Supporting Document

Mandatory Technical Document

PP-Module for SSL/TLS Inspection Proxy

Version 1.0

23 August 2019

National Information Assurance Partnership

Foreword

This is a Supporting Document (SD), intended to complement the Common Criteria version 3 and the associated Common Evaluation Methodology for Information Technology Security Evaluation.

SDs may be “Guidance Documents,” that highlight specific approaches and application of the standard to areas where no mutual recognition of its application is required, and as such, are not of normative nature, or “Mandatory Technical Documents,” whose application is mandatory for evaluations whose scope is covered by that of the SD. The usage of the latter class is not only mandatory, but certificates issued because of their application are recognized under the CCRA.

Technical Editor:

National Information Assurance Partnership (NIAP)

Document history:

V1.0. 23 August 2019 (initial release)

General Purpose:

The purpose of this SD is to define evaluation methods for the functional behavior of SSL/TLS Inspection Proxy network devices. This primarily relates to the implementation of STIP but includes other related functionality.

Field of special use:

SSL/TLS Inspection Proxy functionality that is deployed on standalone hardware network devices.

Acknowledgements:

This SD was developed with support from NIAP Technical Community members, with representatives from industry, Government agencies, Common Criteria Test Laboratories, and members of academia.

Table of Contents

1 Introduction

1.1 Technology Area and Scope of Supporting Document

The scope of the SSL/TLS (STIP) Inspection Proxy PP-Module is to describe the security functionality in terms of [CC] and to define functional and assurance requirements for such products. This PP-Module is intended for use with the following Base-PPs:

- collaborative Protection Profile for Network Devices (NDcPP) v2.1

This SD is mandatory for evaluations of TOEs that claim conformance to the following PP-Module:

- PP-Module for SSL/TLS Inspection Proxy v1.0

Although Evaluation Activities (EAs) are defined mainly for the evaluators to follow, in general they will also help developers to prepare for evaluation by identifying specific requirements for their TOE. The specific requirements in EAs may in some cases clarify the meaning of Security Functional Requirements (SFR), and may identify particular requirements for the content of Security Targets (ST) (especially the TOE Summary Specification), user guidance documentation, and possibly supplementary information (e.g. for entropy analysis or cryptographic key management architecture).

1.2 Structure of the Document

EAs can be defined for both SFRs and Security Assurance Requirements (SAR). These are defined in separate sections of this SD.

If any EA cannot be successfully completed in an evaluation, then the overall verdict for the evaluation is a 'fail'. In rare cases there may be acceptable reasons why an EA may be modified or deemed not applicable for a particular TOE, but this must be agreed with the Certification Body for the evaluation.

In general, if all EAs (for both SFRs and SARs) are successfully completed in an evaluation then it would be expected that the overall verdict for the evaluation is a 'pass'. To reach a 'fail' verdict when the EAs have been successfully completed would require a specific justification from the evaluator as to why the EAs were not sufficient for that TOE.

Similarly, at the more granular level of Assurance Components, if the EAs for an Assurance Component and all of its related SFR EAs are successfully completed in an evaluation then it would be expected that the verdict for the Assurance Component is a 'pass'. To reach a 'fail' verdict for the Assurance Component when these EAs have been successfully completed would require a specific justification from the evaluator as to why the EAs were not sufficient for that TOE.

1.3 Terminology

1.3.1 Glossary

For definitions of standard CC terminology, see [CC] part 1.

Supplementary information

Information that is not necessarily included in the ST or operational guidance, and that may not necessarily be public. Examples of such information could be entropy analysis or description of a cryptographic key management architecture used in (or in support of) the TOE. The requirement for any such supplementary information will be identified in the relevant cPP.

Term	Definition
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation (International Standard ISO/IEC 15408).
Common Criteria Testing Laboratory	Within the context of the Common Criteria Evaluation and Validation Scheme (CCEVS), an IT security evaluation facility, accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the NIAP Validation Body to conduct Common Criteria-based evaluations.
Common Evaluation Methodology (CEM)	Common Evaluation Methodology for Information Technology Security Evaluation.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of products.
Protection Profile Configuration (PP-Configuration)	A comprehensive set of security requirements for a product type that consists of at least one PP and at least one PP-Module.
Protection Profile Module (PP-Module)	An implementation-independent set of security requirements for a specific subset of products described by a PP.
Security Assurance Requirement (SAR)	A requirement for how the TOE's proper implementation of the SFRs is verified by an evaluator.
Security Functional Requirement (SFR)	A requirement for security enforcement by the TOE.
Security Target (ST)	A set of implementation-dependent security requirements for a specific product.
Target of Evaluation (TOE)	The product under evaluation.
TOE Security Functionality (TSF)	The security functionality of the product under evaluation.
TOE Summary Specification (TSS)	A description of how a TOE satisfies the SFRs in an ST.

1.3.2 Acronyms

Acronym	Meaning
EA	Evaluation Activity
SNI	Server Name Indication
STIP	SSL/TLS Inspection Proxy
TDES	Triple Data Encryption Standard

Acronym	Meaning
TTT	Thru Traffic TLS

2 Evaluation Activities for SFRs

The EAs presented in this section capture the actions the evaluator performs to address technology specific aspects covering specific SARs (e.g., ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, and ATE_IND.1) – this is in addition to the CEM work units that are performed in Section 6 (Evaluation Activities for SARs).

Regarding design descriptions (designated by the subsections labeled TSS, as well as any required supplementary material that may be treated as proprietary), the evaluator must ensure there is specific information that satisfies the EA. For findings pertaining to the TSS section, the evaluator's verdicts will be associated with the CEM work unit ASE_TSS.1-1. Evaluator verdicts associated with the supplementary evidence will also be associated with ASE_TSS.1-1, since the requirement to provide such evidence is specified in ASE in the cPP.

For ensuring the guidance documentation provides sufficient information for the administrators and users as it pertains to SFRs, the evaluator's verdicts will be associated with CEM work units ADV_FSP.1-7, AGD_OPE.1-4, and AGD_OPE.1-5.

Finally, the subsection labeled Tests is where the authors have determined that testing of the product in the context of the associated SFR is necessary. While the evaluator is expected to develop tests, there may be instances where it is more practical for the developer to construct tests, or where the developer may have existing tests. Therefore, it is acceptable for the evaluator to witness developer-generated tests in lieu of executing the tests. In this case, the evaluator must ensure the developer's tests are executing both in the manner declared by the developer and as mandated by the EA. The CEM work units that are associated with the EAs specified in this section are ATE_IND.1-3, ATE_IND.1-4, ATE_IND.1-5, ATE_IND.1-6, and ATE_IND.1-7.

2.1 NDcPP Evaluation Activities – Modified SFRs from Base-PP

The EAs defined in this section are applicable in cases where the TOE claims conformance to a PP-Configuration that include the NDcPP.

2.1.1 Security Audit (FAU)

2.1.1.1 Security Audit Data Generation (FAU_GEN)

FAU_GEN.1 Audit Data Generation

There are additional auditable events that serve to extend the FAU_GEN.1 SFR found in the Base-PP.

This SFR is evaluated in the same manner as defined by the EAs for the Base-PP. The only difference is that the evaluator shall also assess the auditable events required for this PP-Module in addition to those defined in the Base-PP

2.1.2 Cryptographic Support (FCS)

2.1.2.1 Cryptographic Key Destruction (FCS_CKM)

FCS_CKM.4 Cryptographic Key Destruction

This SFR is refined in this PP-Module to include requirements for destruction of security critical parameters as well as keys. The Evaluation activities for the Base-PP are extended to include security critical parameters whenever keys are indicated.

2.1.3 Identification and Authentication (FIA)

2.1.3.1 X.509 Certificate Validation (FIA_X509_EXT)

FIA_X509_EXT.1/Rev X.509 Certificate Validation

There is no change to the EAs for this SFR.

FIA_X509_EXT.2 X.509 Certificate Authentication

This SFR is refined in this PP-Module to require certificates for TLS, which is mandatory for this technology type, so this selection-based SFR as defined in the Base-PP is considered to be mandatory for any TOE whose conformance claim includes this PP-Module. There is no change to the EAs associated to the refinement of this SFR.

FIA_X509_EXT.3 X.509 Certificate Requests

There is no change to the text of this SFR or its EAs in this PP-Module. However, this is currently listed as an optional SFR in the Base-PP. For a TOE whose conformance claim includes this PP-Module, this SFR is moved to selection-based because certificate enrollment can be performed either through PKCS#10 (covered by this SFR) or through Enrollment over Secure Transport (EST) (covered by the selection-based SFR FIA_ESTC_EXT.1 in this PP-Module).

2.1.3.2 Specification of Management Functions (FMT_SMF)

FMT_SMF.1 Specification of Management Functions

This PP-Module does not define any additional evaluation activities for this SFR beyond what is defined in the Base-PP. It is expected that performing the other evaluation activities in this PP will demonstrate that each of the management functions claimed by the TOE are provided by the TSF.

2.1.3.3 Restrictions on Security Roles (FMT_SMR)

FMT_SMR.2 Restrictions on Security Roles

TSS

The evaluator shall examine the TSS to ensure it identifies the roles, and the privileges granted to and limitations of each role. The evaluator shall also examine the TSS to ensure it describes the interfaces available to each role and how role separation is ensured.

Guidance

The evaluator shall examine the AGD documents to ensure they contain instructions for using the TOE to assign roles to the corresponding users.

The evaluator shall review the operational guidance to ensure that it contains instructions for how the roles connect to and perform operations on the TOE, and which interfaces are supported.

Test

The evaluator shall perform the following tests:

Test 1: For each supported role, the evaluator shall assume the role and connect to the TOE as specified in the AGD documentation. The evaluator shall verify that the role can perform the documented operations.

Test 2 (conditional, if Auditor role is claimed): The evaluator shall attempt to assume the Auditor role in conjunction with any other role as defined in FMT_SMR.2.1 and shall verify it is not possible.

Test 3 (conditional, if Account Manager role is claimed): The evaluator shall attempt to assume the Account Manager role in conjunction with any other role as defined in FMT_SMR.2.1 and verify it is not possible.

2.2 TOE SFR Evaluation Activities

2.2.1 Security Audit (FAU)

2.2.1.1 Generation of Certificate Repository (FAU_GCR_EXT)

FAU_GCR_EXT.1 Generation of Certificate Repository

TSS
The evaluator shall examine the TSS to determine that it describes the certificate repository. If the certificate repository is provided by the OE, the evaluator shall check the TSS to ensure it describes the interfaces invoked by the TOE to store certificates.

Guidance
The evaluator shall ensure that the guidance describes any operations necessary to cause certificates to be stored in the repository.

Test
Test 1: The evaluator shall cause a certificate to be generated by the TSF. The evaluator shall confirm that the certificate is stored in the certificate repository.

2.2.1.2 Security Audit Event Storage (FAU_STG)

FAU_STG.4 Prevention of Audit Data Loss

TSS
The evaluator shall examine the TSS to ensure it describes the behavior of the TSF when the audit trail cannot be written to. The evaluator shall ensure the TSS describes where the audit trail is stored (locally, remotely, or both), how the TSF detects audit full conditions if the audit trail is stored locally, whether and how the TSF detects audit full conditions for remote audit repositories, and how the TSF detects loss of communication with external audit repositories (if using an external audit server). The evaluator shall also ensure the TSS describes what actions can be performed by the privileged user, if any, in each case where the audit trail cannot be written.

Guidance
The evaluator shall examine the operational guidance to ensure it describes what conditions result in the audit trail not being able to be written to, and how an Auditor recognizes that such a condition has occurred. The evaluator shall also examine the operational guidance to ensure it includes remedial steps for correcting these issues.

Test
The evaluator shall perform the following tests. The tests are conditional on where the audit data are being stored.

Test 1 demonstrates the capability of the TOE to react to an indication that the repository is full; this is always applicable if the audit data are stored locally. If the TOE has a means to detect that a remote audit repository is full, then this test will be run for those types of TOEs as well. Test 2 is only executed in cases where an external repository is supported, and tests the ability of the TOE to detect when the connection to the repository becomes unavailable:

- Test 1: (conditional) The evaluator shall cause the audit trail to become full, verify that the TSF behaves as documented in the TSS, and verify that a privileged user can perform the documented remedial steps.
- Test 2: (conditional) The evaluator shall cause the audit trail to become unavailable, verify that the TSF behaves as documented in the TSS, and verify that a privileged user can perform the documented remedial steps.

2.2.2 Cryptographic Support (FCS)

2.2.2.1 Cryptographic Operation (FCS_COP)

FCS_COP.1/STIP Cryptographic Operation (Data Encryption/Decryption in Support of STIP)

TSS
The evaluator shall verify that the TSS includes a description of encryption functions used for user data encryption, and that this description includes the key sizes and modes of operation.

The evaluator shall check that the TSS describes how the TOE satisfies constraints on key sizes specified in the SFR.

Guidance
The evaluator shall verify that the AGD guidance documentation includes instructions for meeting this requirement, including any configuration required to ensure the TSF only supports Triple Data Encryption Standard (TDES) with three distinct keys.

Test
Test 1: The evaluator shall verify the AES implementation used to support TLS cipher suites in accordance with the requirements by conducting the following tests:

AES-CCM Test

The evaluator shall perform the following tests.

Preconditions for testing:

- Specification of keys as input parameter to the function to be tested
- Specification of required input parameters such as modes
- Specification of user data (plaintext)
- Tapping of encrypted user data (ciphertext) directly in the non-volatile memory

These tests are intended to be equivalent to those described in the NIST document, “The CCM Validation System (CCMVS),” updated 9 Jan 2012, found at http://csrc.nist.gov/groups/STM/cavp/documents/mac/CCMVS.pdf.

It is not recommended that evaluators use values obtained from static sources such as http://csrc.nist.gov/groups/STM/cavp/documents/mac/ccmtestvectors.zip
or use values not generated expressly to exercise the AES-CCM implementation.

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

- **Keys:** All supported and selected key sizes (e.g., 128, 256 bits).
- **Associated Data:** Two or three values for associated data length: The minimum (≥ 0 bytes) and maximum (≤ 32 bytes) supported associated data lengths, and 2^16 (65536) bytes, if supported.
- **Payload:** Two values for payload length: The minimum (≥ 0 bytes) and maximum (≤ 32 bytes) supported payload lengths.
- **Nonces:** All supported nonce lengths (7, 8, 9, 10, 11, 12, 13) in bytes.
- **Tag:** All supported tag lengths (4, 6, 8, 10, 12, 14, 16) in bytes.

The testing for CCM consists of five tests. To determine correctness in each of the below tests, the evaluator shall compare the ciphertext with the result of encryption of the same inputs with a known good implementation.

Variable Associated Data Test

For each supported key size and associated data length, and any supported payload length, nonce length, and tag length, the evaluator shall supply one key value, one nonce value, and 10 pairs of associated data and payload values, and obtain the resulting ciphertext.

Variable Payload Text

For each supported key size and payload length, and any supported associated data length, nonce length, and tag length, the evaluator shall supply one key value, one nonce value, and 10 pairs of associated data and payload values, and obtain the resulting ciphertext.

Variable Nonce Test

For each supported key size and nonce length, and any supported associated data length, payload length, and tag length, the evaluator shall supply one key value, one nonce value, and 10 pairs of associated data and payload values, and obtain the resulting ciphertext.

Variable Tag Test

For each supported key size and tag length, and any supported associated data length, payload length, and nonce length, the evaluator shall supply one key value, one nonce value, and 10 pairs of associated data and payload values, and obtain the resulting ciphertext.

Decryption-Verification Process Test

To test the decryption-verification functionality of AES-CCM, for each combination of supported associated data length, payload length, nonce length, and tag length, the evaluator shall supply a key value and 15 sets of input plus ciphertext, and obtain the decrypted payload. Ten of the 15 input sets supplied should fail verification and five should pass.

Test 2 (conditional): The evaluator shall test the TDES implementation used to support TLS cipher suites in accordance with NIST SP 800-67 Rev 2, by conducting the following tests:

Variable Plaintext/Ciphertext Known Answer Test:

For i=1..64, the evaluator shall verify the encrypt functionality by using Key1=Key2=Key3=0x0101010101010101, and IV=0x0000000000000000, to encrypt plaintext p_1{i}=ith basis vector input as a type 2 input, and comparing the resulting ciphertext=c_1{i} output as a type 2 output to known results indicated in table A.1 of NIST SP800-20.

