Cisco Embedded Services 9300 and 3300 Series Switches (ESS9300 & ESS3300) running IOS-XE 17.15

Security Target

Version: 1.0
Date: March 13, 2026

Table of Contents

List of Tables

List of Figures

Acronyms

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

Table 1. Acronyms

Acronyms/Abbreviations	Definition
AAA	Administration, Authorization, and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
AES-CMAC	Advanced Encryption Standard - Cipher-based Message Authentication Code
AGD	Guidance Document
CAK	Connectivity Association Key
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CC	Common Criteria for Information Technology Security Evaluation
CDP	CRL Distribution Point
CEM	Common Evaluation Methodology for Information Technology Security
CKN	Secure Connectivity Association Key Name
CLI	Command Line Interface
CM	Configuration Management
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CSU	Channel Service Unit
CTR	Counter
CVL	Component Validation List
DH	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
DSU	Data Service Unit
EAP	Extensible Authentication Protocol
ESP	Encapsulating Security Payload
GE	Gigabit Ethernet port
HTTPS	Hyper-Text Transport Protocol Secure
IC2M	IOS Common Cryptographic Module
ICK	Integrity Check Key
ICMP	Internet Control Message Protocol
ICV	Integrity Check Value

IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IOS	Internetworking Operating System
IP	Internet Protocol
IPsec	IP Security
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	Integrated Services Digital Network
ISO	International Organization of Standardization
IT	Information Technology
KCK	Key Confirmation Key
KDF	Key Derivation Function
KEK	Key Encryption Key
KAS	Key Agreement Scheme
KAS-SSC	KAS Shared Secret Computation
KW	Key Wrap
MAC	Media Access Control
MACsec	Media Access Control security
MKA	MACsec Key Agreement Protocol
MKPDU	MACsec Key Agreement Protocol Data Unit
MN	Member Number
MPDU	MAC Protocol Data Unit
NDcPP	collaborative Protection Profile for Network Devices
NIST	National Institute of Standards and Technology
NVRAM	Non-Volatile Random-Access Memory
OCSP	Online Certificate Status Protocol
OS	Operating System
OSI	Open Systems Interconnection
OSP	Organizational Security Policies
PAE	Physical Address Extension
PC	Personal Computer
PKCS	Public Key Cryptographic Standard
PoE	Power over Ethernet
PP	Protection Profile
PRNG	Pseudo Random Number Generator
PSK	Pre-Shared Key
PUB	Publication

RA	Registration Authority
RADIUS	Remote Authentication Dial-In User Service
RFC	Request For Comment
RNG	Random Number Generator
RSA	Rivest, Shamir and Adleman
SA	Security Association
SAK	Security Association Key
SAR	Security Assurance Requirement
SCEP	Simple Certificate Enrollment Protocol
SCI	Secure Channel Identifier
SecTAG	MAC Security TAG
SecY	MAC Security Entity
SFP	Small–form-factor pluggable port
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SNMP	Simple Network Management Protocol
SPD	Security Policy Definition
SSH	Secure Shell
ST	Security Target
TCP	Transport Control Protocol
TD	Technical Decision
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
VPN	Virtual Private Network

Terminology

Table 2. Terminology

Term	Definition
Authorized Administrator	Any user which has been assigned to a privilege level that is permitted to perform all TSF-related functions.
Peer	Another switch on the network that the TOE interfaces with.
Privilege level	Assigns a user specific management access to the TOE to run specific commands. The privilege levels are from 1-15 with 15 having full administrator access to the TOE similar to root access in UNIX or Administrator access on Windows. Privilege level 1 has the most limited access to the CLI. By default, when a user logs in to the Cisco IOS-XE, they will be in user EXEC mode (level 1). From this mode, the administrator has access to some information about the TOE, such as the status of interfaces. However, the administrator can't make any changes or view the running configuration file. The privilege levels are customizable so that an Authorized Administrator can also assign certain commands to certain privilege levels.
MACsec Peer	This includes any MACsec peer with which the TOE participates in MACsec communications. MACsec Peer may be any device that supports MACsec communications
Role	An assigned role gives a user varying access to the management of the TOE. For the purposes of this evaluation the privilege level of user is synonymous with the assigned privilege level.
Security Administrator	Synonymous with Authorized Administrator for the purposes of this evaluation.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
VTY	VTY is a term used by Cisco to describe a single terminal (whereas Terminal is more of a verb or general action term). For configuration purposes VTY defines the line for remote access policies to the switch.

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 Embedded Services 9300 and 3300 Series (ESS9300 & ESS3300). 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.

Revision History

Version	Date	Change
0.1	May 9, 2025	Initial Version
0.2	January 26, 2026	Response to Lab and Validator Comments
1.0	March 13, 2026	Response to Validator Comments

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]
- Annex A: Key Zeroization [Section 7]
- Annex B: References [Section 8]
- Acronyms [Section 9]

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 3. ST and TOE Identification

Name	Description
ST Title	Cisco Embedded Services 9300 and 3300 Series Switches (ESS9300 & ESS3300) running IOS-XE 17.15 Security Target
ST Version	1.0
Publication Date	March 13, 2026
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Embedded Services 9300 and 3300 Series Switches
TOE Hardware Models	ESS-3300-NCP ESS-3300-CON ESS-3300-24T-NCP ESS-3300-24T-CON ESS-9300-10X-E
TOE Software Version	IOS-XE 17.15
Keywords	Switch, Network Appliance, Data Protection, Authentication, Cryptography, Secure Administration, Network Device, MACsec

1.2 TOE Overview

The Cisco Embedded Services 9300 and 3300 Series Switches (herein after referred to as the ESS9300 and ESS3300) are purpose-built, switching platforms that also supports MACsec and IPsec encryption.

Cisco IOS-XE software is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective switching and routing. Although IOS-XE performs many networking functions, this Security Target only addresses the functions that provide for the security of the TOE itself.

The TOE includes the hardware models as defined in **Error! Reference source not found.**.

1.3 TOE Product Type

The TOE is a network device as defined in NDcPP version 3.0e, Functional Package for SSH version 1.0, and pp-Module for MACsec Ethernet Encryption version 1.0.

The ESS9300 and ESS3300 switches are embedded boards in a small form factor optimized to meet specialized form-factor, size, weight, power, port-density, port-media, and ruggedization needs. This allows Cisco partners and integrators to build custom Gigabit Ethernet switching solutions for a range of use cases.

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 4. IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
RADIUS AAA Server	Yes	This includes any IT environment RADIUS AAA server that provides authentication services to TOE Administrators over a secure IPsec trusted channel.
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.
Certification Authority (CA)	Yes	This includes any IT Environment Certification Authority on the TOE network. This can be used to provide the TOE with a valid certificate during certificate enrollment.
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 transmits syslog messages over a secure Internet Protocol security (IPsec) trusted channel.
ESS9300 & ESS3300 Enclosure	Yes	The end user can opt to use an enclosure that accommodates the TOE's size (ESS3300: 3.0 x 3.775 in., ESS9300: 4.3x3.3 in.) and provides no compute capabilities. The TOE functionality is implemented inside the ESS 3300 and 9300 physical chassis, as the chassis includes the underlying board (with or without a cooling plate) and all electronic components attached to it; therefore, no computational capabilities outside of the TOE boundary are required to secure the TOE. During testing, the TOE was enclosed within a Cisco developed hardened enclosure. It is a specially designed enclosure used for Cisco internal testing purposes only. It has no compute capabilities and is not a commercially available product. The enclosure passes network connections directly to the TOE interfaces and does not change or modify TSF functionality. In the evaluated configuration, the enclosures used for testing contain the ESS boards including the integrated multi-pin BTB interface connector with pins

Component	Required	Usage/Purpose Description for TOE performance
		dedicated for power input, ethernet ports, and console ports (two combo Gigabit Ethernet WAN ports, four Gigabit Ethernet LAN ports, and one UART RS232 RJ-45 console port). Refer to Section 1.7 for hardware technical guidance on the ESS boards layout and dimensions and Multi-pin BTB Interface Connector description that includes pinout mapping descriptions for network interfaces and power inputs.

1.5 TOE Description

This section provides an overview of the ESS9300 and ESS3300 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 an industry standard small form factor cards which provide a compact, module, and customizable solution. The hardware models included in the evaluation are: ESS-3300-NCP, ESS-3300-CON, ESS-3300-24T-NCP, ESS-3300-24T-CON and ESS-9300-10X-E. The software is comprised of the Cisco IOS-XE 17.15.

The ESS9300 and ESS3300 models provide secure Layer 2 switching using Enterprise-grade Cisco IOS-XE switching security features to ensure highly secure data communication. The products feature a robust industrial design and support Power over Ethernet.

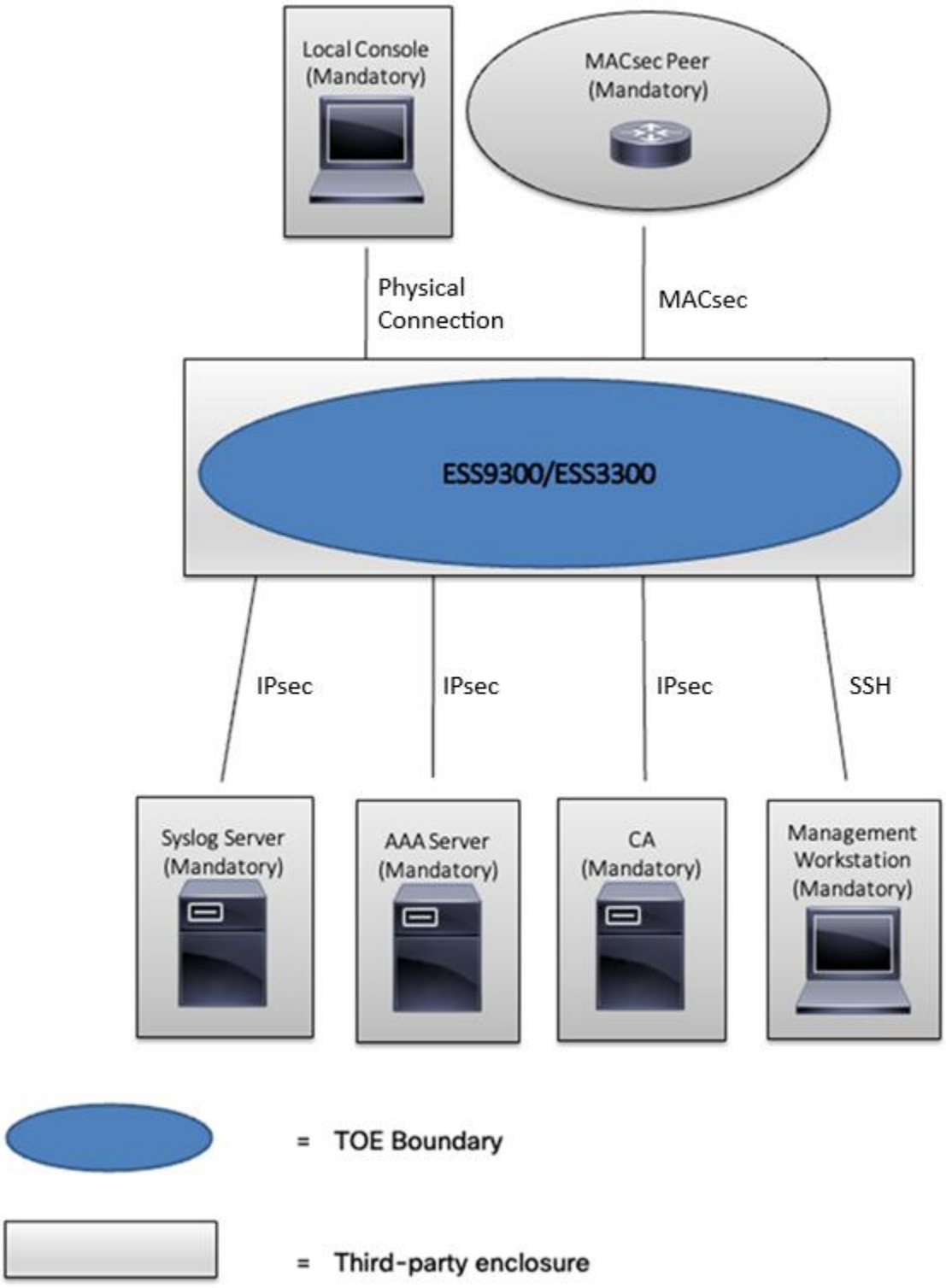
Cisco IOS-XE is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing and switching. Although IOS-XE performs many networking functions, this TOE only addresses the functions that provide for the security of the TOE itself as described in Section 1.8 Logical Scope of the TOE below.

1.6 TOE Evaluated Configuration

Deployment of the TOE in its evaluated configuration consists of at least one TOE switch model following the CC installation and configuration guidance document (AGD). The TOE consists of one or more physical devices as specified in section 1.7 below and includes the Cisco IOS-XE software. The TOE has two or more network interfaces and is connected to at least one internal and one external network. The Cisco IOS-XE configuration determines how packets are handled to and from the TOE's network interfaces. The switch 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.

