Supporting Document
Mandatory Technical Document

PP-Module for MACsec Ethernet Encryption
Version: 1.0
2022-12-16
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 as a result of their application are recognized under the CCRA.

Technical Editor:
National Information Assurance Partnership (NIAP)

Document history:

Version	Date	Comment
1.0	2022-12-16	Initial Release

General Purpose:
The purpose of this SD is to define evaluation methods for the functional behavior of MACsec Ethernet Encryption products.

Acknowledgments:
This SD was developed with support from NIAP MACsec Ethernet Encryption 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 PP-Module for MACsec Ethernet Encryption is to describe the security functionality of MACsec Ethernet Encryption products in terms of [CC] and to define functional and assurance requirements for them. The PP-Module is intended for use with the following Base-PP:

- Network Device, version 2.2e

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

- MACsec Ethernet Encryption, Version 1.0

As such it defines Evaluation Activities for the functionality described in the PP-Module as well as any impacts to the Evaluation Activities to the Base-PP(s) it modifies.

Although Evaluation Activities are defined mainly for the evaluators to follow, in general they also help developers to prepare for evaluation by identifying specific requirements for their TOE. The specific requirements in Evaluation Activities 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

Evaluation Activities can be defined for both SFRs and Security Assurance Requirements (SAR), which are themselves defined in separate sections of the SD.

If any Evaluation Activity 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 Evaluation Activity may be modified or deemed not applicable for a particular TOE, but this must be approved by the Certification Body for the evaluation.

In general, if all Evaluation Activities (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 Evaluation Activities have been successfully completed would require a specific justification from the evaluator as to why the Evaluation Activities were not sufficient for that TOE.

Similarly, at the more granular level of assurance components, if the Evaluation Activities for an assurance component and all of its related SFR Evaluation Activities 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 Evaluation Activities have been successfully completed would require a specific justification from the evaluator as to why the Evaluation Activities were not sufficient for that TOE.

1.3 Terms

The following sections list Common Criteria and technology terms used in this document.

1.3.1 Common Criteria Terms

Assurance	Grounds for confidence that a TOE meets the SFRs [CC].
Base Protection Profile (Base-PP)	Protection Profile used as a basis to build a PP-Configuration.

Collaborative Protection Profile (cPP)	A Protection Profile developed by international technical communities and approved by multiple schemes.
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.
Distributed TOE	A TOE composed of multiple components operating as a logical whole.
Operational Environment (OE)	Hardware and software that are outside the TOE boundary that support the TOE functionality and security policy.
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 Base-PP and at least one PP-Module.
Protection Profile Module (PP-Module)	An implementation-independent statement of security needs for a TOE type complementary to one or more Base-PPs.
Security Assurance Requirement (SAR)	A requirement to assure the security of the TOE.
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 Technical Terms

Carrier Ethernet	Metro Ethernet Forum (MEF) Carrier Ethernet standards define technology-agnostic layer-2 services. The standards include services aimed at end users (Subscriber Ethernet Services) and service providers (Operator Ethernet Services). Other related terms include Metro Ethernet Services, Provider Bridging and Provider Backbone Bridging.
Connectivity Association Key (CAK)	A symmetric key that is used as the master key for MACsec connectivity and is shared between connected MACsec endpoints.
Connectivity Association Key Name	A unique identifier for a specific Connectivity Association Key.

(CKN)	
Ethernet Private Line (EPL)	A service transporting customer data form one User Network Interface (UNI) to another UNI.
Ethernet Virtual Private Line (EVPL)	A Virtual Local Area Network (VLAN)-based service transporting customer data. The UNI is capable of service multiplexing.
Extended Packet Numbering (XPN)	A scheme that allows MACsec communications to persist using a single Secure Association Key for a larger number of frames to reduce overhead and latency associated with key agreement.
Extensible Authentication Protocol over LAN (EAPOL)	A port authentication protocol specified in IEEE 802.1X that is used to facilitate network authentication.
MACsec Key Agreement (MKA)	A key agreement protocol used for distribution of MACsec keys to distributed peers.
MACsec Protocol Data Unit (MPDU)	The basic MACsec frame structure that contains protcol and payload data.
Media Access Control (MAC) Security Entity	An entity (e.g., computer) that is implementing MACsec.
Media Access Control Security (MACsec)	A standard for connectionless data confidentiality and integrity protection at the data link layer of a network connection. Formally defined in IEEE 802.1AE.
Metro Ethernet Forum (MEF)	A non-profit international industry consortium.
Packet Number (PN)	A monotonically increasing value that is guranteed to be unique for each MACsec frame transmitted using a given Secure Association Key (SAK)
SecTag	MAC Security Tag - a protocol header comprising a number of octets, beginning with an EtherType, that is prepended to the service data unit supplied by the client of the protocol and is used to provide security guarantees.
Secure Association (SA)	A mechanism that uses a SAK to provide the MACsec service guarantees and security services for a sequence of transmitted frames.
Secure Association Key (SAK)	A key derived from the CAK that is used to encrypt and decrypt traffic for a given SA.
Secure Channel (SC)	A unidirectional channel (one to one or one to many) that uses symmetric key cryptography to provide a (possibly long lived) Secure Channel.
Secure Device Identifier	A device authentication credential that can be used for EAPOL and is formally defined in IEEE 802.1AR.

