Nokia 7750 SR & 7250 IXR, SROS 24.10.R3, MACsec platforms Security Target

Document Version: 1.2
Date: August 22, 2025

intertek
acumen
security

2400 Research Blvd
Suite 395
Rockville, MD 20850

Revision History

Version	Date	Changes
0.1	August 22, 2024	Initial Draft
0.2	Sept 05, 2024	Deleted FCS_HTTPS_EXT SFR
0.3	Oct 15, 2024	Addressed own comments
0.4	November12, 2024	Addressing peer-review comments
0.5	January 31, 2025	Accepting all changes and closing comments
0.6	February 13, 2025	Addressing Vendor comments
0.7	March 17, 2025	Removing non-MACsec platforms
0.8	March 28, 2025	Addressed comments
0.9	May 12, 2025	Fixed formatting issues
1.0	July 11, 2025	Addressed Peer Lead review and checkout ready
1.1	August 11, 2025	Addressed 1st round of validators comments
1.2	August 22, 2025	Addressed 2sd round of validators comments

Contents

1. INTRODUCTION

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Nokia 7750 SR & 7250 IXR, SROS 24.10.R3, MACsec platforms. This Security Target (ST) defines a set of assumptions about the aspects of the TOE environment, a list of threats that the TOE intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE that meet that set of requirements. Administrators of the TOE will be referred to as Security Administrators in this document.

1.1 SECURITY TARGET AND TOE REFERENCE

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

Table 1 – TOE/ST Identification

Category	Identifier
ST Title	Nokia 7750 SR & 7250 IXR, SROS 24.10.R3, MACsec platforms Security Target
ST Version	1.2
ST Date	August 22, 2025
ST Author	Acumen Security, LLC.
TOE Identifier	Nokia 7750 SR & 7250 IXR, SROS 24.10.R3, MACsec platforms
TOE Hardware	Nokia 7750 SR, 7250 IXR series with MACsec
TOE Software	Nokia SR OS 24.10.R3
TOE Developer	Nokia Corporation
Key Words	Network Device, Nokia, Encryption, SR OS, MACsec

1.2 TOE OVERVIEW

The Nokia 7750 SR & 7250 IXR, SROS 24.10.R3, MACsec platforms (herein referred to as the TOE) is a network device with the high-performance, scale and flexibility supporting service providers, web scale and enterprise networks. The TOE utilizes Nokia's SR operating system version 24.10.R3. The following table lists all the TOE's models that have been evaluated.

Table 2 – TOE's hardware platforms

Platform (part number)	CPU	Speed	Core
7750 SR-1 CPM in: -7750 SR-1 (FP4)	Marvell OCTEON III CN7360 (MIPS64)	1.8GHz	16
7750 SR-1 CPM in: -7750 SR-1-24D -7750 SR-1-48D -7750 SR-1-46S -7750 SR-1-92S	AMD EPYC3251 (ZEN)	2.5GHz	8
7750 SR-1x CPM in: -7750 SR-1x-48D -7750 SR-1x-92S	AMD EPYC3251 (ZEN)	2.5GHz	8

Platform (part number)	CPU	Speed	Core
7750 SR-1se CPM	AMD EPYC3251 (ZEN)	2.5GHz	8
7250 IXR-R6d/dl CPIOM	AMD EPYC3255 (ZEN)	2.5GHz	8
7750 SR-2se CPM-2se	AMD EPYC3251 (ZEN)	2.5GHz	8
7250 IXR-e CPM (Small)	Intel Atom C3708 (Goldmont)	1.7GHz	8
7250 IXR-R4 CPM	Marvell OCTEON III CN7340 (MIPS64)	1.5GHz	8
7250 IXR-R6 CPIOM	Marvell OCTEON III CN7360 (MIPS64)	1.5GHz	16
7750 SR-2s CPM	Marvell OCTEON III CN7360 (MIPS64)	1.8GHz	16
7750 SR-14s/7s CPM-s v2 (SR-s CPM-2S)	Marvell OCTEON III CN7890 (MIPS64)	1.8GHz	48
7750 SR-7/SR-12/SR-12e SR CPM5	Marvell OCTEON II CN6645 (MIPS64)	1.5GHz	10

The TOE Description section provides an overview of the TOE architecture, including physical boundaries, security functions, and relevant TOE documentation and references.

1.2.1 TOE PRODUCT TYPE

The TOE is a network device that is composed of hardware and software and offers a scalable solution to the end users. It satisfies all the criterion to meet the collaborative Protection Profile for Network Devices, Version 3.0e [CPP_ND_V3.0E], Functional Package for Secure Shell (PKG_SSH_V1.0) and PP-Module for MACsec Ethernet Encryption, Version 1.0 [MOD_MACsec_V1.0].

1.3 TOE DESCRIPTION

The TOE portfolio delivers high-performance, scaling and flexibility to support a full array of IP and MPLS services and functions for service providers, web scale and enterprise networks. The Nokia 7750 SR & 7250 IXR portfolios include a wide range of physical platforms that share a mutual architecture and feature set. This allows Nokia customers to select the platform that best addresses their unique business goals and fulfills their scale, density, space, power, and value-added service requirements. The Nokia 7750 SR & 7250 IXR portfolios are chassis-based routers.

The Nokia 7750 Service Router (SR) portfolio consists of hardware platforms intended for use in IP edge and core networking environments. The portfolio includes the 7750 SR-s and 7750 SR series appliance families. The following Table 3 lists the specifically evaluated Nokia platforms:

Table 3 – Nokia 7750 SR Platforms

Platforms (part number)	CPU	Speed	Core
7750 SR-1 CPM in: -7750 SR-1 (FP4)	Marvell OCTEON III CN7360 (MIPS64)	1.8GHz	16
7750 SR-1 CPM in: -7750 SR-1-24D	AMD EPYC3251 (ZEN)	2.5GHz	8

Platforms (part number)	CPU	Speed	Core
-7750 SR-1-48D -7750 SR-1-46S -7750 SR-1-92S			
7750 SR-1x in: -7750 SR-1x-48D -7750 SR-1x-92S	AMD EPYC3251 (ZEN)	2.5GHz	8
7750 SR-1se CPM	AMD EPYC3251 (ZEN)	2.5GHz	8
7750 SR-2se CPM-2se	AMD EPYC3251 (ZEN)	2.5GHz	8
7750 SR-2s CPM	Marvell OCTEON III CN7360 (MIPS64)	1.8GHz	16
7750 SR-14s/7s CPM-s v2	Marvell OCTEON III CN7890 (MIPS64)	1.8GHz	48
7750 SR-7/SR-12/SR-12e SR CPM5	Marvell OCTEON II CN6645 (MIPS64)	1.5GHz	10

The Nokia 7250 IXR portfolio is purpose-built for access and aggregation in mobile anyhaul, fixed-mobile convergence, and mission-critical enterprise applications. They offer compact, temperature-hardened platforms with advanced timing, security and quality of service features. The Nokia 7250 IXR portfolio includes the following appliance families: The 7250 IXR-R, IXR-e, IXR-X and 7250 IXR-s platforms. The following Table 4 lists the specifically evaluated Nokia 7250 IXR platforms:

Table 4 – Nokia 7250 IXR Platforms

Platforms (part number)	CPU	Speed	Core
7250 IXR-R6d/dl CPIOM	AMD EPYC3255 (ZEN)	2.5GHz	8
7250 IXR-e (Small) CPM	Intel Atom C3708 (Goldmont)	1.7GHz	8
7250 IXR-R4 CPM	Marvell OCTEON III CN7340 (MIPS64)	1.5GHz	8
7250 IXR-R6 CPIOM	Marvell OCTEON III CN7360 (MIPS64)	1.5GHz	16

The TOE supports a full array of network functions and services. Every Nokia 7750 series routing appliance is a whole routing system that provides a variety of high-speed interfaces (only Ethernet is within scope of this evaluation) for various scales of networks and various network applications. The TOE utilizes a common Nokia SR operating system, features, and technology for compatibility across all platforms.

Nokia SR OS is mainly responsible for all the functionalities and services provided by the routers. The routers can be accessed either via a local console or via a network connection that is protected using the SSH protocol. Each time a user accesses the routers, either via local console terminal connection or from the network remotely using SSH, the user must ensure to successfully authenticate itself with the correct credentials.

The TOE also supports MACsec functionality between compatible Nokia MACsec peer devices using the Media Dependent Adapter (MDA). On the evaluated configuration, the TOE permits only EAPOL (PAE EtherType 88-8E), MACsec frames (EtherType 88-E5), and MAC control frames (EtherType is 88-08) and discards others.

The TOE's provides AES-GCM MACsec encryption. The MACsec feature is powered by one or more of the network processor chips listed in Table 5:

Table 5 – TOE's MACsec PHYs

Network Chip	Vendor
BCM82399	Broadcom
BCM81392	
BCM81394	
BCM81343	
VSC8258	Microsemi
VSC8490	
VSC8584	
E5	Nokia

The MDAs are pluggable adapter cards. They provide physical interface connectivity to the devices. MDAs can be different in terms of connectivity and density configuration settings. Additionally, the MDA modules vary by chassis. Regardless, they provide the same functionality and security for the related chassis. MDAs support ethernet and multiservice interfaces. For this evaluation, the following Table 6. lists the TOE platforms and their compatible MDA card, in addition to the MACsec PHY:

Table 6 – MDA and MACsec cards used in the TOE's MACsec capable appliances

TOE platforms	MACsec card	MACsec embedded (network processor) PHY (ethernet PHY framer)
7750 SR-1se CPM	ms36-800g-qsfpdd	Nokia E5
7750 SR-1-48D CPM	m48-400g-qsfpdd-1	
7750 SR-1x-92S CPM	m80-200g-sfpdd+12-800g-qsfpdd-1x	
7750 SR-1-92S CPM	m80-200g-sfpdd+12-400g-qsfpdd-1	
7750 SR-1-24D CPM	m24-800g-qsfpdd-1	
7750 SR-1x-48D CPM	m48-800g-qsfpdd-1x	
7750 SR-1-46S CPM	m40-200g-sfpdd+6-800g-qsfpdd-1	
7750 SR-2se CPM	x2-s36-800g-qsfpdd-18.0t	Nokia E5
	x2-s18-800g-qsfpdd	
	x2-s36-800g-qsfpdd-12.0t	
	mse24-200g-sfpdd	
	mse6-800g-cfp2-dco	
	mse14-800g+4-400g	
	m36-800g-qsfpdd	

TOE platforms	MACsec card	MACsec embedded (network processor) PHY (ethernet PHY framer)
	mse6-800g-qsfpdd	
	m36-400g-qsfp112	
7250 IXR-R6d/R6dl CPIOM	m20-10g-sfp+	VSC8258
	m18-25g-sfp28	BCM81392 and BCM81394
	m1-400g-qsfpdd+1-100g-qsfp28	BCM81343
	m46-10g-sfp+	VSC8258
	m2-cfp2	BCM81343
	m32-1g-csfp	VSC8584
	m80-1g-csfp	VSC8584
	m2-100g-qsfp28+16-10g-sfp+	BCM81392 and VSC8258
7750 SR-14s/7s CPM-s v2 (SR-s CPM-2S)	x2-s36-800g-qsfpdd-18.0t	Nokia E5
	x2-s18-800g-qsfpdd	
	x2-s36-800g-qsfpdd-12.0t	
	ms16-sdd+4-qsfp28-b	BCM81343
	ms8-sdd+2-qsfp28-b	BCM81343
	mse24-200g-sfpdd	Nokia E5
	mse6-800g-cfp2-dco	
	mse14-800g+4-400g	
	m36-800g-qsfpdd	
	mse6-800g-qsfpdd	
	m36-400g-qsfp112	
7750 SR-2s CPM	ms16-sdd+4-qsfp28-b	BCM81343
	ms8-sdd+2-qsfp28-b	BCM81343
7750 SR-7 & SR-12 & SR-12e SR CPM5	me16-25gb-sfp28+2-100gb-qsfp-b	BCM81343
7750 SR-1 CPM	me16-25gb-sfp28+2-100gb-qsfp-b	BCM81343
7250 IXR-R6 CPIOM	m10-10g-sfp+	VSC8258
	m20-1g-csfp	VSC8584

TOE platforms	MACsec card	MACsec embedded (network processor) PHY (ethernet PHY framer)
	m6-10g-sfp++1-100g-qsfp28	BCM82399 and VSC8258
	m4-10g-sfp++1-100g-cfp2	BCM82399 and VSC8258
	m6-10g-sfp++4-25g-sfp28	BCM82399 and VSC8258
7250 IXR-R4 CPM	m10-10g-sfp+	VSC8258
	m20-1g-csfp	VSC8584
	m6-10g-sfp++1-100g-qsfp28	BCM82399 and VSC8258
	m4-10g-sfp++1-100g-cfp2	BCM82399 and VSC8258
	m6-10g-sfp++4-25g-sfp28	BCM82399 and VSC8258
7250 IXR-e CPM (small)	m14-10g-sfp++4-1g-tx	VSC8490

Some TOE models, such as the 7250 IXR-R4 and 7250 IXR-R6, can be equipped with an MDA that includes two types of MACsec PHYs. These MDAs use both PHYs to handle MACsec protocols, resulting in certain ports on the MDA card using different PHYs for MACsec traffic encryption.

