Comment: Comment-1-

PP-Module for MACsec Ethernet Encryptions

Version: 1.0
2022-12-16
National Information Assurance Partnership

Revision History

Version	Date	Comment
1.0	2022-12-16	Initial Release

Contents

1.0 National Information Assurance Partnership 2022-12-16 MACsec Ethernet Encryption 1.0 2022-12-16 Initial Release

1 Introduction

1.1 Overview

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

- collaborative Protection Profile for Network Devices, Version 2.2e (NDcPP)

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.

A 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.
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	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	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 Security Entity	An entity (e.g. computer) that is implementing MACsec.
MACsec Key Agreement (MKA)	A key agreement protocol used for distribution of MACsec keys to distributed peers.
MACsec protocol Data Unit (MPDU)	The basic MACsec frame structure that contains protcol and payload data.
Media Access Control Security (MACsec)	A standard for connectionless data confidentiality and integrity protection at the data link layer of a network connection. Formally defined in IEEE 802.1AE.
Metro Ethernet Forum (MEF)	A non-profit international industry consortium.
Packet Number (PN)	A monotonically increasing value that is guranteed to be unique for each MACsec frame transmitted using a given Secure Association Key (SAK)

SecTag	MAC Security Tag - a protocol header comprising a number of octets, beginning with an EtherType, that is prepended to the service data unit supplied by the client of the protocol and is used to provide security guarantees.
Secure Association (SA)	A mechanism that uses a Secure Assocation Key (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/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.

1.4 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.

1.5 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 Connectivity Association Key (CAK) and utilize the MACsec Key Agreement (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 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 cipher suite used to set up a transmit (Tx) Secure Association (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 Metro Ethernet Forum (MEF) specifications. One recent MEF specification is the "E-Line" (*) service type which is based on the use of point to point Ethernet Virtual Circuits (EVCs). A port based service is known as an Ethernet Private Line and a VLAN based service is known as an Ethernet Virtual Private Line (EVPL). EPL provides a point-to-point Ethernet virtual connection (EVC) between a pair of dedicated user–network interfaces (UNIs), with a high degree of transparency. EVPL provides a point-to-point 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

2 Conformance Claims

Conformance Statement

This PP-Module inherits exact conformance as required from the specified Base-PP and as defined in the CC and CEM addenda for Exact Conformance, Selection-Based SFRs, and Optional SFRs (dated May 2017).

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

- PP-Module for Stateful Traffic Filter Firewalls Version 1.4 + Errata 20200625 (MOD_FW)
- PP-Module for Virtual Private Network (VPN) Gateways Version 1.2 (MOD_VPNGW) This previously said 1.1 but that has been sunset

CC Conformance Claims

This PP-Module is conformant to Parts 2 (extended) and 3 (conformant) of Common Criteria Version 3.1, Release 5 [CC].

Package Claims

This PP-Module does not claim conformance to any packages.

3 Security Problem Description

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.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

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. This document does not define any additional assumptions.

3.3 Organizational Security Policies

An organization deploying the TOE is expected to satisfy the organizational security policy listed below in addition to all organizational security policies defined by the claimed Base-PP.

This document does not define any additional OSPs.

4 Security Objectives

4.1 Security Objectives for the TOE

O.AUTHENTICATION_MACSEC

To further address the issues associated with unauthorized disclosure of information, a compliant TOE's authentication ability (MKA) will allow a MACsec peer to establish connectivity associations (CA) with another MACsec peer. MACsec endpoints authenticate each other to ensure they are communicating with an authorized MAC Security Entity (SecY) entity.

Addressed by: FCS_MACSEC_EXT.4, FCS_MKA_EXT.1, FIA_PSK_EXT.1, FCS_DEVID_EXT.1 (selection-based), FCS_EAP-TLS_EXT.1 (selection-based)

O.AUTHORIZED_ADMINISTRATION

All network devices are expected to provide services that allow the security functionality of the device to be managed. The MACsec device, as a specific type of network device, has a refined set of management functions to address its specialized behavior. In order to further mitigate the threat of a compromise of its security functionality, the MACsec device prescribes the ability to limit brute-force authentication attempts by enforcing lockout of accounts that experience excessive failures and by limiting access to security-relevant data that administrators do not need to view.

