HPE Aruba Networking 6300M and 8360v2 Switch Series MACsec Security Target

Version 1.2
May 28, 2024

Prepared For and Updated By:

HPE Aruba Networking

8000 Foothills Blvd.
Roseville, CA 95747

Prepared By:

www.gossamersec.com

LIST OF TABLES

1 Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is HPE Aruba Networking 6300M and 8360v2 Switch Series MACsec provided by HPE Aruba Networking. The TOE is being evaluated as a MACsec network device.

The Security Target contains the following additional sections:

- Conformance Claims (Section 2)
- Security Objectives (Section 3)
- Extended Components Definition (Section 4)
- Security Requirements (Section 5)
- TOE Summary Specification (Section 6)

Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a parenthetical number placed at the end of the component. For example FDP_ACC.1(1) and FDP_ACC.1(2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.1 Security Target Reference

ST Title – HPE Aruba Networking 6300M and 8360v2 Switch Series MACsec Security Target

ST Version – Version 1.2

ST Date – May 28, 2024

1.2 TOE Reference

TOE Identification – HPE Aruba Networking 6300M and 8360v2 Switch Series MACsec running ArubaOS-CX version 10.13

TOE Developer – Aruba, a Hewlett Packard Enterprise Company

Evaluation Sponsor – Aruba, a Hewlett Packard Enterprise Company

1.3 TOE Overview

The Target of Evaluation (TOE) is HPE Aruba Networking 6300M and 8360v2 Switch Series MACsec running Aruba OS-CX version 10.13.

The TOE offers comprehensive Layer 2 and Layer 3 features. The HPE Aruba Networking 6300M and 8360v2 Switch Series provides security and scalability for enterprise edge deployments.

1.4 TOE Description

The TOE is a family of switches designed to support scalability, security and high performance for campus networks.

For the purpose of evaluation, the TOE will be treated as a network device offering CAVP tested cryptographic functions, security auditing, secure administration, trusted updates, self-tests, and secure connections to other servers (e.g., to transmit audit records). The scope of the evaluation is limited to the NDcPP22e and MACSEC10 requirements. Functions outside the scope of the NDcPP22e and MACSEC10 were not evaluated.

1.4.1 TOE Architecture

Table 1-1 identifies the models included in the evaluation. The underlying architecture of each TOE appliance consists of hardware that supports physical network connections, memory, processor and software that implements switching functions, configuration information and drivers. While hardware varies between different appliance models, the software code is shared across all platforms. It is in the software code that all the security functions claimed this security target are enforced. **Table 1-1** identifies the processor associated with each series.

Series Identifier	Processor	Embedded MACsec Hardware
Aruba 6300M	NXP 1046A – ARM Cortex A72	BCM 82399 BCM 54998SM BCM 82756 BCM 82759
Aruba 8360v2	NXP 1046A – ARM Cortex A72	BCM 82399 BCM 82398

Table 1-1 TOE Models and Processors

1.4.1.1 Physical Boundaries

Each TOE appliance runs the 10.13 version of the ArubaOS-CX software and has physical network connections to its environment to facilitate the switching of network traffic. The TOE appliance can also be the destination of network traffic, where it provides interfaces for its own management.

The TOE may be accessed and managed through a PC or terminal in the environment which can be remote from or directly connected to the TOE.

The TOE can be configured to forward its audit records to an external SYSLOG server in the network environment. **Figure 1** shows the TOE depicted in its intended environment.

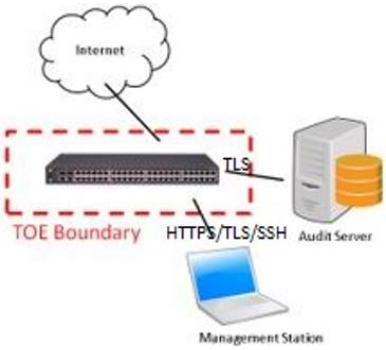

Figure 1: TOE Environment

1.4.1.2 Logical Boundaries

This section summarizes the security functions provided by the TOE:

- Security audit
- Cryptographic support
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

1.4.1.2.1 Security audit

The TOE is able to generate logs for a wide range of security relevant events. The TOE can be configured to store the logs locally so they can be accessed by an administrator and also to send the logs to a designated log server using TLS to protect the logs while in transit on the network.

1.4.1.2.2 Cryptographic support

The TOE provides CAVP certified cryptography in support of its SSHv2, TLS v1.2 and MACsec protocol implementations. Cryptographic services include key management, random bit generation, encryption/decryption, digital signature and secure hashing.

1.4.1.2.3 Identification and authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE, with the exception of reading the login banner. It provides the ability to both assign attributes (user names, passwords and roles) and to authenticate users against these attributes.

1.4.1.2.4 Security management

The TOE provides Command Line Interface (CLI) commands at the console and over SSH, as well as an HTTP over TLS (HTTPS/TLS) Graphical User Interface (GUI) to access the wide range of security management functions to manage its security policies. The TOE also offers HTTPS/TLS protection for REST API interfaces that can be used for administration. All administrative activity and functions including security management commands are limited to authorized users (i.e., administrators) only after they have provided acceptable user identification and authentication data to the TOE. The security management functions are controlled through the use of roles that can be assigned to TOE users. The TOE supports the following roles: Administrators, Operators. The Administrator role can make changes to the TOE configuration while the Operator role is a read-only role.

1.4.1.2.5 Protection of the TSF

The TOE implements a number of measures to protect the integrity of its security features. The TOE protects stored passwords and cryptographic keys so they are not directly accessible in plaintext. The TOE also ensures that reliable time information is available for both log accountability and synchronization with the operating environment by providing a hardware clock and the ability to synchronize with the network time server. The TOE employs both dedicated communication channels as well as cryptographic means to protect communication between itself and other components in the operating environment. The TOE performs self-tests to detect failure and protect itself from malicious updates.

1.4.1.2.6 TOE access

The TOE can be configured to display a logon banner before and after (a post-login banner) a user session is established. The TOE also enforces inactivity timeouts for local and remote sessions.

1.4.1.2.7 Trusted path/channels

The TOE protects communication channels between itself and remote administrators using HTTPS/TLS and SSH. The SSH protocol is used to protect administrative connections utilizing the TOE's command line interface (CLI). Additionally, web-based GUI and REST API interfaces are available for remote administration which are protected using HTTPS/TLS.

The TOE protects communication with network peers, such as a log server, using TLS connections to prevent unintended disclosure or modification of logs. The TOE supports MACsec communication with MACsec peers.

1.4.2 TOE Documentation

Aruba offers a series of documents that describe the installation of the HPE Aruba Networking 6300M and 8360v2 Switch Series MACsec as well as guidance for subsequent use and administration of the applicable security features. The following document was examined as part of the evaluation:

- Common Criteria Administrator Guide: Target of Evaluation: Aruba 6300M and 8360v2 Switch Series, version 2.6 **[CC-Guide]**

2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 5, April 2017.
    - Part 3 Conformant
- Package Claims:
    - PP-Configuration for Network Devices and MACsec Ethernet Encryption, version 1.0, 2023-03-29
        - Base PP: collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e)
        - PP Module: PP-Module for MACsec Ethernet Encryption, Version 1.0, 02 March 2023 (MACSEC10)

Package	**Technical Decision**	**Applied**	**Notes**
NDcPP22e	TD0800 –Updated NIT Technical Decision for IPsec IKE/SA Lifetimes Tolerance	No	Requirement not claimed
NDcPP22e	TD0792 – NIT Technical Decision: FIA_PMG_EXT.1 – TSS EA not in line with SFR	Yes	
NDcPP22e	TD0790 – NIT Technical Decision: Clarification Required for testing IPv6	Yes	
NDcPP22e	TD0738 – NIT Technical Decision for Link to Allowed-With list	Yes	
NDcPP22e	TD0670 - NIT Technical Decision for Mutual and Non-Mutual Auth TLSC Testing	Yes	
NDcPP22e	TD0639 - NIT Technical Decision for Clarification for NTP MAC Keys	No	Requirement not claimed
NDcPP22e	TD0638 - NIT Technical Decision for Key Pair Generation for Authentication	Yes	
NDcPP22e	TD0636 - NIT Technical Decision for Clarification of Public Key User Authentication for SSH	No	Requirement not claimed
NDcPP22e	TD0635 - NIT Technical Decision for TLS Server and Key Agreement Parameters	Yes	
NDcPP22e	TD0632 - NIT Technical Decision for Consistency with Time Data for vNDs	Yes	
NDcPP22e	TD0631 - NIT Technical Decision for Clarification of public key authentication for SSH Server	Yes	
NDcPP22e	TD0592 - NIT Technical Decision for Local Storage of Audit Records	Yes	
NDcPP22e	TD0591 - NIT Technical Decision for Virtual TOEs and hypervisors	Yes	
NDcPP22e	TD0581 - NIT Technical Decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3	Yes	
NDcPP22e	TD0580 - NIT Technical Decision for clarification about use of DH14 in NDcPPv2.2e	Yes	
NDcPP22e	TD0572 - NiT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers	Yes	

NDcPP22e	TD0571 - NiT Technical Decision for Guidance on how to handle FIA_AFL.1	Yes	
NDcPP22e	TD0570 - NiT Technical Decision for Clarification about FIA_AFL.1	Yes	
NDcPP22e	TD0569 - NIT Technical Decision for Session ID Usage Conflict in FCS_DTLSS_EXT.1.7	Yes	
NDcPP22e	TD0564 - NiT Technical Decision for Vulnerability Analysis Search Criteria	Yes	
NDcPP22e	TD0563 - NiT Technical Decision for Clarification of audit date information	Yes	
NDcPP22e	TD0556 - NIT Technical Decision for RFC 5077 question	Yes	
NDcPP22e	TD0555 - NIT Technical Decision for RFC Reference incorrect in TLSS Test	Yes	
NDcPP22e	TD0547 - NIT Technical Decision for Clarification on developer disclosure of AVA_VAN	Yes	
NDcPP22e	TD0546 - NIT Technical Decision for DTLS - clarification of Application Note 63	No	Requirement not claimed
NDcPP22e	TD0537 - NIT Technical Decision for Incorrect reference to FCS_TLSC_EXT.2.3	Yes	
NDcPP22e	TD0536 - NIT Technical Decision for Update Verification Inconsistency	Yes	
NDcPP22e	TD0528 - NIT Technical Decision for Missing EAs for FCS_NTP_EXT.1.4	No	Requirement not claimed
NDcPP22e	TD0527 - Updates to Certificate Revocation Testing (FIA_X509_EXT.1)	Yes	
MACSEC10	TD0728 – Corrections to MACSec PP-Module SD	Yes	
MACSEC10	TD0746 – Correction to FPT_RPL.1 Test 25	Yes	
MACSEC10	TD0748 – Correction to FMT_SMF.1/MACSEC Test 21	Yes	
MACSEC10	TD0787: MACsec Key Agreement and conditional support for group CAK - MACSEC MOD	Yes	
MACSEC10	TD0805: MACsec Data Delay Protection	Yes	

2.1 Conformance Rationale

The ST conforms to the NDcPP22e/MACSEC10. As explained previously, the security problem definition, security objectives, and security requirements have been drawn from the PP.

3 Security Objectives

The Security Problem Definition may be found in the NDcPP22e/MACSEC10 and this section reproduces only the corresponding Security Objectives for operational environment for reader convenience. The NDcPP22e/MACSEC10 offers additional information about the identified security objectives, but that has not been reproduced here and the NDcPP22e/MACSEC10 should be consulted if there is interest in that material.

In general, the NDcPP22e/MACSEC10 has defined Security Objectives appropriate for a network device and as such are applicable to the HPE Aruba Networking 6300M and 8360v2 Switch Series MACsec TOE.

3.1 Security Objectives for the Operational Environment

OE.ADMIN_CREDENTIALS_SECURE The administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.

OE.COMPONENTS_RUNNING (applies to distributed TOEs only)
For distributed TOEs, the Security Administrator ensures that the availability of every TOE component is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. The Security Administrator also ensures that it is checked as appropriate for every TOE component that the audit functionality is running properly.

OE.NO_GENERAL_PURPOSE There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE. Note: For vNDs the TOE includes only the contents of the its own VM, and does not include other VMs or the VS.

OE.NO_THRU_TRAFFIC_PROTECTION The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.

