PP-Module for MACsec Ethernet Encryption

Version: 2.0
2026-04-17
National Information Assurance Partnership

Revision History

Version	Date	Comment
1.0	2023-03-02	Initial Release
2.0	2026-04-17	Incorporate NIAP Technical Decisions, Update to CC:2022

Contents

1 Introduction
1.1 Overview
1.2 Terms
1.2.1 Common Criteria Terms
1.2.2 Technical Terms
1.3 Compliant Targets of Evaluation
1.3.1 TOE Boundary
1.4 Use Cases
1.5 Package Usage
2 Conformance Claims
3 Security Problem Definition
3.1 Threats
3.2 Assumptions
3.3 Organizational Security Policies
4 Security Objectives
4.1 Security Objectives for the Operational Environment
5 Security Requirements
5.1 Collaborative Protection Profile for Network Devices Security Functional Requirements Direction
5.1.1 Modified SFRs
5.2 TOE Security Functional Requirements
5.2.1 Auditable Events for Mandatory SFRs
5.2.2 Class FAU: Security Audit
5.2.3 Class FCS: Cryptographic Support
5.2.4 Class FIA: Identification and Authentication
5.2.5 Class FMT: Security Management
5.2.6 Class FPT: Protection of the TSF
5.2.7 Class FTP: Trusted Path/Channels
5.3 TOE Security Functional Requirements Rationale
5.4 TOE Security Assurance Requirements
6 Consistency Rationale
6.1 Collaborative Protection Profile for Network Devices
6.1.1 Consistency of TOE Type
6.1.2 Consistency of Security Problem Definition
6.1.3 Consistency of OE Objectives
6.1.4 Consistency of Requirements
Appendix A - Optional SFRs
A.1 Strictly Optional Requirements
A.1.1 Auditable Events for Strictly Optional SFRs
A.1.2 Class FIA: vIdentification and Authentication
A.1.3 Class FPT: Protection of the TSF
A.1.4 Class FTP: Trusted Path/Channels
A.2 Objective Requirements

A.3 Implementation-dependent Requirements
Appendix B - Selection-based Requirements
B.1 Auditable Events for Selection-based SFRs
B.2 Class FCS: Cryptographic Support
B.3 Class FMT: Security Management
Appendix C - Extended Component Definitions
C.1 Extended Components Table
C.2 Extended Component Definitions
C.2.1 Class FCS: Cryptographic Support
C.2.1.1 FCS_MACSEC_EXT MACsec
C.2.1.2 FCS_MKA_EXT MACsec Key Agreement
C.2.1.3 FCS_DEVID_EXT Secure Device Identifiers
C.2.1.4 FCS_EAPTLS_EXT EAP-TLS Protocol
C.2.1.5 FCS_SNMP_EXT SNMP Protocol
C.2.2 Class FIA: Identification and Authentication
C.2.2.1 FIA_PSK_EXT Pre-Shared Key Composition
C.2.3 Class FIA: vIdentification and Authentication
C.2.3.1 FIA_AFL_EXT Authentication Failure Handling
C.2.4 Class FMT: Security Management
C.2.4.1 FMT_SNMP_EXT SNMP Management
C.2.5 Class FPT: Protection of the TSF
C.2.5.1 FPT_CAK_EXT Protection of CAK Data
C.2.5.2 FPT_DDP_EXT Data Delay Protection
C.2.5.3 FPT_RPL_EXT Replay Protection
Appendix D - Implicitly Satisfied Requirements
Appendix E - Entropy Documentation and Assessment
Appendix F - Allocation of Requirements in Distributed TOEs
Appendix G - Acronyms
Appendix H - Bibliography

1 Introduction

1.1 Overview

The scope of this Protection Profile Module (PP-Module) is to describe the security functionality of Media Access Control Security (MACsec) encryption in terms of the Common Criteria [CC] and to define functional and assurance requirements for such products. This PP-Module is intended for use with the following Base Protection Profiles (Base-PPs):

- Network Device collaborative Protection Profile, Version 4.0

This Base-PP is valid because a device that implements MACsec encryption is a specific type of network device, and there is nothing about the implementation of MACsec that would prevent any of the security capabilities defined by the Base-PP from being satisfied. MACsec is defined by IEE 802.1AE-2018 augmented with Corrigendum 802.1AE-2018/Cor 1-2020 and Amendment 802.1AEdk-2023. All references to "802.1AE-2018" in this PP-Module are intended to refer to the standard with these augmentations applied.

A Target of Evaluation (TOE) that conforms to a PP-Configuration containing this PP-Module may be a ‘Distributed TOE’ as defined in the NDcPP. This PP-Module does not prohibit the TOE from implementing other security functionality in a distributed manner. For example, a TOE may be deployed in such a manner that distributed nodes establish MACsec connectivity with physically separated networks while a centralized management device is used to configure the behavior of individual nodes.

1.2 Terms

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

1.2.1 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.
Direct Rationale	A type of Protection Profile, PP-Module, or Security Target in which the security problem definition (SPD) elements are mapped directly to the SFRs and possibly to the security objectives for the operational environment. There are no security objectives for the TOE.
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.

1.2.2 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 (CKN)	A unique identifier for a specific Connectivity Association Key.
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.

MAC Privacy Protection	Introduced in IEEE-802.1AEdk, this refers to functionality that is designed to hide the source and destination MAC addresses of user data frames to limit the correlation between frame sizes and timing.
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 protocol 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 [802.1AE]
Metro Ethernet Forum (MEF)	A non-profit international industry consortium.
Packet Number (PN)	A monotonically increasing value that is guaranteed 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.

1.3 Compliant Targets of Evaluation

This PP-Module specifically addresses MACsec, which allows authorized systems using Ethernet Transport to maintain confidentiality of transmitted data and to take measures against frames that are transmitted or modified by unauthorized devices.

MACsec protects communication between trusted components of the network infrastructure, thus protecting the network operation. It facilitates maintenance of correct network connectivity and services as well as isolation of denial of service attacks.

The hardware, firmware, and software of the MACsec device define the physical boundary. All of the security functionality is contained and executed within the physical boundary of the device. For example, given a device with an Ethernet card, the whole device is considered to be within the boundary.

Since this PP-Module builds on the NDcPP, conformant TOEs are obligated to implement the functionality required in the NDcPP along with the additional functionality defined in this PP-Module in response to the threat environment discussed later in this document.

1.3.1 TOE Boundary

The physical boundary for a TOE that conforms to this PP-Module is a hardware appliance that also provides generalized network device functionality, such as auditing, I&A, and cryptographic services for network communications. The TOE's logical boundary includes all functionality required by the claimed Base-PP as well as the MACsec functionality and related capabilities that are defined in this PP-Module. Any functionality that is provided by the network device that is not relevant to the security requirements defined by this PP-Module or the Base-PP is considered to be outside the scope of the TOE.

1.4 Use Cases

A pair of MACsec devices connected by a physical medium can protect Ethernet frames switched or routed from one device to the other. The two MACsec devices are provided with a CAK and use the MKA protocol to create a secure tunnel. MKA is used by the two MACsec devices to agree upon MACsec keys. A policy should be installed to protect traffic between the devices, with the exception of the MKA or Ethernet control traffic such as Extensible Authentication Protocol (EAP) over LAN (EAPOL) frames.

This PP-Module defines two potential use cases for the MACsec TOE.

[USE CASE 1] Classic Hop by Hop Deployment

MACsec can be deployed in a hop by hop manner between Ethernet devices. Two devices will protect traffic originating in protected networks traversing an untrusted link between them. The devices will first exchange MKA frames, which serve to determine the peer is an authorized peer, and agree upon a shared key and MACsec ciphersuite used to set up a transmit (Tx) SA and a receive (Rx) SA. Once the SAs are set up, MACsec-protected frames traverse the unprotected link.

[USE CASE 2] Over Carrier Ethernet Services

In some markets network service providers have standardized their offerings according to various versions of the MEF specifications. One recent MEF specification is the "E-Line" (*) service type which is based on the use of point-to-point (P2P) Ethernet Virtual Circuits. A port-based service is known as an EPL and a VLAN-based service is known as an EVPL. EPL provides a P2P Ethernet virtual connection between a pair of dedicated user–network interfaces (UNIs), with a high degree of transparency. EVPL provides a P2P or point-to-multipoint connection between UNIs. A difference between the EVPL and EPL is the degree of transparency - while EPL is highly transparent, filtering only the pause frames, EVPL is required to either peer or drop most of the Layer 2 Control Protocols. The MEF has also defined other service types such as E-LAN and E-Tree.

(*) From MEF 6.3 – Subscriber Ethernet Services Definition – November 2019 – Table 3

1.5 Package Usage

This section contains selections and assignments that are required when the listed Functional Packages are claimed by this PP-Module.
Package Usage guidance defined in the TOE's relevant Base-PP applies to the usage of the packages for this module, unless explicitly stated otherwise in this section.

Functional Package for Transport Layer Security (TLS), Version 2.1

Required Iteration for TLS Claims

If the ST author iterates the TLS package requirements to support the requirements of this PP-Module, the requirements shall be iterated with the suffix "MACSEC".

Required Role Claims for TLS Support in FCS_TLS_EXT.1.1

If EAP-TLS or SNMP support is claimed by the TOE, the ST author shall select the option to support DTLS or TLS as a client, depending on the protocol support claimed by the TOE.

Required selections for TLS or DTLS and Functionality in FCS_TLSC_EXT.1.1 or FCS_DTLSC_EXT.1.1

If EAP-TLS or SNMP support is claimed by the TOE, the ST author shall select the option to support mutual authentication in its DTLS or TLS requirements, depending on the protocol support claimed by the TOE.

Required Version Selection for TLS or DTLS in FCS_TLSC_EXT.1.1 or FCS_DTLSC_EXT.1.1

If EAP-TLS support is claimed by the TOE, the ST author shall select the option to support the use of TLS or DTLS 1.3.

2 Conformance Claims

Conformance Statement

An ST must claim exact conformance to this PP-Module.

The evaluation methods used for evaluating the TOE are a combination of the workunits defined in [CEM] as well as the Evaluation Activities for ensuring that individual SFRs and SARs have a sufficient level of supporting evidence in the Security Target and guidance documentation and have been sufficiently tested by the laboratory as part of completing ATE_IND.1. Any functional packages this PP claims similarly contain their own Evaluation Activities that are used in this same manner.

CC Conformance Claims

This PP-Module is conformant to Part 2 (extended) and Part 3 (conformant) of Common Criteria CC:2022, Revision 1.

PP Claim

This PP-Module does not claim conformance to any Protection Profile.

The following PPs and PP-Modules are allowed to be specified in a PP-Configuration with this PP-Module:

- Network Device collaborative Protection Profile Version 4.0
- PP-Module for Stateful Traffic Filter Firewalls Version 2.0 (MOD_FW)
- PP-Module for Virtual Private Network (VPN) Gateways Version 2.0 (MOD_VPNGW)

Package Claim

- This PP-Module is Functional Package for Transport Layer Security, Version 2.1 conformant.
- This PP-Module does not conform to any assurance packages.

The functional packages to which the PP conforms may include SFRs that are not mandatory to claim for the sake of conformance. An ST that claims one or more of these functional packages may include any non-mandatory SFRs that are appropriate to claim based on the capabilities of the TSF and on any triggers for their inclusion based inherently on the SFR selections made.