Addressed by: FMT_SMF.1/MACSEC, FPT_CAK_EXT.1, FIA_AFL_EXT.1 (optional), FTP_TRP.1/MACSEC (optional), FMT_SNMP_EXT.1 (selection-based)

O.CRYPTOGRAPHIC_FUNCTIONS_MACSEC

To address the issues associated with unauthorized modification and disclosure of information, compliant TOEs will implement cryptographic capabilities. These capabilities are intended to maintain confidentiality and allow for detection and modification of data that is transmitted outside of the TOE.

Addressed by: FCS_COP.1/CMAC, FCS_COP.1/MACSEC, FCS_MACSEC_EXT.2, FCS_MACSEC_EXT.3, FTP_ITC.1/MACSEC, FTP_TRP.1/MACSEC (optional), FCS_SNMP_EXT.1 (selection-based)

O.PORT_FILTERING_MACSEC

To further address the issues associated with unauthorized network access, a compliant TOE's port filtering capability will restrict the flow of network traffic through the TOE based on layer 2 frame characteristics and whether or not the traffic represents valid MACsec frames and MACsec Key Agreement Protocol Data Units (MKPDUs).

Addressed by: FCS_MACSEC_EXT.1, FIA_PSK_EXT.1, FPT_DDP_EXT.1

O.REPLAY_DETECTION

A MACsec device is expected to help mitigate the threat of MACsec data integrity violations by providing a mechanism to detect and discard replayed traffic for MACsec protocol data units (MPDUs).

Addressed by: FPT_RPL.1, FPT_RPL_EXT.1 (optional)

O.SYSTEM_MONITORING_MACSEC

To address the issues of administrators being able to monitor the operations of the MACsec device, compliant TOEs will implement the ability to log the flow of Ethernet traffic. Specifically, the TOE will provide the means for administrators to configure rules to 'log' when Ethernet traffic grants or restricts access. As a result, the 'log' will result in informative event logs whenever a match occurs. In addition, the establishment of security CAs is auditable, not only between MACsec devices, but also with MAC Security Key Agreement Entities (KaYs).

Addressed by: FAU_GEN.1/MACSEC

O.TSF_INTEGRITY

To mitigate the security risk that the MACsec device may fail during startup, it is required to fail-secure in the event that any self-test failures occur during startup. This ensures that the device will only operate when it is in a known state.

Addressed by: FPT_FLS.1

4.2 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.

4.3 Security Objectives Rationale

This section describes how the assumptions, threats, and organizational security policies map to the security objectives.

Table 1: Security Objectives Rationale

Threat, Assumption, or OSP	Security Objectives	Rationale
T.DATA_INTEGRITY	O.CRYPTOGRAPHIC_FUNCTIONS_MACSEC	The TOE mitigates the threat of data integrity violations by implementing cryptographic functionality that includes integrity protection.
	O.REPLAY_DETECTION	The TOE mitigates the threat of data integrity violations by providing a mechanism to detect and discard replayed traffic for MPDUs.
T.NETWORK_ACCESS	O.PORT_FILTERING_MACSEC	The TOE's port filtering capability reduces the threat of unauthorized access to devices in the TOE's operational environment by restricting the flow of network traffic entering through the TOE interfaces based on layer 2 frame characteristics and whether or not the traffic represents valid MACsec frames and MKPDUs.
T.UNTRUSTED_MACSEC_COMMUNICATION_CHANNELS	O.CRYPTOGRAPHIC_FUNCTIONS_MACSEC	The TOE mitigates the threat of unauthorized disclosure of information via untrusted thru traffic by providing MKA authentication functions to authorize endpoints.

5 Security Requirements

https://www.niap-ccevs.org/profile/Info.cfm?PPID=447&id=447 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. The threats defined by this PP-Module (see section 3.1) supplement those defined in the NDcPP as follows: 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. The threat of data integrity compromise at the layer 2 level is a specific threat that can be countered by MACsec technology. 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. 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. The Base-PP does not define any TOE objectives so PP-Module objectives do not conflict with it. The Base-PP does not define any TOE objectives so PP-Module objectives do not conflict with it. The Base-PP does not define any TOE objectives so PP-Module objectives do not conflict with it. The Base-PP does not define any TOE objectives so PP-Module objectives do not conflict with it. The Base-PP does not define any TOE objectives so PP-Module objectives do not conflict with it. The Base-PP does not define any TOE objectives so PP-Module objectives do not conflict with it. The Base-PP does not define any TOE objectives so PP-Module objectives do not conflict with it.