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 workunits that are performed in Section 3 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 regarding the TSS section, the evaluator’s verdicts will be associated with the CEM workunit 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 PP.

For ensuring the guidance documentation provides sufficient information for the administrators/users as it pertains to SFRs, the evaluator's verdicts will be associated with CEM workunits 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 workunits 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 Collaborative Protection Profile for Network Devices

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

2.1.1 Modified SFRs

The PP-Module does not modify any requirements when the NDcPP is the base.

2.2 TOE SFR Evaluation Activities

2.2.1 Security Audit (FAU)

FAU_GEN.1/MACSEC Audit Data Generation (MACsec)

FAU_GEN.1/MACSEC
The evaluator shall complete the evaluation activity for FAU_GEN.1 as described in the NDcPP for the auditable events defined in the PP-Module in addition to the applicable auditable events that are defined in the NDcPP. The evaluator shall also ensure that the administrative actions defined for this PP-Module are appropriately audited.

2.2.2 Cryptographic Support (FCS)

FCS_COP.1/CMAC Cryptographic Operation (AES-CMAC Keyed Hash Algorithm)

FCS_COP.1/CMAC
TSS

The evaluator shall examine the TSS to ensure that it specifies the following values used by the AES-CMAC function: key length, hash function used, block size, and output MAC length.

Guidance

There are no guidance evaluation activities (EAs) for this component.

Tests
The evaluator shall perform the following tests:

- Test 1: **CMAC Generation Test**
  To test the generation capability of AES-CMAC, the evaluator shall provide to the TSF, for each key length-message length-CMAC length tuple (in bytes), a set of eight arbitrary key-plaintext tuples that will result in the generation of a known MAC value when encrypted. The evaluator shall then verify that the correct MAC was generated in each case.
- Test 2: **CMAC Verification Test**

  To test the verification capability of AES-CMAC, the evaluator shall provide to the TSF, for each key length-message length-CMAC length tuple (in bytes), a set of 20 arbitrary key-MAC tuples that will result in the generation of known messages when verified. The evaluator shall then verify that the correct message was generated in each case.

  The following information should be used by the evaluator to determine the key length-message length-CMAC length tuples that should be tested:

  - Key length: Values will include the following:
    - 16
    - 32
  - Message length: Values will include the following:
    - 0 (optional)
    - Largest value supported by the implementation (no greater than 65536)
    - Two values divisible by 16

        - Two values not divisible by 16
    - CMAC length:
        - Smallest value supported by the implementation (no less than 1)
        - 16
        - Any supported CMAC length between the minimum and maximum values

FCS_COP.1/MACSEC Cryptographic Operation (MACsec AES Data Encryption and Decryption)

FCS_COP.1/MACSEC
TSS

The evaluator shall verify that the TSS describes the supported AES modes that are required for this PP-Module in addition to the ones already required by the NDcPP in FCS_COP.1/DataEncryption.

Guidance

There are no guidance EAs for this component.

Tests
The evaluator shall perform testing for AES-GCM as required by the NDcPP in FCS_COP.1/DataEncryption.

In addition to the tests specified in the NDcPP for other iterations of FCS_COP.1, the evaluator shall perform the following tests:

- Test 3: **KW-AE Test**: To test the authenticated encryption capability of AES key wrap (KW), the evaluator shall provide five sets of 100 messages and keys to the TOE for each key length supported by the TSF. Each set of messages and keys shall correspond to one of five plaintext message lengths (detailed below). The evaluator shall have the TSF encrypt the messages with the associated key. The evaluator shall verify that the correct ciphertext was generated in each case.
- Test 4: **KW-AD Test**: To test the authenticated decryption capability of AES KW, the evaluator shall provide five sets of 100 messages and keys to the TOE for each key length supported by the TSF. Each set of ciphertexts and keys shall correspond to one of five plaintext message lengths (detailed below). For each set of 100 ciphertext values, 20 shall not be authentic (i.e., fail authentication). The evaluator shall have the TSF decrypt the ciphertext messages with the associated key. The evaluator shall then verify the correct plaintext was generated or the failure to authenticate was correctly detected.

