g. trusted channel was established) covering the types of failure for which an override mechanism is defined. |
| **Pass/Fail with Explanation** | Pass. This test is performed in conjunction with the FIA_X509_EXT.1.1/Rev Tests. This meets the testing requirements. |

### 7.94 FCS_TLSS_EXT.2.1&2 Test #8

| Item | Data |
|---|---|
| **Test Assurance Activity** | The purpose of this test is to verify that only selected certificate validation failures could be administratively overridden. **If any override mechanism is defined for failed certificate validation**, the evaluator shall configure a new presented certificate that does not contain a valid entry in one of the mandatory fields or parameters (e.g. inappropriate value in extendedKeyUsage field) but is otherwise valid and signed by a trusted CA.<br>The evaluator shall confirm that the certificate validation fails (i.e. certificate is rejected), and there is no administrative override available to accept such certificate. |
| **Pass/Fail with Explanation** | N/A. SFR does not select any administrator override methods. |

### 7.95 FCS_TLSS_EXT.2.3 Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | The evaluator shall send a client certificate with an identifier that does not match an expected identifier and verify that the server denies the connection. |
| **Test Steps** | • Configure the eAPI Client certificate with a mismatched CN.<br>• Establish a connection between the TOE and eAPI Client using the above created client certificate.<br>• Verify the unsuccessful connection using device logs.<br>• Verify the unsuccessful connection using Packet capture. |
| **Expected Test Results** | • TOE should reject a connection when supplied with an eAPIclient certificate with a mismatched CN.<br>• Log showing unsuccessful connection.<br>• Packet capture showing unsuccessful connection. |
| **Pass/Fail with Explanation** | Pass. Connection attempt fails when the CN filed of the presented certificate did not match the expected username. This meets the testing requirements. |

### 7.96 Update

### 7.97 FPT_TST_EXT.1 Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | It is expected that at least the following tests are performed:<br><br>a) Verification of the integrity of the firmware and executable software of the TOE<br>b) Verification of the correct operation of the cryptographic functions necessary to fulfil any of the SFRs.<br>The evaluator shall either verify that the self-tests described above are carried out during initial start-up or that the developer has justified any deviation from this.<br><br>For distributed TOEs the evaluator shall perform testing of self-tests on all TOE components according to the description in the TSS about which self-test are performed by which component. |
| **Test Steps** | 1. Configure the TOE with the appropriate log-level to see logs for this test.<br>2. Reboot the TOE.<br>3. Verify that the self-test is carried out during initial start-up and verify the integrity of the firmware of the TOE.<br>4. Verify the FIPS cryptographic self-tests were performed at startup.<br>5. Verify the correct operation of cryptographic function has been verified: |
| **Expected Test Results** | 1. The TOE is configured with appropriate log-level for this test.<br>2. The TOE is rebooted.<br>3. The self-test is carried out during initial start-up and the integrity of the firmware is verified.<br>4. The FIPS cryptographic self-test is performed at startup.<br>5. The correct operation of the cryptographic function is verified. |
| **Pass/Fail with Explanation** | Pass - The TOE successfully self-tests crypto and software integrity. |

### 7.98 FPT_TUD_EXT.1 Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 1: The evaluator performs the version verification activity to determine the current version of the product as well as the most recently installed version (should be the same version before updating).<br>The evaluator obtains a legitimate update using procedures described in the guidance documentation and verifies that it is successfully installed on the TOE. |

| | |
|---|---|
| | (For some TOEs loading the update onto the TOE and activation of the update are separate steps ('activation' could be performed e.g. by a distinct activation step or by rebooting the device). In that case the evaluator verifies after loading the update onto the TOE but before activation of the update that the current version of the product did not change but the most recently installed version has changed to the new product version.)<br>After the update, the evaluator performs the version verification activity again to verify the version correctly corresponds to that of the update and that current version of the product and most recently installed version match again. |
| **Test Steps** | 1. Perform the version verification activity to determine the current version of the product as well as the most recently installed version.<br>2. Obtain a legitimate update using the procedures described in the guidance documentation and verify that is it successfully installed on the TOE.<br>3. After the update, the evaluator shall perform the version verification activity again to verify the version correctly corresponds to that of the update and that current version of the product and the most recently installed version match again. |
| **Expected Test Results** | 1. A version verification has been performed determining the current version of the product as well as the most recently installed version.<br>2. A legitimate update using the procedures described in the guidance documentation has been verified and is successfully installed on the TOE.<br>3. A version verification activity is performed again and verifies it correctly corresponds to the newly installed version. |
| **Pass/Fail with Explanation** | Pass - The TOE software was able to be updated when an image that passes the integrity test is used. This meets the testing requirements. |

### 7.99 FPT_TUD_EXT.1 Test #3 (a)

| Item | Data |
|---|---|
| **Test Assurance Activity** | [conditional]: If the TOE itself verifies a hash value over an image against a published hash value (i.e. reference value) that has been imported to the TOE from outside such that the TOE itself authorizes the installation of an image to update the TOE, the following test shall be performed (otherwise the test shall be omitted).<br><br>If the published hash is provided to the TOE by the Security Administrator and the verification of the hash value over the update file(s) against the published hash is performed by the TOE, then the evaluator shall perform the following tests. The evaluator first confirms that no update is pending and then performs the version verification activity to determine the current version of the product, verifying that it is different from the version claimed in the update(s) to be used in this test. The evaluator obtains or produces an illegitimate update such that the hash of the update does not match the published hash. The evaluator provides the published hash value to the TOE and calculates the hash of the update either on the TOE itself (if that functionality is provided by the TOE), or else outside the TOE. The evaluator confirms that the hash values |

| | |
|---|---|
| | are different, and attempts to install the update on the TOE, verifying that this fails because of the difference in hash values (and that the failure is logged). Depending on the implementation of the TOE, the TOE might not allow the Security Administrator to even attempt updating the TOE after the verification of the hash value fails. In that case the verification that the hash comparison fails is regarded as sufficient verification of the correct behaviour of the TOE. |
| **Pass/Fail with Explanation** | Not applicable - Verification of the hash value over the update file(s) against the published hash is not performed by the TOE, but by the administrator. |