3 Security Problem Definition

The security problem is described in terms of the threats that the TOE is expected to address, assumptions about its Operational Environment, and any organizational security policies that the TOE is expected to enforce.

3.1 Threats

The following threats that are defined in this PP-Module extend the threats that are defined by the Base-PP.

T.DATA_INTEGRITY

An attacker may modify data transmitted over the layer 2 link in a way that is not detected by the recipient.

Devices on a network may be exposed to attacks that attempt to corrupt or modify data in transit without authorization. If malicious devices are able to modify and replay data that is transmitted over a layer 2 link, then the data contained within the communications may be susceptible to a loss of integrity.

T.NETWORK_ACCESS

An attacker may send traffic through the TOE that enables them to access devices in the TOE's operational environment without authorization.

A MACsec device may sit on the periphery of a network, which means that it may have an externally-facing interface to a public network. Devices located in the public network may attempt to exercise services located on the internal network that are intended to be accessed only from within the internal network or externally accessible only from specifically authorized devices. If the MACsec device allows unauthorized external devices access to the internal network, these devices on the internal network may be subject to compromise. Similarly, if two MACsec devices are deployed to facilitate end-to-end encryption of traffic that is contained within a single network, an attacker could use an insecure MACsec device as a method to access devices on a specific segment of that network such as an individual LAN.

T.SECURITY_FUNCTIONALITY_FAILURE (from NDcPP)

This threat from the above Base PP also applies to the functionality defined in this PP-Module.

T.UNAUTHORIZED_ADMINISTRATOR_ACCESS (from NDcPP)

This threat from the above Base PP also applies to the functionality defined in this PP-Module.

T.UNDETECTED_ACTIVITY (from NDcPP)

This threat from the above Base PP also applies to the functionality defined in this PP-Module.

T.UNTRUSTED_MACSEC_COMMUNICATION_CHANNELS

An attacker may acquire sensitive TOE or user data that is transmitted to or from the TOE because an untrusted communication channel causes a disclosure of data in transit.

A generic network device may be threatened by the use of insecure communications channels to transmit sensitive data. The attack surface of a MACsec device also includes the MACsec trusted channels. Inability to secure communications channels, or failure to do so correctly, would expose user data that is assumed to be secure to the threat of unauthorized disclosure.

3.2 Assumptions

This PP defines no Assumptions beyond those defined in the claimed Base-PP(s).

All assumptions for the OE of the Base-PP also apply to this PP-Module. A.NO_THRU_TRAFFIC_PROTECTION is still operative, but only for the interfaces in the TOE that are defined by the Base-PP and not the PP-Module.

3.3 Organizational Security Policies

This PP defines no Organizational Security Policies beyond those defined in the claimed Base-PP(s).

4 Security Objectives

4.1 Security Objectives for the Operational Environment

All objectives for the operational environment of the Base-PP also apply to this PP-Module. OE.NO_THRU_TRAFFIC_PROTECTION is still operative, but only for the interfaces in the TOE that are defined by the Base-PP and not the PP-Module.

5 Security Requirements

This chapter describes the security requirements which have to be fulfilled by the product under evaluation. Those requirements comprise functional components from Part 2 and assurance components from Part 3 of [CC]. The following conventions are used for the completion of operations:

- **Refinement** operation (denoted by **bold text** or ~~strikethrough text~~): Is used to add details to a requirement or to remove part of the requirement that is made irrelevant through the completion of another operation, and thus further restricts a requirement.
- **Selection** (denoted by *italicized text*): Is used to select one or more options provided by the [CC] in stating a requirement.
- **Assignment** operation (denoted by *italicized text*): Is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets indicates assignment.
- **Iteration** operation: Is indicated by appending the SFR name with a slash and unique identifier suggesting the purpose of the operation, e.g. "/EXAMPLE1."

5.1 Collaborative Protection Profile for Network Devices Security Functional Requirements Direction

In a PP-Configuration that includes the NDcPP, the TOE is expected to rely on some of the security functions implemented by the Network Device as a whole and evaluated against the NDcPP. The following sections describe any modifications that the ST author must make to the SFRs defined in the NDcPP in addition to what is mandated by Section 5.2 TOE Security Functional Requirements.

5.1.1 Modified SFRs

This PP-Module does not modify any SFRs defined by the NDcPP.

5.2 TOE Security Functional Requirements

The following section describes the SFRs that must be satisfied by any TOE that claims conformance to this PP-Module. These SFRs must be claimed regardless of which PP-Configuration is used to define the TOE.

5.2.1 Auditable Events for Mandatory SFRs

Table 1: Auditable Events for Mandatory Requirements

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1/MACSEC	No events specified	N/A
FCS_COP.1/KDFCMAC	No events specified	N/A
FCS_COP.1/MACSEC	No events specified	N/A
FCS_MACSEC_EXT.1	Session establishment.	Secure Channel Identifier (SCI).
FCS_MACSEC_EXT.2	No events specified	N/A
FCS_MACSEC_EXT.3	Creation and update of SAK.	Creation and update times.
FCS_MACSEC_EXT.4	Creation of CA.	Connectivity Association Key Names (CKNs).

FCS_MKA_EXT.1	No events specified	N/A
FIA_PSK_EXT.1	No events specified	N/A
FMT_SMF.1/MACSEC	No events specified	N/A
FPT_CAK_EXT.1	No events specified	N/A
FPT_FLS.1/MACSEC	No events specified	N/A
FPT_RPL.1	Detected replay attempt	None.
FTP_ITC.1/MACSEC	No events specified	N/A

5.2.2 Class FAU: Security Audit

FAU_GEN.1/MACSEC Audit Data Generation (MACsec)

FAU_GEN.1.1/MACSEC

The TSF shall be able to generate audit data of the following auditable events:

a. Start-up and shutdown of the audit functions;
b. All auditable events for the [*not specified*] level of audit;
c. [*All administrative actions;*
d. *Specifically defined auditable events listed in the Auditable Events table (Table 1)*].

FAU_GEN.1.2/MACSEC

The TSF shall record within the audit data at least the following information:

a. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event;
b. For each auditable event type, based on the auditable event definitions of the functional components included in the PP, PP-Module, functional package or ST, [*information specified in column three of the Auditable Events table (Table 1)*].

Application Note: The Base-PP defines audit requirements for functionality that is within the scope of the SFRs defined by the Base-PP. This includes requirements for secure handling of generated audit data, which includes ability to transmit this data to the operational environment over a secure channel and optionally includes requirements for protection and availability of any audit data that is stored locally. As the audit records for auditable events defined in this PP-Module also comprise "audit data," it is expected that the same requirements in the Base-PP for handling of audit data applies to this audit data as well, and not solely the audit data generated in the Base-PP's iteration of FAU_GEN.1.

Evaluation Activities

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.

5.2.3 Class FCS: Cryptographic Support

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

FCS_COP.1.1/KDFCMAC

The TSF shall perform [*keyed-hash message authentication*] in accordance with a specified cryptographic algorithm [*AES-CMAC*] and cryptographic key sizes [*256 bits and message digest size of 128 bits*] that meet the following: [*NIST SP 800-38B*].

Application Note: AES-CMAC is a keyed hash function that is used as part of the key derivation function (KDF) that is used for key generation.

The Base-PP defines a separate iteration of this SFR, FCS_COP.1/CMAC, to define support for AES-CMAC when the TOE requires its use for NTP. The iteration in this PP-Module's SFR is required to be claimed in any conformant TOE because of the need to support AES-CMAC in the context of MACsec

Evaluation Activities

FCS_COP.1/KDFCMAC

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 FCS_COP.1/KDFCMAC: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 FCS_COP.1/KDFCMAC: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.1.1/MACSEC

The TSF shall perform [*encryption and decryption*] in accordance with a specified cryptographic algorithm [*AES used in AES Key Wrap and GCM modes*] and cryptographic key sizes [*256 bits*] that meet the following: [*AES as specified in ISO/IEC 18033-3, AES Key Wrap as specified in NIST SP 800-38F, GCM as specified in ISO/IEC 19772*].

Application Note: The Base-PP defines its own iterations of FCS_COP.1 that independently include selectable support for these modes. For the sake of clarity, this separate iteration is included specifically for the TOE's support of MACsec communications. Relevant selections of the same AES modes in the Base-PP iterations of FCS_COP.1 may be chosen by the ST author in cases where other parts of the TSF may require the use of those modes (e.g., the TOE's support for AES-GCM in the context of remote administration is selected in the Base-PP's FCS_COP.1/AEAD SFR).

Evaluation Activities

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 FCS_COP.1/MACSEC:1: **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 FCS_COP.1/MACSEC:2: **KW-AD Test**: To test the authenticated decryption capability of AES KW, the evaluator shall provide five sets of 100 ciphertext values 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 semi-block lengths)*
  - *two that are odd multiples of the semi block length (64 bits)*
  - *the largest supported plaintext length less than or equal to 4096 bits*

FCS_MACSEC_EXT.1 MACsec

FCS_MACSEC_EXT.1.1

The TSF shall implement MACsec in accordance with IEEE Standard 802.1AE-2018.

Application Note: The 802.1AE-2018 standard includes the applicable errata Corrigendum 802.1AE-2018/Cor 1-2020 and Amendment 802.1AEdk-2023.

FCS_MACSEC_EXT.1.2

The TSF shall derive a Secure Channel Identifier (SCI) from a peer's MAC address and port to uniquely identify the originator of an MPDU.

FCS_MACSEC_EXT.1.3

The TSF shall reject any MPDUs during a given session that contain an SCI other than the one used to establish that session.

FCS_MACSEC_EXT.1.4

The TSF shall permit only EAPOL (Port Access Entity (PAE) EtherType 88-8E), MACsec frames (EtherType 88-E5), and [**selection**: *MAC control frames (EtherType is 88-08)*, *[**assignment**: list of other permitted EtherTypes]*, *no other frame types*] and shall discard others.

FCS_MACSEC_EXT.1.5

The TSF shall reject MPDUs that fail to meet the following characteristics, as defined by IEEE 802.1ae-2018:

a. It comprises at least 17 octets.
b. Octets 1 and 2 compose the MACsec EtherType.
c. The V bit in the TAG control information (TCI) is clear.
d. If the end station (ES) or the single copy broadcast (SCB) bit in the TCI is set, then the SC bit is clear.
e. Bits 7 and 8 of octet 4 of the SecTAG are clear.
f. If the C and SC bits in the TCI are clear, the MPDU comprises 24 octets plus the number of octets indicated by the SL field if that is non-zero and at least 72 octets otherwise.
g. If the C bit is clear and the SC bit set, then the MPDU comprises 32 octets plus the number of octets indicated by the short length (SL) field if that is non-zero and at least 80 octets otherwise.
h. If the C bit is set and the SC bit clear, then the MPDU comprises 8 octets plus the minimum length of the integrity check value (ICV) as determined by the Cipher Suite in use at the receiving MAC Security Entity (SecY), plus the number of octets indicated by the SL field if that is non-zero and at least 48 additional octets otherwise.
i. If the C and SC bits are both set, the frame comprises at least 16 octets plus the minimum length of the ICV as determined by the Cipher Suite in use at the receiving SecY, plus the number of octets indicated by the SL field if that is non-zero and at least 48 additional octets otherwise.