For i=1..64, evaluator shall verify the decrypt functionality by using Key1=Key2=Key3=0x0101010101010101, and IV=0x0000000000000000, to decrypt ciphertext, c_1{i} and verifying the resulting plaintext to p_1{i}, the ith basis vector.

Inverse/initial Permutation Known Answer Test:

For i=1..64, the evaluator shall verify the encrypt functionality by using Key1=Key2=Key3=0x0101010101010101, and IV=0x0000000000000000, to encrypt plaintext p_2{i}=c_1{i} from the Variable Plaintext Known Answer Test, input as a type 5 input, and verifying the resulting ciphertext, c_2{i} output as type 2 output, is equal to the ith basis vector, p_1{i}.

For i=1..64, the evaluator shall verify the decrypt functionality by using Key1=Key2=Key3=0x0101010101010101, and IV=0x0000000000000000, to decrypt ciphertext c_2{i]=p_1{i}, input as input type 5, and verifying the resulting plaintext, p_2{i} output as type 2 output, is equal to c_1{i}.

Variable Key Known Answer Test:

For i=1..64 not zero mod 8, the evaluator shall verify the encrypt function using Key1{i}=Key2{i}=Key3{i} equal to the vector consisting of a one in the ith position, zeros in all other positions not zero mod 8, and parity bits in positions 0 mod 8 computed to make each byte have odd parity, and using IV=0x0000000000000000, to encrypt plaintext p_3{i}=0x0000000000000000, input as a type 2 input, and comparing the resulting ciphertext, c_3{i} output as a type 2 output to known results indicated in table A.2 of NIST SP800-20..

For i=1..64 not zero mod 8, the evaluator shall verify the decrypt functionality using the same Key1{i}=Key2{i}=Key3{i} above, and IV=0x0000000000000000, to decrypt ciphertext c_3{i} and comparing the resulting plaintext to 0x0000000000000000.

Permutation Operation Known Answer Test:

For i=0..31, the evaluator shall verify the encrypt functionality by using Key1{i}=Key2{i}=Key3{i} equal to the round i key in table A.3 of NIST SP800-20, and IV=0x0000000000000000 to encrypt plaintext = 0x0000000000000000, and verifying that the resulting ciphertext c4{i} matches the known result for round I indicated in table A.3 of NSIT SP800-20.

For i=0..31, the evaluator shall verify the decrypt functionality by using Key1{i}=Key2{i}=Key3{i} equal to the round I key in table A.3 of NIST SP800-20, and IV=0x0000000000000000 to decrypt ciphertext c4{i} above, and verifying that the resulting plaintext for each round equals 0x0000000000000000.

Substitution Table Known Answer Test:

For i=0..18, the evaluator shall verify the encrypt functionality by using Key1{i}=Key2{i}=Key3{i} equal to the round i key in table A.4 of NIST SP800-20, and IV=0x0000000000000000 to encrypt the round i plaintext, p4{i} in table A.4 of NIST SP300-20, and verifying that the resulting ciphertext c4{i} matches the known result for round i indicated in table A.4 of NSIT SP800-20.

For i=0..18, the evaluator shall verify the decrypt functionality by using Key1{i}=Key2{i}=Key3{i} equal to the round i key in table A.4 of NIST SP800-20, and IV=0x0000000000000000 to decrypt ciphertext =c4{i} above, and verifying that the resulting plaintext matches p4{i} above.

Monte Carlo Test:

Three-key test:

- The evaluator shall conduct the Monte Carlo Test for the Cipher Block Chaining (CBC) mode of Triple Data Encryption Algorithm (TDEA) encryption indicated in NIST SP 800-20 Section 2.1.5.6 against the TOE, using three distinct keys, Key1 not equal to Key2, Key2 not equal to Key3 and Key3 not equal to Key1, and validate the results against a known good implementation of TDEA.
- The evaluator shall conduct the Monte Carlo Test for the CBC mode of TDEA decryption indicated in NIST SP 800-20 Section 2.2.5.6 against the TOE, using three distinct keys, Key1 not equal to Key2, Key2 not equal to Key3 and Key3 not equal to Key1, and validate the results against a known good implementation of TDEA.

2.2.2.2 Cryptographic Key Storage (FCS_STG_EXT)

FCS_STG_EXT.1 Cryptographic Key Storage

TSS
The evaluator will check the TSS to ensure it lists each persistent secret and private key needed to meet the requirements in the ST. For each of these items, the evaluator shall confirm that the TSS lists for what purpose it is used, and how it is stored, and that the storage is hardware-protected.

Guidance
There are no AGD evaluation activities for this requirement.

Test
There are no test evaluation activities for this requirement.

2.2.2.3 Thru-Traffic TLS Inspection Client Protocol (FCS_TTTC_EXT)

FCS_TTTC_EXT.1 Thru-Traffic TLS Inspection Client Protocol

FCS_TTTC_EXT.1.1

TSS
The evaluator will check the description of this protocol in the TSS to ensure that the TLS versions and cipher suites supported for inspection of TLS sessions are included. The evaluator shall check the TSS to ensure that the TLS versions and cipher suites specified for processing such traffic include those listed in FCS_TTTC_EXT.1.1, and no others. The evaluator shall ensure the TSS describes how the cipher suites

included in a Client Hello message to a specific requested server might be restricted in accordance with allowances described in the TLS session establishment policy.

Guidance
The evaluator shall check the guidance documentation to ensure it contains instructions on configuring the TOE so that the versions and cipher suites used conform with FCS_TTTC_EXT.1.1 and the configured TLS session establishment policy.

The evaluator shall verify that the AGD guidance includes instructions for setting the reference identifier to be used for the purposes of certificate validation in TLS.

Test
Setup: The evaluator shall establish one or more monitored clients and requested servers that are configured to pass TLS sessions through the TOE, and configure the SSL/TLS inspection proxy policy to use the inspection operation for these clients and servers with all supported versions and cipher suites in its allowed set. The evaluator shall configure the monitored client to present a TLS Client Hello with TLS version 1.2 and the full list of supported cipher suites, and use the SNI extension to indicate the DNS name of the requested server for each test. The evaluator shall establish a certification authority (the trusted CA) able to issue certificates for the servers as indicated in the following tests, and install the certification authority's certificate in appropriate trust anchors within the TSF to validate the issued certificates. Additional configuration instructions for the monitored client, the requested server or the server's certificate are indicated in each of the tests:

Test 1: For each version and cipher suite combination supported, as indicated in FCS_TTTC_EXT.1.1, the evaluator shall configure a server requested by a monitored client to negotiate the version and cipher suite, and issue the server a certificate from the trusted CA containing a subjectAltName (SAN) extension containing the expected DNS name of the server, and which is valid in accordance with FIA_X509_EXT.1/Rev. The evaluator shall then initiate a TLS session from a monitored client through the TOE to the requested server, as indicated in the SNI extension of the Client Hello, and observe that the TLS session between the TOE and the requested server cipher suites is successful. Additionally, the evaluator shall verify that the Client Hello sent from the TSF to the requested server contains the full, ordered list of cipher suites supported for the selected version in accordance with FCS_TTTC_EXT.1.4.

Test 2a: The evaluator shall choose a supported version and cipher suite combination. For each extendedKeyUsage condition for server certificates that allows the TLS session to be completed, as indicated in FIA_X509_EXT.1.1/STIP, the evaluator shall configure a requested server to negotiate the version and cipher suite combination and issue the requested server a new certificate from the trusted CA that has the indicated extendedKeyUsage condition, and is otherwise identical to the certificate used for the similarly configured server from Test 1. The evaluator shall configure the server to present the new certificate in its TLS handshake. The evaluator shall then make a TLS request in turn from a monitored client to each of the reconfigured servers through the TOE, and observe that the TLS session from the TOE to the requested server is established.

Test 2b: The evaluator shall establish a new certificate for a server as configured for Test 2a where the extendedKeyUsageextended key usage field is present, does not include either the 'Any' purpose or ServerAuthentication purpose and which does contain the CodeSigning purpose, and configure the server to present the new certificate in its TLS handshake. The evaluator shall make a request to that server from a monitored client through the TOE and verify that the TLS session between the TSF and the server is attempted, but fails.

Test 3: For each of the following, the evaluator shall issue a new certificate as specified from the trusted CA containing the indicated public key type for a server configured to negotiate a supported version and cipher suite as specified, so the server presents a certificate with a signature or static public key type that is incompatible with the negotiated cipher suite:

a) For a supported cipher suite that uses RSA for signature, the evaluator shall issue a certificate containing an Elliptic Curve Digital Signature Algorithm (ECDSA) public key to represent a server configured to negotiate the cipher suite
b) For a supported cipher suite that uses ECDSA for signature, the evaluator shall issue a certificate containing an RSA public key to represent a server configured to negotiate the cipher suite
c) For a supported cipher suite that uses RSA for key transport, the evaluator shall issue a certificate containing a Diffie-Hellman (DH) public key to represent a server configured to negotiate the cipher suite
d) For a supported cipher suite that uses RSA for key transport, the evaluator shall issue a certificate containing an Elliptic-Curve Diffie-Hellman (ECDH) public key to represent a server configured to negotiate the cipher suite
e) For a supported cipher suite that uses static DH key establishment, the evaluator shall issue a certificate containing an RSA public key to represent a server configured to negotiate the cipher suite
f) For a supported cipher suite that uses static DH key establishment, the evaluator shall issue a certificate containing an ECDH public key to represent a server configured to negotiate the cipher suite
g) For a supported cipher suite that uses static ECDH, the evaluator shall issue a certificate containing an RSA public key that represents a server configured to negotiate the cipher suite
h) For a supported cipher suite that uses static ECDH, the evaluator shall issue a certificate containing a DH public key that represents a server configured to negotiate the cipher suite.

The evaluator shall make, in turn, a TLS request to each so-configured server from a monitored client. In each case, the evaluator shall observe that the TSF attempts to establish a TLS session with the requested server and after the server negotiates the cipher suite, the evaluator shall send the new certificate in a server certificate message to the TSF in the place of the expected certificate message, and observe that the TSF does not establish a TLS session with the server.

Test 4: The evaluator shall configure a server to select the TLS_NULL_WITH_NULL_NULL cipher suite. The evaluator shall make a request from a monitored client to the so configured server and verify that the TLS session between the TSF and the server is attempted but not established.

Test 5: For each of the following, the evaluator shall configure a requested server to negotiate a supported version and cipher suite, as indicated, and use a valid certificate from the trusted CA, but send TLS messages as indicated and otherwise respond as a valid TLS server. For each in turn, the evaluator shall initiate a TLS connection between a monitored client and the requested server through the TOE and observe the indicated behavior of the TOE on receiving the server message:

- Test 5.1: Configure the requested server to send an undefined TLS version (for example, 1.5 represented by the two bytes 03 06) and verify that the TSF rejects the connection.
- Test 5.2: Configure the requested server to send a Server Hello with the TLS version set to SSL 3.0 (represented by the two bytes 03 00) and verify that the TSF rejects the connection.
- Test 5.3: Configure the requested server to use a DHE cipher suite and configure the requested server to send a Server Hello message with at least one byte in the server's nonce

in the Server Hello handshake message modified from the expected response, and verify that the TSF rejects the connection. Repeat this test using a requested server configured to use an ECDHE cipher suite and observe that the TSF rejects the connection.

- Test 5.4: Configure the requested server to respond to a Client Hello with a cipher suite that is not supported by the TSF, and therefore not present in the Client Hello received by the server. The evaluator shall verify that the TSF rejects the connection.
- Test 5.5: Using requested servers configured to use a cipher suite using DHE, and send a KeyExchange handshake message with an invalid signature (e.g., by modifying the signature block in the expected KeyExchange handshake message), and verify that the TSF rejects the connection. Repeat this test with a requested server configured to use a cipher suite using ECDHE and verify that the TSF rejects the connection.
- Test 5.6: Configure the requested server to respond with an invalid Server Finished message (e.g., by modifying a byte in the expected Server Finished handshake message) and verify that the TSF rejects the connection.

FCS_TTTC_EXT.1.2

TSS

The evaluator shall ensure that the TSS describes the TSF method of establishing all reference identifiers for through-traffic processing, including which types of reference identifiers are supported and whether IP addresses and wildcards are supported. The evaluator shall ensure that the TSS describes how the TSF determines reference identifiers from the various identity attributes associated to the requested server and match what is expected by the monitored client. The evaluator shall ensure that the TSS describes how the reference identifiers are matched to the identifiers presented in the server's certificate.

Guidance

The evaluator shall ensure that the guidance contains instructions on establishing reference identifiers if supported through an administrative interface.

Test

Using the setup for FCS_TTTC_EXT.1.1, the evaluator shall perform the following tests. Note that Test 1 of FCS_TTTC_EXT.1.1 confirms the TSF properly validates the reference ID of a certificate containing a DNS name in the subjectAltName matching the SNI contained in the Client Hello of a monitored client, and is not repeated. The remaining tests cover support for other name forms and negative testing.

Test 1: The evaluator shall issue a certificate from the trusted CA that represents a requested server that contains a SAN extension with a valid DNS name type. The evaluator shall configure the requested server to use a valid, supported version and cipher suite combination consistent with the certificate, and provide the certificate in response to a TLS request. The evaluator shall establish a TLS session from a monitored client to the requested server through the TOE using an SNI extension in the Client Hello that does not match the name in the certificate. The evaluator shall ensure the TOE does not succeed in establishing a TLS connection to the requested server.

Test 2: [conditional on the TSF supporting additional reference identifiers not used in FCS_TTTC_EXT.1.1 test 1]: For each additional reference identifier described in the TSS, the evaluator shall establish a monitored client and requested server that causes the TSF to establish a reference identifier of the indicated type. The evaluator shall issue a new certificate for the requested server from the trusted CA which contains a name of the same type in the subject name or the SAN extension as appropriate for the reference identifier, and that matches the reference identifier. The evaluator shall configure the requested server to use a valid, supported version and cipher suite combination consistent with the certificate, and provide the new certificate in a valid server certificate message. The evaluator shall initiate a TLS session from the monitored client to the requested server through the TOE and observe that the TSF establishes the TLS session to the requested server.

Test 3: [conditional on the TSF supporting additional reference identifiers] For each additional reference identifier described in the TSS, the evaluator shall establish a monitored client and requested server to cause the TSF to use the indicated reference identifier and issue a certificate for a server from the trusted CA that contains a name of the same type in the subject name or the SAN extension as appropriate for the reference identifier, but that does not match the reference identifier. The evaluator shall configure the requested server to use a valid, supported version and cipher suite combination consistent with the certificate, and provide the new certificate in a valid server certificate message. The evaluator shall initiate a TLS session between the monitored client and the server through the TOE and observe that the TSF does not establish a valid TLS session to the requested server.

Test 4: The evaluator shall perform the following wildcard tests with each type of reference identifier based on DNS name types. This test is not intended for reference identifiers using IP addresses. The support for wildcards is intended to be optional. If wildcards are supported, the first, second, and third tests below shall be executed. If wildcards are not supported, then the fourth test below shall be executed. For each test, the evaluator shall establish a monitored client and requested server, issue the requested server a valid certificate with the specified identifier from the trusted CA, and configure the server to use a valid version and cipher suite combination consistent with the certificate. The evaluator shall configure the monitored client and requested server in such a way that causes the TSF to establish the indicated reference identifiers. For each certificate identifier presented and for each reference identifier specified, the evaluator shall initiate a TLS session between the monitored client and requested server through the TSF, causing the TSF to attempt to match the presented identifier to the established reference identifier and observe the indicated result:

- Test 4.1: [conditional]: If wildcards are supported, the evaluator shall use a server certificate containing a wildcard that is not in the left-most label of the presented identifier (e.g., foo.*.example.com) and verify that the connection fails.
- Test 4.2: [conditional]: If wildcards are supported, the evaluator shall use a server certificate containing a wildcard in the left-most label but not preceding the public suffix (e.g., *.example.com). The evaluator shall cause the reference identifier to have a single left-most label (e.g., foo.example.com) and verify that the connection succeeds. The evaluator shall cause the reference identifier to be without a left-most label as in the certificate (e.g., example.com) and verify that the connection fails. The evaluator shall cause the reference identifier to have two left-most labels (e.g., bar.foo.example.com) and verify that the connection fails.
- Test 4.3: [conditional]: If wildcards are supported, the evaluator shall use a server certificate containing a wildcard in the left-most label immediately preceding the public suffix (e.g., *.com). The evaluator shall cause the reference identifier to have a single left-most label (e.g., foo.com) and verify that the connection fails. The evaluator shall cause the reference identifier to have two left-most labels (e.g., bar.foo.com) and verify that the connection fails.
- Test 4.4: [conditional]: If wildcards are not supported, the evaluator shall use a server certificate containing a wildcard in the left-most label (e.g., *.example.com). The evaluator shall cause the reference identifier to have a single left-most label (e.g., foo.example.com) and verify that the connection fails.

