



# Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11

## Security Target

**Version:** 1.1

**Date:** January 17, 2025



Americas Headquarters:  
Cisco Systems Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2024 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

**TABLE OF CONTENTS**

**DOCUMENT INTRODUCTION ..... 6**

**1 SECURITY TARGET INTRODUCTION ..... 7**

1.1 ST and TOE Reference..... 7

1.2 TOE Overview ..... 8

1.3 TOE Product Type ..... 8

1.4 Supported non-TOE Hardware/ Software/ Firmware ..... 8

1.5 TOE Description ..... 8

1.6 TOE Evaluated Configuration ..... 9

1.7 Physical Scope of the TOE ..... 11

1.8 Logical Scope of the TOE ..... 13

1.8.1 Security Audit..... 14

1.8.2 Cryptographic Support..... 14

1.8.3 Identification and authentication ..... 16

1.8.4 Security Management..... 16

1.8.5 Protection of the TSF..... 16

1.8.6 TOE Access ..... 16

1.8.7 Trusted path/Channels ..... 17

1.9 Excluded Functionality ..... 17

**2 CONFORMANCE CLAIMS ..... 18**

2.1 Common Criteria Conformance Claim ..... 18

2.2 Protection Profile Conformance ..... 18

2.3 Protection Profile Conformance Claim Rationale ..... 18

2.3.1 TOE Appropriateness..... 18

2.3.2 TOE Security Problem Definition Consistency ..... 18

2.3.3 Statement of Security Requirements Consistency..... 18

**3 SECURITY PROBLEM DEFINITION..... 19**

3.1 Assumptions ..... 19

3.2 Threats..... 20

3.3	Organizational Security Policies .....	22
4	<b>SECURITY OBJECTIVES.....</b>	<b>24</b>
4.1	Security Objectives for the TOE .....	24
4.2	Security Objectives for the Environment.....	25
5	<b>SECURITY REQUIREMENTS .....</b>	<b>27</b>
5.1	Conventions.....	27
5.2	TOE Security Functional Requirements.....	27
5.3	SFRs from NDcPP and MOD_MACSEC .....	29
5.3.1	Security audit (FAU) .....	29
5.3.2	Cryptographic Support (FCS) .....	32
5.3.3	Identification and authentication (FIA).....	37
5.3.4	Security management (FMT) .....	39
5.3.6	Protection of the TSF (FPT).....	40
5.3.7	TOE Access (FTA).....	42
5.3.8	Trusted Path/Channels (FTP) .....	42
5.4	TOE SFR Dependencies Rationale for SFRs Found in PP.....	43
5.5	Security Assurance Requirements.....	44
5.5.1	SAR Requirements .....	44
5.5.2	Security Assurance Requirements Rationale .....	44
5.6	Assurance Measures .....	45
6	<b>TOE SUMMARY SPECIFICATION .....</b>	<b>46</b>
6.1	TOE Security Functional Requirement Measures.....	46
7	<b>ANNEX A: KEY ZEROIZATION .....</b>	<b>60</b>
8	<b>ANNEX B: NIAP TECHNICAL DECISIONS (TDS).....</b>	<b>62</b>
9	<b>ANNEX C: REFERENCES .....</b>	<b>64</b>
10	<b>ANNEX D: OBTAINING DOCUMENTATION AND SUBMITTING A SERVICE REQUEST .....</b>	<b>65</b>
10.1	Document Feedback .....	65
10.2	Obtaining Technical Assistance .....	65

## LIST OF TABLES

TABLE 1	ACRONYMS	5
TABLE 2	ST AND TOE IDENTIFICATION	7
TABLE 3	IT ENVIRONMENT COMPONENTS	8
TABLE 4	HARDWARE MODELS AND SPECIFICATIONS	11
TABLE 5	FIPS REFERENCES	14
TABLE 6	TOE PROVIDED CRYPTOGRAPHY	15
TABLE 7	EXCLUDED FUNCTIONALITY	17
TABLE 8	PROTECTION PROFILES	18
TABLE 9	TOE ASSUMPTIONS	19
TABLE 10	THREATS	20
TABLE 11	ORGANIZATIONAL SECURITY POLICIES	22
TABLE 12	SECURITY OBJECTIVES FOR THE TOE	24
TABLE 13	SECURITY OBJECTIVES FOR THE ENVIRONMENT	25
TABLE 14	SECURITY FUNCTIONAL REQUIREMENTS	27
TABLE 15	AUDITABLE EVENTS	30
TABLE 16	ASSURANCE MEASURES	44
TABLE 17	ASSURANCE MEASURES	45
TABLE 18	HOW TOE SFRS MEASURES	46
TABLE 19	TOE KEY ZEROIZATION	60
TABLE 20	NIAP TECHNICAL DECISIONS	62
TABLE 21	REFERENCES	64

## LIST OF FIGURES

FIGURE 1	TOE EXAMPLE DEPLOYMENT	10
----------	------------------------	----

## ACRONYMS

The following acronyms and abbreviations are common and may be used in this Security Target:

**Table 1 Acronyms**

Acronyms/Abbreviations	Definition
AES	Advanced Encryption Standard
BRI	Basic Rate Interface
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
CSU	Channel Service Unit
DHCP	Dynamic Host Configuration Protocol
DSU	Data Service Unit
EHWIC	Ethernet High-Speed WIC
ESP	Encapsulating Security Payload
ESPr	Embedded Services Processors
GE	Gigabit Ethernet port
HTTPS	Hyper-Text Transport Protocol Secure
IT	Information Technology
NDcPP	collaborative Protection Profile for Network Devices
OS	Operating System
PoE	Power over Ethernet
PP	Protection Profile
SA	Security Association
SFP	Small-form-factor pluggable port
SHS	Secure Hash Standard
ST	Security Target
TCP	Transmission Control Protocol
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
WAN	Wide Area Network
WIC	WAN Interface Card

## Document Introduction

Prepared By:  
Cisco Systems, Inc.  
170 West Tasman Dr.  
San Jose, CA 95134

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), Cisco Aggregation Services Router 9000 (ASR9K). This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE which meet the set of requirements.

# 1 Security Target Introduction

The Security Target contains the following sections:

- Security Target Introduction [Section 1]
- Conformance Claims [Section 2]
- Security Problem Definition [Section 3]
- Security Objectives [Section 4]
- IT Security Requirements [Section 5]
- TOE Summary Specification [Section 6]

The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex A, and Part 3, Chapter 11.

## 1.1 ST and TOE Reference

This section provides information needed to identify and control this ST and its TOE.

**Table 2 ST and TOE Identification**

<b>Name</b>	<b>Description</b>
ST Title	Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11 Security Target
ST Version	1.1
Publication Date	January 17, 2025
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco Aggregation Services Router 9000 (ASR9K)
TOE Hardware Models	ASR-9006-SYS, ASR-9010-SYS, ASR-9902, ASR9903, ASR-9904, ASR-9906, ASR-9910, ASR-9912, ASR-9922
TOE Software Version	IOS-XR 7.11
Keywords	Router, Network Appliance, Data Protection, Authentication, Cryptography, Secure Administration, Network Device, MACsec

## 1.2 TOE Overview

The Cisco Aggregation Services Router 9000 (herein after referred to as the ASR9K) is a purpose-built, routing platform that also supports MACsec encryption. The TOE includes the hardware models as defined in Table 4.

## 1.3 TOE Product Type

The ASR9K is a scalable carrier-class router, which is designed for redundancy, high security and availability, packaging, power, and other requirements needed by service providers. The ASR9K is designed to provide continuous system operation, scalability, security, and high performance.

The ASR9K runs IOS-XR that is a microkernel based network operating system. IOS-XR is able to process data as it comes into the router without buffering delays. The microkernel is responsible for specific functions such as memory management, interrupt handling, scheduling, task switching, synchronization, and inter-process communication. The microkernel's functions do not include other system services such as device drivers, file system, and network stacks; those services are implemented as independent processes outside the kernel, and they can be restarted like any other application.

## 1.4 Supported non-TOE Hardware/ Software/ Firmware

The TOE supports the following hardware, software, and firmware in its environment when the TOE is configured in its evaluated configuration:

**Table 3 IT Environment Components**

Component	Required	Usage/Purpose Description for TOE performance
Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.
Local Console	Yes	This includes any IT Environment Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration.
MACsec Peer	Yes	This includes any MACsec peer with which the TOE participates in MACsec communications. MACsec Peer may be any device that supports MACsec communications.
Audit (syslog) Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages. Also referred to as audit server in the ST
Certificate Authority	Yes	This includes any Operational Environment Certificate Authority on the TOE network. This can be used to provide the TOE with a valid certificate during certificate enrollment.

## 1.5 TOE Description

This section provides an overview of the ASR9K Target of Evaluation (TOE). This section also defines the TOE components included in the evaluated configuration of the TOE. The TOE is comprised of both software and hardware. The hardware is comprised of the following: ASR-9006-SYS, ASR-9010-SYS, ASR-9902, ASR-9903, ASR-9904, ASR-9906, ASR-9910, ASR-9912 and ASR-9922. The software is comprised of the Cisco IOS-XR 7.11.

The TOE consists of a number of components including:

- Chassis: The TOE chassis includes 2-RU, 6-RU, 10-RU, 14-RU, 21-RU, 30-RU and 44-RU form factors. The chassis is the component of the TOE in which all other TOE components are housed.



- Route Switch Processor (RSP): A route processor in each chassis provide the advanced routing capabilities of the TOE. They also monitor and manage the other components in the ASR9K.
- Data is secured at Layer 2 with MACsec. The supporting MACsec hardware includes the A99-4HG-FLEX, A9K-4HG-FLEX, A9K-8HG-FLEX, A9K-20HG-FLEX, A99-10X400GE-X, A99-4T, A9903-8HG-PEC, A9903-20HG-PEC, A99-32X100GE-X (Non-MACsec), A99-32HG (Non-MACsec).

### 1.6 TOE Evaluated Configuration

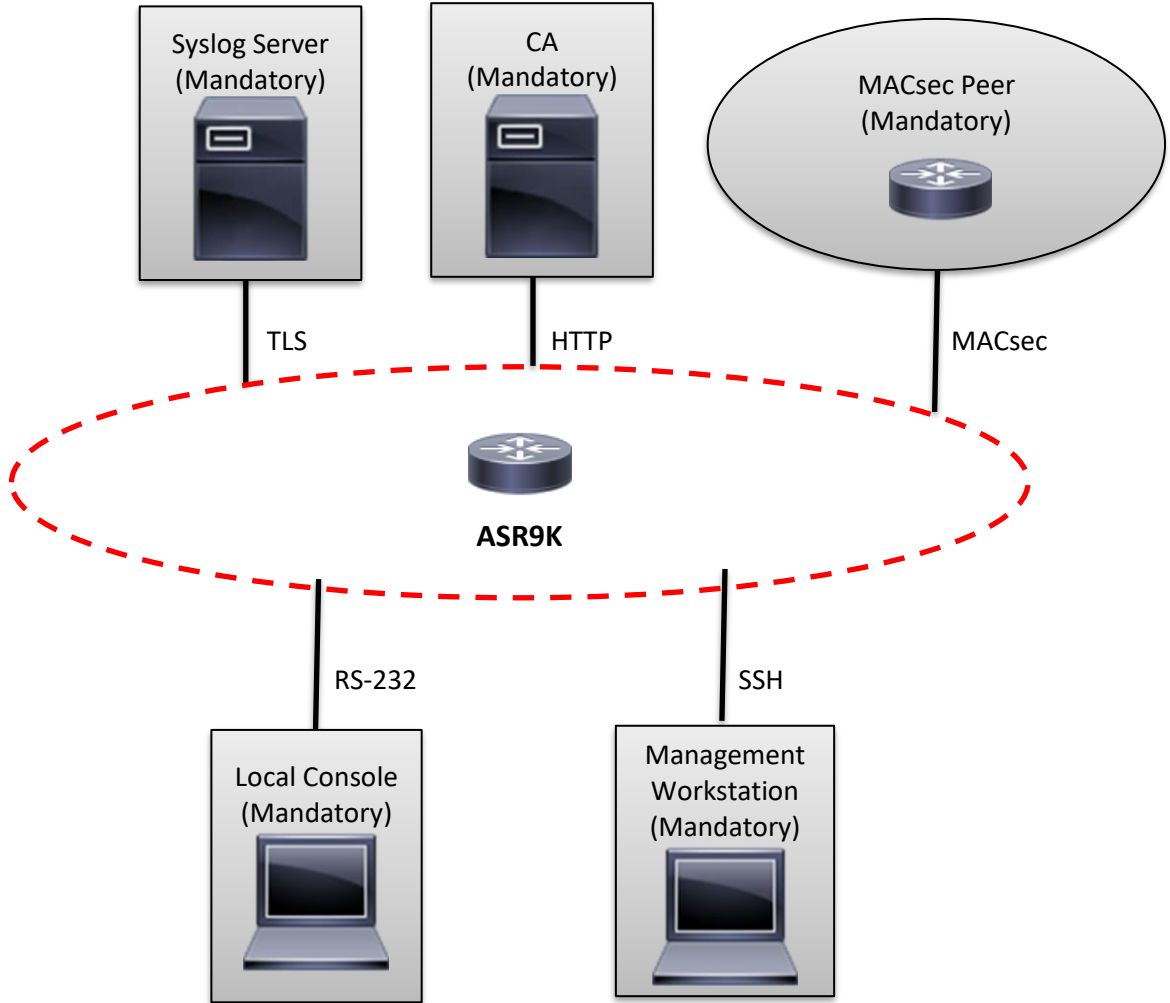
The TOE consists of one or more physical devices as specified in section 1.7 below along with MACsec-supporting hardware A99-4HG-FLEX, A9K-4HG-FLEX, A9K-8HG-FLEX, A9K-20HG-FLEX, A99-10X400GE-X, A99-4T, ASR9902, ASR9903, A9903-8HG-PEC, A9903-20HG-PEC, non-MACsec line cards A99-32X100GE-X (Non-MACsec), A99-32HG (Non-MACsec), and includes the Cisco IOS-XR software. The TOE has two or more network interfaces and is connected to at least one internal and one external network. The Cisco IOS-XR configuration determines how packets are handled to and from the TOE's network interfaces. The router configuration will determine how traffic flows received on an interface will be handled. Typically, packet flows are passed through the internetworking device and forwarded to their configured destination.