Application Note: The 802.1AE-2018 standard includes the applicable errata Corrigendum 802.1AE-2018/Cor 1-2020 and Amendment 802.1AEdk-2023.

Depending on the Carrier Ethernet service provider a TOE might need additional EtherTypes (such as MAC control frames, basic VLAN tag handling abilities, or alternate MKA EAPOL frame types) to be suitable for Use Case 2. Use of the "assignment" in the SFR must only include additional EtherTypes that directly support the use of MKA, MACsec, and MAC control frames. Select "no other frame types" if none other than 88-8E or 88-E5 are supported.

Evaluation Activities

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, including its ability to enforce section 9.12 of IEEE 802.1AE-2018 to

reject improperly constructed MPDUs. The evaluator shall also determine that the TSS describes the ability of the TSF to derive SCI values (or SSCI values if XPN is used) from peer MAC address and port data and to reject traffic that does not have a valid SCI or SSCI. Finally, the evaluator shall check the TSS for an assertion that only the claimed EtherTypes are accepted by the MACsec interface. Where the SFR selection has provided additional EtherType support, the TSS must describe the usage of each of those frame types within the context of MKA, MACsec, and MAC control frame support.

Guidance

If the TOE requires enabling or disabling specific EtherTypes to operate within the evaluated configuration, the guidance documentation must provide this information to the administrator.

Tests

The evaluator shall perform the following tests:

- *Test FCS_MACSEC_EXT.1:1: 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 or SSCI 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 or SSCI 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 FCS_MACSEC_EXT.1:2: 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 described in the SFR. 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.*
- *Test FCS_MACSEC_EXT.1:3: For each MPDU validity check specified in , the evaluator shall transmit traffic to the TOE that represents an invalid MPDU based on that particular check, and verify that in all cases the TSF rejects the invalid MPDUs.*

FCS_MACSEC_EXT.2 MACsec Integrity and Confidentiality

FCS_MACSEC_EXT.2.1

The TOE shall implement MACsec with support for integrity protection with a confidentiality offset of [**selection**: *0, 30, 50*].

FCS_MACSEC_EXT.2.2

The TSF shall provide assurance of the integrity of protocol data units (MPDUs) using an Integrity Check Value (ICV) derived with the SAK.

Application Note: The length of the ICV is dependent on the ciphersuite used but will not be less than 8 octets or more than 16 octets at the end of the MPDU. The ICV protects the destination and source MAC address parameters, as well as all the fields of the MPDU.

FCS_MACSEC_EXT.2.3

The TSF shall provide the ability to derive an Integrity Check Value Key (ICK) from a Connectivity Association Key (CAK) using a KDF.

Evaluation Activities

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 (or SSCI, when XPN is used) as the most significant bits of the initialization vector (IV) and an IV appropriate to the supported ciphersuites (least significant 32 bits as the IV in a non-XPN context, and a 32-bit SSCI and 64-bit packet number as the IV when XPN is used).

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 FCS_MACSEC_EXT.2:1: The evaluator shall transmit MACsec traffic to the TOE from a MACsec-capable peer in the operational environment. The evaluator shall observe that this traffic is unique from packet to packet and has no obviously predictable elements (i.e., it appears to be random).*
- *Test FCS_MACSEC_EXT.2:2: 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.3.1

The TSF shall generate unique Secure Association Keys (SAKs) using [**selection**: *key derivation from Connectivity Association Key (CAK) per section 9.8.1 of IEEE 802.1X-2020, the TOE's random bit generator as specified by FCS_RBG.1*] such that the likelihood of a repeating SAK is no more than 1 in 2 to the power of the size of the generated key.

FCS_MACSEC_EXT.3.2

The TSF shall generate unique nonces for the derivation of SAKs using the TOE's random bit generator as specified by FCS_RBG.1.

Application Note: FCS_RBG.1 is defined in the Base-PP so a conformant MACsec TOE will include this dependency.

Evaluation Activities

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.4.1
The TSF shall support peer authentication using pre-shared keys (PSKs) [**selection**: *EAP-TLS with DevIDs, no other method*].

Application Note: The definition of the peer's CAK as defined by IEEE 802.1X-2020 is synonymous with the peer authentication performed here. If "EAP-TLS with DevIDs" is selected, the FCS_DEVID_EXT.1 and FCS_EAPTLS_EXT.1 SFRs must be claimed.

FCS_MACSEC_EXT.4.2
The TSF shall distribute SAKs between MACsec peers using AES key wrap as specified in FCS_COP.1 /**MACSEC**.

Application Note: This requirement applies to the SAKs that are generated by the TOE. They must be wrapped by the AES Key Wrap method specified in NIST SP 800-38F.

FCS_MACSEC_EXT.4.3
The TSF shall support specifying a lifetime for CAKs.

FCS_MACSEC_EXT.4.4
The TSF shall associate Connectivity Association Key Names (CKNs) with SAKs that are defined by the KDF using the CAK as input data (per IEEE 802.1X-2020, Section 9.8.1).

FCS_MACSEC_EXT.4.5
The TSF shall associate CKNs with CAKs. The length of the CKN shall be an integer number of octets, between 1 and 32 (inclusive).

Evaluation Activities

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.
(conditional, the length of the CKN is configurable) The evaluator shall verify that the guidance describes how to set the CKN length to 1-32 octets.

Tests
The evaluator shall perform the following tests:

- *Test FCS_MACSEC_EXT.4:1: 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 FCS_MACSEC_EXT.4:2: 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

The TSF shall implement Key Agreement Protocol (MKA) in accordance with IEEE 802.1X-2020.

FCS_MKA_EXT.1.2

The TSF shall provide assurance of the integrity of MKA protocol data units (MKPDUs) using an Integrity Check Value (ICV) derived from an Integrity Check Value Key (ICK).

Application Note: The ICV has length 128 bits and is computed according to Section 9.4.1 of IEEE 802.1X-2020. The ICV protects the destination and source MAC address parameters, as well as all the fields of the MAC Service Data Unit of the MKPDU including the allocated EtherType, and up to but not including, the generated ICV.

FCS_MKA_EXT.1.3

The TSF shall provide the ability to derive an Integrity Check Value Key (ICK) from a CAK using a KDF.

FCS_MKA_EXT.1.4

The TSF shall enforce an MKA Lifetime Timeout limit of 6.0 seconds and [**selection**: *MKA Hello Time limit of 2 seconds*, *MKA Bounded Hello Time limit of 0.5 seconds*].

Application Note: If optional requirement FPT_DDP_EXT.1 is claimed, then "MKA Bounded Hello Time limit of 0.5 seconds" must be selected.

FCS_MKA_EXT.1.5

The key server shall refresh a SAK when it expires. The key server shall distribute a SAK by [**selection**:

- *a group CAK, distributed by a group CAK*
- *a group CAK, distributed by pairwise CAKs derived from MKA*
- *a group CAK, distributed by pre-shared key (PSK)*
- *pairwise CAKs, derived from MKA*
- *pairwise CAKs that are PSKs*

].

FCS_MKA_EXT.1.6

The key server shall distribute a fresh SAK whenever a member is added to or removed from the live membership of the CA.

FCS_MKA_EXT.1.7

The TSF shall validate MKPDUs according to IEEE 802.1X-2020 Section 11.11.2. In particular, the TSF shall discard without further processing any MKPDUs to which any of the following conditions apply:

a. The destination address of the MKPDU was an individual address
b. The MKPDU is less than 32 octets long
c. The MKPDU comprises fewer octets than indicated by the Basic Parameter Set body length, as encoded in bits 4 through 1 of octet 3 and bits 8 through 1 of octet 4, plus 16 octets of ICV

d. The CAK Name is not recognized

If an MKPDU passes these tests, then the TSF will begin processing it as follows:

a. If the Algorithm Agility parameter identifies an algorithm that has been implemented by the receiver, the ICV shall be verified as specified in IEEE 802.1X-2020 Section 9.4.1.
b. If the Algorithm Agility parameter is unrecognized or not implemented by the receiver, its value can be recorded for diagnosis but the received MKPDU shall be discarded without further processing.

Each received MKPDU that is validated as specified in this clause and verified as specified in IEEE 802.1X-2020 Section 9.4.1 shall be decoded as specified in IEEE 802.1X-2020 Section 11.11.4.

Evaluation Activities

FCS_MKA_EXT.1.1
There are no evaluation activities for this element.

FCS_MKA_EXT.1.2
Evaluation activities for this requirement are covered in the evaluation activities for FCS_MKA_EXT.1.3.

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 FCS_MKA_EXT.1.3:1: 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 are unique and do not appear to be predictable.*
- *Test FCS_MKA_EXT.1.3:2: 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 using a traffic sniffer to capture

this traffic:

- *Test FCS_MKA_EXT.1.4:1: The evaluator shall configure the TOE to establish a MKA session with a new peer. The evaluator shall verify that the TOE sends a fresh SAK to the peer and sends other MKPDUs required for a new session. The evaluator shall verify from packet captures that MKPDUs are sent at least once every two seconds or every 0.5 seconds, in accordance with the SFR selection.*
- *Test FCS_MKA_EXT.1.4:2: (Conditional - If "EAPTLS with DevIDs" is selected in FCS_MACSEC_EXT.4.1) The evaluator shall use EAP-TLS to derive a CAK and configure the TOE's peer to send "0" in the MKA parameter field for MACsec Capability (Table 11-6 in 802.1X-2020). The evaluator shall observe that the peer is deleted from the connection after MKA Life Time has passed.*
- *Test FCS_MKA_EXT.1.4:3: (Conditional - if any "group CAK" selection is made in FCS_MKA_EXT.1.5) The evaluator shall configure the TOE to send a fresh SAK with two peers as active participants. The evaluator shall verify that the TOE sends a fresh SAK to the peers and sends other MKPDUs required for a new session. The evaluator shall verify from packet captures that MKPDUs are sent at least once every two seconds or every 0.5 seconds in accordance with the SFR selection.*
- *Test FCS_MKA_EXT.1.4:4: (Conditional - if any "group CAK" selection is made in FCS_MKA_EXT.1.5) Disconnect one of the peers. Arbitrarily introduce an artificial delay in sending a fresh SAK following the change in the Live Peer List. For this delayed fresh SAK, use a man-in-the-middle device to observe that the MKA Life Time of 6.0 seconds is enforced by the TSF.*

FCS_MKA_EXT.1.5
Evaluation activities for this requirement are covered in the evaluation activities for FCS_MKA_EXT.1.7.

FCS_MKA_EXT.1.6
Evaluation activities for this requirement are covered in the evaluation activities for FCS_MKA_EXT.1.7.

FCS_MKA_EXT.1.7
TSS
The evaluator shall verify that the TSS describes the TOE's compliance with IEEE 802.1X-2020 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-2020 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 FCS_MKA_EXT.1.7:1: (Conditional - if any "group CAK" selection is made in FCS_MKA_EXT.1.5) 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 FCS_MKA_EXT.1.7:2: The evaluator shall start an MKA session between the TOE and an environmental MACsec peer 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.*

5.2.4 Class FIA: Identification and Authentication

FIA_PSK_EXT.1 Pre-Shared Key Composition

FIA_PSK_EXT.1.1

The TSF shall use PSKs for MKA as defined by IEEE 802.1X-2020, [**selection**: *no other protocols, [**assignment**: other protocols that use PSKs]*].