The MACsec Key Agreement (MKA) protocol uses the Connectivity Association Key (CAK) to derive a Key Encryption Key (KEK), which secures the distribution of transient session keys called Secure Association Keys (SAKs). SAKs and other MKA parameters are required to sustain communication over secure channel and to perform encryption and other MACsec security functions. SAKs, along with other essential control information, are distributed in MKA protocol control packets, also referred to as MKPDUs. MACsec can be deployed in two modes:

- Point-to-point mode
- Multipoint-to-multipoint mode

In the evaluated configuration, MACsec is configured individually on a point-to-point Ethernet link. A pair of MACsec devices can be connected via bridge or a direct connection. To enable secure MACsec communication, devices use the pre-shared Connectivity Association Key (CAK) to authenticate each other and execute the MACsec Key Agreement (MKA) protocol. MKA negotiates and distributes transient Secure Association Keys (SAKs), which are then used to encrypt/decrypt data traffic over the MACsec-secured channel.

In order to determine an authorized peer, both devices must first exchange an MKA frame, and these devices must agree upon a shared key and MACsec cipher suite in order to set up both receive and transmit Security Associations (SA). Once the connections are established, the MACsec frames will be transmitted between devices. Figure 1 depicts the TOE boundary.

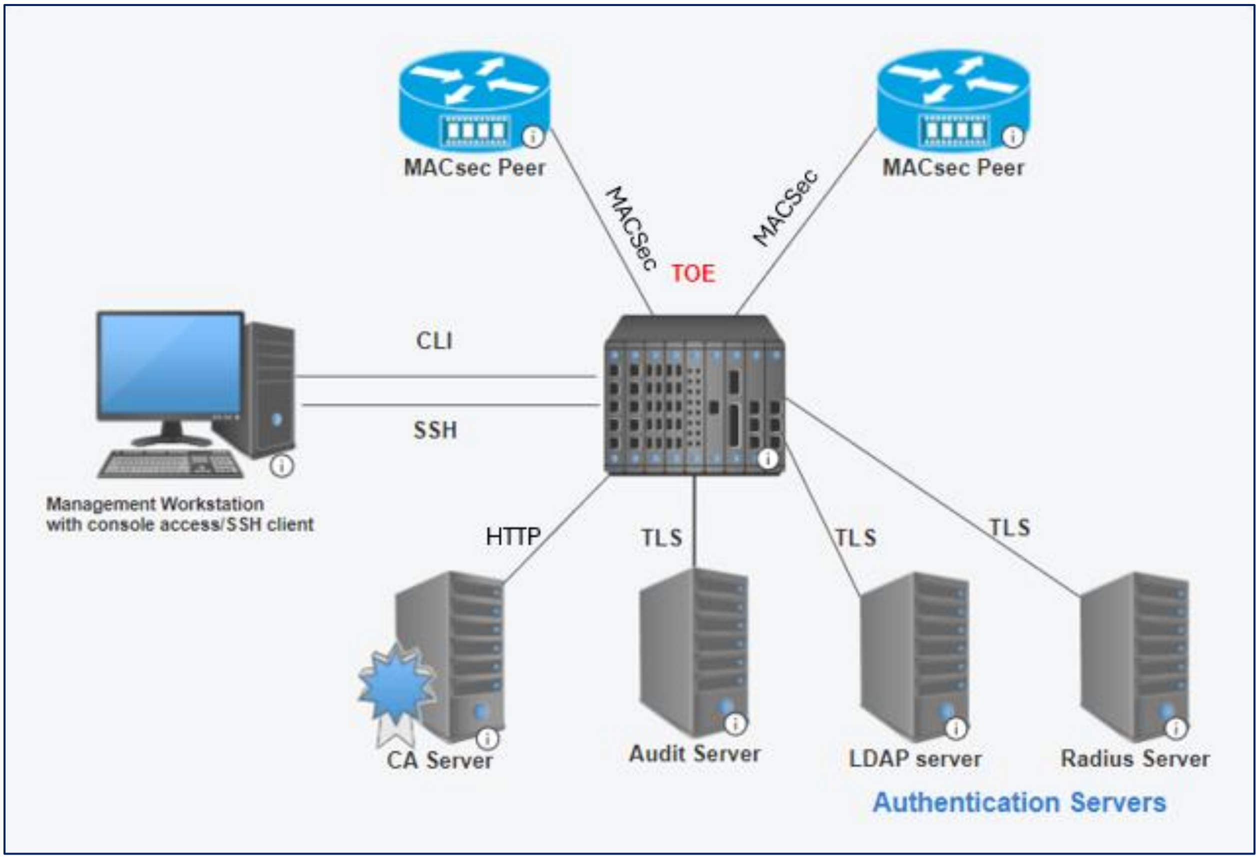

Figure 1 – TOE Boundary Diagram

1.4 TOE EVALUATED CONFIGURATION

In the evaluated configuration, the TOE consists of the platforms as stated in Section 1.3. The TOE supports secure connectivity with another IT environment device as stated in Table 7.

Table 7 – IT Environment Components

Components	Required (Y/N)	Protocols used	Usage
Audit server	Yes	TLS	The audit server supports Syslog over TLS v1.2 to receive audit events securely from the TOE.
LDAP server	Yes	TLS	This server will provide the authentication mechanism to authenticate users.
RADIUS Server	Yes	TLS	This server will provide the authentication mechanism to authenticate users.
MACsec peer	Yes	MACsec	This peer is required to test MACsec functionality.
Management workstation with console access/SSH client	Yes	CLI-SSH	This includes any IT Environment Management workstation with console access and an SSH client.

Components	Required (Y/N)	Protocols used	Usage
Certificate Authority server	Yes	HTTP	The Certificate Authority server is used for issuing, generation and management of X509 certificates to be used with the TOE.

1.5 PHYSICAL SCOPE OF THE TOE

The TOE boundary is the hardware appliance, which is comprised of hardware and software components. The software component is SROS v24.10.R3 running on TiMOS SMP v2.5 and using the SR Crypto Module (SRCM) version 5.0. It is deployed in an environment that contains the various IT components as depicted in Figure 1 above. SROS version 24.10.R3 is a software that includes various router applications, the SR Cryptographic Module (SRCM) and the TiMOS SMP Kernel. The TiMOS SMP Kernel serves as the main interface between the router's physical hardware and the router's applications running on it. The kernel enables multiple applications to share hardware resources by providing access to CPU, memory, mass storage and networking.

1.6 LOGICAL SCOPE OF THE TOE

The TOE implements the following security functional requirements:

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

Each of these security functionalities are listed in more detail in the sections below.

1.6.1 SECURITY AUDIT

The TOE generates audit events for all start-up and shut-down functions and all auditable events as specified in Table 20. Audit events are also generated for management actions specified in FAU_GEN.1. The TOE is capable of storing audit events locally and exporting them to an external audit server using Syslog protocol over TLS v1.2 protocol. The TOE uses the Syslog protocol over TLS to transmit audit events in real-time, as they are generated, to an external audit server. Each audit record includes the date and time of the event, the event type, the identity of the subject, and any relevant event data.

1.6.2 CRYPTOGRAPHIC SUPPORT

The TOE provides cryptographic support for the services described in the tables below. The related CAVP validation details are provided in Table 8. The operating system is SROS version 24.10.R3 running on TiMOS SMP version 2.5. The TOE leverages the Nokia SR Cryptographic Module (SRCM) version 5, which is based on the OpenSSL v3.1.7 library and incorporates the FIPS module 3.1.6-nokia.1.0 as its FIPS provider, to provide its cryptographic functionality.

Table 8 – TOEs CAVP Algorithm References

SFRs	Algorithm in ST	Implementation Name	CAVP Alg	CAVP Cert
FCS_CKM.1	RSA schemes using cryptographic key sizes of [2048, 3072 and 4096 bits] 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.	Nokia SR Cryptographic Module (SRCM) version 5.0	RSA KeyGen (FIPS186-5)	A5455
	ECC schemes using ‘NIST curves’ [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4, 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.		ECDSA KeyGen (FIPS186-5) ECDSA KeyVer (FIPS186-5)	A5455
	FFC Schemes using ‘safe-prime’ groups that meet the following: “NIST Special Publication 800- 56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and [RFC 3526]		Lab tested using known good implementation	No NIST CAVP, CCTL has performed all assurance/evaluation activities and documented in the ETR and AAR accordingly.
FCS_CKM.2	RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017, “Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.2”	Nokia SR Cryptographic Module (SRCM) version 5.0	Lab tested using known good implementation	No NIST CAVP, CCTL has performed all assurance/evaluation activities and documented in the ETR and AAR accordingly.
	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”		KAS-ECC-SSC Sp800-56Ar3	A5455
	FFC Schemes using “safe-prime” groups that meet the following: ‘NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and [groups listed in RFC 3526]		Lab tested using known good implementation	No NIST CAVP, CCTL has performed all assurance/evaluation activities and documented in

SFRs	Algorithm in ST	Implementation Name	CAVP Alg	CAVP Cert
				the ETR and AAR accordingly.
FCS_COP.1/DataEncryption	GCM *mode* and cryptographic key sizes 128 bits, 256 bits that meet: *AES as specified in ISO 18033-3 and* GCM as specified in ISO 19772	Nokia SR Cryptographic Module (SRCM) version 5.0	AES-GCM	A5455
	CBC *mode* and cryptographic key sizes 128 bits, 256 bits that meet: *AES as specified in ISO 18033-3,* CBC as specified in ISO 10116.		AES-CBC	
	CTR *mode* and cryptographic key sizes 128 bits, 256 bits that meet: *AES as specified in ISO 18033-3,* and CTR as specified in ISO 10116.		AES-CTR	
FCS_COP.1/SigGen	RSA Digital Signature Algorithm using key sizes of 2048, 3072 and 4096 bits that meets 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	Nokia SR Cryptographic Module (SRCM) version 5.0	RSA SigGen (FIPS186-5) RSA SigVer (FIPS186-5)	A5455
	ECDSA schemes implementing [P-256, P-384, P-521] curves that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D, Implementing “NIST Recommended" curves ; or FIPS PUB 186-5, "Digital Signature Standard (DSS)", Section 6 and NIST SP 800-186 Section 3.2.1, Implementing Weierstrass curves; or ISO/IEC 14888-3, "IT Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms", Section 6.6.		ECDSA SigGen (FIPS186-5) ECDSA SigVer (FIPS186-5)	
FCS_COP.1/Hash	SHA-1, SHA-256, SHA-384 and SHA-512 and message digest sizes 160, 256, 384 and 512 bits	Nokia SR Cryptographic Module (SRCM) version 5.0	SHA-1 SHA2-256 SHA2-384 SHA2-512	A5455
FCS_COP.1/KeyedHash	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 with key sizes 160 bits, 256 bits, 384 bits, 512 bits and message digest 160, 256, 384, 512 bits	Nokia SR Cryptographic Module (SRCM) version 5.0	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512	A5455

SFRs	Algorithm in ST	Implementation Name	CAVP Alg	CAVP Cert
	that meet the following: ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”			
FCS_COP.1/CMAC	keyed-hash message authentication with AES-CMAC and key sizes 128, 256 bits and message digest size of 128 bits that meets: NIST SP 800-38B.	Nokia SR Cryptographic Module (SRCM) version 5.0	AES-CMAC	A5455
FCS_COP.1/MACSEC	Encryption and decryption in accordance with AES used in AES Key Wrap and key sizes 128 , 256 bits that meets AES as specified in ISO 18033-3, AES Key Wrap as specified in NIST SP 800-38F. Encryption and decryption in accordance with GCM and key sizes 128 , 256 bits that meets AES as specified in ISO 18033-3, GCM as specified in ISO 19772.	Nokia SR Cryptographic Module (SRCM) version 5.0	AES-KW AES-GCM	A5455
FCS_RBG_EXT.1	CTR_DRBG (AES) in accordance with ISO/IEC 18031:2011 with a minimum of 256-bits	Nokia SR Cryptographic Module (SRCM) version 5.0	Counter DRBG	A5455

The Broadcom PHY BCM81394 integrates two BCM81392 dies. As a result, each BCM81392 supports half the data rate per channel on the system side and half the number of 100G/10G ports. Additionally, PHY chips from Broadcom, Microsemi (now part of Microchip), and Nokia’s E5 series are used to perform AES-GCM encryption and decryption for the MACsec protocol. These PHYs have undergone CAVP testing by NIST to validate their cryptographic compliance.