An external syslog server must be used to store audit records. The TOE authenticates those devices with X.509v3 certificates and protects communication channels with the TLS protocol. Secure remote administration is protected with SSH which is implemented with authentication failure handling.

For remote administration, a secure session using SSHv2 must be established.

The following figure provides a visual depiction of an example TOE deployment:

Figure 1 TOE Example Deployment



 = TOE Boundary

The previous figure includes the following:

- Examples of TOE Models
- The following are considered to be in the IT Environment:
  - MACsec Peer
  - Management Workstation
  - Audit (Syslog) Server
  - Local Console
  - Certificate Authority

NOTE: While the previous figure includes several non-TOE IT environment devices, the TOE is only the ASR9K device. Only one TOE device is required for deployment in an evaluated configuration.

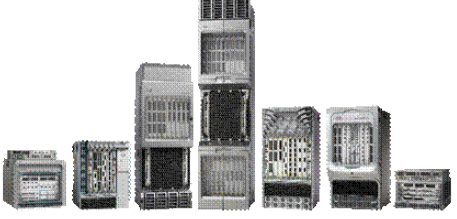


### 1.7 Physical Scope of the TOE








The TOE is a hardware and software solution that makes up the router models as follows:






- Chassis: ASR-9006-SYS, ASR-9010-SYS, ASR-9902, ASR-9903, ASR-9904, ASR-9906, ASR-9910, ASR-9912, ASR-9922
- Route Processors: A99-RP3, A9K-RSP5, A99-RP3-X, A9K-RSP5-X, A99-RP-F
- Line Cards: A99-4HG-FLEX, A9K-4HG-FLEX, A9K-8HG-FLEX, A9K-20HG-FLEX, A99-10X400GE-X, A99-4T, A9903-8HG-PEC, A9903-20HG-PEC, A99-32X100GE-X (Non-MACsec), A99-32HG (Non-MACsec)

The network, on which they reside, is considered part of the environment. The software is pre-installed and is comprised of the Cisco IOS-XR software image Release 7.11. In addition, the software image is also downloadable from the Cisco web site. A login id and password is required to download the software image. The TOE guidance documentation, *Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11 Common Criteria Operational User Guidance*, that is considered to be part of the TOE is also available for download in PDF format. The TOE is comprised of the following physical specifications as described in Table 4 below:

**Table 4 Hardware Models and Specifications**

Hardware	Picture	Specifications
Modular Chassis		<p><b>Physical dimensions</b> (H x W x D in.)</p> <ul style="list-style-type: none"> <li>• 9006: 17.50 x 17.38 x 29.05 - 10 RU</li> <li>• 9010: 36.75 x 17.38 x 28.24 - 21 RU</li> <li>• 9904: 10.38 x 17.57 x 25.02 - 6RU</li> <li>• 9906: 24.39 x 17.60 x 31.45 - 14RU</li> <li>• 9910: 36.69 x 17.60 x 30.41 - 21RU</li> <li>• 9912: 52.5 x 17.60 x 29.25 - 30RU</li> <li>• 9922: 77 x 17.60 x 30.1 - 44RU</li> </ul>
Route Processors	<p style="text-align: center;">A9K-RSP5</p>  <p style="text-align: center;">A99-RP3</p> 	<p><b>RSP5</b></p> <ul style="list-style-type: none"> <li>• CPU - Intel Xeon Silver 4109T (Skylake)</li> <li>• 16, 24 or 40 GB DRAM</li> <li>• 1 RS-232 console</li> <li>• 2 GE management ports</li> <li>• 1 auxiliary port</li> <li>• 1 USB 2.0 port</li> </ul> <p><b>RP3</b></p> <ul style="list-style-type: none"> <li>• CPU - Intel Xeon Silver 4109T (Skylake)</li> </ul>

Hardware	Picture	Specifications
	<p style="text-align: center;">A9K-RSP5-X</p>  <p style="text-align: center;">A99-RP3-X</p> 	<ul style="list-style-type: none"> <li>• 16, 24 or 40 GB DRAM</li> <li>• 1 RS-232 console</li> <li>• 2 GE management ports</li> <li>• 1 auxiliary port</li> <li>• 1 USB 2.0 port</li> </ul> <p><b>RSP5-X</b></p> <ul style="list-style-type: none"> <li>• CPU - Intel Xeon D-1573N (Broadwell)</li> <li>• 24 or 48 GB DRAM</li> <li>• 1 RS-232 console</li> <li>• 2 GE management ports</li> <li>• 1 auxiliary port</li> <li>• 1 USB 2.0 port</li> </ul> <p><b>RP3-X</b></p> <ul style="list-style-type: none"> <li>• CPU - Intel Xeon D-1573N (Broadwell)</li> <li>• 24 or 48 GB DRAM</li> <li>• 1 RS-232 console</li> <li>• 2 GE management ports</li> <li>• 1 auxiliary port</li> <li>• 1 USB 2.0 port</li> </ul>
Line Cards	<p style="text-align: center;">A9K-4HG-FLEX, A99-4HG-FLEX</p>  <p style="text-align: center;">A9K-8HG-FLEX</p>  <p style="text-align: center;">A9K-20HG-FLEX</p>  <p style="text-align: center;">A99-10X400GE-X, A99-4T</p>  <p style="text-align: center;">A99-32X100GE-X, A99-32HG</p> 	<p><b>A9K-4HG-FLEX, A99-4HG-FLEX</b></p> <ul style="list-style-type: none"> <li>• MACsec MPU - Microchip META-DX1 PM6110</li> <li>• 4x40/100GE QSFP ports</li> <li>• 16x10/15GE SFP ports</li> <li>• 24x10GE SFP+ ports</li> </ul> <p><b>A9K-8HG-FLEX</b></p> <ul style="list-style-type: none"> <li>• MACsec MPU - Microchip META-DX1 PM6110</li> <li>• 6x10/40/100GE QSFP ports</li> <li>• 2x10/40/100/200/400GB QSFP ports</li> </ul> <p><b>A9K-20HG-FLEX</b></p> <ul style="list-style-type: none"> <li>• MACsec MPU - Microchip META-DX1 PM6110</li> <li>• 2x10/40/100GE QSFP ports</li> <li>• 5x10/40/100/200/400GE QSFP ports</li> </ul> <p><b>A99-10X400GE-X, A99-4T</b></p> <ul style="list-style-type: none"> <li>• MACsec MPU – Microchip META-DX1 PM6110</li> <li>• 10x10/25/40/100/400GE QSFP ports</li> </ul> <p><b>A99-32X100GE-X, A99-32HG (Non-MACsec)</b></p> <ul style="list-style-type: none"> <li>• 32x100GE QSFP ports</li> </ul>

Hardware	Picture	Specifications
Standalone Chassis	<p style="text-align: center;">A99-RP-F</p>  <p style="text-align: center;">ASR-9902</p>  <p style="text-align: center;">ASR-9903</p>  <p style="text-align: center;">A9903-8HG-PEC</p>  <p style="text-align: center;">A9903-20HG-PEC</p> 	<p><b>A99-RP-F - 9902 / 9903 Route Processor</b></p> <ul style="list-style-type: none"> <li>• CPU - Intel Xeon D-1533N (Broadwell)</li> <li>• 32GB SDRAM</li> <li>• 1 RS-232 console</li> <li>• 2 GE management ports</li> <li>• 1 auxiliary port</li> <li>• 1 USB 2.0 port</li> </ul> <p><b>Dimensions (in.)</b></p> <ul style="list-style-type: none"> <li>• 9902: 3.46 x 17.32 x 19 – 2RU</li> <li>• 9903: 5.18 x 17.475 x 30 – 3RU</li> </ul> <p><b>9902 Integrated Interfaces</b></p> <ul style="list-style-type: none"> <li>• MACsec MPU – Microchip META-DX1 PM6108</li> <li>• 2x10/40/100GE QSFP ports</li> <li>• 6x10/40/100GE QSFP ports</li> <li>• 16x25/10GE SFP, 24x10GE SFP+ ports</li> </ul> <p><b>9903 Integrated Interfaces</b></p> <ul style="list-style-type: none"> <li>• MACsec MPU – Microchip META-DX1 PM6110</li> <li>• 16x10/40/100GE QSFP ports</li> <li>• 20x10GE SFP+ ports</li> </ul> <p><b>A9903-8HG-PEC Line card</b></p> <ul style="list-style-type: none"> <li>• MACsec MPU – Microchip META-DX1 PM6110</li> <li>• 32x25GE/10GE SFP+ ports</li> <li>• 16x10GE SFP+ ports</li> </ul> <p><b>A9903-20HG-PEC Line card</b></p> <ul style="list-style-type: none"> <li>• MACsec MPU – Microchip META-DX1 PM6108</li> <li>• 5x20 400GE/200GE/100GE QSFP ports</li> <li>• 15x100GE QSFP ports</li> </ul>

**Note:** All Cisco HW devices are shipped via courier.

## 1.8 Logical Scope of the TOE

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

These features are described in more detail in the subsections below. In addition, the TOE implements all SFRs of the NDcPP v2.2e and MOD\_MACSEC\_V1.0 as necessary to satisfy testing/assurance measures prescribed therein.

### 1.8.1 Security Audit

The TOE provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The TOE generates an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity. The administrator configures auditable events, performs back-up operations and manages audit data storage. The TOE provides the administrator with a circular audit trail. The TOE is configured to transmit its audit messages to an external syslog server over an encrypted channel using TLS.

### 1.8.2 Cryptographic Support

The TOE provides cryptography in support of other TOE security functionality. All the algorithms claimed have CAVP certificates (Operational Environment – Intel Xeon D-1533N (Broadwell) Intel Xeon D-1573N (Broadwell), Intel Xeon Silver 4109T (Skylake)). In addition, the TOE supports MACsec using the Microchip META-DX1 PM6110 processor (see Table 5 for certificate references).

Table 5 FIPS References

Algorithm	Description	Supported Mode	Module	CAVP Cert. #	SFR
AES	Used for symmetric encryption/decryption	CBC (128 and 256)	FOM 7.3a	A4446	FCS_COP.1/DataEncryption
		GCM (128 and 256)	FOM 7.3a	A4446	FCS_COP.1/DataEncryption
		CMAC (128 and 256)	FOM 7.3a	A4446	FCS_COP.1/CMAC
		AES Key Wrap (128 and 256)	FOM 7.3a	A4446	FCS_COP.1/MACSEC
		GCM (128 and 256)	MACsec	A1104	FCS_COP.1/MACSEC
SHS (SHA1, SHA-256, SHA-384, SHA-512)	Cryptographic hashing services	Byte Oriented	FOM 7.3a	A4446	FCS_COP.1/Hash
HMAC (SHA1, SHA-256, SHA-384, SHA-512)	Keyed hashing services and software integrity test	Byte Oriented	FOM 7.3a	A4446	FCS_COP.1/KeyedHash
DRBG	Deterministic random bit generation services in accordance with ISO/IEC 18031:2011	HMAC_DRBG	FOM 7.3a	A4446	FCS_RBG_EXT.1
RSA	Signature Verification and Key Transport	PKCS#1 v.1.5, 2048 and 3072 bit key	FOM 7.3a	A4446	FCS_COP.1/SigGen

Algorithm	Description	Supported Mode	Module	CAVP Cert. #	SFR
	Key Generation	FIPS 186-4 Key Gen	FOM 7.3a	A4446	FCS_CKM.1
ECDSA	Key Generation	FIPS 186-4 Key Gen	FOM 7.3a	A4446	FCS_CKM.1
KAS-ECC	Key Agreement	NIST Special Publication 800-56A	FOM 7.3a	A4446	FCS_CKM.2

The TOE provides cryptography in support of remote administrative management via SSHv2 and secures the session between the ASR9K and remote syslog server using TLS.

The TOE authenticates and encrypts packets between itself and a MACsec peer. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys to protect data exchanged by the peers.

The cryptographic services provided by the TOE are described in Table 6 below:

**Table 6 TOE Provided Cryptography**

Cryptographic Method	Use within the TOE
Secure Shell Establishment	Used to establish initial SSH session.
RSA Signature Services	Used in SSH session establishment. Used in TLS session establishment. X.509 certificate signing.
SHS	Used to provide SSH traffic integrity verification Used for keyed-hash message authentication
AES	Used to encrypt SSH session traffic. Used to encrypt TLS session traffic. Used to encrypt MACsec traffic.
HMAC	Used for keyed hash, integrity services in SSH session establishment.
TLS	Used to secure traffic to the syslog server.
AES-CMAC	Used to encrypt MACsec keys.
ISO/IEC 18031:2011 HMAC_CRBG)	Used for random number generation, key generation and seeds to asymmetric key generation Used in TLS session establishment Used in SSH session establishment Used in MACsec session establishment

### 1.8.3 Identification and authentication

The TOE provides authentication services for administrative users wishing to connect to the TOEs secure CLI administrator interface. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters as well as mandatory password complexity rules.

After a configurable number of incorrect login attempts, ASR9K will lockout the account until a configured amount of time for lockout expires.

The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the serial console or SSH interfaces. The SSHv2 interface also supports authentication using SSH keys.

The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for TLS connections.

### 1.8.4 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure SSHv2 session or via a local console connection. The TOE provides the ability to securely manage all TOE administrative users, all identification and authentication, all audit functionality of the TOE, all TOE cryptographic functionality, the timestamps maintained by the TOE, and updates to the TOE. The TOE supports a privileged administrator role. Only the privileged administrator can perform the above security relevant management functions.

Administrators can create configurable login banners to be displayed at time of login, and can also define an inactivity timeout for each admin interface to terminate sessions after a set period of inactivity.

### 1.8.5 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Authorized Administrators. The TOE prevents reading of cryptographic keys and passwords. Additionally, Cisco IOS-XR is not a general-purpose operating system and access to Cisco IOS-XR memory space is restricted to only Cisco IOS-XR functions.

The TOE is also able to detect replay of information received via secure channels (MACsec). The detection applied to network packets that terminate at the TOE, such as trusted communications between the TOE and an IT entity (e.g., MACsec peer). If replay is detected, the packets are discarded.

The TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE. Administrators can update the TOE's clock manually. Finally, the TOE performs testing to verify correct operation of the router itself and that of the cryptographic module.

The TOE is able to verify any software updates prior to the software updates being installed on the TOE to avoid the installation of unauthorized software.

### 1.8.6 TOE Access

The TOE can terminate inactive sessions after an Authorized Administrator configurable time-period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session.

The TOE can also display a Security Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE.