### 7.100 FPT_TUD_EXT.1 Test #3 (b)

| Item | Data |
|---|---|
| **Test Assurance Activity** | [conditional]: If the TOE itself verifies a hash value over an image against a published hash value (i.e. reference value) that has been imported to the TOE from outside such that the TOE itself authorizes the installation of an image to update the TOE, the following test shall be performed (otherwise the test shall be omitted).<br><br>If the published hash is provided to the TOE by the Security Administrator and the verification of the hash value over the update file(s) against the published hash is performed by the TOE, then the evaluator shall perform the following tests. The evaluator first confirms that no update is pending and then performs the version verification activity to determine the current version of the product, verifying that it is different from the version claimed in the update(s) to be used in this test.<br>If the TOE allows delayed activation of updates, the TOE must be able to display both the currently executing version and most recently installed version. The handling of version information of the most recently installed version might differ between different TOEs. Depending on the point in time when the attempted update is rejected, the most recently installed version might or might not be updated. The evaluator shall verify that the TOE handles the most recently installed version information for that case as described in the guidance documentation. After the TOE has rejected the update the evaluator shall verify, that both, current version and most recently installed version, reflect the same version information as prior to the update attempt. |
| **Pass/Fail with Explanation** | Not applicable - Verification of the hash value over the update file(s) against the published hash is not performed by the TOE, but by the administrator. |

### 7.101 FPT_TUD_EXT.1 Test #3 (c)

| Item | Data |
|---|---|
| **Test Assurance Activity** | [conditional]: If the TOE itself verifies a hash value over an image against a published hash value (i.e. reference value) that has been imported to the TOE from outside such that the TOE itself authorizes the installation of an image to update the TOE, the following test shall be performed (otherwise the test shall be omitted).<br><br>If the published hash is provided to the TOE by the Security Administrator and the verification of the hash value over the update file(s) against the published hash is performed by the TOE, then the evaluator shall perform the following tests. The |

| | |
|---|---|
| | evaluator first confirms that no update is pending and then performs the version verification activity to determine the current version of the product, verifying that it is different from the version claimed in the update(s) to be used in this test.<br>The evaluator uses a legitimate update and tries to perform verification of the hash value without providing the published hash value to the TOE. The evaluator confirms that this attempt fails. Depending on the implementation of the TOE it might not be possible to attempt the verification of the hash value without providing a hash value to the TOE, e.g. if the hash value needs to be handed over to the TOE as a parameter in a command line message and the syntax check of the command prevents the execution of the command without providing a hash value. In that case the mechanism that prevents the execution of this check shall be tested accordingly, e.g. that the syntax check rejects the command without providing a hash value, and the rejection of the attempt is regarded as sufficient verification of the correct behaviour of the TOE in failing to verify the hash. The evaluator then attempts to install the update on the TOE (in spite of the unsuccessful hash verification) and confirms that this fails. Depending on the implementation of the TOE, the TOE might not allow to even attempt updating the TOE after the verification of the hash value fails. In that case the verification that the hash comparison fails is regarded as sufficient verification of the correct behaviour of the TOE. |
| **Pass/Fail with Explanation** | Not applicable - Verification of the hash value over the update file(s) against the published hash is not performed by the TOE, but by the administrator. |

### 7.102 X509-Rev

### 7.103 FIA_X509_EXT.1.1/Rev Test #1a

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 1a: The evaluator shall present the TOE with a valid chain of certificates (terminating in a trusted CA certificate) as needed to validate the leaf certificate to be used in the function and shall use this chain to demonstrate that the function succeeds. **Test 1a:** shall be designed in a way that the chain can be 'broken' in Test 1b by either being able to remove the trust anchor from the TOEs trust store, or by setting up the trust store in a way that at least one intermediate CA certificate needs to be provided, together with the leaf certificate from outside the TOE, to complete the chain (e.g. by storing only the root CA certificate in the trust store). |
| **Test Steps** | • Configure the TOE for a valid ssl profile.<br>• Show the created certificate chain.<br>• Establish connection between the TOE and eAPI Client.<br>• Verify the successful connection using TOE logs.<br>• Verify the successful connection using Packet capture. |
| **Expected Test Results** | • When a complete certificate chain is present, the TOE should establish a successful TLS connection.<br>• Screenshot evidence of the packet capture showing successful TLS connection. |
| **Pass/Fail with Explanation** | Pass. The TOE can make a successful connection when a complete certificate trust chain is present. This meets the test requirements. |

### 7.104 FIA_X509_EXT.1.1/Rev Test #1b

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 1b: The evaluator shall then 'break' the chain used in Test 1a by either removing the trust anchor in the TOE's trust store used to terminate the chain, or by removing one of the intermediate CA certificates (provided together with the leaf certificate in Test 1a) to complete the chain. The evaluator shall show that an attempt to validate this broken chain fails. |
| **Test Steps** | • Use the same ssl profile and certificate chain as used in Test 1a.<br>• From the uploaded certificate chain and we remove an intermediary certificate named “intermediate.crt” from the TOE.<br>• Attempt to establish connection between the TOE and eAPI Client.<br>• Verify the unsuccessful connection using device logs.<br>• Verify the unsuccessful connection using Packet capture. |
| **Expected Test Results** | • When an incomplete certificate chain is present, the TOE should not establish a connection.<br>• Evidence (screenshot or CLI output) showing removal of certificate.<br>• Log showing unsuccessful connection.<br>• Packet capture showing unsuccessful connection. |
| **Pass/Fail with Explanation** | Pass. The TOE rejects the connection when an incomplete certificate trust chain is present. This meets the test requirements. |