Table 9 – MACsec PHYs CAVP Algorithm Testing References

Cryptographic Algorithms	CAVPS	Implementation Library	PHY devices	Operational Environment (OE)
AES-GCM	AES 3969	Microsemi Intellisec 10G PHY	VSC8258	Microsemi Intellisec 10G PHY
	AES 3191	Vitesse Intellisec 10G PHY	VSC8258	Vitesse Intellisec 10G PHY
	AES 3504	Microsemi Intellisec 1G PHY	VSC85xx	Microsemi Intellisec 1G PHY
	AES 2781	Vitesse Intellisec 10G PHY	VSC8490/91	Mentor Graphics Questasim 10.0d
	AES 4545	AES ECB 128bit & 256bit Encryption/Decryption Engine	BCM82396, BCM59202, BCM82399	AES ECB 128bit & 256bit Encryption/Decryption Engine
	C1877	AES ECB 128bit & 256bit Encryption/Decryption Engine	BCM81343, BCM81392, BCM81394, BCM81398	AES ECB 128bit & 256bit Encryption/Decryption Engine
	A5786	400G MACsec Encryption/Decryption Engine on Nokia E5	Nokia E5	Synopsys VCS 2023.03-SP2

1.6.3 IDENTIFICATION AND AUTHENTICATION

The TOE supports Role Based Access Control. All users must be authenticated to the TOE prior to carrying out any management actions. The TOE supports password-based authentication and public key-based authentication. Based on the assigned role, a user is granted a set of privileges to access the system.

1.6.4 SECURITY MANAGEMENT

The TOE supports local and remote management of its security functions including:

- Ability to administer the TOE remotely
- Ability to configure the access banner
- Ability to configure the remote session inactivity time before session termination
- Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates
- Ability to configure local audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full; changes to local audit storage size)
- Ability to modify the behaviour of the transmission of audit data to an external IT entity
- Ability to configure the cryptographic functionality
- Ability to configure thresholds for SSH rekeying
- Ability to set the time which is used for time-stamps
- Ability to manage the cryptographic keys
- 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
- Ability to configure the list of supported (D)TLS ciphers;
- Manage a PSK-based CAK and install it in the device
- Manage the key server to create, delete, and activate MKA participants [as specified in IEEE 802.1X-2020, Sections 9.13 and 9.16 (cf. MIB object ieee8021XKayMkaParticipant Entry) and section 12.2 (cf. function createMKA()]
- Specify the lifetime of a CAK
- Enable, disable, or delete a PSK-based CAK using [[CLI management command]]
- Manage generation of a PSK-based CAK

1.6.5 TOE ACCESS

Prior to establishing an administration session with the TOE, a banner is displayed to the user. The banner messaging is customizable. The TOE will terminate an interactive session after configurable number of minutes of session inactivity. A user can terminate their local CLI session and remote CLI session by entering the appropriate command at the prompt.

1.6.6 PROTECTION OF THE TSF

The TOE protects all passwords, pre-shared keys, symmetric keys, and private keys from unauthorized disclosure. Pre-shared keys, symmetric keys, and private keys are stored in encrypted format. Passwords are stored as a non-reversible hash value generated using a configurable hash function. The TOE executes self-tests during initial start-up to ensure correct operation and enforcement of its security functions. An administrator can install software updates to the TOE. The TOE internally maintains the date and time.

1.6.7 TRUSTED PATH/CHANNELS

The TOE supports syslog protocol over TLS v1.2 for secure communication to the audit server. The TOE supports TLS v1.2 for secure communication to LDAP and Radius servers for authentication. The TOE supports local CLI and uses SSH v2 for secure remote administration.

1.7 EXCLUDED FUNCTIONALITY

The following interfaces are not included as part of the evaluated configuration:

- NTP server.
- gRPC is disabled.
- telnet is disabled.
- MPLS is not evaluated.
- SNMP is not evaluated.
- Netconf is not evaluated.

1.8 TOE DOCUMENTATION

The table below lists the TOE guidance documentation. The Common Criteria (CC) guidance document and TOE ST are provided in .pdf form on the NIAP portal.

Table 10 – TOE Documentation

Reference	Title	Version	Date
[CC]	Nokia 7750 SR & 7250 IXR, SROS 24.10.R3, MACsec platforms Common Criteria Supplement Guide	0.7	August 22, 2025
[ST]	Nokia MACsec 7x50 SROS 24.10.R3 Security Target	1.2	August 22, 2025

1.9 OTHER REFERENCES

In addition to the TOE documentation, the following references are applied within this ST:

- Collaborative Protection Profile for Network Devices, Version 3.0e [CPP_ND_V3.0E]
- PP-Module for MACsec Ethernet Encryption, Version 1.0 [MOD_MACsec_V1.0]
- Functional Package for SSH Version 1.0 [PKG_SSH_V1.0]

2. CONFORMANCE CLAIMS

This section identifies the TOE conformance claims, conformance rationale, and relevant Technical Decisions (TDs).

2.1 CC CONFORMANCE CLAIMS

The TOE is conformant to the following:

- Common Criteria for Information Technology Security Evaluations Part 1, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 5, April 2017: Part 2 extended
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 5, April 2017: Part 3 conformant

2.2 PROTECTION PROFILE CONFORMANCE

This ST claims exact conformance to the following:

- PP-Configuration for Network Devices and MACsec Ethernet Encryption, 2023-03-29

This PP-Configuration includes the following:

- Collaborative Protection Profile for Network Devices, Version 3.0e (CPP_ND_V3.0E)
- PP-Module for MACsec Ethernet Encryption, Version 1.0 (MOD_MACsec_V1.0)

This ST also claims exact conformance to the following package:

- Functional Package for SSH Version 1.0 [PKG_SSH_V1.0]

2.3 CONFORMANCE RATIONALE

This ST provides exact conformance to the items listed in the previous section. The security problem definition, security objectives, and security requirements in this ST are all taken from the Protection Profile (PP) and Module/Package, performing only the operations defined there.

2.4 TECHNICAL DECISIONS

All NIAP Technical Decisions (TDs) issued to date and applicable to CPP_ND_V3.0E, MOD_MACsec_V1.0 and PKG_SSH_V1.0 have been addressed. Table 11 identifies all TDs relevant to CPP_ND_V3.0E**.** Table 12 identifies all TDs relevant to MOD_MACsec_V1.0. Table 13 identifies all TDs relevant to PKG_SSH_V1.0.

Table 11 – Technical Decisions for CPP_ND_V3.0e

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable)
TD0923 - NIT Technical Decision: Auditable event for FAU_STG_EXT.1 in FAU_GEN.1.2	Yes	

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable)
TD0921 - NIT Technical Decision: Addition of FIPS PUB 186-5 and Correction of Assignment	Yes	
TD0900 - NIT Technical Decision: Clarification to Local Administrator Access in FIA_UIA_EXT.1.3	Yes	
TD0899 - NIT Technical Decision: Correction of Renegotiation Test for TLS 1.2	Yes	
TD0886 - Clarification to FAU_STG_EXT.1 Test 6	Yes	
TD0880 - NIT Decision: Removal of Duplicate Selection in FMT_SMF.1.1	Yes	
TD0879 - NIT Decision: Correction of Chapter Headings in CPP_ND_V3.0E	Yes	
TD0868 - NIT Technical Decision: Clarification of time frames in FCS_IPSEC_EXT.1.7 and FCS_IPSEC_EXT.1.8	No	ST does not claim IPSEC SFR
TD0836 - NIT Technical Decision: Redundant Requirements in FPT_TST_EXT.1	Yes	

Table 12 – Technical Decisions for MOD_MACSEC_V1.0

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable)
TD0891 - Correlation of Implicitly Satisfied Requirements when CPP_ND_V3.0E is the Base-PP	Yes	
TD0889 - Correction for Tests Incorrectly Requiring Group MACsec	Yes	
TD0884 - Expansion of Permitted EtherTypes in FCS_MACSEC_EXT.1.4	Yes	
TD0882 - MACsec Data Delay Protection, Key Agreement, and Conditional Support for Group CAK	Yes	
TD0881 - Correction to MN Usage for FPT_RPL.1 Test	Yes	
TD0870 - Security Objectives Rationale for MOD_MACSEC_V1.0	Yes	
TD0840 - Alignment of Test 22.1 to FMT_SMF.1/MACSEC	Yes	

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable)
TD0826 - Aligning MOD_MACSEC_V1.0 with CPP_ND_V3.0E	Yes	
TD0816 - Clarity for MACsec Self-Test Failure Response	Yes	
TD0803 - Clarification for Configurable MACsec CKN Length	Yes	
TD0746 - Correction to FPT_RPL.1 Test 25	Yes	
TD0728 - Corrections to MACSec PP-Module SD	Yes	

Table 13 – Technical Decisions for PKG_SSH_V1.0

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable)
TD0909 - Updates to FCS_SSH_EXT.1.1 App Note in SSH FP 1.0	Yes	
TD0777 - Clarification to Selections for Auditable Events for FCS_SSH_EXT.1	Yes	
TD0732 - FCS_SSHS_EXT.1.3 Test 2 Update	Yes	
TD0695 - Choice of 128 or 256 bit size in AES-CTR in SSH Functional Package.	Yes	
TD0682 - Addressing Ambiguity in FCS_SSHS_EXT.1 Tests	Yes	

3. SECURITY PROBLEM DEFINITION

The security problem definition has been taken directly from CPP_ND_V3.0E, MOD_MACsec_V1.0 and PKG_SSH_V1.0 and is reproduced here for the convenience of the reader. The security problem is described in terms of the threats that the TOE is expected to address, assumptions about the operational environment, and any Organizational Security Policies (OSPs) that the TOE is expected to enforce.

3.1 THREATS

The threats included in Table 14 are drawn directly from the [CPP_ND_V3.0E], [PKG_SSH_V1.0] and [MOD_MACsec_V1.0].

Table 14 – Threats

ID	Threat
T.DATA_INTEGRITY	An attacker may modify data transmitted over the layer 2 link in a way that is not detected by the recipient. Devices on a network may be exposed to attacks that attempt to corrupt or modify data in transit without authorization. If malicious devices are able to modify and replay data that is transmitted over a layer 2 link, then the data contained within the communications may be susceptible to a loss of integrity.
T. NETWORK_ACCESS	An attacker may send traffic through the TOE that enables them to access devices in the TOE's operational environment without authorization. A MACsec device may sit on the periphery of a network, which means that it may have an externally facing interface to a public network. Devices located in the public network may attempt to exercise services located on the internal network that are intended to be accessed only from within the internal network or externally accessible only from specifically authorized devices. If the MACsec device allows unauthorized external devices access to the internal network, these devices on the internal network may be subject to compromise. Similarly, if two MACsec devices are deployed to facilitate end-to-end encryption of traffic that is contained within a single network, an attacker could use an insecure MACsec device as a method to access devices on a specific segment of that network such as an individual LAN.
T.UNTRUSTED_MACSEC_COMMUNICATION_CHANNELS	An attacker may acquire sensitive TOE or user data that is transmitted to or from the TOE because an untrusted communication channel causes a

ID	Threat
	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.
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 tunneling 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

ID	Threat
	and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the network device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials 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.

3.2 ASSUMPTIONS

The assumptions included in Table 15 are drawn directly from the [CPP_ND_V3.0E], [PKG_SSH_V1.0] and [MOD_MACsec_V1.0].

Table 15 – Assumptions

ID	Assumption
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).
A.NO_THRU_TRAFFIC_PROTECTION	standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).