OE.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

OE.RESIDUAL_INFORMATION The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.

OE.TRUSTED_ADMIN TOE Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For vNDs, this includes the VS Administrator responsible for configuring the VMs that implement ND functionality.
For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.

OE.UPDATES The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

OE.VM_CONFIGURATION (applies to vNDs only)
For vNDs, the Security Administrator ensures that the VS and VMs are configured to

- reduce the attack surface of VMs as much as possible while supporting ND functionality (e.g., remove unnecessary virtual hardware, turn off unused inter-VM communications mechanisms), and
- correctly implement ND functionality (e.g., ensure virtual networking is properly configured to support network traffic, management channels, and audit reporting).

The VS should be operated in a manner that reduces the likelihood that vND operations are adversely affected by virtualisation features such as cloning, save/restore, suspend/resume, and live migration.

If possible, the VS should be configured to make use of features that leverage the VS's privileged position to provide additional security functionality. Such features could include malware detection through VM introspection, measured VM boot, or VM snapshot for forensic analysis.

4 Extended Components Definition

All of the extended requirements in this ST have been drawn from the NDcPP22e/MACSEC10. The NDcPP22e/MACSEC10 defines the following extended requirements and since they are not redefined in this ST the NDcPP22e/MACSEC10 should be consulted for more information in regard to those CC extensions.

Extended SFRs:

- NDcPP22e:FAU_STG_EXT.1: Protected Audit Event Storage
- NDcPP22e:FCS_HTTPS_EXT.1: HTTPS Protocol
- MACSEC10:FCS_MACSEC_EXT.1: MACsec
- MACSEC10:FCS_MACSEC_EXT.2: MACsec Integrity and Confidentiality
- MACSEC10:FCS_MACSEC_EXT.3: MACsec Randomness
- MACSEC10:FCS_MACSEC_EXT.4: MACsec Key Usage
- MACSEC10:FCS_MKA_EXT.1: MACsec Key Agreement
- NDcPP22e:FCS_RBG_EXT.1: Random Bit Generation
- NDcPP22e:FCS_SSHS_EXT.1: SSH Server Protocol - per TD0631
- NDcPP22e:FCS_TLSC_EXT.1: TLS Client Protocol Without Mutual Authentication - per TD0670
- NDcPP22e:FCS_TLSS_EXT.1: TLS Server Protocol Without Mutual Authentication - per TD0635
- NDcPP22e:FIA_PMG_EXT.1: Password Management
- MACSEC10:FIA_PSK_EXT.1: Extended: Pre-Shared Key Composition
- NDcPP22e:FIA_UAU_EXT.2: Password-based Authentication Mechanism
- NDcPP22e:FIA_UIA_EXT.1: User Identification and Authentication
- NDcPP22e:FIA_X509_EXT.1/Rev: X.509 Certificate Validation
- NDcPP22e:FIA_X509_EXT.2: X.509 Certificate Authentication
- NDcPP22e:FIA_X509_EXT.3: X.509 Certificate Requests
- NDcPP22e:FPT_APW_EXT.1: Protection of Administrator Passwords
- MACSEC10:FPT_CAK_EXT.1: Protection of CAK Data
- NDcPP22e:FPT_SKP_EXT.1: Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
- NDcPP22e:FPT_STM_EXT.1: Reliable Time Stamps - per TD0632
- NDcPP22e:FPT_TST_EXT.1: TSF testing
- NDcPP22e:FPT_TUD_EXT.1: Trusted update
- NDcPP22e:FTA_SSL_EXT.1: TSF-initiated Session Locking

5 Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

The SFRs have all been drawn from the NDcPP22e/MACSEC10. The refinements and operations already performed in the NDcPP22e/MACSEC10 are not identified (e.g., highlighted) here, rather the requirements have been copied from the NDcPP22e/MACSEC10 and any residual operations have been completed herein. Of particular note, the NDcPP22e/MACSEC10 made a number of refinements and completed some of the SFR operations defined in the Common Criteria (CC) and that PP should be consulted to identify those changes if necessary.

The SARs are also drawn from the NDcPP22e/MACSEC10. The NDcPP22e/MACSEC10 should be consulted for the assurance activity definitions.

5.1 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by the HPE Aruba Networking 6300M and 8360v2 Switch Series MACsec TOE.

Requirement Class	Requirement Component
FAU: Security audit	NDcPP22e/MACSEC10:FAU_GEN.1: Audit Data Generation
	NDcPP22e:FAU_GEN.2: User identity association
	NDcPP22e:FAU_STG_EXT.1: Protected Audit Event Storage
FCS: Cryptographic support	NDcPP22e:FCS_CKM.1: Cryptographic Key Generation
	NDcPP22e:FCS_CKM.2: Cryptographic Key Establishment
	NDcPP22e:FCS_CKM.4: Cryptographic Key Destruction
	NDcPP22e:FCS_COP.1/DataEncryption: Cryptographic Operation (AES Data Encryption/Decryption)
	MACSEC10:FCS_COP.1/MACSEC: Cryptographic Operation (MACsec AES Data Encryption and Decryption))
	NDcPP22e:FCS_COP.1/Hash: Cryptographic Operation (Hash Algorithm)
	NDcPP22e:FCS_COP.1/KeyedHash: Cryptographic Operation (Keyed Hash Algorithm)
	MACSEC10:FCS_COP.1/KeyedHashCMAC: Cryptographic Operation (AES-CMAC Keyed Hash Algorithm)
	NDcPP22e:FCS_COP.1/SigGen: Cryptographic Operation (Signature Generation and Verification)
	NDcPP22e:FCS_HTTPS_EXT.1: HTTPS Protocol
	MACSEC10:FCS_MACSEC_EXT.1: MACsec
	MACSEC10:FCS_MACSEC_EXT.2: MACsec Integrity and Confidentiality
	MACSEC10:FCS_MACSEC_EXT.3: MACsec Randomness
	MACSEC10:FCS_MACSEC_EXT.4: MACsec Key Usage
	MACSEC10:FCS_MKA_EXT.1: MACsec Key Agreement
	NDcPP22e:FCS_RBG_EXT.1: Random Bit Generation
	NDcPP22e:FCS_SSHS_EXT.1: SSH Server Protocol - per TD0631
	NDcPP22e:FCS_TLSC_EXT.1: TLS Client Protocol Without Mutual Authentication - per FTD0670
	NDcPP22e:FCS_TLSC_EXT.2: TLS Client Support for Mutual Authentication
	NDcPP22e:FCS_TLSS_EXT.1: TLS Server Protocol Without Mutual Authentication - per TD0635
FIA: Identification and authentication	MACSEC10:FIA_AFL_EXT.1: Authentication Attempt Limiting
	NDcPP22e:FIA_AFL.1: Authentication Failure Management
	NDcPP22e:FIA_PMG_EXT.1: Password Management
	MACSEC10:FIA_PSK_EXT.1: Pre-Shared Key Composition

	NDcPP22e:FIA_UAU.7: Protected Authentication Feedback
	NDcPP22e:FIA_UAU_EXT.2: Password-based Authentication Mechanism
	NDcPP22e:FIA_UIA_EXT.1: User Identification and Authentication
	NDcPP22e:FIA_X509_EXT.1/Rev: X.509 Certificate Validation
	NDcPP22e:FIA_X509_EXT.2: X.509 Certificate Authentication
	NDcPP22e:FIA_X509_EXT.3: X.509 Certificate Requests
FMT: Security management	NDcPP22e:FMT_MOF.1/ManualUpdate: Management of security functions behaviour
	NDcPP22e:FMT_MTD.1/CoreData: Management of TSF Data
	NDcPP22e:FMT_MTD.1/CryptoKeys: Management of TSF Data
	NDcPP22e:FMT_SMF.1: Specification of Management Functions - per TD0631
	MACSEC10: FMT_SMF.1/MACSEC Specification of Management Functions – per TD0748
	NDcPP22e:FMT_SMR.2: Restrictions on Security Roles
FPT: Protection of the TSF	NDcPP22e:FPT_APW_EXT.1: Protection of Administrator Passwords
	MACSEC10:FPT_CAK_EXT.1: Protection of CAK Data
	MACSEC10:FPT_FLS.1: Failure with Preservation of Secure State
	MACSEC10:FPT_RPL.1: Replay Detection-per TD0746
	NDcPP22e:FPT_SKP_EXT.1: Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
	NDcPP22e:FPT_STM_EXT.1: Reliable Time Stamps - per TD0632
	NDcPP22e:FPT_TST_EXT.1: TSF testing
	NDcPP22e:FPT_TUD_EXT.1: Trusted update
FTA: TOE access	NDcPP22e:FTA_SSL.3: TSF-initiated Termination
	NDcPP22e:FTA_SSL.4: User-initiated Termination
	NDcPP22e:FTA_SSL_EXT.1: TSF-initiated Session Locking
	NDcPP22e:FTA_TAB.1: Default TOE Access Banners
FTP: Trusted path/channels	MACSEC10:FTP_ITC.1/MACSEC: Inter-TSF Trusted Channel (MACsec Communications)
	NDcPP22e:FTP_ITC.1: Inter-TSF trusted channel - per TD0639
	NDcPP22e:FTP_TRP.1/Admin: Trusted Path - per TD0639

Table 5-1 TOE Security Functional Components

5.1.1 Security audit (FAU)

5.1.1.1 Audit Data Generation (NDcPP22e/MACSEC10:FAU_GEN.1)

NDcPP22e/MACSEC10:FAU_GEN.1.1

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

a) Start-up and shut-down of the audit functions;
b) All auditable events for the not specified level of audit; and
c) All administrative actions comprising:
   - Administrative login and logout (name of user account shall be logged if individual user accounts are required for administrators).
   - Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).
   - Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).
   - Resetting passwords (name of related user account shall be logged).
   - [***no other actions***];
d) Specifically defined auditable events listed in **Table 5-2**.

NDcPP22e/MACSEC10:FAU_GEN.1.2

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, 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 cPP/ST, information specified in column three of **Table 5-2**.

Requirement	Audit Event	Additional Contents
FAU_GEN.1	None	None
FAU_GEN.2	None	None
FAU_STG_EXT.1	None	None
FCS_CKM.1	None	None
FCS_CKM.2	None	None
FCS_CKM.4	None	None
MACSEC10:FCS_COP.1/CMAC	None	None
MACSEC10:FCS_COP.1/MACSEC	None	None
FCS_COP.1/DataEncryption	None	None
FCS_COP.1/Hash	None	None
FCS_COP.1/KeyedHash	None	None
FCS_COP.1/SigGen	None	None
MACSEC10:FCS_MACSEC_EXT.1	Session establishment	Secure Channel Identifier (SCI)
MACSEC10:FCS_MACSEC_EXT.2	None	None
MACSEC10:FCS_MACSEC_EXT.3	Creation and update of SAK	Creation and update times
MACSEC10:FCS_MACSEC_EXT.4	Creation of CA	Connectivity Association Key Names (CKNs)
MACSEC10:FCS_MKA_EXT.1	None	None
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	Reason for failure.
FCS_RBG_EXT.1	None	None
FCS_SSHS_EXT.1	Failure to establish an SSH session.	Reason for failure.
FCS_TLSC_EXT.1	Failure to establish a TLS Session.	Reason for failure.
FCS_TLSC_EXT.2	None	None
FCS_TLSS_EXT.1	Failure to establish a TLS Session.	Reason for failure.
FIA_AFL.1	Unsuccessful login attempt limit is met or exceeded.	Origin of the attempt (e.g., IP address).
FIA_PMG_EXT.1	None	None
MACSEC10:FIA_PSK_EXT.1	None	None
FIA_UAU.7	None	None
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate. Any addition, replacement or removal of trust anchors in the TOE's trust store	Reason for failure of certificate validation Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store
FIA_X509_EXT.2	None	None
FIA_X509_EXT.3	None	None
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update.	None

FMT_MTD.1/CoreData	None	None
FMT_MTD.1/CryptoKeys	None	None
FMT_SMF.1	All management activities of TSF data.	None
FMT_SMR.2	None	None
FPT_APW_EXT.1	None	None
MACSEC10:FPT_CAK_EXT.1	None	None
MACSEC10:FPT_FLS.1	None	None
MACSEC10:FPT_RPL.1	Detected replay attempt	None
FPT_SKP_EXT.1	None	None
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FPT_TST_EXT.1	None	None
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure).	None
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None
FTA_SSL.4	The termination of an interactive session.	None
FTA_SSL_EXT.1	(if 'lock the session' is selected) Any attempts at unlocking of an interactive session. (if 'terminate the session' is selected) The termination of a local session by the session locking mechanism.	None
FTA_TAB.1	None	None
MACSEC10:FTP_ITC.1/MACSEC	None	None
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	None

Table 5-2 Audit Events

5.1.1.2 User identity association (NDcPP22e:FAU_GEN.2)

NDcPP22e:FAU_GEN.2.1

For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.1.1.3 Protected Audit Event Storage (NDcPP22e:FAU_STG_EXT.1)

NDcPP22e:FAU_STG_EXT.1.1

The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1.