### 7.105 FIA_X509_EXT.1.1/Rev Test #2

| Item | Data |
|---|---|
| **Test Assurance Activity** | The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE.<br>Test 2: The evaluator shall demonstrate that validating an **expired certificate** results in the function failing. |
| **Test Steps** | • Create an expired eAPI Client certificate; for connecting with the TOE.<br>• Show clock on the TOE.<br>• Attempt to connect to the TOE with an expired certificate and verify that it fails.<br>• Verify the unsuccessful connection using device logs.<br>• Verify the unsuccessful connection using packet capture. |
| **Expected Test Results** | • The TOE should deny connection when the certificate is expired<br>• Evidence (screenshot or CLI output) showing connection attempts.<br>• Log showing unsuccessful connection. |

| | |
|---|---|
| | • Packet capture showing unsuccessful connection. |
| **Pass/Fail with Explanation** | Pass. The TOE denied the connection because of the expired certificate. This meets the testing requirements. |

### 7.106 FIA_X509_EXT.1.1/Rev Test #3

| Item | Data |
|---|---|
| **Test Assurance Activity** | The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE.<br>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, then a test shall be performed for each method. The evaluator shall test revocation of the peer certificate and revocation of the peer intermediate CA certificate i.e. the intermediate CA certificate should be revoked by the root CA. The evaluator shall 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.<br>Revocation checking is only applied to certificates that are not designated as trust anchors. Therefore, the revoked certificate(s) used for testing shall not be a trust anchor. |
| **Test Steps** | **Valid Certificate:**<br>• Using the XCA tool to generate a 3-length certificate chain and CRL.<br>• Load the Root CA and ICA on the TOE and configure the TOE for CRL.<br>• Establish connection between the TOE and eAPI Client.<br>• Verify the successful connection using logs.<br>• Verify the successful connection using Packet capture.<br><br>**Invalid End Entity Certificate:**<br>• Revoke the eAPIAdmin certificate and generate CRL.<br>• Attempt to establish connection between the TOE and eAPIAdmin.<br>• Verify the unsuccessful connection using device logs.<br>• Verify the unsuccessful connection using Packet capture.<br><br>**Invalid Intermediate CA Certificate:**<br>• Revoke the Intermediate certificate and generate CRL.<br>• Attempt to establish connection between the TOE and eAPIAdmin. |

| | |
|---|---|
| | • Verify the unsuccessful connection using device logs.<br>• Verify the unsuccessful connection using Packet capture. |
| **Expected Test Results** | • The TOE should deny connection when the certificate is revoked.<br>• Logs showing successful TLS connection when used valid certificates and unsuccessful TLS connection when used revoked certificates.<br>• Packet capture showing successful TLS connection when used valid certificates and unsuccessful TLS connection when used revoked certificates. |
| **Pass/Fail with Explanation** | Pass. The TOE does not communicate with peers that either have a revoked certificate or one of their intermediate CA certificates are revoked. When presented non-revoked certificates, the TOE accepts the certificate. This meets the testing requirements. |

### 7.107 FIA_X509_EXT.1.1/Rev Test #4

| Item | Data |
|---|---|
| **Test Assurance Activity** | The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE.<br>Test 4: If OCSP 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 Steps** | • The evaluator used the XCA tool to create a 3-length chain certificates where the intermediate certificate (AcumenInterCAnocRLsign) does not have the CRLsign key usage bit set.<br>• Load this certificate chain onto the TOE.<br>• As the ssl profile becomes invalid, the HTTPS server on the TOE shuts down.<br>• Attempt to establish connection between the TOE and eAPI Client, this will fail as the HTTPS server on the TOE is shut down due to the ssl profile becoming invalid due to the intermediate certificate (AcumenInterCAnocRLsign) not having the CRLsign key usage bit set.<br>• Verify the unsuccessful connection using packet capture. |
| **Expected Test Results** | • The validation of the CRL should fail and the TOE should deny the TLS connection attempt when CRLsign key usage bit is not set in any of the CA certificates.<br>• Screenshot evidence of the packet capture showing unsuccessful TLS connection. |

| | |
|---|---|
| **Pass/Fail with Explanation** | Pass. The TOE rejected the CRL when the CA signing the CRL does not have the cRLsign key usage bit set. This meets the testing requirements. |

### 7.108 FIA_X509_EXT.1.1/Rev Test #5

| Item | Data |
|---|---|
| **Test Assurance Activity** | The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE.<br>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 Steps** | • Run the acumen-tlss tool with modified byte within the first 8 bytes of the certificate, the connection should fail.<br>• Verify the error with logs on the TOE showing failure due to wrong tag.<br>• Verify the unsuccessful connection with packet capture. |
| **Expected Test Results** | • TOE rejects connections when the first 8 bytes of the certificate are modified.<br>• Screenshot evidence of the packet capture showing unsuccessful TLS connection.<br>• Logs showing unsuccessful TLS connection. |
| **Pass/Fail with Explanation** | Pass. The TOE rejects connections when the first byte of the certificate is modified. This meets the testing requirements |

### 7.109 FIA_X509_EXT.1.1/Rev Test #6

| Item | Data |
|---|---|
| **Test Assurance Activity** | The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE.<br>Test 6: The evaluator shall modify any byte in the certificate signatureValue field (see RFC5280 Sec. 4.1.1.3), which is normally the last field in the certificate, and demonstrate that the certificate fails to validate. (The signature on the certificate will not validate.) |
| **Test Steps** | • Run the acumen-tlss tool with modified byte in the signatureValue field of the cert.<br>• Verify the error with logs on the device showing certificate verification failed.<br>• Verify the unsuccessful connection with packet capture. |
| **Expected Test Results** | • TOE rejects connections when the last byte of the certificate is modified.<br>• Screenshot evidence of the packet capture showing unsuccessful TLS connection. |

| | |
|---|---|
| **Pass/Fail with Explanation** | Pass. The TOE rejects connections when the last byte in the certificate SignatureValue field is modified. This meets the testing requirements. |

### 7.110 FIA_X509_EXT.1.1/Rev Test #7

| Item | Data |
|---|---|
| **Test Assurance Activity** | The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE.<br>Test 7: The evaluator shall modify any byte in the public key of the certificate and demonstrate that the certificate fails to validate. (The hash of the certificate will not validate.) |
| **Test Steps** | • Run the acumen-tlss tool with modified public key in the certificate.<br>• Verify the error with logs on the device failure due to invalid public key.<br>• Verify the unsuccessful connection with packet capture. |
| **Expected Test Results** | • Log showing unsuccessful connection.<br>• Packet capture showing unsuccessful connection. |
| **Pass/Fail with Explanation** | Pass. The TOE rejects connections when the public key of the certificate is modified. This meets the testing requirements. |