  The messages in each set for both tests shall be the following lengths:

    - two that are non-zero multiples of 128 bits (two semiblock lengths)
    - two that are odd multiples of the semiblock length (64 bits)
    - the largest supported plaintext length less than or equal to 4096 bits

FCS_MACSEC_EXT.1 MACsec

FCS_MACSEC_EXT.1
TSS

The evaluator shall examine the TSS to verify that it describes the ability of the TSF to implement MACsec in accordance with IEEE 802.1AE-2018. The evaluator shall also determine that the TSS describes the ability of the TSF to derive SCI values from peer MAC address and port data and to reject traffic that does not have a valid SCI. Finally, the evaluator shall check the TSS for an assertion that only EAPOL, MACsec Ethernet frames, and MAC control frames are accepted by the MACsec interface.

Guidance

There are no guidance EAs for this component.

Tests
The evaluator shall perform the following tests:

- Test 5: The evaluator shall successfully establish a MACsec channel between the TOE and a MACsec-capable peer in the operational environment and verify that the TSF logs the communications. The evaluator shall capture the traffic between the TOE and the operational environment to determine the SCI that the TOE uses to identify the peer. The evaluator shall then configure a test system to capture traffic between the peer and the TOE to modify the SCI that is used to identify the peer. The evaluator then verifies that the TOE does not reply to this traffic and logs that the traffic was discarded.
- Test 6: The evaluator shall send Ethernet traffic to the TOE's MAC address that iterates through the full range of supported EtherType values (refer to List of Documented EtherTypes) and observes that traffic for all EtherType values is discarded by the TOE except for the traffic which has an EtherType value of 88-8E, 88-E5, or 8808. Note that there are a large number of EtherType values so the evaluator is encouraged to execute a script that automatically iterates through each value.

FCS_MACSEC_EXT.2 MACsec Integrity and Confidentiality

FCS_MACSEC_EXT.2

TSS

The evaluator shall examine the TSS to verify that it describes the methods that the TOE implements to provide assurance of MACsec integrity. This should include any confidentiality offsets used, the use of an ICV (including the supported length), and ICV generation with the SAK, using the SCI as the most significant bits of the initialization vector (IV) and the 32 least significant bits of the PN as the IV.

Guidance

If any integrity verifications are configurable, such as any confidentiality offsets used or the mechanism used to derive an ICK, the evaluator shall verify that instructions for performing these functions are documented.

Tests
The evaluator shall perform the following tests:

- Test 7: The evaluator shall transmit MACsec traffic to the TOE from a MACsec-capable peer in the operational environment. The evaluator shall verify via packet captures, audit logs, or both that the frame bytes after the MACsec Tag values in the received traffic is not obviously predictable.
- Test 8: The evaluator shall transmit valid MACsec traffic to the TOE from a MACsec-capable peer in the operational environment that is routed through a test system set up as a man-in-the-middle. The evaluator shall use the test system to intercept this traffic to modify one bit in a packet payload before retransmitting to the TOE. The evaluator shall verify that the traffic is discarded due to an integrity failure.

FCS_MACSEC_EXT.3 MACsec Randomness

FCS_MACSEC_EXT.3
TSS

The evaluator shall examine the TSS to verify that it describes the method used to generate SAKs and nonces and that the strength of the CAK and the size of the CAK's key space are provided.

Guidance

There are no guidance EAs for this component.

Tests
Testing of the TOE's MACsec capabilities and verification of the deterministic random bit generator is sufficient to demonstrate that this SFR has been satisfied.

FCS_MACSEC_EXT.4 MACsec Key Usage

FCS_MACSEC_EXT.4
TSS

The evaluator shall check the TSS to ensure that it describes how the SAK is wrapped prior to being distributed using the AES implementation specified in this PP-Module.

Guidance

If the method of peer authentication is configurable, the evaluator shall verify that the guidance provides instructions on how to configure this. The evaluator shall also verify that the method of specifying a lifetime for CAKs is described.

Tests
The evaluator shall perform the following tests:

- Test 9: For each supported method of peer authentication in FCS_MACSEC_EXT.4.1, the evaluator shall follow the operational guidance to configure the supported method (if applicable). The evaluator shall set up a packet sniffer between the TOE and a MACsec-capable peer in the operational environment. The evaluator shall then initiate a connection between the TOE and the peer such that authentication occurs and a secure connection is established. The evaluator shall wait one minute and then disconnect the TOE from the peer and stop the sniffer. The evaluator shall use the packet captures to verify that the SC was established via the selected mechanism and that the non-VLAN EtherType of the first data frame sent between the TOE and the peer is 88-E5.
- Test 10: The evaluator shall capture traffic between the TOE and a MACsec-capable peer in the operational environment. The evaluator shall then cause the TOE to distribute a SAK to that peer, capture the MKPDUs from that operation, and verify the key is wrapped in the captured MKPDUs.

FCS_MKA_EXT.1 MACsec Key Agreement

FCS_MKA_EXT.1.1
FCS_MKA_EXT.1.2
FCS_MKA_EXT.1.3
TSS

The evaluator shall examine the TSS to verify that it describes the methods that the TOE implements to provide assurance of MKA integrity, including the use of an ICV and the ability to use a KDF to derive an ICK.