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

Figure 1. TOE Example Deployment



The previous figure includes the following:

- Examples of TOE Models
- The following are in the IT Environment:
  - Third-party enclosure
  - MACsec Peer
  - Management Workstation
  - RADIUS AAA (Authentication) Server
  - Audit (Syslog) Server
  - Local Console
  - Certification Authority (CA)

NOTE: While the previous figure includes several non-TOE IT environment devices, the TOE is only the ESS9300 and ESS3300 devices. Only one TOE device is required for deployment in an evaluated configuration.

The TOE can be administered interactively using a CLI over a local console connection via the RJ45 serial port or remotely over SSH.

The operational environment of the TOE will include at least one MACsec peer. The environment will also include an audit (syslog) server, a RADIUS server, and a Management Workstation. The syslog server is used to store audit records, where the TOE uses IPsec to secure the transmission of the records. The RADIUS server is used for remote authentication, where the TOE uses IPsec to secure the transmission of data related to remote authentication. The Management Workstation is used for remote management of the TOE by an Administrator, where the TOE uses SSH to secure transmission of management sessions.

1.7 Physical Scope of the TOE

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

- ESS-3300-NCP
- ESS-3300-CON
- ESS-3300-24T-NCP
- ESS-3300-24T-CON
- ESS-9300-10X-E

The network, on which they reside, is considered part of the environment. The software is pre-installed and is comprised of the Cisco IOS-XE software image Release 17.15. In addition, the software image is also downloadable from the Cisco website. A login id and password are required to download the software image. The TOE is comprised of the following physical specifications as described in **Error! Reference source not found.** below:

Table 5. Hardware Models and Specifications

Hardware	Processor	Features
Cisco Embedded Services 3300 Series ESS-3300-NCP ESS-3300-CON ESS-3300-24T-NCP ESS-3300-24T-CON  	Xilinx ZU3EG (ARMv8 Cortex A53) MACsec: Broadcom BCM54194	**Physical dimensions (W x D)** • ESS-3300-NCP: 103mm x 96mm • ESS-3300-16T-NCP: 91mm x 96mm • ESS-3300-CON: 103mm x 96mm • ESS-3300-16T-CON: 91mm x 96mm **Main Board Interfaces*** • 2 1G/10 GE ports (copper or fiber) • 4 1G combo ports** (1G Copper – 1000BaseT/100BaseTX/10Base-T or 1G Fiber SFP 100BASE-X) • 4 1G ports (1G copper – 1000BaseT/100Base-TX/10Base-T) • RS-232 Console Interface • USB 2.0 Console Interface **Expansion Board Interfaces*** • 4 1G combo ports** (1G Copper – 1000BaseT/100BaseTX/10Base-T or 1G Fiber SFP 100BASE-X) • 12 1G ports (1G copper – 1000BaseT/100Base-TX/10Base-T) **Memory** • 4 GB DDR4 DRAM • 4 GB onboard eMMC flash storage **Power** • Power supply – 3.3Vdc and +5Vdc (+/–3%) • Power consumption – 16W * The Interfaces listed above are pin-outs within the integrated board-to-board (BTB) connector. ** A Combo port is a GE port and a SFP port that share the same switch fabric and port number. Each combo port uses different pins and are two different physical ports that can only be used one at a time.

Hardware	Processor	Features
Cisco Catalyst ESS9300 Embedded Series Switch ESS-9300-10X-E 	Cisco Cray64 (ARMv8 Cortex A53) integrated into DopplerGS ASIC MACSec: UADP MSC MACsec embedded in ASICs v1.1	**Physical dimensions (W x D)** • ESS-9300-10X-E: 110 x 85 mm **Board Interfaces*** • 10 ports of 10G /1G (approved SFP+/SFPs) • 1 management port of 10/100/1000BASE-T • RS-232 Console Interface • USB 2.0 Console Interface **Memory** • 4 GB DDR4 DRAM • 8 GB onboard eMMC flash storage (2.5GB usable space) **Power** • Power supply – 3.3VDC and +5VDC (+/–3%) • Power consumption – 35W * The Interfaces listed above are pin-outs within the integrated board-to-board (BTB) connector.

A pinout listing for the I/O and network interface connectors and power requirements can be found in the Cisco Embedded Service 3300 Series Switches Hardware Technical Guide and Cisco Catalyst ESS-9300-10X Embedded Switch Hardware Technical Guide.

Both 100BASE-X and 1000BASE-X SFP transceivers are supported by the eight combo ports, four on the Main Board and four on the Expansion Board. Supported SFP modules can be found in the Cisco Embedded Service 3300 Series Switches Hardware Technical Guide and Cisco Catalyst ESS-9300-10X Embedded Switch Hardware Technical Guide.

The enclosure in which the TOE is inserted provides physical protection for the TOE itself. The TOE is self-contained and does not rely on the enclosure for any ports or connections. The TOE encompasses connectors that provide power and interface connections to external devices and to each other. The enclosure selected can be any off–the- shelf enclosure that supports PC104 or small-factor based cards and provides no computational services. In addition, the enclosure does not provide any access points that would interfere with the security functions provided by the TOE in the evaluated configuration.

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.

1. Security Audit
2. Cryptographic Support
3. Identification and Authentication
4. Security Management
5. Protection of the TSF
6. TOE Access
7. Trusted Path/Channels

These features are described in more detail in the subsections below. In addition, the TOE implements all RFCs of the NDcPP v3.0e and MOD_MACSEC v1.0 as necessary to satisfy testing/assurance measures prescribed therein.

1.8.1 Security Audit

Auditing allows Security Administrators to discover intentional and unintentional issues with the TOE's configuration and/or operation. Auditing of administrative activities provides information that may be used to hasten corrective action should the system be configured incorrectly. Security audit data can also provide an indication of failure of critical portions of the TOE (e.g. a communication channel failure or anomalous activity (e.g. establishment of an administrative session at a suspicious time, repeated failures to establish sessions or authenticate to the TOE) of a suspicious nature.

The TOE provides extensive capabilities to generate audit data targeted at detecting such activity. 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 TOE stores audit messages in a circular audit trail configurable by the Security Administrator. All audit logs are transmitted to an external audit server over a trusted channel protected with IPsec.

1.8.2 Cryptographic Support

The TOE provides cryptographic functions to implement SSH, IPsec, and MACsec protocols. The cryptographic algorithm implementation has been validated for CAVP conformance. This includes key generation and random bit generation, key establishment methods, key destruction, and the various types of cryptographic operations to provide AES encryption/decryption, signature verification, hash generation, and keyed hash generation. A high-level summary of the crypto graphic services provided by the TOE and their uses are shown in Table 6. TOE Cryptography Use below.

Table 6. TOE Cryptography Use

Cryptographic Method	Use within the TOE
Internet Key Exchange	Used to establish initial IPsec session.
Secure Shell Establishment	Used to establish initial SSH session.
RSA Signature Services	Used in IPsec session establishment. Used in SSH session establishment. X.509 certificate signing
NIST SP 800-90A DRBG	Used for random number generation, key generation and seeds to asymmetric key generation Used in IPsec session establishment. Used in SSH session establishment. Used in MACsec session establishment.
SHS	Used to provide IPsec traffic integrity verification Used to provide SSH traffic integrity verification Used for keyed-hash message authentication
AES	Used to encrypt IPsec session traffic. Used to encrypt SSH session traffic. Used to encrypt MACsec traffic.
EC-DH	Used as the Key exchange method for SSH and IPsec

The TOE provides cryptographic support for remote administrative management via SSHv2 and IPsec to secure the transmission of audit records to the remote syslog server. In addition, IPsec is used to secure the session between the TOE and the authentication servers. SSH and IPsec protocols are implemented using the IOS Common Cryptographic Module (IC2M) version Rel5a cryptographic modules.

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 ESS3300 supports MACsec using the Broadcom BCM54194 a fully integrated octal Gigabit transceiver with standard compliant IEEE 802.1AE 256bit MACsec functionality (Cert # AES 4544). The tested environment is AES ECB 128bit & 256bit Encryption/Decryption Engine.

The ESS9300 supports MACsec using the proprietary Unified Access Data Plane (UADP) MSC version 1.1 (Cert. # AES 4848). The MACsec Controller (MSC) is embedded within the ASICs that are utilized within Cisco hardware platforms. The tested environment is Synopsys VCS v2011.12mx-SP1-3.

All the algorithms claimed have CAVP certificates. Refer to Table 7. CAVP Certificates for identification of the relevant CAVP certificates.

Table 7. CAVP Certificates

SFR	Selection	Algorithm	Implementation	Standard	Certificate Number
FCS_CKM.1 – Cryptographic Key Generation	2048 3072 P-256 P-384	RSA ECDSA	IC2M Rel5a	FIPS PUB 186-4	A1462
FCS_CKM.2 – Cryptographic Key Establishment	P-256 P-384	KAS-ECC	IC2M Rel5a	NIST SP 800-56A Rev 3	A1462
FCS_COP.1/DataEncryption – AES Data Encryption/Decryption	AES-CBC-128 AES-CBC-256 AES-GCM-128 AES-GCM-256	AES	IC2M Rel5a	ISO/IEC 18033-3 (AES) ISO/IEC 10116 (CBC) ISO/IEC 19772 (GCM)	A1462
FCS_COP.1/MACSEC Cryptographic Operation (MACsec AES Data Encryption and Decryption)	AES-GCM-128 AES-GCM-256	AES	MACsec	ISO/IEC 18033-3 (AES) ISO/IEC 19772 (GCM)	4544 (ESS3000) 4848 (ESS9300)
FCS_COP.1/MACSEC Cryptographic Operation (MACsec AES Data Encryption andDecryption)	AES-KW 128 bits	AES	IC2M Rel5a	NIST SP 800-38F (AES Key Wrap)	A1462
FCS_COP.1/SigGen – Cryptographic Operation (Signature Generation and Verification)	2048 3072	RSA	IC2M Rel5a	FIPS PUB 186-4	A1462

SFR	Selection	Algorithm	Implementation	Standard	Certificate Number
FCS_COP.1/Hash – Cryptographic Operation (Hash Algorithm)	SHA-1 SHA-256 SHA-384 SHA-512	SHS	IC2M Rel5a	ISO/IEC 10118-3:2004	A1462
FCS_COP.1/KeyedHash – Cryptographic Operation (Keyed Hash Algorithm)	HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	HMAC	IC2M Rel5a	ISO/IEC 9797-2:2011	A1462
FCS_COP.1/CMAC Cryptographic Operation (AES-CMAC Keyed Hash Algorithm)	AES-CMAC 128 bits 256 bits	AES-CMAC	IC2M Rel5a	NIST SP 800-38B	A1462
FCS_RBG_EXT.1– Random Bit Generation	CTR_DRBG (AES) 256 bits	DRBG	IC2M Rel5a	ISO/IEC 18031:2011	A1462

1.8.3 Identification and Authentication

The TOE implements three types of authentications to provide a trusted means for Security Administrators and remote servers/endpoints to securely communicate: X.509v3 certificate-based authentication per RFC 5280 for IPSec connections to remote syslog or RADIUS AAA servers, password-based and public key based (SSH) authentication for Security Administrators, and pre-shared keys for MACsec endpoints.

Security Administrators have the ability to compose strong passwords which are stored using a SHA-2 hash. Additionally, the TOE detects and tracks successive unsuccessful remote authentication attempts and provides an automatic lockout when a user attempts to authenticate and enters invalid information. After a defined number of authentication attempts exceeding the configured allowable attempts within a configured time interval, the user or administrators account is locked out until the configured amount of time has passed.

The TOE provides authentication services for administrative users to connect to the TOE's secure CLI administrator interface. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE provides administrator authentication against a local user database. The TOE supports the use of a RADIUS AAA server (part of the IT Environment) for authentication of administrative users attempting to connect to the TOE's CLI.

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:

- Administer of the TOE locally and remotely;
- Configure the access banner;
- Configure the session inactivity time before session termination or locking;
- Update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates;
- Configure the authentication failure parameters for FIA_AFL.1;
- Configure the number of failed administrator authentication attempts that will cause an account to be locked out;

- Configure audit behavior (e.g. changes to storage locations for audit; changes to behavior when local audit storage space is full);
- Manage the cryptographic keys;
- Configure the cryptographic functionality;
- Configure thresholds for SSH rekeying;
- Configure the lifetime for IPsec SAs;
- Set the time which is used for time-stamps;
- Configure the reference identifier for the peer;
- Manage the TOE's trust store and designate X509.v3 certificates as trust anchors;
- Import X509.v3 certificates to the TOE's trust store;
- Manage the trusted public keys database;
- Manage a PSK-based CAK and install it in the device;
- Manage the Key Server to create, delete, and activate MKA participants [as specified in 802.1X, sections 9.13 and 9.16 (cf. MIB object ieee8021XkayMkaParticipantEntry) and section. 12.2 (cf. function createMKA())];
- Specify a lifetime of a CAK;
- Enable, disable, or delete a PSK-based CAK using CLI management commands.

The TOE supports two separate administrator roles: non-privileged administrator and privileged administrator. Only the privileged administrator can perform the above security relevant management functions. Management of the TSF data is restricted to Security Administrators. The ability to enable, disable, determine and modify the behavior of all of the security functions of the TOE is restricted to authorized administrators.