Application Note: If other protocols can use PSKs, they should be listed in the assignment as well; otherwise “no other protocols” should be chosen.

FIA_PSK_EXT.1.2

The TSF shall be able to [**selection**: *accept, generate using the random bit generator specified in FCS_RBG.1*] bit-based PSKs.

Application Note: The ST author specifies whether the TSF merely accepts bit-based PSKs or if it is also capable of generating them. If it generates them, the requirement specifies that they must be generated using the RBG provided by the TOE.

Evaluation Activities

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.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 FIA_PSK_EXT.1:1: (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 FIA_PSK_EXT.1:2: (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 FIA_PSK_EXT.1:3: (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.*

5.2.5 Class FMT: Security Management

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

FMT_SMF.1.1/MACSEC

The TSF shall be capable of performing the following management functions **related to MACsec functionality**: [*Ability of a Security Administrator to:*

- *Manage a PSK-based CAK and install it in the device*
- *Manage the key server to create, delete, and activate MKA participants [**selection**: as specified in IEEE 802.1X-2020, Sections 9.13 and 9.16 (cf. MIB object ieee8021XKayMkaParticipant Entry) and section 12.2 (cf. function createMKA()), [**assignment**: other management function]]*
- *Specify the lifetime of a CAK*
- *Enable, disable, or delete a PSK-based CAK using [**selection**: the MIB object ieee8021XKayMkaPartActivateControl, [**assignment**: other management function]]*

*[**selection**:*

- *Cause key server to generate a new group CAK (i.e., rekey the CA) using [**selection**: MIB object ieee8021XKayCreateNewGroup, [**assignment**: other management function]]*
- *Manage generation of a PSK-based CAK*
- *Support YANG configuration and operational state modes as specified in IEEE 802.1AEdk.*
- *No other MACsec management functions*

]].

Application Note: IEEE 802.1X-2020 specifies Management Information Base (MIB) objects for management functionality but configuration of management functions via other approved methods is acceptable. The ST author should select either the MIB object or provide the function used to achieve this management functionality.

If a selection containing "group CAK" is chosen in FCS_MKA_EXT.1.5, then "Cause key server to generate a new group CAK…" must be selected.

Evaluation Activities

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 FMT_SMF.1/MACSEC:1: 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.*
  - *(conditional, the length of the CKN is not configurable) Repeat this test again for CKN of invalid lengths zero and 33, and observe failure.*
  - *(conditional, the length of the CKN is configurable) The evaluator shall observe that the admin guidance instructs the admin to configure the TOE to only allow CKN lengths of 1-32 bytes.*
- *Test FMT_SMF.1/MACSEC:2: (Conditional: "Cause key server to generate a new group CAK..." is selected) 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 cannot communicate with device C. The evaluator shall re-enable the MKA participant of device C and observe that the TOE is now able to communicate with devices B and C.*
- *Test FMT_SMF.1/MACSEC:3: 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 FMT_SMF.1/MACSEC:3.1: (Conditional: The TOE supports MKA keychains with multiple CKN/CAKs) 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 FMT_SMF.1/MACSEC:3.2: 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 FMT_SMF.1/MACSEC:4: (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.*

5.2.6 Class FPT: Protection of the TSF

FPT_CAK_EXT.1 Protection of CAK Data

FPT_CAK_EXT.1.1

The TSF shall prevent reading of CAK values by administrators.

Application Note: The intent is for the TOE to protect CAK data from unauthorized disclosure. This data should only be accessed for the purposes of its assigned security functionality and there is no need for it to be displayed or accessed at any other time. This requirement does not prevent the device from providing indication that these exist, are in use, or are still valid. It does, however, restrict the reading of the values outright.

Evaluation Activities

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

The evaluator shall examine the operational guidance to determine that it identifies the locations where administrators can view information about CAKs or associated settings.

Tests

The evaluator shall follow the operational guidance to view the locations where information about CAKs or associated settings are stored and verify that these locations do not expose CAK values. If the administrator has console access to the TOE's operating system, the evaluator shall verify that plaintext CAK values are not accessible on the file system.

FPT_FLS.1/MACSEC Failure with Preservation of Secure State (MACsec)

FPT_FLS.1.1/MACSEC

The TSF shall **fail-secure** when **any of** the following types of failures occur: [*failure of the power-on self-tests, failure of integrity check of the TSF executable image, failure of noise source health tests*].

Application Note: The intent of this requirement is to express the fail secure capabilities that the TOE possesses. This means that the TOE must be able to attain a secure/safe state (e.g., shutdown) when any of the identified failures occur. Fail secure is defined as a state where data cannot be passed without adhering to the TOE's security policies, and ensures the continued protection of any key material and user data. For a TOE with redundant failover capability (that continues to operate if power-on self-test (POST) passes on the redundant component), in the event of a POST failure on a redundant component, the specific component that received the POST failure will attain a secure/safe state (e.g., shutdown). For conformance with other PP-Modules it might be a requirement for the fail-secure state to be “shut down.”

Evaluation Activities

FPT_FLS.1/MACSEC

TSS

The evaluator shall examine the TSS to determine that it indicates that the TSF will attain a secure/safe state (e.g., shutdown) 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 attain a secure/safe state (e.g., shutdown) 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 FPT_FLS.1/MACSEC:1: For each failure mode specified in the ST that can be deliberately induced, the evaluator shall ensure that the TOE attains a secure state (e.g., shutdown) after initiating each failure mode type. For TOEs with redundant failover capability, the evaluator shall determine that the failed components attain a secure state 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.1.1

The TSF shall detect replay for the following entities: [*MPDUs, MKA frames*].

FPT_RPL.1.2

The TSF shall perform [*discarding of the replayed data, logging of the detected replay attempt*] when replay is detected.

Application Note: IEEE 802.1X-2020 and IEEE 802.1AE-2018 describe this capability as "replay protection".
As per IEEE 802.1AE-2018, replay is detected by examining the PN value that is embedded in the SecTag that is at the header of the MPDU. The PN is encoded in octets 5 through 8 of the SecTag to support replay protection. As per IEEE 802.1X-2020, section 9.4.2, MKA frame replay is detected by examining the combination of the member identifier (MI) and the message number (MN) in the Basic Parameter set.

Evaluation Activities

FPT_RPL.1
TSS
The evaluator shall examine the TSS to determine that it describes how replay is detected for MKPDUs and MPDUs and how replayed MKPDUs and 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 MN and PN values are incremented separately for each direction.

- *Test FPT_RPL.1:1: 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 SA is a duplicate of the original connection and 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 FPT_RPL.1:2: The evaluator shall capture frames during an MKA session and record the lowest MN from the Basic Parameter set observed in a particular time range. The evaluator shall then send a frame with a lower MN, and then verify that this frame is dropped. The evaluator shall verify that the device logged this event.*

5.2.7 Class FTP: Trusted Path/Channels

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

FTP_ITC.1.1/MACSEC
The TSF shall provide a communication channel between itself and **a MACsec peer** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/MACSEC
The TSF shall permit [**selection**: *the TSF, another trusted IT product*] to initiate communication via the trusted channel.

FTP_ITC.1.3/MACSEC
The TSF shall initiate communication via the trusted channel for [*communications with MACsec peers that require the use of MACsec*].

Evaluation Activities

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

5.3 TOE Security Functional Requirements Rationale

The following rationale provides justification for each SFR for the TOE, showing that the SFRs are suitable to address the specified threats:

Table 2: SFR Rationale

Threat	Addressed by	Rationale
T.DATA_INTEGRITY	FCS_COP.1/KDFCMAC	Mitigates the threat by using a secure keyed-hash function as part of the process generate MACsec keys.
	FCS_COP.1/MACSEC	Mitigates the threat by using secure encryption/decryption functions to encrypt traffic over MACsec.
	FCS_MACSEC_EXT.2	Mitigates the threat by utilizing integrity protection features of MACsec.
	FCS_MACSEC_EXT.3	Mitigates the threat by using a secure process to generate traffic-protecting keys.

	FCS_SNMP_EXT.1 (selection-based)	Mitigates the threat by using a secure configuration of SNMP to administer the TSF.
	FPT_RPL_EXT.1 (optional)	Mitigates the threat by utilizing extended standards to number packets, thus enabling the detection of replay attempts.
	FPT_RPL.1	Mitigates the threat by detecting and blocking replay attempts.
	FTP_ITC.1/MACSEC	Mitigates the threat by providing a secure communication channel for the use of MACsec.
	FTP_TRP.1/MACSEC (optional)	Mitigates the threat by providing a secure communication channel for the administration of the TSF over a secure protocol.
T.NETWORK_ACCESS	FCS_DEVID_EXT.1 (selection-based)	Mitigates the threat by identifying devices using a secure device identifier.
	FCS_EAPTLS_EXT.1 (selection-based)	Mitigates the threat by utilizing the EAP-TLS protocol to authenticate communication peers.
	FCS_MACSEC_EXT.1	Mitigates the threat by utilizing the MACsec protocol to secure traffic transmitted between an external and internal network.
	FCS_MACSEC_EXT.4	Mitigates the threat by authenticating the communication peers utilizing a secure credential (pre-shared key or EAP-TLS).
	FCS_MKA_EXT.1	Mitigates the threat by securely generating, agreeing upon, and transmitting keys used for MACsec traffic.
	FIA_PSK_EXT.1	Mitigates the threat by utilizing secure pre-shared keys as part of the authentication process for MACsec.
	FPT_DDP_EXT.1 (optional)	Mitigates the threat by preventing traffic that is delayed from being accepted, reducing the risk of replay or other modifications to the traffic.
T.SECURITY_ FUNCTIONALITY_FAILURE (from NDcPP)	FPT_FLS.1/MACSEC	Mitigates the threat by attaining a secure state (e.g., shutdown) upon the failure of TSF-relevant health tests.
T.UNAUTHORIZED_ ADMINISTRATOR_ACCESS (from NDcPP)	FIA_AFL_EXT.1 (optional)	Mitigates the threat by limiting the rate of authentication if too many authentication failures have occurred.
	FMT_SMF.1/MACSEC	Mitigates the threat by specifying functionality that must be restricted to administrators.
	FMT_SNMP_EXT.1 (selection-based)	Mitigates the threat by utilizing a secure configuration of SNMP to administer the TSF.
	FPT_CAK_EXT.1	Mitigates the threat by preventing sensitive data (CAK values) from being disclosed, even to an administrator.

	FTP_TRP.1/MACSEC (optional)	Mitigates the threat by using a secure path to administer the TSF, preventing secure values from being recorded, replayed, or otherwise impersonated.
T.UNDETECTED_ACTIVITY (from NDcPP)	FAU_GEN.1/MACSEC	Mitigates the threat by logging traffic and actions relevant to secure operations.
T.UNTRUSTED_MACSEC_COMMUNICATION_CHANNELS	FCS_COP.1/KDFCMAC	Mitigates the threat by utilizing keyed-hash functions to ensure message authentication.
	FCS_COP.1/MACSEC	Mitigates the threat by utilizing encryption/decryption functions to ensure message integrity and confidentiality.
	FCS_MACSEC_EXT.2	Mitigates the threat by utilizing MACsec in a configuration to protect the integrity of transmissions to or from the TOE.
	FCS_MACSEC_EXT.3	Mitigates the threat by ensuring that MACsec Secure Association Keys are generated unpredictably, thus lessening the possibility of a loss in integrity.
	FCS_SNMP_EXT.1 (selection-based)	Mitigates the threat by providing a secure channel for administrative configuration that utilizes SNMP, preventing passwords or other secure values from disclosure.
	FTP_ITC.1/MACSEC	Mitigates the threat by providing a secure channel for communication that utilizes the prescribed configurations of MACsec.
	FTP_TRP.1/MACSEC (optional)	Mitigates the threat by providing a secure channel for administrative configuration that utilizes MACsec, preventing passwords or other secure values from disclosure.