NDcPP22e:FAU_STG_EXT.1.2

The TSF shall be able to store generated audit data on the TOE itself. In addition [***the TOE shall consist of a single standalone component that stores audit data locally***].

NDcPP22e:FAU_STG_EXT.1.3

The TSF shall [***overwrite previous audit records according to the following rule: [oldest log file is cleared]***] when the local storage space for audit data is full.

5.1.2 Cryptographic support (FCS)

5.1.2.1 Cryptographic Key Generation (NDcPP22e:FCS_CKM.1)

NDcPP22e:FCS_CKM.1.1

The TSF shall generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm: [

- ***RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.3,***
- ***ECC schemes using 'NIST curves' [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.4,***
- ***FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.1,***
- ***FFC Schemes using 'safe-prime' groups that meet the following: "NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [RFC 3526]***].

5.1.2.2 Cryptographic Key Establishment (NDcPP22e:FCS_CKM.2)

NDcPP22e:FCS_CKM.2.1

The TSF shall perform cryptographic key establishment in accordance with a specified cryptographic key establishment method: [

- ***RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, 'Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1,***
- ***Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" (TD0581 applied),***
- ***Finite field-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, 'Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography',***
- ***FFC Schemes using 'safe-prime' groups that meet the following: 'NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [groups listed in RFC 3526] (TD0580 applied)***].

5.1.2.3 Cryptographic Key Destruction (NDcPP22e:FCS_CKM.4)

NDcPP22e:FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method

- For plaintext keys in volatile storage, the destruction shall be executed by a [***single overwrite consisting of [zeroes]***];
- For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that [***logically addresses the storage location of the key and performs a [single] overwrite consisting of [zeroes]***]

that meets the following: No Standard.

5.1.2.4 Cryptographic Operation (AES Data Encryption/Decryption) (NDcPP22e:FCS_COP.1/DataEncryption)

NDcPP22e:FCS_COP.1.1/DataEncryption

The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in [***CBC, CTR, GCM***] mode and cryptographic key sizes [***128 bits, 256 bits***] that meet the following: AES as specified in ISO 18033-3, [***CBC as specified in ISO 10116, CTR as specified in ISO 10116, GCM as specified in ISO 19772***].

5.1.2.5 Cryptographic Operation (MACsec AES Data Encryption/Decryption) (MACSEC10:FCS_COP.1/MACSEC)

MACSEC10: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, GCM and cryptographic key sizes [***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.

5.1.2.6 Cryptographic Operation (Hash Algorithm) (NDcPP22e:FCS_COP.1/Hash)

NDcPP22e:FCS_COP.1.1/Hash

The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm [***SHA-1, SHA-256, SHA-384, SHA-512***] and message digest sizes [***160, 256, 384, 512***] bits that meet the following: ISO/IEC 10118-3:2004.

5.1.2.7 Cryptographic Operation (Keyed Hash Algorithm) (NDcPP22e:FCS_COP.1/KeyedHash)

NDcPP22e:FCS_COP.1.1/KeyedHash

The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm [***HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512***] and cryptographic key sizes [**160, 256, 384, 512**] and message digest sizes [***160, 256, 384, 512***] bits that meet the following: ISO/IEC 9797-2:2011, Section 7 'MAC Algorithm 2'.

5.1.2.8 Cryptographic Operation (AES-CMAC Keyed Hash Algorithm) (MACSEC10:FCS_COP.1/KeyedHashCMAC)

MACSEC10:FCS_COP.1.1/KeyedHashCMAC

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

5.1.2.9 Cryptographic Operation (Signature Generation and Verification) (NDcPP22e:FCS_COP.1/SigGen)

NDcPP22e:FCS_COP.1.1/SigGen

The TSF shall perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm [

- ***RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [2048, 3072 bits],***
- ***Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [256 bits]***]

that meet the following: [

- ***For RSA schemes: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,***
- ***For ECDSA schemes: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Section 6 and Appendix D, Implementing 'NIST curves' [P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4***].

5.1.2.10 HTTPS Protocol (NDcPP22e:FCS_HTTPS_EXT.1)

NDcPP22e:FCS_HTTPS_EXT.1.1
The TSF shall implement the HTTPS protocol that complies with RFC 2818.

NDcPP22e:FCS_HTTPS_EXT.1.2
The TSF shall implement HTTPS using TLS.

NDcPP22e:FCS_HTTPS_EXT.1.3
If a peer certificate is presented, the TSF shall [***not establish the connection***] if the peer certificate is deemed invalid.

5.1.2.11 MACsec (MACSEC10:FCS_MACSEC_EXT.1)

MACSEC10:FCS_MACSEC_EXT.1.1
The TSF shall implement MACsec in accordance with IEEE Standard 802.1AE-2018.

MACSEC10: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.

MACSEC10: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.

MACSEC10:FCS_MACSEC_EXT.1.4
The TSF shall permit only EAPOL (Port Access Entity (PAE) EtherType 88-8E), MACsec frames (EtherType 88-E5), and MAC control frames (EtherType is 88-08) and shall discard others

5.1.2.12 MACsec Integrity and Confidentiality (MACSEC10:FCS_MACSEC_EXT.2)

MACSEC10:FCS_MACSEC_EXT.2.1
The TOE shall implement MACsec with support for integrity protection with a confidentiality offset of [***0, 30, 50***].

MACSEC10: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.

MACSEC10: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.

5.1.2.13 MACsec Randomness (MACSEC10:FCS_MACSEC_EXT.3)

MACSEC10:FCS_MACSEC_EXT.3.1
The TSF shall generate unique Secure Association Keys (SAKs) using [***key derivation from Connectivity Association Key (CAK) per section 9.8.1 of IEEE 802.1X-2010***] 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.

MACSEC10: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_EXT.1.

5.1.2.14 MACsec Key Usage (MACSEC10:FCS_MACSEC_EXT.4)

MACSEC10:FCS_MACSEC_EXT.4.1
The TSF shall support peer authentication using pre-shared keys (PSK) [***no other method***].

MACSEC10:FCS_MACSEC_EXT.4.2
The TSF shall distribute SAKs between MACsec peers using AES key wrap as specified in FCS_COP.1/MACSEC.

MACSEC10:FCS_MACSEC_EXT.4.3
The TSF shall support specifying a lifetime for CAKs.

MACSEC10: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 802.1X, section 9.8.1).

MACSEC10: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).

5.1.2.15 MACsec Key Agreement (MACSEC10:FCS_MKA_EXT.1)

MACSEC10:FCS_MKA_EXT.1.1
The TSF shall implement Key Agreement Protocol (MKA) in accordance with IEEE 802.1X-2010 and 802.1Xbx-2014.

MACSEC10: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).

MACSEC10: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.

MACSEC10:FCS_MKA_EXT.1.4
The TSF shall enforce an MKA Lifetime Timeout limit of 6.0 seconds and [***MKA Bounded Hello Time limit of 0.5 seconds***]. (TD0805 applied)

MACSEC10:FCS_MKA_EXT.1.5
The Key Server shall refresh a SAK when it expires. The Key Server shall distribute a SAK by [
pairwise CAKs, derived from MKA,
pairwise CAKs that are PSKs].

MACSEC10: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.

MACSEC10: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
e. 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 802.1X, section 11.11.4.

5.1.2.16 Random Bit Generation (NDcPP22e:FCS_RBG_EXT.1)

NDcPP22e:FCS_RBG_EXT.1.1
The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [***CTR_DRBG (AES)***].

NDcPP22e:FCS_RBG_EXT.1.2
The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [***[one] software-based noise source***] with a minimum of [***256 bits***] of entropy at least equal

to the greatest security strength, according to ISO/IEC 18031:2011Table C.1 'Security Strength Table for Hash Functions', of the keys and hashes that it will generate.

5.1.2.17 SSH Server Protocol - per TD0631 (NDcPP22e:FCS_SSHS_EXT.1)

NDcPP22e:FCS_SSHS_EXT.1.1
The TSF shall implement the SSH protocol that complies with: RFC(s) 4251, 4252, 4253, 4254, [***5656, 6668***].

NDcPP22e:FCS_SSHS_EXT.1.2
The TSF shall ensure that the SSH protocol implementation supports the following user authentication methods as described in RFC 4252: public key-based, [***password-based***].

NDcPP22e:FCS_SSHS_EXT.1.3
The TSF shall ensure that, as described in RFC 4253, packets greater than [**262127**] bytes in an SSH transport connection are dropped.

NDcPP22e:FCS_SSHS_EXT.1.4
The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [***aes128-cbc, aes256-cbc, aes128-ctr, aes256-ctr***].

NDcPP22e:FCS_SSHS_EXT.1.5
The TSF shall ensure that the SSH public-key based authentication implementation uses [***ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521***] as its public key algorithm(s) and rejects all other public key algorithms.

NDcPP22e:FCS_SSHS_EXT.1.6
The TSF shall ensure that the SSH transport implementation uses [***hmac-sha1, hmac-sha2-256, hmac-sha2-512***] as its MAC algorithm(s) and rejects all other MAC algorithm(s).

NDcPP22e:FCS_SSHS_EXT.1.7
The TSF shall ensure that [***diffie-hellman-group14-sha1, ecdh-sha2-nistp256***] and [***ecdh-sha2-nistp384***] are the only allowed key exchange methods used for the SSH protocol.

NDcPP22e:FCS_SSHS_EXT.1.8
The TSF shall ensure that within SSH connections, the same session keys are used for a threshold of no longer than one hour, and each encryption key is used to protect no more than one gigabyte of data. After any of the thresholds are reached, a rekey needs to be performed.

5.1.2.18 TLS Client Protocol Without Mutual Authentication - per TD0670 (NDcPP22e:FCS_TLSC_EXT.1)

NDcPP22e:FCS_TLSC_EXT.1.1
The TSF shall implement [***TLS 1.2 (RFC 5246)***] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites: [
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_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
] and no other ciphersuites.

NDcPP22e:FCS_TLSC_EXT.1.2
The TSF shall verify that the presented identifier matches [***the reference identifier per RFC 6125 section 6, IPv4 address in CN or SAN***].

NDcPP22e:FCS_TLSC_EXT.1.3
When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the server certificate is invalid. The TSF shall also [***Not implement any administrator override mechanism***].

NDcPP22e:FCS_TLSC_EXT.1.4
The TSF shall [***present the Supported Elliptic Curves/Supported Groups Extension with the following curves/groups: [secp256r1, secp384r1, secp521r1] and no other curves/groups***] in the Client Hello.

5.1.2.19 TLS Client Support for Mutual Authentication (NDcPP22e:FCS_TLSC_EXT.2)

NDcPP22e:FCS_TLSC_EXT.2.1
The TSF shall support TLS communication with mutual authentication using X.509v3 certificates.

5.1.2.20 TLS Server Protocol Without Mutual Authentication - per TD0635 (NDcPP22e:FCS_TLSS_EXT.1)

NDcPP22e:FCS_TLSS_EXT.1.1
The TSF shall implement [***TLS 1.2 (RFC 5246)***] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites: [
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
] and no other ciphersuites.

NDcPP22e:FCS_TLSS_EXT.1.2
The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and [***TLS 1.1***].

NDcPP22e:FCS_TLSS_EXT.1.3
The TSF shall perform key establishment for TLS using [***ECDHE curves [secp384r1] and no other curves***].

NDcPP22e:FCS_TLSS_EXT.1.4
The TSF shall support [***session resumption based on session IDs according to RFC 4346 (TLS1.1) or RFC 5246 (TLS1.2)***].

