SENETAS

Security without compromise

Senetas Distributed by Thales

CN Series Encryptors 5.5.0

Security Target

Version 1.7

December 2024

Document prepared by

Lightship Security

www.lightshipsec.com

Document History

Version	Date	Author	Description
1.0	07 Oct 2024	M Baldock	Published, addressing OR09
1.1	09 Oct 2024	M Baldock	TSS Update
1.2	23 Oct 2024	M Baldock	Addressing OR10
1.3	25 Oct 2024	M Baldock	AGD Updates
1.4	06 Nov 2024	M Baldock	Addressing OR12
1.5	11 Nov 2024	B King	Updated User Guide titles in section 2.4.2
1.6	13 Dec 2024	M Baldock	Addressing ECR Comments
1.7	16 Dec 2024	M Baldock	Addressing CAVP Comments

Table of Contents

List of Tables

1 Introduction

1.1 Overview

1 This Security Target (ST) defines the Senetas Distributed by Thales CN Series Encryptors 5.5.0 Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

2 The TOE is a high-speed, standards-based encryptor designed to secure voice, data and video information transmitted over Ethernet networks. The TOE also provide access control facilities using access rules for each defined Ethernet connection.

1.2 Identification

Table 1: Evaluation identifiers

Target of Evaluation	Senetas Distributed by Thales CN Series Encryptors 5.5.0 Build: 31224
Security Target	Senetas Distributed by Thales CN Series Encryptors 5.5.0 Security Target, v1.7, December 2024

1.3 Conformance Claims

3 This ST supports the following conformance claims:

a) CC version 3.1 revision 5

b) CC Part 2 extended

c) CC Part 3 conformant

d) collaborative Protection Profile for Network Devices, v3.0e (referenced within as NDcPP)

e) Functional Package for SSH, v1.0 (reference within as PKG_SSH) conformant

f) NIAP Technical Decisions per Table 2

Table 2: NIAP Technical Decisions

TD #	Name	References	Applicability Rationale	Source
TD0682	Addressing Ambiguity in FCS_SSHS_EXT.1 Tests	FCS_SSHS_EXT.1	Applicable	PKG_SSH
TD0695	Choice of 128 or 256 bit size in AES-CTR in SSH Functional Package.	Section 1.3, FCS_COP.1	Applicable	PKG_SSH
TD0732	FCS_SSHS_EXT.1.3 Test 2 Update	FCS_SSH_EXT.1.3	Applicable	PKG_SSH
TD0777	Clarification to Selections for Auditable Events for FCS_SSH_EXT.1	Section 3.1, Table 1	Applicable	PKG_SSH

TD #	Name	References	Applicability Rationale	Source
TD0836	NIT Technical Decision: Redundant Requirements in FPT_TST_EXT.1	FPT_TST_EXT.1, CPP_ND_V3.0E-SD, Section 4.1.5	Applicable	NDcPP
TD0868	NIT Technical Decision: Clarification of time frames in FCS_IPSEC_EXT.1.7 and FCS_IPSEC_EXT.1.8	FCS_IPSEC_EXT.1.7, FCS_IPSEC_EXT.1.8	Not Applicable. FCS_IPSEC_EXT.1 not claimed	NDcPP
TD0879	NIT Decision: Correction of Chapter Headings in CPP_ND_V3.0E	Appendix B.6.3, Appendix B.7	Applicable	NDcPP
TD0880	NIT Decision: Removal of Duplicate Selection in FMT_SMF.1.1	FMT_SMF.1.1	Applicable	NDcPP
TD0886	Clarification to FAU_STG_EXT.1 Test 6	FAU_STG_EXT.1, CPP_ND_V3.0E-SD	Applicable	NDcPP

1.4 Terminology

Table 3: Terminology

Term	Definition
Activation	Process of replacing default user credentials using RSA
CA	Certification Authority
CC	Common Criteria
CI	Connection Identifier (represents an established security association)
CLI	Command Line Interface
CM7	Senetas PC based remote Management Application
CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter
DEK	Data Encryption Key
EAL	Evaluation Assurance Level
ECDH	Elliptic Curve Diffie-Hellman