### 1.8.7 Trusted path/Channels

The TOE establishes a trusted path between the appliance and the CLI using SSHv2 and the syslog server using TLS. MACsec is used to secure communication channels between MACsec peers at Layer 2.

## 1.9 Excluded Functionality

The following functionality is excluded from the evaluation:

**Table 7 Excluded Functionality**

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation	This mode of operation includes non-FIPS allowed operations.

These services will be disabled by configuration settings. The exclusion of this functionality does not affect compliance to the NDcPP v2.2e and MOD\_MACSEC\_V1.0.

## 2 Conformance Claims

### 2.1 Common Criteria Conformance Claim

The TOE and ST are compliant with the Common Criteria (CC) Version 3.1, Revision 5, dated: April 2017. The TOE and ST are CC Part 2 extended and CC Part 3 conformant.

### 2.2 Protection Profile Conformance

The TOE and ST are conformant with the Protection Profiles as listed in Table 8 below. This ST applies the NIAP Technical Decisions as described in Table 20.

**Table 8 Protection Profiles**

Protection Profile Configuration	Date
PP-Configuration for Network Devices and MACsec Ethernet Encryption (CFG_NDcPP-MACsec_V1.0)	March 29, 2023
<ul style="list-style-type: none"> <li>Base-PP: collaborative Protection Profile for Network Devices, Version 2.2e (CPP_ND_V2.2E)</li> <li>PP-Module: PP-Module for MACsec Ethernet Encryption, Version 1.0 (MOD_MACsec_V1.0)</li> </ul>	March 23, 2020 March 2, 2023

### 2.3 Protection Profile Conformance Claim Rationale

#### 2.3.1 TOE Appropriateness

The TOE provides all of the functionality at a level of security commensurate with that identified in the U.S. Government Protection Profile and extended package:

- collaborative Protection Profile for Network Devices (NDcPP) Version 2.2e
- PP-Module for MACsec Ethernet Encryption Version 1.0 (MOD\_MACSEC\_V1.0)

#### 2.3.2 TOE Security Problem Definition Consistency

The Assumptions, Threats, and Organizational Security Policies included in the Security Target represent the Assumptions, Threats, and Organizational Security Policies specified in the collaborative Protection Profile for Network Devices (NDcPP) Version 2.2e and MOD\_MACSEC\_V1.0 for which conformance is claimed verbatim. All concepts covered in the Protection Profile Security Problem Definition are included in the Security Target Statement of Security Objectives Consistency.

The Security Objectives included in the Security Target represent the Security Objectives specified in the NDcPP Version 2.2e and MOD\_MACSEC\_V1.0 for which conformance is claimed verbatim. All concepts covered in the Protection Profile's Statement of Security Objectives are included in the Security Target.

#### 2.3.3 Statement of Security Requirements Consistency

The Security Functional Requirements included in the Security Target represent the Security Functional Requirements specified in the NDcPP v2.2e and MOD\_MACSEC\_V1.0 for which conformance is claimed verbatim. All concepts covered in the Protection Profile's Statement of Security Requirements are included in this Security Target. Additionally, the Security Assurance Requirements included in this Security Target are identical to the Security Assurance Requirements included in the NDcPP Version 2.2e and the MOD\_MACSEC\_V1.0.

### 3 Security Problem Definition

This chapter identifies the following:

- Assumptions about the TOE's operational environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.
- Threats addressed by the TOE and the IT Environment.
- Organizational Security Policies imposed by an organization on the TOE to address its security needs.

This document identifies assumptions as A.assumption with “assumption” specifying a unique name. Threats are identified as T.threat with “threat” specifying a unique name. Organizational Security Policies (OSPs) are identified as P.osp with “osp” specifying a unique name.

#### 3.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

**Table 9 TOE Assumptions**

Assumption	Assumption Definition
A.PHYSICAL_PROTECTION	The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/ services that could be deemed as general purpose computing. For example the device should not provide computing platform for general purpose applications (unrelated to networking functionality).  If a virtual TOE evaluated as a pND, following Case 2 vNDs as specified in Section 1.2, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of a distributed TOE run inside more than one virtual machine (VM) on a single VS. In Case 2 vND, no non-TOE guest VMs are allowed on the platform.
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by

Assumption	Assumption Definition
	cPPs for particular types of Network Devices (e.g, firewall).
A.TRUSTED_ADMINISTRATOR	<p>The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device.</p> <p>For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', 'trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).</p>
A.REGULAR_UPDATES	The Network Device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.RESIDUAL_INFORMATION	The Administrator must ensure 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.

### 3.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

Table 10 Threats

Threat	Threat Definition
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain administrator access to the Network Device by nefarious means such as masquerading as an administrator to the device, masquerading as the device to an administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between Network Devices. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.

T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the Network Device without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials include replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or device credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other Network Devices.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.
T.DATA_INTEGRITY	An attacker may modify data transmitted over the layer 2 link in a way that is not detected by the recipient.  Devices on a network may be exposed to attacks that attempt

	to corrupt or modify data in transit without authorization. If malicious devices are able to modify and replay data that is transmitted over a layer 2 link, then the data contained within the communications may be susceptible to a loss of integrity.
T.NETWORK_ACCESS	<p>An attacker may send traffic through the TOE that enables them to access devices in the TOE’s operational environment without authorization.</p> <p>A MACsec device may sit on the periphery of a network, which means that it may have an externally facing interface to a public network. Devices located in the public network may attempt to exercise services located on the internal network that are intended to be accessed only from within the internal network or externally accessible only from specifically authorized devices. If the MACsec device allows unauthorized external devices access to the internal network, these devices on the internal network may be subject to compromise. Similarly, if two MACsec devices are deployed to facilitate end-to-end encryption of traffic that is contained within a single network, an attacker could use an insecure MACsec device as a method to access devices on a specific segment of that network such as an individual LAN.</p>
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target Network Devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the Network Device itself.
T.UNTRUSTED_MACSEC_COMMUNICATION_CHANNELS	<p>An attacker may acquire sensitive TOE or user data that is transmitted to or from the TOE because an untrusted communication channel causes a disclosure of data in transit.</p> <p>A generic network device may be threatened by the use of insecure communications channels to transmit sensitive data. The attack surface of a MACsec device also includes the MACsec trusted channels. Inability to secure communications channels, or failure to do so correctly, would expose user data that is assumed to be secure to the threat of unauthorized disclosure.</p>

### 3.3 Organizational Security Policies

The following table lists the Organizational Security Policies imposed by an organization to address its security needs.

**Table 11 Organizational Security Policies**

Policy Name	Policy Definition
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

## 4 Security Objectives

This section identifies the security objectives of the TOE and the IT Environment. The security objectives identify the responsibilities of the TOE and the TOE's IT environment in meeting the security needs.

This document identifies objectives of the TOE as O.objective with objective specifying a unique name. Objectives that apply to the IT environment are designated as OE.objective with objective specifying a unique name.

### 4.1 Security Objectives for the TOE

The following table, Security Objectives for the TOE, identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies. The security objectives below have been drawn verbatim from [MOD\_MACSEC\_V1.0].

**Table 12 Security Objectives for the TOE**

TOE Objective	TOE Security Objective Definition
O.AUTHENTICATION_MACSEC	To further address the issues associated with unauthorized disclosure of information, a compliant TOE's authentication ability (MKA) will allow a MACsec peer to establish connectivity associations (CAs) with another MACsec peer. MACsec endpoints authenticate each other to ensure they are communicating with an authorized MAC Security Entity (SecY) entity. Addressed by: FCS_MACSEC_EXT.4, FCS_MKA_EXT.1, FIA_PSK_EXT.1, FCS_DEVID_EXT.1 (selection-based), FCS_EAP-TLS_EXT.1 (selectionbased)
O.AUTHORIZED_ADMINISTRATION	All network devices are expected to provide services that allow the security functionality of the device to be managed. The MACsec device, as a specific type of network device, has a refined set of management functions to address its specialized behavior. In order to further mitigate the threat of a compromise of its security functionality, the MACsec device prescribes the ability to limit brute-force authentication attempts by enforcing lockout of accounts that experience excessive failures and by limiting access to security-relevant data that administrators do not need to view. Addressed by: FMT_SMF.1/MACSEC, FPT_CAK_EXT.1, FIA_AFL_EXT.1 (optional), FTP_TRP.1/MACSEC (optional), FMT_SNMP_EXT.1 (selection-based)
O.CRYPTOGRAPHIC_FUNCTIONS_MACSEC	To address the issues associated with unauthorized modification and disclosure of information, compliant TOEs will implement cryptographic capabilities. These capabilities are intended to maintain confidentiality and allow for detection and modification of data that is transmitted outside of the TOE. Addressed by: FCS_COP.1/CMAC, FCS_COP.1/MACSEC, FCS_MACSEC_EXT.2, FCS_MACSEC_EXT.3, FTP_ITC.1/MACSEC, FTP_TRP.1/MACSEC (optional), FCS_SNMP_EXT.1 (selection-based)



TOE Objective	TOE Security Objective Definition
O.PORT_FILTERING_MACSEC	To further address the issues associated with unauthorized network access, a compliant TOE's port filtering capability will restrict the flow of network traffic through the TOE based on layer 2 frame characteristics and whether or not the traffic represents valid MACsec frames and MACsec Key Agreement Protocol Data Units (MKPDUs). Addressed by: FCS_MACSEC_EXT.1, FIA_PSK_EXT.1, FPT_DDP_EXT.1
O.REPLAY_DETECTION	A MACsec device is expected to help mitigate the threat of MACsec data integrity violations by providing a mechanism to detect and discard replayed traffic for MPDUs. Addressed by: FPT_RPL.1, FPT_RPL_EXT.1 (optional)
O.SYSTEM_MONITORING_MACSEC	To address the issues of administrators being able to monitor the operations of the MACsec device, compliant TOEs will implement the ability to log the flow of Ethernet traffic. Specifically, the TOE will provide the means for administrators to configure rules to 'log' when Ethernet traffic grants or restricts access. As a result, the 'log' will result in informative event logs whenever a match occurs. In addition, the establishment of security CAs is auditable, not only between MACsec devices, but also with MAC Security Key Agreement Entities (KaYs). Addressed by: FAU_GEN.1/MACSEC
O.TSF_INTEGRITY	To mitigate the security risk that the MACsec device may fail during startup, it is required to fail-secure if any self-test failures occur during startup. This ensures that the device will only operate when it is in a known state. Addressed by: FPT_FLS.1

## 4.2 Security Objectives for the Environment

All of the assumptions stated in section 3.1 are considered to be security objectives for the environment. The following are the Protection Profile non-IT security objectives, which, in addition to those assumptions, are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

**Table 13 Security Objectives for the Environment**

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

Environment Security Objective	IT Environment Security Objective Definition
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.TRUSTED_ADMIN	<p>Security 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.</p> <p>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.</p>
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.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.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.

## 5 Security Requirements

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements in this section are drawn from [CC\_PART2], [NDcPPv2.2e], [MOD\_MACSEC\_V1.0], and NIAP Technical Decisions.

### 5.1 Conventions

[CC\_PART1] defines operations on Security Functional Requirements. This document uses the following conventions to identify the operations permitted by [NDcPPv2.2e], [MOD\_MACSEC\_V1.0], and NIAP Technical Decisions.

- Assignment: Indicated with *italicized* text;
- Assignment completed within a selection in the cPP: the completed assignment text is indicated with *italicized and underlined text*
- Refinement: Indicated with **bold** text;
- Selection: Indicated with underlined text;
- Iteration: indicated by adding a string starting with “/” (e.g. “FCS\_COP.1/Hash”)
- Where operations were completed in the NDcPP itself, the formatting used in the NDcPP has been retained.

The following conventions were used to resolve conflicting SFRs between the NDcPP and MOD\_MACSEC:

- All SFRs from MOD\_MACSEC reproduced as-is
- SFRs that appear in both NDcPP and MOD\_MACSEC are modified based on instructions specified in MOD\_MACSEC.

### 5.2 TOE Security Functional Requirements

This section identifies the Security Functional Requirements for the TOE. The TOE Security Functional Requirements that appear in the following table are described in more detail in the following subsections.

**Table 14 Security Functional Requirements**

Class Name	Component Identification	Component Name
FAU: Security audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.1/MACSEC	MACSEC Audit Data Generation
	FAU_GEN.2	User identity association
	FAU_STG_EXT.1	Protected Audit Event Storage
FCS: Cryptographic support	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.2	Cryptographic Key Establishment
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1/DataEncryption	Cryptographic Operation (for data encryption/decryption)
	FCS_COP.1/SigGen	Cryptographic Operation (for cryptographic signature)
	FCS_COP.1/Hash	Cryptographic Operation (for cryptographic hashing)
	FCS_COP.1/KeyedHash	Cryptographic Operation (for keyed-hash message authentication)
	FCS_COP.1/CMAC	Cryptographic Operation (AES-CMAC Keyed Hash Algorithm)

Class Name	Component Identification	Component Name
	FCS_COP.1/MACSEC	Cryptographic Operation (MACsec AES Data Encryption and Decryption)
	FCS_MACSEC_EXT.1	MACsec
	FCS_MACSEC_EXT.2	MACsec Integrity and Confidentiality
	FCS_MACSEC_EXT.3	MACsec Randomness
	FCS_MACSEC_EXT.4	MACsec Key Usage
	FCS_MKA_EXT.1	MACsec Key Agreement
	FCS_SSHS_EXT.1	SSH Server Protocol
	FCS_TLSC_EXT.1	TLS Client Protocol
	FCS_RBG_EXT.1	Random Bit Generation
FIA: Identification and authentication	FIA_AFL.1	Authentication Failure Management
	FIA_PMG_EXT.1	Password Management
	FIA_PSK_EXT.1	Pre-Shared Key Composition
	FIA_UIA_EXT.1	User Identification and Authentication
	FIA_UAU_EXT.2	Password-based Authentication Mechanism
	FIA_UAU.7	Protected Authentication Feedback
	FIA_X509_EXT.1/Rev	X.509 Certificate Validation
	FIA_X509_EXT.2	X.509 Certificate Authentication
FMT: Security management	FMT_MOF.1/ManualUpdate	Trusted Update - Management of security functions behaviour
	FMT_MTD.1/CryptoKeys	Management of TSF Data
	FMT_MTD.1/CoreData	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMF.1/MACSEC	Specification of Management Functions (MACsec)
	FMT_SMR.2	Restrictions on security roles
FPT: Protection of the TSF	FPT_APW_EXT.1	Protection of Administrator Passwords
	FPT_CAK_EXT.1	Protection of CAK Data
	FPT_FLS.1	Failure with Preservation of Secure State
	FPT_RPL.1	Replay Detection
	FPT_RPL_EXT.1	Replay Detection for XPN
	FPT_SKP_EXT.1	Protection of TSF Data (for reading of all symmetric keys)

Class Name	Component Identification	Component Name
	FPT_STM_EXT.1	Reliable Time Stamps
	FPT_TST_EXT.1	Extended: TSF Testing
	FPT_TUD_EXT.1	Extended: Trusted Update
FTA: TOE Access	FTA_SSL_EXT.1	TSF-initiated Session Locking
	FTA_SSL.3	TSF-initiated Termination
	FTA_SSL.4	User-initiated Termination
	FTA_TAB.1	Default TOE Access Banners
FTP: Trusted path/channels	FTP_ITC.1	Inter-TSF trusted channel
	FTP_ITC.1/MACSEC	Inter-TSF Trusted Channel (MACsec Communications)
	FTP_TRP.1/Admin	Trusted Path

## 5.3 SFRs from NDcPP and MOD\_MACSEC

### 5.3.1 Security audit (FAU)

#### 5.3.1.1 FAU\_GEN.1 Audit data generation

**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 administrator 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 15.*

**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 15.*

5.3.1.2 FAU\_GEN.1/MACSEC Audit Data Generation (MACSEC)

**FAU\_GEN.1.1/MACSEC** The TSF shall be able to generate an audit record of the following auditable events:

- a) Start-up and shut-down of the audit functions
- b) All auditable events for the *[not specified]* level of audit;
- c) **All administrative actions;**
- d) ***[Specifically defined auditable events listed in the Auditable Events table (Table 15)]***

**FAU\_GEN.1.2/MACSEC** The TSF shall record within each audit record at least the following information:

- a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- b) For each audit event type, based on the auditable event definitions of the functional components included in the PP-Module/ST, *[information specified in column three of the Auditable Events table (Table 15)]*.