FCS_TTTC_EXT.1.3

TSS

The evaluator shall ensure that the TSS describes the TSF's behavior for certificate validation results, including any dependencies on the configured TLS session establishment policy for establishing a TLS session when revocation information is not available, as indicated in the selection for FIA_X509_EXT.2.2.

Guidance

If the TSS indicates that the TLS session establishment policy is used to determine the TSF's behaviour for establishing a TLS session for through-traffic processing when certificate revocation information is not available, the evaluator shall validate that the AGD guidance includes instructions to configure the allowances to allow or not allow such connections.

Test

Setup: Using the setup for test 1 of FCS_TTTC_EXT.1.1, the evaluator shall establish one or more trusted subordinate CAs by issuing them valid CA certificates from the trusted CA. The evaluator shall establish a certificate status capability for both the trusted subordinate CAsand the trusted CA that uses a method supported by the TSF. The evaluator shall also establish an untrusted CA to use a self-signed CA certificate not loaded into the TSF trust store. The evaluator shall establish one or more requested servers to use a valid TLS version and cipher suite combination and to respond using valid TLS handshake messages except for the certificate message and certificate verify messages as described in each test. The evaluator shall issue certificates for the following tests to the requested server that have the indicated failures, initiate a TLS session from a monitored client through the TOE to the requested server presenting the certificate with the indicated failures, and verify that the TSF terminates the TLS handshake with the requested server:

Test 1: The evaluator shall issue a valid certificate for the requested server from the untrusted CA. The evaluator shall confirm that the TSF rejects the TLS session with the requested server when it presents a valid certificate message and certificate verify message using the certificate issued by the untrusted CA.

Test 2: The evaluator shall issue a valid certificate for the requested server by the subordinate CA, but not load it into the TSF trust store, and shall ensure the requested server does not provide the subordinate CA in the certificate chain. The evaluator shall confirm that the TSF rejects the TLS session with the requested server when the server presents a valid certificate message and certificate verify message using the certificate that does not properly chain to a trusted root.

Test 3: The evaluator shall establish a valid certificate for the requested server issued by the subordinate CA, and establish valid revocation information from the trusted subordinate CA using a supported mechanism for end-entity certificates, indicating the requested server's certificate is revoked. The evaluator shall ensure the subordinate CA is included in the certificate chain provided by the requested server and the revocation information is available. The evaluator shall confirm that authentication fails.

Test 4: The evaluator shall issue a valid certificate for the requested server from the subordinate CA, and establish valid revocation information from the subordinate CA using a supported mechanism for end-entity certificates, indicating the requested server's certificate is revoked. The evaluator shall ensure the subordinate CA is included in the certificate chain provided by the requested server and ensure the revocation information is not available to the TSF. The evaluator shall confirm that the default behavior for revocation information not available is performed by the TSF. If this behavior is configurable (the first item is claimed in the first selection for FIA_X509_EXT.2.2), the evaluator shall in turn follow AGD documentation to configure the TSF for each response, and initiate the TLS session from the monitored client to demonstrate the TSF performs the configured behavior.

Test 5: The evaluator shall issue a valid certificate for the requested server from the subordinate CA, and generate valid revocation information from the trusted subordinate CA using a supported mechanism for end-entity certificates, indicating the requested server's certificate is valid, and generate valid revocation information from the trusted CA using a supported mechanism for CA certificates, indicating the subordinate CA's certificate is revoked. The evaluator shall ensure the subordinate CA is included in the certificate chain provided by the requested server and all revocation information is available. The evaluator shall confirm that authentication fails.

Test 6: The evaluator shall issue a valid certificate for the requested server from trusted subordinate CA, and generate valid revocation information from the trusted subordinate CA using a supported mechanism for end-entity certificates indicating the requested server's certificate is valid, and generate valid revocation information from the trusted CA using a supported mechanism for CA certificates, indicating the subordinate CA's certificate is revoked. The evaluator shall ensure the subordinate CA is included in the certificate chain provided by the requested server and the revocation information from the subordinate CA is available, but revocation information from the trusted CA is not available to the TSF. The evaluator shall confirm that the default behavior for revocation information not available is performed by the TSF. If this behavior is configurable (the first item is claimed in the selection for FIA_X509_EXT.2.2), the evaluator shall, in turn, follow AGD documentation to configure the TSF for each response, and initiate the TLS session from the monitored client to demonstrate the TSF performs the configured behavior.

Test 7: The evaluator shall issue a valid certificate from the trusted CA for the requested server that expires prior to initiating the TLS session from the monitored client, and generate revocation information indicating the requested server's certificate is not revoked. The evaluator shall initiate a TLS session from the monitored client to the requested server through the TOE after the certificate has expired, and ensure the certificate status information from the trusted CA is available to the TSF. The evaluator shall observe that the TSF fails to establish the TLS connection with the requested server, demonstrating that a server using a certificate which has passed its expiration date results in an authentication failure.

Test 8: The evaluator shall establish a new subordinate CA from the trusted CA, by issuing the subordinate CA a certificate that expires prior to initiating the TLS session from the monitored client. The evaluator shall issue a valid certificate for the requested server from the subordinate CA but which does not expire prior to initiating the TLS session from the monitored client and generate valid revocation information using supported methods indicating both the subordinate CA and the server's certificate are not revoked. The evaluator shall initiate a TLS session from the monitored client to the requested server through the TOE and observe that the TLS session between the TSF and requested server fails, demonstrating that a server using a valid certificate (not yet expired) issued by a subordinate CA that has passed its expiration date results in an authentication failure.

FCS_TTTC_EXT.1.4

TSS

The evaluator shall ensure that the TSS includes a description of cipher suite dependence on the TLS session establishment policy allowances and that the ordering of cipher suites within a Client Hello sent by the TSF to a requested server is in accordance with FCS_TTTC_EXT.1.4.

Guidance

The evaluator shall ensure that the AGD guidance documents include instructions on configuring the TLS session establishment policy to restrict the inclusion of cipher suites in a Client Hello to a particular requested server for through-traffic processing.

Test

Setup: The evaluator shall establish one or more monitored clients and requested servers that are configured to pass TLS sessions through the TOE, and configure the TLS session establishment policy to use the inspection operation for these clients and servers, allowing negotiation of TLS 1.2, but not any other version, and allowing only a subset of cipher suites indicated in FCS_TTTC_EXT.1.1 consisting of a single cipher suite supported for each supported TLS version. The evaluator shall issue certificates for the servers that are valid in accordance with FIA_X509_EXT.1/STIP, and install the appropriate trust anchors within the TSF to validate the certificates (the trusted CA). Additional configuration instructions for the monitored client, the requested server or the server's certificate are indicated in each of the tests.

Test 1: For each supported version other than TLS 1.2, the evaluator shall configure a server requested by a monitored client to negotiate the version and an allowed cipher suite for that version, regardless of the Client Hello message received. The evaluator shall, in turn, establish a TLS connection from the monitored client to the requested server through the TOE and observe that the TSF sends a Client Hello to the requested server that includes the allowed version and cipher suites, in the order indicated in FCS_TTTC_EXT.1.1. The evaluator shall confirm that the requested server sends the TOE a Server Hello indicating the configured version and cipher suite, and confirm that the TSF responds by terminating the TLS handshake with the requested server.

Test 2: The evaluator shall follow AGD guidance to reconfigure the TLS session establishment policy to allow any supported version to the requested servers, but only allow the subset of cipher suites as indicated in the setup. For each supported version, the evaluator shall configure the requested server to negotiate the version and a valid cipher suite for that version which is included in FCS_TTTC_EXT.1.1, but not allowed for the requested server, as in the setup, regardless of the Client Hello received. The evaluator shall in turn initiate a TLS session from the monitored client to the requested server configured for the supported version, through the TOE. The evaluator shall observe that the Client Hello generated by the TSF specifies version 1.2 and the allowed cipher suites in the order indicated in FCS_TTTC_EXT.1.1. The evaluator shall confirm that the server sends the TOE a Server Hello message as configured and confirm that the TSF responds by terminating the TLS handshake with the requested server.

FCS_TTTC_EXT.5 Thru-Traffic TLS Inspection Client Support for Supported Groups Extension

TSS

The evaluator shall check the TSS and ensure that it describes the supported groups extension. The evaluator shall ensure the TSS describes any configurable aspects of the use of supported groups, including configuration of allowances controlling the use of curves other than the NIST named curves, secp256r1, secp384r1, or secp521r1, if supported.

Guidance

If the TSS indicates that the TOE must be configured to meet FCS_TTTC_EXT.5.1 requirements for the Supported Elliptic Curves Extension, the evaluator shall verify the AGD guidance includes instructions for configuration of the Supported Elliptic Curves Extension.

Test

Test 1: The evaluator shall establish a requested server to negotiate a supported version and cipher suite using ECDSA signature and ECDHE key exchange using a custom elliptic curve not included in FCS_TTTC_EXT.5.1, regardless of the Client Hello received. The evaluator shall follow AGD guidance to configure the TLS session establishment policy so the TSF inspects traffic to the so configured server from a monitored client. The evaluator shall initiate a TLS session to the requested server from the monitored client through the TOE and observe that the TSF sends a Client Hello to the requested server, and receives the configured server Hello Message from the requested server. The evaluator shall confirm that the TSF terminates the TLS handshake with the requested server.

Test 2: (conditional on whether additional elliptic curves are supported and managed via TLS session establishment policy allowances):

For each elliptic curve claimed in the assignment of FCS_TTTC_EXT.5.1, the evaluator shall establish a requested server to use the curve in a TLS handshake with a supported version and cipher suite using ECDSA signature and ECDHE key exchange, using the curve. The evaluator shall follow AGD guidance to configure the TLS session establishment policy to perform the inspection operation for TLS traffic to the server and allow the server to negotiate the additional curve. The evaluator shall initiate a TLS request from a monitored client to the server and observe that the Client Hello sent from the TSF to the requested includes the allowed curve. The evaluator shall confirm that the configured server sends a Server Hello message to the TSF that selects the curve, and that the TSF accepts the connection.

Test 3: (conditional on whether additional elliptic curves are supported and managed via TLS session establishment policy allowances):

For each elliptic curve claimed in the assignment of FCS_TTTC_EXT.5.1, the evaluator shall establish a requested server to use the curve in a TLS handshake with a supported version and cipher suite using ECDSA signature and ECDHE key exchange, regardless of the Client Hello received. The evaluator shall follow AGD guidance to configure the TLS session establishment policy to perform the inspection operation for TLS traffic to the server, but not allow the server to negotiate the additional curve. The evaluator shall initiate a TLS request from a monitored client to the server and observe that the Supported Groups extension Client Hello sent from the TSF to the requested does not include the curve. The evaluator shall confirm that the configured server sends a Server Hello message to the TSF that selects the curve, and that the TSF terminates the TLS handshake with the requested server.

2.2.2.4 Thru-Traffic TLS Inspection Server Protocol (FCS_TTTS_EXT)

FCS_TTTS_EXT.1 Thru-Traffic TLS Inspection Server Protocol

FCS_TTTS_EXT.1.1

TSS

The evaluator shall check the description of this protocol in the TSS to ensure that the TLS versions and cipher suites supported for establishing a TLS session with a monitored client include those listed in FCS_TTTS_EXT.1.1 and determine if configuration is needed to restrict the use of other versions or cipher suites. The evaluator shall ensure the TSS description of TLS includes all TLS server handshake messages and error alerts used, and conditions for which error alerts are used.

Guidance

The evaluator shall check the guidance documentation to ensure it contains instructions as indicated in the TSS on configuring the TOE so that the versions and cipher suites used conform with FCS_TTTS_EXT.1.1.

Test

Setup: The evaluator shall establish one or more monitored clients and servers that are configured to pass TLS sessions through the TOE, and configure the TLS session establishment policy to use the inspection operation for these clients and servers with the required versions and cipher suites. The evaluator shall establish certificates for the servers that are valid in accordance with FIA_X509_EXT.1/STIP and install the appropriate trust anchors within the TSF to validate the certificates. Additional configuration instructions for the monitored client, the requested server or the server's certificate are indicated in each of the tests:

Test 1: For each version and each valid cipher suite for the version, as indicated in FCS_TTTS_EXT.1.1, the evaluator shall configure the monitored client to include the version and a list consisting of a single element specifying the indicated cipher suite in the Client Hello. The evaluator shall follow AGD guidance to configure the TLS session establishment policy to allow the TSF to negotiate the version and cipher suite for that client. The evaluator shall then initiate a TLS session from the so configured monitored client through the TOE to a requested server and observe that a TLS session between the monitored client and the TSF using the specified version and cipher suite is successful.

Test 2: For each supported version indicated in FCS_TTTS_EXT.1.1, the evaluator shall select a valid cipher suite in FCS_TTTS_EXT.1.1 and configure a monitored client to present the version and a cipher suite list containing the single cipher suite. The evaluator shall follow AGD guidance to configure the TLS session establishment policy so that use of the cipher suite is not allowed for the client. The evaluator shall initiate a TLS session from the monitored client through the TOE to a requested server and observe that a TLS session between the monitored client and the TSF is denied.

Test 3: For each supported version other than TLS 1.2 indicated in FCS_TTTS_EXT.1.1, the evaluator shall configure a monitored client to include the version and a cipher suite list consisting of a cipher suite valid for TLS 1.2 and another valid for the version in its Client Hello. The evaluator shall follow AGD guidance to configure the TLS session establishment policy to only allow the client to use TLS 1.2. The evaluator shall initiate a TLS session from the monitored client to a requested server through the TOE and observe that a TLS session between the monitored client and the TSF is not established.

Test 4: For each supported version indicated in FCS_TTTS_EXT.1.1, the evaluator shall configure a monitored client to include the version and a cipher suite list consisting of a single TLS_NULL_WITH_NULL_NULL cipher suite. The evaluator shall follow AGD guidance to configure the TLS session establishment policy to allow any version and cipher suite for the client. The evaluator shall initiate a TLS session from the monitored client to a requested server through the TOE and observe that the TLS session between the monitored client and the TSF is denied.

FCS_TTTS_EXT.1.2

TSS

The evaluator shall verify that the TSS contains a description of the denial of SSL versions and TLS versions consistent with the selections in FCS_TTTS_EXT.1.2 and determine if configuration is needed to restrict the use of those versions.

Guidance

The evaluator shall check the guidance documentation to ensure it contains instructions on configuring the TOE as indicated in the TSS so that the versions indicated in FCS_TTTS_EXT.1.2 are denied.

Test

Test 1: For each SSL or TLS version indicated in FCS_TTTS_EXT.1.2, the evaluator shall configure a monitored client to include the version in its Client Hello. The evaluator shall initiate a TLS session from the monitored client to a requested server through the TOE and observe that a TLS session between the monitored client and the TOE is not established.

FCS_TTTS_EXT.1.3

TSS

The evaluator shall verify that the TSS describes the TOE's supported key agreement parameters for a server key exchange message with a monitored client to ensure TOE supports the required key agreement parameters and can be limited to use only those indicated in FCS_TTTS_EXT.1.3.

Guidance

The evaluator shall check the guidance documentation to ensure it contains instructions on configuring the TOE so that the key exchange parameters used conforms with FCS_TTTS_EXT.1.3.

Test

Setup: The evaluator shall establish one or more monitored clients and servers that are configured to pass TLS sessions through the TOE, and configure the TLS session establishment policy to use the inspection operation for these clients and servers with the required versions and cipher suites. The evaluator shall establish certificates for valid servers in accordance with FIA_X509_EXT.1/STIP and install the appropriate trust anchors within the TSF to validate the certificates. Additional configuration instructions for the monitored client, the requested server, or the server's certificate are indicated in each of the tests.