### 7.111 FIA_X509_EXT.1.1/Rev Test #8a

| Item | Data |
|---|---|
| **Test Assurance Activity** | **(Conditional on support for EC certificates as indicated in FCS_COP.1/SigGen)**<br>**(Conditional on support for a minimum certificate path length of three certificates)**<br>**(Conditional on TOE ability to process CA certificates presented in certificate message)**<br>Test 8a: The test shall be designed in a way such that only the EC root certificate is designated as a trust anchor, and by setting up the trust store in a way that the EC Intermediate CA certificate needs to be provided, together with the leaf certificate, from outside the TOE to complete the chain (e.g. by storing only the EC root CA certificate in the trust store). The evaluator shall present the TOE with a valid chain of EC certificates (terminating in a trusted CA certificate), where the elliptic curve parameters are specified as a named curve. The evaluator shall confirm that the TOE validates the certificate chain.<br>**TD0527 (12/1 Update) has been applied.** |
| **Pass/Fail with Explanation** | **N/A: EC curve is not supported as per the FCS_COP.1/SigGen** |

### 7.112 FIA_X509_EXT.1.1/Rev Test #8b

| Item | Data |
|---|---|
| **Test Assurance Activity** | **(Conditional on support for EC certificates as indicated in FCS_COP.1/SigGen)**<br>**(Conditional on support for a minimum certificate path length of three certificates)**<br>**(Conditional on TOE ability to process CA certificates presented in certificate message)**<br>The test shall be designed in a way such that only the EC root certificate is designated as a trust anchor, and by setting up the trust store in a way that the EC Intermediate CA certificate needs to be provided, together with the leaf certificate, from outside the TOE to complete the chain (e.g. by storing only the EC root CA certificate in the trust store). The evaluator shall present the TOE with a chain of EC certificates (terminating in a trusted CA certificate), where the intermediate certificate in the certificate chain uses an explicit format version of the Elliptic Curve parameters in the public key information field, and is signed by the trusted EC root CA, but having no other changes. The evaluator shall confirm the TOE treats the certificate as invalid.<br>**TD0527 (12/1 Update) has been applied.** |
| **Pass/Fail with Explanation** | **N/A** |

### 7.113 FIA_X509_EXT.1.1/Rev Test #8c

| Item | Data |
|---|---|
| **Test Assurance Activity** | **(Conditional on support for EC certificates as indicated in FCS_COP.1/SigGen)**<br>**(Conditional on support for a minimum certificate path length of three certificates)**<br>Test 8c: The evaluator shall establish a subordinate CA certificate, where the elliptic curve parameters are specified as a named curve, that is signed by a trusted EC root CA. The evaluator shall attempt to load the certificate into the trust store and observe that it is accepted into the TOE's trust store. The evaluator shall then establish a subordinate CA certificate that uses an explicit format version of the elliptic curve parameters, and that is signed by a trusted EC root CA. The evaluator shall attempt to load the certificate into the trust store and observe that it is rejected, and not added to the TOE's trust store.<br>**TD0527 (12/1 Update) has been applied.** |
| **Pass/Fail with Explanation** | **N/A** |

### 7.114 FIA_X509_EXT.1.2/Rev Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | The tests described must be performed in conjunction with the other certificate services assurance activities, including the functions in FIA_X509_EXT.2.1/Rev. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. Where the TSS identifies any of the rules for extendedKeyUsage fields (in |

| | |
|---|---|
| | FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied) then the associated extendedKeyUsage rule testing may be omitted.<br>The goal of the following tests is to verify that the TOE accepts a certificate as a CA certificate only if it has been marked as a CA certificate by using basicConstraints with the CA flag set to True (and implicitly tests that the TOE correctly parses the basicConstraints extension as part of X509v3 certificate chain validation).<br>For each of the following tests the evaluator shall create a chain of at least three certificates:<br>- a self-signed root CA certificate,<br>- an intermediate CA certificate and<br>- a leaf (node) certificate.<br>The properties of the certificates in the chain are adjusted as described in each individual test below (and this modification shall be the only invalid aspect of the relevant certificate chain).<br>Test 1: The evaluator shall ensure that at least one of the CAs in the chain does not contain the basicConstraints extension. The evaluator confirms that the TOE rejects such a certificate at one (or both) of the following points:<br>*(i) as part of the validation of the leaf certificate belonging to this chain;*<br>*(ii) when attempting to add a CA certificate without the basicConstraints extension to the TOE's trust store (i.e. when attempting to install the CA certificate as one which will be retrieved from the TOE itself when validating future certificate chains).* |
| **Test Steps** | • Create an ICA with no basicConstraint.<br>• Upload the created ICA to TOE.<br>• Verify that the TOE discards the certificate.<br>• Verify the failed connection using TOE logs. |
| **Expected Test Results** | • The TOE should reject certificates signed by CA that does not contain the BasicConstraints Extension.<br>• Failure logs on the TOE showing it discards the certificate. |
| **Pass/Fail with Explanation** | Pass. The TOE rejects certificates signed by a CA that do not contain the basicConstraints extension. This meets the testing requirements. |