**Table 15 Auditable Events**

SFR	Auditable Event	Additional Audit Record 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.
FCS_COP.1/DataEncryption	None.	None.
FCS_COP.1/SigGen	None.	None.
FCS_COP.1/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.
FCS_MACSEC_EXT.1	Session establishment	Secure Channel Identifier (SCI)
FCS_MACSEC_EXT.3	Creation and update of SAK	Creation and update times
FCS_MACSEC_EXT.4	Creation of CA	Connectivity Association Key Names (CKNs)
FCS_RBG_EXT.1	None.	None.

SFR	Auditable Event	Additional Audit Record Contents
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure.
FCS_TLSC_EXT.1	Failure to establish an TLS session	Reason for failure.
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address)
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address)
FIA_UAU_EXT.2	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
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.
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_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_RPL.1	Detected replay attempt	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_TUD_EXT.1	Initiation of update. result of the update attempt (success or failure)	None.

SFR	Auditable Event	Additional Audit Record Contents
FPT_TST_EXT.1	None.	None.
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	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_TAB.1	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.

#### 5.3.1.3 FAU\_GEN.2 User Identity Association

**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.

#### 5.3.1.4 FAU\_STG\_EXT.1 Protected Audit Event Storage

**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.

**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,

**FAU\_STG\_EXT.1.3** The TSF shall [overwrite previous audit records according to the following rule: [oldest audit records are overwritten]] when the local storage space for audit data is full.

### 5.3.2 Cryptographic Support (FCS)

#### 5.3.2.1 FCS\_CKM.1 Cryptographic Key Generation

**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.

*] and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list*



*of standards].*

#### 5.3.2.2 FCS\_CKM.2 Cryptographic Key Establishment

**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 meets the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography".] ~~that meets the following: [assignment: list of standards].~~

#### 5.3.2.3 FCS\_CKM.4 Cryptographic Key Destruction

**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.*

#### 5.3.2.4 FCS\_COP.1/DataEncryption Cryptographic Operation (AES Data Encryption/Decryption)

**FCS\_COP.1.1/DataEncryption** The TSF shall perform *encryption/decryption* in accordance with a specified cryptographic algorithm *AES used in [CBC, 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, GCM as specified in ISO 19772].*

#### 5.3.2.5 FCS\_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)

**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 bits, 3072 bits],

]-and cryptographic key sizes [assignment: cryptographic key sizes]

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,

].

#### 5.3.2.6 FCS\_COP.1/Hash Cryptographic Operation (Hash Algorithm)

**FCS\_COP.1.1/Hash** The TSF shall perform *cryptographic hashing services* in accordance with a specified cryptographic algorithm [SHA1, SHA-256, SHA-384, SHA-512] and cryptographic key sizes [~~assignment: cryptographic key sizes~~] and message digest sizes [160, 256, 384, 512] bits that meet the following: *ISO/IEC 10118-3:2004*.

#### 5.3.2.7 FCS\_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)

**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, implicit] and cryptographic key sizes [160-bit, 256-bit, 512-bit] and message digest sizes [160, 256, 384, 512] bits that meet the following: *ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"*.

#### 5.3.2.8 FCS\_COP.1/CMAC Cryptographic Operation (AES-CMAC Keyed Hash Algorithm)

**FCS\_COP.1.1/CMAC** The TSF shall perform [*keyed-hash message authentication*] in accordance with a specified cryptographic algorithm [AES-CMAC] and cryptographic key sizes [128, 256] bits and message digest size of 128 bits that meets the following: [*NIST SP 800-38B*].

#### 5.3.2.9 FCS\_COP.1/MACSEC Cryptographic Operation (MACsec AES Data Encryption and Decryption)

**FCS\_COP.1.1/MACSEC** The TSF shall perform [*encryption and decryption*] in accordance with a specified cryptographic algorithm [AES used in AES Key Wrap, GCM] and cryptographic key sizes [128 bits, 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].

#### 5.3.2.10 FCS\_MACSEC\_EXT.1 MACsec

**FCS\_MACSEC\_EXT.1.1** The TSF shall implement MACsec in accordance with IEEE Standard 802.1AE-2018.

**FCS\_MACSEC\_EXT.1.2** The TSF shall derive a Secure Channel Identifier (SCI) from a peer's MAC address and port to uniquely identify the originator of an MPDU.

**FCS\_MACSEC\_EXT.1.3** The TSF shall reject any MPDUs during a given session that contain an SCI other than the one used to establish that session.

**FCS\_MACSEC\_EXT.1.4** The TSF shall permit only EAPOL (Port Access Entity (PAE) EtherType 88-8E), MACsec frames (EtherType 88-E5), and [*EtherType 0x876F*] and shall discard others.

#### 5.3.2.11 FCS\_MACSEC\_EXT.2 MACsec Integrity and Confidentiality

**FCS\_MACSEC\_EXT.2.1** The TOE shall implement MACsec with support for integrity protection with a confidentiality offset of [0, 30, 50].

**FCS\_MACSEC\_EXT.2.2** The TSF shall provide assurance of the integrity of protocol data units (MPDUs) using an Integrity Check Value (ICV) derived with the SAK.

**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.

#### 5.3.2.12 FCS\_MACSEC\_EXT.3 MACsec Randomness

**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.

**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.

#### 5.3.2.13 FCS\_MACSEC\_EXT.4 MACsec Key Usage

**FCS\_MACSEC\_EXT.4.1** The TSF shall support peer authentication using pre-shared keys (PSKs), [no other method].

**FCS\_MACSEC\_EXT.4.2** The TSF shall distribute SAKs between MACsec peers using AES key wrap as specified in FCS\_COP.1/MACSEC.

**FCS\_MACSEC\_EXT.4.3** The TSF shall support specifying a lifetime for CAKs.

**FCS\_MACSEC\_EXT.4.4** The TSF shall associate Connectivity Association Key Names (CKN) with SAKs that are defined by the KDF using the CAK as input data (per IEEE 802.1X, section 9.8.1).

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

#### 5.3.2.14 FCS\_MKA\_EXT.1 MACsec Key Agreement

**FCS\_MKA\_EXT.1.1** The TSF shall implement Key Agreement Protocol (MKA) in accordance with IEEE 802.1X-2010 and 802.1Xbx-2014.

**FCS\_MKA\_EXT.1.2** The TSF shall provide assurance of the integrity of MKA protocol data units (MKPDUs) using an Integrity Check Value (ICV) derived from an Integrity Check Value Key (ICK).

**FCS\_MKA\_EXT.1.3** The TSF shall provide the ability to derive an Integrity Check Value Key (ICK) from a CAK using a KDF.

**FCS\_MKA\_EXT.1.4** The TSF shall enforce an MKA Lifetime Timeout limit of 6.0 seconds and [MKA Hello Time limit of 2 seconds].

**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 that are PSKs

].

**FCS\_MKA\_EXT.1.6** The key server shall distribute a fresh SAK whenever a member is added to or removed from the live membership of the CA.

**FCS\_MKA\_EXT.1.7** The TSF shall validate MKPDUs according to IEEE 802.1X-2010 Section 11.11.2. In particular, the TSF shall discard without further processing any MKPDUs to which any of the following conditions apply:

- a) The destination address of the MKPDU was an individual address
- b) The MKPDU is less than 32 octets long

- c) The MKPDU comprises fewer octets than indicated by the Basic Parameter Set body length, as encoded in bits 4 through 1 of octet 3 and bits 8 through 1 of octet 4, plus 16 octets of ICV
- d) The CAK Name is not recognized

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

- a) If the Algorithm Agility parameter identifies an algorithm that has been implemented by the receiver, the ICV shall be verified as specified in IEEE 802.1X-2010 Section 9.4.1.
- b) If the Algorithm Agility parameter is unrecognized or not implemented by the receiver, its value can be recorded for diagnosis but the received MKPDU shall be discarded without further processing.

Each received MKPDU that is validated as specified in this clause and verified as specified in IEEE 802.1X-2010 section 9.4.1 shall be decoded as specified in IEEE 802.1X-2010, section 11.11.4.

#### 5.3.2.15 FCS\_RBG\_EXT.1 Random Bit Generation

**FCS\_RBG\_EXT.1.1** The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [HMAC\_DRBG (any)].

**FCS\_RBG\_EXT.1.2** The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [1 platform based noise source] with a minimum of [256 bits] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.

#### 5.3.2.16 FCS\_SSHS\_EXT.1 SSH Server Protocol

**FCS\_SSHS\_EXT.1.1** The TSF shall implement the SSH protocol in accordance with: RFCs 4251, 4252, 4253, 4254 [4256, 5647, 5656, 6668, 8308 section 3.1, 8332].

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

**FCS\_SSHS\_EXT.1.3** The TSF shall ensure that, as described in RFC 4253, packets greater than [1,262,144] bytes in an SSH transport connection are dropped.

**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-gcm@openssh.com, aes256-gcm@openssh.com].

**FCS\_SSHS\_EXT.1.5** The TSF shall ensure that the SSH public-key based authentication implementation uses [rsa-sha2-256, rsa-sha2-512] as its public key algorithm(s) and rejects all other public key algorithms.

**FCS\_SSHS\_EXT.1.6** The TSF shall ensure that the SSH transport implementation uses [hmac-sha2-256, hmac-sha2-512, implicit] as its MAC algorithm(s) and rejects all other MAC algorithm(s).

**FCS\_SSHS\_EXT.1.7** The TSF shall ensure that [ecdh-sha2-nistp256] and [ecdh-sha2-nistp384, ecdh-sha2-nistp521] are the only allowed key exchange methods used for the SSH protocol.

**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.

#### 5.3.2.17 FCS\_TLSC\_EXT.1 TLS Client Protocol

**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\_RSA\_WITH\_AES\_128\_CBC\_SHA as defined in RFC 3268
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA as defined in RFC 3268

]

and no other ciphersuites.

**FCS\_TLSC\_EXT.1.2** The TSF shall verify that the presented identifier matches: [the reference identifiers defined in RFC 6125 section 6 and no other attribute types].

**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].

**FCS\_TLSC\_EXT.1.4** The TSF shall [not present the Supported Elliptic Curves/Supported Groups Extension] in the Client Hello.

### 5.3.3 Identification and authentication (FIA)

#### 5.3.3.1 FIA\_AFL.1 Authentication Failure Management

**FIA\_AFL.1.1** The TSF shall detect when an Administrator configurable positive integer within [1 to 24] unsuccessful authentication attempts occur related to *Administrators attempting to authenticate remotely using a password*.

**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].

#### 5.3.3.2 FIA\_PMG\_EXT.1 Password Management

**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 [8] and [253] characters.

#### 5.3.3.3 FIA\_PSK\_EXT.1 Pre-Shared Key Composition

**FIA\_PSK\_EXT.1.1** The TSF shall use PSKs for MKA as defined by IEEE 802.1X-2010, [no other protocols].

**FIA\_PSK\_EXT.1.2** The TSF shall be able to [accept] bit-based PSKs.

#### 5.3.3.4 FIA\_UIA\_EXT.1 User Identification and Authentication

**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].

**FIA\_UIA\_EXT.1.2** The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated action on behalf of that administrative user.

#### 5.3.3.5 FIA\_UAU\_EXT.2 Password-based Authentication Mechanism

**FIA\_UAU\_EXT.2.1** The TSF shall provide a local [password-based] authentication mechanism to perform local administrative user authentication.

#### 5.3.3.6 FIA\_UAU.7 Protected Authentication Feedback

**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**.

#### 5.3.3.7 FIA\_X509\_EXT.1/Rev – X.509 Certificate Validation

**FIA\_X509\_EXT.1.1/Rev** The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation **supporting a minimum path length of three certificates**.
- The certificate 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 [a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3].
- 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.*

**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.

#### 5.3.3.8 FIA\_X509\_EXT.2 – X.509 Certificate Authentication

**FIA\_X509\_EXT.2.1** The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [TLS], and [no additional uses].

**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].

### 5.3.4 Security management (FMT)

#### 5.3.4.1 FMT\_MOF.1/ManualUpdate Management of Security Functions Behavior

**FMT\_MOF.1/ManualUpdate** The TSF shall restrict the ability to enable the functions to perform manual update to Security Administrators.

#### 5.3.4.2 FMT\_MTD.1/CoreData Management of TSF Data

**FMT\_MTD.1/CoreData** The TSF shall restrict the ability to manage the TSF data to Security Administrators.

#### 5.3.4.3 FMT\_MTD.1/CryptoKeys Management of TSF Data

**FMT\_MTD.1.1/CryptoKeys** The TSF shall restrict the ability to manage the cryptographic keys to Security Administrators.