Guidance

There are no guidance EAs for this element.

Tests

The evaluator shall perform the following tests:

- Test 11: The evaluator shall transmit MKA traffic (MKPDUs) to the TOE from an MKA-capable peer in the operational environment. The evaluator shall verify via packet captures, audit logs, or both that the last 16 octets of the MKPDUs in the received traffic do not appear to be predictable.
- Test 12: The evaluator shall transmit valid MKA traffic to the TOE from an MKA-capable peer in the operational environment that is routed through a test system set up as a man-in-the-middle. The evaluator shall use the test system to intercept this traffic to modify one bit in a packet payload before retransmitting to the TOE. The evaluator shall verify that the traffic is discarded due to an integrity failure.

FCS_MKA_EXT.1.4
TSS

There are no TSS EAs for this element.

Guidance

There are no guidance EAs for this element.

Tests

The tests below require the TOE to be deployed in an environment with two MACsec-capable peers, identified as devices B and C, that the TOE can communicate with. Prior to performing these tests, the evaluator shall follow the steps in the guidance documentation to configure the TOE as the key server and principal actor (peer). The evaluator shall then perform the following tests:

- Test 13: The evaluator shall send a fresh SAK that includes both peers as active participants. The evaluator shall start an MKA session between the TOE and the two active participant peers and send MKPDUs. The evaluator shall verify from packet captures that MKPDUs are sent at least once every half-second.
- Test 14: Disconnect one of the peers. Using a man-in-the-middle device, arbitrarily introduce an artificial delay in sending a fresh SAK following the change in the Live Peer List. Repeat Test 1 delaying a fresh SAK for MKA Lifetime traffic and observe that the timeout of 6.0 seconds is enforced by the TSF.

FCS_MKA_EXT.1.5
FCS_MKA_EXT.1.6
FCS_MKA_EXT.1.7
TSS

The evaluator shall verify that the TSS describes the TOE’s compliance with IEEE 802.1X-2010 and 802.1Xbx-2014 for MKA, including the values for MKA and Hello timeout limits and support for data delay protection. The evaluator shall also verify that the TSS describes the ability of the PAE of the TOE to establish unique CAs with individual peers and group CAs using a group CAK such that a new group SAK is distributed every time the group’s membership changes. The evaluator shall also verify that the TSS describes the invalid MKPDUs that are discarded automatically by the TSF in a manner that is consistent with the SFR, and that valid MKPDUs are decoded in a manner consistent with IEEE 802.1X-2010 section 11.11.4.

Guidance

The evaluator shall verify that the guidance documentation provides instructions on how to configure the TOE to act as the key server in an environment with multiple MACsec-capable devices.

Tests

The tests below require the TOE to be deployed in an environment with two MACsec-capable peers, identified as devices B and C, that the TOE can communicate with. Prior to performing these tests, the evaluator shall follow the steps in the guidance documentation to configure the TOE as the key server and principal actor (peer). The evaluator shall then perform the following tests:

- Test 15: The evaluator shall perform the following steps:
  1. Load one PSK onto the TOE and device B and a second PSK onto the TOE and device C. This defines two pairwise CAs.
  2. Generate a group CAK for the group of three devices using ieee8021XKayCreateNewGroup.
  3. Observe via packet capture that the TOE distributes the group CAK to the two peers, protected by AES key wrap using their respective PSKs.
  4. Verify that B can form an SA with C and connect securely.
  5. Disable the KaY functionality of device C using ieee8021XPaePortKayMkaEnable.

6. Generate a group CAK for the TOE and B using ieee8021XKayCreateNewGroup and observe they can connect.
7. The evaluator shall have B attempt to connect to C and observe this fails.
8. Re-enable the KaY functionality of device C.
9. Invoke ieee8021XKayCreateNewGroup again.
10. Verify that both the TOE can connect to C and that B can connect to C.

- Test 16: The evaluator shall start an MKA session between the TOE and the two environmental MACsec peers and then perform the following steps:
  1. Send an MKPDU to the TOE's individual MAC address from a peer. Verify the frame is dropped and logged.
  2. Send an MKPDU to the TOE that is less than 32 octets long. Verify the frame is dropped and logged.
  3. Send an MKPDU to the TOE whose length in octets is not a multiple of four. Verify the frame is dropped and logged.
  4. Send an MKPDU to the TOE that is one byte short. Verify the frame is dropped and logged.
  5. Send an MKPDU to the TOE with unknown Agility Parameter. Verify the frame is dropped and logged.

2.2.3 Identification and Authentication (FIA)

FIA_PSK_EXT.1 Pre-Shared Key Composition

FIA_PSK_EXT.1
TSS

The evaluator shall examine the TSS to ensure it describes the process by which the bit-based PSKs are generated (if the TOE supports this functionality), and confirm that this process uses the RBG specified in FCS_RBG_EXT.1.