1.8.5 Protection of the TSF

The TOE protects critical security data including keys and passwords against tampering by untrusted subjects. The TOE prevents reading of cryptographic keys and passwords. The TOE provides reliable timestamps to support monitoring local and remote interactive administrative sessions for inactivity, validating X.509 certificates (to determine if a certificate has expired), and to support accurate audit records.

The TOE provides self-tests to ensure it is operating correctly, including the ability to detect software integrity failures. Additionally, the TOE provides an ability to perform software updates and to verify those software updates are from Cisco Systems, Inc.

Whenever a self-test failure occurs within the TOE, the TOE ceases operation (crashes). In the event of a crash appropriate information is displayed on the console screen and saved in the crashinfo file.

Additionally, Cisco IOS-XE is not a general-purpose operating system and access to Cisco IOS-XE memory space is restricted to only Cisco IOS-XE functions.

1.8.6 TOE Access

The TOE monitors both local and remote admin sessions for inactivity and terminates when a threshold time period is reached. Once a session has been terminated the TOE requires the user to re-authenticate. Sessions can also be terminated by an Authorized Administrator.

The TOE also displays a Security Administrator specified advisory notice and consent warning message prior to initiating identification and authentication for each administrative user.

1.8.7 Trusted path/Channels

The TOE provides encryption (protection from disclosure and detection of modification) for communication paths between itself and remote endpoints.

The TOE allows trusted paths to be established to itself from remote administrators over SSHv2 and initiates outbound IPsec tunnels to transmit audit messages to remote syslog servers. In addition, IPsec is used to secure the session

between the TOE and the authentication servers. The TOE also supports MACsec secured trusted channels between itself and MACsec peers.

In addition, the TOE provides two-way authentication of each endpoint in a cryptographically secure manner, meaning that even if there was a malicious attacker between the two endpoints, any attempt to represent themselves to either endpoint of the communications path as the other communicating party would be detected.

1.9 Excluded Functionality

The following functionality is excluded from the evaluation:

Table 8. Excluded Functionality

Excluded Functionality	Exclusion Rationale
USB console access	USB console access was not tested. The RS-232 RJ45 console port was used during testing.
USB Host interface for USB Flash Memory Device	USB Host interface for USB Flash Memory Device was not tested and is not required.
Transport Layer Security (TLS)	TLS is not associated with Security Functional Requirements claimed in [NDcPP]. Use tunnelling through IPsec.
HTTP/HTTPS	Remote Management is performed using SSH
SNMP	Remote Management is performed using SSH
Telnet	Telnet for management purposes is enabled by default and must be disabled in the evaluated configuration. Remote Management is performed using SSH

These services will be disabled by configuration settings as described in the Guidance documents (AGD). The exclusion of this functionality does not affect compliance to the NDcPP v3.0e, PGK_SSH v1.0, 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 **Error! Reference source not found.** below:

Table 9. Protection Profiles

Protection Profile	Version	Date	Short Name
PP-Configuration for Network Devices and MACsec Ethernet Encryption	2.0	April 25, 2024	CFG_NDcPP-MACsec_V2.0
The PP-Configuration includes the following components:			
• Base-PP: collaborative Protection Profile for Network Devices	3.0e	December 6, 2023	CPP_ND_V3.0E
• PP-Module: PP-Module for MACsec Ethernet Encryption	1.0	March 2, 2023	MOD_MACsec_V1.0
Protection Profile	**Version**	**Date**	**Short Name**
Functional Package for Secure Shell (SSH)	1.0	May 13, 2021	PKG_SSH_V1.0

This ST applies the following NIAP Technical Decisions:

Table 10. NIAP Technical Decisions (TD)

TD Identifier	TD Name	Protection Profiles	Applicable?	Exclusion Rationale
TD0967	Allowance of Kex-strict in PKG_SSH_V1.0	PKG_SSH_V1.0	Yes	
TD0939	Updated Conformance Claims for MOD_MACSEC	MOD_MACSEC_V1.0	Yes	
TD0923	NIT Technical Decision: Auditable event for FAU_STG_EXT.1 in FAU_GEN.1.2	CPP_ND_V3.0E	Yes	
TD0921	NIT Technical Decision: Addition of FIPS PUB 186-5 and Correction of Assignment	CPP_ND_V3.0E	Yes	
TD0909	Updates to FCS_SSH_EXT.1.1 App Note in SSH FP 1.0	PKG_SSH_V1.0	Yes	
TD0900	NIT Technical Decision: Clarification to Local Administrator Access in FIA_UIA_EXT.1.3	CPP_ND_V3.0E	Yes	
TD0899	NIT Technical Decision: Correction of Renegotiation Test for TLS 1.2	CPP_ND_V3.0E	Yes	
TD0891	Correlation of Implicitly Satisfied Requirements when CPP_ND_V3.0E is the Base-PP	MOD_MACSEC_V1.0	Yes	

TD0889	Correction For Tests Incorrectly Requiring Group MACsec	MOD_MACSEC_V1.0	Yes	
TD0886	Clarification to FAU_STG_EXT.1 Test 6	CPP_ND_V3.0E	Yes	
TD0884	Expansion of Permitted EtherTypes in FCS_MACSEC_EXT.1.4	MOD_MACSEC_V1.0	Yes	
TD0882	MACsec Data Delay Protection, Key Agreement, and Conditional Support for Group CAK	MOD_MACSEC_V1.0	Yes	
TD0881	Correction to MN Usage for FPT_RPL.1 Test	MOD_MACSEC_V1.0	Yes	
TD0880	NIT Decision: Removal of Duplicate Selection in FMT_SMF.1.1	CPP_ND_V3.0E	Yes	
TD0879	NIT Decision: Correction of Chapter Headings in CPP_ND_V3.0E	CPP_ND_V3.0E	Yes	
TD0870	Security Objectives Rationale for MOD_MACSEC_V1.0	MOD_MACSEC_V1.0	Yes	
TD0868	NIT Technical Decision: Clarification of time frames in FCS_IPSEC_EXT.1.7 and FCS_IPSEC_EXT.1.8	CPP_ND_V3.0E	Yes	
TD0840	Alignment of Test 22.1 to FMT_SMF.1/MACSEC	MOD_MACSEC_V1.0	Yes	
TD0836	NIT Technical Decision: Redundant Requirements in FPT_TST_EXT.1	CPP_ND_V3.0E	Yes	
TD0826	Aligning MOD_MACSEC_V1.0 with CPP_ND_V3.0E	MOD_MACSEC_V1.0	Yes	
TD0825	Correction to IEEE 802.1X Reference	MOD_MACSEC_V1.0	Yes	
TD0816	Clarity for MACsec Self Test Failure Response	MOD_MACSEC_V1.0	Yes	
TD0803	Clarification for Configurable MACsec CKN Length	MOD_MACSEC_V1.0	Yes	
TD0777	Clarification to Selections for Auditable Events for FCS_SSH_EXT.1	PKG_SSH_V1.0	Yes	
TD0746	Correction to FPT_RPL.1 Test 25	MOD_MACSEC_V1.0	Yes	
TD0732	FCS_SSHS_EXT.1.3 Test 2 Update	PKG_SSH_V1.0	Yes	
TD0728	Corrections to MACSec PP-Module SD	MOD_MACSEC_V1.0	Yes	
TD0695	Choice of 128 or 256 bit size in AES-CTR in SSH Functional Package.	PKG_SSH_V1.0	Yes	
TD0682	Addressing Ambiguity in FCS_SSHS_EXT.1 Tests	PKG_SSH_V1.0	Yes	

2.2.1 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 PP-Module:

- collaborative Protection Profile for Network Devices (NDcPP), Version 3.0e
- PP-Module for MACsec Ethernet Encryption Version 1.0 (MOD_MACSEC), Version 1.0
- Functional Package for Secure Shell (SSH) (PKG_SSH), Version 1.0

2.2.2 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 3.0e, PP-Module for MACsec Ethernet Encryption (MOD_MACSEC) Version 1.0, and Functional Package for Secure Shell (PKG_SSH) Version 1.0 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 v3.0e, MOD_MACSEC v1.0, and PKG_SSH 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.

2.2.3 Statement of Security Requirements Consistency

The Security Functional Requirements included in the Security Target represent the Security Functional Requirements specified in the NDcPP v3.0e, MOD_MACSEC v1.0, and PKG_SSH 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 v3.0e, MOD_MACSEC v1.0, and PKG_SSH v1.0.

3 Security Problem Definition

This section 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.

The security problem definition below has been drawn verbatim from [NDcPP], [MOD_MACSEC], and [Pkg_SSH].

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 11. 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 a 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

Assumption	Assumption Definition
	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 cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).
A.TRUSTED_ADMINISTRATOR	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 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. 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).
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 12. 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.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.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints, e.g. a 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.

Threat	Threat Definition
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 includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.
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	An attacker may send traffic through the TOE that enables them to access devices in the TOE's operational environment without authorization. A MACsec device may sit on the periphery of a network, which means that it may have an externally-facing interface to a public network. Devices located in the public network may attempt to exercise services located on the internal network that are intended to be accessed only from within the internal network or externally accessible only from specifically authorized devices. If the MACsec device allows unauthorized external devices access to the internal network, these devices on the internal network may be subject to compromise. Similarly, if two MACsec devices are deployed to facilitate end-to-end encryption of traffic that is contained within a single network, an attacker could use an insecure MACsec device as a method to access devices on a specific segment of that network such as an individual LAN.

Threat	Threat Definition
T.UNTRUSTED_MACSEC_COMMUNICATION_CHANNELS	An attacker may acquire sensitive TOE or user data that is transmitted to or from the TOE because an untrusted communication channel causes a disclosure of data in transit. A generic network device may be threatened by the use of insecure communications channels to transmit sensitive data. The attack surface of a MACsec device also includes the MACsec trusted channels. Inability to secure communications channels, or failure to do so correctly, would expose user data that is assumed to be secure to the threat of unauthorized disclosure.

3.3 Organizational Security Policies

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

Table 13. 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 Chapter 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 identifies the Security Objectives for 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].

Table 14. 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. The TOE further mitigates this threat originally defined in the Base-PP by defining additional authentication requirements that establish connectivity between authenticated MACsec peers. Addressed by: FCS_MACSEC_EXT.4, FCS_MKA_EXT.1, FIA_PSK_EXT.1, FCS_DEVID_EXT.1 (selection-based), FCS_EAP-TLS_EXT.1 (selection-based)
O.AUTHORIZED_ADMINISTRATION	All network devices are expected to provide services that allow the security functionality of the device to be managed. The MACsec device, as a specific type of network device, has a refined set of management functions to address its specialized behavior. In order to further mitigate the threat of a compromise of its security functionality, the MACsec device prescribes the ability to limit brute-force authentication attempts by enforcing lockout of accounts that experience excessive failures and by limiting access to security-relevant data that administrators do not need to view. Addressed by: FMT_SMF.1/MACSEC, FPT_CAK_EXT.1, FIA_AFL_EXT.1 (optional), FTP_TRP.1/MACSEC (optional), FMT_SNMP_EXT.1 (selection-based)
O.CRYPTOGRAPHIC_FUNCTIONS_MACSEC	To address the issues associated with unauthorized modification and disclosure of information, compliant TOEs will implement cryptographic capabilities. These capabilities are intended to maintain confidentiality and allow for detection and modification of data that is transmitted outside of the TOE. Addressed by: FCS_COP.1/CMAC, FCS_COP.1/MACSEC, FCS_MACSEC_EXT.2, FCS_MACSEC_EXT.3, FTP_ITC.1/MACSEC, FTP_TRP.1/MACSEC (optional), FCS_SNMP_EXT.1 (selection-based)
O.PORT_FILTERING_MACSEC	To further address the issues associated with unauthorized network access, a compliant TOE's port filtering capability will restrict the flow of network traffic through the TOE based on layer 2 frame characteristics and whether or not the traffic represents valid MACsec

TOE Objective	TOE Security Objective Definition
	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. The TOE further mitigates this threat originally defined in the Base-PP by implementing measures to fail securely if any self-test failures occur during startup, ensuring the device only operates when in a known state. Addressed by: FPT_FLS.1

4.2 Security Objectives for the Environment

The following table identifies the Security Objectives for the Environment. 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 [NDcPP] and [MOD_MACSEC].

Table 15. 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.
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	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.

Environment Security Objective	IT Environment Security Objective Definition
	For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.
OE.UPDATES	The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
OE.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.

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], [NDcPP], [MOD_MACSEC], [PKG_SSH], 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 [NDcPP], [MOD_MACSEC], [PKG_SSH], and NIAP Technical Decisions:

- Unaltered SFRs are stated in the form used in [CC2] or their extended component definition (ECD);
- Refinement made in the PP: the refinement text is indicated with **bold text** and ~~strikethroughs~~;
- Selection wholly or partially completed in the PP: the selection values (i.e. the selection values adopted in the PP or the remaining selection values available for the ST) are indicated with underlined text
  - e.g. "[selection: disclosure, modification, loss of use]" in [CC2] or an ECD might become "disclosure" (completion) or "[selection: disclosure, modification]" (partial completion) in the PP;
- Assignment wholly or partially completed in the PP: indicated with *italicized text*;
- Assignment completed within a selection in the PP: the completed assignment text is indicated with *italicized and underlined text*
  - e.g. "[selection: change_default, query, modify, delete, [assignment: other operations]]" in [CC2] or an ECD might become "change_default, *select_tag*" (completion of both selection and assignment) or "[selection: change_default, *select_tag, select_value*]" (partial completion of selection, and completion of assignment) in the PP;
- Iteration: indicated by adding a string starting with "/" (e.g. "FCS_COP.1/Hash").