5.0.1 Security Audit (FAU)

FAU_GEN.1/MACsec Audit Data Generation (MACsec)

FAU_GEN.1.1/MACsec

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

a. Start-up and shutdown of the audit functions;
b. All auditable events for the [*not specified*] level of audit;
c. **All administrative actions;**
d. **[*Specifically defined auditable events listed in the Auditable Events table (Table 2)*]**

Requirement	Auditable Events	Additional Audit Record Contents
FCS_MACSEC_EXT.1	Session establishment	Secure Channel Identifier (SCI)
FCS_MACSEC_EXT.3	Creation and update of Secure Association Key	Creation and update times
FCS_MACSEC_EXT.4	Creation of Connectivity Association	Connectivity Association Key Names
FPT_RPL.1	Detected replay attempt	None

Table 2: Auditable Events

FAU_GEN.1.2/MACsec

The TSF shall record within each audit record 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; and
b. For each audit event type, based on the auditable event definitions of the functional components included in the PP-**Module**/ST, [*information specified in column three of the Auditable Events table (Table 2)*].

5.0.2 Cryptographic Support (FCS)

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

FCS_COP.1.1/CMAC

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

Application Note #1: AES-CMAC is a keyed hash function that is used as part of the key derivation function (KDF) that is used for key generation.

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

FCS_COP.1.1/MACSEC

The TSF shall perform [*encryption/decryption*] in accordance with a specified cryptographic algorithm [*AES used in AES Key Wrap, GCM*] and cryptographic key sizes **[selection: *128, 256*] bits** that meets the following: [*AES as specified in ISO 18033-3, AES Key Wrap as specified in NIST SP 800-38F, GCM as specified in ISO 19772*].

FCS_MACSEC_EXT.1 MACsec

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 a MACsec Protocol Data Unit (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 (PAE EtherType 88-8E), MACsec frames (EtherType 88-E5), control frames (EtherType 88-08) and [**assignment**: *specific VLAN tag frames*] and discard others.

Application Note #2: Depending on the Carrier Ethernet service provider a TOE might need basic VLAN tag handling abilities such as a simple add or discard to be suitable for Use Case 2.

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 Secure Association Key (SAK).

Application Note #3: The length of the ICV is dependent on the cipher suite 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 CAK using a KDF.

FCS_MACSEC_EXT.3 MACsec Randomness

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 nonce for the derivation of SAKs using the TOE's random bit generator as specified by FCS_RBG_EXT.1.

Application Note #4: FCS_RBG_EXT.1 is defined in the Base-PP so a conformant MACsec TOE will include this dependency.

FCS_MACSEC_EXT.4 MACsec Key Usage

FCS_MACSEC_EXT.4.1

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

Application Note #5: The definition of the peer's CAK as defined by IEEE 802.1X-2010 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 defined in 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 #6: 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 Secure Association Key (SAK)s that are defined by the key derivation function using the CAK as input data (per IEEE 802.1X-2010, Section 9.8.1).

FCS_MACSEC_EXT.4.5

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

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-2010 and 802.1Xbx-2014.

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 #7: The ICV has length 128 bits and is computed according to Section 9.4.1 of IEEE 802.1X-2010. The ICV protects the destination and source MAC address parameters, as well as all the fields of the MAC Service Data Unit (MSDU) 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 MKA Bounded Hello Timeout limit of 0.5 seconds.

Application Note #8: The Key Server may also distribute a group CAK established by pairwise CAKs.

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*
- *pairwise CAKs, derived from MKA*
- *pairwise CAKs that are pre-shared keys*

].

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-2010 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-2010 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-2010 Section 9.4.1 shall be decoded as specified in IEEE 802.1X-2010 Section 11.11.4.

5.0.3 Identification and Authentication (FIA)

FIA_SIPT_EXT.1 Session Initiation Protocol Trunking

FIA_SIPT_EXT.1.1

The TSF shall use pre-shared keys for MKA as defined by IEEE 802.1X-2010, [**selection**: *no other protocols*, *[**assignment**: other protocols that use pre-shared keys]*].

Application Note #9: If other protocols can use pre-shared keys, they should be listed in the assignment as well; otherwise “no other protocols” should be chosen.