5.4 TOE Security Assurance Requirements

This PP-Module does not define any Security Assurance requirements. The SARs from the Base-PP must be satisfied.

6 Consistency Rationale

6.1 Collaborative Protection Profile for Network Devices

6.1.1 Consistency of TOE Type

When this PP-Module is used to extend the NDcPP, the TOE type for the overall TOE is still a network device. The TOE boundary is simply extended to include MACsec functionality that is provided by the network device.

6.1.2 Consistency of Security Problem Definition

The threats defined by this PP-Module (see section 3.1) supplement those defined in the NDcPP as follows:

Table 3: Consistency of Security Problem Definition (NDcPP base)

PP-Module Threat, Assumption, OSP	Consistency Rationale
T.DATA_INTEGRITY	The threat of data integrity compromise at the layer 2 level is a specific threat that can be countered by MACsec technology.
T.NETWORK_ACCESS	The threat of a malicious entity accessing protected network resources without authorization is a specific example of the T.UNTRUSTED_COMMUNICATION_CHANNELS threat defined in the Base-PP.
T.UNTRUSTED_MACSEC_COMMUNICATION_CHANNELS	The threat of disclosure of data in protected communications channels is the same as the T.UNTRUSTED_COMMUNICATION_CHANNELS threat in the NDcPP. This PP-Module expands on that by introducing additional logical interfaces (MACsec, SNMP) that this threat applies to.

6.1.3 Consistency of OE Objectives

This PP-Module does not define any environmental objectives, but does note that OE.NO_THRU_TRAFFIC_PROTECTION from the NDcPP only applies to the Base-PP external interfaces. This is because the MACsec interface defined by this PP-Module does enforce through-traffic protection.

6.1.4 Consistency of Requirements

This PP-Module identifies several SFRs from the NDcPP that are needed to support MACsec Ethernet Encryption functionality. This is considered to be consistent because the functionality provided by the NDcPP is being used for its intended purpose. The rationale for why this does not conflict with the claims defined by the NDcPP are as follows:

Table 4: Consistency of Requirements (NDcPP base)

PP-Module Requirement	Consistency Rationale
Modified SFRs	
This PP-Module does not modify any requirements when the NDcPP is the base.	
Additional SFRs	

This PP-Module does not add any requirements when the NDcPP is the base.

Mandatory SFRs	
FAU_GEN.1/MACSEC	This SFR is an iteration of a Base-PP requirement that defines additional auditable events for MACsec functionality that the Base-PP could not be expected to cover.
FCS_COP.1/KDFCMAC	This PP-Module iterates an SFR defined in the Base-PP to define new cryptographic operations that are specific to the protocols defined in the PP-Module.
FCS_COP.1/MACSEC	This PP-Module iterates an SFR defined in the Base-PP to define new cryptographic operations that are specific to the protocols defined in the PP-Module.
FCS_MACSEC_EXT.1	This SFR applies to MACsec functionality, which is beyond the original scope of the Base-PP.
FCS_MACSEC_EXT.2	This SFR applies to MACsec functionality, which is beyond the original scope of the Base-PP.
FCS_MACSEC_EXT.3	This SFR applies to MACsec functionality, which is beyond the original scope of the Base-PP.
FCS_MACSEC_EXT.4	This SFR applies to MACsec functionality, which is beyond the original scope of the Base-PP.
FCS_MKA_EXT.1	This SFR applies to a MACsec peer authentication mechanism, which is beyond the original scope of the Base-PP, though it is based on the TLS implementation specified in the Base-PP.
FIA_PSK_EXT.1	This SFR applies to PSKs for MKA, which is beyond the original scope of the Base-PP.
FMT_SMF.1/MACSEC	This SFR applies to management functions related to MACsec, which is beyond the original scope of the Base-PP.
FPT_CAK_EXT.1	This SFR requires that keys specific to MACsec be protected. This is similar to FPT_SKP_EXT.1 in the Base-PP but applies to keys that were beyond the original scope of the Base-PP.
FPT_FLS.1/MACSEC	This SFR requires the TSF to react in a specific manner upon failure of specific self-tests. The Base-PP defines FPT_TST_EXT.1 for self-test functionality, but does not define specific self-tests. This PP-Module implies that certain self-tests must be done at minimum, but this does not conflict with what is permitted by the Base-PP.
FPT_RPL.1	This SFR applies to replay detection functionality, which is beyond the original scope of the Base-PP.
FTP_ITC.1/MACSEC	This PP-Module defines an additional trusted channel function for MACsec communications, which is beyond the original scope of the Base-PP.
Optional SFRs	
FIA_AFL_EXT.1	This SFR defines a specific authentication limiting mechanism that exists on top of what FIA_AFL.1 in the Base-PP may also require.
FPT_DDP_EXT.1	Data delay protection uses packet counting information from MKA packets to drop differentially delayed MACsec packets at the receiver.
FPT_RPL_EXT.1	This SFR applies to replay detection functionality, which is beyond the original scope of the Base-PP.

FTP_TRP.1/MACSEC	This PP-Module defines an optional method of administration for MACsec functionality using trusted protocols that are not defined in the Base-PP. As this functionality is optional, a conformant TOE may also use the Base-PP's trusted path to administer these functions.
Objective SFRs	
This PP-Module does not define any Objective requirements.	
Implementation-dependent SFRs	
This PP-Module does not define any Implementation-dependent requirements.	
Selection-based SFRs	
FCS_DEVID_EXT.1	This SFR applies to a MACsec peer authentication mechanism, which is beyond the original scope of the Base-PP.
FCS_EAPTLS_EXT.1	This SFR applies to a MACsec peer authentication mechanism, which is beyond the original scope of the Base-PP, though it is based on the TLS implementation specified in the Functional Package for TLS.
FCS_SNMP_EXT.1	This SFR applies to implementation of the SNMP protocol, which is beyond the original scope of the Base-PP, though it is based on the TLS implementation specified in the Base-PP.
FMT_SNMP_EXT.1	This SFR defines requirements for use of SNMP as a management interface, which is beyond the original scope of the Base-PP.

Appendix A - Optional SFRs

A.1 Strictly Optional Requirements

A.1.1 Auditable Events for Strictly Optional SFRs

Table 5: Auditable Events for Strictly Optional Requirements

Requirement	Auditable Events	Additional Audit Record Contents
FIA_AFL_EXT.1	No events specified	N/A
FPT_DDP_EXT.1	No events specified	N/A
FPT_RPL_EXT.1	No events specified	N/A
FTP_TRP.1/MACSEC	No events specified	N/A

A.1.2 Class FIA: vIdentification and Authentication

FIA_AFL_EXT.1 Authentication Attempt Limiting

FIA_AFL_EXT.1.1

When three unsuccessful authentication attempts have been made to the local console, the TSF shall limit the rate of login attempts to one per minute.

Application Note: This requirement applies to an administrator at a local console. This anti-hammering requirement is to slow down brute force password guessing.

Evaluation Activities

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 FIA_AFL_EXT.1:1: 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.

A.1.3 Class FPT: Protection of the TSF

FPT_DDP_EXT.1 Data Delay Protection

FPT_DDP_EXT.1.1

The TSF shall enable data delay protection for MKA that ensures data frames protected by MACsec are not delayed by more than two seconds.

Application Note: If FPT_DDP_EXT.1 is claimed, then the corresponding selection of "MKA Bounded Hello Time limit of 0.5 seconds" must be made in FCS_MKA_EXT.1.4.

Evaluation Activities

FPT_DDP_EXT.1
TSS
There are no TSS EAs for this component.

Guidance
There are no guidance EAs for this component.

Tests
- *Test FPT_DDP_EXT.1:1: 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.1.1

The TSF shall support extended packet numbering (XPN) as per IEEE 802.1AE-2018.

FPT_RPL_EXT.1.2

The TSF shall support [*GCM-AES-XPN-256*] as per IEEE 802.1AE-2018.

Application Note: XPN support is expected for devices that are capable of 40 Gbps or higher throughput. This SFR is optional because not all conformant TOEs are expected to provide this level of bandwidth. For XPN the full 64-bit PN is recovered using the 32 least significant bits conveyed in the SecTag and the 32 most significant bits are recovered on receipt of a frame.

Evaluation Activities

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 FPT_RPL_EXT.1:1: 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. The evaluator shall verify that the encrypted frames are different as the IV is unique.*

  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 and amendment AEdk-2023.
- *Test FPT_RPL_EXT.1:2: If both ciphersuites were selected, then the evaluator shall reconfigure the TOE using the second ciphersuite and rerun Test FPT_RPL_EXT.1:1 to demonstrate support for both ciphersuites.*

A.1.4 Class FTP: Trusted Path/Channels

FTP_TRP.1/MACSEC Trusted Path (MACsec Administration)

FTP_TRP.1.1/MACSEC

The TSF shall provide a communication path between itself and [*remote*] users **using [selection: *MACsec*, *SNMPv3*]** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [*modification, disclosure*].

FTP_TRP.1.2/MACSEC

The TSF shall permit [*remote users*] to initiate communication via the trusted path.

FTP_TRP.1.3/MACSEC

The TSF shall require the use of the trusted path for [*remote administration of MACsec management functions as defined in FMT_SMF.1/MACSEC*].

Application Note: This SFR is optional because it is permissible for the management functions defined in this PP-Module to be implemented solely through the trusted path defined in FTP_TRP.1/Admin in the Base-PP. If SNMP is selected, the FCS_SNMP_EXT.1 and FMT_SNMP_EXT.1 SFRs must be claimed.

Evaluation Activities

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).

A.2 Objective Requirements

This PP-Module does not define any Objective SFRs.

A.3 Implementation-dependent Requirements

This PP-Module does not define any Implementation-dependent SFRs.

Appendix B - Selection-based Requirements

B.1 Auditable Events for Selection-based SFRs

Table 6: Auditable Events for Selection-based Requirements

Requirement	Auditable Events	Additional Audit Record Contents
FCS_DEVID_EXT.1	No events specified	N/A
FCS_EAPTLS_EXT.1	No events specified	N/A
FCS_SNMP_EXT.1	No events specified	N/A
FMT_SNMP_EXT.1	No events specified	N/A

B.2 Class FCS: Cryptographic Support

FCS_DEVID_EXT.1 Secure Device Identifiers

The inclusion of this selection-based component depends upon selection in FCS_MACSEC_EXT.4.1.

FCS_DEVID_EXT.1.1
The TSF shall implement Secure Device Identifiers (DevIDs) following IEEE Standard 802.1AR-2018.

FCS_DEVID_EXT.1.2
The TSF shall contain an Initial DevID (IDevID) as specified in Section 6 of IEEE 802.1AR-2018.