Term	Definition
ECDSA	Elliptic Curve Digital Signature Algorithm
EtherType	A field in an Ethernet frame used to indicate which protocol is encapsulated in the payload of the frame.
ETSI	European Telecommunications Standards Institute
FIPS PUB	Federal Information Processing Standard Publication
FTP	File Transfer Protocol
FTPS	File Transfer Protocol Secure
HMAC	Hash-based Message Authentication Code
IP	Internet Protocol
KDK	Key Derivation Key
KEK	Key Encrypting Key
KID	Key ID
KMIP	Key Management Interoperability Protocol
KMS	Key Management Service
MAC	Media Access Control
NAE	Network-Attached Encryption – Safenet proprietary key management protocol.
NDcPP	collaborative Protection Profile for Network Devices
NIST	National Institute of Standards and Technology
OAEP	Optimal Asymmetric Encryption Padding
OSP	Organisational Security Policy
PP	Protection Profile
QKD	Quantum Key Distribution – network distribution of QRA generated keys in accordance with defined standards (ETSI).
QRA	Quantum Resistant Algorithms – Candidate algorithms supported by the Open Quantum Safe project.
RFC	Request for Comment
RSA	Rivest Shamir Adleman Public Key Algorithm

Term	Definition
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SFTP	SSH File Transfer Protocol
SME	Secure Message Exchange
SMK	System Master Key
SNMPv3	Simple Network Management Protocol Version 3
SSH	Secure Shell
TACACS+	Terminal Access Control Access Control Server
TOE	Target of Evaluation
TIM	Transport Independent Mode – Allows concurrent secure connections between encryptors over network layers 2, 3 and 4.
Traffic Analysis	The process of intercepting and examining messages in order to deduce information from patterns in communication.
TRANSEC	Transmission Security - used to disguise patterns in network traffic to prevent traffic analysis.
TSF	TOE Security Functionality
TSS	TOE Summary Specification
Tunnel	Equivalent to CI
VLAN	Virtual Local Area Network
X.509	Digital Certificate Standard

2 TOE Description

2.1 Type

4 The TOE is a network device.

2.2 Usage

5 The CN Series Encryptors are typically installed between an operator’s private network equipment and public network connection and are used to secure data transiting over Ethernet networks. When operating at full bandwidth, the Ethernet Encryptor will not discard any valid Ethernet frame in all modes of operation.

6 Different user roles with different privileges are defined. The four defined roles are Administrator, Supervisor, Operator and Upgrader. Only the Administrator has unrestricted access to the security features that are required for the encryptor to start operation. The encryptors also provide an audit capability to support the effective management of the security features of the device. The audit capability records all management activities for security relevant events.

2.2.1 Deployment

7 CN Series Ethernet Encryptors operate in point-to-point and point-to-multipoint network topologies and at data rates ranging from 10Mb/s to 10Gb/s. Encryptors are typically installed between an operator’s private network equipment and public network connection and are used to secure data travelling over either fibre optic or CAT5/6 cables.

8 The point-to-point and point-to-multipoint functionality is additional functionality outside the management scope of the TOE.