Guidance

The evaluator shall examine the operational guidance to determine that it provides guidance to administrators on the composition of strong PSKs, and (if the selection indicates keys of various lengths can be entered) that it provides information on the range of lengths supported.

The evaluator shall confirm the operational guidance contains instructions for either entering bit-based PSKs for each protocol identified in the requirement, generating a bit-based PSK, or both.

Tests

The evaluator shall also perform the following tests for each protocol (or instantiation of a protocol, if performed by a different implementation on the TOE). Note that one or more of these tests can be performed with a single test case.

- Test 17: (conditional, the TOE supports PSKs of multiple lengths) The evaluator shall use the minimum length, the maximum length, a length inside the allowable range, and invalid lengths beyond the supported range (both higher and lower). The minimum, maximum, and included length tests should be successful, and the invalid lengths must be rejected by the TOE.
- Test 18: (conditional, the TOE does not generate bit-based PSKs) The evaluator shall obtain a bit-based PSK of the appropriate length and enter it according to the instructions in the operational guidance. The evaluator shall then demonstrate that a successful protocol negotiation can be performed with the key.
- Test 19: (conditional, the TOE can generate bit-based PSKs) The evaluator shall generate a bit-based PSK of the appropriate length and use it according to the instructions in the operational guidance. The evaluator shall then demonstrate that a successful protocol negotiation can be performed with the key.

2.2.4 Security Management (FMT)

FMT_SMF.1/MACSEC Specification of Management Functions (MACsec)

FMT_SMF.1/MACSEC
TSS

The evaluator shall verify that the TSS describes the ability of the TOE to provide the management functions defined in this SFR.

Guidance

The evaluator shall examine the operational guidance to determine that it provides instructions on how to perform each of the management functions defined in this SFR.

Tests

The evaluator shall set up an environment where the TOE can connect to two other MACsec devices, identified as devices B and C, with the ability of PSKs to be distributed between them. The evaluator shall configure the devices so that the TOE will be elected key server and principal actor, i.e., has highest key

server priority.

The evaluator shall follow the relevant operational guidance to perform the tests listed below. Note that if the TOE claims multiple management interfaces, the tests should be performed for each interface that supports the functions.

- Test 20: The evaluator shall connect to the PAE of the TOE and install a PSK. The evaluator shall then specify a CKN and that the PSK is to be used as a CAK.
  - Repeat this test for both 128-bit and 256-bit key sizes.
  - Repeat this test for a CKN of valid length (1-32 octets), and observe success.
  - Repeat this test again for CKN of invalid lengths zero and 33, and observe failure.
- Test 21: The evaluator shall test the ability of the TOE to enable and disable MKA participants using the management function specified in the ST. The evaluator shall install PSKs in devices B and C, and take any necessary additional steps to create corresponding MKA participants. The evaluator shall disable the MKA participant on device C, then observe that the TOE can communicate with B but neither the TOE nor B can communicate with device C. The evaluator shall re-enable the MKA participant of device B and observe that the TOE is now able to communicate with devices B and C.
- Test 22: For TOEs using only PSKs, the TOE should be the key server in both tests and only one peer (B) needs to be tested. The tests are:
  - Test 22.1: Switch to unexpired CKN: TOE and Peer B have CKN1(10 minutes) and CKN2. CKN2 can either be configured with a longer overlapping lifetime (20 minutes) or be configured with a lifetime starting period of more than 10 minutes after the CKN1 start. The TOE and Peer B start using CKN1 and after 10 minutes, verify that the TOE expires SAK1. This can be verified by either 1) seeing the TOE immediately distribute a new SAK to the peer if the lifetime of CKN2 overlaps CKN1, or 2) by terminating the connection with CKN1 and distributing a new SAK once the lifetime period of CKN2 begins.
  - Test 22.2: Reject CA with expired CKN: TOE has CKN1 (10 minutes). Peer B has CKN1 (20 minutes). TOE and Peer B start using CKN1 and after 10 minutes, verify that the TOE rejects (or ignores) peer’s request to use (or distribute) a SAK using CKN1.
- Test 23: (conditional, "Cause key server to generate a new group CAK..." is selected) The evaluator shall connect to the PAE of the TOE, set the management function specified in the ST (e.g., set ieee8021XKayCreateNewGroup to true), and observe that the TOE distributes a new group CAK.

2.2.5 Protection of the TSF (FPT)

FPT_CAK_EXT.1 Protection of CAK Data

FPT_CAK_EXT.1
TSS

The evaluator shall examine the TSS to determine that it details how CAKs are stored and that they are unable to be viewed through an interface designed specifically for that purpose. If these values are not stored in plaintext, the TSS shall describe how they are protected or obscured.

Guidance

There are no guidance EAs for this component.

Tests

There are no test EAs for this component.