5.1.3 Identification and authentication (FIA)

5.1.3.1 Authentication Failure Management (NDcPP22e:FIA_AFL.1)

NDcPP22e:FIA_AFL.1.1
The TSF shall detect when an Administrator configurable positive integer within [**1-10**] unsuccessful authentication attempts occur related to Administrators attempting to authenticate remotely using a password.

NDcPP22e:FIA_AFL.1.2
When the defined number of unsuccessful authentication attempts has been met, the TSF shall [***prevent the offending Administrator from successfully establishing a remote session using any authentication method that involves a password until an Administrator defined time period has elapsed***].

5.1.3.2 Password Management (NDcPP22e:FIA_PMG_EXT.1)

NDcPP22e:FIA_PMG_EXT.1.1
The TSF shall provide the following password management capabilities for administrative passwords:

a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [
'!', '@', '#', '$', '%', '^', '&', '*', '(',
['`', '+', '-', '.', '/', ':', ';', '<', '>', '=', '?', '[', ']', '_', '"', ')', '\', '|', '~']
];

b) Minimum password length shall be configurable to between [**1**] and [**32**] characters.

5.1.3.3 Pre-Shared Key Composition (MACSEC10:FIA_PSK_EXT.1)

MACSEC10:FIA_PSK_EXT.1.1
The TSF shall use PSKs for MKA as defined by IEEE 802.1X-2010, [***no other protocols***].

MACSEC10:FIA_PSK_EXT.1.2

The TSF shall be able to [***accept***] bit-based PSKs.

5.1.3.4 Protected Authentication Feedback (NDcPP22e:FIA_UAU.7)

NDcPP22e:FIA_UAU.7.1

The TSF shall provide only obscured feedback to the administrative user while the authentication is in progress at the local console.

5.1.3.5 Password-based Authentication Mechanism (NDcPP22e:FIA_UAU_EXT.2)

NDcPP22e:FIA_UAU_EXT.2.1

The TSF shall provide a local [***password-based, SSH public key-based***] authentication mechanism to perform local administrative user authentication.

5.1.3.6 User Identification and Authentication (NDcPP22e:FIA_UIA_EXT.1)

NDcPP22e:FIA_UIA_EXT.1.1

The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;
- [***no other actions***].

NDcPP22e:FIA_UIA_EXT.1.2

The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that administrative user.

5.1.3.7 X.509 Certificate Validation (NDcPP22e:FIA_X509_EXT.1/Rev)

NDcPP22e:FIA_X509_EXT.1.1/Rev

The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certification path validation supporting a minimum path length of three certificates.
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [***the Online Certificate Status Protocol (OCSP) as specified in RFC 6960***]
- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
  - Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
  - Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
  - OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.

NDcPP22e:FIA_X509_EXT.1.2/Rev

The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

5.1.3.8 X.509 Certificate Authentication (NDcPP22e:FIA_X509_EXT.2)

NDcPP22e:FIA_X509_EXT.2.1

The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [***HTTPS, TLS***], and [***no additional uses***].

NDcPP22e:FIA_X509_EXT.2.2

When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [***not accept the certificate***].

5.1.3.9 X.509 Certificate Requests (NDcPP22e:FIA_X509_EXT.3)

NDcPP22e:FIA_X509_EXT.3.1

The TSF shall generate a Certification Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [***Common Name, Organization, Country***].

NDcPP22e:FIA_X509_EXT.3.2

The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

5.1.4 Security management (FMT)

5.1.4.1 Management of security functions behaviour (NDcPP22e:FMT_MOF.1/ManualUpdate)

NDcPP22e:FMT_MOF.1.1/ManualUpdate

The TSF shall restrict the ability to enable the functions to perform manual updates to Security Administrators.

5.1.4.2 Management of TSF Data (NDcPP22e:FMT_MTD.1/CoreData)

NDcPP22e:FMT_MTD.1.1/CoreData

The TSF shall restrict the ability to manage the TSF data to Security Administrators.

5.1.4.3 Management of TSF Data (NDcPP22e:FMT_MTD.1/CryptoKeys)

NDcPP22e:FMT_MTD.1.1/CryptoKeys

The TSF shall restrict the ability to manage the cryptographic keys to Security Administrators.

5.1.4.4 Specification of Management Functions-per TD0631 (NDcPP22e/ MACSEC10:FMT_SMF.1)

NDcPP22e:FMT_SMF.1.1

The TSF shall be capable of performing the following management functions:

- Ability to administer the TOE locally and remotely;
- Ability to configure the access banner;
- Ability to configure the session inactivity time before session termination or locking;
- Ability to update the TOE, and to verify the updates using [***digital signature***] capability prior to installing those updates;
- Ability to configure the authentication failure parameters for FIA_AFL.1;
- [***Ability to modify the behavior of the transmission of audit data to an external IT entity,***
- ***Ability to manage the cryptographic keys,***
- ***Ability to configure the cryptographic functionality,***
- ***Ability to set the time which is used for time-stamps,***
- ***Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors,***
- ***Ability to import X509v3 certificates to the TOE's trust store,***
- ***Ability to manage the trusted public keys database***].

5.1.4.5 Specification of Management Functions (MACsec) (MACSEC10:FMT_SMF.1/MACSEC)-per TD0748

FMT_SMF.1/MACSEC.1:

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 [as specified in 802.1X-2020, sections 9.13 and 9.16 (cf. MIB object ieee8021XKayMkaParticipantEntry) and section.12.2 (cf. function createMKA())]***
- ***Specify a lifetime of a CAK***
- ***Enable, disable, or delete a PSK-based CAK using [the MIB object ieee8021XKayMkaPartActivateControl]***
- ***[No other management functions].***

5.1.4.6 Restrictions on Security Roles (NDcPP22e:FMT_SMR.2)

NDcPP22e:FMT_SMR.2.1

The TSF shall maintain the roles: - Security Administrator.

NDcPP22e:FMT_SMR.2.2

The TSF shall be able to associate users with roles.

NDcPP22e:FMT_SMR.2.3

The TSF shall ensure that the conditions

- The Security Administrator role shall be able to administer the TOE locally;
- The Security Administrator role shall be able to administer the TOE remotely

are satisfied.

5.1.5 Protection of the TSF (FPT)

5.1.5.1 Protection of Administrator Passwords (NDcPP22e:FPT_APW_EXT.1)

NDcPP22e:FPT_APW_EXT.1.1

The TSF shall store administrative passwords in non-plaintext form.

NDcPP22e:FPT_APW_EXT.1.2

The TSF shall prevent the reading of plaintext administrative passwords.

5.1.5.2 Protection of CAK Data (MACSEC10:FPT_CAK_EXT.1)

MACSEC10:FPT_CAK_EXT.1.1

The TSF shall prevent reading of CAK values by administrators.

5.1.5.3 Failure with Preservation of Secure State (MACSEC10:FPT_FLS.1)

MACSEC10: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.

5.1.5.4 Replay Detection - per TD0746 (MACSEC10:FPT_RPL.1)

MACSEC10:FPT_RPL.1.1

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

MACSEC10:FPT_RPL.1.2

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

5.1.5.5 Replay Detection for XPN (MACSEC10:FPT_RPL_EXT.1)

MACSEC10:FPT_RPL_EXT.1.1
The TSF shall support extended packet numbering (XPN) as per IEEE 802.1AE-2018..
MACSEC10:FPT_RPL_EXT.1.2
The TSF shall support [GCM-AES-XPN-128, GCM-AES-XPN-256] as per IEEE 802.1AE-2018.

5.1.5.6 Protection of TSF Data (for reading of all pre-shared, symmetric and private keys) (NDcPP22e:FPT_SKP_EXT.1)

NDcPP22e:FPT_SKP_EXT.1.1
The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

5.1.5.7 Reliable Time Stamps - per TD0632 (NDcPP22e:FPT_STM_EXT.1)

NDcPP22e:FPT_STM_EXT.1.1
The TSF shall be able to provide reliable time stamps for its own use.
NDcPP22e:FPT_STM_EXT.1.2
The TSF shall [***allow the Security Administrator to set the time***].

5.1.5.8 TSF testing (NDcPP22e:FPT_TST_EXT.1)

NDcPP22e:FPT_TST_EXT.1.1
The TSF shall run a suite of the following self-tests [***during initial start-up (on power on)***] to demonstrate the correct operation of the TSF: [**integrity, AES, SHS, HMAC, RSA, ECDSA and DRBG**].

5.1.5.9 Trusted update (NDcPP22e:FPT_TUD_EXT.1)

NDcPP22e:FPT_TUD_EXT.1.1
The TSF shall provide Security Administrators the ability to query the currently executing version of the TOE firmware/software and [***the most recently installed version of the TOE firmware/software***].
NDcPP22e:FPT_TUD_EXT.1.2
The TSF shall provide Security Administrators the ability to manually initiate updates to TOE firmware/software and [***no other update mechanism***].
NDcPP22e:FPT_TUD_EXT.1.3
The TSF shall provide means to authenticate firmware/software updates to the TOE using a [***digital signature***] prior to installing those updates.

5.1.6 TOE access (FTA)

5.1.6.1 TSF-initiated Termination (NDcPP22e:FTA_SSL.3)

NDcPP22e:FTA_SSL.3.1
The TSF shall terminate a remote interactive session after a Security Administrator-configurable time interval of session inactivity.

5.1.6.2 User-initiated Termination (NDcPP22e:FTA_SSL.4)

NDcPP22e:FTA_SSL.4.1
The TSF shall allow Administrator-initiated termination of the Administrator's own interactive session.

5.1.6.3 TSF-initiated Session Locking (NDcPP22e:FTA_SSL_EXT.1)

NDcPP22e:FTA_SSL_EXT.1.1

The TSF shall, for local interactive sessions, [***terminate the session***] after a Security Administrator-specified time period of inactivity.

5.1.6.4 Default TOE Access Banners (NDcPP22e:FTA_TAB.1)

NDcPP22e:FTA_TAB.1.1

Before establishing an administrative user session the TSF shall display a Security Administrator-specified advisory notice and consent warning message regarding use of the TOE.

5.1.7 Trusted path/channels (FTP)

5.1.7.1 Inter-TSF Trusted Channel (MACsec Communications) (MACSEC10:FTP_ITC.1/MACSEC)

MACSEC10: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.

MACSEC10:FTP_ITC.1.2/MACSEC

The TSF shall permit [***the TSF***] to initiate communication via the trusted channel.

MACSEC10: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.

5.1.7.2 Inter-TSF trusted channel - per TD0639 (NDcPP22e:FTP_ITC.1)

NDcPP22e:FTP_ITC.1.1

The TSF shall be capable of using [***TLS***] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, [***no other capabilities***] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

NDcPP22e:FTP_ITC.1.2

The TSF shall permit the TSF or the authorized IT entities to initiate communication via the trusted channel.

NDcPP22e:FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for [**audit server**].

5.1.7.3 Trusted Path - per TD0639 (NDcPP22e:FTP_TRP.1/Admin)

NDcPP22e:FTP_TRP.1.1/Admin

The TSF shall be capable of using [***SSH, HTTPS, TLS***] to provide a communication path between itself and authorized remote Administrators that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure and provides detection of modification of the channel data.

NDcPP22e:FTP_TRP.1.2/Admin

The TSF shall permit remote Administrators to initiate communication via the trusted path.

NDcPP22e:FTP_TRP.1.3/Admin

The TSF shall require the use of the trusted path for initial Administrator authentication and all remote administration actions.

5.2 TOE Security Assurance Requirements

The SARs for the TOE are the components as specified in Part 3 of the Common Criteria. Note that the SARs have effectively been refined with the assurance activities explicitly defined in association with both the SFRs and SARs.

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1: Basic Functional Specification
AGD: Guidance documents	AGD_OPE.1: Operational User Guidance
	AGD_PRE.1: Preparative Procedures
ALC: Life-cycle support	ALC_CMC.1: Labelling of the TOE
	ALC_CMS.1: TOE CM Coverage
ATE: Tests	ATE_IND.1: Independent Testing - Conformance
AVA: Vulnerability assessment	AVA_VAN.1: Vulnerability Survey

Table 5-3 Assurance Components

5.2.1 Development (ADV)

5.2.1.1 Basic Functional Specification (ADV_FSP.1)

ADV_FSP.1.1d
The developer shall provide a functional specification.