FCS_DEVID_EXT.1.3
The TSF shall contain the credential chain as specified in Section 6.3 of IEEE 802.1AR-2018.

FCS_DEVID_EXT.1.4
The TSF shall verify that both the Supplicant and Authenticator DevIDs presented for EAP-TLS have credentials that chain to one of the specified Certificate Authorities.

FCS_DEVID_EXT.1.5
The TSF shall not establish a trusted channel if the Supplicant DevID is invalid.

FCS_DEVID_EXT.1.6
The TSF shall support mutual authentication using DevIDs.

FCS_DEVID_EXT.1.7
The TSF shall support the following operations as specified in Section 7.2 of IEEE 802.1AR-2018:

1. Enable or disable DevID credential
2. Enable or disable DevID key

Evaluation Activities

FCS_DEVID_EXT.1.1
This element is evaluated through completion of the evaluation activities for FCS_DEVID_EXT.1.5 through 1.7.

FCS_DEVID_EXT.1.2
This element is evaluated through completion of the evaluation activities for FCS_DEVID_EXT.1.5 through 1.7.

FCS_DEVID_EXT.1.3
This element is evaluated through completion of the evaluation activities for FCS_DEVID_EXT.1.5 through 1.7.

FCS_DEVID_EXT.1.4
This element is evaluated through completion of the evaluation activities for FCS_DEVID_EXT.1.5 through 1.7.

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 FCS_DEVID_EXT.1.5:1:*
  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 FCS_DEVID_EXT.1.5:2:*
  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 FCS_DEVID_EXT.1.5:3:*
  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 FCS_DEVID_EXT.1.6:1:*

- *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 FCS_DEVID_EXT.1.7:1:*
  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 FCS_DEVID_EXT.1.7:2:*
  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

The inclusion of this selection-based component depends upon selection in FCS_MACSEC_EXT.4.1.

FCS_EAPTLS_EXT.1.1

The TSF shall implement the Extensible Authentication Protocol (EAP) as specified in RFC 9190 and EAP-Transport Layer Security (EAP-TLS) as specified in RFC 5216 as updated by RFC 8996 with TLS implemented using mutual authentication in accordance with [*FCS_TLS_EXT.1 and [**selection**:*

- *FCS_DTLSC_EXT.1 and FCS_DTLSC_EXT.2*
- *FCS_DTLSS_EXT.1 and FCS_DTLSS_EXT.2*
- *FCS_TLSC_EXT.1 and FCS_TLSC_EXT.2*
- *FCS_TLSS_EXT.1 and FCS_TLSS_EXT.2*

*] **from the Functional Package for Transport Layer Security (TLS), version 2.1***].

Application Note: If this SFR is selected, the appropriate selections in FCS_TLS_EXT.1 must be made according to the functionality claimed in this SFR. A claim for the FCS_(D)TLSC_EXT or FCS_(D)TLSS SFRs identified in this requirement must also be included.

The Functional Package for TLS specifies support for either TLS 1.2 or TLS 1.3, but this PP-Module requires TLS 1.3 to be claimed in order to conform with RFC 9190.

Evaluation Activities

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

The inclusion of this selection-based component depends upon selection in FTP_TRP.1.1/MACSEC.

FCS_SNMP_EXT.1.1

The TSF shall support SNMP using TLS as specified in RFC 6353 as updated by RFC 8996 with TLS implemented using mutual authentication in accordance with [**selection**:

- *FCS_DTLSC_EXT.1 and FCS_DTLSC_EXT.2*
- *FCS_DTLSS_EXT.1 and FCS_DTLSS_EXT.2*
- *FCS_TLSC_EXT.1 and FCS_TLSC_EXT.2*
- *FCS_TLSS_EXT.1 and FCS_TLSS_EXT.2*

] **from the Functional Package for Transport Layer Security (TLS), version 2.1**.

Application Note: If this SFR is selected, the appropriate FCS_(D)TLSC_EXT and FCS_(D)TLSS_EXT SFRs from the Base-PP must be included.

Evaluation Activities

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 FCS_SNMP_EXT.1:1: 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 FCS_SNMP_EXT.1:2: 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 Functional Package for Transport Layer Security (TLS), version 2.1.

B.3 Class FMT: Security Management

FMT_SNMP_EXT.1 SNMP Management

The inclusion of this selection-based component depends upon selection in FTP_TRP.1.1/MACSEC.

FMT_SNMP_EXT.1.1
The TSF shall implement Simple Network Management Protocol (SNMP) with TLS security in conformance with RFC 6353 “Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP).”

FMT_SNMP_EXT.1.2
The TSF shall permit access to TSF management functions using only SNMP version 3.

FMT_SNMP_EXT.1.3
The TSF shall support the following password quality metrics for SNMPv3 passwords: [*character selections and minimum length defined in FIA_PMG_EXT.1 (from [NDcPP])*].

Application Note: FIA_PMG_EXT.1 is defined in the Base-PP so a conformant MACsec TOE will include this dependency.

Evaluation Activities

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 FMT_SNMP_EXT.1:1: The evaluator shall attempt to connect to the TOE using SNMPv2 and observe that the connection is not successful.*

- *Test FMT_SNMP_EXT.1:2: 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.

Appendix C - Extended Component Definitions

This appendix contains the definitions for all extended requirements specified in the PP-Module.

C.1 Extended Components Table

All extended components specified in the PP-Module are listed in this table:

Table 7: Extended Component Definitions

Functional Class	Functional Components
Class FCS: Cryptographic Support	FCS_DEVID_EXT Secure Device Identifiers FCS_EAPTLS_EXT EAP-TLS Protocol FCS_MACSEC_EXT MACsec FCS_MKA_EXT MACsec Key Agreement FCS_SNMP_EXT SNMP Protocol
Class FIA: Identification and Authentication	FIA_PSK_EXT Pre-Shared Key Composition
Class FIA: vIdentification and Authentication	FIA_AFL_EXT Authentication Failure Handling
Class FMT: Security Management	FMT_SNMP_EXT SNMP Management
Class FPT: Protection of the TSF	FPT_CAK_EXT Protection of CAK Data FPT_DDP_EXT Data Delay Protection FPT_RPL_EXT Replay Protection

C.2 Extended Component Definitions

C.2.1 Class FCS: Cryptographic Support

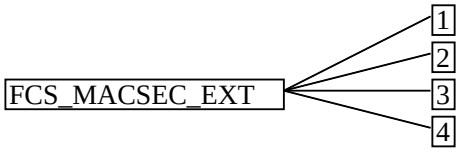
This PP-Module defines the following extended components as part of the class originally defined by CC Part 2:

C.2.1.1 FCS_MACSEC_EXT MACsec

Family Behavior

This family defines requirements for implementation of MACsec functionality.

Component Leveling



FCS_MACSEC_EXT.1, MACsec, requires the TSF to implement MACsec in a specified manner.

FCS_MACSEC_EXT.2, MACsec Integrity and Confidentiality, requires the TSF to implement MACsec with support for integrity and confidentiality protection.

FCS_MACSEC_EXT.3, MACsec Randomness, requires the TSF to generate keys and key data using sufficient randomness.

FCS_MACSEC_EXT.4, MACsec Key Usage, requires the TSF to specify the supported methods of MACsec peer authentication and to define the lifecycle for keys used in support of this.

Management: FCS_MACSEC_EXT.1

No specific management functions are identified.

Audit: FCS_MACSEC_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Session establishment.

FCS_MACSEC_EXT.1 MACsec

Hierarchical to: No other components.

Dependencies to: No dependencies.

FCS_MACSEC_EXT.1.1

The TSF shall implement MACsec in accordance with IEEE Standard 802.1AE-2018.

FCS_MACSEC_EXT.1.2

The TSF shall derive a Secure Channel Identifier (SCI) from a peer's MAC address and port to uniquely identify the originator of an MPDU.

FCS_MACSEC_EXT.1.3

The TSF shall reject any MPDUs during a given session that contain an SCI other than the one used to establish that session.

FCS_MACSEC_EXT.1.4

The TSF shall permit only EAPOL (Port Access Entity (PAE) EtherType 88-8E), MACsec frames (EtherType 88-E5), and [**selection**: *MAC control frames (EtherType is 88-08), [**assignment**: list of other permitted EtherTypes], no other frame types*] and shall discard others.

FCS_MACSEC_EXT.1.5

The TSF shall reject MPDUs that fail to meet the following characteristics, as defined by IEEE 802.1ae-2018:

a. It comprises at least 17 octets.
b. Octets 1 and 2 compose the MACsec EtherType.
c. The V bit in the TAG control information (TCI) is clear.
d. If the end station (ES) or the single copy broadcast (SCB) bit in the TCI is set, then the SC bit is clear.
e. Bits 7 and 8 of octet 4 of the SecTAG are clear.
f. If the C and SC bits in the TCI are clear, the MPDU comprises 24 octets plus the number of octets indicated by the SL field if that is non-zero and at least 72 octets otherwise.
g. If the C bit is clear and the SC bit set, then the MPDU comprises 32 octets plus the number of octets indicated by the short length (SL) field if that is non-zero and at least 80 octets otherwise.
h. If the C bit is set and the SC bit clear, then the MPDU comprises 8 octets plus the minimum length of the integrity check value (ICV) as determined by the Cipher Suite in use at the receiving MAC Security Entity (SecY), plus the number of octets indicated by the SL field if that is non-zero and at least 48 additional octets otherwise.

i. If the C and SC bits are both set, the frame comprises at least 16 octets plus the minimum length of the ICV as determined by the Cipher Suite in use at the receiving SecY, plus the number of octets indicated by the SL field if that is non-zero and at least 48 additional octets otherwise.

Management: FCS_MACSEC_EXT.2

No specific management functions are identified.

Audit: FCS_MACSEC_EXT.2

There are no auditable events foreseen.

FCS_MACSEC_EXT.2 MACsec Integrity and Confidentiality

Hierarchical to: No other components.

Dependencies to: FCS_MACSEC_EXT.1 MACsec

FCS_MACSEC_EXT.2.1

The TOE shall implement MACsec with support for integrity protection with a confidentiality offset of [**assignment**: *supported confidentiality offset value(s)*].

FCS_MACSEC_EXT.2.2

The TSF shall provide assurance of the integrity of protocol data units (MPDUs) using an Integrity Check Value (ICV) derived with the SAK.

FCS_MACSEC_EXT.2.3

The TSF shall provide the ability to derive an Integrity Check Value Key (ICK) from a Connectivity Association Key (CAK) using a KDF.

Management: FCS_MACSEC_EXT.3

No specific management functions are identified.

Audit: FCS_MACSEC_EXT.3

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Creation and update of Secure Association Key.

FCS_MACSEC_EXT.3 MACsec Randomness

Hierarchical to: No other components.

Dependencies to: FCS_MACSEC_EXT.1 MACsec
FCS_RBG.1 Random Bit Generation

FCS_MACSEC_EXT.3.1

The TSF shall generate unique Secure Association Keys (SAKs) using [**assignment**: *key generation or derivation method*] such that the likelihood of a repeating SAK is no less than 1 in 2 to the power of the size of the generated key.

FCS_MACSEC_EXT.3.2

The TSF shall generate unique nonces for the derivation of SAKs using the TOE's random bit generator as specified by FCS_RBG.1.