Formatting conventions outside of operations and iterations matches the formatting specified within the NDcPP v3.0e, MOD_MACSEC v1.0, and PKG_SSH v1.0.

The following conventions were used to resolve conflicting SFRs between NDcPP v3.0e and MOD_MACSEC v1.0:

- All SFRs from MOD_MACSEC reproduced as-is
- SFRs that appear in both NDcPP and MOD_MACSEC are modified based on instructions specified in the MOD_MACSEC
- All SFRs from PKG_SSH reproduced as-is

5.2 TOE Security Functional Requirements

This section identifies the Security Functional Requirements for the TOE. Where operations were completed in the [NDcPP] itself, the formatting used in the [NDcPP] has been retained. Formatting used in [NDcPP], [MOD_MACSEC], and [PKG_SSH} that is inconsistent with the listed conventions has not been retained in the ST.

The TOE Security Functional Requirements are identified in the following table are described in more detail in the following subsections.

Table 16. TOE Security Functional Requirements

Class Name	Component Identification	Component Name	Drawn From
FAU: Security audit	FAU_GEN.1	Audit Data Generation	[NDcPP]
	FAU_GEN.1/MACSEC	Audit Data Generation (MACsec)	[MOD_MACSEC]
	FAU_GEN.2	User identity association	[NDcPP]
	FAU_STG_EXT.1	Protected Audit Event Storage	[NDcPP]
	FCS_CKM.1	Cryptographic Key Generation	[NDcPP]

Class Name	Component Identification	Component Name	Drawn From
FCS: Cryptographic support	FCS_CKM.2	Cryptographic Key Establishment	[NDcPP]
	FCS_CKM.4	Cryptographic Key Destruction	[NDcPP]
	FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/ Decryption)	[NDcPP]
	FCS_COP.1/SigGen	Cryptographic Operation (Signature Generation and Verification)	[NDcPP]
	FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)	[NDcPP]
	FCS_COP.1KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)	[NDcPP]
	FCS_COP.1/CMAC	Cryptographic Operation (AES-CMAC Keyed Hash Algorithm)	[MOD_MACSEC]
	FCS_COP.1/MACSEC	Cryptographic Operation (MACsec AES Data Encryption and Decryption)	[MOD_MACSEC]
	FCS_IPSEC_EXT.1	IPsec Protocol	[NDcPP]
	FCS_MACSEC_EXT.1	MACsec	[MOD_MACSEC]
	FCS_MACSEC_EXT.2	MACsec Integrity and Confidentiality	[MOD_MACSEC]
	FCS_MACSEC_EXT.3	MACsec Randomness	[MOD_MACSEC]
	FCS_MACSEC_EXT.4	MACsec Key Usage	[MOD_MACSEC]
	FCS_MKA_EXT.1	MACsec Key Agreement	[MOD_MACSEC]
	FCS_RBG_EXT.1	Random Bit Generation	[NDcPP]
	FCS_SSH_EXT.1	SSH Protocol	[PKG_SSH]
	FCS_SSHS_EXT.1	SSH Server Protocol	[PKG_SSH]
FIA: Identification and authentication	FIA_AFL.1	Authentication Failure Management	[NDcPP]
	FIA_PMG_EXT.1	Password Management	[NDcPP]
	FIA_PSK_EXT.1	Pre-Shared Key Composition	[MOD_MACSEC]
	FIA_UIA_EXT.1	User Identification and Authentication	[NDcPP]
	FIA_UAU.7	Protected Authentication Feedback	[NDcPP]
	FIA_X509_EXT.1/Rev	X.509 Certificate Validation	[NDcPP]
	FIA_X509_EXT.2	X.509 Certificate Authentication	[NDcPP]
	FIA_X509_EXT.3	X.509 Certificate Requests	[NDcPP]
FMT: Security management	FMT_MOF.1/ManualUpdate	Management of Security Functions Behaviour	[NDcPP]
	FMT_MTD.1/CoreData	Management of TSF Data	[NDcPP]
	FMT_MTD.1/ CryptoKeys	Management of TSF Data	[NDcPP]
	FMT_SMF.1	Specification of Management Functions	[NDcPP]
	FMT_SMF.1/MACSEC	Specification of Management Functions (MACsec)	[MOD_MACSEC]

Class Name	Component Identification	Component Name	Drawn From
	FMT_SMR.2	Restrictions on Security Roles	[NDcPP]
FPT: Protection of the TSF	FPT_APW_EXT.1	Protection of Administrator Passwords	[NDcPP]
	FPT_CAK_EXT.1	Protection of CAK Data	[MOD_MACSEC]
	FPT_FLS.1	Failure with Preservation of Secure State	[MOD_MACSEC]
	FPT_RPL.1	Replay Detection	[MOD_MACSEC]
	FPT_SKP_EXT.1	Protection of TSF Data (for reading of all symmetric keys)	[NDcPP]
	FPT_STM_EXT.1	Reliable Time Stamps	[NDcPP]
	FPT_TST_EXT.1	Extended: TSF Testing	[NDcPP]
	FPT_TUD_EXT.1	Extended: Trusted Update	[NDcPP]
FTA: TOE Access	FTA_SSL_EXT.1	TSF-initiated Session Locking	[NDcPP]
	FTA_SSL.3	TSF-initiated Termination	[NDcPP]
	FTA_SSL.4	User-initiated Termination	[NDcPP]
	FTA_TAB.1	Default TOE Access Banners	[NDcPP]
FTP: Trusted path/channels	FTP_ITC.1	Inter-TSF trusted channel	[NDcPP]
	FTP_ITC.1/MACSEC	Inter-TSF Trusted Channel (MACsec Communications)	[MOD_MACSEC]
	FTP_TRP.1/Admin	Trusted Path	[NDcPP]

5.2.1 Security Audit (FAU)

5.2.1.1 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)];*

d) Specifically defined auditable events listed in Table 17.

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 17*

Table 17. Auditable Events

SFR	Auditable Event	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG_EXT.1	Configuration of local audit settings.	Identity of account making changes to the audit configuration.
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_IPSEC_EXT.1	Failure to establish an IPsec SA.	Reason for failure.
FCS_RBG_EXT.1	None.	None.
FCS_SSH_EXT.1	Failure to establish an SSH session. Establishment of SSH connection Termination of SSH connection session Dropping of packet(s) outside de-fined size limits	Reason for failure and Non-TOE end-point of attempted connection (IP Address) Non-TOE endpoint of attempted connection (IP Address) Non-TOE endpoint of attempted connection (IP Address) Packet size
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.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.
FIA_X509_EXT.3	None.	None.
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.

SFR	Auditable Event	Additional Audit Record Contents
FMT_MTD.1/CoreData	None.	None.
FMT_MTD.1/CryptoKeys	None.	None.
FMT_SMF.1	All management activities of TSF data	None.
FMT_SMR.2	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_STM_EXT.1	Discontinuous changes to time – either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FPT_TUD_EXT.1	Initiation of update. Result of the update attempt (success or failure)	None.
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.	• None • None • Reason for failure
FTP_TRP.1/Admin	• Initiation of the trusted path. • Termination of the trusted path. • Failure of the trusted path functions.	• None • None • Reason for failure

5.2.1.2 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 shutdown of the audit functions;
b) All auditable events for the not specified level of audit; and
c) All administrator actions;
d) Specifically defined auditable events listed in the MACSEC Auditable Events table (Table 18).

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 MACSEC Auditable Events table (Table 18).*

Table 18. MACSEC Auditable Events

SFR	Auditable Event	Additional Audit Record Contents
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)
FPT_RPL.1	Detected replay attempt	None.

5.2.1.3 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.

5.2.1.4 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.
[
- The TOE shall consist of a single standalone component that stores audit data locally,]

FAU_STG_EXT.1.3 The TSF shall maintain a [buffer] of audit records in the event that an interruption of communication with the remote audit server occurs.

FAU_STG_EXT.1.4 The TSF shall be able to store [nonpersistent] audit records locally with a minimum storage size of [4096 bytes].

FAU_STG_EXT.1.5 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.

FAU_STG_EXT.1.6 The TSF shall provide the following mechanisms for administrative access to locally stored audit records [ability to view locally].

5.2.2 Cryptographic Support (FCS)

5.2.2.1 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, 3072-bit*] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3 or FIPS PUB 186-5, "Digital Signature Standard (DSS)", A.1;
- ECC schemes using ‘NIST curves’ [P-256, P-384] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4, or FIPS PUB 186-5, “Digital Signature Standard (DSS)”, Appendix A.2, or ISO/IEC 14888-3, “IT Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms”, Section 6.6 .

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

~~*of standards]*~~.

5.2.2.2 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: [

- Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography".

] ~~that meets the following: [assignment: list of standards].~~

5.2.2.3 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, a new value of the key]];
- 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-pass] overwrite consisting of [zeroes]

  ]

that meets the following: No Standard.

5.2.2.4 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].

5.2.2.5 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

[

- For RSA: [*modulus 2048 bits, modulus 3072 bits*],

]

that meet the following: [

- For RSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 or FIPS PUB 186-5, "Digital Signature Standard (DSS)", Section 5.4 using PKCS #1 v2.2 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,

].

5.2.2.6 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 [SHA-1, 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.

5.2.2.7 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-256, HMAC-SHA-384, HMAC-SHA-512] and cryptographic key sizes [256-bit, 384-bit, 512-bit] and **message digest sizes [256, 384, 512] bits** that meet the following: ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2".

5.2.2.8 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 SP800-38B.**

5.2.2.9 FCS_COP.1/MACSEC Cryptographic Operation (MACsec 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, 256**] **bits** that meet 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**.

5.2.2.10 FCS_IPSEC_EXT.1 Extended: IPSEC

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec architecture as specified in RFC 4301.

FCS_IPSEC_EXT.1.2 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched and discards it.

FCS_IPSEC_EXT.1.3 The TSF shall implement [tunnel mode, transport mode].

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms [AES-CBC-128 (RFC3602), AES-CBC-256 (RFC3602), AES-GCM-128 (RFC 4106), AES-GCM-256 (RFC 4106)] together with a Secure Hash Algorithm (SHA)-based HMAC [HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512].

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [

- IKEv2 as defined in RFC 7296 and [with no support for NAT traversal and [RFC 4868 for hash functions]

].

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [IKEv2] protocol uses the cryptographic algorithms [AES-CBC-128, AES-CBC-256 (specified in RFC 3602), AES-GCM-128, AES-GCM-256 (specified in RFC 5282)].

FCS_IPSEC_EXT.1.7 The TSF shall ensure that [

- IKEv2 SA lifetimes can be configured by an Security Administrator based on
  [
    - length of time, where the time values can configured between [*2 minutes – 24 hours*];

  ].

]

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [

- IKEv2 Child SA lifetimes can be configured by an Security Administrator based on
  [
    - number of bytes
    - length of time, where the time values can be configured between [*2 minutes – 8 hours*];

  ]

FCS_IPSEC_EXT.1.9 The TSF shall generate the secret value x used in the IKE Diffie-Hellman key exchange ("x" in g^x mod p) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least [*128 (for DH Group*

19), 192 (for DH Group 20)] *bits*.

FCS_IPSEC_EXT.1.10 The TSF shall generate nonces used in [IKEv2] exchanges of length [
- at least 128 bits in size and at least half the output size of the negotiated pseudorandom function (PRF) hash

].

FCS_IPSEC_EXT.1.11 The TSF shall ensure that all IKE protocols implement DH Groups [
- [19 (256-bit Random ECP), 20 (384-bit Random ECP)] according to RFC 5114.

].

FCS_IPSEC_EXT.1.12 The TSF shall be able to ensure by default that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [IKEv2 IKE_SA] connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [IKEv2 CHILD_SA] connection.

FCS_IPSEC_EXT.1.13 The TSF shall ensure that all IKE protocols perform peer authentication using [RSA] that use X.509v3 certificates that conform to RFC 4945 and [Pre-shared Keys].

FCS_IPSEC_EXT.1.14 The TSF shall only establish a trusted channel if the presented identifier in the received certificate matches the configured reference identifier, where the presented and reference identifiers are of the following fields and types: [SAN: IP address, SAN: Fully Qualified Domain Name (FQDN)] and [no other reference identifier type].

5.2.2.11 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 [no other frame types] and shall discard others.

5.2.2.12 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.

5.2.2.13 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-2020] 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.

5.2.2.14 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 methods].

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 (CKNs) with SAKs that are defined by the KDF using the CAK as input data (per IEEE 802.1X-2020, section 9.8.1).

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

5.2.2.15 FCS_MKA_EXT.1 MACsec Key Agreement

FCS_MKA_EXT.1.1 The TSF shall implement Key Agreement Protocol (MKA) in accordance with IEEE 802.1X-2020 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 Bounded Hello Time limit of 0.5 seconds].