ADV_FSP.1.2d
The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.1.1c
The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2c
The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3c
The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

ADV_FSP.1.4c
The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2e
The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.2 Guidance documents (AGD)

5.2.2.1 Operational User Guidance (AGD_OPE.1)

AGD_OPE.1.1d
The developer shall provide operational user guidance.

AGD_OPE.1.1c
The operational user guidance shall describe, for each user role, the user accessible functions and

privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2c

The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3c

The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4c

The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5c

The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences, and implications for maintaining secure operation.

AGD_OPE.1.6c

The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7c

The operational user guidance shall be clear and reasonable.

AGD_OPE.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2.2 Preparative Procedures (AGD_PRE.1)

AGD_PRE.1.1d

The developer shall provide the TOE, including its preparative procedures.

AGD_PRE.1.1c

The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2c

The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

AGD_PRE.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2e

The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.3 Life-cycle support (ALC)

5.2.3.1 Labelling of the TOE (ALC_CMC.1)

ALC_CMC.1.1d

The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.1.1c

The TOE shall be labelled with its unique reference.

ALC_CMC.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.2 TOE CM Coverage (ALC_CMS.1)

ALC_CMS.1.1d
The developer shall provide a configuration list for the TOE.

ALC_CMS.1.1c
The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2c
The configuration list shall uniquely identify the configuration items.

ALC_CMS.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Tests (ATE)

5.2.4.1 Independent Testing - Conformance (ATE_IND.1)

ATE_IND.1.1d
The developer shall provide the TOE for testing.

ATE_IND.1.1c
The TOE shall be suitable for testing.

ATE_IND.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2e
The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.2.5 Vulnerability assessment (AVA)

5.2.5.1 Vulnerability Survey (AVA_VAN.1)

AVA_VAN.1.1d
The developer shall provide the TOE for testing.

AVA_VAN.1.1c
The TOE shall be suitable for testing.

AVA_VAN.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.1.2e
The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3e
The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6 TOE Summary Specification

This chapter describes the security functions:

- Security audit
- Cryptographic support
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

6.1 Security audit

The TOE is a standalone device that is able to generate and store audit records of security relevant events as they occur. The events that can cause an audit record to be logged include starting and stopping the audit function, any use of an administrator command via the CLI interface, as well as all of the events identified in **Table 5-2 Audit Events**.

Audit logs are stored as strings and have a format which includes the severity, date and time of the event, the nature or type of the triggering event, an indication of whether the event succeeded, failed or had some other outcome, and the identity of the agent responsible for the event.

The audit records are protected against unauthorized access by only allowing authorized administrators to have access to local audit logs. The logged audit records also include event-specific content that includes at least all of the content required in **Table 5-2**. For cryptographic keys, the act of importing a key is audited and the associated administrator account that performed the action is recorded.

The TOE supports storage of local audit records in two types of logs visible through two CLI commands. The accounting log is visible using the command "show accounting log" while the event log is visible using the command "show logging". Each command displays the contents of the files storing the applicable log type (accounting or event). Once the TOE is capable of rotating through a set of compressed files for each log type. The TOE will check periodically to determine whether or not to rotate its logs based upon log size. The TOE fills one file, the TOE rotates the contents of the current log into a compressed file, while rotating previously compressed files until finally deleting the oldest compressed file. The event log maintains six (6) total log files with one current file and 5 rotated files. The accounting log maintains two log files with one current and one rotated file. The TOE audit storage is “full” when the current file must be rotated and the oldest file (the 5th compressed event log file, or the 2nd accounting log file) must be deleted.

The accounting log predominately includes the TOE’s audit records of CLI commands. The event log holds all other audit records. The administrator can configure the TOE to export all audit data to an external syslog server through a TLS protected connection. The TOE stores audit records related to client SSH public key operations (add/remove), time/date changes, and trusted updates (initiation and success/failure) in its event log.

Once configured to export audit records, the TOE attempts to transmit all logs in real-time, will temporarily maintain unsent records in the event of a disrupted syslog connection, and sends those records when the remote audit server successfully reestablishes the connection. The TOE uses the TLS protocol to protect audit records transmitted to the external syslog server.

The Security audit function satisfies the following security functional requirements:

NDcPP22e/MACSEC10:FAU_GEN.1: Each audit record identifies the date/time, event type, outcome of the event, responsible subject/user, as well as the additional event-specific content indicated in **Table 5-2 Audit Events**. When logging the administrative tasks of generating/importing/deleting MACsec PSKs, the TOE logs the entire command that defines the key, including the key and target address.

NDcPP22e:FAU_GEN.2: The TOE identifies the responsible user for each event based on the specific administrator or network entity (identified by IP address) that caused the event.

NDcPP22e:FAU_STG_EXT.1: The TOE can be configured to export audit records to an external SYSLOG server. This communication is protected with TLS

6.2 Cryptographic support

The TOE's uses CAVP tested internal cryptographic libraries and hardware provided cryptography as follows:

- Aruba AOS-CX Cryptographic Module version 1.0
  - TLS connections, SSH connections, Key generation and establishment,
  - Random number generator
  - Trusted updates, Product integrity
  - ECDSA Key Generation & Verification
  - AES CMAC and AES Key Wrap supporting MACsec
- Aruba AOS-CX RSA Engine
  - RSA Key Generation
- AES ECB 128bit & 256bit Encryption/Decryption Engine
  - MACsec AES GCM cryptography

The product implements and uses an SP 800-90A AES-256 CTR_DRBG.

The following functions have been CAVP tested to meet the associated SFRs.

Functions	Requirement	Standard	Certificate #
Encryption/Decryption			
AES CBC (128 and 256 bits)	FCS_COP.1/DataEncryption	FIPS Pub 197 ISO 10116 NIST SP 800-38A ISO 19772	A4592
AES-CTR (128 and 256 bits)	FCS_COP.1/DataEncryption	FIPS Pub 197 ISO 10116 NIST SP 800-38A ISO 19772	A4592
AES GCM (128 and 256 bits)	FCS_COP.1/DataEncryption	ISO 19772 FIPS Pub 197 NIST SP 800-38A	A4592
Cryptographic hashing			
SHA-1, SHA-256, SHA-384, SHA-512	FCS_COP.1/Hash	FIPS Pub 180-4 ISO/IEC 10118-3:2004	A4592
Keyed-hash message authentication			
HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 (digest sizes and block sizes of 160, 256, 384 and 512 bits)	FCS_COP.1/KeyedHash	FIPS Pub 198-1 FIPS Pub 180-4 ISO/IEC 9797-2:2011	A4592
Cryptographic signature services			
RSA Digital Signature (rDSA) (2048, 3072 bits)	FCS_COP.1/SigGen	FIPS Pub 186-4 ISO/IEC 9796-2	A4592
ECDSA Digital Signature (P-256, P-384, P-521)	FCS_COP.1/SigGen	FIPS Pub 186-4 ISO/IEC 14888-3	A4592
Random bit generation			
CTR_DRBG(AES) with sw based noise sources with a minimum of 256 bits of non-determinism	FCS_RBG_EXT.1	FIPS SP 800-90A ISO/IEC 18031:2011	A4592
Key generation			
RSA Key Generation (2048-bit)	FCS_CKM.1	FIPS Pub 186-4 ISO/IEC 9796-2	A4590

ECC Key Generation (P-256, P-384, P-521)	FCS_CKM.1	FIPS PUB 186-4	A4592	
FFC Scheme using key sies of 2048-bit or greater DSA KeyPairGen	FCS_CKM.1	FIPS PUB 186-4	A4592	
FFC Scheme using Diffie-Hellman Group 14	FCS_CKM.1	Per Policy 5: No NIST CAVP, CCTL must perform all assurance/evaluation activities		
Key establishment				
RSA	FCS_CKM.2	RSAES-PKCS1-v1_5	Tested with known good implementation	
KAS ECC P-256, P-384, P-521	FCS_CKM.2	NIST SP 800-56A Rev 3	A4591	
KAS FFC	FCS_CKM.2	NIST SP 800-56A Rev 3	A4591	
FFC Schemes using 'safe-prime' groups	FCS_CKM.2	NIST SP 800-56A Rev 3	Tested with known good implementation	
MACsec				
AES-CMAC 128 & 256 bits	FCS_COP.1/KeyedHashCMAC	SP 800-38B	A4592	
AES Key Wrap 128 & 256 bits	FCS_COP.1/MACSEC	SP 800-38F (wrap)	A4592	
AES GCM 128 & 256 bits	FCS_COP.1/MACSEC	ISO 18033-3 (AES) ISO 19722 (GCM)	BCM 54998SM	C1869
			BCM 82756	AES 4550
			BCM 82759	AES 4550
			BCM 82399	AES 4545
			BCM 82398	AES 4545

Table 6-1 TOE Cryptographic Algorithms

The Cryptographic support function satisfies the following security functional requirements:

NDcPP22e:FCS_CKM.1 & NDcPP22e:FCS_CKM.2:

Functions	Requirement	Standard	Certificate #
Encryption/Decryption			
AES CBC (128 and 256 bits)	FCS_COP.1/DataEncryption	FIPS Pub 197 ISO 10116 NIST SP 800-38A ISO 19772	A4592
AES-CTR (128 and 256 bits)	FCS_COP.1/DataEncryption	FIPS Pub 197 ISO 10116 NIST SP 800-38A ISO 19772	A4592
AES GCM (128 and 256 bits)	FCS_COP.1/DataEncryption	ISO 19772 FIPS Pub 197 NIST SP 800-38A	A4592
Cryptographic hashing			
SHA-1, SHA-256, SHA-384, SHA-512	FCS_COP.1/Hash	FIPS Pub 180-4 ISO/IEC 10118-3:2004	A4592
Keyed-hash message authentication			
HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 (digest sizes and block sizes of 160, 256, 384 and 512 bits)	FCS_COP.1/KeyedHash	FIPS Pub 198-1 FIPS Pub 180-4 ISO/IEC 9797-2:2011	A4592
Cryptographic signature services			
RSA Digital Signature (rDSA) (2048, 3072 bits)	FCS_COP.1/SigGen	FIPS Pub 186-4 ISO/IEC 9796-2	A4592

ECDSA Digital Signature (P-256, P-384, P-521)	FCS_COP.1/SigGen	FIPS Pub 186-4 ISO/IEC 14888-3	A4592	
Random bit generation				
CTR_DRBG(AES) with sw based noise sources with a minimum of 256 bits of non-determinism	FCS_RBG_EXT.1	FIPS SP 800-90A ISO/IEC 18031:2011	A4592	
Key generation				
RSA Key Generation (2048-bit)	FCS_CKM.1	FIPS Pub 186-4 ISO/IEC 9796-2	A4590	
ECC Key Generation (P-256, P-384, P-521)	FCS_CKM.1	FIPS PUB 186-4	A4592	
FFC Scheme using key sies of 2048-bit or greater DSA KeyPairGen	FCS_CKM.1	FIPS PUB 186-4	A4592	
FFC Scheme using Diffie-Hellman Group 14	FCS_CKM.1	Per Policy 5: No NIST CAVP, CCTL must perform all assurance/evaluation activities		
Key establishment				
RSA	FCS_CKM.2	RSAES-PKCS1-v1_5	Tested with known good implementation	
KAS ECC P-256, P-384, P-521	FCS_CKM.2	NIST SP 800-56A Rev 3	A4591	
KAS FFC	FCS_CKM.2	NIST SP 800-56A Rev 3	A4591	
FFC Schemes using 'safe-prime' groups	FCS_CKM.2	NIST SP 800-56A Rev 3	Tested with known good implementation	
MACsec				
AES-CMAC 128 & 256 bits	FCS_COP.1/KeyedHashCMAC	SP 800-38B	A4592	
AES Key Wrap 128 & 256 bits	FCS_COP.1/MACSEC	SP 800-38F (wrap)	A4592	
AES GCM 128 & 256 bits	FCS_COP.1/MACSEC	ISO 18033-3 (AES) ISO 19722 (GCM)	BCM 54998SM	C1869
			BCM 82756	AES 4550
			BCM 82759	AES 4550
			BCM 82399	AES 4545
			BCM 82398	AES 4545

Table 6-1 indicates that the TOE supports RSA key generation using 2048-bit keys, and ECC key generation using curves P-256, P-384 and P-521. These can be used to generate keys for use with a Certificate Signing Request, as well as in support of key establishment methods identified by