#### 5.3.4.4 FMT\_SMF.1 Specification of Management Functions

**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 [hash comparison] capability prior to installing those updates;*
- *Ability to configure the authentication failure parameters for FIA\_AFL.1;*
  - [
  - *Ability to configure audit behavior (e.g. changes to storage locations for audit; changes to behavior when local audit storage space is full);*
  - *Ability to configure the cryptographic functionality;*
  - *Ability to configure thresholds for SSH rekeying;*
  - *Ability to set the time which is used for time-stamps;*
  - *Ability to configure the reference identifier for the peer;*
  - *Ability to import X.509v3 certificates to the TOE's trusted store;*
  - *Ability to manage the trusted public keys database;*
  - ].

#### 5.3.4.5 FMT\_SMF.1/MACSEC Specification of Management Functions (MACsec)

**FMT\_SMF.1.1/MACSEC** The TSF shall be capable of performing the following management functions **related to MACsec functionality**: [*Ability of a Security Administrator to:*

- *Manage a PSK-based CAK and install it in the device*
- *Manage the key server to create, delete, and activate MKA participants [as specified in IEEE 802.1X-2020, Sections 9.13 and 9.16 (cf. MIB object ieee8021XKayMkaParticipant Entry) and section. 12.2 (cf. function createMKA())]*
- *Specify a lifetime of a CAK*
- *Enable, disable, or delete a PSK-based CAK using [[CLI management commands]]*  
[
- *No other MACsec management functions*

]].

#### 5.3.4.6 FMT\_SMR.2 Restrictions on Security Roles

**FMT\_SMR.2.1** The TSF shall maintain the roles:

- *Security Administrator.*

**FMT\_SMR.2.2** The TSF shall be able to associate users with roles.

**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.

### 5.3.5 Protection of the TSF (FPT)

#### 5.3.5.1 FPT\_APW\_EXT.1 Extended: Protection of Administrator Passwords

**FPT\_APW\_EXT.1.1** The TSF shall store administrative passwords in non-plaintext form.

**FPT\_APW\_EXT.1.2** The TSF shall prevent the reading of plaintext administrative passwords.

#### 5.3.5.2 FPT\_CAK\_EXT.1 Protection of CAK Data

**FPT\_CAK\_EXT.1.1** The TSF shall prevent reading of CAK values by administrators.

#### 5.3.5.3 FPT\_FLS.1 Failure with Preservation of Secure State

**FPT\_FLS.1.1** The TSF shall **fail-secure** when **any of** the following types of failures occur: [*failure of the power-on self-tests, failure of integrity check of the TSF executable image, failure of noise source health tests*].

#### 5.3.5.4 FPT\_RPL.1 Replay Detection

**FPT\_RPL.1.1** The TSF shall detect replay for the following entities: [*MPDUs, MKA frames*].



**FPT\_RPL.1.2** The TSF shall perform [*discarding of the replayed data, logging of the detected replay attempt*] when replay is detected.

5.3.5.5 FPT\_RPL\_EXT.1 Replay Detection for XPN

**FPT\_RPL\_EXT.1.1** The TSF shall support extended packet numbering (XPN) as per IEEE 802.1AE-2018.

**FPT\_RPL\_EXT.1.2** The TSF shall support [GCM-AES-XPN-128, GCM-AES-XPN-256] as per IEEE 802.1AE-2018.

5.3.5.6 FPT\_SKP\_EXT.1: Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)

**FPT\_SKP\_EXT.1.1** The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

5.3.5.7 FPT\_STM\_EXT.1 Reliable Time Stamps

**FPT\_STM\_EXT.1.1** The TSF shall be able to provide reliable time stamps for its own use.

**FPT\_STM\_EXT.1.2** The TSF shall [allow the Security Administrator to set the time].

5.3.5.8 FPT\_TST\_EXT.1: TSF Testing

**FPT\_TST\_EXT.1.1** The TSF shall run a suite of the following self-tests [during initial start-up (on power on), periodically during normal operation] to demonstrate the correct operation of the TSF: [

- *AES Known Answer Test*
- *RSA Signature Known Answer Test (both signature/verification)*
- *RNG/DRBG Known Answer Test*
- *HMAC Known Answer Test*
- *SHA-1/256/512 Known Answer Test*
- *Software Integrity Test*
- *Noise Source Health Tests*

].

5.3.5.9 FPT\_TUD\_EXT.1 Extended: Trusted Update

**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 [no other TOE firmware/software version].

**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].

**FPT\_TUD\_EXT.1.3** The TSF shall provide a means to authenticate firmware/software updates to the TOE using a [published hash] prior to installing those updates.

### 5.3.6 TOE Access (FTA)

#### 5.3.6.1 FTA\_SSL\_EXT.1 TSF-initiated Session Locking

**FTA\_SSL\_EXT.1.1** The TSF shall, for local interactive sessions, [

- terminate the session]

after a Security Administrator-specified time period of inactivity.

#### 5.3.6.2 FTA\_SSL.3 TSF-initiated Termination

**FTA\_SSL.3.1:** The TSF shall terminate a **remote** interactive session after a *Security Administrator-configurable time interval of session inactivity*.

#### 5.3.6.3 FTA\_SSL.4 User-initiated Termination

**FTA\_SSL.4.1** The TSF shall allow **Administrator**-initiated termination of the **Administrator's** own interactive session.

#### 5.3.6.4 FTA\_TAB.1 Default TOE Access Banners

**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.

### 5.3.7 Trusted Path/Channels (FTP)

#### 5.3.7.1 FTP\_ITC.1 Inter-TSF trusted channel

**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**.

**FTP\_ITC.1.2** The TSF shall permit **the TSF or the authorized IT entities** to initiate communication via the trusted channel.

**FTP\_ITC.1.3** The TSF shall initiate communication via the trusted channel for *[communications with the following:*

- *external audit servers using TLS*

*].*

#### 5.3.7.2 FTP\_ITC.1/MACSEC Inter-TSF Trusted Channel (MACsec Communications)

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

**FTP\_ITC.1.2/MACSEC** The TSF shall permit [the TSE] to initiate communication via the trusted channel.

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

#### 5.3.7.3 FTP\_TRP.1/Admin Trusted Path

**FTP\_TRP.1.1/Admin:** The TSF shall **be capable of using [SSH] 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**.

**FTP\_TRP.1.2/Admin** The TSF shall permit remote Administrators to initiate communication via the trusted path.

**FTP\_TRP.1.3/Admin** The TSF shall require the use of the trusted path for *initial Administrator authentication and all remote administration actions*.

## 5.4 TOE SFR Dependencies Rationale for SFRs Found in PP

The NDcPP v2.2e and MOD\_MACSEC\_V1.0 contain all the requirements claimed in this Security Target. As such the dependencies are not applicable since the PP and EP have been approved.

## 5.5 Security Assurance Requirements

### 5.5.1 SAR Requirements

The TOE assurance requirements for this ST are taken directly from the NDcPP which are derived from Common Criteria Version 3.1, Revision 5. The assurance requirements are summarized in the table below:

**Table 16 Assurance Measures**

Assurance Class	Components	Components Description
Security Target (ASE)	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_REQ.1	Stated security requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE summary specification
Development (ADV)	ADV_FSP.1	Basic Functional Specification
Guidance documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative User guidance
Life cycle support (ALC)	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests (ATE)	ATE_IND.1	Independent testing - conformance
Vulnerability assessment (AVA)	AVA_VAN.1	Vulnerability analysis

### 5.5.2 Security Assurance Requirements Rationale

The Security Assurance Requirements (SARs) in this Security Target represent the SARs identified in the NDcPPv2.2e and MOD\_MACSEC\_V1.0. As such, the NDcPP SAR rationale is deemed acceptable since the PPs have been validated.

## 5.6 Assurance Measures

The TOE satisfies the identified assurance requirements. This section identifies the Assurance Measures applied by Cisco to satisfy the assurance requirements. The table below lists the details.

**Table 17 Assurance Measures**

Component	How requirement is met
ADV_FSP.1	The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes). The development evidence also contains a tracing of the interfaces to the SFRs described in this ST.
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.
AGD_PRE.1	The Installation Guide describes the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.1	The Configuration Management (CM) document(s) describes how the consumer (end-user) of the TOE can identify the evaluated TOE (Target of Evaluation). The CM document(s), identifies the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked, how potential changes are incorporated, and the degree to which automation is used to reduce the scope for error. The TOE will also be provided along with the appropriate administrative guidance.
ALC_CMS.1	
ATE_IND.1	Cisco provides the TOE for testing.
AVA_VAN.1	Cisco provides the TOE for testing.

## 6 TOE Summary Specification

### 6.1 TOE Security Functional Requirement Measures

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

**Table 18 How TOE SFRs Measures**

TOE SFRs	How the SFR is Met
FAU_GEN.1 FAU_GEN.1/MACSEC	<p>The TOE generates an audit record whenever an audited event occurs. The types of events that cause audit records to be generated include: startup and shutdown of the audit mechanism, cryptography related events, identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in the table within the FAU_GEN.1 SFR, "Auditable Events Table").</p> <p>Each of the events is specified in syslog records in enough detail to identify the user for which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred such as generating keys, including the type of key and a key reference. Additionally, the startup and shutdown of the audit functionality is audited.</p> <p>The audit trail consists of the individual audit records; one audit record for each event that occurred. The audit record can contain up to 80 characters and a percent sign (%), which follows the time-stamp information. As noted above, the information includes at least all of the required information. Example audit events are included below:</p> <pre>RP/0/RP0/CPU0:Nov 14 2024 15:44:16.365 EST: exec[67642]: %SECURITY-LOGIN-6-AUTHEN_SUCCESS : Successfully authenticated user 'admin' from 'console' on 'con0_RP0_CPU0'</pre> <p>In the above log events a date and timestamp is displayed as well as an event description.</p> <p>The log buffer is circular, so newer messages overwrite older messages after the buffer is full. Administrators are instructed to monitor the log buffer using the show logging command to view the audit records. The first message displayed is the oldest message in the buffer. There are other associated commands to clear the buffer, to set the logging level, etc.</p> <p>The administrator can set the level of the audit records to be displayed on the console or sent to the syslog server. For instance all emergency, alerts, critical, errors, and warning messages can be sent to the console alerting the administrator that some action needs to be taken as these types of messages mean that the functionality of the TOE is affected. All notifications and information type message can be sent to the syslog server.</p>
FAU_GEN.2	<p>The TOE shall ensure that each auditable event is associated with the user that triggered the event and as a result, they are traceable to a specific user. For example, a human user, user identity or related session ID would be included in the audit record. For an IT entity or device, the IP address, MAC address, host name, or other configured identification is presented. A sample audit record is below:</p>

TOE SFRs	How the SFR is Met																								
	<p>RP/0/RP0/CPU0:Dec 4 2024 14:32:34.459 EST: config[67725]: %MGBL-CONFIG-6-DB_COMMIT : Configuration committed by user 'admin'. Use 'show configuration commit changes 1000000104' to view the changes.</p> <p>RP/0/RP0/CPU0:SPITFIRE(config)#show configuration commit changes 1000000104 Building configuration... !! IOS XR Configuration logging buffered debugging</p> <p>RP/0/RP0/CPU0:Nov 14 2024 15:49:25.467 EST: config[65679]: %MGBL-SYS-5-CONFIG_I : Configured from console by admin</p>																								
FAU_STG_EXT.1	<p>The TOE is a standalone TOE configured to export syslog records to a specified, external syslog server in real-time. The TOE protects communications with an external syslog server via TLS. If the connection fails, the TOE will store audit records on the TOE when it discovers it can no longer communicate with its configured syslog server. When the connection is restored, the TOE will transmit the buffer contents when connected to the syslog server.</p> <p>For audit records stored internally to the TOE the audit records are stored in a circular log file where the TOE overwrites the oldest audit records when the audit trail becomes full. The size of the logging files on the TOE is configurable by the administrator with the minimum value being 2097152 to 125000000 bytes of available disk space.</p> <p>Only Authorized Administrators are able to clear the local logs, and local audit records are stored in a directory that does not allow administrators to modify the contents.</p>																								
FCS_CKM.1	<p>The following table describes the key generation algorithms the TOE implements to generate asymmetric keys:</p>																								
FCS_CKM.2	<table border="1" data-bbox="646 1224 1469 1381"> <thead> <tr> <th>Scheme</th> <th>Standard</th> <th>Key Size/ NIST Curve</th> <th>SFR</th> <th>Service</th> </tr> </thead> <tbody> <tr> <td>RSA</td> <td>FIPS PUB 186-4</td> <td>2048 3072</td> <td>FCS_SSHS_EXT.1</td> <td>SSH Remote Administration</td> </tr> </tbody> </table> <p>The following table shows the key generation algorithms the TOE implements to generate asymmetric keys used for <b>key establishment</b>:</p> <table border="1" data-bbox="646 1495 1469 1680"> <thead> <tr> <th>Scheme</th> <th>Standard</th> <th>Key Size/ NIST Curve</th> <th>SFR</th> <th>Service</th> </tr> </thead> <tbody> <tr> <td>ECC</td> <td>FIPS PUB 186-4</td> <td>P-256 P-384 P-521</td> <td>FCS_SSHS_EXT.1</td> <td>SSH Remote Administration</td> </tr> </tbody> </table> <p>The following table shows the methods the TOE implements for <b>key establishment</b>:</p> <table border="1" data-bbox="646 1768 1469 1824"> <thead> <tr> <th>Scheme</th> <th>Standard</th> <th>SFR</th> <th>Service</th> </tr> </thead> <tbody> </tbody> </table>	Scheme	Standard	Key Size/ NIST Curve	SFR	Service	RSA	FIPS PUB 186-4	2048 3072	FCS_SSHS_EXT.1	SSH Remote Administration	Scheme	Standard	Key Size/ NIST Curve	SFR	Service	ECC	FIPS PUB 186-4	P-256 P-384 P-521	FCS_SSHS_EXT.1	SSH Remote Administration	Scheme	Standard	SFR	Service
Scheme	Standard	Key Size/ NIST Curve	SFR	Service																					
RSA	FIPS PUB 186-4	2048 3072	FCS_SSHS_EXT.1	SSH Remote Administration																					
Scheme	Standard	Key Size/ NIST Curve	SFR	Service																					
ECC	FIPS PUB 186-4	P-256 P-384 P-521	FCS_SSHS_EXT.1	SSH Remote Administration																					
Scheme	Standard	SFR	Service																						