FCS_MKA_EXT.1.5 The key server shall refresh a SAK when it expires. The Key Server shall distribute a SAK by [

- Pairwise CAK's that are PSK's

].

FCS_MKA_EXT.1.6 The Key Server shall distribute a fresh SAK whenever a member is added to or removed from the live membership of the CA.

FCS_MKA_EXT.1.7 The TSF shall validate MKPDUs according to IEEE 802.1X-2020, Section 11.11.2. In particular, the TSF shall discard without further processing any MKPDUs to which any of the following conditions apply:

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

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

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

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

5.2.2.16 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 [CTR_DRBG (AES)].

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.

5.2.2.17 FCS_SSH_EXT.1 SSH Protocol

FCS_SSH_EXT.1.1 The TOE shall implement SSH acting as a [server] in accordance with that complies with RFCs 4251, 4252, 4253, 4254, [5647, 5656, 6668, 8308, 8332] and [*no other standard*].

FCS_SSH_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods: [

- password, complying with [RFC 4252]
- "publickey" (RFC 4252): [
  - rsa-sha2-256 (RFC 8332)
  - rsa-sha2-512 (RFC 8332)
    ]

] and no other methods.

FCS_SSH_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [65806 bytes] in an SSH transport connection are dropped.

FCS_SSH_EXT.1.4 The TSF shall protect data in transit from unauthorized disclosure using the following mechanisms: [

- aes128-cbc (RFC 4253)
- aes256-cbc (RFC 4253)
- aes128-gcm@openssh.com (RFC 5647)
- aes256-gcm@openssh.com (RFC 5647)

] and no other mechanisms.

FCS_SSH_EXT.1.5 The TSF shall protect data in transit from modification, deletion, and insertion using: [

- hmac-sha2-256 (RFC 6668)
- hmac-sha2-512 (RFC 6688)
- implicit

] and no other mechanisms.

FCS_SSH_EXT.1.6 The TSF shall establish a shared secret with its peer using: [

- ecdh-sha2-nistp256 (RFC 5656)
- ecdh-sha2-nistp384 (RFC 5656)

] and no other mechanisms.

FCS_SSH_EXT.1.7 The TSF shall use SSH KDF as defined in [

- RFC 5656 (Section 4)

] to derive the following cryptographic keys from a shared secret: session keys.

FCS_SSH_EXT.1.8 The TSF shall ensure that [

- a rekey of the session keys,

] occurs when any of the following thresholds are met:

- one hour connection time
- no more than one gigabyte of transmitted data, or
- no more than one gigabyte of received data.

].

5.2.2.18 FCS_SSH_EXT.1 SSH Protocol

FCS_SSHS_EXT.1.1 The TSF shall authenticate itself to its peer (SSH Client) using: [

- ssh-rsa (RFC 4253),
- rsa-sha2-256 (RFC 8332),
- rsa-sha2-512 (RFC 8332)

].

5.2.3 Identification and authentication (FIA)

5.2.3.1 FIA_AFL.1 Authentication Failure Management (Refinement)

FIA_AFL.1.1: The TSF shall detect when an Administrator configurable positive integer with [1-25] 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*].

5.2.3.2 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: [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”[*Additional Special Characters listed in Table 19*]*;*

Table 19. Additional Password Special Characters

Special Character	Name
	Space
;	Semicolon
:	Colon
“	Double Quote
‘	Single Quote
|	Vertical Bar
+	Plus
-	Minus
=	Equal Sign
.	Period
,	Comma
/	Slash
\	Backslash
<	Less Than
>	Greater Than
_	Underscore
`	Grave accent (backtick)
~	Tilde
{	Left Brace

}	Right Brace

b) Minimum password length shall be configurable to between [*1*] and [*127*] characters.

5.2.3.3 FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition

FIA_PSK_EXT.1.1 The TSF shall use PSKs for MKA as defined by IEEE 802.1X-2020, [*IPsec protocols*].

FIA_PSK_EXT.1.2 The TSF shall be able to [accept] bit-based PSKs.

5.2.3.4 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.

FIA_UIA_EXT.1.3 The TSF shall provide the following remote authentication mechanisms [SSH password, SSH public key] and [no other mechanism]. The TSF shall provide the following local authentication mechanisms [password-based].

FIA_UIA_EXT.1.4 The TSF shall authenticate any administrative user's claimed identity according to each authentication mechanism specified in FIA_UIA_EXT.1.3.

5.2.3.5 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**.

5.2.3.6 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 [Certificate Revocation List (CRL) as specified in RFC 5759 Section 5].
- 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.

5.2.3.7 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 [IPsec], 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].

5.2.3.8 FIA_X509_EXT.3 X.509 Certificate Requests

FIA_X509_EXT.3.1 The TSF shall generate a Certificate Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [Common Name, Organization, Organizational Unit, Country].

FIA_X509_EXT.3.2 The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

5.2.4 Security management (FMT)

5.2.4.1 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*.

5.2.4.2 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*.

5.2.4.3 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*.

5.2.4.4 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 remotely;*
- *Ability to configure the access banner;*
- *Ability to configure the session inactivity time before session termination or locking;*
- *Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates;*
- [
  - *Ability to configure local audit behavior (e.g. changes to storage locations for audit; changes to behavior when local audit storage space is full; changes to local audit storage size);*
  - *Ability to modify the behavior of the transmission of audit data to an external IT entity;*
  - *Ability to manage the cryptographic keys;*
  - *Ability to configure the cryptographic functionality;*
  - *Ability to configure thresholds for SSH rekeying;*
  - *Ability to configure the lifetime for IPsec SAs;*
  - *Ability to set the time which is used for time-stamps;*
  - *Ability to configure the reference identifier for the peer;*
  - *Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;*
  - *Ability to generate Certificate Signing Request (CSR) and process CA certificate response;*

- *Ability to administer the TOE locally;*
- *Ability to configure the local session inactivity time before session termination or locking;*
- *Ability to configure the authentication failure parameters for FIA_AFL.1;*
- *Ability to manage the trusted public keys database*

].

5.2.4.5 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 ieee8021XKayMkaParticipantEntry) and section. 12.2 (cf. function createMKA())];*
- *Specify the lifetime of a CAK;*
- *Enable, disable, or delete a PSK-based CAK using [[CLI management commands]];[*
- *No other MACsec management functions]*

].

5.2.4.6 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 remotely*

are satisfied.

5.2.5 Protection of the TSF (FPT)

5.2.5.1 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.

5.2.5.2 FPT_CAK_EXT.1 Protection of CAK Data

FPT_CAK_EXT.1.1 The TSF shall prevent reading of CAK values by administrators.

5.2.5.3 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].

5.2.5.4 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.

5.2.5.5 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.

5.2.5.6 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].

5.2.5.7 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) to verify the integrity of the TOE firmware and software;
- Prior to providing any cryptographic service and [on-demand] to verify correct operation of cryptographic implementation necessary to fulfil the TSF;
- [no other] self-tests [*none*].

to demonstrate the correct operation of the TSF.

FPT_TST_EXT.1.2 The TSF shall respond to [all failures] by [rebooting].

5.2.5.8 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 [digital signature**]** prior to installing those updates.

5.2.6 TOE Access (FTA)

5.2.6.1 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.

5.2.6.2 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*.

5.2.6.3 FTA_SSL.4 User-initiated Termination

FTA_SSL.4.1 The TSF shall allow ~~user~~ **Administrator**-initiated termination of the ~~user's~~ **Administrator**'s own interactive session.

5.2.6.4 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 ~~unauthorised~~ use of the TOE.

5.2.7 Trusted Path/Channels (FTP)

5.2.7.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 Refinement: The TSF shall be capable of using [**IPsec] to** provide a trusted communication channel between itself and ~~another trusted IT product~~ **authorized IT entities supporting the following capabilities: audit server, [authentication 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 ~~modification or~~ disclosure **and detection of modification of the channel data**.

FTP_ITC.1.2 The TSF shall permit [the TSF, **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 *[*

- ***external audit servers using IPsec,***
- ***remote AAA servers using IPsec***

].

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

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

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

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

5.2.7.3 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** ~~user's~~ 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*.

5.3 TOE SFR Dependencies Rationale

The Security Functional Requirements (SFRs) in this Security Target represent the SFRs identified in the NDcPP v3.0e and MOD_MACSEC v1.0. As such, the NDcPP v3.0e and MOD_MACSEC v1.0 SFR dependency rationale is deemed acceptable since the PP has been validated.

5.4 Security Assurance Requirements

5.4.1 SAR Requirements

The TOE assurance requirements for this ST are taken directly from the NDcPP v3.0e, which are derived from Common Criteria Version 3.1, Revision 5, dated April 2017. The assurance requirements are summarized in the table below:

Table 20. Assurance Requirements

Assurance Class	Assurance 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 procedures
Life cycle support (ALC)	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage
	ALC_FLR.2	Flaw Reporting Procedures
Tests (ATE)	ATE_IND.1	Independent testing – conformance
Vulnerability assessment (AVA)	AVA_VAN.1	Vulnerability analysis

5.4.2 Security Assurance Requirements Rationale

The Security Assurance Requirements (SARs) in this Security Target represent the SARs identified in the NDcPP v3.0e. As such, the NDcPP v3.0e rationale is deemed acceptable since the PP has been validated.

5.5 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 21. Assurance Measures

Component	How requirement will be met
ASE_CCL.1 ASE_ECD.1 ASE_INT.1 ASE_OBJ.1 ASE_REQ.1 ASE_SPD.1 ASE_TSS.1	Cisco provided this Security Target document.
ADV_FSP.1	No additional "functional specification" documentation was provided by Cisco to satisfy the Evaluation Activities.
AGD_OPE.1 AGD_PRE.1	Cisco will provide the guidance documents with the ST.
ALC_CMC.1 ALC_CMS.1	Cisco will identify the TOE such that it can be distinguished from other products or versions from the Cisco and can be easily specified when being procured by an end user.
ALC_FLR.2	Cisco will provide the flaw remediation and reporting procedures to document how TOE users can submit security flaw reports to the developer and how the security flaw reports will be appropriately acted upon.
ATE_IND.1	Cisco will provide the TOE for testing.
AVA_VAN.1	Cisco will provide 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 22. How TOE SFRs Are Satisfied

TOE SFRs	How the SFR is Met
FAU_GEN.1 FAU_GEN.1/MACSEC	The TOE generates an audit record whenever an audited event occurs. The types of events that cause audit records to be generated include start-up and shut-down 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 **Error! Reference source not found.** and Table 18. MACSEC Auditable Events above. Each of the events is specified in the audit record is 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 "key name" which is assigned to the "label" of the *crypto* command. Additionally, the start-up and shut-down of the audit functionality is audited. The audit trail consists of the individual audit records; one audit record for each event that occurred. As noted above, the information includes at least all the required information. Additional information can be configured. Following is the audit record format: seq no:timestamp: %facility-severity-MNEMONIC:description (hostname-n) Example audit events are included below: *Aug 24 2024 13:14:25: %CRYPTO-5-SELF_TEST_START: Crypto algorithms release (Rel5a) begin self-test *Aug 24 202413:14:26: %CRYPTO-5-SELF_TEST_END: Crypto algoritms self-test completed successfully All tests passed. The logging buffer size can be configured from a range of 4096 (default) to 2147483647 bytes. It is noted, do not make the buffer size too large because the TOE could run out of memory for other tasks. Use the show memory privileged EXEC command to view the free processor memory on the TOE. However, this value is the maximum available, and the buffer size should not be set to this amount. Configurations changes made with the command-line interface (CLI) can be logged. The administrator can configure the size of the configuration log from 1 to 1000 entries (the default is 100). The AGD details the enabling logging of configuration changes. 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 privileged EXEC 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. 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

TOE SFRs	How the SFR is Met
	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. To configure the TOE to send audit records to a syslog server, the 'logging host' command is used. A maximum of three syslog servers can be configured. The audit records are transmitted using an IPsec tunnel to the syslog server. If communications to the syslog server are lost, the TOE will store all audit records locally and when the connection to the remote syslog server is restored, all stored audit records will be transmitted to the remote syslog server.
FAU_GEN.2	The TOE ensures 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.
FAU_STG_EXT.1	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 IPsec. If the IPsec 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. 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 4096 (default) to 2147483647 bytes of available disk space Refer to the Common Criteria Configuration Guide for command description and usage information. 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.

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td>FCS_CKM.1
FCS_CKM.2</td><td>
The following table describes the key generation algorithms the TOE implements to generate asymmetric keys used for device authentication:
<table>
<tr><th>Scheme</th><th>Standard</th><th>Key Size/ NIST Curve</th><th>SFR</th><th>Service</th></tr>
<tr><td>RSA</td><td>FIPS PUB 186-4</td><td>2048
3072</td><td>FCS_SSH_EXT.1

FCS_SSHS_EXT.1</td><td>SSH Remote Administration</td></tr>
<tr><td></td><td></td><td></td><td>FCS_IPSEC_EXT.1</td><td>Transmit generated audit data to an external IT entity and remote authentication with a RADIUS server</td></tr>
</table>
NOTE: For IPsec authentication, the keys are used to generate certificate signing requests (CSRs) in which the public key is associated with an X.509 certificate.