FPT_FLS.1 Failure with Preservation of Secure State

FPT_FLS.1
TSS

The evaluator shall examine the TSS to determine that it indicates that the TSF will shut down if a self-test failure is detected. For TOEs with redundant failover capability, the evaluator shall examine the TSS to determine that it indicates that the failed components will shut down if a self-test failure is detected.

Guidance

The evaluator shall examine the operational guidance to verify that it describes the behavior of the TOE following a self-test failure and actions that an administrator should take if it occurs.

Tests

The following test may require the vendor to provide access to a test platform that provides the evaluator with the ability to modify the TOE internals in a manner that is not provided to end customers:

- Test 24: The evaluator shall modify the TSF in a way that will cause a self-test failure to occur. The evaluator shall determine that the TSF shuts down and that the behavior of the TOE is consistent with the operational guidance. The evaluator shall repeat this test for each type of self-test that can be deliberately induced to fail. For TOEs with redundant failover capability, the evaluator shall determine

that the failed components shut down and the behavior of the TOE is consistent with the operational guidance. For each component, the evaluator shall repeat each type of self-test that can be deliberately induced to fail.

FPT_RPL.1 Replay Detection

FPT_RPL.1
TSS

The evaluator shall examine the TSS to determine that it describes how replay is detected for MPDUs and how replayed MPDUs are handled by the TSF.

Guidance

There are no guidance EAs for this component.

Tests

The evaluator shall perform the following tests:

Before performing each test, the evaluator shall successfully establish a MACsec channel between the TOE and a MACsec-capable peer in the operational environment sending enough traffic to see it working and verify the PN values increase for each direction.

- Test 25: The evaluator shall set up a MACsec connection with an entity in the operational environment. The evaluator shall then capture traffic sent from this remote entity to the TOE. The evaluator shall retransmit copies of this traffic to the TOE in order to impersonate the remote entity where the PN values in the SecTag of these packets are less than the lowest acceptable PN for the SA. The evaluator shall observe that the TSF does not take action in response to receiving these packets and that the audit log indicates that the replayed traffic was discarded.

  The evaluator shall establish a MACsec connection between the TOE and a test system. The evaluator shall then capture traffic sent from the test system to the TOE. The evaluator shall retransmit copies of this traffic to the TOE in order to impersonate the remote entity where the PN values in the SecTag of these packets are less than the lowest acceptable PN for the SA. The evaluator shall observe that the TSF does not take action in response to receiving these packets and that the audit log indicates that the replayed traffic was discarded.

- Test 26: The evaluator shall capture frames during an MKA session and record the lowest PN observed in a particular time range. The evaluator shall then send a frame with a lower PN, and then verify that this frame is dropped. The evaluator shall verify that the device logged this event.

2.2.6 Trusted Path/Channels (FTP)

FTP_ITC.1/MACSEC Inter-TSF Trusted Channel (MACsec Communications)

FTP_ITC.1/MACSEC
This SFR is addressed through evaluation of FCS_MACSEC_EXT.1 through FCS_MACSEC_EXT.4.

2.3 Evaluation Activities for Optional SFRs

2.3.1 Identification and Authentication (FIA)

FIA_AFL_EXT.1 Authentication Attempt Limiting

FIA_AFL_EXT.1
TSS

The evaluator shall examine the TSS to determine that it describes the ability of the TSF to limit the rate at which authentication attempts can be made at the local console following three successive failed attempts.

Guidance

If the TOE requires configuration to be put into a state where authentication attempt limiting is enforced, the evaluator shall review the operational guidance to verify that it describes the procedures to configure the TOE into this state.

Tests

- Test 27: The evaluator shall follow the operational guidance to configure the TOE into a state that enforces authentication attempt limiting (if applicable). The evaluator shall successfully log in to the TOE at a local console, log back out, and immediately log back in in order to demonstrate that successive authentication attempts can be made in under a minute. The evaluator shall then enter an incorrect password three consecutive times for the same account to trigger authentication attempt limiting. Once

the TOE is in this state, the evaluator shall attempt to log in to the TOE periodically over several attempts of varying time intervals and observe that authentication attempts cannot be made any more frequently than once per minute.

2.3.2 Protection of the TSF (FPT)

FPT_DDP_EXT.1 Data Delay Protection

FPT_DDP_EXT.1
TSS

There are no TSS EAs for this component.

Guidance

There are no guidance EAs for this component.

Tests

The test below requires the TOE to be deployed in an environment with two MACsec-capable peers, identified as devices B and C, that the TOE can communicate with. Prior to performing this test, the evaluator shall follow the steps in the guidance documentation to configure the TOE as the key server and principal actor. The evaluator shall then perform the following test:

- Test 28: The evaluator shall use a peer device to send traffic to the TOE, arbitrarily inducing artificial delays in their transmission using a man-in-the-middle setup. The evaluator shall observe that traffic delayed longer than 2.0 seconds is rejected.