TOE SFRs	How the SFR is Met			
	EC-DH	NIST SP 800-56A Revision 3	FCS_SSHS_EXT.1	SSH Remote Administration
	RSA	RFC 3447	FCS_TLSC_EXT.1	Transmit generated audit data to an external IT entity
FCS_CKM.4	<p>The TOE meets all requirements specified in FIPS 140-2 for destruction of keys and Critical Security Parameters (CSPs) when no longer required for use.</p> <p>See Table 19: TOE Key Zeroization in Section 7 Key Zeroization. The information provided in the table includes all of the all secrets, keys and associated values, the description, and the method used to zeroization when no longer required for use.</p> <p>The information is provided in the reference section for ease and readability of all of the all secrets, keys and associated values, their description and zeroization methods.</p>			
FCS_COP.1/DataEncryption	<p>The TOE provides symmetric encryption and decryption capabilities using AES in CBC mode and GCM mode (128 and 256 bits) as described in ISO/IEC 18033-3, ISO/IEC 10116, and ISO/IEC 19772. AES is implemented in the SSH and TLS protocols. Refer to Table 5 for the FIPS validated algorithm certificate numbers.</p>			
FCS_COP.1/SigGen	<p>The TOE provides cryptographic signature services using RSA Digital Signature Algorithm with key size of 2048 or 3072 as specified in FIPS PUB 186-4.</p> <p>The TOE provides cryptographic signatures in support of SSH, TLS and for trusted updates.</p> <p>Refer to Table 5 for the FIPS validated algorithm certificate numbers.</p>			
FCS_COP.1/Hash	<p>The TOE provides cryptographic hashing services using SHA-1, SHA-256, SHA-384, and SHA-512 as specified in ISO/IEC 10118-3:2004 (with key sizes and message digest sizes of 160, 256, 384, and 512 bits respectively).</p>			
FCS_COP.1/KeyedHash	<p>The TOE provides keyed-hashing message authentication services using HMAC-SHA-1, HMAC-SHA-256 that operates on 512-bit blocks and HMAC-SHA-384 and HMAC-SHA-512 operating on 1024-bit blocks of data, with key sizes and message digest sizes of 160 bits, 256 bits, 384 bits, and 512 bits respectively as specified in ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”.</p> <p>SHA-512 hashing is used as part of digital signature verification of software image integrity.</p> <p>The TOE provides SHS hashing and HMAC message authentication in support of SSHv2 and TLSv1.2 for secure communications. Management of the cryptographic algorithms is provided through the CLI with auditing of those commands. SHS hashing and HMAC message authentication (SHA2) is used in the establishment of TLS and SSHv2 sessions.</p> <p>Refer to Table 5 for the FIPS validated algorithm certificate numbers.</p>			



TOE SFRs	How the SFR is Met
<p>FCS_COP.1/CMAC FCS_COP.1/MACSEC</p>	<p>The TOE provides keyed-hash message authentication in accordance with AES-CMAC and cryptographic key sizes 128 and 256 bits with message digest size of 128 bits, block size of 128 bits, and MAC length of 128 bits which meets NIST SP 800-38B.</p> <p>The TOE provides symmetric encryption and decryption capabilities using AES in AES Key Wrap and GCM mode (128 and 256 bits) as described in AES as specified in ISO 18033-3, AES Key Wrap in CMAC mode as specified in NIST SP 800-38F, GCM as specified in ISO 19772. AES is implemented in MACsec protocol.</p> <p>The relevant FIPS certificate numbers are listed in Table 5 FIPS References.</p>
<p>FCS_RBG_EXT.1</p>	<p>The TOE implements an HMAC Deterministic Random Bit Generator (DRBG) as defined in section 10.1.2 of NIST SP 800-90A, using HMAC w/SHA-256 seeded by an entropy source that accumulates entropy from a TSF-platform based noise source.</p> <p>The deterministic RBG is seeded with a minimum of 256 bits of entropy, which is at least equal to the greatest security strength of the keys and hashes that it will generate.</p>
<p>FCS_MACSEC_EXT.1</p>	<p>The TOE implements MACsec in compliance with Institute of Electrical and Electronics Engineers (IEEE) Standard 802.1AE-2018. The MACsec connections maintain confidentiality of transmitted data and takes measures against frames transmitted or modified by unauthorized devices. In addition, the TOE implementation provides configuration options and management of the MACsec functionality.</p> <p>The Secure Channel Identifier (SCI) is composed of a globally unique 48-bit Message Authentication Code (MAC) Address and the Secure System Address (port). The SCI is part of the SecTAG if the Secure Channel (SC) bit is set and will be at the end of the tag. Any MAC Protocol Data Units (MPDUs) during a given session that contain an SCI other than the one used to establish that session is rejected.</p> <p>Only Extensible Authentication Protocol over LAN (EAPOL) (Physical Address Extension (PAE) EtherType 88-8E), MACsec frames (EtherType 88-E5), and EtherType 0x876F are permitted. All others are rejected.</p> <p>The EtherType 0x876F has been officially allocated to Cisco for WAN MACsec use cases.</p>
<p>FCS_MACSEC_EXT.2</p>	<p>The TOE implements the MACsec requirement for integrity protection with the confidentiality offsets of 0, 30 and 50 using the “mka-policy confidentiality-offset” command.</p> <p>An offset value of 0 does not offset the encryption and offset values of 30 and 50 offset the encryption by 30 and 50 characters respectively.</p> <p>An Integrity Check Value (ICV) that is 16 bytes in length is derived with the Secure Association Key (SAK) and is used to provide assurance of the integrity of MPDUs.</p> <p>The TOE derives the ICV from a CAK using KDF, using the SCI as the most significant bits of the IV and the 32 least significant bits of the PN as the IV.</p>

TOE SFRs	How the SFR is Met
FCS_MACSEC_EXT.3	<p>Each SAK is generated using the KDF specified in SP800-108 (KDF Validation System), clause 6.2.1 using the following transform - KS-nonce = a nonce of the same size as the required SAK, obtained from an RNG each time an SAK is generated.</p> <p>The CAK is based on AES cipher in CMAC mode, with key sizes of 128 and 256 bits. Each of the keys used by MKA is derived from the CAK.</p> <p>The key string is the CAK that is used for ICV validation by the MKA protocol. The CAK is not used directly, but derives two further keys from the CAK using the AES cipher in CMAC mode.</p> <p>The derived keys, which are derived via key derivation function as defined in SP800-108 KDF (CMAC) are tied to the identity of the CAK, and thus restricted to use with that particular CAK. These are the ICV Key (ICK) used to verify the integrity of MPDUs and to prove that the transmitter of the MKPDU possesses the CAK, and the Key Encrypting Key (KEK) used by the Key Server, elected by MKA, to transport a succession of SAKs, for use by MACsec, to the other member(s) of a CA.</p> <p>The size of the key is based on the configured AES key sized used. If using AES 128-bit CMAC mode encryption, the key string will be 32-bit hexadecimal in length. If using 256-bit encryption, the key string will be 64-bit hexadecimal in length.</p> <p>The TOE's random bit generator is used for creating unique nonces.</p>
FCS_MACSEC_EXT.4	<p>MACsec peer authentication is achieved by only using pre-shared keys.</p> <p>The SAKs are distributed between these peers using AES Key Wrap. Prior to distribution of the SAKs between these peers, the TOE uses AES Key Wrap GCM with a key size of 128 or 256 bits in accordance with AES as specified in ISO 18033-3, AES Key Wrap in CMAC mode as specified in NIST SP 800-38F, and GCM as specified in ISO 19772.</p> <p>The "key-chain macsec lifetime" key configuration command is used to specify the lifetime for CAKs.</p> <p>The "MACSEC key-chain key" configuration command is used to specify the length of the CKN that is allowed to be between 1 and 32 octets.</p>
FCS_MKA_EXT.1	<p>The TOE implements Key Agreement Protocol (MKA) in accordance with IEEE 802.1X-2010 and 802.1Xbx-2014.</p> <p>An MKA Lifetime Timeout limit of 6.0 seconds and Hello Timeout limit of 2.0 seconds is enforced by the TOE.</p> <p>The TOE discards MKPDUs that do not satisfy the requirements listed under FCS_MKA_EXT.1.7 in Section 5.3.2.14. All valid MKPDUs that meet the requirements as defined under FCS_MKA_EXT.1.7 are decoded in a manner conformant to IEEE 802.1x-2010 Section 11.11.4.</p> <p>On successful peer authentication, a connectivity association is formed between the peers and a secure Connectivity Association Key Name (CKN) is exchanged. After the exchange, the MKA ICV is validated using an Integrity Check Value Key (ICK).</p> <p>For the Data Integrity Check, MACsec uses MKA to generate an Integrity Check Value (ICV) for the frame arriving on the port. If the generated ICV is the same as</p>

TOE SFRs	How the SFR is Met
	<p>the ICV in the frame, then the frame is accepted; otherwise it is dropped. The key string is the Connectivity Association Key (CAK) that is used for ICV validation by the MKA protocol. To ensure the integrity of MACsec frames, the TOE uses a KDF for deriving the ICK from the CAK.</p> <p>The Key Server distributes a SAK by pairwise CAKs.</p>
FCS_SSHS_EXT.1	<p>The TSF implements SSHv2 conformant to RFCs 4251, 4252, 4253, 4254, 4256, 5647, 5656, 6668, 8308 section 3, and 8332 to provide a secure command line interface for remote administration. The TOE implementation of SSHv2 supports the following:</p> <ul style="list-style-type: none"> <li>• TSF’s SSH transport implementation supports the following public-key algorithms for Hostkey authentication: rsa-sha2-512 and rsa-sha2-256.</li> <li>• Local password-based authentication for administrative users accessing the TOE through SSHv2.</li> <li>• When the SSH client presents a public key, the TSF verifies it matches the one configured for the Administrator account. If the presented public key does not match the one configured for the Administrator account, access is denied.</li> <li>• The TSF’s SSH transport implementation supports the following public-key algorithms for both Client Authentication and Hostkey authentication: rsa-sha2-256 and rsa-sha2-512.</li> <li>• Remote CLI SSHv2 sessions are limited to an administrator configurable session timeout period.</li> <li>• Encryption algorithms, aes128-cbc, aes256-cbc, aes128-gcm@openssh.com, and aes256-gcm@openssh.com to ensure confidentiality of the session. <i>Note: When aes*-gcm@openssh.com is negotiated as the encryption algorithm, the MAC algorithm field is ignored and GCM is implicitly used as the MAC.</i></li> <li>• The TOE’s implementation of SSHv2 supports hashing algorithm hmac-sha2-256 and hmac-sha2-512 to ensure the integrity of the session.</li> <li>• The TOE’s implementation of SSHv2 can be configured to only allow ecdh-sha2-nistp256, ecdh-sha2-nistp384, and ecdh-sha2-nistp521 key exchange methods.</li> <li>• Packets greater than 1,262,144 bytes in an SSH transport connection are dropped. Large packets are detected by the SSH implementation, and dropped internal to the SSH process.</li> <li>• The TOE can also be configured to ensure that SSH re-key of no longer than one hour and no more than one gigabyte of transmitted data for the session key. Rekeying is performed upon reaching the threshold that is hit first.</li> </ul> <p>Please refer to Table 5 for all the CAVP references.</p>
FCS_TLSC_EXT.1	<p>The TOE supports TLS v1.2 to protect the sessions to the remote audit server. TLS is also used to protect the TLS sessions with the TOE, which supports the mandatory ciphersuite as well as the following optional ciphersuite:</p> <ul style="list-style-type: none"> <li>• <i>TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268</i></li> <li>• <i>TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268</i></li> </ul> <p>The TOE does not support NIST Curves in the TLS Client Hello.</p>

TOE SFRs	How the SFR is Met
	<p>The TOE will only establish a connection if the peer presents a valid certificate during the handshake.</p> <p>Where the TOE is the client, such as connecting to the remote syslog server, the handshake above is the same process except the server (remote syslog server) would not request the client certificate in the Server Hello, see the following:</p> <div data-bbox="646 520 1383 1381" style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <pre> sequenceDiagram     participant Client     participant Server     Note over Client: Client Hello Client sends the server the version of TLS it would like to use along with supported cipher. The client also sends a random string to be used later in the negotiation     Client-&gt;&gt;Server:      Note over Server: Server Hello The server sends the TLS version and cipher that will be used. The server also sends a random string that will be used by the client later in the session. The server sends its certificate; proof of identification and 'done'     Server--&gt;&gt;Client:      Note over Client: Client sends secret that was generated using the random strings that is encrypted with the public key from the server's certificate. The client lets the server know that all messages will now be encrypted and 'finished'     Client-&gt;&gt;Server:      Note over Server: The server sends a message to the client that all messages will now be encrypted using the keys that were negotiated and 'finished'.     Server--&gt;&gt;Client:      Note over Client: data     Note over Server: data     Client &lt;--&gt; Server: data             </pre> </div> <p>Any session where the server offers the following in the server hello: SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1 will be rejected by the TOE (client). Certificate pinning is not supported.</p> <p>The TOE supports Subject Alternative Name (SAN) and Common Name (CN) “the reference identifiers” for a successful connection. SANs contain one or more alternate names and uses any variety of name forms for the entity that is bound by the Certificate Authority (CA) to the certified public key. Possible names include:</p> <ul style="list-style-type: none"> <li>• DNS name</li> </ul>
FIA_AFL.1	<p>The TOE provides the privileged administrator the ability to specify the maximum number of unsuccessful authentication attempts before privileged administrator or non-privileged administrator is locked out through the administrative CLI using a privileged CLI command. While the TOE supports a range from 1-24, in the evaluated configuration, the maximum number of failed attempts is recommended to be set to 3.</p>