The following table shows the key generation algorithms the TOE implements to generate asymmetric keys used for key establishment:
<table>
<tr><th>Scheme</th><th>Standard</th><th>Key Size/ NIST Curve</th><th>SFR</th><th>Service</th></tr>
<tr><td>ECC</td><td>FIPS PUB 186-4</td><td>DH Group 19 (P-256)

DH Group 20 (P-384)</td><td>FCS_IPSEC_EXT.1</td><td>Transmit generated audit data to an external IT entity and remote authentication with a RADIUS server</td></tr>
<tr><td></td><td></td><td>P-256
P-384</td><td>FCS_SSH_EXT.1
FCS_SSHS_EXT.1</td><td>SSH Remote Administration</td></tr>
</table>
The following table shows the methods the TOE implements for key establishment:
<table>
<tr><th>Scheme</th><th>Standard</th><th>SFR</th><th>Service</th></tr>
<tr><td>EC-DH</td><td>NIST SP 800-56A Revision 3</td><td>FCS_IPSEC_EXT.1</td><td>Transmit generated audit data to an external IT entity and remote authentication with a RADIUS server</td></tr>
<tr><td></td><td></td><td>FCS_SSH_EXT.1
FCS_SSHS_EXT.1</td><td>SSH Remote Administration</td></tr>
</table>
</td></tr>
</table>

TOE SFRs	How the SFR is Met
FCS_CKM.4	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. See section 7 below for additional details on key zeroization.
FCS_COP.1/DataEncryption	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 IPsec protocols. Refer to Table 7 for the FIPS validated algorithm certificate numbers.
FCS_COP.1/SigGen	The TOE provides cryptographic signature services using an RSA Digital Signature Algorithm with key size of 2048 or 3072 as specified in FIPS PUB 186-4. Refer to Table 7 above for the FIPS validated algorithm certificate numbers.
FCS_COP.1/Hash FCS_COP.1/KeyedHash	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). The TOE provides keyed-hashing message authentication services using 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 256 bits, 384 bits, and 512 bits respectively as specified in ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”. SHA-512 hashing is used for verification of software image integrity. Refer to Table 7. CAVP Certificates above for the FIPS validated algorithm certificate numbers.
FCS_COP.1/CMAC FCS_COP.1/MACSEC	The TSF implements 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. The TSF implements symmetric encryption and decryption capabilities using AES in AES Key Wrap (128 bits) and GCM mode (128 and 256 bits) as described in AES as specified in ISO/IEC 18033-3, AES Key Wrap as specified in NIST SP800-38F, GCM as specified in ISO/IEC 19772. AES is implemented in the MACsec protocol. Refer to Table 7 above for the FIPS validated algorithm certificate numbers.
FCS_IPSEC_EXT.1	The TSF implements IPsec to provide authentication and encryption services to prevent unauthorized viewing or modification of syslog data and authentication data as it travels over the external network. The TSF’s implementation of the IPsec standard (in accordance with the RFCs noted in the SFR) uses the Encapsulating Security Payload (ESP) protocol to provide authentication and encryption supporting the following algorithms: • AES-CBC-128 and AES-CBC-256 with HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 • AES-GCM-128 and AES-GCM-256 The TOE supports both transport and tunnel mode for IPsec communications between the TOE and an external audit server.

TOE SFRs	How the SFR is Met
	The administrator defines the traffic that needs to be protected between two IPsec peers by configuring access lists and applying these access lists to interfaces using crypto map sets. A crypto map set can contain multiple entries, each with a different access list. The crypto map entries are searched in a sequence--the router attempts to match the packet to the access list specified in that entry. When a packet matches a permit entry in a particular access list, and the corresponding crypto map entry is tagged connections are established, if necessary. If the crypto map entry is tagged as ipsec-isakmp, IPsec is triggered. If there is no SA that the IPsec can use to protect this traffic to the peer, IPsec uses IKE to negotiate with the re-mote peer to set up the necessary IPsec SAs on behalf of the data flow. The negotiation uses information specified in the crypto map entry as well as the data flow information from the specific access list entry. Once established, the set of SAs (outbound to the peer) is then applied to the triggering packet and to subsequent applicable packets as those packets exit the Controller. "Applicable" packets are packets that match the same access list criteria that the original packet matched. For example, all applicable packets could be encrypted be-fore being forwarded to the remote peer. The corresponding inbound SAs are used when processing the incoming traffic from that peer. Access lists associated with IPsec crypto map entries also represent the traffic that the Controller needs protected by IPsec. Inbound traffic is processed against crypto map entries. If an unprotected packet matches a permit entry in a particular access list associated with an IPsec crypto map entry, that packet is dropped because it was not sent as an IPsec-protected packet. The traffic matching the permit ACLs would then flow through the IPsec tunnel and be classified as “PROTECTED”. Traffic that does not match a permit ACL in the crypto map, but that is not disallowed by other ACLs on the interface is allowed to BYPASS the tunnel. Traffic that does not match a permit ACL and is also blocked by other non-crypto ACLs on the interface would be DISCARDED. Rules applied to an access control list can be applied to either inbound or outbound traffic. IPsec Internet Key Exchange, also called ISAKMP, is the negotiation protocol that lets two peers agree on how to build an IPsec Security Association (SA). The strength of the symmetric algorithm negotiated to protect the IKEv2 IKE_SA connection is greater than or equal to the strength of the symmetric algorithm negotiated to protect the IKEv2 CHILD_SA connection. The IKE protocols implement Peer Authentication using RSA X.509v3 certificates or pre-shared keys. IKE separates negotiation into two phases: IKEv2 SA and IKEv2 Child SA. The IKEv2 SA creates the first tunnel, which protects later ISAKMP negotiation messages. The key negotiated during the IKEv2 SA enables IKE peers to negotiate IKE v2 Child SA and establishes the IPsec SA to communicate securely. IKE maintains a trusted channel, referred to as a Security Association (SA), between IPsec peers that is also used to manage IPsec connections, including: • The negotiation of mutually acceptable IPsec options between peers (including peer authentication parameters, either signature based or pre-shared key based), • The establishment of additional Security Associations to protect packets flows using Encapsulating Security Payload (ESP), and • The agreement of secure bulk data encryption AES keys for use with ESP. IKEv2 payload data is encrypted using the following cryptographic algorithms:

TOE SFRs	How the SFR is Met
	• AES-CBC-128 and AES-CBC-256 • AES-GCM-128 and AES-GCM-256 The resulting potential strength of the symmetric key will be 128 or 256 bits of security depending on the algorithms negotiated between the two IPsec peers. As part of this negotiation, the TOE verifies that the negotiated IKE Child SA symmetric algorithm key strength is at most as large as the negotiated IKE SA key strength as configured on the TOE and peer via an explicit check. Each IKE negotiation begins by agreement of both peers on a common (shared) IKE policy. This policy states which security parameters will be used to protect subsequent IKE negotiations and mandates how the peers are authenticated. The Security Administrator can configure multiple, prioritized policies on each peer, each with a different combination of parameter values. However, at least one of these policies must contain exactly the same encryption, hash, authentication, and Diffie-Hellman parameter values as one of the policies on the remote peer. For each policy created, the Security Administrator assign's a unique priority (1 through 10,000, with 1 being the highest priority). When the IKE negotiation begins, IKE searches for an IKE policy that is the same on both peers. The peer that initiates the negotiation will send all its policies to the remote peer, and the remote peer will try to find a match. The remote peer looks for a match by comparing its own highest priority policy against the policies received from the other peer. The remote peer checks each of its policies in order of its priority (highest priority first) until a match is found. After the two peers agree upon a policy, the security parameters of the policy are identified by an SA established at each peer, and these IKE SAs apply to all subsequent IKE traffic during the negotiation. When a packet is processed by the TOE and it determines it requires IPsec, it uses active SA settings or creates new SAs for initial connections with the IPsec peer. The TOE supports IKEv2 session establishment. The TOE supports configuration of session lifetimes for both IKEv2 SAs and IKEv2 Child SAs using the following the command “lifetime.” The time values for IKEv2 SAs can be limited up to 24 hours and for IKEv2 Child SAs up to 8 hours. The IKEv2 Child SA lifetimes can also be configured by an Administrator based on number of bytes. The TOE supports Diffie-Hellman Group 19 and 20. The TSF generates the secret value 'x' used in the IKEv2 Diffie-Hellman key exchange ('x' in g^x mod p) using the NIST approved DRBG specified in FCS_RBG_EXT.1 and having possible lengths of 256 or 384 bits. The TOE generates nonces used in IKEv2 exchanges, of at least 128 bits in size and at least half the output size of the negotiated pseudorandom function (PRF) hash. When a random number is needed for a nonce, the probability that a specific nonce value will be repeated during the life a specific IPsec SA is less than 1 in 2^{128}. The nonce is likewise generated using the AES-CTR DRBG. The TOE supports authentication of IPsec peers using RSA X.509 certificates. The TOE validates the presented identifier provided supporting the following fields and types: SAN: IP address, SAN: Fully Qualified Domain Name (FQDN). Certificate maps provide the ability for a certificate to be matched with a given set of criteria. The Administrator is instructed in the CC Configuration Guide to specify one or more certificate fields together with their matching criteria and the value to match.

TOE SFRs	How the SFR is Met
	In the evaluated configuration, the field name must specify the SAN (alt-subject-name) field. Match criteria should be "eq" for equal. SAN example: alt-subject-name eq <peer.cisco.com> The TOE will reject the IKE connection in any of these situations: 1) If the data ID Payload for any of those ID Types does not match the peer's certificate exactly; 2) If an ID Payload is not provided by the peer; 3) If multiple ID Types are provided in the ID Payload. The TOE also supports of IPsec peers using pre-shared key-based authentication and encryption services. Preshared keys can be configured using the "crypto isakmp key" key command and may be proposed by each of the peers negotiating the IKE establishment. The command specified which key to share with peer (designated by IP address or hostname)The SA cannot be established between the IPsec peers (TOE and peer) until both IPsec peers are configured for the same preshared key.
FCS_MACSEC_EXT.1	The TOE implements MACsec in compliance with 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, The Security Channel Identifier (SCI) is composed of a globally unique 48-bit 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. Only Extensible Authentication Protocol over LAN EAPOL (Physical Address Extension (PAE) EtherType 88-8E) and MACsec frames (EtherTYpe 88-E5) are permitted. All others are rejected.
FCS_MACSEC_EXT.2	The TOE implements the MACsec requirement for integrity protection with the confidentiality offsets of 0, 30 and 50 through the CLI command of "mka policy <policyname>, confidentiality-offset" commands. 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. 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. The TOE derives the ICK 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.
FCS_MACSEC_EXT.3	Each SAK is generated using key derivation from Connectivity Association Key (CAK) per IEEE 802.1X-2020 section 9.8.1. The likelihood of a repeating SAK is no less than 1 in 2 to the power of the size of the generated key.

TOE SFRs	How the SFR is Met
	Each SAK is generated using the KDF specified in IEEE 802.1X-2020 section 6.2.1 using the following transform - KS-nonce = a nonce of the same size as the required SAK, obtained from a Random Number Generator (RNG) each time an SAK is generated. Each of the keys used by MKA is derived from the CAK. 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. The derived keys 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. The key size is 32-bit hexadecimal in length for AES 128-bit CMAC mode encryption, and the key size is 64-bit hexadecimal in length for AES 256-bit CMAC mode encryption.
FCS_MACSEC_EXT.4	MACsec peer authentication is achieved by only using pre-shared keys. 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 as specified in NIST SP 800-38F, and GCM as specified in ISO 19772.
FCS_MKA_EXT.1	The TOE implements Key Agreement Protocol (MKA) in accordance with IEEE 802.1X-2020 and 802.1Xbx-2014. The data delay protection is enabled for MKA as a protection guard against an attack on the configuration protocols that MACsec is designed to protect by alternately delaying and delivering their PDUs. The Delay protection does not operate if and when MKA operation is suspended. An MKA Lifetime Timeout limit of 6.0 seconds and MKA Bounded Hello Timeout limit of 0.5 seconds is enforced by the TOE. The TOE discards MKPDUs that do not satisfy the requirements listed under FCS_MKA_EXT.1.7 in Section 5.2.2.15. This includes the following • The destination address of the MKPDU was an individual address • The MKPDU is less than 32 octets long • 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. • The CAK Name is not recognized. • Rhe Algorithm Agility parameter is unrecognized or not implemented by the receiver Each received MKPDU that is validated as specified in this clause and verified as specified in IEEE 802.1x-2020, section 9.4.1 shall be decoded as specified in IEEE 802.1x-2020, section 11.11.4. All valid MKPDUs that meet the requirements as defined