Test 1: For each of the key parameter selections in FCS_TTTS_EXT.1.3, the evaluator shall configure a monitored client to use a valid supported version and cipher suite combination that supports the key parameter, and follow AGD guidance to configure the TSF to use a cipher suite supporting the parameters. The evaluator shall initiate a TLS session from the monitored client to a requested server through the TOE, and observe that a TLS session between the monitored client and the TLS uses the key parameters and is successful.

Test 2: The intent of this test is to show that the TSF properly handles unexpected KeyExchange messages from a client that does not agree with the negotiated cipher suite.

For each of the key parameter selections claimed for FCS_TTTS_EXT.1.3, the evaluator shall configure a monitored client and follow AGD guidance to configure the TSF to use a cipher suite supporting the parameters.

For each such configuration, the evaluator shall, in turn, initiate a number of TLS sessions from the monitored client to a requested server through the TOE, interrupting the TLS exchanges after receiving a server certificate from the TSF and sending the specified client KeyExchange message and observe the results as indicated below:

a) For a cipher suite that uses RSA for key transport, the evaluator shall, in turn, perform each of the following:

i. In the first instance of test 2.a, the evaluator shall send a KeyExchange message of RSA type with the EncryptedPreMasterSecret field consisting of a randomly generated value of size equal to the size of the EncryptedPreMasterSecret expected in the key parameter. The evaluator shall observe that the TSF sends a fatal TLS alert message and note the specific alert type received agrees with the TSS description of error messages.
ii. In the second instance of test 2.a, the evaluator shall send a KeyExchange message of RSA type with the EncryptedPreMasterSecret field consisting of a randomly generated value of size 1024 bits. The evaluator shall observe that the TSF sends a fatal TLS alert message.
iii. In the third instance of test 2.a, the evaluator shall send the TSF a KeyExchange message of DHE type containing a randomly generated ClientDiffieHellmanPublic value of size 2048 bits, and observe that the TSF sends a fatal TLS alert message and notes whether the error message is different than that received test 2.a.i.
iv. in the fourth instance of test 2.a, the evaluator shall send the TSF a KeyExchange message of ECDH type, containing a random point on a curve supported by the TSF, in a EC point format supported by the TSF. The evaluator shall observe that the TSF sends a fatal TLS alert message and notes whether the error message is different than that received in test 2.a.i.

If the alert messages in 2.a.iii and 2.a.iv are identical to that received in 2.a.i, the evaluator shall attempt to verify that the errors are a result of the unexpected KeyExchange message, and not just due to an invalid finished message. It might be necessary to configure additional (debug) logs to be generated by the TSF or examine detailed behavior of the TSF to distinguish unexpected KeyExchange messages from other errors.

b) For a cipher suite that uses ephemeral DH key establishment:

i. In the first instance of test 2.b, the evaluator shall modify a byte in the ClientDiffieHellmanPublic value produced by the client, send the modified KeyExchange message to the TSF, and observe that the TSF sends a fatal TLS alert message and note that the specific error message agrees with the TSS description of error messages.
ii. In the second instance of test 2.b, the evaluator shall ensure the TSF is not configured to request client authentication. The evaluator shall send a KeyExchange message consisting of a null value, specifying an implicit Client DiffieHellman Public key. The evaluator shall send the modified KeyExchange message to the TSF, and observe that the TSF sends a fatal TLS alert message and notes whether the error message is different than that received in test 2.b.i.
iii. In the third instance of test 2.b, the evaluator shall send the TSF a KeyExchange message of RSA type, containing a randomly generated EncryptedPreMasterSecret value of size 2048 bits. The evaluator shall observe that the TSF sends a fatal TLS alert message and notes whether the error message is different than that received in test 2.b.i.
iv. [conditional on client authentication support]: In the fourth instance of test 2.b, the evaluator shall configure the TSF to request client authentication. After the TSF sends the client certificate request message, the evaluator shall send the TOE a valid client certificate message followed by a KeyExchange message of ECDH type that contains a random point on a curve supported by the TSF in an ECpoint format supported by the TSF. The evaluator shall observe that the TSF sends a fatal TLS alert message and notes whether the error message is different than that received in test 2.b.i.

If the error messages in 2.b.ii, 2.b.iii or 2.b.iv are identical to that provided in 2.b.i, the evaluator shall attempt to verify that the errors are a result of the unexpected KeyExchange message, and not just due to an invalid finished message. It might be necessary to configure additional (debug) logs to be generated by the TSF or examine detailed behavior of the TSF to distinguish unexpected KeyExchange messages from other errors.

c) If the cipher suite uses ephemeral ECDH key establishment

   i. In the first instance of test 2.c, the evaluator shall replace the EC point in the KeyExchange message produced by the client with a random point on the curve specified by the TSF's Server key exchange message, using the same EC point format used in the client's expected KeyExchangeMessage. The evaluator shall observe that the TSF sends a fatal TLS alert message and the specific alert message agrees with the error message description in the TSS.
   ii. In the second instance of test 2.c, the evaluator shall ensure the TSF is not configured to request client authentication, and send the TSF a KeyExchange message consisting of the null value, indicating an implicit client Elliptic Curve Diffie Hellman Public key. The evaluator shall observe that the TSF sends a fatal TLS alert message and notes whether the error message is different than that received in test 2.c.i.
   iii. In the third instance of test 2.c, the evaluator shall send the TSF a KeyExchange message of RSA type with a randomly generated 2048-bit value used for the EncryptedPreMasterSecret value. The evaluator shall observer that the TSF sends a fatal TLS alert message and notes whether the error message is different than that received in test 2.c.i.
   iv. In the fourth instance of test 2.c, the evaluator shall send the TSF a KeyExchange message of type DH with a randomly generated 2048-bit value for the ClientDiffieHellman value in place of the ephemeral public key. The evaluator shall observe that the TSF sends a fatal TLS alert message and notes whether the error message is different than that received in test 2.c.i.

If the error messages received in 2.c.ii, 2.c.iii, or 2.c.iv are identical to that received in 2.c.i, the evaluator shall attempt to verify that the errors are a result of the unexpected KeyExchange message, and not just due to an invalid finished message. It might be necessary to configure additional (debug) logs to be generated by the TSF or examine detailed behavior of the TSF to distinguish unexpected KeyExchange messages from other errors.

d) (Conditional on support for client authentication): The evaluator shall configure the TSF to request client authentication. For a cipher suite that uses static DH for key transport, the evaluator shall send the TSF a valid client certificate message, followed by a KeyExchange message of DHE type containing a randomly generated ClientDiffieHellmanPublic value of size 2048 bits, and observe that the TSF sends a fatal TLS alert message.

e) For a cipher suite that uses static ECDH for key transport, the evaluator shall send the TSF a valid certificate message, followed by a KeyExchange message of ECDHE type, containing a random point on a curve supported by the TSF, in a ECpoint format supported by the TSF, and observe that the TSF sends a fatal TLS alert message.

Test 3: The intent of this test is to ensure the TSF, when negotiating cipher suites using RSA key transport, responds to invalid RSA KeyExchange messages consistently in order to resist a well-known class of chosen ciphertext attacks against RSA key transport mechanisms, which are especially problematic in TLS 1.0.

Initial setup: The evaluator shall establish a monitored client with full debugging and control of the TLS functions to send a TLS Client Hello indicating support for TLS 1.0 and a single cipher suite using RSA key transport. The evaluator shall establish a requested server configured to negotiate TLS 1.0 with the cipher suite indicated by the monitored client. The evaluator shall configure the TSF to inspect traffic between the monitored client and requested server and to allow the version and cipher suite for the client and server, and note this initial configuration for subsequent sub-tests:

Test 3, part a: The evaluator shall send a Client Hello from the monitored client to the requested server and observe that the Server Hello from the TSF selects TLS 1.0 and the desired cipher suite in its Server Hello message. The evaluator shall note the size and formatting of pre-master secret input to the client's KeyExchange message, continue the handshake from the client, and confirm that the TSF successfully establishes a TLS connection with the client.

Test 3, part b: The evaluator shall terminate the TLS sessions and restore the TSF, monitored client and requested server to the initial configuration for Test 3 above. The evaluator shall compute the following KeyExchange based on encrypting the following tailored messages with the server's public key, using a random value, *ran*, of size equal to that of the correctly computed pre-master secret, but having a different value, and properly formatted padding, pad(), of length determined so that the message is of the proper size.

- M1= 0x0002|| pad()||0x00||TLSversion||*ran*
- M2= 0x4117|| pad()
- M3= 0x0002|| pad()||0x0011
- M4= 0x0002|| pad()
- M5= 0x0002|| pad()||0x00||0x0202||*ran*

For each message in turn, the evaluator shall forward the KeyExchange message including the encrypted message to the TSF as part of a complete TLS handshake with the server, and observe the TLS error alert response provided by the TSF. Between each iteration, the evaluator shall terminate any residual TLS sessions, reset any cache, and restore the configuration of the monitored client, requested server, and TOE to its initial configuration for Test 3.

Test 3, part c: The evaluator shall observe that each error alert response provided by the TSF for the iterations in part b match the description in the TSS and is identical for each message M1 through M5.

2.2.3 User Data Protection (FDP)

2.2.3.1 Certificate Usage (FDP_CER_EXT)

FDP_CER_EXT.1 Certificate Profiles for Server Certificates

TSS
The evaluator shall examine the TSS to ensure it describes the certificate profile function in accordance with FDP_CER_EXT.1.1 The TSS shall describe how certificate profiles are configured and then selected to issue certificates in accordance with FDP_CER_EXT.1.2.

Guidance
The evaluator shall examine the operational guidance to ensure that instructions are available to configure certificate profiles used for certificate generation in accordance with this requirement.

Test

The evaluator shall perform the following tests:

Test 1: The evaluator shall configure a certificate profile using the available guidance, and establish a server with a certificate that satisfies FDP_CER_EXT.1.2 items a, b, e, f, h, i, j, and k, has valid values in all extensions in item g (a-e), and passes all certificate validation criteria as a TLS server certificate (having extended key usage field of server authentication) in FIA_X509_EXT.1/Rev. The evaluator shall establish a monitored client and request a TLS session to the server through the TOE so that the inspection operation is implemented, and then examine the certificate received at the client from the TOE to ensure it matches the configured certificate profile.

Test 2: The evaluator shall specifically examine the certificate generated in Test 1 and compare it to both the embedded CA's certificate and the requested server's certificate to ensure that it satisfies all field constraints in FDP_CER_EXT.1.2, FDP_CER_EXT.1.3, and FDP_CER_EXT.1.4 as configured in the certificate profile.

Test 3: The evaluator shall conduct the following tests by establishing a server with certificate identical to that used in Test 1, except for the differences described as follows (each in turn). The evaluator shall make any configuration changes to the TOE as indicated, establish a monitored client, and submit a TLS request for the server through the TOE so that the inspection operation is performed, and observe the certificate received at the monitored client has the indicated features:

- **notBefore field test:** The evaluator shall assign a notBefore value in the established server certificate that precedes both the current time and the value of notBefore field in the TOE's embedded CA's certificate, and observe that the generated certificate has a notBefore value that does not precede the current time.
- **notAfter field test a:** The evaluator shall configure the maximum validity duration so that the notAfter value of the TOE's embedded CA certificate does not exceed the current time by more than the maximum validity duration. The evaluator shall assign a notAfter value in the established server certificate that exceeds the current time by more than the maximum validity period, and observe that the notAfter field of the generated certificate has a notAfter value that does not exceed the notAfter value of the embedded CA's certificate
- **notAfter field test b:** The evaluator shall configure the maximum validity duration so that the notAfter value in the TOE's embedded CA certificate exceeds the current time by more than maximum validity duration, assign a notAfter value in the established server certificate that exceeds the notAfter value in the TOE's embedded CA's certificate, and observe that the notAfter value of the generated certificate does not exceed the current time by more than the maximum validity duration.
- **notAfter field test c:** The evaluator shall assign a notAfter value in the established server certificate that precedes both the notAfter value in the TOE's embedded CA's certificate, and the current time plus the maximum validity duration, and observe that the generated certificate has a notAfter value that does not exceed the notAfter value of the established server's certificate.
- **keyUsage field test:** The evaluator shall assign a KeyUsage value in the established server certificate that indicates additional usage indicators (e.g., keyCertSign) and observe that generated certificate has only the digitalSignature and/or keyEncipherment indicators.
- **extendedKeyUsage field test a:** The evaluator shall omit the extendedKeyUsage field in the established server certificate and observe that the generated certificate contains the extendedKeyUsage field with value indicating only TLS server authentication.

- **extendedKeyUsage field test b:** The evaluator shall populate the extendedKeyUsage field in the established server's certificate to indicate both TLS server authentication and code signing, and observe that the generated certificate only indicates TLS server authentication.
- **extendedKeyUsage field test c:** The evaluator shall populate the extendedKeyUsage field in the established server's certificate to indicate any usage, and observe that the generated certificate only indicates TLS server authentication.

FDP_CER_EXT.2 Certificate Request Matching of Server Certificates

TSS

The evaluator shall examine the TSS to ensure it describes the linkage between submitted requests and issued certificates and indicates where this linkage is recorded.

Guidance

The evaluator shall examine the operational guidance to ensure it contains instructions for how to trace a submitted request to an issued certificate and vice versa via the TOE's interface.

Test

The evaluator shall perform the following test:

Test 1: The evaluator shall configure a certificate profile using the available guidance and establish a server with a server certificate which is consistent (would allow the CA to issue a certificate) with the profile. The evaluator shall establish a client and request a TLS session with the server so that the inspection operation is selected. The evaluator shall follow the administrative guidance for determining the linkage and verify that it provides linkage between the validated server certificate and issued certificate.

FDP_CER_EXT.3 Certificate Issuance Rules for Server Certificates

TSS

The evaluator shall examine the TSS to ensure it describes the certificate issuance rules, and verify that any interfaces available for external certificate requests (CMC, EST, PKCS#10 or any other request format) are identified.

Guidance

The evaluator shall examine the operational guidance to ensure that it contains instructions for any configuration aspects of any certificate issuance approval function and the steps needed to prevent receipt and approval of external requests.

Test

The evaluator shall perform the following test:

Test 1: (Conditional – Applies to each interface, if any, that could be used to receive external certificate requests): The evaluator shall configure the certificate issuance approval function in accordance with the operational guidance. The evaluator shall create a certificate request and submit it to the TOE. The evaluator shall access the TOE using the defined interface and verify that the submitted request is rejected.

Test 2: The intent of this test is to exercise a representative set of SSL/TLS inspection proxy rules for the supported features of the TLS session establishment policy and demonstrate certificates are generated by the TSF only when the inspection operation is authorized.

The evaluator shall follow AGD guidance to configure a set of rules for the TLS session establishment policy that exercises the inspection operation, bypass operation, and block operation for a representative sample of supported monitored client requested server abstractions as indicated in FDP_TEP_EXT.1.4.

The evaluator shall further configure rules that specify allowances restricting a subset of the monitored client, requested server abstractions associated with the inspection operation to specific TLS versions, cipher suites, supported groups, and other constraints as indicated in the selection of FDP_TEP_EXT.1.5.

The evaluator shall establish TLS servers with certificates issued by an external certification authority, such that for each rule specified, at least one server has attributes satisfying the rule. The evaluator shall establish monitored clients so that for each rule, at least one monitored client has attributes satisfying the rule. If client authentication is supported, the evaluator shall issue certificates to monitored clients from a certification authority trusted by the TSF as required to exercise the rules.

For each rule restricting the TLS allowances, the evaluator shall establish monitored clients, requested servers, and certificates as necessary that match rules associated with the inspection operation, but violate the allowances for the requested server and monitored client pair.

The evaluator shall initiate TLS requests from monitored clients through the TOE, to requested servers to exercise the rules. The evaluator shall observe the resulting logs to confirm the rule is exercised as intended.

For each instance where the rule is associated with the inspection operation and no TLS allowances are violated, the evaluator shall inspect the TLS server certificate message sent from the TOE to the monitored client and confirm the TOE's embedded CA issues the certificate. The evaluator shall search the certificate repository to identify the issued certificate associated with the requested server and that the certificate in the repository matches the certificate sent to the monitored client.