TOE SFRs	How the SFR is Met
	<p>Once the remote user is locked out, their account will not be accessible until the configured timer for lockout has been exceeded. Once the lockout time is over, then the administrator user can attempt to login again. At no point is administrator access completely unavailable when remote administrators are locked out due to unsuccessful password attempts. Local console access is always available. Administrator lockouts are not applicable to the local console.</p>
FIA_PMG_EXT.1	<p>The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “\$”, “%”, “^”, “&amp;”, “*”, “(”, and “)”). Minimum password length is settable by the Authorized Administrator, and can be configured for minimum password lengths between 8 and 253 characters.</p>
FIA_PSK_EXT.1	<p>The TOE supports use of pre-shared keys for MACsec key agreement protocols. The pre-shared keys are not generated by the TOE, but the TOE accepts the keys in the form of HEX strings. This is done via the CLI configuration command – “key chain &lt;key name&gt; macsec.”</p>
FIA_UIA_EXT.1	<p>The TOE requires all users to be successfully identified and authenticated before allowing any TSF mediated actions to be performed except for the login warning banner that is displayed prior to user authentication.</p>
FIA_UAU_EXT.2	<p>Administrative access to the TOE is facilitated through the TOE’s CLI. The TOE mediates all administrative actions through the CLI. Once a potential administrative user attempts to access the CLI of the TOE through either a directly connected console or remotely through an SSHv2 secured connection, the TOE prompts the user for a username and password. Only after the administrative user presents the correct authentication credentials will access to the TOE administrative functionality be granted. No access is allowed to the administrative functionality of the TOE until an administrator is successfully identified and authenticated.</p> <p>The TOE provides a local password based authentication mechanism for authentication of authorized administrators.</p> <p>The process for authentication is the same for administrative access whether administration is occurring via a directly connected console or remotely via SSHv2 secured connection.</p> <p>At initial login, the administrative user is prompted to provide a username. After the user provides the username, the user is prompted to provide the administrative password associated with the user account. The TOE then either grants administrative access (if the combination of username and password is correct) or indicates that the login was unsuccessful. The TOE does not provide a reason for failure in the cases of a login failure.</p>
FIA_UAU.7	<p>When a user enters their password at the local console, the TOE displays no characters so that the user password is obscured. For remote session authentication, the TOE does not echo any characters as they are entered.</p>

TOE SFRs	How the SFR is Met
FIA_X509_EXT.1/Rev	<p>The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for TLS connections. Public key infrastructure (PKI) credentials are stored securely. The identification and authentication, and authorization security functions protect an unauthorized user from gaining access to the storage.</p>
FIA_X509_EXT.2	<p>The certificate validation checking takes place during the TLS session establishment and at time of import. The TOE conforms to standard RFC 5280 for certificate and path validation. CRLs can be checked for all certs in the chain except the trust anchor. And if any cert is revoked, then the TLS session is rejected.</p> <p>The certificate chain establishes a sequence of trusted certificates, from a peer certificate to the root CA certificate. Within the PKI hierarchy, all enrolled peers can validate the certificate of one another if the peers share a trusted root CA certificate or a common subordinate CA. Each CA corresponds to a trust point. When a certificate chain is received from a peer, the default processing of a certificate chain path continues until the first trusted certificate, or trust point, is reached.</p> <p>Checking is also done for the basicConstraints extension and the CA flag to determine whether they are present and set appropriately. The local certificate that was imported must contain the basic constraints extension with the CA flag set to true, the check also ensures that the key usage extension is present, and the keyEncipherment bit or the keyAgreement bit or both are set. If they are not, the certificate is not accepted. Only one certificate is imported since the only device is a syslog server, so the TOE chooses this certificate. basicConstraints checking is performed at the time of authentication during the connection attempt. If the connection to determine the certificate validity cannot be established, the certificate is not accepted.</p> <p>The administrators can configure a trust chain by importing the CA certificate(s) that signed and issued the server (syslog) certificate. This will tell the TOE which CA certificate(s) to use during the validation process. If the TOE does not find the trusted root CA, the TLS connection to the syslog server will fail.</p> <p>CRLs are used to determine revocation status, and are used during an authentication step. The CRL for the issuer is found in the CDP of the issued certificate. When the TOE is able to contact the CRL distribution point for certificate revocation checking, the TOE will reject the TLS session if the remote trust point's (e.g. syslog server's) certificate has been revoked. If the connection to determine the certificate validity cannot be established, the certificate is not accepted, and the connection will not be established.</p>
FMT_MOF.1/ManualUpdate	<p>The TOE provides administrative users with a CLI to interact with and manage the security functions of the TOE.</p> <p>The term "Authorized Administrator" is used in this ST to refer to any user which has been assigned to a privilege level that is permitted to perform the relevant action; therefore, has the appropriate privileges to perform the requested functions.</p>
FMT_MTD.1/CoreData	<p>Therefore, semi-privileged administrators with only a subset of privileges may also manage and modify TOE data based on the privileges assigned.</p>
FMT_MTD.1/CryptoKeys	<p>The TOE provides the ability for Authorized Administrators to access TOE data, such as user accounts and roles, audit data, audit server information, configuration data, security attributes, X509 certificates, login banners, inactivity timeout values, password complexity setting, TOE updates and session thresholds via the CLI. The TOE restricts the access to manage TSF data that can affect security functions of the TOE to the Authorized Administrator/Security Administrator roles.</p>

TOE SFRs	How the SFR is Met
	<p>Manual software updates can only be done by the authorized administrator through the CLI.</p> <p>The Security Administrators ( Authorized Administrators) can query the software version running on the TOE, and can initiate updates to (replacements of) software images. When software updates are made available by Cisco, the Authorized Administrators can obtain and install those updates.</p> <p>The Security Administrator is able to manage the cryptographic keys (generating keys, importing keys, or deleting keys) that are used in TLS and SSH communications. These keys can be managed via CLI as part of following operations:</p> <ol style="list-style-type: none"> <li>1 TLS public keys, –certificate import/export, Trust store management, delete/zeroize</li> <li>2 SSH public/private keys – generate keypair, import/export public keys, public key-based authentication, delete/zeroize</li> <li>3 MACsec keys – via the CKN and CAK assignments, delete/zeroize</li> </ol>
<p>FMT_SMF.1 FMT_SMT.1/MACSEC</p>	<p>The TOE provides all the capabilities necessary to securely manage the TOE and the services provided by the TOE. The management functionality of the TOE is provided through the TOE CLI. The specific management capabilities available from the TOE include -</p> <ul style="list-style-type: none"> <li>• Local and remote administration of the TOE and the services provided by the TOE via the TOE CLI, as described above;</li> <li>• The ability to manage the warning banner message and content – allows the Authorized Administrator the ability to define warning banner that is displayed prior to establishing a session (note this applies to the interactive (human) users; e.g. administrative users</li> <li>• The ability to manage the time limits of session inactivity which allows the Authorized Administrator the ability to set and modify the inactivity time threshold.</li> <li>• The ability to update the IOS-XR software. The validity of the image is provided using digital signature prior to installing the update</li> <li>• The ability to manage audit behavior and the audit logs which allows the Authorized Administrator to configure the audit logs, view the audit logs, and to clear the audit logs</li> <li>• The ability to manage the cryptographic functionality which allows the Authorized Administrator the ability to identify and configure the algorithms used to provide protection of the data, such as generating the RSA keys to enable SSHv2</li> <li>• The ability to configure the authentication failure parameters for FIA_AFL.1.</li> <li>• The ability to configure thresholds for SSH rekeying.</li> <li>• The ability to set the time which is used for time-stamps.</li> <li>• The ability to configure the reference identifier for the peer.</li> <li>• The ability to import X.509v3 certificates to the TOE’s trusted store.</li> <li>• The ability to manage the trusted public keys database.</li> </ul> <p>Management functionality related to MACsec:</p> <ul style="list-style-type: none"> <li>• The ability to manage a PSK-based CAK and install it in the device;</li> <li>• The ability to manage the Key Server to create, delete, and activate MKA participants as specified in 802.1X, sections 9.13 and 9.16 (cf. MIB object</li> </ul>

TOE SFRs	How the SFR is Met
	<p>ieee8021XKeyMkaParticipantEntry) and section 12.2 (cf. function createMKA());</p> <ul style="list-style-type: none"> <li>• The ability to specify a lifetime of a CAK;</li> <li>• The ability to enable, disable, or delete a PSK-based CAK using a CLI management command.</li> </ul>
FMT_SMR.2	<p>The TOE platform maintains both privileged and semi-privileged administrator roles. The terms “Authorized Administrator” and “Security Administrator” are used interchangeably in this ST to refer to any user that has been assigned to a privilege level that is permitted to perform the relevant action; therefore, has the appropriate privileges to perform the requested functions. The assigned role determines the functions the user can perform; hence the authorized administrator with the appropriate privileges.</p> <p>The TOE supports both local administration via a directly connected console cable and remote administration via SSH.</p>
FPT_CAK_EXT.1	<p>During the setup and configuration of the TOE and the MACsec functionality, the Authorized Administrator issues the command – “password6 encryption aes”. This prevents the CAK value from being shown in clear text to the administrators on the CLI when the “show run” output is displayed.</p> <p>In addition, CAK data is stored in secure directory that is not readily accessible to administrators.</p>
FPT_FLS.1	<p>Whenever a failure occurs within the TOE that results in the TOE ceasing operation, the TOE securely disables its interfaces to prevent the unintentional flow of any information to or from the TOE. The TOE shuts down by reloading and will continue to reload as long as the failures persist. This functionally prevents any failure of power-on self-tests, failure of integrity check of the TSF executable image, failure of noise source health tests from causing an unauthorized information flow. There are no failures that circumvent this protection.</p>
FPT_RPL.1 FPT_RPL_EXT.1	<p>MPDUs are replay protected in the TOE. Per IEEE 802.1AE-2018, each MAC Protocol Data Unit (MPDU) includes a Packet Number (PN) within the SecTag in its header for replay protection. The receiving device checks this PN against expected values and a replay window to detect and reject replayed frames. This mechanism ensures MPDUs are authenticated and protects the integrity of data transmission against replay attacks. The MKA frames are guarded against replay (If a MKPDU with duplicate MN (message number) and not latest MN comes along, then this MKPDU will be dropped and not processed further). MKA frames are checked for replay by checking the MN plus the MI for the participant. Replay data is discarded and logged by the TOE.</p> <p>Extended Packet Numbering (XPN) uses a 64-bit Sequence Number (SN) field and an anti-replay window to detect replayed MPDUs. The device checks the received SN against the anti-replay window of the Inbound Secure Association (SA). If the SN falls outside the window, indicating a replayed frame, the MPDU is discarded. This mechanism ensures that only valid and non-replayed frames are processed, thereby securing the TSF against replay attacks.</p>



TOE SFRs	How the SFR is Met
FPT_SKP_EXT.1 FPT_APW_EXT.1	<p>The TOE stores all private keys in a secure directory that is not readily accessible to administrators. All pre-shared and symmetric keys are stored in a hashed format that are non-readable, hence no interface access.</p> <p>All passwords are obscured via hashing in a secure directory. The passwords are non-readable. In this manner, the TOE ensures that plaintext user passwords will not be disclosed even to administrators. This is provided by default.</p>
FPT_STM_EXT.1	<p>The TOE provides a source of date and time information used in audit event timestamps. The clock function is reliant on the system clock. This date and time is used as the time stamp that is applied to TOE generated audit records and used to track inactivity of administrative sessions account lockout and resumption, cert expiry checks, and MACsec timing operations.</p>
FPT_TUD_EXT.1	<p>An Authorized Administrator can query the software version running on the TOE with the 'show version' command and can initiate updates to software images. When software updates are made available by Cisco, an administrator can obtain and install those updates. The updates can be downloaded from software.cisco.com. The cryptographic hashes (i.e., public hashes/SHA-512) are used to verify software/firmware update files (to ensure they have not been modified from the originals distributed by Cisco) before they are used to update the applicable TOE components.</p> <p>The hash value can be displayed by hovering over the software image name under details on the Cisco.com web site. If the hashes do not match, contact Cisco Technical Assistance Center (TAC).</p> <p>To verify the system software release version at the CLI the command "show version" is used, while the command "show install active" command will display the currently running system image filename and the system software release version.</p>
FPT_TST_EXT.1	<p>The TOE is designed to run a suite of power-on self-tests that comply with the FIPS140-2 requirements for self-test (e.g. known answer tests (KATs) and zeroization tests), during initial start-up to verify its correct operation. If any of the tests fail the security administrator will have to log into the CLI to determine which test failed and why. If the tests pass successfully the router will continue bootup and normal operation.</p> <p>During the system bootup process (power on or reboot), all the Power on Startup Test (POST) components for all the cryptographic modules perform the POST for the corresponding component (hardware or software). These tests include:</p> <ul style="list-style-type: none"> <li>• AES Known Answer Test – For the encrypt test, a known key is used to encrypt a known plain text value resulting in an encrypted value. This encrypted value is compared to a known encrypted value to ensure that the encrypt operation is working correctly. The decrypt test is just the opposite. In this test a known key is used to decrypt a known encrypted value. The resulting plaintext value is compared to a known plaintext value to ensure that the decrypt operation is working correctly.</li> <li>• RSA Signature Known Answer Test (both signature/verification) – This test takes a known plaintext value and Private/Public key pair and used the public key to encrypt the data. This value is compared to a known encrypted value to verify that encrypt operation is working properly. The encrypted data is then</li> </ul>

TOE SFRs	How the SFR is Met
	<p>decrypted using the private key. This value is compared to the original plaintext value to ensure the decrypt operation is working properly.</p> <ul style="list-style-type: none"> <li>• RNG/DRBG Known Answer Test – For this test, known seed values are provided to the DRBG implementation. The DRBG uses these values to generate random bits. These random bits are compared to known random bits to ensure that the DRBG is operating correctly.</li> <li>• HMAC Known Answer Test – For each of the hash values listed, the HMAC implementation is fed known plaintext data and a known key. These values are used to generate a MAC. This MAC is compared to a known MAC to verify that the HMAC and hash operations are operating correctly.</li> <li>• SHA-1/256/512 Known Answer Test – For each of the values listed, the SHA implementation is fed known data and key. These values are used to generate a hash. This hash is compared to a known value to verify they match and the hash operations are operating correctly.</li> <li>• Software Integrity Test – The Software Integrity Test is run automatically whenever the IOS system images is loaded and confirms that the image file that’s about to be loaded has maintained its integrity.</li> <li>• Noise Source Health Tests – The Noise Source Health Tests check the functioning of the Noise Source that supplies randomness to the Entropy Source. The tests are designed to detect failure of the Noise Source. These tests are run at startup and continuously during normal operation.</li> </ul> <p>If any component reports failure for the POST, the system crashes and appropriate information is displayed on the screen, and saved in the crashinfo file.</p> <p>All ports are blocked from moving to forwarding state during the POST. If all components of all modules pass the POST, the system is placed in FIPS PASS state and ports are allowed to forward data traffic.</p> <p>These tests are sufficient to verify that the cryptographic operations are all performing as expected.</p>
FTA_SSL_EXT.1	An administrator can configure maximum inactivity times individually for both local and remote administrative sessions through the use of the “session-timeout” setting applied to the console. When a session is inactive (i.e., no session input from the administrator) for the configured period of time the TOE will terminate the session, and no further activity is allowed requiring the administrator to log in (be successfully identified and authenticated) again to establish a new session. If a remote user session is inactive for a configured period of time, the session will be terminated and will require authentication to establish a new session.
FTA_SSL.3	The allowable inactivity timeout range is from 1 to 65535 seconds.
FTA_SSL.4	An administrator is able to exit out of both local and remote administrative sessions. Each administrator logged onto the TOE can manually terminate their session using the “exit” command.