FIA_SIPT_EXT.1.2

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

Application Note #10: The ST author specifies whether the TSF merely accepts bit-based pre-shared keys 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.

5.0.4 Security Management (FMT)

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 ieee8021XKeyCreateNewGroup, [**assignment**: other management function]]*
- *Manage generation of a PSK-based CAK*
- *No other MACsec management functions*

]].

Application Note #11: IEEE 802.1X-2010 specifies 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.

5.0.5 Protection of the TSF (FPT)

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 #12: 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.

FPT_FLS.1 Failure with Preservation of Secure State

FPT_FLS.1.1

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 #13: 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 (shutdown) when any of the identified failures occur. For a TOE with redundant failover capability (that continues to operate if 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 be shut down. For conformance with other PP-Modules it might be a requirement for the fail-secure state to be “shut down”.

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 #14: As per IEEE 802.1AE-2018, replay is detected by examining the Packet Number (PN) value that is embedded in the Security Tag (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.

5.0.6 Trusted Path/Channels (FTP)

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*].

5.0.7 Identification and Authentication (FIA)

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

5.0.8 Protection of the TSF (FPT)

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 2 seconds.

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

Application Note #16: XPN support is expected for devices that are capable of 40Gbps 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.

5.0.9 Trusted Path/Channels (FTP)

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 #17: 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.

5.0.10 Cryptographic Support (FCS)

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/disable DevID credential
2. Enable/disable DevID key

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) (RFC 3748) and EAP-Transport Layer Security (EAP-TLS) (RFC 5216).

FCS_EAPTLS_EXT.1.2

The TSF shall implement [**selection**: *TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)*] supporting the following ciphersuites: [**selection**:

- *TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268*
- *TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268*
- *TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268*
- *TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268*
- *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492*
- *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492*
- *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492*
- *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492*
- *TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246*
- *TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246*
- *TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246*
- *TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246*
- *TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288*
- *TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288*
- *TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288*
- *TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288*
- *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289*

].

Application Note #18: The ciphersuites are chosen by the ST author to suit the TLS version(s) selected. If this SFR is selected, the FCS_TLSC_EXT and/or FCS_TLSS_EXT SFRs from the Base-PP must be included.

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 implement support SNMP using TLS in accordance with RFC 6353 supporting the following ciphersuites: [**selection**:

- *TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268*
- *TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268*
- *TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268*
- *TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268*
- *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492*
- *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492*
- *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492*
- *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492*
- *TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246*
- *TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246*
- *TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246*
- *TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246*
- *TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288*
- *TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288*
- *TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288*
- *TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288*
- *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289*

].

Application Note #19: The cipher suites are chosen by the ST writer to suit the versions of TLS and DTLS compatible with SNMP referenced RFCs (and updates) and (D)TLS versions specified in NDcPP v2.2e. This allows TLS 1.1, TLS 1.2, DTLS 1.0, and DTLS 1.2. This may be a different set of (D)TLS versions compared to those allowed for other purposes. If this SFR is selected, the appropriate FCS_(D)TLSC_EXT and FCS_(D)TLSS_EXT SFRs from the Base-PP must be included. For SNMP to support both polling and notification (trap or inform) modes, the managed device agent must support both (D)TLS server and client functions.

5.0.11 Security Management (FMT)

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*].

Application Note #20: FIA_PMG_EXT.1 is defined in the Base-PP so a conformant MACsec TOE will include this dependency.

Appendix A - 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, 8.2 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 3: 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_UAU_EXT.2, which defines authentication mechanisms specific to network devices.

Appendix B - 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/CMAC	Cryptographic Operation (AES-CMAC Keyed Hash Algorithm)	Feature Dependent
FCS_COP.1/MACSEC	Cryptographic Operation (MACsec AES Data Encryption/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	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 C - Entropy Documentation and Assessment

The TOE does not require any additional supplementary information to describe its entropy source(s) 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.
[CC] Common Criteria for Information Technology Security Evaluation -

- Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017.
- Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017.
- Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017.

[NDcPP] collaborative Protection Profile for Network Devices, Version 2.2e, March 23, 2020 [NDcPP SD] Supporting Document - Evaluation Activities for Network Device cPP, Version 2.2, December 2019 [MOD_FW] PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625, June 25, 2020 [MOD_VPNGW] PP-Module for VPN Gateways, Version 1.2, March 31, 2022