ID	Assumption
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 being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. 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.

3.3 ORGANIZATIONAL SECURITY POLICIES

The OSPs included in Table 16 are drawn directly from the [CPP_ND_V3.0E], [PKG_SSH_V1.0] and [MOD_MACsec_V1.0].

Table 16 – OSPs

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

4. SECURITY OBJECTIVES

The security objectives have been taken from CPP_ND_V3.0E, MOD_MACsec_V1.0 and PKG_SSH_V1.0 and are reproduced here for the convenience of the reader.

4.1 SECURITY OBJECTIVES FOR THE TOE

The following security objectives for the TOE assist the TOE in correctly providing its security functionality. These track with the assumptions about the TOE.

Table 17 – Security Objectives

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

ID	Security Objectives
	security-relevant data that administrators do not need to view.
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.
O.AUTHENTICATION_MACSEC [TD0870]	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.TSF_INTEGRITY [TD0870]	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 OPERATIONAL ENVIRONMENT

The security objectives have been taken from CPP_ND_V3.0E and are reproduced here for the convenience of the reader. The table below describes the Objectives for the Operational Environment:

Table 18 – Security Objectives for the Operational Environment

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

ID	Objectives for the Operational 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 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. 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. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.

5. SECURITY REQUIREMENTS

This section identifies the Security Functional Requirements (SFRs) for the TOE. The SFRs included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revisions 5, April 2017, and all international interpretations.

Table 19 – SFRs

Requirement	Description
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_STG_EXT.1	Protected Audit Event Storage
FAU_GEN.1/MACSEC	Audit Data Generation (MACsec)
FCS_CKM.1	Cryptographic Key Generation
FCS_CKM.2	Cryptographic Key Establishment
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/Decryption)
FCS_COP.1/SigGen	Cryptographic Operation (Signature Generation and Verification)
FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)
FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)
FCS_COP.1/CMAC	Cryptographic Operation (AES-CMAC Keyed Hash Algorithm)
FCS_COP.1/MACSEC	Cryptographic Operation (MACsec AES Data Encryption/Decryption)
FCS_MACSEC_EXT.1	MACsec
FCS_MACSEC_EXT.2	MACsec Integrity and Confidentiality
FCS_MACSEC_EXT.3	MACsec Randomness
FCS_MACSEC_EXT.4	MACsec Key Usage
FCS_MKA_EXT.1	MACsec Key Agreement
FCS_RBG_EXT.1	Random Bit Generation
FCS_SSH_EXT.1	SSH Protocol
FCS_SSHS_EXT.1	SSH Server Protocol
FCS_TLSC_EXT.1	TLS Client Protocol
FCS_TLSC_EXT.2	TLS Client Protocol with Mutual Authentication
FIA_AFL.1	Authentication Failure Handling
FIA_PMG_EXT.1	Password Management
FIA_PSK_EXT.1	Pre-shared Key Composition
FIA_UIA_EXT.1	User Identification and Authentication
FIA_UAU.7	Protected Authentication Feedback
FIA_X509_EXT.1/Rev	X.509 Certificate Validation
FIA_X509_EXT.2	Certificate Authentication

Requirement	Description
FIA_X509_EXT.3	Certificate Requests
FMT_MOF.1/Functions	Management of security functions behaviour
FMT_MOF.1/ManualUpdate	Management of security functions behaviour
FMT_MTD.1/CoreData	Management of TSF Data
FMT_MTD.1/CryptoKeys	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMF.1/MACSEC	Specification of Management Functions (MACsec)
FMT_SMR.2	Restrictions on security roles
FPT_APW_EXT.1	Protection of Administrator Passwords
FPT_CAK_EXT.1	Protection of CAK Data
FPT_FLS.1	Failure with Preservation of Secure State
FPT_RPL.1	Replay Detection
FPT_SKP_EXT.1	Protection of TSF Data (for reading of all symmetric keys)
FPT_STM_EXT.1	Reliable Time Stamps
FPT_TST_EXT.1	TSF Testing
FPT_TUD_EXT.1	Trusted Update
FTA_SSL_EXT.1	TSF-initiated Session Locking
FTA_SSL.3	TSF-initiated Termination
FTA_SSL.4	User-initiated Termination
FTA_TAB.1	Default TOE Access Banner
FTP_ITC.1	Inter-TSF trusted channel
FTP_ITC.1/MACSEC	Inter-TSF trusted channel (MACsec Communications)
FTP_TRP.1/Admin	Trusted Path

5.1 CONVENTIONS

The CC allows the following types of operations to be performed on the functional requirements: assignments, selections, refinements, and iterations. The following font conventions are used within this document to identify operations defined by CC:

- Assignment: Indicated with *italicized* text.
- Refinement: Indicated with **bold** text.
- Selection: Indicated with underlined text.
- Iteration: Indicated by appending the iteration identifier after a slash, e.g., /SigGen.
- Where operations were completed in the PP and relevant EPs/Modules/Packages, the formatting used in the PP has been retained, except strikeout texts has been removed.
- Extended SFRs are identified by the addition of "EXT" after the requirement name.

5.2 SECURITY FUNCTIONAL REQUIREMENTS

This section includes the security functional requirements for this ST.

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) Auditable events for the not specified level of audit; and

c) *All administrative actions comprising:*

- *Administrative login and logout (name of Administrator account shall be logged if individual 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 Administrator account shall be logged)];*

d) Specifically defined auditable events listed in Table 20.

FAU_GEN.1.2 [TD0777]

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 cPP/ST, *information specified in column three of Table 20.*

Table 20 – Security Functional Requirements and Auditable Events

Requirement	Auditable Events	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_COP.1/CMAC	None.	None.
FCS_TLSC_EXT.1	Failure to establish a TLS Session.	Reason for failure.
FCS_TLSC_EXT.2	None.	None.

Requirement	Auditable Events	Additional Audit Record Contents
FCS_SSH_EXT.1 [TD0777]	[Failure to establish SSH connection]	[Reason for failure and Non-TOE endpoint of attempted connection (IP Address)]
	[Establishment of SSH connection]	[Non-TOE endpoint of connection (IP Address)]
	[Termination of SSH connection session]	[Non-TOE endpoint of connection (IP Address)]
	[Dropping of packet(s) outside defined size limits]	[Packet size]
FCS_SSHS_EXT.1	No events specified	
FCS_RBG_EXT.1	None.	None.
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).
FIA_X509_EXT.1/Rev	- Unsuccessful attempt to validate a certificate - Any addition, replacement or removal of trust anchors in the TOE's trust store	- Reason for failure of certificate validation - Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store
FIA_X509_EXT.2	None.	None.
FIA_X509_EXT.3	None.	None.
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address)
FIA_UAU.7	None.	None.
FMT_MOF.1/Functions	None.	None.
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.
FMT_MTD.1/CoreData	None.	None.
FMT_MTD.1/CryptoKeys	None.	None.
FMT_SMF.1	All management activities of TSF data.	None.
FMT_SMR.2	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_SKP_EXT.1	None	None
FPT_STM.1_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FPT_TST_EXT.1	None.	None.

Requirement	Auditable Events	Additional Audit Record Contents
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None.
FTA_SSL_EXT.1 (if "terminate the session is selected)	The termination of a local session by the session lock	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.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.

5.2.1.3 FAU_STG_EXT.1 PROTECTED AUDIT EVENT STORAGE

FAU_STG_EXT.1.1
The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1.

FAU_STG_EXT.1.2
The TSF shall be able to store generated audit data on the TOE itself. In addition [

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

].

FAU_STG_EXT.1.3
The TSF shall maintain a [*log file*] 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 [persistent] audit records locally with a minimum storage size of [*50 to 3000 records and file size of 6.8GB*].

FAU_STG_EXT.1.5
The TSF shall [overwrite previous audit records according to the following rule: [*the oldest log file is 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].

5.2.1.4 FAU_GEN.1/MACSEC AUDIT DATA GENERATION (MACSEC)

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

a. Start-up and shutdown of the audit functions;
b. All auditable events for the [*not specified*] level of audit;
c. **All administrative actions;**
d. **[*Specifically defined auditable events listed in the Auditable Events table (Table 21)*]**

Table 21 – Auditable Events for MACsec

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

FAU_GEN.1.2/MACSEC
The TSF shall record within each audit record at least the following information:

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP-**Module**/ST, [*information specified in column three of the Auditable Events table (Table 21)*].

5.2.2 CRYPTOGRAPHIC SUPPORT (FCS)

5.2.2.1 FCS_CKM.1 CRYPTOGRAPHIC KEY GENERATION

FCS_CKM.1.1 [TD0921]
The TSF shall generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm: [

- RSA schemes using cryptographic key sizes of [*2048, 3072 and 4096 bits*] 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, P-521] 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.;
- FFC Schemes using 'safe-prime' groups that meet the following: "NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [RFC 3526].

]

5.2.2.2 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: [

- RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.2";
- 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";
- FFC Schemes using "safe-prime" groups that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [groups listed in RFC 3526].

]

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]]*;*
- *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 [*
    - instructs a part of the TSF to destroy the abstraction that represents the key]

that meets the following: *No Standard.*

5.2.2.4 FCS_COP.1/DATAENCRYPTION CRYPTOGRAPHIC OPERATIONS (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, CTR, GCM] *mode* and cryptographic key sizes [128 bits, 256 bits] that meet the following: *AES as specified in ISO 18033-3,* [CBC as specified in ISO 10116, CTR as specified in ISO 10116, GCM as specified in ISO 19772].

5.2.2.5 FCS_COP.1/SIGGEN CRYPTOGRAPHIC OPERATION (SIGNATURE GENERATION AND VERIFICATION)

FCS_COP.1.1/SigGen [TD0921]
The TSF shall perform *cryptographic signature services (generation and verification)* in accordance with a specified cryptographic algorithm [

- RSA Digital Signature Algorithm,
- Elliptic Curve Digital Signature Algorithm

]
and cryptographic key sizes [

- For RSA: [modulus 2048, 3072 and 4096 bits],
- For ECDSA: [256, 384, and 521 bits]

]
that meets 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,
- For ECDSA schemes implementing [P-256, P-384, P-521] curves that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D, Implementing “NIST Recommended” curves ; or FIPS PUB 186-5, "Digital Signature Standard (DSS)", Section 6 and NIST SP 800-186 Section 3.2.1, Implementing Weierstrass curves; or ISO/IEC 14888-3, "IT Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms", Section 6.6,

].

5.2.2.6 FCS_COP.1/HASH CRYPTOGRAPHIC OPERATIONS (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 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-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512] and cryptographic key sizes [160 bits, 256 bits, 384 bits, 512 bits] **and message digest sizes** [160, 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 SP 800-38B*].

5.2.2.9 FCS_COP.1/MACSEC CRYPTOGRAPHIC OPERATION (MACSEC AES DATA ENCRYPTION AND DECRYPTION)

FCS_COP.1.1/MACSEC
The TSF shall perform [*encryption and decryption*] in accordance with a specified cryptographic algorithm [*AES used in AES Key Wrap, GCM*] and cryptographic key sizes [*128, 256*] **bits** that meets the following: [*AES as specified in ISO 18033-3, AES Key Wrap as specified in NIST SP 800-38F, GCM as specified in ISO 19772*].

5.2.2.10 FCS_MACSEC_EXT.1 MACSEC

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

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

FCS_MACSEC_EXT.1.3
The TSF shall reject any MPDUs during a given session that contain an SCI other than the one used to establish that session.

FCS_MACSEC_EXT.1.4 [TD0884]
The TSF shall permit only EAPOL (Port Access Entity (PAE) EtherType 88-8E), MACsec frames (EtherType 88-E5), and [MAC control frames (EtherType is 88-08)] and shall discard others.

5.2.2.11 FCS_MACSEC_EXT.2 MACSEC INTEGRITY AND CONFIDENTIALITY

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

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

FCS_MACSEC_EXT.2.3
The TSF shall provide the ability to derive an Integrity Check Value Key (ICK) from a Connectivity Association Key (CAK) using a KDF.

5.2.2.12 FCS_MACSEC_EXT.3 MACSEC RANDOMNESS

FCS_MACSEC_EXT.3.1
The TSF shall generate unique Secure Association Keys (SAKs) using [the TOE's random bit generator as specified by FCS_RBG_EXT.1] such that the likelihood of a repeating SAK is no less than 1 in 2 to the power of the size of the generated key.