### 7.115 FIA_X509_EXT.1.2/Rev Test #2

| Item | Data |
|---|---|
| **Test Assurance Activity** | The tests described must be performed in conjunction with the other certificate services assurance activities, including the functions in FIA_X509_EXT.2.1/Rev. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. Where the TSS identifies any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied) then the associated extendedKeyUsage rule testing may be omitted. |

| | |
|---|---|
| | The goal of the following tests it to verify that the TOE accepts only certificates that have been marked as CA certificates by using basicConstraints with the CA flag set to True (and implicitly that the TOE correctly parses the basicConstraints extension as part of X509v3 certificate chain validation).<br>For each of the following tests the evaluator shall create a chain of at least three certificates:<br>- a self-signed root CA certificate,<br>- an intermediate CA certificate and<br>- a leaf (node) certificate.<br>The properties of the certificates in the chain are adjusted as described in each individual test below (and this modification shall be the only invalid aspect of the relevant certificate chain).<br>Test 2: The evaluator shall ensure that at least one of the CA certificates in the chain has a basicConstraints extension in which the CA flag is set to FALSE. The evaluator confirms that the TOE rejects such a certificate at one (or both) of the following points:<br>(i) As part of the validation of the leaf certificate belonging to this chain;<br>(ii) When attempting to add a CA certificate with the CA flag set to FALSE to the TOE's trust store (i.e. when attempting to install the CA certificate as one which will be retrieved from the TOE itself when validating future certificate chains). |
| **Test Steps** | • Create an ICA with the basicConstraints extension set to FALSE.<br>• Upload the created ICA to TOE.<br>• Verify that the TOE discards the certificate.<br>• Verify the failure using device logs. |
| **Expected Test Results** | • The TOE should reject certificates signed by CA that has the basicConstraints extension set to FALSE.<br>• Failure logs on the TOE showing it discards the certificate. |
| **Pass/Fail with Explanation** | Pass. The TOE rejects certificates signed by a CA that has the CA flag in the basicConstraints extension set to FALSE. This meets the testing requirements. |

### 7.116 FIA_X509_EXT.2 Test #1

| Item | Data |
|---|---|
| **Test Assurance Activity** | The evaluator shall perform the following test for each trusted channel:<br>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.<br>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 guidance documentation to determine that all supported administrator-configurable options behave in their documented manner. |
| **Test Steps** | • Show the configuration on the TOE for communication between the TOE and CRL server.<br>• To verify that the script works, we start the CRL server and we can see hits coming from the TOE on to the CRL server every six minutes.<br>• Verify the session between TOE and CRL server using TOE logs.<br>• Verify the session between TOE and CRL server using packet capture.<br>• Establish connection between the TOE and eAPI Client.<br>• Verify the successful connection using TOE logs.<br>• Verify the successful connection using Packet capture.<br>• Attempt to establish a connection between the TOE and eAPI Client.<br>• Verify the successful connection using TOE logs.<br>• Verify the successful connection using Packet capture.<br>• Manipulating the environment by terminating the current session between the TOE and the CRL server. Now any attempt from the TOE to download the CRL's should fail.<br>• Verify the failed CRL attempt by the TOE using TOE logs.<br>• Verify the failed CRL attempt by the TOE using packet capture.<br>• Due to the above failed CRL attempt, the ssl profile on the TOE becomes invalid and as a result the HTTPS server on the TOE shuts down.<br>• Attempt to establish connection between the TOE and eAPI Client, this will fail as the HTTPS server on the TOE is shut down.<br>• Verify the failed connection attempt using packet capture. |
| **Expected Test Results** | • Evidence (screenshot or CLI output) showing configuration of CRL.<br>• Evidence (screenshot or CLI output) showing session between TOE and CRL server.<br>• Log showing successful/unsuccessful connection.<br>• Packet capture showing successful/unsuccessful connection. |
| **Pass/Fail with Explanation** | Pass. The TOE successfully rejects certificates when validation service is unavailable. This meets the testing requirements. |

### 7.117 FIA_X509_EXT.3 Test #1

| Item | Data |
|---|---|

| | |
|---|---|
| **Test Assurance Activity** | Test 1: The evaluator shall use the guidance documentation to cause the TOE to generate a Certification Request. The evaluator shall capture the generated message and ensure that it conforms to the format specified. The evaluator shall confirm that the Certification Request provides the public key and other required information, including any necessary user-input information. |
| **Test Steps** | • From the TOE, generate a CSR.<br>• Ensure the CSR contains the following fields.<br>  ○ Common Name (CN)<br>  ○ Organization (O)<br>  ○ Organizational Unit (OU)<br>  ○ Country (C) |
| **Expected Test Results** | • The TOE should generate CSR containing the required fields selected in the SFR.<br>• Evidence (screenshot or CLI output) showing generation of CSR. |
| **Pass/Fail with Explanation** | Pass. The TOE is able to generate a CSR with all the requisite information. This meets the testing requirements. |

### 7.118 FIA_X509_EXT.3 Test #2

| Item | Data |
|---|---|
| **Test Assurance Activity** | Test 2: The evaluator shall demonstrate that validating a response message to a Certification Request without a valid certification path results in the function failing. The evaluator shall then load a certificate or certificates as trusted CAs needed to validate the certificate response message and demonstrate that the function succeeds. |
| **Test Steps** | • Show the current working chain of certificates and the ssl profile.<br>• Remove an intermediate certificate from the chain of certificates<br>• Verify that the TOE rejects the certificate because the full trust chain of the CA is not present using logs.<br>• Add the intermediate certificate back to the TOE certificate store to ensure that the TOE has a full certificate path.<br>• Re-attempt to load the signed certificate on the TOE.<br>• Verify that the TOE accepts the certificate using logs. |
| **Expected Test Results** | • The TOE should not validate a signed CSR if the full trust chain is not present. When a full trust chain is present, the TOE should validate the signed CSR.<br>• Evidence (screenshot or CLI output) showing generation of CSR.<br>• CLI output showing successful signing of CSR. |

| | |
|---|---|
| | • CLI output showing unsuccessful signing of CSR when the trustpoint is removed. |
| **Pass/Fail with Explanation** | Pass. The TOE does not install CSR responses signed by a CA without a full trust path. The TOE does install a CSR response signed by a CA with a full trust path. This meets the testing requirements. |

# 8 Security Assurance Requirements

## 8.1 ADV_FSP.1 Basic Functional Specification

### 8.1.1 ADV_FSP.1

#### 8.1.1.1 ADV_FSP.1 Activity 1

| | |
|---|---|
| Objective | The evaluator shall examine the interface documentation to ensure it describes the purpose and method of use for each TSFI that is identified as being security relevant. |
| Evaluator Findings | The evaluator examined the AGD (interface documentation) to verify that it describes the purpose and method of use for each TSFI that is identified as being security relevant. The evaluator examined the entire AGD. The evaluator verified the AGD describes the purpose and method of use for each security relevant TSFI by verifying the AGD satisfies all of the Guidance Evaluation Activities.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