TOE SFRs	How the SFR is Met
	under FCS_MKA_EXT.1.7 are decoded in a manner conformant to IEEE 802.1x-2020 Section 11.11.4. On successful peer authentication, a unique 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 with a Connectivity Association Key (CAK), which is effectively a secret key. 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 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. The TOE does not support group CAK.
FCS_SSH_EXT.1 FCS_SSHS_EXT.1	The TSF implements SSHv2 conformant to RFCs 4251, 4252, 4253, 4254, 5656, 6668, 8308 section 3.1, and 8332 to provide a secure command line interface for remote administration. The TOE uses ssh-rsa, rsa-sha2-512 and rsa-sha2-256 for host key authentication and uses rsa-sha2-512 and rsa-sha2-256 for user public key authentication. User password-based authentication is also supported. SSHv2 connections will be dropped if the TOE receives a packet larger than 65,806 bytes. Large packets are detected by the SSHv2 implementation and dropped internal to the SSH process. The TSF's SSH transport implementation supports the following encryption algorithms: • aes128-cbc • aes256-cbc • aes128-gcm@openssh.com • aes256-gcm@openssh.com All connection attempts from remote SSH clients requesting any other encryption algorithm is denied. The TSF's SSH transport implementation supports the following MAC algorithms when aes128-cbc or aes-256-cbc is used: • hmac-sha2-256 • hmac-sha2-512 When aes128-gcm@openssh.com or aes256-gcm@openssh.com is used as the encryption algorithm the MAC algorithm is implicit. All connection attempts from remote SSH clients requesting any other MAC algorithm is denied. The TSF's SSH transport implementation supports the following public-key algorithms for Hostkey authentication: • ssh-rsa

TOE SFRs	How the SFR is Met
	• rsa-sha2-256 • rsa-sha2-512 The TSF's SSH transport implementation supports the following public-key algorithms for Client Authentication: • rsa-sha2-256 • rsa-sha2-512 The public-key algorithm is consistent with the RSA digital signature algorithm in FCS_COP.1/SigGen. 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. The TSF's SSH key exchange implementation supports the following key exchange algorithms: • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 The TSF's SSH implementation will perform a rekey after no longer than one hour or more than one gigabyte of data has been transmitted with the same session key. Both thresholds are checked. Rekeying is performed upon reaching whichever threshold is met first. The Administrator can configure lower rekey values if desired. The minimum time value is 10 minutes. The minimum volume value is 100 kilobytes.
FCS_RBG_EXT.1	The TOE implements a NIST-approved AES-CTR DRBG, as specified in NIST SP800-90A seeded by an entropy source that accumulates entropy from a TSF-hardware based noise source. The DRBG 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.
FIA_AFL.1	The privileged administrator can use the "aaa authentication rejected" command to specify the maximum number of unsuccessful authentication attempts within a configured time interval allowed before the privileged administrator or non-privileged administrator is locked out. The command also allows the privileged administrator to define the lockout period, after which the affected privileged administrator or non-privileged may again login.. The administrator needs to configure the Switch for SSH public key authentication. This is necessary to avoid a potential situation where password failures by remote Administrators lead to no Administrator access for a temporary period of time. While the TOE supports a range of failure attempts from 1-65535, in the evaluated configuration, the maximum number of failed attempts is recommended to be set to 3.

TOE SFRs	How the SFR is Met
	The time window over which login failures are counted is configurable from 1-65535 seconds. In the evaluated configuration, the time interval is recommended to be set to 120 seconds (two minutes). The lockout period is configurable from 1-65535 seconds. In the evaluated configuration, the time interval is recommended to be set to 360 seconds (five minutes). Using the recommended settings above, then if the maximum number of failed attempts is recommended set to 3, the time window over which failures are counted is set to 2 minutes, and the lockout period is set to 3 minutes, then if 3 successive unsuccessful logins for a single administrator ID occur in 2 minutes or less, the administrator will be locked out and unable to log in. The administrator will then be able to login 3 minutes after the failed login attempt.
FIA_PMG_EXT.1	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: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)” and other special characters listed in table 19. Minimum password length is settable by the Authorized Administrator, and can be configured for minimum password lengths of 1 character and maximum of 127 characters.
FIA_PSK_EXT.1	Through the implementation of the CLI, the TOE supports use of IKEv2 pre-shared keys for authentication of IPsec tunnels. Preshared keys can be entered as American Standard Code for Information Interchange (ASCII) character strings, or HEX values. The TOE supports keys that are from 1 character in length up to 127 characters in length and composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”. The data that is input is conditioned by the cryptographic module prior to use via SHA-1. The pre-shared keys are not generated by the TOE, but the TOE accepts the keys in the form of HEX strings. The TOE supports use of pre-shared keys for MACsec key agreement protocols as defined by IEEE 802.1X-2020. This is done via the CLI configuration command ‘key chain test_key macsec’. 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.

TOE SFRs	How the SFR is Met
FIA_UIA_EXT.1	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. The users can login to the TOE through the remote SSH or local console interfaces. Administrative access to the TOE is facilitated through a local password-based authentication and SSH public key authentication mechanisms on the TOE through which all Administrator actions are mediated. Once a potential (unauthenticated) administrative user attempts to access the TOE through an interactive administrative interface, the TOE prompts the user for a user name and password or SSH public key authentication. Only after the administrative user presents the correct authentication credentials will access to the TOE administrative functionality be granted. No access is granted to the administrative functionality of the TOE until an administrator is successfully identified and authenticated. The TOE provides a local password-based authentication mechanism as well as RADIUS AAA server for remote authentication. The administrator authentication policies include authentication to the local user database or redirection to a remote authentication server. Interfaces can be configured to try one or more remote authentication servers, and then fail back to the local user database if the remote authentication servers are inaccessible. 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. 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 grant administrative access (if the combination of username and password is correct) or indicate that the login was unsuccessful. The TOE does not provide a reason for failure in the cases of a login failure.
FIA_UAU.7	When a user enters their password at the local console, the TOE does not echo any characters as the password is entered. For remote session authentication, the TOE does not echo any characters as they are entered.
FIA_X509_EXT.1/Rev FIA_X509_EXT.2	The TOE uses X.509v3 certificates to support authentication for iPsec connections. The TSF determines the validity of certificates when received for authentication, by ensuring that the certificate and the certificate path are valid in accordance with RFC 5280. The certificate path is validated by ensuring that all the CA certificates have the basicConstraints extension and the CA flag is set to TRUE and the certificate path must terminate with a trusted CA certificate. CRL revocation checking is supported by the TOE. Revocation checking is performed on the leaf and intermediate certificate(s) when authenticating a certificate chain provided by the remote peer. The signing CA must have the cRLSign Key Usage or the

TOE SFRs	How the SFR is Met
FIA_X509_EXT.3	CRL will be deemed invalid and the TOE will reject the certificate. There are no functional differences if a full certificate chain or only a leaf certificate is presented. The TOE determines which certificate to use based upon the trustpoint configured. The instructions for configuring trustpoints are provided in CC Configuration Guide. If a network connection cannot be established to verify the revocation status of certificate for an external peer the connection will be rejected. A Certificate Request Message can be generated as specified by RFC 2986 and provide the following information in the request – Common Name (CN), Organization (O), Organizational Unit (OU), and Country. The TOE can validate the chain of certificates from the Root CA when the CA Certificate Response is received.
FMT_MOF.1/ManualUpdate FMT_MTD.1/CoreData FMT_MTD.1/CryptoKeys	The TOE provides the ability for Security Administrators to access TOE data, such as audit data, configuration data, security attributes, session thresholds, cryptographic keys and to perform manual updates to the TOE. Only Security Administrators can access the TOE's trust store. Each of the predefined and administratively configured roles has create (set), query, modify, or delete access to the TOE data, though with some privilege levels, the access is limited. The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the privileged and semi-privileged roles. For the purposes of this evaluation, the privileged level is equivalent to full administrative access to the CLI, which is the default access for IOS-XE privilege level 15; and the semi-privileged level equates to any privilege level that has a subset of the privileges assigned to level 15. Privilege levels 0 and 1 are defined by default and are customizable, while levels 2-14 are undefined by default and also customizable. By default, privilege levels 0 and 1 have the same level of capabilities. They are essentially read-only and allow for basic management and support. Admins assigned to these privilege levels cannot modify configurations, re-load the device, delete files from flash memory, clear logs, or run debugs. The term "Authorized Administrator" is used 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 semi-privileged Administrators with only a subset of privileges may also manage and modify TOE data based on the privileges assigned. The TOE does not provide automatic updates to the software version running on the TOE. 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, verify the integrity of, and install those updates. The Authorized Administrator generates RSA key pairs to be used in the IKE protocol and RSA key pairs to be used in SSH protocol. Zeroization of these keys is provided in Table 23 below. However, no administrative functionality is available prior to administrative login. TOE administrators can control (generate/delete) the following keys, IKE RSA Key Pairs and

TOE SFRs	How the SFR is Met
	SSH RSA Key Pairs by following the instructions in the AGD. An authorized administrator can also add/delete MACsec keys, IPsec PSK, and RADIUS PSKs
FMT_SMF.1 FMT_SMF.1/MACSEC	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 to perform these functions via SSHv2 secured connection or a local console. The console port is an asynchronous serial port that allows you to connect to the device for initial configuration through a standard RS-232 port with an RJ-45 connector. The specific management capabilities available from the TOE include: • Local and remote administration of the TOE and the services provided by the TOE via the TOE CLI, as described above • The ability to manage the warning banner message and content which allows the Authorized Administrator the ability to define warning banner that is displayed prior to establishing a session

TOE SFRs	How the SFR is Met
	• The ability to set and modify the time limits of session inactivity for both local and remote sessions • Configure the number of failed administrator authentication attempts that will cause an account to be locked out locked out and how long they will be locked out for • The ability to update the IOS-XE software. The validity of the image is provided using digital signature prior to installing the update • The ability to manage audit behaviour and the audit logs which allows the Authorized Administrator to configure the audit logs, view the audit logs, and to clear the audit logs • Ability to configure thresholds for SSH rekeying • Ability to manage the trusted public keys database. • 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 • The ability to configure the lifetime for the IPsec Sas, which supports the secure connections to the audit server and the remote authentication server • The ability to manage the TOE's trust store and designating X509v3 certificates as trust anchors • The ability to generate Certificate Signing Requests (CSRs) and process the CA certificate responses • The ability to manage the Key Server and associated MKA participants • The ability to generate a PSK and install in the CAK cache • The ability to specify the lifetime of a CAK and to enable, disable or delete a PSK in the CAK cache of a device • The ability to configure and set the time clock • The ability to configure the reference identifiers • Ability to modify the behavior of the transmission of audit data to an external IT entity
FMT_SMR.2	The TOE platform maintains privileged and semi-privileged administrator roles. The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the semi-privileged and privileged roles. The privileged role is equivalent to full administrative access to the CLI, which is the default access for IOS-XE privilege level 15; and the semi-privileged role equates to any privilege level that has a subset of the privileges assigned to level 15. Privilege levels 0 and 1 are defined by default and are customizable, while levels 2-14 are undefined by default and are also customizable. Note: the levels are not hierarchical. By default, privilege levels 0 and 1 have the same level of capabilities. They are essentially read-only and allow for basic management and support. Admins assigned to these privilege levels cannot modify configurations, re-load the device, delete files from flash memory, clear logs, or run debugs. The term "Security 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. The privilege level determines the functions the user can perform; hence the Security Administrator with the appropriate privileges. Refer to the Guidance documentation and IOS-XE Command Reference Guide for available commands and associated roles and privilege levels.

TOE SFRs	How the SFR is Met
	The TOE can and shall be configured to authenticate all access to the command line interface using a username and password. The TOE supports both local administration via a directly connected console cable and remote administration via SSH.
FPT_CAK_EXT.1	A CAK value is specified in the configuration file by the Administrator using a bit-based (hex) format. The interface specifically implemented in the TSF for viewing the configuration file is the “show running-config” or “show startup-config “CLI commands. When the TOE is operating in the evaluated configuration, and the Administrator executes the “show running-config” or “show startup-config” CLI commands, the CAK data will not be displayed. This protects the CAK data from unauthorized disclosure.
FPT_FLS.1	Whenever a failure occurs (power-on self-tests, integrity check of the TSF executable image and/or the noise source health-tests) 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 and reloads. If the failures persist, the TOE will continue to reload in an attempt to correct the failure. This functionally prevents any failure from causing an unauthorized information flow. There are no failures that circumvent this protection. If the rebooting continues, the Authorized Administrator should contact Cisco Technical Assistance Center (TAC).
FPT_RPL.1	Replayed data is discarded by the TOE and the attempt to replay data is logged. The TOE ensures MAC Protocol Data Units (MPDUs) are replay protected by ensuring the received 32-bit (packet number) PN in the SecTAG of the frame is not less than the lowest acceptable 32-bit PN for the SA. If the PN is less that the lowest acceptable PN for the security association (SA), the MPDU will be dropped and not processed further. The Replay Protection Window Size determines the lowest acceptable PN for the SA. The Replay Protection Window Size may be set to zero to enforce strict replay protection. The TOE protects against replayed MKPDUs by ensuring if a MKPDU contains a duplicate Member Number (MN) and not the most current MN in the Basic Parameter set, then the MKPDU will be dropped and not processed further.