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.

5.2.2.13 FCS_MACSEC_EXT.4 MACSEC KEY USAGE

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

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

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

FCS_MACSEC_EXT.4.4
The TSF shall associate Connectivity Association Key Names (CKNs) with SAKs that are defined by the KDF using the CAK as input data (per IEEE 802.1X-2010, 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).

5.2.2.14 FCS_MKA_EXT.1 MACSEC KEY AGREEMENT

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

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

FCS_MKA_EXT.1.3
The TSF shall provide the ability to derive an Integrity Check Value Key (ICK) from a CAK using a KDF.

FCS_MKA_EXT.1.4 [TD0882]
The TSF shall enforce an MKA Lifetime Timeout limit of 6.0 seconds and [MKA Bounded Hello Timeout 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 CAKs that are PSKs

].

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

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

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

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

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

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

5.2.2.15 FCS_RBG_EXT.1 RANDOM BIT GENERATION

FCS_RBG_EXT.1.1
The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [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*] software-based noise source] with a minimum of [256 bits] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”, of the keys and hashes that it will generate.

5.2.2.16 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, [4344, 5656, 6668, 8268, 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” (RFC 4252),
- “publickey” (RFC 4252): [
  - ssh-rsa (RFC 4253),
  - rsa-sha2-256 (RFC 8332),
  - rsa-sha2-512 (RFC 8332),
  - ecdsa-sha2-nistp256 (RFC 5656),

  - ecdsa-sha2-nistp384 (RFC 5656),
  - ecdsa-sha2-nistp521 (RFC 5656),

]

] and no other methods.

FCS_SSH_EXT.1.3
The TSF shall ensure that, as described in RFC 4253, packets greater than [*256K*] in an SSH transport connection are dropped.

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

- aes128-ctr (RFC 4344),
- aes256-ctr (RFC 4344),
- aes128-cbc (RFC 4253),
- aes256-cbc (RFC 4253),

] 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 6668),

] and no other mechanisms.

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

- diffie-hellman-group14-sha256 (RFC 8268),
- diffie-hellman-group16-sha512 (RFC 8268),

] and no other mechanisms.

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

- RFC 4253 (Section 7.2),
- 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.

5.2.2.17 FCS_SSHS_EXT.1 SSH PROTOCOL – SERVER

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

- rsa-sha2-256 (RFC 8332),
- rsa-sha2-512 (RFC 8332),
- ecdsa-sha2-nistp256 (RFC 5656),
- ecdsa-sha2-nistp384 (RFC 5656),
- ecdsa-sha2-nistp521 (RFC 5656),

].

5.2.2.18 FCS_TLSC_EXT.1 TLS CLIENT PROTOCOL

FCS_TLSC_EXT.1.1
The TSF shall implement [TLS 1.2 (RFC 5246)] supporting the following ciphersuites: [

- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC5246
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

] and no other ciphersuites.

FCS_TLSC_EXT.1.2
The TSF shall verify that the presented identifier matches [the reference identifier per RFC 6125 Section 6, IPv4 address in the CN or in the SAN, IPv6 address in the CN or in the SAN, and no other attribute types].

FCS_TLSC_EXT.1.3
The TSF shall not establish a trusted channel if the server certificate is invalid [

- without any administrator override mechanism.

].

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

FCS_TLSC_EXT.1.5
The TSF shall [

- present the signature algorithms extension with support for the following algorithms: [
  - rsa_pkcs1 with sha256(0x0401),
  - rsa_pkcs1with sha384(0x0501),
  - rsa_pkcs1 with sha512(0x0601),
  - rsa_pss_rsae with sha256(0x0804),
  - rsa_pss_rsae with sha384(0x0805),
  - rsa_pss_rsae with sha512(0x0806),
  - rsa_pss_pss with sha256(0x0809),
  - rsa_pss_pss with sha384(0x080a),

- rsa_pss_pss with sha512(0x080b)
-] and no other algorithms;

].

FCS_TLSC_EXT.1.6
The TSF [provides] the ability to configure the list of supported ciphersuites as defined in FCS_TLSC_EXT.1.1.

FCS_TLSC_EXT.1.7
The TSF shall prohibit the use of the following extensions:

- Early data extension
- Post-handshake client authentication according to RFC 8446, Section 4.2.6.

FCS_TLSC_EXT.1.8
The TSF shall [not use PSKs].

FCS_TLSC_EXT.1.9
The TSF shall [support TLS 1.2 secure renegotiation through use of the "renegotiation_info" TLS extension in accordance with RFC 5746, reject [TLS 1.2] renegotiation attempts].

Application Note: TOE supports TLS v1.2 secure renegotiation when operating in the role of a RADIUS or LDAP clients. However, TOE does not accept TLS v1.2 secure renegotiation requests when establishing connections to external syslog server.

5.2.2.19 FCS_TLSC_EXT.2 TLS CLIENT SUPPORT FOR MUTUAL AUTHENTICATION

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

5.2.3 IDENTIFICATION AND AUTHENTICATION (FIA)

5.2.3.1 FIA_AFL.1 AUTHENTICATION FAILURE HANDLING

FIA_AFL.1.1
The TSF shall detect when an Administrator configurable positive integer within *[1-64]* 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: ["~" "!" "@" "#" "$" "%" "^" "&" "*" "(" ")" "-" "_" "+" "=" "[" "{" "]" "}" "\" "|" ";" ":" "'" "," "<" "." ">" "/" "?"];

b) Minimum password length shall be *configurable to between [6] and [50] characters.*

5.2.3.3 FIA_PSK_EXT.1 PRE-SHARED KEY COMPOSITION

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

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

5.2.3.4 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 actions on behalf of that administrative user.

FIA_UIA_EXT.1.3 [TD0900]
The TSF shall provide the following remote authentication mechanisms [SSH password, SSH public key] and [external authentication server]. The TSF shall provide the following local authentication mechanisms [password-based, [*RADIUS, LDAP*]*].*

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 certification path validation **supporting a minimum path length of three certificates**.

- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [*a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3*].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
    - *Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.*
    - *Server certificates presented for DTLS/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 DTLS/TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsagefield.*
    - *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 [TLS] and [no additional uses].

FIA_X509_EXT.2.2

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

5.2.3.8 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/FUNCTIONS MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOUR

FMT_MOF.1.1/Functions
The TSF shall restrict the ability to [modify the behaviour of] the functions [transmission of audit data to an external IT entity] to *Security Administrators*.

5.2.4.2 FMT_MOF.1/MANUALUPDATE MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOR

FMT_MOF.1.1/ManualUpdate
The TSF shall restrict the ability to enable the functions *to perform manual updates* to *Security Administrators.*

5.2.4.3 FMT_MTD.1/COREDATA MANAGEMENT OF TSF DATA

FMT_MTD.1.1/CoreData
The TSF shall restrict the ability to *manage* the *TSF data* to *Security Administrators*.

5.2.4.4 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*.

5.2.4.5 FMT_SMF.1 SPECIFICATION OF MANAGEMENT FUNCTIONS

FMT_SMF.1.1 [TD0880]
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 remote session inactivity time before session termination;*
- *Ability to update the TOE, and to verify the updates using* digital signature *capability prior to installing those updates;*
- [
    - ○ Ability to configure local audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full; changes to local audit storage size);
    - ○ Ability to modify the behaviour 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 set the time which is used for time-stamps;
    - ○ Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;
    - ○ Ability to 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;
    - ○ Ability to configure the list of supported (D)TLS ciphers*;*

  ].

5.2.4.6 FMT_SMF.1/MACSEC SPECIFICATION OF MANAGEMENT FUNCTIONS (MACSEC)

FMT_SMF.1.1/MACSEC

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

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

[

- Manage generation of a PSK-based CAK

]].

5.2.4.7 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 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_SKP_EXT.1 PROTECTION OF TSF DATA (FOR READING OF ALL SYMMETRIC KEYS)

FPT_SKP_EXT.1.1

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

5.2.5.3 FPT_CAK_EXT.1 PROTECTION OF CAK DATA

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

5.2.5.4 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*].

5.2.5.5 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.

5.2.5.6 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 [TD0836]
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 [[*periodically at the conditions [BIOS checks, cryptographic library functionality test, and firmware integrity checks*]] 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 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 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 **Administrator**-initiated termination of the **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 use of the TOE.

5.2.7 TRUSTED PATH/CHANNELS (FTP)

5.2.7.1 FTP_ITC.1 INTER-TSF TRUSTED CHANNEL (REFINEMENT)

FTP_ITC.1.1

The TSF shall **be capable of using [TLS] to** provide a **trusted** communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, [**authentication servers] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure **and detection of modification of the channel data**.

FTP_ITC.1.2

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

FTP_ITC.1.3

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

5.2.7.2 FTP_ITC.1/MACSEC INTER-TSF TRUSTED CHANNEL (MACSEC COMMUNICATIONS)

FTP_ITC.1.1/MACSEC

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

FTP_ITC.1.2/MACSEC

The TSF shall permit [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** 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 FOR SFRS

The PP and any relevant Modules/Packages contain(s) all the requirements claimed in this ST. As such, the dependencies are not applicable since the PP has been approved.

5.4 SECURITY ASSURANCE REQUIREMENTS

The TOE assurance requirements for this ST are taken directly from the PP and any relevant Modules/Packages, which is/are derived from Common Criteria Version 3.1, Revision 5. The assurance requirements are summarized in Table 22.

Table 22 – Security Assurance Requirements

Assurance Class	Assurance Components	Component Description
Security Target	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_FSP.1	Basic functional specification
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life Cycle Support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_IND.1	Independent testing – conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability survey

5.5 ASSURANCE MEASURES

The TOE satisfied the identified assurance requirements. This section identifies the Assurance Measures applied by Nokia to satisfy the assurance requirements. The following table lists the details.

Table 23 – TOE Security Assurance Measures

SAR Component	How the SAR will be met
ASE_TSS.1.1C Refinement	The TOE summary specification shall describe how the TOE meets each SFR. In the case of entropy analysis, the TSS is used in conjunction with required supplementary information on Entropy.
ADV_FSP.1	The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error

SAR Component	How the SAR will be met
	messages (identifies the condition that generated it, what the message is, and the meaning of any error codes).
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.
AGD_PRE.1	The Installation Guide describes the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.1	The Configuration Management (CM) documents describe how the consumer identifies the evaluated TOE. The CM documents identify the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked and how potential changes are incorporated.
ALC_CMS.1	
ATE_IND.1	Nokia will provide the TOE for testing
AVA_VAN.1	Nokia will provide the TOE for testing. Nokia will provide a document identifying the list of software and hardware components.

6. TOE SUMMARY SPECIFICATION

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

Table 24 – TOE Summary Specification SFR Description

Requirement	TSS Description
FAU_GEN.1 FAU_GEN.1/MACSEC	The TOE produces audit events for start-up and shutdown of the audit functions as well as the following: administrative login and logout; password resets; changes to the TOE data related to configuration; the generation, import of, changing, or deletion of cryptographic keys, and for auditable events defined in the MACsec v1.0 PP-Module. Audit records include the identity of the administrator initiating the cryptography related events such as, key generation (e.g. RSA), import, or deletion. The audit record contains information such as, the identity of the key (unique name including the size and type), the date and time of the event, type of event, and the outcome of the event. The following is an example of an audit record for key generation: 1436 2025/03/10 15:43:14.483 UTC MINOR: SECURITY #2231 management admin “admin certificate gen-keypair cf3:/test.key1 size 2048 type rsa : success” The following is an example of an audit record for key import: 197 2021/03/24 17:35:22.606 UTC MINOR: SECURITY #2232 management admin "admin certificate import type certificate input cf3:\client_ixre.pem output client.pem format pem : success" The following is an example of an audit record for key deletion: 198 2021/03/24 17:36:53.864 UTC MINOR: SECURITY #2234 management admin "File cf3-A:\system-pki\test.key delete: success" Only Authorized Administrators can access the audit events and have the ability to clear the audit events. The TOE creates audit records for events and provides contents as required for all SFRs specified in Table 20 and 21.
FAU_GEN.2	For audit events that result from actions of identified users, the TOE can associate each auditable event with the identity of the user that caused the event.
FAU_STG_EXT.1	The TOE is a standalone TOE that stores audit data locally and can be configured to export audit data to a specified, external audit server. The TOE protects communications with an external audit server via syslog over TLS v1.2. The TOE transmit audit data to the external audit server in real time as soon as the audit event is generated through the syslog protocol over TLS v1.2. The TOE can rollover from one log file to the next log file based on rollover time. For the TOE to successfully create a log file, the compact flash disk must have a minimum of 10% or 5MB of free space. The TOE is designed to store 6.8 GB records in a compact flash drive. When the local storage space for audit data is full, the TOE will overwrite the oldest log file. Upon TOE’s reboot, power-off, or power failure, the local audit logs remain persistent.