For each instance where the rule is associated with the inspection operation but the TLS allowances are violated, the evaluator shall inspect the TSF logs to confirm the session was blocked. When the server TLS allowances associated with the Client Hello received from the monitored client (version, cipher suites), with the Server Hello received from the requested server (version, cipher suite, supported groups and critical extensions), or with the requested server certificate validation (including certificate revocation information not available when inspection is not allowed), are violated, the evaluator shall search the certificate repository to ensure no certificate matching the subject field in the requested server's certificate is associated to the current session, and search the certificate repository to ensure no certificate matching any of the names in the subject alternate name extension in the requested server's certificate is associated with the current session.

Note: Certain allowances (associated with key exchange messages or client certificate messages received after the server certificate message is sent) may only be determined to be violated after the TSF issues a certificate for the requested server.

For each instance where the rule is associated with the bypass operation, the evaluator shall inspect the TLS server certificate message sent from the TOE to the monitored client, and the TLS server certificate message sent from the requested server to the TOE. The evaluator shall: verify that the certificate sent to the monitored client matches the certificate sent from the requested server exactly, confirm that the certificate issuer indicated in the certificate is the CA trusted by the TOE, and not the TOE's embedded CA, and search the certificate repository for the certificate to confirm the certificate is not present as an issued certificate.

For each instance where the rule is associated with the block operation, the evaluator shall search the certificate repository for any certificate matching the subject field of the requested server's certificate and observe that no certificate was issued in response to the request. The evaluator shall also search the certificate repository for any certificate matching any of the names included in the requested server's subject alternate name extension and observe that no certificate was issued in response to the request.

Test 3: (Conditional – Applies when the TOE supports caching of issued certificates): The evaluator shall configure the TSF to retain certificates in the cache, and initiate a TLS session from a monitored client to a requested server as in Test 2 where the monitored client requested server combination matches a rule associated with the inspection operation without allowance violations. The evaluator shall confirm that the certificate issued by the TOE's embedded CA is contained in the certificate repository. The evaluator shall then establish a second monitored client for which the second monitored client and same requested server also match a rule associated with the inspection operation without allowance violations. The evaluator shall initiate a TLS session from the second client to the same requested server, observe logs to verify that the inspection operation was performed, and search the certificate repository to confirm that a new certificate for the request was not issued.

2.2.3.2 Certificate Status Information Required (FDP_CSIR_EXT)

FDP_CSIR_EXT.1 Certificate Status Information Required

TSS

The evaluator shall examine the TSS to ensure it describes whether certificate status information is provided.

Guidance

The evaluator shall examine the operational guidance to ensure that it contains instructions for any configuration aspects of the validity period that are necessary for the TSF to operate in compliance with this requirement.

Test

Based on the selections, the evaluator shall perform the following tests. If certificate status information is provided, testing is associated with the certificate status information requirements claimed in Appendix B.1 of the STIP PP-Module:

Test 1 (conditional – If the ST claims that validity periods are less than 24 hours): The evaluator shall follow AGD documentation to configure the TSF in compliance with this SFR. The evaluator shall establish a monitored client and a requested server whose certificate is valid for one year, and configure the TSF to inspect TLS traffic between the monitored client and requested server. The evaluator shall initiate a TLS session between the monitored client and requested server. The evaluator shall observe that a certificate is received at the monitored client, which is issued by the TSF and shall verify that its validity is less than 24 hours.

2.2.3.3 Plaintext Processing Policy (FDP_PPP_EXT)

FDP_PPP_EXT.1 Plaintext Processing Policy

TSS

The evaluator shall examine the TSS to validate that internal routing functions or controls associated with the Plaintext Processing Policy are described.

The evaluator shall examine the TSS to ensure that all events that initiate a transition to the block operation based on internal routing function indicators are described.

Guidance
The evaluator shall inspect the operational guidance documents and ensure that instructions for any configurable features of the Plaintext Processing Policy function are provided.

Test
Test 1: For each routing option described in the routing policy, the evaluator shall attempt to construct a data flow that exercises the routing option and observe the intended routing occurs.

Test 2: For each routing option described in the routing policy, the evaluator shall attempt to construct a data flow that violates the routing option and observe that the violation is detected and the flow blocked.

2.2.3.4 Plaintext Routing Control (FDP_PRC_EXT)

FDP_PRC_EXT.1 Plaintext Routing Control

TSS
The evaluator shall examine the TSS to validate that each interface between inspection processing functional components and TLS decryption/encryption buffers that can be used to control the routing of decrypted plaintext associated to a TLS session thread and the internal routing events or rules that control internal routing of decrypted plaintext at each interface are described.

Guidance
The evaluator shall inspect the operational guidance documents and ensure that instructions for any configurable features of the Plaintext Routing function are provided.

Test
Test 1: The evaluator shall configure the TSF and establish monitored clients and requested servers to establish multiple TLS session threads through the inspection processing functional components, in which the plaintext in each thread is distinguishable, either by the expected response of an inspection processing functional component, or by logs. The evaluator shall examine the observable responses and logs to confirm that the threads are treated separately.

Test 2 (conditional – If any plaintext processing rules can be established to exclude plaintext processing by a particular inspection processing functional component): The evaluator shall configure the TSF, configure a plaintext processing policy, and establish monitored clients and requested servers to establish a TLS session thread through the inspection processing functional components for which the configured plaintext processing rules prohibits the processing of the data by a particular inspection processing component. The evaluator shall examine the logs and/or inspection processing response to determine that data is not processed by the component.

2.2.3.5 Subset Residual Information Protection (FDP_RIP)

FDP_RIP.1 Subset Residual Information Protection

TSS
The evaluator shall examine the TSS to ensure that, at a minimum, it describes how the previous information content is made unavailable, and at what point in the buffer processing this occurs.

Guidance
There are no AGD evaluation activities for this requirement beyond what is necessary to satisfy the requirements in [CEM].

Test
There are no ATE evaluation activities for this requirement beyond what is necessary to satisfy the requirements in [CEM].

2.2.3.6 User Data Storage (FDP_STG_EXT)

FDP_STG_EXT.1 Certificate Data Storage

TSS
The evaluator shall examine the TSS to ensure it describes the trusted public keys and certificates implemented, including trust stores that contain root CA certificates used to meet the requirements of this PP. This description shall contain information pertaining to how certificates are loaded into the store, and (if the first selection in this SFR is selected) how the store is protected from unauthorized access in accordance with the permissions established in FMT_SMF.1 and FMT_MOF.1.

Guidance
The evaluator shall examine the operational guidance to ensure it contains instructions for how to load certificates and public keys into, and remove certificates and public keys from the protected storage or apply (trust) or remove (untrust) the indicated protection mechanism.

Test
This test is conditional on the first option in the selection of this SFR being chosen. If the second option is chosen, the evaluator does not perform this and instead performs the actions called for in FCS_CKM_EXT.5.

The evaluator shall perform the following test:

Test 1 (conditional): The evaluator shall attempt to modify the contents of the Trust Anchor Database in a way that violates the documented permissions and verify that the attempt fails.

2.2.3.7 SSL/TLS Inspection Proxy Functions (FDP_STIP_EXT)

FDP_STIP_EXT.1 SSL/TLS Inspection Proxy Functions

FDP_STIP_EXT.1.1

TSS
The evaluator shall examine the TSS to ensure that inspection operation is described.

The evaluator shall examine the TSS to ensure that the logical components of a TLS session thread are described, and that a method for tracking the data flows associated to a TLS session is described. The evaluator shall check the TSS and verify that all components of a TLS session thread are included in the TLS session thread description. The evaluator shall examine the TSS to ensure that separation mechanisms between TLS session threads is described. If TLS resumption is supported, as indicated by the final selection in FCS_TTTC_EXT.1, and/or the final selection in FCS_TTTS_EXT.1, the evaluator shall examine the TSS and verify that the description explains how TLS resumption does not create TLS sessions that are included in multiple TLS session threads.

Guidance

The evaluator shall examine the AGD operational guidance to ensure instructions for any configurable features of the inspection operation, and any configurable features of the TLS session thread management to meet the requirements are provided.

Test

Setup: The evaluator shall follow AGD guidance to configure the TSF. The evaluator shall establish two monitored clients (client a, and b) able to initiate a TLS session that is compliant with FCS_TLSC_EXT.1, and two servers (servers 1 and 2) able to establish TLS sessions in accordance with FCS_TLSS_EXT.1, each of which which has certificate that is valid in accordance with FIA_X509_EXT.1/STIP, and which is issued by a CA, different than the TOE's embedded CA, that is trusted by the TOE. If the TSF supports TLS resumption, the evaluator shall configure server 1 to support TLS resumption using a mechanism (tickets or session number) supported by the TSF, and configure server 2 to refuse TLS resumption and instead respond with a full TLS handshake when requested to do resumption. The evaluator shall follow AGD guidance to configure the TLS session establishment policy so TLS sessions through the TOE between each of the client-server combinations will be inspected. The evaluator shall use appropriate tools to monitor the traffic between the clients and the TOE, and between the TOE and the server to observe the TLS handshake messages. If the TSF supports TLS session resumption, the evaluator shall clear any TLS session state that might be retained by the TSF and configure the TSF to use session resumption. Note that tests 1 and 2 have additional instructions if TLS resumption is supported, but apply regardless of TLS resumption support. Test 3 should only be performed if TLS resumption is supported.

The evaluator shall perform the following tests, in order:

Test 1: The evaluator shall initiate a TLS session from client 'a' to server 1, and initiate a TLS session from client 'b' to server 2. The evaluator shall observe the traffic between the TOE and the servers the data decrypted at the servers to verify that the TLS sessions are distinct. The evaluator shall also observe the traffic between the clients and the TOE and observe that the TLS sessions are distinct. The evaluator shall note and retain the TLS session information for the remaining tests and ensure that the sessions are not terminated during Test 2.

Test 2: The evaluator shall retain the state of the TOE from Test 1. If TLS resumption is supported, the evaluator shall ensure the TLS state in server 1 is retained. The evaluator shall initiate a TLS session from client 'b' to server 1 through the TOE. The evaluator shall observe the traffic between the TOE and server 1, and data received at server 1 to confirm the TLS session thread between client 'b' and server 1 is different than the TLS session between the TOE and server 1 associated to the TLS session thread between client 'a' and server 1 established in Test 1. The evaluator shall observe that the TLS session between client 'b' and the TOE associated to the TLS session thread between client 'b' and server 1 is different than the TLS session between client 'b' and the TOE associated to the TLS session thread between client b and server 2 established in test 1. The evaluator shall terminate the TLS sessions from client 'b' to the TOE and observe that both TLS sessions associated to the TLS session threads, one to server 1 and the other to server 2, are terminated.

Test 3 (conditional: if the TSF supports resumption): The evaluator shall initiate a TLS session resumption between client 'b' and server 2 through the TOE, and observe that the TSF responds with a full TLS handshake.

FDP_STIP_EXT.1.2

TSS
The evaluator shall examine the TSS to ensure it contains a description of the TOEs embedded certification authority function and any certificate caching in support of the inspection operation.

Guidance
The evaluator shall examine the operational guidance to ensure instructions to configure the TOE's embedded CA function and any certificate caching function required to meet the requirements is provided.

Test
The evaluator shall perform the following tests.

Test 1: The evaluator shall configure and establish a monitored client and a requested server, and ensure the requested server has a certificate issued by a CA trusted by the TSF, but different than the TOE's embedded CA. The requested server certificate shall contain a valid identifier of DNS name type identifying the requested server subject alternate name extension. The monitored client will be configured to send the same DNS name for the requested server in the SNI extension of its Client Hello. The evaluator shall follow AGD guidance to configure the TLS session establishment policy to inspect TLS sessions between the monitored client and the requested server. The evaluator shall initiate a TLS session between the monitored client and the requested server through the TOE, and observe that the certificate received in the server certificate message at the monitored client is issued by the TOE's embedded signing certificate and contains the same DNS name for the server in the subject alternate name extension, as requested by the client.

Test 2: [Conditional on support for certificate cache]: The evaluator shall follow AGD guidance to configure the TSF to retain generated certificates in cache for a short time. The evaluator shall establish three monitored clients and a single requested server, and follow AGD guidance to ensure TLS sessions between the monitored clients and the requested server are inspected as in Test 1. The evaluator shall establish a TLS session from two of the monitored clients to the same requested server within the configured cache time, and confirm that the certificates received at each client are identical. The evaluator shall wait until the cache time has expired, and then initiate a TLS connection from the third monitored client and note that the certificate received at the third client is different than the previous certificates receive at the first two clients.

FDP_STIP_EXT.1.3

TSS
The evaluator shall examine the TSS to ensure it describes the mechanism used to determine clients have consented to monitoring in accordance with the requirement. If the second option in the selection is claimed, the evaluator shall confirm that the TSS includes a description of the confirmation exchange between the TSF and monitored clients.

Guidance
The evaluator shall examine the operational guidance to confirm that any instructions to configure the TSF to meet this requirement are provided. If the second option in the selection is claimed, the evaluator shall confirm that instructions for configuring the consent banner is provided.

Test

Test 1 [conditional on support for a consent to monitor banner provided to monitored clients]: The evaluator shall establish a monitored client and requested server, and follow AGD guidance to configure the TSF to present monitored clients a consent to monitor banner. The evaluators shall follow AGD guidance to inspect TLS traffic between the monitored client and requested server, and initiate a TLS session from the monitored client to the requested server through the TOE. The evaluator shall observe that the consent to monitor banner is provided to the client and that no traffic from the client is inspected until consent is provided.

FDP_STIP_EXT.1.4

TSS

The evaluator shall examine the TSS and ensure that the Bypass Operation is described.

Guidance

The evaluator shall examine the operational guidance to verify that instructions for configuring the bypass operation, to include logging of bypassed TLS sessions, is provided.

Test

The evaluator shall perform the following test:

Test 1: The evaluator shall establish a monitored client and a requested server. The evaluator shall follow AGD guidance to configure the TOE and its TLS session establishment policy so that TLS traffic between the monitored client and the requested server is processed via the Bypass Operation and so that bypassed TLS sessions are logged. The evaluator shall initiate a TLS session from the monitored client to the requested server through the TOE. The evaluator shall monitor traffic between the monitored client and the TOE and between the TOE and the requested server. The evaluator shall then observe that the TLS client handshake messages between the client and the TOE are identical to the client handshake messages between the TOE and the server, and that the TLS server handshake messages between the server and the TOE are identical to the TLS server handshake messages between the TOE and the client. The evaluator shall observe the TOE logs to ensure that the TLS session between the client and server is logged.

FDP_STIP_EXT.1.5

TSS

The evaluator shall examine the TSS to ensure that the block operation is described and includes the response to the monitored client when TLS sessions are blocked.

The evaluator shall examine the TSS to ensure that all events that initiate a transition to the block operation are described.

Guidance

The evaluator shall examine operational documentation and verify that instructions to configure any configurable features of the block operation are provided.

Test

Test 1: The evaluator shall establish a monitored client and a requested server. The evaluator shall follow AGD guidance to configure the TOE and its TLS session establishment policy so that TLS sessions between the monitored client and the requested server through the TOE are processed by the block operation. The evaluator shall initiate a TLS session from the monitored client to the requested server through the TOE and observe that the TLS session is blocked. The evaluator shall confirm that the monitored client receives the specified error message.

2.2.3.8 TLS Establishment Policy (FDP_TEP_EXT)

FDP_TEP_EXT.1 SSL/TLS Inspection Proxy Policy

TSS

The evaluator shall examine the TSS and verify that the TLS session establishment policy is adequately described. The evaluator shall verify that the TSS description of the TLS session establishment policy includes a discussion of the TOE's initialization/startup process, which clearly indicates where processing of TLS messages begins and provides a discussion that supports the assertion that TLS messages are dropped during this process.

The evaluator shall verify that the TSS also includes a narrative that identifies the components involved in processing TLS messages and describe the safeguards that would prevent inspection or Bypass Operation functions being performed in the event of a component failure. This could include the failure of a component or a failure within a component. The evaluator shall also verity that the TSS description indicates how the TLS protocol is recognized at each client side and server side interface.

The evaluator shall examine the TSS and verify that it describes any non-configurable rules implementing the TLS session establishment policy and that it describes how such rules invoke the inspect, bypass, or block operations based on the subject attributes included in FDP_TEP_EXT.1.2.

The evaluator shall verify that the TSS describes a TLS session establishment policy and the attributes identified in FDP_TEP_EXT.1.2 are identified as being configurable within the TLS session establishment policy rules. The evaluator shall verify that each configurable rule of the TLS session establishment policy can identify the block, bypass or inspect operation, with the option to log block and bypass operation.