Management: FCS_MACSEC_EXT.4

The following actions could be considered for the management functions in FMT:

- Specify the lifetime of a CAK.

Audit: FCS_MACSEC_EXT.4

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Creation of CA.

FCS_MACSEC_EXT.4 MACsec Key Usage

Hierarchical to:	No other components.
Dependencies to:	FCS_COP.1 Cryptographic Operation FCS_MACSEC_EXT.1 MACsec FIA_PSK_EXT.1 Pre-Shared Key Composition

FCS_MACSEC_EXT.4.1

The TSF shall support peer authentication using pre-shared keys (PSKs) [**selection**: *EAP-TLS with DevIDs, no other method*].

FCS_MACSEC_EXT.4.2

The TSF shall distribute SAKs between MACsec peers using AES key wrap as specified in FCS_COP.1.

FCS_MACSEC_EXT.4.3

The TSF shall support specifying a lifetime for CAKs.

FCS_MACSEC_EXT.4.4

The TSF shall associate Connectivity Association Key Names (CKNs) with SAKs that are defined by the KDF using the CAK as input data (per IEEE 802.1X-2020, Section 9.8.1).

FCS_MACSEC_EXT.4.5

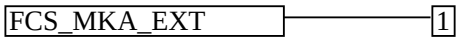
The TSF shall associate CKNs with CAKs. The length of the CKN shall be an integer number of octets, between 1 and 32 (inclusive).

C.2.1.2 FCS_MKA_EXT MACsec Key Agreement

Family Behavior

This family defines requirements for MKA.

Component Leveling



FCS_MKA_EXT.1, MACsec Key Agreement, defines the TSF's implementation of the Key Agreement Protocol.

Management: FCS_MKA_EXT.1

The following actions could be considered for the management functions in FMT:

- Ability to create, delete, and activate MKA participants.
- Ability to generate a group CAK.

Audit: FCS_MKA_EXT.1

There are no auditable events foreseen.

FCS_MKA_EXT.1 MACsec Key Agreement

Hierarchical to: No other components.

Dependencies to: FCS_MACSEC_EXT.1 MACsec

FCS_MKA_EXT.1.1

The TSF shall implement Key Agreement Protocol (MKA) in accordance with IEEE 802.1X-2020.

FCS_MKA_EXT.1.2

The TSF shall provide assurance of the integrity of MKA protocol data units (MKPDUs) using an Integrity Check Value (ICV) derived from an Integrity Check Value Key (ICK).

FCS_MKA_EXT.1.3

The TSF shall provide the ability to derive an Integrity Check Value Key (ICK) from a CAK using a KDF.

FCS_MKA_EXT.1.4

The TSF shall enforce an MKA Lifetime Timeout limit of 6.0 seconds and [**selection**: *MKA Hello Time limit of 2 seconds*, *MKA Bounded Hello Time limit of 0.5 seconds*].

FCS_MKA_EXT.1.5

The key server shall refresh a SAK when it expires. The key server shall distribute a SAK by [**assignment**: *key type and distribution method*].

FCS_MKA_EXT.1.6

The key server shall distribute a fresh SAK whenever a member is added to or removed from the live membership of the CA.

FCS_MKA_EXT.1.7

The TSF shall validate MKPDUs according to IEEE 802.1X-2020 Section 11.11.2. In particular, the TSF shall discard without further processing any MKPDUs to which any of the following conditions apply:

a. The destination address of the MKPDU was an individual address
b. The MKPDU is less than 32 octets long
c. The MKPDU comprises fewer octets than indicated by the Basic Parameter Set body length, as encoded in bits 4 through 1 of octet 3 and bits 8 through 1 of octet 4, plus 16 octets of ICV
d. The CAK Name is not recognized

If an MKPDU passes these tests, then the TSF will begin processing it as follows:

a. If the Algorithm Agility parameter identifies an algorithm that has been implemented by the receiver, the ICV shall be verified as specified in IEEE 802.1X-2020 Section 9.4.1.

b. If the Algorithm Agility parameter is unrecognized or not implemented by the receiver, its value can be recorded for diagnosis but the received MKPDU shall be discarded without further processing.

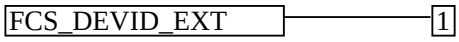
Each received MKPDU that is validated as specified in this clause and verified as specified in IEEE 802.1X-2020 Section 9.4.1 shall be decoded as specified in IEEE 802.1X-2020 Section 11.11.4.

C.2.1.3 FCS_DEVID_EXT Secure Device Identifiers

Family Behavior

This family defines requirements for the implementation and use of Secure DevIDs.

Component Leveling



FCS_DEVID_EXT.1, Secure Device Identifiers, requires the TSF to implement and use DevIDs according to acceptable standards.

Management: FCS_DEVID_EXT.1

No specific management functions are identified.

Audit: FCS_DEVID_EXT.1

There are no auditable events foreseen.

FCS_DEVID_EXT.1 Secure Device Identifiers

Hierarchical to: No other components.

Dependencies to: FCS_EAPTLS_EXT.1 EAP-TLS Protocol

FCS_DEVID_EXT.1.1

The TSF shall implement Secure Device Identifiers (DevIDs) following IEEE Standard 802.1AR-2018.

FCS_DEVID_EXT.1.2

The TSF shall contain an Initial DevID (IDevID) as specified in Section 6 of IEEE 802.1AR-2018.

FCS_DEVID_EXT.1.3

The TSF shall contain the credential chain as specified in Section 6.3 of IEEE 802.1AR-2018.

FCS_DEVID_EXT.1.4

The TSF shall verify that both the Supplicant and Authenticator DevIDs presented for EAP-TLS have credentials that chain to one of the specified Certificate Authorities.

FCS_DEVID_EXT.1.5

The TSF shall not establish a trusted channel if the Supplicant DevID is invalid.

FCS_DEVID_EXT.1.6

The TSF shall support mutual authentication using DevIDs.

FCS_DEVID_EXT.1.7

The TSF shall support the following operations as specified in Section 7.2 of IEEE 802.1AR-2018:

1. Enable or disable DevID credential
2. Enable or disable DevID key

C.2.1.4 FCS_EAPTLS_EXT EAP-TLS Protocol

Family Behavior

This family defines requirements for how the TSF implements EAP and EAP-Transport Layer Security.

Component Leveling

FCS_EAPTLS_EXT.1, EAP-TLS Protocol, requires the TSF to implement EAP and EAP-TLS according to appropriate standards.

Management: FCS_EAPTLS_EXT.1

No specific management functions are identified.

Audit: FCS_EAPTLS_EXT.1

There are no auditable events foreseen.

FCS_EAPTLS_EXT.1 EAP-TLS Protocol

Hierarchical to:	No other components.
Dependencies to:	FCS_TLS_EXT.1 TLS Protocol and [[FCS_DTLSC_EXT.1 DTLS Client Protocol and FCS_DTLSC_EXT.2 DTLS Client Support for Mutual Authentication], or [FCS_DTLSS_EXT.1 DTLS Server Protocol and FCS_DTLSS_EXT.2 DTLS Server Support for Mutual Authentication], or [FCS_TLSC_EXT.1 TLS Client Protocol and FCS_TLSC_EXT.2 TLS Client Support for Mutual Authentication], or [FCS_TLSS_EXT.1 TLS Server Protocol and FCS_TLSS_EXT.2 TLS Server Support for Mutual Authentication]]

FCS_EAPTLS_EXT.1.1

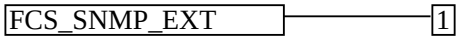
The TSF shall implement the Extensible Authentication Protocol (EAP) as specified in RFC 3748 and EAP-Transport Layer Security (EAP-TLS) as specified in RFC 5216 as updated by RFC 8996 with TLS implemented using mutual authentication in accordance with [**assignment**: *TLS or DTLS implementation that supports mutual authentication*].

C.2.1.5 FCS_SNMP_EXT SNMP Protocol

Family Behavior

This family defines requirements for implementation of SNMP.

Component Leveling



FCS_SNMP_EXT.1, SNMP Protocol, requires the TSF to implement and support SNMP using TLS using only algorithms that meet certain standards.

Management: FCS_SNMP_EXT.1

No specific management functions are identified.

Audit: FCS_SNMP_EXT.1

There are no auditable events foreseen.

FCS_SNMP_EXT.1 SNMP Protocol

Hierarchical to:	No other components.
Dependencies to:	[(FCS_DTLSC_EXT.1 DTLS Client Protocol and FCS_DTLSC_EXT.2 DTLS Client Support for Mutual Authentication), or FCS_DTLSS_EXT.1 DTLS Server Protocol and FCS_DTLSS_EXT.2 DTLS Server Support for Mutual Authentication), or (FCS_TLSC_EXT.1 TLS Client Protocol and FCS_TLSC_EXT.2 TLS Client Support for Mutual Authentication), or FCS_TLSS_EXT.1 TLS Server Protocol and FCS_TLSS_EXT.2 TLS Server Support for Mutual Authentication)]

FCS_SNMP_EXT.1.1

The TSF shall support SNMP using TLS as specified in RFC 6353 as updated by RFC 8996 with TLS implemented using mutual authentication in accordance with [**assignment**: *TLS or DTLS implementation that supports mutual authentication*].

C.2.2 Class FIA: Identification and Authentication

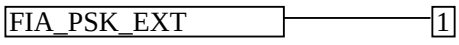
This PP-Module defines the following extended components as part of the class originally defined by CC Part 2:

C.2.2.1 FIA_PSK_EXT Pre-Shared Key Composition

Family Behavior

This family defines requirements for the generation and use of PSKs.

Component Leveling



FIA_PSK_EXT.1, Pre-Shared Key Composition, defines the TSF's uses for PSKs and how they are obtained by the TOE.

Management: FIA_PSK_EXT.1

The following actions could be considered for the management functions in FMT:

- Generate and install a PSK-based CAK.
- Enable, disable, or delete a PSK-based CAK.

Audit: FIA_PSK_EXT.1

There are no auditable events foreseen.

FIA_PSK_EXT.1 Pre-Shared Key Composition

Hierarchical to: No other components.

Dependencies to: No dependencies

FIA_PSK_EXT.1.1

The TSF shall use PSKs for MKA as defined by IEEE 802.1X-2020, [**selection**: *no other protocols*, *[**assignment**: other protocols that use PSKs]*].

FIA_PSK_EXT.1.2

The TSF shall be able to [**selection**: *accept*, *generate using the random bit generator specified in FCS_RBG.1*] bit-based PSKs.

C.2.3 Class FIA: vIdentification and Authentication

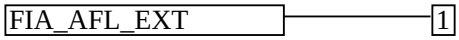
This PP-Module defines the following extended components as part of the class originally defined by CC Part 2:

C.2.3.1 FIA_AFL_EXT Authentication Failure Handling

Family Behavior

This family defines requirements for handling of authentication failures beyond those defined in the Part 2 family FIA_AFL.

Component Leveling



FIA_AFL_EXT.1, Authentication Attempt Limiting, requires the TSF to limit the rate of login attempts to a certain interval after a certain number of failed authentication attempts have occurred.

Management: FIA_AFL_EXT.1

No specific management functions are identified.

Audit: FIA_AFL_EXT.1

There are no auditable events foreseen.