<table>
<tr><th>Requirement</th><th>TSS Description</th></tr>
<tr><td></td><td>The TOE allows to create/manage administrators with different privileges. Some available options to configure such administrators are: “user profile membership”, “grant/deny a user access permission for console ftp grpc li netconf or snmp”, “restrict user to home directory”.
Only Authorized Administrators can access the audit events and have the ability to clear the audit events. The TOE does not allow non-privileged administrators to modify the audit records that are stored locally on the device.</td></tr>
<tr><td>FCS_CKM.1</td><td>To support the cryptographic protocols, the TOE uses RSA schemes using cryptographic key sizes of 2048, 3072 and 4096 bits that meet the following: FIPS PUB 186-5, “Digital Signature Standard (DSS)”, Appendix A.1. The TOE supports FFC Schemes using ‘safe-prime’ groups that meet the following: “NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and RFC 3526. The TOE supports ECC schemes using ‘NIST curves’ [P-256, P-384, P-521] that meet FIPS PUB 186-5, “Digital Signature Standard (DSS)”, Appendix A.2.
The TOE supports DHG14 and DHG16 key generation in support of DH key exchanges as part of SSH.
For both TLS and SSH communications, the RSA and EC keys are used in support of digital signatures.
The relevant NIST CAVP certificate numbers are listed in Table 8.</td></tr>
<tr><td>FCS_CKM.2</td><td>The TOE performs cryptographic key establishment in accordance with RSA key establishment schemes that are conformant to RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017, “Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.2”. The TOE supports FFC Schemes using “safe-prime” groups that meet the following: ‘NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and groups listed in RFC 3526. The TOE supports elliptic curve-based key establishment schemes that meets NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”.
The relevant NIST CAVP certificate numbers are listed in Table 8.
<table>
<tr><th>Scheme</th><th>SFR</th><th>Service</th></tr>
<tr><td>FFC/DHG14/DHG16</td><td>FCS_SSHS_EXT.1</td><td>Administration</td></tr>
<tr><td></td><td>FCS_TLSC_EXT.1</td><td>Audit server</td></tr>
<tr><td></td><td>FCS_TLSC_EXT.1</td><td>Radius server</td></tr>
<tr><td></td><td>FCS_TLSC_EXT.1</td><td>LDAP server</td></tr>
<tr><td>ECC</td><td>FCS_TLSC_EXT.1</td><td>LDAP server</td></tr>
<tr><td></td><td>FCS_TLSC_EXT.1</td><td>Radius server</td></tr>
<tr><td></td><td>FCS_TLSC_EXT.1</td><td>Audit Server</td></tr>
</table>
</td></tr>
<tr><td>FCS_CKM.4</td><td>The TOE destroys all cryptographic keys using the following methods:
• For plaintext keys in volatile storage, the TOE uses a single overwrite consisting of zeroes.
• For all plaintext keys in non-volatile storage, the TOE destroys keys via invocation of a command line interface provided by a part of the TOE that instructs TOE to destroy the abstraction that represents the key.</td></tr>
</table>

<table>
<tr><th>Requirement</th><th>TSS Description</th></tr>
<tr><td></td><td>There are no configurations or circumstances that may not conform to the key destruction mechanism. Please refer to Table 25.</td></tr>
<tr><td>FCS_COP.1/DataEncryption</td><td>The TOE supports AES encryption and decryption conforming to ISO 18033-3, ISO 10116 and ISO 19772.
The AES key sizes supported are 128 bits and 256 bits and the AES modes supported are: CBC, CTR and GCM. The TOE provides AES encryption and decryption in support of TLS v1.2, RBG and SSHv2 for secure communications.
The relevant NIST CAVP certificate numbers are listed in Table 8.</td></tr>
<tr><td>FCS_COP.1/SigGen</td><td>The TOE supports cryptographic signature services such as generation and verification using RSA Digital Signature Algorithm that meet the RSA scheme specified in FIPS PUB 186-5, “Digital Signature Standard (DSS)”, Section 5.4, using PKCS #1 v2.2 Signature Schemes RSASSA-PKCS1v1_5.
The RSA key size supported are 2048, 3072 and 4096 bits. The ECDSA key sizes supported are 256, 384 and 521 bits.
The relevant NIST CAVP certificate numbers are listed in Table 8.</td></tr>
<tr><td>FCS_COP.1/Hash</td><td>The TOE supports Cryptographic hashing services conforming to ISO/IEC 10118-3:2004. The hashing algorithms are used in SSH, and TLS connections for secure communications. In addition, the TOE uses hashing for password file protection with a configurable hash function and employs the SHA-256 algorithm for software update digital signature verification.
The following hashing algorithms are supported: SHA-1, SHA-256, SHA-384, and SHA-512.
The message digest sizes supported are: 160, 256, 384, and 512 bits.
The relevant NIST CAVP certificate numbers are listed in Table 8.</td></tr>
<tr><td>FCS_COP.1/KeyedHash</td><td>The TOE performs keyed-hash message authentication in accordance with ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”.
The details of Key Size and Message Digest Size are given below with the respective HMAC Algorithm.
<table>
<tr><th>HMAC Algorithm</th><th>Hash Function</th><th>Block Size</th><th>Key Lengths</th><th>MAC Lengths</th></tr>
<tr><td>HMAC-SHA-1</td><td>SHA-1</td><td>512 bits</td><td>160 bits</td><td>160 bits</td></tr>
<tr><td>HMAC-SHA-256</td><td>SHA-256</td><td>512 bits</td><td>256 bits</td><td>256 bits</td></tr>
<tr><td>HMAC-SHA-384</td><td>SHA-384</td><td>1024 bits</td><td>384 bits</td><td>384 bits</td></tr>
<tr><td>HMAC-SHA-512</td><td>SHA-512</td><td>1024 bits</td><td>512 bits</td><td>512 bits</td></tr>
</table>
The TOE leverages HMAC algorithm in support of TLS and SSH sessions.
The relevant NIST CAVP certificate numbers are listed in Table 8.</td></tr>
<tr><td>FCS_COP.1/CMAC</td><td>The TOE supports keyed-hash message authentication in accordance with AES-CMAC algorithm conforming to NIST SP 800-38B, with supported key sizes of 128 bits and 256 bits, a fixed block size of 128 bits, and a message digest size of 128 bits.</td></tr>
<tr><td>FCS_COP.1/MACSEC</td><td>The TOE supports AES encryption and decryption conforming to ISO 18033-3, AES Key Wrap as specified in NIST SP 800-38F and GCM as specified in ISO 19772.</td></tr>
</table>

Requirement	TSS Description
	The AES key sizes supported are 128 bits and 256 bits and the AES modes supported are: AES key Wrap, and GCM. The TOE provides AES encryption and decryption in support of MACsec for secure communications with MACsec peers. The relevant NIST CAVP certificate numbers are listed in Table 8.
FCS_MACSEC_EXT.1 FTP_ITC.1/MACSEC	The TOE implements MACsec in accordance with IEEE Standard 802.1AE-2018. The TOE conforms to IEEE 802.1AE-2018, Sections 5.3a-h, 5.3j-q, 5.4e-h, 8, 9, 10.5,10.6 and 14; IEEE 802.1AEbw-2013 sections 8, 9, 10 and 14. The MACsec connections preserve confidentiality of communicated data and act to protect against frames that are wrongly transmitted. The TOE receives SCI based on the port MAC address and sub-port/VLAN ID (1 to 1023). The TOE rejects data with an incorrect SCI value. The TOE permits only EAPOL (PAE EtherType 88-8E), MACsec frames (EtherType 88-E5), and MAC control frames (EtherType is 88-08) and discards others.
FCS_MACSEC_EXT.2	The TOE provides integrity protection by limiting confidentially offsets to 0, 30 and 50 values. The TOE derives the ICV from a CAK using KDF, using the SCI as the most significant bits of the IV and the 32 least significant bits of the PN as the IV. The supported ICV length is 16 octets. An ICV derived with the SAK is used to provide assurance of the integrity of MPDUs. The ICV is generated in 2 modes: • With the compliance of 802.1AE, L2 MAC is in clear, and all other bytes are encrypted and also part of the ICV calculation. • When VLAN is clear, 802.1q tags are not part of the ICV calculation.
FCS_MACSEC_EXT.3	The TOE supports CAK of 32 hex characters for aes-128-cmac encryption algorithm and 64 hex characters for aes-256-cmac encryption algorithm. The TOE supports CAK, which is based on AES cipher in CMAC mode and key sizes of 128 and 256 bits. Each of the keys used by MKA is derived from the CAK. When the TOE uses AES 128-bit CMAC mode encryption, the supported key string is 32-bit hexadecimal in length. When the TOE uses 256-bit encryption, the supported key size is 64-bit hexadecimal in length. SAKs are generated using the Key Server's RNG function, 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.4 FTP_ITC.1/MACSEC	The TOE ensures MACsec peer authentication by only using pre-shared keys. The TOE uses AES Key Wrap as specified in FCS_COP.1.1/MACSEC to distribute the SAKs between peers. The TOE supports aes-128-cmac or aes-256-cmac for SAK Wrapping.
FCS_MKA_EXT.1	The TOE supports Key Agreement Protocol (MKA) in agreement with standard IEEE 802.1X-2010 and 802.1Xbx-2014. The TOE implements MKA Lifetime Timeout limit of 6 to 18 seconds and a Hello Timeout limit of 2 sec with Hello Timeout configuration values of 500ms, and 1 to 6 sec.

Requirement	TSS Description
	The TOE allows for the configuration of the replayWindow size. For any encrypted data packets arriving with a PN in the SecTag, if the PN falls out of the replayWindow, it gets dropped and LatePkt counter is incremented. The TOE runs assurance of the integrity of MKA protocol data units using an ICV derived from the ICK. The ICK is derived from the CAK as per IEEE 802.1X-2010, Section 9.3.3 derived keys using AES-CMAC. The ICV is checked on the reception of each MKA PDU. The TOE refreshes the SAK in the following situations: • When a live peer leaves the CA or a new host has joined the CA domain and becomes a member. • When PN (Packet Number) reaches 0xc0000000 (or XPN 0xc000000000000000) a new SAK is generated in order to avoid PN exhaustion. • When a new PSK is configured and a rollover of PSK has been executed. The TOE supports pairwise CAK. Additionally, the TOE discards the MKPDU with individual addresses. The TOE checks the MKPDU length and discards MKPDUs smaller than 32 octets. The TOE also verifies and discards MKPDUs that are not multiples of 4 octets long. The TOE verifies the size as required by the basic parameter set body length and discards MKPDUs with unrecognized CKN. If an MKPDU passes these tests, then the TOE 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 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.
FCS_RBG_EXT.1	The TOE produces all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using CTR_DRBG (AES). The TOE uses a deterministic RBG, which is seeded by one entropy source that accumulate entropy. The source of entropy is from a software-based noise source. The CTR_DRBG is seeded with a minimum of 256 bits of entropy.
FCS_SSH_EXT.1 FCS_SSHS_EXT.1	The TOE implements the SSH protocol and acts as an SSH server in compliance with RFCs 4251, 4252, 4253, 4254, 4344, 5656, 6668, 8268, 8308, and 8332. The TOE supports public key authentication and password-based authentication. For SSH user authentication, the following public key algorithms are supported: ssh-rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384 and ecdsa-sha2-nistp521. TOE also supports LDAP and Radius as authentication servers while using password-based authentication. This list conforms to FCS_SSH_EXT.1.2. The SSH client’s public key is compared to an authorized keys file which is stored on the TOE. The TOE ensures that packets greater than 256K bytes in an SSH transport connection are dropped as described in RFC 4253. When the TOE detects packets greater than 256K, the connection is disconnected.