Functions	Requirement	Standard	Certificate #
Encryption/Decryption			
AES CBC (128 and 256 bits)	FCS_COP.1/DataEncryption	FIPS Pub 197 ISO 10116 NIST SP 800-38A ISO 19772	A4592
AES-CTR (128 and 256 bits)	FCS_COP.1/DataEncryption	FIPS Pub 197 ISO 10116 NIST SP 800-38A ISO 19772	A4592
AES GCM (128 and 256 bits)	FCS_COP.1/DataEncryption	ISO 19772 FIPS Pub 197 NIST SP 800-38A	A4592
Cryptographic hashing			
SHA-1, SHA-256, SHA-384, SHA-512	FCS_COP.1/Hash	FIPS Pub 180-4 ISO/IEC 10118-3:2004	A4592

Keyed-hash message authentication			
HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 (digest sizes and block sizes of 160, 256, 384 and 512 bits)	FCS_COP.1/KeyedHash	FIPS Pub 198-1 FIPS Pub 180-4 ISO/IEC 9797-2:2011	A4592
Cryptographic signature services			
RSA Digital Signature (rDSA) (2048, 3072 bits)	FCS_COP.1/SigGen	FIPS Pub 186-4 ISO/IEC 9796-2	A4592
ECDSA Digital Signature (P-256, P-384, P-521)	FCS_COP.1/SigGen	FIPS Pub 186-4 ISO/IEC 14888-3	A4592
Random bit generation			
CTR_DRBG(AES) with sw based noise sources with a minimum of 256 bits of non-determinism	FCS_RBG_EXT.1	FIPS SP 800-90A ISO/IEC 18031:2011	A4592
Key generation			
RSA Key Generation (2048-bit)	FCS_CKM.1	FIPS Pub 186-4 ISO/IEC 9796-2	A4590
ECC Key Generation (P-256, P-384, P-521)	FCS_CKM.1	FIPS PUB 186-4	A4592
FFC Scheme using key sies of 2048-bit or greater DSA KeyPairGen	FCS_CKM.1	FIPS PUB 186-4	A4592
FFC Scheme using Diffie-Hellman Group 14	FCS_CKM.1	Per Policy 5: No NIST CAVP, CCTL must perform all assurance/evaluation activities	
Key establishment			
RSA	FCS_CKM.2	RSAES-PKCS1-v1_5	Tested with known good implementation
KAS ECC P-256, P-384, P-521	FCS_CKM.2	NIST SP 800-56A Rev 3	A4591
KAS FFC	FCS_CKM.2	NIST SP 800-56A Rev 3	A4591
FFC Schemes using 'safe-prime' groups	FCS_CKM.2	NIST SP 800-56A Rev 3	Tested with known good implementation
MACsec			
AES-CMAC 128 & 256 bits	FCS_COP.1/KeyedHashCMAC	SP 800-38B	A4592
AES Key Wrap 128 & 256 bits	FCS_COP.1/MACSEC	SP 800-38F (wrap)	A4592
AES GCM 128 & 256 bits	FCS_COP.1/MACSEC	ISO 18033-3 (AES) ISO 19722 (GCM)	BCM 54998SM C1869 BCM 82756 AES 4550 BCM 82759 AES 4550 BCM 82399 AES 4545 BCM 82398 AES 4545

Table 6-1.

For asymmetric key pairs used for authentication, the TOE can generate ECDSA SSH host keys (public and private) of size P-256, P-384, and P-521 and can, upon command, regenerate a new ECDSA host key. Additionally, the administrator can load and remove user SSH public keys that the TOE will use to authenticate SSH clients. The TOE is capable of generating RSA and ECDSA key pairs for use with a certificate signing requests. For TLS, the TOE generates DH, and ECDH asymmetric keys as part of TLS key establishment as part of TLS. The TOE acts a client and as a server with the TLS protocol.

For asymmetric key pairs used for key exchange, the TOE supports generating ephemeral ECDH keys and DH keys for the SSHv2 key exchange methods selected in FCS_SSHS_EXT.1.7. This implies that the TOE generates ephemeral 256/384-bit ECDH keys using ECC schemes for P-256/384 curves and 2048/3072-bit keys using FFC schemes for DH keys for prime group DH14. The TOE supports DH group 14 key establishment scheme that meets

standard RFC 3526, section 3 for interoperability. Because the TOE is an SSH server, it always acts as the recipient/responder in the key exchange process.

NDcPP22e:FCS_CKM.4: The following table presents the crypto security parameters (CSPs), secret keys, and private keys provided by the TOE. The table also identifies when each CSP or key is cleared.

CSP or Key:	Stored in	Zeroized upon:	Zeroized by:
SSH host ECDSA private key	On Disk	Command	Overwriting with zeros
SSH host ECDSA public key	On Disk	Command	Overwriting with zeros
SSH client ECDSA public key	On Disk	Command	Overwriting with zeros
SSH session key	In Memory	Close of session	Overwriting with zeros
TLS session key	In Memory	Close of session	Overwriting with zeros
Password hash	On Disk	Command	Overwriting with zeros

Table 6-2 Key Zeroization

Keys are zeroized when they are no longer needed by the TOE, and additionally, the TOE saves keys to persistent storage. Whether saving or destroying keys, the TOE delays the operation at the physical layer until the administrator issues the "write memory" command, which saves the running configuration to the startup configuration.

MACSEC10:FCS_COP.1/KeyedHashCMAC: The TOE supports keyed-hash message authentication in accordance with AES-CMAC algorithm with key sizes 128 bits and 256 bits, the message digest size (output size) of 128 bits and block size of 128-bits. The algorithm conforms to NIST SP 800-38B.

MACSEC10:FCS_COP.1/MACSEC: The TOE performs AES key wrap with AES-GCM. AES is specified in ISO 18033-3, AES Key Wrap is specified in NIST SP 800-38F, GCM is specified in ISO 19772.

NDcPP22e:FCS_COP.1/DataEncryption: As seen in

Functions	Requirement	Standard	Certificate #
Encryption/Decryption			
AES CBC (128 and 256 bits)	FCS_COP.1/DataEncryption	FIPS Pub 197 ISO 10116 NIST SP 800-38A ISO 19772	A4592
AES-CTR (128 and 256 bits)	FCS_COP.1/DataEncryption	FIPS Pub 197 ISO 10116 NIST SP 800-38A ISO 19772	A4592
AES GCM (128 and 256 bits)	FCS_COP.1/DataEncryption	ISO 19772 FIPS Pub 197 NIST SP 800-38A	A4592
Cryptographic hashing			
SHA-1, SHA-256, SHA-384, SHA-512	FCS_COP.1/Hash	FIPS Pub 180-4 ISO/IEC 10118-3:2004	A4592
Keyed-hash message authentication			
HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 (digest sizes and block sizes of 160, 256, 384 and 512 bits)	FCS_COP.1/KeyedHash	FIPS Pub 198-1 FIPS Pub 180-4 ISO/IEC 9797-2:2011	A4592
Cryptographic signature services			
RSA Digital Signature (rDSA) (2048, 3072 bits)	FCS_COP.1/SigGen	FIPS Pub 186-4 ISO/IEC 9796-2	A4592
ECDSA Digital Signature (P-256, P-384, P-521)	FCS_COP.1/SigGen	FIPS Pub 186-4 ISO/IEC 14888-3	A4592
Random bit generation			

CTR_DRBG(AES) with sw based noise sources with a minimum of 256 bits of non-determinism	FCS_RBG_EXT.1	FIPS SP 800-90A ISO/IEC 18031:2011	A4592	
Key generation				
RSA Key Generation (2048-bit)	FCS_CKM.1	FIPS Pub 186-4 ISO/IEC 9796-2	A4590	
ECC Key Generation (P-256, P-384, P-521)	FCS_CKM.1	FIPS PUB 186-4	A4592	
FFC Scheme using key sies of 2048-bit or greater DSA KeyPairGen	FCS_CKM.1	FIPS PUB 186-4	A4592	
FFC Scheme using Diffie-Hellman Group 14	FCS_CKM.1	Per Policy 5: No NIST CAVP, CCTL must perform all assurance/evaluation activities		
Key establishment				
RSA	FCS_CKM.2	RSAES-PKCS1-v1_5	Tested with known good implementation	
KAS ECC P-256, P-384, P-521	FCS_CKM.2	NIST SP 800-56A Rev 3	A4591	
KAS FFC	FCS_CKM.2	NIST SP 800-56A Rev 3	A4591	
FFC Schemes using 'safe-prime' groups	FCS_CKM.2	NIST SP 800-56A Rev 3	Tested with known good implementation	
MACsec				
AES-CMAC 128 & 256 bits	FCS_COP.1/KeyedHashCMAC	SP 800-38B	A4592	
AES Key Wrap 128 & 256 bits	FCS_COP.1/MACSEC	SP 800-38F (wrap)	A4592	
AES GCM 128 & 256 bits	FCS_COP.1/MACSEC	ISO 18033-3 (AES) ISO 19722 (GCM)	BCM 54998SM	C1869
			BCM 82756	AES 4550
			BCM 82759	AES 4550
			BCM 82399	AES 4545
			BCM 82398	AES 4545

Table 6-1 TOE Cryptographic Algorithms above, the TOE supports the CBC and CTR modes of AES as available ciphers for SSH and GCM mode for TLS ciphersuites (all with both 128 and 256-bit keys).

NDcPP22e:FCS_COP.1/Hash: The TOE uses the SHA-1, 256, 384, and 512 hashing algorithms as part of SSHv2 integrity algorithms (see FCS_SSHS_EXT.1.6) and TLS ciphersuites. The TOE also uses SHA-256 during verification of a new image (trusted updates).

NDcPP22e:FCS_COP.1/KeyedHash: The TOE uses the HMAC algorithms described below as part of SSHv2 (for integrity) and TLS.

HMAC Algorithm	Hash Alg	Key size	Block Size	Output MAC
HMAC-SHA-1	SHA-1	160	512	160 bits
HMAC-SHA-256	SHA-256	256	512	256 bits
HMAC-SHA-384	SHA-384	384	1024	384 bits
HMAC-SHA-512	SHA-512	512	1024	512 bits

Table 6-3 HMAC Details

NDcPP22e:FCS_COP.1/SigGen: As seen in

Functions	Requirement	Standard	Certificate #
Encryption/Decryption			
AES CBC (128 and 256 bits)	FCS_COP.1/DataEncryption	FIPS Pub 197 ISO 10116	A4592

		NIST SP 800-38A ISO 19772	
AES-CTR (128 and 256 bits)	FCS_COP.1/DataEncryption	FIPS Pub 197 ISO 10116 NIST SP 800-38A ISO 19772	A4592
AES GCM (128 and 256 bits)	FCS_COP.1/DataEncryption	ISO 19772 FIPS Pub 197 NIST SP 800-38A	A4592
Cryptographic hashing			
SHA-1, SHA-256, SHA-384, SHA-512	FCS_COP.1/Hash	FIPS Pub 180-4 ISO/IEC 10118-3:2004	A4592
Keyed-hash message authentication			
HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 (digest sizes and block sizes of 160, 256, 384 and 512 bits)	FCS_COP.1/KeyedHash	FIPS Pub 198-1 FIPS Pub 180-4 ISO/IEC 9797-2:2011	A4592
Cryptographic signature services			
RSA Digital Signature (rDSA) (2048, 3072 bits)	FCS_COP.1/SigGen	FIPS Pub 186-4 ISO/IEC 9796-2	A4592
ECDSA Digital Signature (P-256, P-384, P-521)	FCS_COP.1/SigGen	FIPS Pub 186-4 ISO/IEC 14888-3	A4592
Random bit generation			
CTR_DRBG(AES) with sw based noise sources with a minimum of 256 bits of non-determinism	FCS_RBG_EXT.1	FIPS SP 800-90A ISO/IEC 18031:2011	A4592
Key generation			
RSA Key Generation (2048-bit)	FCS_CKM.1	FIPS Pub 186-4 ISO/IEC 9796-2	A4590
ECC Key Generation (P-256, P-384, P-521)	FCS_CKM.1	FIPS PUB 186-4	A4592
FFC Scheme using key sies of 2048-bit or greater DSA KeyPairGen	FCS_CKM.1	FIPS PUB 186-4	A4592
FFC Scheme using Diffie-Hellman Group 14	FCS_CKM.1	Per Policy 5: No NIST CAVP, CCTL must perform all assurance/evaluation activities	
Key establishment			
RSA	FCS_CKM.2	RSAES-PKCS1-v1_5	Tested with known good implementation
KAS ECC P-256, P-384, P-521	FCS_CKM.2	NIST SP 800-56A Rev 3	A4591
KAS FFC	FCS_CKM.2	NIST SP 800-56A Rev 3	A4591
FFC Schemes using 'safe-prime' groups	FCS_CKM.2	NIST SP 800-56A Rev 3	Tested with known good implementation
MACsec			
AES-CMAC 128 & 256 bits	FCS_COP.1/KeyedHashCMAC	SP 800-38B	A4592
AES Key Wrap 128 & 256 bits	FCS_COP.1/MACSEC	SP 800-38F (wrap)	A4592
AES GCM 128 & 256 bits	FCS_COP.1/MACSEC	ISO 18033-3 (AES) ISO 19722 (GCM)	BCM 54998SM C1869 BCM 82756 AES 4550 BCM 82759 AES 4550 BCM 82399 AES 4545 BCM 82398 AES 4545

Table 6-1 above, the TOE supports both RSA and ECDSA signing and verification. The TOE verifies RSA signatures on firmware updates (see FPT_TUD_EXT.1 in 6.5 below) and supports ECDSA authentication during SSH.