The evaluator shall examine the TSS and verify that rules to define server allowances, client allowances, and other entity allowances (if supported) for TLS parameter usage and TLS processing errors that depend on the TLS session establishment policy is described and includes all conditions indicated in FDP_TEP_EXT.1.5. If both 'block' and 'bypass' are selected in FDP_TEP_EXT.1.7, the evaluator shall confirm that the 'mutual authentication block-bypass' specification is claimed in FDP_TEP_EXT.1.5 and a description of the processing rules for a TLS client certificate request are included in the TSS description of the TLS session establishment policy.

If mutual authentication for through-traffic processing is supported, the evaluator shall examine the TSS and verify that policy rules to define when mutual authentication is allowed are described.

The evaluator shall examine the TSS and verify that description of the TLS protocol and TLS session establishment policy describe the policy-specified behavior that results from TLS protocol errors as required in FDP_TEP_EXT.1.8.

The evaluator shall examine the TSS and verify that the default rules indicated in FDP_TEP_EXT.1.9 and FDP_TEP_EXT.1.10 are described.

Guidance

The evaluator shall examine the AGD guidance documents and verify that instructions to configure the TLS session establishment policy are provided.

The evaluator shall examine the AGD guidance documents and verify that they identify all attributes included in FDP_TEP_EXT.1.2 as being configurable within the TLS session establishment policy, which is that all configurable features of the TLS session establishment policy function are described in the operational guidance.

The evaluator shall examine the AGD guidance documents and verify they indicate each rule can identify the following operations: block, bypass, and inspect. The evaluator shall confirm that instructions for configuring the inspection, bypass, and block operations within rules are included.

The evaluator shall examine the AGD guidance documents and verify they specify each rule indicating block or bypass operations can designate whether logging or counting of TLS Client Hello messages invoking the operation is performed.

The evaluator shall examine the AGD guidance documents and verify they provide instructions on configuring the TLS parameter allowances identified in FDP_TEP_EXT.1.5 and those responses to TLS protocol errors identified in FDP_TEP_EXT.1.8.are indicated.

The evaluator shall examine the AGD guidance documents and verify that any instructions required to configure the TLS session establishment policy to meet the requirements in this component are provided.

Test
Setup: The evaluator shall configure one or more monitored clients to present TLS requests to various TLS servers through the TOE. The TLS servers will obtain certificates issued by an external certification authority trusted by the TSF. The client, server, and the server certificates will meet the conditions described in each test. The evaluator shall configure the TOE according to operational guidance to have non-trivial rules for all TLS session establishment policy states. The evaluator shall conduct the following tests, establishing any additional configuration requirements as indicated in each.

Test 1: For each rule of the TLS establishment policy indicating inspection operation processing, the evaluator shall ensure the monitored client is configured to meet the requirements for FCS_TLSC_EXT.1, the requested server is configured to meet the requirements for FCS_TLSS_EXT.1, and the server certificate is valid according to FIA_X509_EXT.1/STIP. The evaluator shall configure the TSF so the rule applies to the monitored client and requested server. The evaluator shall establish a TLS session from the monitored client to the requested server through the TOE. The evaluator shall then observe the TSF audit record, certificate repository, TLS Server Hello data received at the client, plaintext encrypted at the client, and plaintext decrypted by the requested server. The evaluator shall then confirm that the TSF established a TLS session with the requested server, issued a certificate representing the requested server, established a TLS session with the monitored client, decrypted the data, performed any inspection processing, and presented the data to the requested server via the established TLS session.

Test 2: For each rule of the TLS establishment policy indicating bypass processing, the evaluator shall establish a monitored client, requested server, and server certificate that meets the rule. The evaluator shall send a TLS request from the monitored client to the requested server through the TOE, and then inspect logs, certificate repository, certificate received by the monitored client in the Server Hello message, plaintext encrypted by the monitored client, and plaintext decrypted by the requested server to confirm that bypass processing occurred.

Test 3: The evaluator shall follow AGD guidance to ensure the TSF is configured to log blocked TLS sessions. For each rule of the TLS establishment policy indicating blocking of the TLS session, as indicated in any element of this component, the evaluator shall establish that a monitored client, a requested server, and a server certificate meet the rule. The evaluator shall send a TLS session from the monitored client to the requested server through the TOE and observe that the monitored client receives an error response in accordance with FDP_STIP_EXT.1.5 indicating that the session was blocked. The evaluator shall inspect the TSF logs to verify that each session was recorded as blocked.

Test 4: For each event that initiates a transition from the inspection operation to the block operation, the evaluator shall attempt to establish a monitored client and requested server, and configure the TOE and its TLS session establishment policy to invoke the event. For each such event, the evaluator shall initiate a TLS session from the monitored client to the requested server through the TOE. The evaluator shall monitor traffic between the monitored client and the TOE, and monitor traffic between the TOE and the requested client, observing that TLS handshake messages prior to the event are sent, and that any TLS sessions established prior to the event are terminated on transition of the session to the block operation. The evaluator shall observe that the monitored client receives the specified error message indicating that the TLS session is blocked.

2.2.4 Identification and Authentication (FIA)

2.2.4.1 Certificate Enrollment (FIA_ENR_EXT)

FIA_ENR_EXT.1 Certificate Enrollment

TSS
The evaluator shall examine the TSS to ensure that it describes the certificate enrollment function options.

Guidance
The evaluator shall examine the operational guidance documentation and confirm that it contains instructions for obtaining a certificate for the embedded CA using the options claimed in FIA_ENR_EXT.1.1.

Test
Testing is covered under the tests for the referenced SFR of the claimed options.

2.2.4.2 Authentication Using X.509 Certificates (FIA_X509_EXT)

FIA_X509_EXT.1/STIP Certificate Validation (STIP)

TSS
The evaluator shall ensure the TSS describes where the check of validity of requested server TLS certificates, associated OCSP certificates, and if mutual authentication for through-traffic processing is supported, where the check of validity of monitored client TLS certificates takes place.

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.

It is expected that revocation checking is performed when a certificate is used in an authentication step and on both leaf and intermediate CA certificates when a leaf certificate is presented to the TOE as part of the certificate chain during authentication. Revocation checking of any CA certificate designated a trust anchor is not required. It is not sufficient to perform a revocation check of a CA certificate that is not designated a trust anchor (e.g., for an intermediate CA), only when it is loaded onto the device.

Guidance

There are no guidance activities.

Test

The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication of a requested server certificate, or, if mutual authentication for through-traffic processing is supported, a monitored client certificate, as well as CA certificates included in the certificate path and any for OCSP responses used in validating these certificates. The evaluator shall perform the following tests for FIA_X509_EXT.1.1/STIP. These tests must be repeated for each distinct security function that uses X.509v3 certificates in association with through-traffic processing. For example, if the TOE implements mutual authentication for through-traffic processing, then it shall be tested with each of FCS_TTTC_EXT.1 and FCS_TTTS_EXT.3.

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 the function succeeds. Test 1a shall be designed so 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 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 2: The evaluator shall demonstrate that validating an expired certificate results in the function failing.

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 shall then attempt 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. Revocation checking is only applied to certificates not designated as trust anchors. Therefore, the revoked certificates used for testing shall not be a trust anchor.

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 5: The evaluator shall modify any byte in the first eight bytes of the certificate and demonstrate that the certificate fails to validate. (The certificate will fail to parse correctly.)

Test 6: The evaluator shall modify any byte in the last byte of the certificate and demonstrate that the certificate fails to validate. (The signature on the certificate will not validate.)

Test 7: The evaluator shall modify any byte in the public key of the certificate and demonstrate that the certificate fails to validate. (The hash of the certificate will not validate.)

The evaluator shall perform the following tests for FIA_X509_EXT.1.2/STIP. The tests described must be performed in conjunction with the other certificate services assurance activities, including FCS_TTTC_EXT.1 and FCS_TTTS_EXT.3 if claimed. 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 for through-traffic processing (in FIA_X509_EXT.1.1/STIP).

The goal of the following tests to verify 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).

For each of the following tests the evaluator shall create a chain of at least three certificates: a self-signed root CA certificate, an intermediate CA certificate, and a leaf (node) certificate. 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).

Test 1: The evaluator shall ensure that at least one of the CAs in the chain does not contain the BasicConstraints extension. The evaluator shall confirm that the TOE rejects such a certificate at one (or both) of the following points: (i) as part of the validation of the leaf certificate belonging to this chain or (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 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 shall confirm that the TOE rejects such a certificate at one (or both) of the following points: (i) as part of the validation of the leaf certificate belonging to this chain or (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).

The evaluator shall repeat these tests for each distinct use of certificates for through-traffic processing. For example, use of certificates for establishing a TLS connection to a requested server is distinct from use of certificates for client authentication of a monitored client, if supported, and both of these uses would be tested.

2.2.5 Security Management (FMT)

2.2.5.1 Management of Security Functions Behavior (FMT_MOF)

FMT_MOF.1 Management of Security Functions Behavior

TSS

The evaluator shall examine the TSS to ensure it identifies the restrictions consistent with this requirement. For every function specified across all iterations, the TSS must specify how the restriction is achieved and by whom.

Guidance

If the role restriction mechanism is configurable, the evaluator shall examine the operational guidance to determine that the necessary instructions to meet the requirement for the TOE in its evaluated configuration are provided. This applies only to management functions implemented by or accessible through the TSF.

Test
Testing only applies to functions implemented by or accessible through the TSF. The evaluator shall, for each management function, assume the role defined for that function and demonstrate that the assigned role can perform the functions. The evaluator shall, for each management function, assume each role not assigned to that function, attempt to use the function, and verify that the TSF does not permit it.

2.2.6 Protection of the TSF (FPT)

2.2.6.1 Fail Secure (FPT_FLS)

FPT_FLS.1 Failure with Preservation of Secure State

TSS
The evaluator shall examine the TSS to determine that the TOE's implementation of the fail secure functionality is documented, including all secure states for the TOE. The evaluator shall first examine the TSS section to ensure that all failure modes specified in the ST are described. The evaluator shall then ensure that the TOE will attain a secure state after inserting each specified failure mode type. The evaluator shall review the TSS to determine that the definition of secure state is defined and is suitable to ensure protection of key material and user data.

Guidance
The evaluator shall examine the operational guidance to ensure it describes the actions that might occur and provides remedial instructions for the administrator.

Test
The evaluator shall perform the following test:

Test 1: The evaluator shall attempt to cause each documented failure to occur and shall verify that the actions taken by the TSF are those specified in FPT_FLS.1.1. For those failures that the evaluator cannot cause, the evaluator shall provide a justification to explain why the failure could not be induced.

2.2.6.2 Key Storage (FPT_KST_EXT)

FPT_KST_EXT.1 No Plaintext Key Export

TSS
The evaluator shall examine the TSS to ensure it lists all keys and specifies what interfaces exist to export key data, if any.

Guidance
There are no AGD evaluation activities for this requirement beyond what is necessary to satisfy the requirements in [CEM].

Test
The evaluator shall perform the following test:

Test 1: The evaluator shall access each export interface of the TOE, if any, and shall verify that the interface prevents the export of all keys listed in the TSS.

FPT_KST_EXT.2 TSF Key Protection

TSS
The evaluator shall examine the TSS to ensure it describes how unauthorized use of TSF private and secret keys is prevented for both users and processes.

Guidance
The evaluator shall examine the AGD guidance to ensure it contains instructions for configuring the TOE or Operational Environment to prevent unauthorized access to TSF secret and private keys by users or processes.

Test
The evaluator shall perform the following test:

Test 1: The evaluator shall assume each of the non-Administrator roles supported by the TOE and shall attempt to use the available TOE interface to access the keys. The evaluator shall verify that these attempts fail.

2.2.6.3 Trusted Recovery (FPT_RCV)

FPT_RCV.1 Manual Trusted Recovery

TSS
The evaluator shall examine the TSS to determine that, for each failure or service discontinuity identified in the SFR, it describes how the TOE enters a maintenance mode after a failure and the possible actions that can take place while in that mode.

Guidance
The evaluator shall examine the AGD guidance to ensure it contains instructions for restoring the TOE to a secure state when it enters the maintenance mode, including the steps necessary to perform while in this state.

Test
The evaluator shall perform the following test:

Test 1: The evaluator shall attempt to cause each documented failure to occur and shall verify that the result of this failure is that the TSF enters a maintenance mode. The evaluator shall also verify that the maintenance mode can be exited and the TSF can be restored to a secure state. This testing may be performed in conjunction with FPT_FLS.1.

3 Evaluation Activities for Optional Requirements

3.1 Security Audit (FAU)

3.1.1 Security Audit Review (FAU_SAR)

FAU_SAR.1 Audit Review

This activity should be accomplished in conjunction with the testing of FAU_GEN.1. Review of each of the generated audit records demonstrates that these records are reviewable.

FAU_SAR.3 Selectable Audit Review

This activity should be accomplished in conjunction with the testing of FAU_GEN.1.

3.2 User Data Protection (FDP)

3.2.1 Certificate Pinning (FDP_PIN_EXT)

FDP_PIN_EXT.1 Certificate Pinning

TSS

The evaluator shall review the TSS to ensure the Pinning function is described.

Guidance

The evaluator shall review the AGD guidance to ensure it contains instructions for any configurable aspects of the Pinning function.

Test

Test 1: The evaluator shall establish a monitored client and requested server with multiple certificates issued by one or more external certification authorities. The evaluator shall configure the TSF, to either pin one of the certificates, or to pin on the first certificates seen, and to alert on differences between the issued certificates for the requested server. If caching is supported, the evaluator shall either disable caching, or clear cache between TLS requests from the client. The evaluator shall then use the client to request a TLS session with the server using the first of the certificates, and observe that the Pinning response is not observed. The evaluator shall then configure the server to use the second certificate, make a second request from the monitored client, and observe that the pinning alert response is observed.

4 Evaluation Activities for Selection-Based Requirements

4.1 Certificate Status Information

FDP_CRL_EXT.1 Certificate Revocation List Generation

TSS

The evaluator shall examine the TSS to ensure it indicates whether the TOE supports CRL generation and, if so, describes the CRL generation function. In addition, the evaluator shall ensure that the TSS identifies which of the values identified in FDP_CRL_EXT.1.1 can be included in CRLs.

Guidance

If the TOE supports configuration of the CRL issuing function, the evaluator shall examine the operational guidance to ensure that instructions are available to configure issuance of CRL in accordance with FDP_CRL_EXT.1.1.

Test

The evaluator shall perform the following tests.

Test 1: The evaluator shall configure the CRL function using available user guidance and request a CRL in order to ensure that the resulting CRL satisfies all field constraints in FDP_CRL_EXT.1.1.

Test 2: For each field defined in FDP_CRL_EXT.1.1, the evaluator shall attempt to create a CRL that violates the required conditions of the field. The evaluator shall determine that all such attempts are rejected by the TSF.

Test 3: The evaluator shall make a selection of fields from a configured CRL function and shall attempt to create a CRL that violates the required conditions of the field. The evaluator shall determine that all such attempts are rejected by the TSF.

FDP_CSI_EXT.1 Certificate Status Information

TSS

The evaluator shall examine the TSS to ensure it describes the certificate status function and applicable formats, in accordance with this requirement, that can be used to issue certificate status. The TSS must reflect the selection made by the ST author as well as the selection-based requirements from Appendix B.1 of the STIP PP-Module. The evaluator shall also ensure that the TSS describes the process for approving changes to the status of a certificate, including the interfaces that must be used.

If OCSP stapling is selected in FDP_CSI_EXT.1.3, but only CRLs are generated (OCSP responses are not generated by the TSF) as indicated in FDP_CSI_EXT.1.1, the evaluator shall examine the operational guidance to ensure it describes the interfaces to the operational environment required to generate the responses.

Guidance

The evaluator shall examine the operational guidance to ensure that it contains instructions for any configuration aspects of the certificate status change function and the steps needed to perform an approval, as well as any configuration required for interfaces to external certificate status providers.

Test

Based on the selections, the evaluator shall perform the following tests. It is recommended that these be performed in conjunction with applicable tests associated with the requirements claimed in Appendix B.1 of the STIP PP-Module:

Test 1: For each certificate status format identified in FCS_CSI_EXT.1.1, the evaluator shall issue a valid certificate from the TOE. The evaluator shall then cause the TOE to issue certificate status information. The evaluator shall check the certificate status information using all indicated methods identified in FCS_CSI_EXT.1.3 to verify that each reflects that the certificate is valid.