Requirement	TSS Description
	The TOE supports the following encryption algorithms: aes128-cbc, aes256-cbc, aes128-ctr, and aes256-ctr for SSH transport. There are no optional characteristics specified for FCS_SSH_EXT.1.4. This list is identical to those claimed for FCS_SSH_EXT.1.4. For SSH peer authentication, the following public key algorithms are supported: rsa-sha2-256 and rsa-sha2-512, ecdsa-sha2-nistp256 (RFC 5656), ecdsa-sha2-nistp384 (RFC 5656), ecdsa-sha2-nistp521 (RFC 5656). There are no optional characteristics specified for FCS_SSHS_EXT.1.1. This list is identical to those claimed for FCS_SSH_EXT.1.1. The TOE supports the following data integrity MAC algorithms: hmac-sha2-256, hmac-sha2-512. This list corresponds to the list in FCS_SSH_EXT.1.5. The TOE supports diffie-hellman-group-14-sha256 and diffie-hellman-group-16-sha512. This list corresponds to the list in FCS_SSH_EXT.1.6. The TOE uses the KDF for SSH defined in RFC 4253 (Section 7.2) and RFC 5656 (Section 4) to derive session keys from a shared secret. This list corresponds to the list in FCS_SSH_EXT.1.7. The TOE is capable of rekeying. The TOE verifies the following thresholds: • No longer than one hour • No more than one gigabyte of transmitted or received data. The TOE continuously checks both conditions. When either of the conditions are met, the TOE will initiate a rekey.
FCS_TLSC_EXT.1 FCS_TLSC_EXT.2	The TOE implements TLS v1.2 (RFC 5246) and rejects all other TLS and SSL versions. The TOE supports TLS communications with mutual authentication using X.509v3 certificates. This authentication process is applied when connecting to audit servers, LDAP and RADIUS servers. When establishing a trusted channel as specified by SFR: FTP_ITC.1, the TOE employs consistent ciphersuites and features across all communications, with no variation in implementation. The TOE supports the following configurable ciphersuites: • TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 • TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246 • TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288 • TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 The cipher suites specified are those listed in FCS_TLSC_EXT.1. The TOE presents the Supported Elliptic Curves/Supported Groups Extension in the Client Hello. The TOE only supports the following signature_algorithms extension for TLS connections: • rsa_pkcs1 with sha256(0x0401), • rsa_pkcs1with sha384(0x0501), • rsa_pkcs1 with sha512(0x0601), • rsa_pss_rsae with sha256(0x0804), • rsa_pss_rsae with sha384(0x0805), • rsa_pss_rsae with sha512(0x0806), • rsa_pss_pss with sha256(0x0809), • rsa_pss_pss with sha384(0x080a),

Requirement	TSS Description
	• rsa_pss_pss with sha512(0x080b) If the claimed signature_algorithm is present in the 'CLIENT HELLO', then the connection is accepted otherwise it denies the connection. By default, the signature_algorithms extension is supported in certificates generated via OpenSSL. TLS is used to establish encrypted sessions with other instances of the TOE and IT entities to send/receive audit data or authentication information. The TOE verifies that the presented identifier matches the reference identifiers. The TOE supports reference identifiers according to RFC 6125, Section 6, which includes DNS-ID and CN-ID, IPv4 address in CN or SAN, and IPv6 address in the CN or SAN. The TOE enforces canonical format for IPv6 and IPv4 as defined in RFC 5952 for IPv6, and RFC 3986 for IPv4. The TOE supports wildcards. The TOE does not support certificate pinning. When presented with X509 certificates, the TOE verifies the certificate path and certification validation process by verifying the following rules: • RFC 5280 certificate validation and certification path validation supporting a minimum path length of three certificates. The certification path must terminate with a trusted CA certificate designated as a trust anchor. • The TOE validates 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 TOE validates the revocation status of the certificate using a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3. • The TOE validates the extendedKeyUsage field according to the following rules: ○ Server certificates presented for TLS must 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 must have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field. The TOE will only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE. When establishing a trusted channel, by default the TOE will not establish a trusted channel if the server certificate is invalid. The TOE does not implement any administrator override mechanism. The use of CRL is configurable and can be used for certificate revocation. If the TOE is unable to establish a connection to determine the validity of a certificate, the TOE will not accept the certificate. By default, the TOE's TLS client supports the Supported Groups Extension with the following elliptic curve groups: • secp256r1 (NIST P-256) • secp384r1 (NIST P-384) • secp521r1 (NIST P-521) These supported groups allow for secure key exchange during the TLS handshake process.

Requirement	TSS Description
	TOE supports TLS v1.2 secure renegotiation when operating in the role of RADIUS or LDAP clients. However, TOE does not accept TLS v1.2 secure renegotiation requests when establishing connections to external syslog server.
FIA_AFL.1	The Security Administrator can configure the maximum number of failed attempts for all remote authentication methods (SSH, RADIUS, and LDAP) through both SSH and local CLI interfaces. The TOE allows the administrator to configure the number of successive failed authentication attempts. When a user fails to authenticate a number of times equal to the configured limit, the TOE locks the claimed user identity until the configured time is reached. Administrators can configure unsuccessful authentication attempts range between 1 – 64 within a configurable time limit of 0 to 60 minutes. When the account is locked, the TOE does not permit any further actions until the account is accessible. The authentication failures cannot lead to a situation where no administrator access is available. A user would be configured to access the LDAP server which would provide local access to the TOE.
FIA_PMG_EXT.1	The TOE provides the following password management capabilities for administrator passwords: a) Passwords can be composed of any combination of upper and lower case letters, numbers, and the following special characters: "~" "!" "@" "#" "$" "%" "^" "&" "*" "(" ")" "-" "_" "+" "=" "[" "{" "]" "}" "\\" "|" ";" ":" "'" "," "<" "." ">" "/" "?". b) Minimum password length is configurable to between 6 to 50 characters.
FIA_PSK_EXT.1	The TOE supports the use of pre-shared keys for MACsec key agreement protocols as defined by IEEE 802.1X. The pre-shared keys are not generated by the TOE but rather the TOE will accept bit based pre-shared keys. The CAK in PSK can be configured as follow: 128-bit CAK is 32 Hex digits, 256-bit CAK is 64 hex digits.
FIA_UIA_EXT.1	The TOE does not permit any actions prior to Administrators logging into the TOE. They are able to view the banner at the login prompt. The TOE mandates that every user must be authenticated by accessing the local console or by remotely using SSH. Security Administrators can access the console by connecting to the console port using RJ45-DB9 or by remotely connecting to each appliance via SSHv2. The TOE supports RSA public key authentication as a server, password-based authentication for remote and local authentication, and LDAP/Radius Server authentication for remote and local users. For password-based authentication, users must provide the correct credentials before accessing the TOE. If the user enters incorrect user credentials, they will not be allowed to access and will be presented the login page again.
FIA_UAU.7	When a user enters their password, the information is obscured. For local session authentication, the TOE does not echo any characters when they are entered.
FIA_X509_EXT.1/Rev	The TOE supports the X.509v3 certificates as defined by RFC 5280 to support authentication of external TLS peers.

Requirement	TSS Description
	When an X.509 certificate is presented, the TOE verifies the certificate path, and certification validation process by verifying the following rules: • RFC 5280 certificate validation and certification path validation supporting a minimum path length of three certificates. • The certification path must terminate with a trusted CA certificate designated as a trust anchor. • The TOE validates 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 TOE validates the revocation status of the certificate using a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3 • The TOE validates the extendedKeyUsage field according to the following rules: ○ Server certificates presented for TLS must 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 must have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field. The TOE will only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE. When the TOE receives a remote certificate during the secure channel establishment, the validity of the remote entity certificate is verified. The TOE also verifies the chain of trust by validating each certificate contained in the chain and verifying that a certificate path consists of trusted CA certificates and verify the validity of the certificates. These checks are done prior to loading the certificates onto the TOE. The use of CRL is configurable and can be used for certificate revocation. Revocation checks are performed on end-entity and intermediate certificates. If the TOE is unable to establish a connection to determine the validity of a certificate, the TOE will not accept the certificate.
FIA_X509_EXT.2	X.509 certificate can be used to authenticate and establish secure communication channel for LDAP, syslog and Radius servers. RSA based certificates: The supported RSA key size shall be 2048, 3072 and 4096 bits. When establishing any TLS secure connection and the TOE cannot determine the validity of a certificate, the TOE will not accept the certificate. To validate a peer certificate on the TOE, an authenticated administrator must import its CA certificates and CRLs. CA profiles must be created and enabled for each imported CA certificate and CRL. The administrator must configure at least one trust anchor to limit the list of CA certificates. Furthermore, the administrator can create a client profile to specify the cipher-list and client certificate to use.
FIA_X509_EXT.3	The TOE generates a Certificate Request as specified by RFC 2986 and is able to provide the following information in the request: public key and Common Name, Organization, Organizational Unit and Country.

Requirement	TSS Description
	The TOE validates the chain of certificates from the Root CA upon receiving the CA Certificate Response. The TOE does not support the “device-specific information” within Certificate Request message.
FMT_MOF.1/Functions	The TOE restricts the ability to modify the behaviour of transmission of audit data to an audit server to Security Administrators. The Security Administrator has the ability to configure and modify the IP address of the designated audit server, as well as to configure, modify, or replace the TLS security profile associated with the audit server connection. These capabilities include selecting the approved cipher suites, and managing the X.509 certificates and keys used for establishing a secure channel to the audit server.
FMT_MOF.1/ManualUpdate	Security Administrators have the ability to query the current version of the TOE and they are able to perform manual software updates. The currently active version of the TOE can be queried by issuing the “show version” command. The TOE provides means to authenticate software updates to the TOE using a digital signature prior to installing the software. Customers must log in to https://customer.nokia.com/support, portal to download software updates. This updated software package is then copied onto the compact flash (CF) of the active CPM card. Before the software is allowed to be activated a digital signature verification on the package must be performed using the command "admin system security image-digital-signature-validate". If this check fails the new image will not be allowed to be activated. If this check passes then the image is allowed to be activated using the command "bof primary-image <url>". At which point in redundant CPM systems the validated image is reconciled to the standby CPM by the system. This switchover mechanism provides minimal service interruption during a software upgrade for customers and the administrator must authorize the activation of the new software image before it can be deployed. For non-redundant systems, the image that is downloaded from Nokia server must be placed on the CF, the OS needs to point to the new image. The OS will run the digital signature verification process using an RSA key size of 2048bits and a sha2-256 hash algorithm to check the validity of the software image. If the image is validated the TOE’s administrator will reboot the TOE, which will start using the new software image.
FMT_MTD.1/CoreData	The TOE implements Role Based Access Control (RBAC). Security Administrative must login before they can access any administrative functions. Only administrators can manage the certificates in TOE’s trust store. The TOE maintains the following roles: Admin and User. Each role defined has a set of permissions that will grant them access to the TOE data. The only interfaces available to an unauthenticated user are the TOE login prompts. Only authorized security administrators may authenticate to the TOE and interact with TSF data. The TOE prevents non-security administrators from modifying any TSF element or security function. There are two types of trust stores in the TOE: Active and Inactive. In volatile memory, the trust store is active, and the other inactive trust store resides on the persistent store in the form of files. The Administrator can assign privileges to non-administrative user by configuring the capabilities in specifically user’s profile.
FMT_MTD.1/CryptoKeys	The Security Administrator has the ability to configure, modify and delete the pre-shared key for MACsec functionality, as well as to modify, generate, and delete the key for SSH.

Requirement	TSS Description
	For TLS, the Security Administrator can configure the parameters used for TLS operation, initiate the generation of new session keys during handshake operations, and terminate (delete) active sessions, which results in the secure destruction of the associated session keys. Session keys cannot be directly modified but are regenerated as part of a new TLS handshake. For X.509 certificates, the Security Administrator can configure certificates for use by the TOE, generate new certificate signing requests (CSRs) and associated key pairs, import externally generated certificates and keys, and delete certificates and associated keys from the TOE's storage. The TOE restricts the ability to manage SSH (session keys), TLS (session keys), and any configured X.509 certificates (public and private key pairs) to security administrators via command line.
FMT_SMF.1 FMT_SMF.1/MACSEC	The TOE supports the following roles: Administrator and User. The TOE can be accessed via local CLI and remote SSH. The Administrator can perform the following management functions: • Ability to administer the TOE remotely • Ability to configure the access banner • Ability to configure the remote session inactivity time before session termination • Ability to update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates; • Ability to configure local audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full; changes to local audit storage size); • Ability to modify the behaviour of the transmission of audit data to an external IT entity; • Ability to configure the cryptographic functionality; • Ability to configure thresholds for SSH rekeying; • Ability to set the time which is used for time-stamps; • Ability to manage the cryptographic keys; • 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; • Ability to configure the list of supported (D)TLS ciphers; • Manage a PSK-based CAK and install it in the device. • Manage the key server to create, delete, and activate MKA participants. • Specify the lifetime of a CAK. • Enable, disable, or delete a PSK-based CAK using [[CLI management command]]. • Manage generation of a PSK-based CAK.