TOE SFRs	How the SFR is Met
FPT_SKP_EXT.1 FPT_APW_EXT.1	The TOE is designed specifically to not disclose any keys stored in the TOE. The TOE stores all private keys in a secure directory that cannot be viewed or accessed, even by the Administrator. The TOE stores symmetric keys only in volatile memory. Pre-shared keys (MACsec CAKS) may be specified in the configuration file by the Administrator using a bit-based (hex) format. While only the Administrator may view the configuration file, the CAKs can be configured so they are excluded from display when viewing the configuration file via “show running-config” or “show startup-config“ CLI commands. Pre-shared keys for IPsec may be specified in the configuration file by the Administrator using a bit-based (hex) or text-based format . While only the Administrator may view the configuration file, the IPsec PSKs can be configured so they are stored encrypted using AES. The TOE is designed specifically to not disclose any passwords stored in the TOE. All passwords are stored using a SHA-2 hash. ‘Show’ commands display only the hashed password. The CC Configuration Guide instructs the Administrator to use the algorithm-type sha256 or scrypt sub-command when passwords are created or updated. The SHA256 sub-command is password type 8 while scrypt is password type 9. Both password types use SHA-2.
FPT_STM_EXT.1	The TSF implements a clock function to provide a source of date and time. The clock function is reliant on the system clock provided by the underlying hardware. All Switch models have a real-time clock (RTC) with battery to maintain time across reboots and power loss. The TOE relies upon date and time information for the following security functions: ■ To monitor local and remote interactive administrative sessions for inactivity (FTA_SSL_EXT.1, FTA_SSL.3); ■ Validating X.509 certificates to determine if a certificate has expired (FIA_X509_EXT.1/Rev); ■ To determine when SSH session keys have expired and to initiate a rekey (FCS_SSH_EXT.1); ■ To determine when IKEv2 SA lifetimes have expired and to initiate a rekey (FCS_IPSEC_EXT.1); ■ To determine when IPsec Child SA lifetimes have expired and to initiate a rekey (FCS_IPSEC_EXT.1); ■ To provide accurate timestamps in audit records (FAU_GEN.1.2).
FPT_TUD_EXT.1	An Authorized Administrator can query the software version running on the TOE and can initiate updates to (replacements of) software images. The current active version can be verified by executing the “show version” command from the TOE’s CLI. When software updates are made available by Cisco, an Administrator can obtain, verify the integrity of, and install the updates. The updates can be downloaded from https://software.cisco.com/ The TOE will authenticate the image using a digital signature verification check to ensure it has not been modified since distribution using the following process: Prior to being made publicly available, the software image is hashed using a SHA512 algorithm and then digitally signed. The digital signature is embedded to the image (hence the

TOE SFRs	How the SFR is Met
	image is signed). The TOE uses a Cisco public key to validate the digital signature to obtain the SHA512 hash. The TOE then computes its own hash of the image using the same SHA512 algorithm and verifies the computed hash against the embedded hash. If they match the image has not been modified or tampered since distributed from Cisco meaning the software is authenticated. If they do not match the image will not install.
FPT_TST_EXT.1	The TOE runs a suite of self-tests during initial start-up to verify its correct operation. For testing of the TSF, the TOE automatically runs checks and tests at start-up, during resets and periodically during normal operation to ensure the TOE is operating correctly, including checks of image integrity and all cryptographic functions. 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). The TOE performs the following tests: **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. If the encrypted texts match, the test passes; otherwise, the test fails. 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. If the decrypted texts match, the test passes; otherwise, the test fails. **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. If the encrypted values, the test passes; otherwise, the test fails. The encrypted data is then decrypted using the private key. This value is compared to the original plaintext value. If the decrypted values match, the test passes; otherwise, the test fails. **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. If the random bits match, the test passes; otherwise, the test fails. **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. If the MAC values match, the test passes; otherwise, the test fails. **Software Integrity Test:** The Software Integrity Test is run automatically whenever the IOS-XE system images is loaded and confirms that the image file that's about to be loaded has maintained its integrity. The software contains a SHA-512 hash. This hash is compared to a pre-loaded hash. If the hash values match, the test passes; otherwise, the test fails.

TOE SFRs	How the SFR is Met
	SHA-1/256/384/512 Known Answer Test: For each of the values listed, the SHA implementation is fed known data and a key. These values are used to generate a hash. This hash is compared to a known value. If the hash values match, the test passes; otherwise, the test fails. If any component reports failure for the POST, the system crashes. Appropriate information is displayed on the screen and saved in the crashinfo file. All ports are blocked during the POST. If all components pass the POST, the system is placed in FIPS PASS state and ports can forward data traffic. If an error occurs during the self-test, a SELF_TEST_FAILURE system log is generated. Example Error Message: %CRYPTO-0-SELF_TEST_FAILURE: Crypto algorithms self-test failed (SHA hashing)" These tests are sufficient to verify that the correct version of the TOE software is running as well as that the cryptographic operations are all performing as expected because any deviation in the TSF behaviour will be identified by the failure of a self-test.
FTA_SSL_EXT.1 FTA_SSL.3	Administratively configurable timeouts are also available for the EXEC level access (access above level 1) through use of the “exec-timeout” setting. An Authorized Administrator can configure maximum inactivity times separately for both local and remote administrative sessions using the “exec-timeout” setting applied to the console and/or virtual terminal (VTY) lines. The configuration of the VTY lines sets the configuration for the remote console access. VTY line configuration determines how many users can be logged onto the TOE concurrently. The line console settings are not immediately activated for the current session. The current line console session must be exited. When the user logs back in, the inactivity timer will be activated for the new session. If a local user session is inactive for a configured period, the session will be terminated and will require reidentification and authentication to login. If a remote user session is inactive for a configured period, the session will be terminated and will require re- identification and authentication to establish a new session. The allowable inactivity timeout range is from 1 to 35,791 seconds.
FTA_SSL.4	An authorized administrator can exit out of both local and remote administrative sessions. Each administrator logged onto the TOE can manually terminate their session using the “exit” or “logout” command.
FTA_TAB.1	The Administrator can configure an access banner that describes restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE. The banner will display on the local console port and SSH interfaces

TOE SFRs	How the SFR is Met
	prior to allowing any administrative access
FTP_ITC.1 FTP_ITC.1/MACSEC	The TOE protects communication between the TOE and the remote audit server using IPsec. This provides a secure channel to transmit log events. Communications between the TOE and the remote authentication (RADIUS) server is secured using IPsec. MACsec is used to secure communication channels between MACsec peers at Layer 2.
FTP_TRP.1 /Admin	All remote administrative communications take place over a secure encrypted SSHv2 session. The SSHv2 session is encrypted using AES encryption. The remote users can initiate SSHv2 communications with the TOE.

7 Annex A: Key Zeroization

The following table describes the key zeroization referenced by FCS_CKM.4 provided by the TOE.

Table 23. Key Zeroization

Name	Description of Key	Zeroization
Diffie-Hellman Secret	This is the shared secret used as part of the Diffie-Hellman key exchange. This key is stored in SDRAM.	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 SDRAM.	Zeroized upon completion of DH exchange. Overwritten with: 0x00
Skeyid	This is an IKE intermittent value used to create skeyid_d. This key is stored in SDRAM.	Automatically after IKE session terminated. Overwritten with: 0x00
skeyid_d	This is an IKE intermittent value used to derive keying data for IPsec. This key is stored in SDRAM.	Automatically after IKE session terminated. Overwritten with: 0x00
IKE session encrypt key	This the key IPsec key used for encrypting the traffic in an IPsec connection. This key is stored in SDRAM.	Automatically after IKE session terminated. Overwritten with: 0x00
IKE session authentication key	This the key IPsec key used for authenticating the traffic in an IPsec connection. This key is stored in SDRAM.	Automatically after IKE session terminated. Overwritten with: 0x00
ISAKMP preshared	This is the configured pre-shared key for ISAKMP negotiation. This key is stored in NVRAM.	Zeroized using the following command: **# no crypto isakmp key** Overwritten with: 0x00
IKE RSA Private Key	The RSA private-public key pair is created by the device itself using the key generation CLI described below. Afterwards, the device's public key must be put into the device certificate. The device's certificate is created by creating a trustpoint on the device. This trustpoint authenticates with the CA server to get the CA	Zeroized using the following command: **# crypto key zeroize rsa** Overwritten with: 0x00

Name	Description of Key	Zeroization
	certificate and also enrolls with the CA server to generate the device certificate. In the IKE authentication step, the device's certificate is firstly sent to other device to be authenticated. The other device verifies that the certificate is signed by CA's signing key, then sends back a random secret encrypted by the device's public key in the valid device certificate. Only the device with the matching device private key can decrypt the message and obtain the random secret. This key is stored in NVRAM.	
IPSec encryption key	This is the key used to encrypt IPsec sessions. This key is stored in SDRAM.	Automatically when IPSec session terminated. Overwritten with: 0x00
IPSec authentication key	This is the key used to authenticate IPsec sessions. This key is stored in SDRAM.	Automatically when IPSec session terminated. 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.	Automatically when MACsec session terminated. The value is zeroized by overwriting with another key or freed when the session expires.
MACsec Connectivity Association Key (CAK)	The CAK secures the control plane traffic. This key is stored in internal ASIC register.	Automatically when MACsec session terminated. The value is zeroized by overwriting with another key or freed when the session expires.
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.	Automatically when MACsec session terminated. The value is zeroized by overwriting with another key or freed when the session expires.
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.	Automatically when MACsec session terminated. The value is zeroized by overwriting with another key or freed when the session expires.

Name	Description of Key	Zeroization
RADIUS secret	Shared secret used as part of the Radius authentication method. This key is stored in NVRAM.	Zeroized using the following command: **# no radius-server key** Overwritten with: 0x00
SSH Private Key	Once the function has completed the operations requiring the RSA key object, the module over writes the entire object (no matter its contents) using memset. This overwrites the key with all 0's. This key is stored in NVRAM.	Zeroized using the following command: **# crypto key zeroize rsa** Overwritten with: 0x00
SSH Session Key	The results zeroized using the poisoning in free to overwrite the values with 0x00. This is called by the ssh_close function when a session is ended. This key is stored in SDRAM.	Automatically when the SSH session is terminated. Overwritten with: 0x00
RNG Seed	This seed is for the RNG. The seed is stored in DRAM.	Zeroized upon power cycle of the device Overwritten with: 0x00
RNG Seed Key	This is the seed key for the RNG. The seed is stored in DRAM.	Zeroized upon power cycle of the device Overwritten with: 0x00

NOTE: In the event of an unexpected shutdown (e.g. crash or power loss), keys stored in volatile storage would be cleared from memory as a result of the loss of power/shutdown. For private keys in NVRAM (non-volatile storage), if an unexpected shutdown occurs during administrator-initiated zeroization of a private key, the administrator should run the command again when the TOE is back in its operational state to ensure no residual portions of the private keys remain.

8 Annex B: References

The following documentation was used to prepare this ST:

Table 24. 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 3.0e, December 6, 2023
[SD]	Supporting Document – Evaluation Activities for Network Device cPP, version 3.0e, December 6, 2023
[PKG_SSH]	Functional Package for Secure Shell (SSH), version 1.0, May 13, 2021
[MOD_MACSEC]	Network Device Protection Profile Extended Package MACsec Ethernet Encryption (MOD_MACSEC), Version 1.0, March 2, 2023
IEEE 802.1X-2020	IEEE Standard for Local and metropolitan area networks—Port-Based Network Access Control
IEEE 802.1Xbx-2014	IEEE Standard for Local and metropolitan area networks -- Port-Based Network Access Control Amendment 1: MAC Security Key Agreement Protocol (MKA) Extensions
IEEE Standard 802.1AE-2018	IEEE Standard for Local and metropolitan area networks-Media Access Control (MAC) Security
ISO 18033-3	Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers
ISO 10116	Information technology -- Security techniques -- Modes of operation for an n-bit block cipher
ISO 19772	Information technology -- Security techniques -- Authenticated encryption
ISO/IEC 10118-3:2004	Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions
ISO/IEC 9797-2:2011	Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function
ISO/IEC 18031:2011	Information technology -- Security techniques -- Random bit generation
[NIST SP800-38B]	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication
[NIST SP800-38F]	Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping
[NIST SP 800-56Arev3]	NIST Special Publication 800-56Arev3 Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography April 2018
[NIST SP 800-56Brev2]	NIST Special Publication 800-56Brev2 Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography March 2019
[NIST SP 800-90A Rev 1]	NIST Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators January 2015

Identifier	Description
[NIST SP 800-90B rev1]	NIST Special Publication 800-90B Recommendation for the Entropy Sources Used for Random Bit Generation January 2018
[FIPS 140-2]	FIPS PUB 140-2 Federal Information Processing Standards Publication
[FIPS PUB 180-3]	FIPS PUB 180-3 Federal Information Processing Standards Publication Secure Hash Standard (SHS) October 2008
[FIPS PUB 186-4]	FIPS PUB 186-4 Federal Information Processing Standards Publication Digital Signature Standard (DSS) July 2013

9 Annex C: Obtaining Documentation and Submitting a Service Request

The Cisco Embedded Services 3300 and 9300 Series Switches (ESS3300 & ESS9300) running IOS-XE 17.15 Common Criteria Configuration Guide (AGD) should be obtained from the Product Listing on the NIAP site.

For information on obtaining other 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

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at:

http://www.cisco.com/go/offices

9.1 Documentation 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.

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.

9.2 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