NDcPP22e:FCS_HTTPS_EXT.1: An HTTPS/TLS connection is available which presents Web GUI and Rest API administrative interfaces. The TOE implements HTTPS per RFC 2818. A connection can be established only if the peer initiates the connection.

MACSEC10:FCS_MACSEC_EXT.1: The TOE implements MACsec in accordance with IEEE 802.1AE-2018. The TOE derives a Secure Channel Identifier (SCI) from a peer's MAC address and port data to uniquely identify the originator of a MACsec Protocol Data Unit (MPDU) and rejects any MPDUs that do not contain the identifier. Once configured on an interface, only EAPOL (PAE EtherType 88-8E), MACsec Ethernet frames (EtherType 88-E5) and MAC control frames are permitted and others are rejected.

MACSEC10:FCS_MACSEC_EXT.2: The TOE implements MACsec with support for integrity protection with a confidentiality offset of 0, 30, 50. The TSF provides assurance of the integrity of protocol data units (MPDUs) using an Integrity Check Value (ICV) of 16 bytes derived with the Secure Association Key (SAK). The TOE provides the ability to derive an Integrity Check Value Key (ICK) from a CAK using a KDF, using the SCI as the most significant bits of the Initialization Vector (IV) and the 32 least significant bits of the PN as the IV. The ICV is derived from the SCI and PN. This forms the 96-bit IV used by GCM.

MACSEC10:FCS_MACSEC_EXT.3: The TOE generates unique Secure Association Keys (SAKs) using key derivation from Connectivity Association Key (CAK) per section 9.8.1 of IEEE 802.1X-2010 and the TOE's random bit generator as specified by FCS_RBG_EXT.1 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. The TOE generates unique nonce for the derivation of SAKs using the TOE's random bit generator as specified by FCS_RBG_EXT.1.

MACSEC10:FCS_MACSEC_EXT.4: The TOE supports peer authentication using only pre-shared keys. The TOE distributes SAKs between MACsec peers using AES key wrap as specified in FCS_COP.1/MACSEC. The TOE supports specifying a lifetime for CAKs. The TOE associates Connectivity Association Key Names (CKNs) with CAKs that are defined by the key derivation function using the CAK as input data (per 802.1X, section 9.8.1). The TOE associates Connectivity Association Key Names (CKNs) with CAKs. The length of the CKN is an integer number of octets, between 1 and 32 (inclusive).

MACSEC10:FCS_MKA_EXT.1: The TOE implements Key Agreement Protocol (MKA) in accordance with IEEE 802.1X-2010 and 802.1Xbx-2014. The TOE enables data delay protection for MKA. The TOE provides assurance of the integrity of MKA protocol data units (MKPDUs) using an Integrity Check Value (ICV) derived from an Integrity Check Value Key (ICK). The TOE provides the ability to derive an Integrity Check Value Key (ICK) from a CAK using a KDF. The TOE enforces an MKA Lifetime Timeout limit of 6.0 seconds and Hello Timeout limit of 2.0 seconds. The TOE behaves as a Key Server. The Key Server refreshes a SAK when it expires. The Key Server distributes a SAK by using a pairwise CAK. The pairwise CAK is derived from MKA or a pre-shared key. The Key Server refreshes a CAK when it expires. The Key Server distributes a fresh SAK whenever a member is added to or removed from the live membership of the CA.

The TOE validates MKPDUs according to 802.1X-2010, Section 11.11.2. In particular, the TOE discards 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 is not a multiple of 4 octets long.

d) 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.

e) The CAK Name is not recognized.

If an MKPDU passes these tests, then the TOE begins 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 802.1X-2010, section 9.4.1 shall be decoded as specified in 802.1X-2010, section 11.11.4.

When Data Delay Protection (DDP) is enabled, MKA PDUs are exchanged every 0.5 seconds instead of every 2.0 seconds. The PN advertised by the peer is updated as the LPN in the Rx channel of the TOE.

NDcPP22e:FCS_RBG_EXT.1: See

Functions	Requirement	Standard	Certificate #
Encryption/Decryption			
AES CBC (128 and 256 bits)	FCS_COP.1/DataEncryption	FIPS Pub 197 ISO 10116 NIST SP 800-38A ISO 19772	A4592
AES-CTR (128 and 256 bits)	FCS_COP.1/DataEncryption	FIPS Pub 197 ISO 10116 NIST SP 800-38A ISO 19772	A4592
AES GCM (128 and 256 bits)	FCS_COP.1/DataEncryption	ISO 19772 FIPS Pub 197 NIST SP 800-38A	A4592
Cryptographic hashing			
SHA-1, SHA-256, SHA-384, SHA-512	FCS_COP.1/Hash	FIPS Pub 180-4 ISO/IEC 10118-3:2004	A4592
Keyed-hash message authentication			
HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 (digest sizes and block sizes of 160, 256, 384 and 512 bits)	FCS_COP.1/KeyedHash	FIPS Pub 198-1 FIPS Pub 180-4 ISO/IEC 9797-2:2011	A4592
Cryptographic signature services			
RSA Digital Signature (rDSA) (2048, 3072 bits)	FCS_COP.1/SigGen	FIPS Pub 186-4 ISO/IEC 9796-2	A4592
ECDSA Digital Signature (P-256, P-384, P-521)	FCS_COP.1/SigGen	FIPS Pub 186-4 ISO/IEC 14888-3	A4592
Random bit generation			
CTR_DRBG(AES) with sw based noise sources with a minimum of 256 bits of non-determinism	FCS_RBG_EXT.1	FIPS SP 800-90A ISO/IEC 18031:2011	A4592
Key generation			
RSA Key Generation (2048-bit)	FCS_CKM.1	FIPS Pub 186-4 ISO/IEC 9796-2	A4590
ECC Key Generation (P-256, P-384, P-521)	FCS_CKM.1	FIPS PUB 186-4	A4592
FFC Scheme using key sies of 2048-bit or greater DSA KeyPairGen	FCS_CKM.1	FIPS PUB 186-4	A4592
FFC Scheme using Diffie-Hellman Group 14	FCS_CKM.1	Per Policy 5: No NIST CAVP, CCTL must perform all assurance/evaluation activities	
Key establishment			
RSA	FCS_CKM.2	RSAES-PKCS1-v1_5	Tested with known good implementation

KAS ECC P-256, P-384, P-521	FCS_CKM.2	NIST SP 800-56A Rev 3	A4591	
KAS FFC	FCS_CKM.2	NIST SP 800-56A Rev 3	A4591	
FFC Schemes using 'safe-prime' groups	FCS_CKM.2	NIST SP 800-56A Rev 3	Tested with known good implementation	
MACsec				
AES-CMAC 128 & 256 bits	FCS_COP.1/KeyedHashCMAC	SP 800-38B	A4592	
AES Key Wrap 128 & 256 bits	FCS_COP.1/MACSEC	SP 800-38F (wrap)	A4592	
AES GCM 128 & 256 bits	FCS_COP.1/MACSEC	ISO 18033-3 (AES) ISO 19722 (GCM)	BCM 54998SM	C1869
			BCM 82756	AES 4550
			BCM 82759	AES 4550
			BCM 82399	AES 4545
			BCM 82398	AES 4545

Table 6-1 TOE Cryptographic Algorithms above. The TOE instantiates its AES-256 CTR_DRBG with a 384-bit seed (containing a minimum of 365 bits of entropy) from a software-based noise source.

NDcPP22e:FCS_SSHS_EXT.1: The TOE supports SSHv2 interactive command-line secure administrator sessions and syslog export as indicated above. The TOE implements the SSHv2 protocol, compliant to the following RFCs: 4251, 4252, 4253, 4254, 5656, and 6668. The TOE supports public key-based and password-based authentication. The TOE allows use of the ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, and ecdsa-sha2-nistp521 algorithms for public key authentication. The TOE establishes a user identity when an SSH client presents an identity along with a valid public key[1] or correct password. The TOE supports AES-CBC and AES-CTR (both 128 and 256 keyed variants) ciphers for data encryption and hmac-sha1/sha2-256/sha2-512 for data integrity (and does not allow the "none" MAC algorithm). The TOE uses Diffie-hellman-group14-sha1 (using the 2048-bit prime specified in section 3 of RFC 3526) along with ecdh-sha2-nistp256/384 for SSHv2 key exchange. The TOE's SSHv2 implementation limits SSH packets to a size of 262,127 kilobytes. Anything larger will be dropped by the TOE. The TOE initiates a rekey before 1 hour has passes or before 1GB of data transfer occurs, whichever comes first.

NDcPP22e:FCS_TLSC_EXT.1: The TOE provides TLS v1.2 for use when exporting audit records to a SYSLOG server. The following ciphersuites are supported by default:

- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

The TOE does not support certificate pinning. The TOE supports the use of FQDN and IPv4 addresses as reference identifiers within a certificate's Common Name (CN) or Subject Alternate Name (SAN) extension. The TOE checks the SAN/CN when performing certificate validation as described in NDcPP22e:FIA_X509_EXT.1/Rev. Wildcards are allowed in certificates. IP addresses are converted to binary by parsing decimals delimited by periods. The conversion happens before any comparisons are made. Canonical format is enforced. Elliptical curves P-256, P-384, and P-521 are supported as well as DH 2048/3072. These are not configurable.

NDcPP22e:FCS_TLSC_EXT.2: The TOE can be configured with an X509 certificate which it will send to a TLS server in response to a certificate request message sent by the TLS server.

NDcPP22e:FCS_TLSS_EXT.1: An HTTPS/TLS connection is available which presents a Web GUI and RestAPI administrative interface. Thus, the TOE acts as a TLS server supporting TLSv1.2 only. No older versions of TLS, and no version of SSL are supported. The TOE supports the following ciphersuites:

[1] A public key must be previously installed and mapped to a TOE user account before public key authentication for that user can occur.

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

These ciphersuites are not configurable. Key exchanges using secp384r1 are supported. Key exchanges are not configurable. The TOE does support session resumption using session ID values.

Scheme	SFR	Service
RSA-based key establishment	FCS_SSHS_EXT.1	Remote Administration
EC key establishment	FCS_TLSS_EXT.1, FCS_TLSC_EXT.1, FCS_HTTPS_EXT.1	Trusted Channel & Remote Administration
FFC key establishment	FCS_TLSS_EXT.1, FCS_TLSC_EXT.1, FCS_HTTPS_EXT.1	Trusted Channel & Remote Administration
FFC Schemes using 'safe-prime' groups	FCS_SSHS_EXT.1	Remote Administration

Table 6-4 Key Establishment Uses

6.3 Identification and authentication

The TOE requires users to be identified and authenticated before they can access any of the TOE functions except to display a warning banner without identification or authentication. In the evaluated configuration, users can connect to the TOE via a local console or remotely using SSHv2, WebUI or RestAPI.