#### 8.1.1.2 ADV_FSP.1 Activity 2

| | |
|---|---|
| Objective | The evaluator shall examine the interface documentation to ensure it describes the purpose and method of use for each TSFI that is identified as being security relevant. |
| Evaluator Findings | The evaluator examined the AGD (interface documentation) to develop a mapping of the interfaces to SFRs. The evaluator examined the entire AGD. Each Guidance Evaluation Activity is associated with a specific SFR. The Evaluation Findings for each Guidance Evaluation Activity identify the relevant interfaces, thus providing a mapping.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

#### 8.1.1.3 ADV_FSP.1 Activity 3

| | |
|---|---|
| Objective | The evaluator shall check the interface documentation to ensure it identifies and describes the parameters for each TSFI that is identified as being security relevant. |

| | |
|---|---|
| Evaluator Findings | The evaluator examined the AGD (interface documentation) to verify that it identifies and describes the parameters for each TSFI that is identified as being security relevant. The evaluator examined the entire AGD. The evaluator verified the AGD describes the parameters for each security relevant TSFI by verifying the AGD satisfies all of the Guidance Evaluation Activities.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

## 8.2 AGD_OPE.1 Operational User Guidance

### 8.2.1 AGD_OPE.1

#### 8.2.1.1 AGD_OPE.1 Activity 1

| | |
|---|---|
| Objective | The evaluator shall ensure the Operational guidance documentation is distributed to Security Administrators and users (as appropriate) as part of the TOE, so that there is a reasonable guarantee that Security Administrators and users are aware of the existence and role of the documentation in establishing and maintaining the evaluated configuration. |
| Evaluator Findings | The evaluator checked the requirements below are met by the guidance documentation. Guidance documentation shall be distributed to administrators and users (as appropriate) as part of the TOE, so that there is a reasonable guarantee that administrators and users are aware of the existence and role of the documentation in establishing and maintaining the evaluated configuration. Upon investigation, the evaluator found that the CC guidance will be published with the CC certificate on www.niap-ccevs.org..<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

#### 8.2.1.2 AGD_OPE.1 Activity 2

| | |
|---|---|
| Objective | The evaluator shall ensure that the Operational guidance is provided for every Operational Environment that the product supports as claimed in the Security Target and shall adequately address all platforms claimed for the TOE in the Security Target. |
| Evaluator Findings | The evaluator ensured that the Operational guidance is provided for every Operational Environment that the product supports as claimed in the Security Target. The section titled **1.1.4 Operational Environment** of the AGD was used to determine the verdict of this assurance activity. The AGD specifies that the platforms supported are:<br><br>• Local Console Administrative Access<br>  ○ RS-232 Serial Console.<br>  ○ VT-100 terminal emulation program.<br>• Remote Management<br>  ○ SSH client for remote interactive session utilizing SSH. |

| | |
|---|---|
| | ○ eAPI JSON-RPC Client capable of establishing a mutually authenticated TLS session.<br>• Audit Server<br>○ Syslog server capable of accepting an SSHv2 tunnel utilizing SSH Protocol Version 2 (SSHv2).<br>• Certificate Revocation List (CRL) Server<br>○ Server from where CRLs can be downloaded on TOE to check validity of X509v3 certificates.<br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

8.2.1.3 AGD_OPE.1 Activity 3

| | |
|---|---|
| Objective | The evaluator shall ensure that the Operational guidance contains instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE. |
| Evaluator Findings | The evaluator ensured that the Operational guidance contains instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE. While performing the Guidance Evaluation Activities for the cryptographic SFRs, the evaluator ensured guidance contained the necessary instructions for configuring the cryptographic engines.<br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

8.2.1.4 AGD_OPE.1 Activity 4

| | |
|---|---|
| Objective | The evaluator shall ensure the Operational guidance makes it clear to an administrator which security functionality and interfaces have been assessed and tested by the EAs. |
| Evaluator Findings | The entire AGD was used to determine the verdict of this work unit. Each confirmation command indicates tested options. Additionally, the section titled “Usage Assumptions” specifies features that are not assessed and tested by the EAs. The evaluator ensured the Operational guidance makes it clear to an administrator which security functionality and interfaces have been assessed and tested by the EAs.<br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

8.2.1.5 AGD_OPE.1 Activity 5 **[TD0536]**

| | |
|---|---|
| Objective | In addition, the evaluator shall ensure that the following requirements are also met. |

| | |
|---|---|
| | a) The guidance documentation shall contain instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE.<br>b) The documentation must describe the process for verifying updates to the TOE for each method selected for FPT_TUD_EXT.1.3 in the Security Target. The evaluator shall verify that this process includes the following steps:<br>i) Instructions for obtaining the update itself. This should include instructions for making the update accessible to the TOE (e.g., placement in a specific directory).<br>ii) Instructions for initiating the update process, as well as discerning whether the process was successful or unsuccessful. This includes instructions that describe at least one method of validating the hash/digital signature.<br>c) The TOE will likely contain security functionality that does not fall in the scope of evaluation under this cPP. The guidance documentation shall make it clear to an administrator which security functionality is covered by the Evaluation Activities. |
| Evaluator Findings | The evaluator verified the guidance documentation contains instructions for configuring any cryptographic engines in AGD_OPE.1 Test #3.<br>The evaluator verified the guidance documentation describes the process for verifying updates in FPT_TUD_EXT.1 Guidance 2.<br>The evaluator verified the guidance documentation makes it clear which security functionality is covered by the Evaluation Activities in AGD_OPE.1 Test #4.<br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