FPT_RPL_EXT.1 Replay Protection for XPN

FPT_RPL_EXT.1
TSS

The evaluator shall examine the TSS to determine that it includes XPN in the description of how replay is detected for MPDUs and how replayed MPDUs are handled by the TSF.

Guidance

If the use of XPN or the XPN ciphersuites used by the TOE are configurable, the evaluator shall examine the guidance documentation to determine that it describes how this is configured.

Tests

The evaluator shall perform the following tests:

- Test 29: The evaluator shall establish a MACsec connection between the TOE and a test system using the GCM-AES-XPN-128 ciphersuite if selected, otherwise use GCM-AES-XPN-256. The evaluator shall write or obtain a script to send a small frame with a known payload (such as five bytes of all zeroes) to the TOE. The evaluator shall activate a packet capture tool on the connection between the TOE and the test system and then use the test system to send this frame to the TOE 4,294,967,267 (2^32 + 1) times. The evaluator shall use the packet capture tool to verify that for the first and last frames sent, the least significant 32 bits are the same. This means the most significant bits should have been incremented during this test. Since the IV is different the two encrypted frames should be different.

  Note that if traffic is sent to the TOE at a rate of 10 GB/s, this will take approximately five minutes as per IEEE 802.1AE-2018.

- Test 30: If both ciphersuites were selected, then the evaluator shall reconfigure the TOE using the second ciphersuite and rerun Test 1 to demonstrate support for both ciphersuites.

2.3.3 Trusted Path/Channels (FTP)

FTP_TRP.1/MACSEC Trusted Path (MACsec Administration)

FTP_TRP.1/MACSEC

If “MACsec” is selected in FTP_TRP.1.1/MACSEC, this SFR is addressed through evaluation of FCS_MACSEC_EXT.1 through FCS_MACSEC_EXT.4.

If “SNMPv3” is selected in FTP_TRP.1.1/MACSEC, this SFR is addressed through evaluation of FCS_SNMP_EXT.1 and FMT_SNMP_EXT.1.

For these EAs, the evaluator shall ensure that the testing is performed on the management interface (e.g., if “MACsec” is selected in FTP_TRP.1.1/MACSEC, the evaluator shall repeat the testing as needed for the management interface and not rely on the testing of an outbound connection to an arbitrary MACsec peer).

2.4 Evaluation Activities for Selection-Based SFRs

2.4.1 Cryptographic Support (FCS)

FCS_DEVID_EXT.1 Secure Device Identifiers

FCS_DEVID_EXT.1.1
FCS_DEVID_EXT.1.2
FCS_DEVID_EXT.1.3
FCS_DEVID_EXT.1.4
FCS_DEVID_EXT.1.5
TSS

The evaluator shall check the TSS to verify that it describes how the TSF implements and validates DevIDs.

Guidance

There are no guidance EAs for this element.

Tests

The evaluator shall perform the following tests:

- Test 31:
  1. The evaluator shall install a DevID in the Supplicant that has one octet changed to invalidate the signature.
  2. The evaluator shall cause the Supplicant to initiate an EAP-TLS session with the Authenticator.
  3. The evaluator shall verify that the connection fails.
- Test 32:
  1. The evaluator shall install a DevID in the Supplicant with a valid signature but from an issuer not recognized by the Authenticator.
  2. The evaluator shall cause the Supplicant to initiate an EAP-TLS session with the Authenticator.
  3. The evaluator shall verify that the connection fails.
- Test 33:
  1. The evaluator shall cause the Supplicant to initiate an EAP-TLS session with the Authenticator.
  2. The evaluator shall intercept, manipulate, and retransmit the packets sent by the Supplicant so that the presented name differs from the name in the DevID.
  3. The evaluator shall verify that the connection fails.

FCS_DEVID_EXT.1.6
TSS

The evaluator shall check the TSS to verify that it describes the ability of the TSF to support mutual authentication using DevIDs.

Guidance

There are no guidance EAs for this element.

Tests

The evaluator shall perform the following test:

- Test 34:
  - Step 1: The evaluator shall cause the Supplicant to initiate an EAP-TLS session with the Authenticator in which mutual authentication is requested.
  - Step 2: The evaluator shall verify that the EAP-TLS packet with a Client Certificate Request message is sent and that the Supplicant responds with its DevID.

FCS_DEVID_EXT.1.7
TSS

The evaluator shall check the TSS to verify that it describes the ability of the TSF to support the signing, enable and disable DevID credential, and enable and disable DevID key operations.

Guidance

There are no guidance EAs for this element.

Tests

The evaluator shall perform the following tests:

- Test 35:
  1. The evaluator shall disable the Supplicant public key by setting MIB object devIDPublicKeyEnabled to false.

2. The evaluator shall cause Supplicant to initiate an EAP-TLS session with the Authenticator.
3. The evaluator shall verify that the Supplicant is unable to authenticate.
4. The evaluator shall re-enable the public key, then verify the Supplicant can authenticate.