Test 2: For each selected certificate status format (CRLv2 or OCSP) identified in FCS_CSI_EXT.1.1, and for each mechanism indicated in FDP_CSI_EXT.1.2, the evaluator shall cause a valid certificate from the TOE to be revoked. The evaluator shall then cause the TOE to issue certificate status information. The evaluator shall check the certificate status information using all methods (cRLDistributionPoints, authorityInfoAccess, or OCSP Stapling) identified in FCS_CSI_EXT.1.3 to verify that each method reflects that the certificate is revoked.

FDP_OCSP_EXT.1 OCSP Basic Response Generation

TSS

The evaluator shall examine the TSS to ensure it indicates whether the TOE supports OCSP and, if so, describes the OCSP response function. In addition, the evaluator shall ensure that the TSS identifies which of the values identified in FDP_OCSP_EXT.1.1 can be included in OCSP responses.

Guidance

If the TOE supports configuration of the OCSP function, the evaluator shall examine the operational guidance to ensure that instructions are available to configure the OCSP response function in accordance with FDP_OCSP_EXT.1.1.

Test

The evaluator shall perform the following tests.

Test 1: The evaluator shall configure the OCSP response function, establish a monitored client and shall, in turn, cause an OCSP response by the TSF for the status of a certificate issued by the TOE's embedded CA which has not been revoked, a certificate issued by the TOE's embedded CA which has been revoked, and a certificate not issued by the TOE's embedded CA. The evaluator shall ensure that the response satisfies all constraints in FDP_OCSP_EXT.1.1 and provides an accurate status indication in accordance with RFC 6960

Test 2: For each of the constraints in FDP_OCSP_EXT.1.1, the evaluator shall attempt to create an OCSP response that violates the constraints. The evaluator shall determine that all such attempts are rejected by the TSF.

FDP_OCSPS_EXT.1 OCSP Stapling

For any selection, evaluation activities are included in the TSS, guidance portions, and Tests 2 and 3 within the Test portion of the evaluation activities in FDP_CSI_EXT.1. Additional activities if the first option of FDP_OCSPS_EXT.1.2 is claimed are covered under the evaluation activities for FDP_OCSP_EXT.1.

4.2 Certificate Enrollment

FIA_ESTC_EXT.1 Enrollment over Secure Transport (EST) Client

TSS

The evaluator shall examine the TSS to ensure it describes the implementation of this protocol, the certificates obtained, and any pre-existing certificates or trust anchor databases used by the protocol.

Guidance

The evaluator shall examine the operational guidance to ensure it contains instructions on configuring the TOE so that EST conforms to the description in the TSS.

The evaluator shall examine the operational guidance to ensure it contains instructions for obtaining or configuring the TA database (implicit or explicit) and initial certificates.

Test

The evaluator shall perform the following tests.

Test 1: The evaluator shall establish an external CA and EST server, and configure the TOE as indicated in the AGD to authorize the EST server for EST services using the external CA. The evaluator shall examine the TOE logs and TA databases using available interfaces to ensure the EST server and external CA's certificates are authorized for EST services.

Test 2: For each authentication method specified in FIA_ESTC_EXT.1.4, the evaluator shall generate one or more certificate enrollment requests using the authentication method to obtain TOE required certificates from the authorized CA via the EST server established in Test 1. In accordance with guidance documentation, the evaluator shall obtain a sufficient number of certificates in aggregate to allow the TOE to issue certificates to requested servers.

Test 3: The evaluator shall establish a server with a valid certificate and a monitored client. The evaluator shall configure the TOE so that a TLS session between the monitored client and established through the TOE results in the inspection operation being implemented. The evaluators shall establish a TLS session between the monitored client and the established server through the TOE and observe that the certificate chain returned to the client contains a server certificate issued by the embedded CA's certificate, and the embedded CA's certificate issued by the external CA.

Test 4: The evaluator shall generate a re-enrollment request and submit it to the authorized EST server in accordance with FIA_ESTC_EXT.1 to update the TOE's embedded CA's signing certificate. The evaluator shall clear any cache, revoke the original CA certificate, and repeat Test 3, observing that the updated certificate for the embedded CA is included in the certificate chain returned to the monitored client.

Test 5: The evaluator shall establish a second EST server configured to authorize the TOE's EST client but which is not authorized by the client to provide EST services. The evaluator shall generate an enrollment request for the TOE's embedded CA signing certificate, and submit it to the second EST server. The evaluator shall clear any cache and repeat Test 3, observing that the certificate returned by the second EST server is not contained in the certificate chain returned to the monitored client.

4.3 Inspection Policy Banner

FTA_TAB.1/TLS TOE Access Banner (Consent to Monitor Banners for TLS Inspection)

TSS

The evaluator shall examine the TSS to ensure it details when advisory notice and consent warning messages are used in association with TLS inspection and the circumstances for requiring user consent.

Guidance

The evaluator shall examine the operational guidance to ensure it contains instructions on configuring the TOE to display consent banners for TLS inspection traffic.

Test

The evaluator shall also perform the following test.

Test 1: The evaluator follows the guidance documentation to configure a notice and consent warning message for TLS inspection traffic, and configure rules for displaying the message to monitored clients when requesting TLS sessions to specific servers. The evaluator shall establish a client and server subject to the configured rules, and establish a TLS session through the TOE to the server. The evaluator shall verify that the notice and consent message is displayed.

4.4 Authentication of Monitored Clients

FCS_TTTC_EXT.3 Thru-Traffic TLS Inspection Client Protocol with Mutual Authentication Representing Monitored Clients

TSS

The evaluator shall ensure that the TSS description of the TLS protocol for TLS session establishment includes the use of client-side certificates for TLS mutual authentication to servers when allowed by the configured TLS session establishment policy, described in FDP_TEP_EXT.1.

Guidance

The evaluator shall check the guidance documentation to ensure it contains instructions on configuring the TOE so that the TSF supports inspection of TLS sessions with client authentication. The evaluator shall verify that the AGD guidance provides instructions on how to configure the TLS session establishment policy to identify requested servers it may support for mutual authentication inspection.

Test

Setup: The evaluator shall establish one or more monitored clients and one or more requested servers that are configured to pass TLS sessions through the TOE and configure the TLS session establishment policy to use the inspection operation for those clients and servers with a supported version and cipher suite. The evaluator shall establish certificates for the servers that are valid in accordance with FIA_X509_EXT.1/STIP and appropriate for the selected cipher suite. For each signature type supported for mutual authentication, the evaluator shall issue a certificate for a monitored client that is valid in accordance with FIA_X509.EXT.1/STIP. The evaluator shall install the appropriate trust anchors within the TSF to validate the client and server certificates. Additional configuration of the requested servers, monitored clients, and TSF are specified in the tests below.

Test 1: The evaluator shall configure the TOE's TLS session establishment policy to allow client authentication to the servers used in this test. For each certificate established for a monitored client, the evaluator shall initiate a TLS session between the monitored client and a requested server configured to require client authentication via a certificate of the indicated type. The evaluator shall then verify that the TLS session between the proxy and the requested server includes a client certificate message containing a certificate issued by the TSF, and that the certificate verifies messages that authenticate the TSF as controlling the private key associated to the certificate.

Test 2: The evaluator shall configure the TOE's TLS session establishment policy to allow client authentication to the servers used in this test. The evaluator shall configure a requested server to send a certificate request message to clients with a CA field that does not contain the embedded CA of the TOE. The evaluator shall initiate a TLS session from a monitored client using one of the issued certificates for client authentication to the so configured server through the TSF and observe that the TSF does not establish a TLS session with the requested server.

Test 3: The evaluator shall configure the TOE's TLS session establishment policy to allow client authentication to the servers used in this test. The evaluator shall configure a requested server not to send a certificate request message to clients. The evaluator shall initiate a TLS session from a monitored client using one of the issued certificates for client authentication to the so configured server through the TSF and observe that the TSF does not send a client certificate message or certificate verify message to within its handshake with requested server.

Test 4: The evaluator shall configure the TOE's TLS session establishment policy to not allow client authentication to the servers used in this test, and if the TSF supports a block-bypass allowance, to block mutual authentication requests to the server. The evaluator shall configure a requested server to send a certificate request message to clients. The evaluator shall initiate a TLS session from a monitored client using one of the issued certificates for client authentication to the so configured server through the TSF and observe that the TSF does not send a client certificate message or certificate verify message to within its handshake with requested server.

Test 5 (conditional on support for block-bypass specifications in the TLS session establishment policy): The evaluator shall configure the TOE's TLS session establishment policy to not allow client authentication to the requested server used in this test, and to bypass mutual authentication requests to that server. The evaluator shall configure the requested server to trust the CA used to issue a certificate issued to the monitored client and to send a certificate request messages to clients. The evaluator shall initiate a TLS session from the monitored client using the certificate issued by the CA and trusted by the requested server for client authentication to the so configured server through the TSF. The evaluator shall then observe that the TSF performs the bypass operations and sends a client certificate message containing the certificate established for the monitored client and a certificate verify message that validates the monitored client to the requested server.

FCS_TTTS_EXT.3 Thru-Traffic TLS Inspection Server Protocol with Mutual Authentication of Monitored Clients

TSS

The evaluator shall ensure the TSS description of the TLS protocol for TLS session establishment includes the use of client authentication for monitored clients in accordance with the TLS session establishment policy described in FDP_TEP_EXT.1.

Guidance

The evaluator shall check the guidance documentation to ensure it contains instructions on configuring the TOE so that the TSF supports TLS with client authentication for monitored clients. The evaluator shall verify that the AGD guidance provides instructions on how to specify the conditions for when the TSF requests client authentication of monitored clients.

Test

Setup: The evaluator shall establish one or more monitored clients and servers that are configured to pass TLS sessions through the TOE, and configure the TLS session establishment policy to require mutual authentication for these clients. The evaluator shall establish certificates for the servers that are valid in accordance with FIA_X509_EXT.1/STIP. Note: Depending on optional features supported by the TOE, it might also be necessary to configure the requested servers to require mutual authentication, and configure the TLS session establishment policy to allow mutual authentication to the requested servers to induce a client certificate request from the TSF.

Test 1: For each certificate signature algorithm supported, the evaluator shall establish a monitored client with a certificate signed by a trusted CA using the certificate algorithm, where the client properly supports client authentication. For each such client, the evaluator shall initiate a TLS session to a requested server through the TSF. In each case, the evaluator shall observe that valid TLS sessions between the monitored client and the TSF is established and that during the TLS handshake the TSF sends a certificate request message to each monitored client.

Test 2: The evaluator shall initiate a TLS session between a monitored client and a requested server through the TSF, where the client does not provide a certificate message. The evaluator shall observe that a TLS session between the client and the TSF is not established, and that any TLS session between the TSF and the requested server associated to that TLS session thread is terminated.

Test 3: The evaluator shall initiate a TLS session between a monitored client and requested server through the TSF, where the monitored client's certificate is issued by a subordinate CA of a trusted root CA and only the root CA is in the TSF trust store. In response to the certificate request, the evaluator shall replace the last byte of the subordinate CA certificate in a valid certificate message from the client to the TSF and send the modified certificate message, along with a valid Certificate Verify message and Finished message to the TSF. The evaluator shall observe TSF logs to verify that the certificate is deemed invalid, that the TSF does not establish a TLS session with the client, and that any TLS session between the TSF and the requested server associated to that TLS session thread is terminated.

Test 4: The evaluator shall configure the TSF trust store so the root certificate authority that issues the certificate for a monitored client is not trusted. The evaluator shall then initiate a TLS session between a monitored client and requested server using client authentication through the TSF and observe that the TSF does not establish a TLS session with the client and that any TLS session between the TSF and the requested server associated to that TLS session thread is terminated.

Test 5: The evaluator shall establish a monitored client whose otherwise valid certificate issued by a trusted CA does not include the client authentication purpose in the extended key usage field. The evaluator shall initiate a TLS session between the monitored client and a requested server through the TSF. The evaluator shall observe that the TLS session between the monitored client and the TSF is not established, and that any TLS session between the TSF and the requested server associated to that TLS session thread is terminated.

Test 6 (conditional on whether the TLS session establishment supports authenticated attributes of a client in exception specifications): The evaluator shall configure a TLS establishment policy in the TSF to perform mutual authentication for a client. The evaluator shall establish a monitored client subject to the exception specification but having a valid certificate issued by a trusted CA, where the subject identifier and subject alternate name do not match the exception specification. The evaluator shall establish a TLS session from the monitored client to a requested server through the TSF and observe that the TLS session between the client and the TSF is not established and any TLS session between the TSF and the requested server associated to that TLS session thread is terminated.

FDP_CER_EXT.4 Certificate Profiles for Client Certificates

TSS

The evaluator shall examine the TSS to ensure it describes the certificate profile function in accordance with FDP_CER_EXT.4.1 The TSS shall describe how certificate profiles are configured and then selected to issue certificates in accordance with FDP_CER_EXT.4.2. The evaluator shall also ensure that the TSS describes how the TSF ensures that a certificate-requesting subject possesses the applicable private key.

Guidance

The evaluator shall examine the operational guidance to ensure that instructions are available to configure certificate profiles used for certificate generation in accordance with this requirement.

Test

Test 1: The evaluator shall configure a certificate profile using the available guidance, and establish a server with a certificate that satisfies FDP_CER_EXT.4.2 items a, b, e, f, h, j, and k, has valid values in all extensions in item g (g.a-g.g), and passes all certificate validation criteria as a TLS server certificate (having extended key usage field of server authentication) in FIA_X509_EXT.1/Rev. The evaluator shall establish a monitored client and request a TLS session to the server through the TOE so that the mutual authentication inspection operation is implemented, and then examine the certificate received at the server from the TOE to ensure it matches the configured certificate profile.

Test 2: The evaluator shall specifically examine the certificate generated in Test 1 and compare it to both the embedded CA’s certificate and the monitored client’s certificate to ensure that it satisfies all field constraints in FDP_CER_EXT.4.2, FDP_CER_EXT.4.3, and FDP_CER_EXT.4.4 as configured in the certificate profile.

Test 3: The evaluator shall conduct the following tests by establishing a monitored client with certificate identical to that used in Test 1, except for the differences described as follows (each in turn). The evaluator shall make any configuration changes to the TOE as indicated, establish a monitored client and submit a TLS request for a requested server requiring mutual authentication through the TOE so that the mutual authentication inspection operation is performed, and observe the certificate received at the requested server has the indicated features:

- **notBefore field test:** The evaluator shall assign a notBefore value in the monitored client certificate that precedes both the current time and the value of the notBefore field in the TOE’s embedded CA’s certificate, and observe the generated certificate has a notBefore value that does not precede the current time.
- **notAfter field test a:** The evaluator shall configure the maximum validity duration so that the notAfter value of the TOE’s embedded CA certificate does not exceed the current time by more than the maximum validity duration. The evaluator shall assign a notAfter value in the monitored client certificate that exceeds the current time by more than the maximum validity period, and observe that the notAfter field of the generated certificate has a notAfter value that does not exceed the notAfter value of the embedded CA’s certificate

- **notAfter field test b:** The evaluator shall configure the maximum validity duration so that the notAfter value in the TOE's embedded CA certificate exceeds the current time by more than maximum validity duration, assign a notAfter value in the monitored client certificate that exceeds the notAfter value in the TOE's embedded CA's certificate, and observe that the notAfter value of the generated certificate does not exceed the current time by more than the maximum~~-~~ validity duration.
- **notAfter field test c:** The evaluator shall assign a notAfter value in the monitored client certificate that precedes both the notAfter value in the TOE's embedded CA's certificate, and the current time plus the maximum validity duration, and observe that the generated certificate has a notAfter value that does not exceed the notAfter value of the monitored client's certificate.
- **keyUsage field test:** The evaluator shall assign a keyUsage value in the established server certificate that indicates additional usage indicators (e.g., KeyCertSign) and observe that generated certificate has only the Digital Signature and/or Key Encipherment indicators.
- **extendedKeyUsage field test a:** The evaluator shall omit the **extendedKeyUsage** field in the established server certificate and observe that the generated certificate contains the **extendedKeyUsage** field with value indicating only TLS client authentication.
- **extendedKeyUsage field test b:** The evaluator shall populate the **extendedKeyUsage** field in the established server's certificate to indicate both TLS client authentication and code signing, and observe that the generated certificate only indicates TLS client authentication.
- **extendedKeyUsage field test c:** The evaluator shall populate the **extendedKeyUsage** field in the established server's certificate to indicate any usage, and observe the generated certificate only indicates TLS client authentication.