## 8.3 AGD_PRE.1 Preparative Procedures

### 8.3.1 AGD_PRE.1

#### 8.3.1.1 AGD_PRE.1 Activity 1

| | |
|---|---|
| Objective | The evaluator shall examine the Preparative procedures to ensure they include a description of how the Security Administrator verifies that the operational environment can fulfil its role to support the security functionality (including the requirements of the Security Objectives for the Operational Environment specified in the Security Target). |
| Evaluator Findings | The evaluator examined the Preparative procedures to ensure they include a description of how the administrator verifies that the operational environment can fulfil its role to support the security functionality. The evaluator reviewed the sections titled “Operational Environment” of the AGD. The evaluator found that these sections describe how the Operational Environment must meet:<br>• Local Console Administrative access<br>• Remote Management |

| | |
|---|---|
| | • Audit Server<br>• Certificate Revocation List (CRL) Server<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

8.3.1.2 AGD_PRE.1 Activity 2

| | |
|---|---|
| Objective | The evaluator shall examine the Preparative procedures to ensure they are provided for every Operational Environment that the product supports as claimed in the Security Target and shall adequately address all platforms claimed for the TOE in the Security Target. |
| Evaluator Findings | The evaluator checked the requirements below are met by the preparative procedures. The entire AGD was used to determine the verdict of this work unit. Upon investigation, the evaluator found that the guidance documentation describes each of the devices in the operating environment, including,<br><br>• Local Console Administrative Access<br>  ○ RS-232 Serial Console.<br>  ○ VT-100 terminal emulation program.<br>• Remote Management<br>  ○ SSH client for remote interactive session utilizing SSH.<br>  ○ eAPI JSON-RPC Client capable of establishing a mutually authenticated TLS session.<br>• Audit Server<br>  ○ Syslog server capable of accepting an SSHv2 tunnel utilizing SSH Protocol Version 2 (SSHv2).<br>• Certificate Revocation List (CRL) Server<br>  ○ Server from where CRLs can be downloaded on TOE to check validity of X509v3 certificates.<br><br>The section titled **1.1.5 TOE Description** of AGD identifies the following supported platform:<br><br>• 7280CR<br>• 7280SR<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

#### 8.3.1.3 AGD_PRE.1 Activity 3

| | |
|---|---|
| Objective | The evaluator shall examine the preparative procedures to ensure they include instructions to successfully install the TSF in each Operational Environment. |
| Evaluator Findings | The evaluator checked the requirements are met by the preparative procedures. The entire AGD was used to determine the verdict of this work unit. Upon investigation, the evaluator found that AGD describes all of the functions necessary to install and configure the TOE to work in the target operating environment, including,<br>• Configuring Administrative Accounts and Passwords<br>• Configuring Console Timeout<br>• Configuring SSH and Console Connections<br>• Configuring the Remote Syslog Server<br>• Configuring Audit Log Options<br>• Configuring Event Logging<br>• Configuring TLS server<br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

#### 8.3.1.4 AGD_PRE.1 Activity 4

| | |
|---|---|
| Objective | The evaluator shall examine the preparative procedures to ensure they include instructions to manage the security of the TSF as a product and as a component of the larger operational environment. |
| Evaluator Findings | The evaluator ensured the preparative procedures include instructions to manage the security of the TSF as a product and as a component of the larger operational environment. The entire AGD was used to determine the verdict of this work unit. The same commands, configurations, and interfaces used to install the TOE are also used for ongoing management, so this is satisfied by AGD_PRE.1 Test #3.<br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

#### 8.3.1.5 AGD_PRE.1 Activity 5

| | |
|---|---|
| Objective | In addition, the evaluator shall ensure that the following requirements are also met.<br>The preparative procedures must |

| | |
|---|---|
| | a) include instructions to provide a protected administrative capability; and<br>b) identify TOE passwords that have default values associated with them and instructions shall be provided for how these can be changed. |
| Evaluator Findings | The evaluator ensured the preparative procedures include instructions to provide a protected administrative capability and changing default passwords. The sections titled “Default Accounts Protection” and “SSH Configuration” were used to determine the verdict of this work unit. The AGD describes changing the default password associated with the root account and configuring SSH for remote administration.<br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

## 8.4 ALC Assurance Activities

### 8.4.1 ALC_CMC.1

#### 8.4.1.1 ALC_CMC.1 Activity 1

| | |
|---|---|
| Objective | When evaluating that the TOE has been provided and is labelled with a unique reference, the evaluator performs the work units as presented in the CEM. |
| Evaluator Findings | The evaluator verified that the ST, TOE and Guidance are all labeled with the same hardware versions and software. The information is specific enough to procure the TOE and it includes hardware models and software versions. The evaluator checked the TOE software version and hardware identifiers during testing by examining the actual machines used for testing.<br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

### 8.4.2 ALC_CMS.1

#### 8.4.2.1 ALC_CMS.1 Activity 1

| | |
|---|---|
| Objective | When evaluating the developer’s coverage of the TOE in their CM system, the evaluator performs the work units as presented in the CEM. |
| Evaluator Findings | The evaluator verified that the ST, TOE and Guidance are all labeled with the same hardware versions and software. The information is specific enough to procure the TOE and it includes hardware models and software versions. The evaluator checked the TOE software version and hardware identifiers during testing by examining the actual machines used for testing. |

| | |
|---|---|
| | Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

## 8.5 ATE_IND.1 Independent Testing – Conformance

### 8.5.1 ATE_IND.1

#### 8.5.1.1 ATE_IND.1 Activity 1

| | |
|---|---|
| Objective | The evaluator performs the CEM work units associated with the ATE_IND.1 SAR. Specific testing requirements and EAs are captured for each SFR in Sections 2, 3 and 4.<br><br>The evaluator should consult Appendix 709 when determining the appropriate strategy for testing multiple variations or models of the TOE that may be under evaluation. |
| Evaluator Findings | The evaluator examined the TOE to determine that the test configuration is consistent with the configuration under evaluation as specified in the ST. Upon investigation, the evaluator found that each instance of the TOE used in testing was consistent with TOE description found in the Security Target. Additionally, the evaluator found that the TOE version is consistent with what was specified in the Security Target. The evaluator examined the TOE to determine that it has been installed properly and is in a known state. The details of the installed TOE and any configuration performed with the TOE are found in the separate Test Reports. The evaluator prepared a test plan that covers all of the testing actions for ATE_IND.1 in the CEM and in the SFR-related Evaluation Activities.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