<table>
<tr><th>Requirement</th><th>TSS Description</th></tr>
<tr><td>FMT_SMR.2</td><td>Security Administrators can configure user's privilege that grant or deny access to TSF data and functions.
The Security Administrator can also configure the user's profile to set the following restrictions:
<table>
<tr><th>Functionality</th><th>Description</th></tr>
<tr><td>cli-session-gr</td><td>To Add/remove cli-session-group the profile belongs to</td></tr>
<tr><td>combined-max-s</td><td>To define Maximum number of concurrent SSH & Telnet sessions</td></tr>
<tr><td>default-action</td><td>To get Default action for the profile</td></tr>
<tr><td>entry</td><td>To find the Match criteria entry for the profile</td></tr>
<tr><td>ssh-max-session</td><td>To create Maximum number of concurrent SSH sessions</td></tr>
</table>
The TOE enables both local console access and remote access via SSHv2 secure connection.</td></tr>
<tr><td>FPT_APW_EXT.1</td><td>All passwords are stored in a secure directory that is not readily accessible to administrators. The TOE stores passwords as non-reversible hashes.</td></tr>
<tr><td>FPT_CAK_EXT.1</td><td>The TOE stores CAKs in an encrypted form. This prevents the CAK value from being displayed in clear text to the administrators on the CLI.
The TOE uses AES-256 to encrypt and protect the CAKs.</td></tr>
<tr><td>FPT_FLS.1</td><td>When a failure occurs within the TOE (e.g., power-on self-tests or integrity check of the TOE executable image tests), it securely disables its interfaces and then reboots.
When the TOE boots in FIPS mode, it runs a diagnostic against the FIPS module and algorithms. Any failure in this self-diagnostic will cause the TOE to reboot.</td></tr>
<tr><td>FPT_RPL.1</td><td>The TOE discards the replayed data, and replay data is logged by the TOE.
When the TOE receives a valid MKA PDU (size and ICV size checks pass), the Message Number (MN) is checked to ensure that it is greater than the previous MN received from its peer.
If the MN is not greater than the previous MN, logs are generated. If the situation persists, then the MKA operational state will switch off based on the MKA timeout. Additionally, the attempt to replay data is logged.</td></tr>
<tr><td>FPT_SKP_EXT.1</td><td>The TOE stores all private keys, session keys or public keys in secure storage that is not accessible through an interface to administrators. All keys stored in plaintext are located in volatile memory and are inaccessible to any users or administrators. When the TOE is rebooted, all keys stored in volatile memory are subject to the clearing methods present in FCS_CKM.4.
For the CSPs that are stored in Non-Volatile memory, they are cryptographically obfuscated using the AES256-GCM algorithm, therefore they are not accessible through any standard TOE's interface.
Please refer to Table 25 for the complete list of CSP information used in the TOE and their corresponding storage location and how they are stored.</td></tr>
</table>

Requirement	TSS Description
FPT_STM_EXT.1	The TOE provides reliable time stamps. The clock function is reliant on the system clock provided by the underlying hardware. The clock is utilized for providing reliable time stamps used in the following functions: • Audit events • Local and remote Session inactivity • X.509 certificate expiration validation.
FPT_TST_EXT.1	The TOE performs an integrity check of the installed software by validating its digital signature using a trusted public certificate. If the signature verification fails (indicating tampering or unauthorized modification), the inactive CPM will reboot periodically until the CF is replaced with authentic, cryptographically signed software. The TOE also performs self-tests for the cryptographic module during boot up, and if any component reports failure for the self-test, the system will reboot and display the appropriate information on the local console. All ports are blocked from moving to forwarding state during the POST. If all components of all modules pass the POST, the system is placed in FIPS PASS state and ports are allowed to forward data traffic. When any of the tests fail, a message is displayed to the local console. The TOE executes the following power-on self-tests: • Software Integrity check Test: During the system boot-up process, the CPM performs software integrity verification by computing the digital signature of the software image stored in memory. This computed signature is then compared against the known, pre-stored signature value. If the signatures do not match, an error message is displayed on the console, and the device initiates a reboot. Conversely, if the signatures match, the boot sequence proceeds as expected. • AES Known Answer Test -The AES encryption and AES decryption algorithms are tested using test vectors. The results are compared against pre-computed results to ensure the algorithms are operating properly. • GCM Known Answer Test - In this test, A known plaintext is encrypted using AES-GCM with a known 256-bit key, and the computed ciphertext is compared to the expected ciphertext. If they match, then the computed ciphertext is decrypted using the same key, and the recovered plaintext is compared with the original known plaintext. If they do not match, the test fails. If they match, the test passes. • HMAC-SHA-1/256/384/512 Known Answer Test - the HMAC algorithm is tested using test vector. The results are compared against pre-computed results to ensure the algorithm is operating properly. • SHA-1/256/384/512 Known Answer Test - the SHA algorithm is tested using test vector. The results are compared against pre-computed results to ensure the algorithm is operating correctly. • RSA Signature Known Answer Test - the RSA Signature is tested using test vector. The results are compared against pre-computed results to ensure the algorithm is operating properly. • ECDSA Signature Known Answer Test - the ECDSA Signature is tested using test vector. The results are compared against pre-computed results to ensure the algorithm is operating properly. • DRBG Known Answer Test - the DRBG is seeded with a pre-determined entropy and the RNG output is compared with output values expected for the pre-determined seed.

Requirement	TSS Description
	- The cryptographic module Integrity Test - is run automatically on start-up, and whenever the system images are loaded. 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. - There is also a Noise Source Health test that is executed as part of the self-test requirements.
FPT_TUD_EXT.1	Security Administrators have the ability to query the current version of the TOE and they are able to perform manual software updates. The currently active version of the TOE can be queried by issuing the "show version" command. The TOE provides means to authenticate software updates to the TOE using an RSA key size of 2048bits and a sha2-256 as hash algorithm for verifying the digital signature prior to installing the software. Customers must log in to the Nokia Support Portal to download software updates. The downloaded software package is then copied onto the compact flash of the active CPM card. Before activation, a digital signature verification must be performed using the command: *#admin system security image-digital-signature validate software-image <software-image>* If the validation fails, the new image will not be permitted for installation. However, if the check is successful, the image can be activated using the command and a reboot is needed to complete the installation process: *#bof exclusive* *# image primary-location <url>* *# commit* In redundant CPM systems, once the image is validated, it is automatically synchronized with the standby CPM by the system. For non-redundant systems the image that is downloaded from Nokia server must be placed on the CF, the OS needs to point to the new image. The OS will run the digital signature process to check the validity of the software image, if the image is validated the TOE's administrator will reboot the TOE, which will start using the new software image. The TOE does not support delayed activation.
FTA_SSL_EXT.1	The TOE will terminate a local interactive session after a configurable time interval of session inactivity. A configured inactivity period will be applied to local sessions. When the local session has been idle for more than the configured period, the session will be terminated and will require authentication to establish a new session. The allowable inactivity timeout range is from 1 to 1440 minutes.
FTA_SSL.3	If a remote user session is inactive for a configured period of time, the session will be terminated and will require re-identification and authentication to establish a new session. When the user logs back in, the inactivity timer will be activated for the new session. A configured inactivity period will be applied to both local and remote sessions in the same manner. The allowable inactivity timeout range is from 1 to 1440 minutes.

Requirement	TSS Description
FTA_SSL.4	The Security Administrator is able to terminate their CLI. Security Administrators can terminate their own sessions by typing "Logout" to exit the console and remote sessions.
FTA_TAB.1	Security Administrators can create a customized login banner that will be displayed at the following interfaces: • Local CLI (Serial Port) • Remote CLI (SSH Administration) This banner will be displayed prior to allowing Security Administrator access through those interfaces.
FTP_ITC.1	The TOE supports secure TLS v1.2 with mutual-authentication when communicating to the following IT entities as a TLS client: Audit server, Radius server and LDAP server. The TOE protects communications with an external audit server using syslog over TLS v1.2 protocol. The TOE uses TLS v1.2 protocol with X.509 certificate-based mutual authentication. The TOE secures communication between its peers using the MACsec at Layer 2. The protocols listed are consistent with those specified in the requirement.
FTP_TRP.1/Admin	The TOE supports SSH v2.0 for secure remote administration of the TOE. Each SSH v2.0 session is encrypted using AES to protect confidentiality and uses HMACs to protect the integrity of traffic. The protocols listed are consistent with those specified in the requirement.

6.1 CRYPTOGRAPHIC KEY DESTRUCTION

The table below describes the key zeroization provided by the TOE and as referenced in FCS_CKM.4.

Table 25 – Key Zeroization

Keys/CSPs	Purpose	Storage Location	Method of Zeroization
Diffie-Hellman Shared Secret	The shared secret used in Diffie-Hellman (DH) exchange. Created per the Diffie-Hellman Exchange.	RAM (plaintext)	A single overwrite consisting of zeroes.
Diffie Hellman private key	The private key used in Diffie-Hellman (DH) Exchange	RAM (plaintext)	A single overwrite consisting of zeroes.
SSH Private key	The SSH server host private key is stored on the local filesystem	RAM (plaintext) CF (obfuscated using AES-256-GCM) if preserve-key is enabled.	RAM: A single overwrite consisting of zeroes. CF: Deleted via an OS call.
SSH Session Key	These are the session keys for SSH.	RAM (plaintext)	A single overwrite consisting of zeroes.
TLS Session Keys	These are the session keys for TLS.	RAM (plaintext)	A single overwrite consisting of zeroes.
RSA key pairs	Used for TLS and SSH secure channels.	RAM (plaintext) CF (obfuscated using AES-256-GCM)	RAM: A single overwrite consisting of zeroes. CF: Deleted via an OS call.

Keys/CSPs	Purpose	Storage Location	Method of Zeroization
MACsec Security Association Key (SAK)	The SAK is used to secure data plane traffic.	RAM (plaintext)	A single overwrite consisting of zeroes.
MACsec Connectivity Association Key (CAK)	A symmetric key that is used as the master key to derive the ICK and KEK.	RAM (plaintext) CF (obfuscated using AES-256-GCM)	RAM: A single overwrite consisting of zeroes. CF: deleted via an OS call.
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).	RAM (plaintext)	A single overwrite consisting of zeroes.
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.	RAM (plaintext)	A single overwrite consisting of zeroes.
RNG Seed Key	This is the seed key for the RNG.	RAM (plaintext)	A single overwrite consisting of zeroes.
RNG Seed	This seed is for the RNG.	RAM (plaintext)	A single overwrite consisting of zeroes.

7. ACRONYM TABLE

Acronyms should be included as an Appendix in each document.

Table 26 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
BIOS	Basic Input/Output System
CAK	Connectivity Association Key
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security
CBC	Cipher Block Chaining
CLI	Command Line Interface
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DH	Diffie-Hellman
DHE	Diffie-Hellman Ephemeral
DNS	Domain Name System
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
FIPS	Federal Information Processing Standards
GCM	Galois Counter Mode
gRPC	gRPC Remote Procedure Calls
GUI	Graphical User Interface
HMAC	Hash Message Authentication Code
IP	Internet Protocol
KAT	Known Answer Test
KDF	Key Derivation Function
LDAP	Lightweight Directory Access Protocol
MB	Megabyte
MKA	MACsec Key Agreement
MPLS	Multiprotocol Label Switching
NIAP	National Information Assurance Partnership
NTP	Network Time Protocol
OSP	Organizational Security Policy
PCT	Pairwise Consistency Test

Acronym	Definition
PP	Protection Profile
PKCS	Public Key Cryptography Standards
RAM	Random Access Memory
RFC	Requests for Comments
RSA	Rivest-Shamir-Adleman
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SFP	Security Policy Database
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSO	Single Sign On
ST	Security Target
TOE	Target of Evaluation
TLS	Transport Layer Security
TSF	TOE Security Functionality
TSFI	TSF Interface
TSS	TOE Summary Specification
UI	User Interface
URI	Uniform Resource Identifier