FIA_AFL_EXT.1 Authentication Attempt Limiting

Hierarchical to: No other components.

Dependencies to: FIA_UAU.1 Timing of Authentication

FIA_AFL_EXT.1.1

When three unsuccessful authentication attempts have been made to the local console, the TSF shall limit the rate of login attempts to one per minute.

C.2.4 Class FMT: Security Management

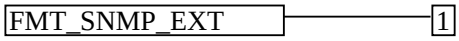
This PP-Module defines the following extended components as part of the class originally defined by CC Part 2:

C.2.4.1 FMT_SNMP_EXT SNMP Management

Family Behavior

This family defines the TOE's use of SNMP as a management interface.

Component Leveling



FMT_SNMP_EXT.1, SNMP Management, requires the TSF to implement SNMP with (D)TLS in conformance with specific standards for use as a management interface.

Management: FMT_SNMP_EXT.1

No specific management functions are identified.

Audit: FMT_SNMP_EXT.1

There are no auditable events foreseen.

FMT_SNMP_EXT.1 SNMP Management

Hierarchical to: No other components.

Dependencies to: FCS_SNMP_EXT.1 SNMP Protocol

FMT_SNMP_EXT.1.1

The TSF shall implement Simple Network Management Protocol (SNMP) with TLS security in conformance with RFC 6353 "Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP)."

FMT_SNMP_EXT.1.2

The TSF shall permit access to TSF management functions using only SNMP version 3.

FMT_SNMP_EXT.1.3

The TSF shall support the following password quality metrics for SNMPv3 passwords: [**assignment**: *password quality metrics*].

C.2.5 Class FPT: Protection of the TSF

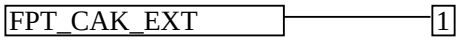
This PP-Module defines the following extended components as part of the class originally defined by CC Part 2:

C.2.5.1 FPT_CAK_EXT Protection of CAK Data

Family Behavior

This family defines confidentiality requirements for CAK data.

Component Leveling



FPT_CAK_EXT.1, Protection of CAK Data, requires the TSF to prevent administrators from being able to read the CAK values.

Management: FPT_CAK_EXT.1

No specific management functions are identified.

Audit: FPT_CAK_EXT.1

There are no auditable events foreseen.

FPT_CAK_EXT.1 Protection of CAK Data

Hierarchical to: No other components.

Dependencies to: No dependencies

FPT_CAK_EXT.1.1

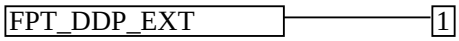
The TSF shall prevent reading of CAK values by administrators.

C.2.5.2 FPT_DDP_EXT Data Delay Protection

Family Behavior

This family defines requirements for enforcement of data delay protection.

Component Leveling



FPT_DDP_EXT.1, Data Delay Protection, requires the TSF to use MKA PN information to enforce a data delay protection check of two seconds on MACsec protected frames.

Management: FPT_DDP_EXT.1

No specific management functions are identified.

Audit: FPT_DDP_EXT.1

There are no auditable events foreseen.

FPT_DDP_EXT.1 Data Delay Protection

Hierarchical to: No other components.

Dependencies to: FCS_MACSEC_EXT.4 MACsec Key Usage
FCS_MKA_EXT.1 MACsec Key Agreement

FPT_DDP_EXT.1.1

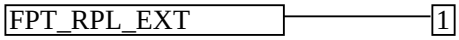
The TSF shall enable data delay protection for MKA that ensures data frames protected by MACsec are not delayed by more than two seconds.

C.2.5.3 FPT_RPL_EXT Replay Protection

Family Behavior

This family defines replay detection methods that are not defined in the Part 2 family FPT_RPL.

Component Leveling



FPT_RPL_EXT.1, Replay Protection for XPN, requires the TSF to support XPN as a method for detection of replayed traffic.

Management: FPT_RPL_EXT.1

No specific management functions are identified.

Audit: FPT_RPL_EXT.1

There are no auditable events foreseen.

FPT_RPL_EXT.1 Replay Protection for XPN

Hierarchical to: No other components.

Dependencies to: FCS_COP.1 Cryptographic Operation

FPT_RPL_EXT.1.1

The TSF shall support extended packet numbering (XPN) as per IEEE 802.1AE-2018.

FPT_RPL_EXT.1.2

The TSF shall support [**selection**: *GCM-AES-XPN-128, GCM-AES-XPN-256*] as per IEEE 802.1AE-2018.

Appendix D - Implicitly Satisfied Requirements

This appendix lists requirements that should be considered satisfied by products successfully evaluated against this PP-Module. These requirements are not featured explicitly as SFRs and should not be included in the ST. They are not included as standalone SFRs because it would increase the time, cost, and complexity of evaluation. This approach is permitted by [CC] Part 1, 8.3 Dependencies between components.

This information benefits systems engineering activities which call for inclusion of particular security controls. Evaluation against the PP-Module provides evidence that these controls are present and have been evaluated.

Table 8: Implicitly Satisfied Requirements

Requirement	Rationale for Satisfaction
FIA_UAU.1 – Timing of Authentication	FIA_AFL_EXT.1 has a dependency on FIA_UAU.1 because the notion of authentication failure handling implies the existence of an authentication mechanism. This dependency is addressed by a conformant TOE through the Base-PP requirement FIA_UIA_EXT.1.3, which defines authentication mechanisms specific to network devices.

Appendix E - Entropy Documentation and Assessment

The TOE does not require any additional supplementary information to describe its entropy source beyond the requirements outlined in the Base-PP. As with other Base-PP requirements, the only additional requirement is that the entropy documentation also applies to the specific MACsec Ethernet encryption capabilities of the TOE that require random data, in addition to any functionality required by the Base-PP.

Appendix F - Allocation of Requirements in Distributed TOEs

For a distributed TOE, the SFRs in this PP-Module need to be met by the TOE as a whole, but not all SFRs will necessarily be implemented by all components. The following categories are defined in order to specify when each SFR must be implemented by a component:

- **All Components ("All"):** All components that comprise the distributed TOE must independently satisfy the requirement.
- **At least one Component ("One"):** This requirement must be fulfilled by at least one component within the distributed TOE.
- **Feature Dependent ("Feature Dependent"):** These requirements will only be fulfilled where the feature is implemented by the distributed TOE component (note that the requirement to meet the PP-Module as a whole requires that at least one component implements these requirements if they are claimed by the TOE).

The table below specifies how each of the SFRs in this PP-Module must be met, using the categories above.

Requirement	Description	Distributed TOE SFR Allocation
FAU_GEN.1/MACSEC	Audit Data Generation (MACsec)	All
FCS_COP.1/KDFCMAC	Cryptographic Operation (AES-CMAC Keyed Hash Algorithm)	Feature Dependent
FCS_COP.1/MACSEC	Cryptographic Operation (MACsec AES Data Encryption and Decryption)	Feature Dependent
FCS_MACSEC_EXT.1	MACsec	Feature Dependent
FCS_MACSEC_EXT.2	MACsec Integrity and Confidentiality	Feature Dependent
FCS_MACSEC_EXT.3	MACsec Randomness	Feature Dependent
FCS_MACSEC_EXT.4	MACsec Key Usage	Feature Dependent
FCS_MKA_EXT.1	MACsec Key Agreement	Feature Dependent
FIA_PSK_EXT.1	Pre-Shared Key Composition	Feature Dependent
FMT_SMF.1/MACSEC	Specification of Management Functions (MACsec)	One
FPT_CAK_EXT.1	Protection of CAK Data	Feature Dependent
FPT_FLS.1/MACSEC	Failure with Preservation of Secure State	All
FPT_RPL.1	Replay Detection	Feature Dependent
FPT_ITC.1/MACSEC	Inter-TSF Trusted Channel (MACsec Communications)	Feature Dependent
FIA_AFL_EXT.1	Authentication Attempt Limiting	One
FPT_DDP_EXT.1	Data Delay Protection	Feature Dependent

FPT_RPL_EXT.1	Replay Detection for XPN	Feature Dependent
FTP_TRP.1/MACSEC	Trusted Path (MACsec Administration)	One
FCS_DEVID_EXT.1	Secure Device Identifiers	Feature Dependent
FCS_EAPTLS_EXT.1	EAP-TLS Protocol	Feature Dependent
FCS_SNMP_EXT.1	SNMP Protocol	Feature Dependent
FMT_SNMP_EXT.1	SNMP Management	Feature Dependent

Appendix G - Acronyms

Table 9: Acronyms

Acronym	Meaning
Base-PP	Base Protection Profile
CA	Connectivity Association
CAK	Connectivity Association Key
CC	Common Criteria
CEM	Common Evaluation Methodology
CKN	Connectivity Association Key Name
CMAC	Cipher-based Message Authentication Code
cPP	Collaborative Protection Profile
DevID	Device Identifier
EA	Evaluation Activity
EAP	Extensible Authentication Protocol
EAP-TLS	EAP Transport Layer Security
EAPOL	Extensible Authentication Protocol over LAN
EPL	Ethernet Private Line
EVPL	Ethernet Virtual Private Line
ICK	Integrity Check Value Key
ICV	Integrity Check Value
IEEE	Institute of Electrical and Electronics Engineers
IV	Initialization Vector
KaY	Key Agreement Entity
KDF	Key Derivation Function
KW	Key Wrap
LAN	Local Area Network
MAC	Media Access Control
MACsec	Media Access Control Security

MEF	Metro Ethernet Forum
MIB	Management Information Base
MKA	MACsec Key Agreement
MKPDU	MACsec Key Agreement Protocol Data Unit
MPDU	MACsec Protocol Data Unit
NDcPP	collaborative Protection Profile for Network Devices
OE	Operational Environment
P2P	Point-to-Point
PAE	Port Access Entity
PN	Packet Number
POST	Power On Self Test
PP	Protection Profile
PP-Configuration	Protection Profile Configuration
PP-Module	Protection Profile Module
PSK	Pre-Shared Key
RFC	Request for Comment
SA	Secure Association
SAK	Secure Association Key
SAR	Security Assurance Requirement
SC	Secure Channel
SCI	Secure Channel Identifier
SFR	Security Functional Requirement
SNMP	Simple Network Management Protocol
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
TSS	TOE Summary Specification
UNI	User Network Interface
VLAN	Virtual Local Area Network
XPN	Extended Packet Numbering

Appendix H - Bibliography

Table 10: Bibliography

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation - • Part 1: Introduction and general model, CCMB-2022-11-001, CC:2022, Revision 1, November 2022. • Part 2: Security functional requirements, CCMB-2022-11-002, CC:2022, Revision 1, November 2022. • Part 3: Security assurance requirements, CCMB-2022-11-003, CC:2022, Revision 1, November 2022. • Part 4: Framework for the specification of evaluation methods and activities, CCMB-2022-11-004, CC:2022, Revision 1, November 2022. • Part 5: Pre-defined packages of security requirements, CCMB-2022-11-005, CC:2022, Revision 1, November 2022.
[CEM]	Common Methodology for Information Technology Security Evaluation - • Evaluation methodology, CCMB-2022-11-006, CC:2022, Revision 1, November 2022.
[802.1AE]	IEEE 802.1AE-2018, IEEE Standard for Local and metropolitan area networks-Media Access Control (MAC) Security
[NDcPP]	collaborative Protection Profile for Network Devices, Version 4.0, December 22, 2025