## 8.6 AVA_VAN.1 Vulnerability Survey

### 8.6.1 AVA_VAN.1

#### 8.6.1.1 AVA_VAN.1 Activity 1 [**TD0564, Labgram #116]**

| | |
|---|---|
| Objective | The evaluator shall document their analysis and testing of potential vulnerabilities with respect to this requirement. |
| Evaluator Findings | The evaluator documented their analysis and testing of potential vulnerabilities with respect to this requirement.<br><br>Public searches were performed against all keywords found within the Security Target and AGD that may be applicable to specific TOE components. This included protocols, TOE software version, and TOE hardware to ensure sufficient coverage under AVA. The evaluator searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The sources of the publicly available information are provided below.<br><br>• https://nvd.nist.gov/view/vuln.search |

| | |
|---|---|
| | • http://cve.mitre.org/cve<br>• https://www.cvedetails.com/vulnerability-search.php<br>• https://www.kb.cert.org/vuls/search/<br>• www.exploitsearch.net<br>• www.securiteam.com<br>• http://nessus.org/plugins/index.php?view=search<br>• http://www.zerodayinitiative.com/advisories<br>• https://www.exploit-db.com<br>• https://www.rapid7.com/db/vulnerabilities<br>• https://www.arista.com/<br><br>The initial public domain vulnerability search was conducted on March 15, 2023, that was documented in proprietary Vulnerability assessment report version 0.2, followed by another on July 05, 2023, documented in a new version 0.4 of the same document. The evaluator carried out both searches utilizing the following specified keywords:<br><br>• Arista<br>• Arista networks<br>• Arista networks 7280<br>• EOS 4.28<br>• 7280CR<br>• 7280SR<br>• Intel Pentium D1519<br>• nginx 1.21.4<br>• rsyslog 8.2001.0<br>• linux kernel 4.19.142<br>• jitterentropy-rngd-1.0.6<br>• openssl 1.0.2k<br>• openssl-fips 2.0.16<br>• openssh 7.8p1<br>• eAPI<br>• Arista eAPI<br>• TLS 1.2<br>• TCP |

| | |
|---|---|
| | The evaluation lab examined each result provided from NVD and Exploit Search to determine if the current TOE version or component within the environment was vulnerable. Based upon the analysis, any issues found that were generated were patched in the TOE version and prior versions, mitigating the risk factor.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

8.6.1.2 AVA_VAN.1 Activity 2

| | |
|---|---|
| Objective | Type 4 Hypotheses – Tool-Generated<br><br>The evaluator shall perform the following activities to generate type 4 flaw hypotheses:<br><br>• Fuzz testing<br>  ○ Examine effects of sending:<br>  ▪ mutated packets carrying each 'Type' and 'Code' value that is undefined in the relevant RFC for each of ICMPv4 (RFC 792) and ICMPv6 (RFC 4443)<br>  ▪ mutated packets carrying each 'Transport Layer Protocol' value that is undefined in the respective RFC for IPv4 (RFC 791) IPv6 (RFC 2460) should also be covered if it is supported and claimed by the TOE.<br><br>Since none of these packets will belong to an allowed session, the packets should not be processed by the TOE, and the TOE should not be adversely affected by this traffic. Any results that are unexpected (e.g., core dumps) are candidates for a flaw hypothesis.<br><br>○ Mutation fuzz testing of the remaining fields in the required protocol headers. This testing requires sending mutations of well- formed packets that have both carefully chosen and random values inserted into each header field in turn (i.e. testing is to include both carefully chosen and random insertion test cases). The original well-formed packets would be accepted as part of a normal existing communication stream and may still be accepted as valid packets when subject to the carefully chosen mutations (the individual packet alone would be valid although its contents may not be valid in the context of preceding and/or following packets), but will often not be valid packets when random values are inserted into fields. The carefully chosen values should include semantically significant values that can be determined from the type of the data that the field represents, such as values indicating positive and negative integers, boundary conditions, invalid binary combinations (e.g. for flag sets with dependencies between bits), and missing start or end values. Randomly chosen values may not result in well-formed packets but are included nonetheless to see whether they can lead to the device entering an insecure state. Any results that are unexpected (e.g., core dumps) are candidates for a flaw hypothesis.<br><br>Type 3 Hypotheses – Evaluation-Team-Generated |

| | |
|---|---|
| | Type 3 flaws are formulated by the evaluator based on information presented by the product (through on-line help, product documentation and user guides, etc.) and product behaviour during the (functional) testing activities. The evaluator is also free to formulate flaws that are based on material that is not part of the baseline evidence (e.g., information gleaned from an Internet mailing list, or reading interface documentation on interfaces not included in the set provided by the developer), although such activities have the potential to vary significantly based upon the product and evaluation facility performing the analysis.<br><br>If the evaluators discover a Type 3 flaw that they believe should be considered as a Type 2 flaw in future versions of this cPP, they should work with their Certification Body to determine the appropriate means of submitting the flaw for consideration by the iTC. |
| Evaluator Findings | Type 4 Hypotheses – Tool-Generated<br><br>The evaluator documented the fuzz testing results with respect to this requirement.<br><br>The evaluation lab examined each result from fuzz testing to determine if the TOE improperly processes packets. Based upon the analysis, no unexpected results occurred. Therefore, no Type 4 hypotheses were generated.<br><br>Type 3 Hypotheses – Evaluation-Team-Generated<br><br>The evaluation team has formulated Type 3 flaw hypotheses in compliance with Sections A.1.3, A.1.4, and A.2 of the NDcPP v2.2e protection profile document. Importantly, no remaining vulnerabilities were found that could be exploited by attackers with Basic Attack Potential. For further information on the vulnerability analysis test carried out during the evaluation, please refer to the Vulnerability Assessment report, which provides comprehensive details.<br><br>Based on these findings, this assurance activity is considered satisfied. |
| Verdict | Pass |

# 9 Conclusion

The testing shows that all test cases required for conformance have passed testing.

# End of Document