TOE SFRs	How the SFR is Met
FTA_TAB.1	<p>The TOE displays a privileged Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE. This interface is applicable for both local (via console) and remote (via SSH) TOE administration.</p>
FTP_ITC.1 FTP_ITC.1/MACSEC	<p>The TOE protects communications with the external audit server using TLS to secure the communications channel. TLS uses the keyed hash as defined in FCS_COP.1/KeyedHash and cryptographic hashing functions FCS_COP.1/Hash. This protects the data from modification of data by hashing that verify that data has not been modified in transit. In addition, encryption of the data as defined in FCS_COP.1/DataEncryption is provided to ensure the data is not disclosed in transit.</p> <p>To assure identification of a non-TSF endpoint, the endpoint presents its X.509 certificate. The TOE verifies this certificate to confirm the endpoint's identity, establishing a secure and trusted communication channel.</p> <p>The TOE protects communications between the TOE and the remote audit server using TLS. This provides a secure channel to transmit the log events.</p> <p>MACsec is used to secure communication channels between MACsec peers at Layer 2. The TOE can act as a client or server for MACsec secure channels.</p>
FTP_TRP.1 /Admin	<p>All remote administrative communications take place over a secure encrypted SSHv2 session. The SSHv2 session is encrypted using AES encryption. The remote users are able to initiate SSHv2 communications with the TOE.</p>

## 7 Annex A: Key Zeroization

The following table describes the key zeroization referenced by FCS\_CKM.4 provided by the TOE.

**Table 19 TOE Key Zeroization**

Name	Description of Key	Zeroization
Diffie-Hellman Shared Secret	This is the shared secret used as part of the Diffie-Hellman key exchange in SSH. This key is stored in DRAM (volatile).	Automatically after completion of DH exchange.  Overwritten with: 0x00
Diffie Hellman private exponent	This is the private exponent used as part of the Diffie-Hellman key exchange. This key is stored in DRAM (volatile).	Zeroized upon completion of DH exchange.  Overwritten with: 0x00
MACsec Security Association Key (SAK)	The SAK is used to secure the control plane traffic. This key is stored in internal ASIC register (volatile).	Automatically when MACsec session terminated.  Overwritten with: 0x00
MACsec Connectivity Association Key (CAK)	The CAK secures the control plane traffic. This key is stored in internal ASIC register (volatile).	Automatically when MACsec session terminated.  Overwritten with: 0x00
MACsec Key Encryption Key (KEK)	The Key Encrypting Key (KEK) is used by Key Server, elected by MKA, to transport a succession of SAKs, for use by MACsec, to the other member(s) of a Secure Connectivity Association (CA). This key is stored in internal ASIC register (volatile).	Automatically when MACsec session terminated.  Overwritten with: 0x00
MACsec Integrity Check Key (ICK)	The ICK is used to verify the integrity of MPDUs and to prove that the transmitter of the MKPDU possesses the CAK, This key is stored in internal ASIC register (volatile).	Automatically when MACsec session terminated.  Overwritten with: 0x00
SSH Private Key	Once the function has completed the operations requiring the RSA key object, the module overwrites the entire object (no matter its contents) using memset. This overwrites the key with all 0's. This key is stored in NVRAM (nonvolatile).	Zeroized using the following command: <b># crypto key zeroize rsa</b>  Overwritten with: 0x00
SSH Session Key	Once the function has completed the operations requiring the RSA key object, the module overwrites the entire object (no matter its contents). This is called by the ssh_close function when a session is ended. This key is stored in DRAM (volatile).	Automatically when the SSH session is terminated.  Overwritten with: 0x00
User Password	This is a variable 15+ character password that is used to authenticate local users. The password is stored in NVRAM (nonvolatile).	Zeroized by overwriting with new password
Enable Password (if used)	This is a variable 15+ character password that is used to authenticate local users at a higher privilege level. The password is stored in NVRAM (nonvolatile).	Zeroized by overwriting with new password
RNG Seed Key	This is the seed key for the RNG. The seed key is stored in DRAM (volatile).	Zeroized upon power cycle the device

Name	Description of Key	Zeroization
AES Key	<p>The results are zeroized by overwriting the values with 0x00. This is called by the ssh_close function when a session is ended.</p> <p>This key is stored in DRAM (volatile).</p>	<p>Automatically when the SSH session is terminated.</p> <p>Overwritten with: 0x00</p>
TLS pre-master secret	<p>The pre-master secret is the client and server exchange of random numbers and a special number, the pre-master secret, This pre-master secret is using asymmetric cryptography from which new TLS session keys can be created. The key is stored in SDRAM (volatile).</p>	<p>Automatically after TLS session terminated.</p> <p>The value is overwritten with "0x00."</p>
TLS session encryption key	<p>The session encryption key is unique for each session and is based on the shared secrets that were negotiated at the start of the session. The Key is used to encrypt TLS session data. The key is stored in SDRAM (volatile).</p>	<p>Automatically after TLS session terminated.</p> <p>The value is overwritten with "0x00."</p>
TLS session integrity key	<p>This key is used for TLS data integrity protection. The key is stored in SDRAM (volatile).</p>	<p>Automatically after TLS session terminated.</p> <p>The entire object is overwritten with zeros</p>

## 8 Annex B: NIAP Technical Decisions (TDs)

The following Technical Decisions apply to the NDcPPv2.2e and MOD\_MACSEC\_V1.0:

**Table 20 NIAP Technical Decisions**

TD Identifier	TD Name	Protection Profiles	Publication Date	Applicable?
TD0891	Correlation of Implicitly Satisfied Requirements when CPP_ND_V3.0E is the Base-PP	MOD_MACSEC_V1.0	11/20/2024	Yes
TD0889	Correction For Tests Incorrectly Requiring Group MACsec	MOD_MACSEC_V1.0	10/31/2024	Yes
TD0884	Expansion of Permitted EtherTypes in FCS_MACSEC_EXT.1.4	MOD_MACSEC_V1.0	10/16/2024	Yes
TD0882	MACsec Data Delay Protection, Key Agreement, and Conditional Support for Group CAK	MOD_MACSEC_V1.0	10/28/2024	Yes
TD0881	Correction to MN Usage for FPT_RPL.1 Test	MOD_MACSEC_V1.0	9/20/2024	Yes
TD0870	Security Objectives Rationale for MOD_MACSEC_V1.0	MOD_MACSEC_V1.0	2024.08.08	Yes
TD0840	Alignment of Test 22.1 to FMT_SMF.1/MACSEC	MOD_MACSEC_V1.0	2024.08.14	Yes
TD0826	Aligning MOD_MACSEC_V1.0 with CPP_ND_V3.0E	MOD_MACSEC_V1.0	2024.04.25	Yes
TD0816	Clarity for MACsec Self Test Failure Response	MOD_MACSEC_V1.0	2024.03.22	Yes
TD0803	Clarification for Configurable MACsec CKN Length	MOD_MACSEC_V1.0	10/31/2024	Yes
TD0800	Updated NIT Technical Decision for IPsec IKE/SA Lifetimes Tolerance	CPP_ND_V2.2E	2023.11.13	No, SFRs not claimed
TD0792	NIT Technical Decision: FIA_PMG_EXT.1 - TSS EA not in line with SFR	CPP_ND_V2.2E	2023.09.27	Yes
TD0790	NIT Technical Decision: Clarification Required for testing IPv6	CPP_ND_V2.2E	2023.09.27	Yes
TD0746	Correction to FPT_RPL.1 Test 25	MOD_MACSEC_V1.0	2023.05.29	Yes
TD0738	NIT Technical Decision for Link to Allowed-With List	CPP_ND_V2.2E	2023.05.19	Yes
TD0728	Corrections to MACSec PP-Module SD	MOD_MACSEC_V1.0	2023.04.03	Yes
TD0670	NIT Technical Decision for Mutual and Non-Mutual Auth TLSC Testing	CPP_ND_V2.2E	2022.09.16	No
TD0639	NIT Technical Decision for Clarification for NTP MAC Keys	CPP_ND_V2.2E	2022.08.26	No, SFR not claimed
TD0638	NIT Technical Decision for Key Pair Generation for Authentication	CPP_ND_V2.2E	2022.08.05	Yes
TD0636	NIT Technical Decision for Clarification of Public Key User Authentication for SSH	CPP_ND_V2.2E	2022.03.21	No, SFR not claimed
TD0635	NIT Technical Decision for TLS Server and Key Agreement Parameters	CPP_ND_V2.2E	2022.03.21	No, SFR not claimed
TD0632	NIT Technical Decision for Consistency with Time Data for vNDs	CPP_ND_V2.2E	2022.03.21	Yes
TD0631	NIT Technical Decision for Clarification of public key authentication for SSH Server	CPP_ND_V2.2E	2022.03.21	Yes
TD0592	NIT Technical Decision for Local Storage of Audit Records	CPP_ND_V2.2E	2021.05.21	Yes
TD0591	NIT Technical Decision for Virtual TOEs and hypervisors	CPP_ND_V2.2E	2021.05.21	Yes

TD Identifier	TD Name	Protection Profiles	Publication Date	Applicable?
TD0581	NIT Technical Decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3	CPP_ND_V2.2E	2021.04.09	Yes
TD0580	NIT Technical Decision for clarification about use of DH14 in NDCPPv2.2e	CPP_ND_V2.2E	2021.04.09	Yes
TD0572	NiIT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers	CPP_ND_V2.1, CPP_ND_V2.2E	2021.01.29	Yes
TD0571	NiIT Technical Decision for Guidance on how to handle FIA_AFL.1	CPP_ND_V2.1, CPP_ND_V2.2E	2021.01.29	Yes
TD0570	NiIT Technical Decision for Clarification about FIA_AFL.1	CPP_ND_V2.1, CPP_ND_V2.2E	2021.01.29	Yes
TD0569	NIT Technical Decision for Session ID Usage Conflict in FCS_DTLSS_EXT.1.7	CPP_ND_V2.2E	2021.01.28	No, SFR not claimed
TD0564	NiIT Technical Decision for Vulnerability Analysis Search Criteria	CPP_ND_V2.2E	2021.01.28	Yes
TD0563	NiIT Technical Decision for Clarification of audit date information	CPP_ND_V2.2E	2021.01.28	Yes
TD0556	NIT Technical Decision for RFC 5077 question	CPP_ND_V2.2E	2020.11.06	No, SFR not claimed
TD0555	NIT Technical Decision for RFC Reference incorrect in TLSS Test	CPP_ND_V2.2E	2020.11.06	No, SFR not claimed
TD0547	NIT Technical Decision for Clarification on developer disclosure of AVA_VAN	CPP_ND_V2.1, CPP_ND_V2.2E	2020.10.15	Yes
TD0546	NIT Technical Decision for DTLS - clarification of Application Note 63	CPP_ND_V2.2E	2020.10.15	No, SFR not claimed
TD0537	The NIT has issued a technical decision for Incorrect reference to FCS_TLSC_EXT.2.3	CPP_ND_V2.2E	2020.07.13	Yes
TD0536	The NIT has issued a technical decision for Update Verification Inconsistency	CPP_ND_V2.1, CPP_ND_V2.2E	2020.07.13	Yes
TD0528	The NIT has issued a technical decision for Missing EAs for FCS_NTP_EXT.1.4	CPP_ND_V2.1, CPP_ND_V2.2E	2020.07.13	No, SFR not claimed
TD0527	Updates to Certificate Revocation Testing (FIA_X509_EXT.1)	CPP_ND_V2.2E	2020.07.01	Yes

## 9 Annex C: References

The following documentation was used to prepare this ST:

**Table 21 References**

Identifier	Description
[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated April 2017, version 3.1, Revision 5
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated April 2017, version 3.1, Revision 5
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, April 2017, version 3.1, Revision 5
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, April 2017, version 3.1, Revision 5
[NDcPP]	collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020
[MOD_MACSEC]	PP-Module for MACsec Ethernet Encryption Version 1.0 (MOD_MACSEC), Version 1.0, March 2, 2023
[800-38A]	NIST Special Publication 800-38A Recommendation for Block 2001 Edition Recommendation for Block Cipher Modes of Operation Methods and Techniques December 2001
[800-56A]	NIST Special Publication 800-56A, March, 2007 Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)
[800-56B]	NIST Special Publication 800-56B Recommendation for Pair-Wise, August 2009 Key Establishment Schemes Using Integer Factorization Cryptography
[FIPS 140-2]	FIPS PUB 140-2 Federal Information Processing Standards Publication Security Requirements for Cryptographic Modules May 25, 2001
[FIPS PUB 186-3]	FIPS PUB 186-3 Federal Information Processing Standards Publication Digital Signature Standard (DSS) June, 2009
[FIPS PUB 186-4]	FIPS PUB 186-4 Federal Information Processing Standards Publication Digital Signature Standard (DSS) July 2013
[FIPS PUB 198-1]	Federal Information Processing Standards Publication The Keyed-Hash Message Authentication Code (HMAC) July 2008
[NIST SP 800-90A Rev 1]	NIST Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators January 2015
[FIPS PUB 180-3]	FIPS PUB 180-3 Federal Information Processing Standards Publication Secure Hash Standard (SHS) October 2008



## 10 Annex D: Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation at:

With CCO login: <http://www.cisco.com/en/US/partner/docs/general/whatsnew/whatsnew.html>

Without CCO login: <http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the What's New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

You can access the most current Cisco documentation on the World Wide Web at the following sites:

<http://www.cisco.com>

### 10.1 Document Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click Feedback in the toolbar and select Documentation. After you complete the form, click Submit to send it to Cisco.

You can e-mail your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc., Document Resource Connection  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

### 10.2 Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at any time, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

<http://www.cisco.com>