FDP_CER_EXT.5 Certificate Issuance Rules for Client Certificates

TSS

The evaluator shall examine the TSS to ensure it describes the certificate issuance rules, and verify that any interfaces available for external certificate requests (CMC, EST, PKCS#10 or any other request format) are identified.

Guidance

The evaluator shall examine the operational guidance to ensure that it contains instructions for any configuration aspects of any certificate issuance approval function and the steps needed to prevent receipt and approval of external requests.

Test

Test 1: Generate certificates that originate external to the TOE and verify that it is rejected.

FDP_CSI_EXT.2 Certificate Status Information for Client Certificates

TSS

The evaluator shall examine the TSS to ensure it describes the certificate status function and applicable formats, in accordance with this requirement, that can be used to issue certificate status. The TSS must reflect the selection made by the ST author as well as the selection-based requirements from Appendix B.1 of the STIP PP- for CRL or OCSP information. The evaluator shall also ensure that the TSS describes the process for approving changes to the status of a certificate, including the interfaces that must be used.

Guidance

The evaluator shall examine the operational guidance to ensure that it contains instructions for any configuration aspects of the certificate status change function and the steps needed to perform an approval, as well as any configuration required for interfaces to external certificate status providers.

Test

Based on the selections, the evaluator shall perform the following tests. It is recommended that these be performed in conjunction with applicable tests associated with the requirements claimed in Appendix B.1:

Test 1: For each certificate status format identified in FCS_CSI_EXT.2.1, the evaluator shall cause a valid client certificate to be issued by the TOE. The evaluator shall then cause the TOE to issue certificate status information. The evaluator shall check the certificate status information using all indicated methods identified in FCS_CSI_EXT.2.3 to verify that each reflects that the certificate is valid.

Test 2: For each selected certificate status format (CRLv2 or OCSP) identified in FCS_CSI_EXT.2.1, and for each mechanism indicated in FDP_CSI_EXT.2.2, the evaluator shall cause a valid client certificate from the TOE to be revoked. The evaluator shall then cause the TOE to issue certificate status information. The evaluator shall check the certificate status information using all methods (cRLDistributionPoints, authorityInfoAccess, or OCSP Stapling) identified in FCS_CSI_EXT.2.3 to verify that each method reflects that the certificate is revoked.

FDP_STIP_EXT.2 Mutual Authentication Inspection Operation

TSS

The evaluator shall examine the TSS to ensure that inspection of mutually authenticated TLS sessions is described and meets the requirements of FDP_STIP_EXT.2.

If the selection in FDP_STIP_EXT.2.2 indicates client certificate caching is supported, the evaluator shall examine the TSS to ensure that the cache is described, as well as the mechanism to determine when certificates are cached and when new certificates are obtained.

The evaluator shall examine the TSS and confirm that the TSF only sends a TSF-generated certificate message and certificate validate message to a requested server matching an exception specification after it verifies that the certificate meets the configured certificate profile associated to a validated client certificate received from the monitored client requesting TLS to the server.

Guidance

The evaluator shall examine operational documentation and verify that instructions to configure the mutual authentication inspection operation is provided.

Test

Setup: The evaluator shall follow AGD guidance to configure the TSF. The evaluator shall establish a monitored client able to initiate a TLS session compliant with FCS_TLSC_EXT.2 and which is issued a certificate compliant with FIA_X509_EXT.1/STIP for client authentication from a trusted CA that is different than the embedded CA of the TOE.

The evaluator shall ensure the validity of the client's certificate is short enough to accommodate Test 3 below. The evaluator shall establish a server able to establish TLS sessions in accordance with FCS_TLSS_EXT.2 and configured to support mutual authentication of the client and which is configured to trust the TOE's embedded CA.

The evaluator shall ensure the server is issued a certificate issued by a trusted CA that is different than the TOE's embedded CA, and which is valid in accordance with FIA_X509_EXT.1/STIP for server authentication.

The evaluator shall follow AGD guidance to configure the TLS session establishment policy so mutually authenticated TLS sessions through the TOE between the client and server is allowed and will be inspected.

The evaluator shall use appropriate tools to monitor the traffic between the clients and the TOE, and between the TOE and the server to observe the TLS handshake messages. The evaluator shall implement the following tests in order.

Test 1: The evaluator shall configure the server to not require mutual authentication of the client, initiate a TLS session to the server through the TSF, and observe a TLS session between the TSF and the server is established and does not include a certificate message or certificate verify message from the TSF. The evaluator shall inspect the server certificate received at the client to confirm that it was issued by the embedded CA of the TOE, confirming that the inspection operation was implemented. The evaluator shall inspect the certificate repository of the TOE and confirm that no certificate representing the client is present.

Test 2: The evaluator shall configure the server to require mutual authentication of the client, initiate a TLS session from the client to the requested server, and observe the traffic between the TOE and the server to verify that the TSF sends a certificate message containing a certificate issued by the embedded CA of the TOE, and a certificate verify message that validates the TSF's possession of the corresponding private key. The evaluator shall examine the certificate repository of the TOE to confirm that the certificate observed in the certificate message is present in the repository.

Test 3: Adjusting the time of the TSF if necessary so that the initial certificate issued to the client is expired, the evaluator shall establish a new certificate for the client, using the same subject but using a validity period that is valid in the current time setting. The evaluator shall initiate a TLS session between the client and the server requiring mutual authentication through the TOE and observe that a TLS session containing a certificate message with a new certificate generated by the embedded CA of the TOE, and a certificate verify message that validates the TSF's possession of the associated private key. The evaluator shall examine the certificate repository of the TOE and verify that both certificates representing the client are present.

Test 4: The evaluator shall initiate a new TLS session between the client and server through the TOE, where the certificate in the certificate message from the client is modified in the last byte, and a valid certificate verify message is sent for the unmodified certificate. The evaluator shall observe that a TLS session between the client and the TSF is not established, and that any TLS session between the TSF and the server associated to that TLS session thread is terminated.

4.5 Other Selection-Based SFRs

FAU_SCR_EXT.1 Certificate Repository Review

TSS

The evaluator shall examine the TSS to ensure it describes the certificate repository if the TSF stores it, or describes the interfaces to the operational environment if the certificate repository is stored external to the TOE. The evaluator shall check the TSS to ensure it describes how to search the certificate repository for the selected items

Guidance
The evaluator shall examine the operational guidance to ensure it contains instructions for searching the specified information.

Test
The following activities apply regardless of the selection made in the first selection in the SFR. The test activities can be conducted in conjunction with those for FDP_CER_EXT.1 and FAU_GCR_EXT.1.

Test 1: The evaluator shall generate a sufficient number and variety of certificates to populate the repository with certificates having at least two values for each of the search fields selected in this SFR. The evaluator shall then—following the instructions in the operational guidance—search the repository or audit record for certificates containing specific values for each search field included in the ST, and confirm all certificates matching the search criteria are returned, that all returned certificates match the criteria, and that the object identifier for each matched item is returned. The evaluator shall confirm that the object identifier returned matches the audit events associated with generation of the certificates in accordance with FAU_GEN.1.

FCS_CKM_EXT.5 Public Key Integrity

TSS
The evaluator shall examine the TSS to ensure it describes each applicable public key, where it is stored and protected, the purpose of the public key, the mechanism used to protect the public key from undetected modification, and the method (for each public key) by which the integrity of the key is checked in accordance with FCS_CKM_EXT.5.2.

Guidance
There are no AGD evaluation activities for this requirement beyond what is necessary to satisfy the requirements in [CEM].

Test
NOTE: It might not be possible to access public keys via the TOE interface. If that is the case, then the evaluator must describe the interface and indicate why the interface does not allow access to the public keys.

For each public key identified in the TSS, the evaluator shall perform the following test:

Test 1: The evaluator shall perform an action to invalidate the integrity of each public key and then verify that the TSF detects the invalid key.

FCS_TTTC_EXT.4 STIP Client-Side Support for Renegotiation

TSS
The evaluator shall examine the TSS to validate that it describes the method used to support renegotiation.

Guidance
There are not guidance activities for this component.

Test
The evaluator shall perform the following tests.

Test 1: The evaluator shall use a network packet analyzer and/or sniffer to capture the traffic between the TSF and a requested server during inspection of a TLS session between a monitored client and the requested server through the TOE. The evaluator shall verify that either the renegotiation_info field or the SCSV cipher suite is included in the Client Hello message during the initial handshake.

Test 2: The evaluator shall verify the TSF's handling of Server Hello messages received from a requested server during an authorized inspection of a TLS session between a monitored client and the requested server through the TOE, during the initial handshake that include the renegotiation_info extension. The evaluator shall modify the length portion of this field in the Server Hello message to be non-zero and verify that the TSF sends a failure and terminates the connection. The evaluator shall verify that a properly formatted field during an authorized inspection of traffic to the server results in a successful TLS connection between the TSF and the requested server.

Test 3: The evaluator shall cause the TSF to initiate renegotiation with the requested server and verify that the Client Hello message received by the requested server contains the renegotiation_info extension. The evaluator shall cause the requested server to send a Server Hello message with a renegotiation info extension containing data in which one or both of the client_verify_data or server_verify_data value is modified. The evaluator shall verify that the TSF terminates the connection.

FCS_TTTC_EXT.4.3

TSS

The evaluator shall verify that the TSS describes the mechanisms used to specify when renegotiation occurs.

Guidance

The evaluator shall check the AGD guidance documentation to ensure that instructions for any configurable features of the TLS implementation required to meet this requirement are provided.

Test

Test 1: For any mechanism specified, the evaluator will establish one or more monitored client and requested servers configured to use each of the supported cipher suites through the TSF. For each supported cipher suite, the evaluator shall initiate a session between the monitored client to a requested server and observe network traffic between the TOE and the requested server to confirm that the indicated cipher suite is negotiated successfully. The evaluator shall then send application data over the inspected channel between the monitored client until the renegotiation criteria is met. The evaluator shall observe that the TSF terminates or renegotiates the TLS session as specified by the renegotiation mechanism.

Test 2 (conditional): The evaluator shall establish one or more monitored client and requested servers configured to use each of the supported cipher suites using TDES through the TSF. For each supported cipher suite using TDES, the evaluator shall configure the TLS session establishment of the TSF to inspect such traffic, to include setting appropriate exception specifications. The evaluator shall initiate a session between the monitored client to a requested server and observe network traffic between the TOE and the requested server to confirm that the indicated cipher suite using TDES is negotiated successfully. The evaluator shall then send application data over the inspected channel between the monitored client and the requested server so that the number of data blocks encrypted under TDES will exceed 2^20. The evaluator shall observe that the TSF terminates or renegotiates the TLS session before the number of data blocks encrypted to the requested server exceeds 2^20.

FCS_TTTS_EXT.4 STIP Server-Side Support for Renegotiation

TSS

The evaluator shall examine the TSS to validate it describes the method used to support renegotiation.

Guidance

There are not guidance activities for this component.

Test

The evaluator shall establish a monitored client that supports secure renegotiation and the renegotiation_info extension, and a requested server that is authorized for the inspection operation.

Test 1: The evaluator shall use a network packet analyzer or sniffer to capture the traffic between the TSF and a monitored client. The evaluator shall initiate a TLS session between the monitored client and the requested server through the TOE, and verify the renegotiation_info field is included in the Server Hello message sent from the TSF to the monitored client.

Test 2: The evaluator shall initiate a new (initial) TLS session between the monitored client and the requested server through the TOE, where the Client Hello message includes a renegotiation_info extension with non-zero length, and verify the TSF sends a failure and terminates the connection. The evaluator shall verify that a properly formatted field results in a successful TLS connection.

Test 3: The evaluator shall send a renegotiation request from the monitored client to the TSF containing a modified client_verify_data value in the Client Hello message. The evaluator shall verify the TSF terminates the connection.

5 Evaluation Activities for Objective Requirements

5.1 Identification and Authentication (FIA)

5.1.1 Enrollment over Secure Transport Client Protocol (FIA_ESTC_EXT)

FIA_ESTC_EXT.2 Client Use of TLS-Unique Value

TSS

The evaluator shall examine the TSS to ensure the description of EST includes implementation of TLS-unique values.

Guidance

The evaluator shall examine the operational guidance to ensure it contains instructions on configuring the TOE so that EST conforms to the description in the TSS, to include any configuration associated to the inclusion of TLS-unique values in certificate requests.

Test

The evaluator shall perform the following tests.

Test 1: The evaluator shall follow guidance documentation to implement the EST request function to include TLS-unique values in the certificate request. The evaluator shall establish trust with an external EST server and associated CA and submit a simple certificate request. The evaluator shall review the request received by the EST server and observe that the request contains the TLS-unique value and that it matches the TLS-unique value established under the TLS session.

6 Evaluation Activities for SARs

It is important to note that a TOE that is evaluated against the PP-Module is inherently evaluated against the Base-PP. This PP includes a number of EAs associated with both SFRs and SARs. Additionally, the PP-Module includes a number of SFR-based EAs that similarly refine the SARs of the Base-PPs. The evaluation laboratory will evaluate the TOE against the chosen Base-PP and supplement that evaluation with the necessary SFRs that are taken from the PP-Module.

6.1 AVA: Vulnerability Assessment

Refinement of AVA_VAN.1 work units and EAs established by the Base-PP are found in Appendix A.

7 Required Supplementary Information

This Supporting Document has no required supplementary information beyond the ST, operational guidance, and testing.

8 References

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation – • Part 1: Introduction and General Model CCMB-2012-09-001, Version 3.1 Revision 5, April 2017 • Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 5, April 2017 • Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, CCMB-2012-09-004, Version 3.1 Revision 5, April 2017
[NDcPP]	collaborative Protection Profile for Network Devices, Version 2.0, 05 May 2017
[STIP Module]	PP-Module for SSL/TLS Inspection Proxy Version 0.11, 09 July 2018

A Vulnerability Analysis

A.1 Sources of Vulnerability Information

A.1.1 Type 1 Hypotheses – Public Vulnerability-Based

This section is refined to require phrases consisting of “TLS” in conjunction with each of the supported specific cipher suite components (e.g. “TLS TDES,” “TLS CBC,” “TLS_SHA1”…) and with each supported version (e.g. “TLS 1.0,” “TLS 1.2,”…) be added as search criteria. Search criteria shall also include all names used to represent this technology (e.g., “SSL inspection,” “TLS inspection proxy,” “middle box,” “Deep inspection Firewall,”…).

A.1.2 Type 2 Hypotheses – iTC-Sourced

This section is refined to add any flaws specific to this PP-module will be submitted to the NIAP TC for SSL/TLS inspection proxy.

A.1.3 Type 3 Hypotheses – Evaluation-Team-Generated

There are no modifications for this section.

A.1.4 Type 4 Hypothesis – Tool-generated

There are no modifications for this section.

A.2 Process for Evaluator Vulnerability Analysis

There are no modifications for this section.

A.3 Reporting

There are no modifications for this section.

A.4 Public Vulnerability Sources

There are no modifications for this section.

A.5 Additional Flaw Hypothesis

This section is refined to include assessment of the following hypotheses, which are associated with TLS requirements where mitigations are not standardized.

The inclusion of deprecated TLS versions and cipher suites using obsolete algorithms in order to inspect traffic from servers that only support these versions and cipher suites requires the TSF implement specific mitigations against known exploits. The following type 2 flaw hypothesis are not specifically addressed by SFRs and will be included in AVA analysis.

A.5.1 RSA flaws

Bleichenbacher type side-channel based padding Oracle flaw (CVE-2018-16868 and equivalent)

- This flaw is typically mitigated by randomizing computations associated with key material.

Bleichenbacher RSA padding Oracle flaw (CVE-2017-17428 and equivalent)

- This flaw is typically mitigated by ensuring consistency of error alerts for various events related to decrypting the master key.

A.5.2 CBC mode flaws

TLS Padding Oracle Vulnerability (CVE-2019-6485 and equivalent)

- This flaw is typically mitigated by randomizing the IV via insertion of empty fragments into application data.

A.5.3 SHA-1 flaws

SHA-1 collision flaws (CVE-2005-4900 and equivalent)

- For this technology, a mitigation may include limiting the validity of issued certificates to limit the number of spoofing attempts.