The user is required to log in prior to successfully establishing a session through which TOE functions can be exercised. Passwords can be composed of any alphabetic, numeric, and a wide range of special characters (identified in FIA_PMG_EXT.1). Required minimum password length can be configured by an administrator to be between 1-32 characters. When logging in the TOE will not echo passwords so that passwords are not inadvertently displayed to the user and any other users that might be able to view the login display.

The Authorized Administrator can set a lockout failure count for login attempts as the TOE's default configuration does not enforce a failed login limit. If the count is exceeded, the targeted account is locked (preventing remote administrators from logging in through SSH under the locked account/username) for an administrator-configurable time limit. Note that the TOE does not lock administrative access through local console, only remote/SSHv2 administrator access. Therefore, the local console must be co-located with the TOE and protected with equivalent physical security measures.

The Identification and authentication function satisfies the following security functional requirements:

NDcPP22e:FIA_AFL.1: An administrator account can be locked after failed authentication attempts. In order to re-establish the account, an administrator configured time period must elapse.

NDcPP22e:FIA_PMG_EXT.1: The TOE offers a wide range of characters for passwords as described above.

MACSEC10:FIA_PSK_EXT.1: The TOE supports the use of pre-shared keys for MKA as defined by IEEE 802.1X-2010. The pre-shared keys are not generated by the TOE but rather the TOE will accept a PSK as a string of hexadecimal characters.

NDcPP22e:FIA_UAU.7: The TOE does not echo passwords as they are entered.

NDcPP22e:FIA_UAU_EXT.2: The TOE uses local password-based and SSH public key-based authentication.

NDcPP22e:FIA_UIA_EXT.1: The TOE does not offer any services or access to its functions, except for displaying a warning banner, without requiring a user to be identified and authenticated.

NDcPP22e:FIA_X509_EXT.1/Rev: OCSP is supported for X509v3 certificate validation. Certificates are validated as part of the authentication process when they are presented to the TOE and when they are loaded into the TOE. The following fields are verified:

- Chain length
- Certificate revocation check with OCSP
- Certificate Validity
- CA validity check
- keyUsage verification
- Signature verification
- SAN/CN check with wild card support

NDcPP22e:FIA_X509_EXT.2: Certificates are checked and if found not valid are not accepted or if the OCSP server cannot be contacted for validity checks, then the connection is rejected.

NDcPP22e:FIA_X509_EXT.3: The TOE generates certificate requests and validates the CA used to sign the certificates.

6.4 Security management

The TOE provides two roles: Administrators (Security Administrator) and Operators. The Security Administrator role is simply an admin and has full control over the device whereas the Operator role may view status information only. Upon successful authentication to the TOE, the admin can manage the TSF data.

The TOE offers command line functions which are accessible via the CLI. The CLI is a text-based interface which can be accessed from a directly connected terminal or via a remote terminal using SSHv2. These command line functions can be used to manage every security policy, as well as the non-security relevant aspects of the TOE. The TOE also permits administrators to perform administrative tasks using an HTTPS/TLS protected communication channel offering a Web-based GUI and upload certificates through a RESTAPI interface.

Once authenticated (none of these functions is available to any user before being identified and authenticated), authorized administrators have access to the following security functions:

- Ability to administer the TOE locally and remotely;
- Ability to configure the access banner;
- Ability to configure the session inactivity time before session termination or locking;
- Ability to update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates;
- Ability to configure the authentication failure parameters for FIA_AFL.1;
- Ability to modify the behavior of the transmission of audit data to an external IT entity,
- Ability to manage the cryptographic keys;
- Ability to configure the cryptographic functionality;
- Ability to set the time which is used for time-stamps;
- Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;
- Ability to import X.509v3 certificates to the TOE's trust store;
- Ability to manage the trusted public keys database;
- Manage a PSK-based CAK and install it in the device;
- Manage the Key Server to create, delete, and activate MKA participants as specified in 802.1X-2020, sections 9.13 and 9.16 (cf. MIB object ieee8021XKayMkaParticipantEntry) and section.12.2 (cf. function createMKA());
- Specify a lifetime of a CAK; and
- Enable, disable, or delete a PSK-based CAK using the MIB object ieee8021XKayMkaPartActivateControl.

The Security management function satisfies the following security functional requirements:

NDcPP22e:FMT_MOF.1/ManualUpdate: Only the administrator can initiate product updates.

NDcPP22e:FMT_MTD.1/CoreData: Only the administrator can configure TSF-related functions. The trust store is accessed when administrators import/remove certificates as described in the [CC Guide]. The trust store is protected by default and is restricted such that only administrators have access.

NDcPP22e:FMT_MTD.1/CryptoKeys: Only administrators can perform management operations including the command to generate, import and delete cryptographic keys as defined by Table 6-2 Key Zeroization.

NDcPP22e:FMT_SMF.1: The TOE includes the functions necessary to manage its cryptographic functionality and associated functions, configure the warning banner, manage user accounts, set time, and to manage and verify updates of the TOE software and firmware.

MACSEC10:FMT_SMF.1/MACSEC: As enumerated in the text above, the TOE include management functions to manage, install and configure constraints on a CAK. The TOE can also manage the key server to create, delete, and activate MKA participants as described above.

NDcPP22e:FMT_SMR.2: The TOE includes a manager account that corresponds to the required 'Authorized Administrator' also referred to as 'Security Administrator' in some requirements or text.

6.5 Protection of the TSF

The TOE is an appliance and does not offer general purpose operating system interfaces to users. The TOE is designed to not provide access to locally stored passwords and also, while cryptographic keys can be entered, the TOE does not disclose any cryptographic keys stored in the TOE.

The TOE is a hardware appliance that includes a reliable real-time clock. The TOE uses the clock to support several security functions including timestamps for audit records, timing elements of cryptographic functions, and inactivity timeouts. The TOE provides the administrator the ability to manually set the clock.

The TOE performs diagnostic self-tests during start-up and generates audit records to document failure. Some low-level critical failure modes can prevent TOE start-up and as a result will not generate audit records. In such cases, the TOE appliance will enter failure mode displaying error codes, typically displayed on the console. The TOE will reboot with errors displayed when non-critical errors are encountered. The cryptographic library performs self-tests during startup; the messages are displayed on the console and syslog records generated for both successful and failed tests.

Upgrading the ArubaOS-CX firmware is a manual process performed by an authorized administrator. An administrator can use the "show version" and "show images" commands to query the TOE's loaded and active firmware versions. The firmware is digitally signed with RSA 3072 using SHA-256. The TOE uses one of two embedded (within the TOE's firmware images) public keys to verify the digital signature (the vendor includes a primary and a backup signing public key). The firmware is readily available on the Hewlett Packard Enterprise (HPE) website. Uploading the firmware to the devices does require successful authentication to the devices in order to issue the CLI commands needed to update. The TOE will validate the firmware validation during the loading process and will reject the firmware if validation fails. HPE signs the firmware images and includes the HPE signing public keys within the running firmware. Once the TOE has successfully verified a new firmware image, it is loaded and becomes active upon the next reboot.

The Protection of the TSF function satisfies the following security functional requirements:

NDcPP22e:FPT_APW_EXT.1: The TOE maintains and protects passwords for administrative user accounts as authentication data. Locally defined passwords are not stored in plaintext form, instead the TOE stores the password as salted SHA-512 hashes. The TOE does not offer any functions that will disclose to any user a plain text password.

MACSEC10:FPT_CAK_EXT.1: The CAK is stored in an encrypted form in the configuration. There is no mechanism provided for the administrator to decrypt the key and reveal the plain-text form.

MACSEC10:FPT_FLS.1/SelfTest: If the TOE encounters a self-test failure, failure of integrity check of the TSF executable image, or failure of noise source health tests it will shut down. The TOE will not restart as long as it has a failure and will need administrator intervention.

MACSEC10:FPT_RPL.1: The TOE detects and logs all attempts to replay MPDUs and MKA frames. The TOE allows an administrator to enables replay protection within the MACsec policy context with either a default or admin-specified window size. With replay protection enabled, packets are expected to arrive within the replay protection window number of packets. For example, with a window size of 10, any packet arriving out-of-sequence by more than 10 packets will be discarded. A window size of 0 (the default) enforces strict order of packet reception, discarding all packets not received in perfect sequence. The no form of this command disables replay protections and resets the window size to its 0 default.

MACSEC10:FPT_RPL_EXT.1: The TOE supports extended packet numbering (XPN) per IEE 802.1AE-2018 using a MACsec policy configured with XPN specific GCM cipher suites that are based on 128-bit or 256-bit AES keys. When leveraging an XPN cipher suite, the counter used to detect replayed packets is extended to 64 bits. All other replay detection logic and mechanisms remain the same.

NDcPP22e:FPT_SKP_EXT.1: The TOE stores it's SSH host private keys and TLS server certificate private keys in plaintext form but does not offer any functions to output the cryptographic key value. Similarly, there is no function to view any other encrypted key.

NDcPP22e:FPT_STM_EXT.1: The TOE includes its own hardware clock and allows the administrator to manually configure the time.

NDcPP22e:FPT_TST_EXT.1: The TOE performs a suite of self-tests to verify its integrity. The TOE performs an integrity test of its firmware (by validating the firmware's RSA digital signature) product and also performs a set of power-up self-tests including AES, SHS, HMAC, RSA, ECDSA and DRBG known answer tests. The TOE automatically performs its known answer power on self-tests (POST) on its CryptoComply cryptography library by computing a trial cryptographic operation (e.g., AES encryption) and then comparing the calculated result to the known correct result (already compiled into the library). This ensures that the TOE's implementations work correctly. Should any of the tests fail, the TOE halts the boot process.

NDcPP22e:FPT_TUD_EXT.1: The TOE provides the administrator a CLI command to manually install digitally signed (using RSA 3072 with SHA-256) updates.

6.6 TOE access

The TOE can be configured by an administrator to set an inactivity session timeout value (any integer value in minutes). The inactivity timeout is 30 minutes by default. This session timeout value is applicable to both local and remote CLI sessions. An SSHv2, Web, or RestAPI remote session that is inactive (i.e., no commands issuing from the remote client) for the defined timeout value will be terminated. A local session that is similarly inactive for the defined timeout period will be terminated. The user will be required to re-enter their user ID and their password so they can establish a new session once a session is terminated. If the user ID and password match those of the user that was locked, the session is reconnected with the console and normal input/output can again occur for that user.

The TOE can be configured to display administrator-configured advisory banners. A login banner can be configured to display warning information along with login prompts. The banners will be displayed when accessing the TOE via the console, SSH, and Web interfaces.

The TOE access function satisfies the following security functional requirements:

NDcPP22e:FTA_SSL.3: The TOE terminates remote SSHv2, Web and RestAPI sessions that have been inactive for an administrator-configured period of time. The TOE RestAPI interface is not interactive, but does enforce the same session timeout as the Web interface.

NDcPP22e:FTA_SSL.4: The TOE allows a user to terminate both local and remote sessions (including SSH, Web and RestAPI sessions). The TOE accepts the 'exit' command to terminate local and remote CLI sessions. The TOE offers a logout Web operation and a RestAPI logout URL to terminate Web and RestAPI sessions.

NDcPP22e:FTA_SSL_EXT.1: The TOE terminates local sessions that have been inactive for an administrator-configured period of time.

NDcPP22e:FTA_TAB.1: The TOE can be configured to display a warning banner before administrators successfully establish interactive sessions with the TOE (i.e., console, SSH CLI and WebUI), allowing users to terminate their session prior to performing any functions.

6.7 Trusted path/channels

The Trusted path/channels function satisfies the following security functional requirements:

MACSEC10:FTP_ITC.1: In the evaluated configuration, the TOE can be configured to establish MACsec connections with MACsec capable peers.

NDcPP22e:FTP_ITC.1: In the evaluated configuration, the TOE must be configured to use TLS to ensure that any exported audit records are sent only to the configured server so they are not subject to inappropriate disclosure or modification. The TOE is acting as a client in this instance and receives a certificate from the audit server for identification.

NDcPP22e:FTP_TRP.1/Admin: The TOE provides multiple methods of remote administration. A command line interface is available remotely via an SSH protected channel. Additionally, an HTTPS/TLS connection is available which presents a Web GUI administrative interface and the REST API interface. The administrator can initiate the remote session. The remote session is secured (disclosure and modification) using CAVP tested cryptographic operations, and all remote security management functions require the use of an SSHv2 protected channel or HTTPS/TLS protected channel.