- Test 36:
  1. The evaluator shall disable the Supplicant DevID by setting MIB object devIDCredentialEnabled to false.
  2. The evaluator shall cause Supplicant to initiate an EAP-TLS session with the Authenticator.
  3. The evaluator shall verify that the Supplicant is unable to authenticate.
  4. The evaluator shall re-enable the DevID, then verify the Supplicant can authenticate.

FCS_EAPTLS_EXT.1 EAP-TLS Protocol

FCS_EAPTLS_EXT.1
TSS

The evaluator shall check the TSS to verify that it describes the ability of the TSF to support EAP-TLS.

Guidance

There are no guidance EAs for this component.

Tests

The evaluator shall set up an environment where the TOE can connect to a second MACsec device, identified as device B. The evaluator shall configure the devices to use EAP-TLS as the authentication method. The evaluator shall set up an authentication server, which may run on the TOE or be a separate device that connects to the test environment.

The evaluator shall then perform the following modifications to Request EAP packets from device B to the TOE:

1. The evaluator shall increment the length field of a Request EAP packet and verify that the TOE does not respond (i.e., silently discards the packet).
2. The evaluator shall append at least one octet to the end of a Request EAP packet and verify that the TOE responds as if there was no change (i.e., ignores the additional octets).
3. The evaluator shall modify the code field of a Request EAP packet to 5 and verify that the TOE does not respond (i.e., silently discards the packet).

Testing of the security of the (D)TLS protocol is performed as part of FCS_(D)TLSS_EXT.1 and .2 or FCS_(D)TLSC_EXT.1 and .2 in the Base-PP.

FCS_SNMP_EXT.1 SNMP Protocol

FCS_SNMP_EXT.1
TSS

The evaluator shall check the TSS to verify that it describes the ability of the TSF to support SNMP-TLS.

Guidance

There are no guidance EAs for this component.

Tests

The evaluator shall perform the following tests:

- Test 37: The evaluator shall attempt to connect to the TOE using one of the SNMP-TLS ciphersuites supported by the TOE. The evaluator shall confirm that the connection is successful.
- Test 38: The evaluator shall attempt to connect to the TOE using an SNMP-TLS ciphersuite not supported by the TOE. The evaluator shall confirm that the connection is not successful.

Testing of the security of the (D)TLS protocol is performed as part of testing FCS_(D)TLSS_EXT.1 and .2, or FCS_(D)TLSC_EXT.1 and .2 from the Base-PP.

2.4.2 Security Management (FMT)

FMT_SNMP_EXT.1 SNMP Management

FMT_SNMP_EXT.1
TSS

The evaluator shall examine the TSS to determine that it describes the ability of the TSF to support SNMPv3 for remote management for connections to authorized IT entities (per FTP_TRP.1/MACSEC), and that it can apply appropriate password restrictions to this interface.

Guidance

If the TOE requires configuration to be put into a state where SNMPv3 is the only version of SNMP that is accepted, the evaluator shall verify that the operational guidance provides instructions on how to disable unsupported versions of SNMP.

Tests

The evaluator shall configure the TOE in accordance with its operational guidance to accept no versions of SNMP other than SNMPv3 (if applicable). The evaluator shall then perform the following tests:

- Test 39: The evaluator shall attempt to connect to the TOE using SNMPv2 and observe that the connection is not successful.
- Test 40: The evaluator shall attempt to connect to the TOE using SNMPv1 and observe that the connection is not successful.

Testing of the security of the SNMPv3 trusted path is done as part of FCS_SNMP_EXT.1. Testing of the password complexity policy is performed as part of FIA_PMG_EXT.1 in the Base-PP. Testing of the ability to manage the TSF using SNMPv3 is carried out as part of FMT_SMF.1/MACSEC.

2.5 Evaluation Activities for Objective SFRs

The PP-Module does not define any objective requirements.

3 Evaluation Activities for SARs

The PP-Module does not define any SARs beyond those defined within the base NDcPP to which it must claim conformance. It is important to note that a TOE that is evaluated against the PP-Module is inherently evaluated against this Base-PP as well. The NDcPP includes a number of Evaluation Activities associated with both SFRs and SARs. Additionally, the PP-Module includes a number of SFR-based Evaluation Activities that similarly refine the SARs of the Base-PPs. The evaluation laboratory will evaluate the TOE against the Base-PP and supplement that evaluation with the necessary SFRs that are taken from the PP-Module.

4 Required Supplementary Information

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

Appendix A - References

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation - • Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017. • Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017. • Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017.
[NDcPP]	collaborative Protection Profile for Network Devices, Version 2.2e, March 23, 2020
[NDcPP SD]	Supporting Document - Evaluation Activities for Network Device cPP, Version 2.2, December 2019
[MOD_FW]	PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625, June 25, 2020
[MOD_VPNGW]	PP-Module for VPN Gateways, Version 1.2, March 31, 2022