9 Figure 1 depicts an example deployment of the TOE devices (enclosed in red).

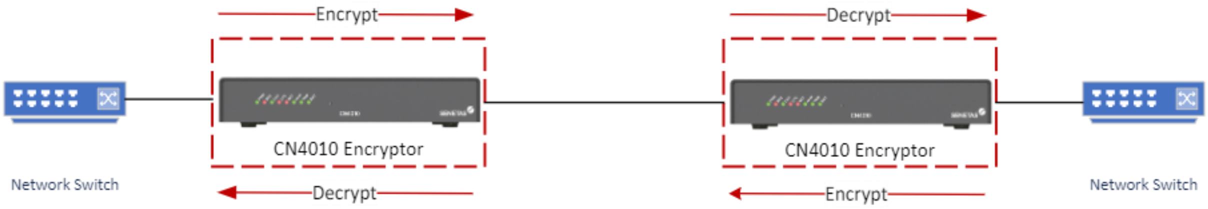

Figure 1: Example TOE deployment

2.2.2 Interfaces

10 The TOE management interfaces are shown in Figure 2.

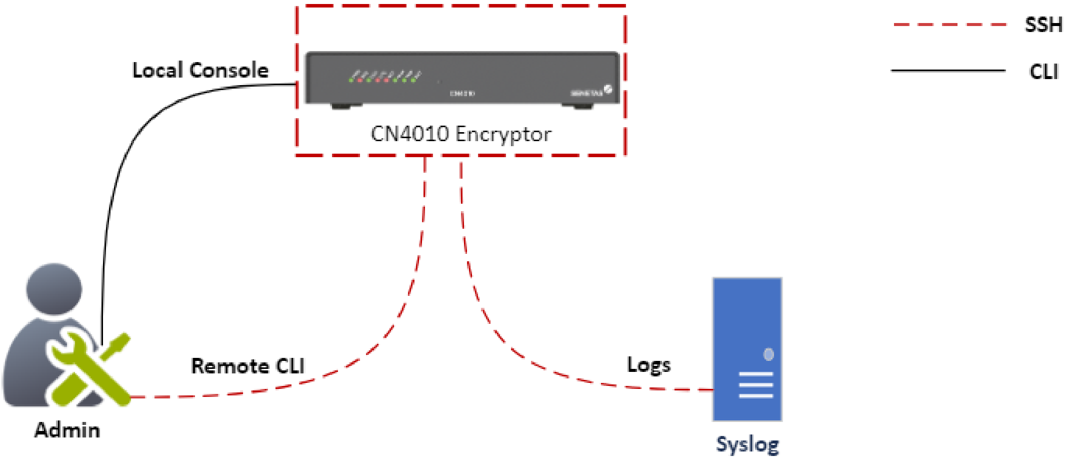

Figure 2: TOE interfaces

11 The TOE interfaces are as follows:

a) **CLI.** Local management via serial access to the CLI.

b) **SSH.** Remote management via SSH / SSHS access to the CLI.

c) **Syslog.** Remote syslog server via SSH / SSHS.

2.3 Security Functions / Logical Scope

12 The TOE provides the following security functions:

a) **Trusted Path/Channels.** The TOE protects the integrity and confidentiality of communications as noted in section 2.2.2 above, and using cryptographic algorithms as described in Table 4.

b) **Security Management.** The TOE enables secure management of its security functions, including:

i) Administrator authentication with passwords

ii) Configurable password policies

iii) Role Based Access Control

iv) Access banners

v) Management of critical security functions and data

vi) Protection of cryptographic keys and passwords

c) **Protection of the TSF.** The TOE performs a suite of self-tests to ensure the correct operation and enforcement of its security functions. The TOE performs diagnostic self-tests and cryptographic module self-tests during start-up and generates audit records to record a failure. Self-tests comply with the FIPS 140-2 requirements for self-testing.

d) **Identification and Authentication.** The TOE ensures that all users must be authenticated before accessing its functions and data. The TOE uses public keys for authentication for SSH.

e) **TOE Access.** TOE can be accessed directly via serial connection or remotely via SSH connection. When a user account has sequentially failed authentication the configured number of times, the account will not be locked.

f) **Security Audit.** The TOE generates audit records of user and administrator actions. The TOE includes the user identity in audit events resulting from actions of identified users. The Security Administrator can configure the TOE to send logs in real-time to a syslog server via SSH.

g) **Cryptographic Support** The TOE implements a cryptographic module. The cryptographic module has the ability to generate, destroy cryptographic keys, authenticate keys, perform key exchanges in protected communications and validate signatures in image upgrades. Cryptographic functions are primarily used with the SSH protocol. Relevant Cryptographic Algorithm Validation Program (CAVP) certificates are shown in Table 4.

Table 4: CAVP Certificates

SFR	Algorithm	Implementation name	Operational Environment	CAVP Alg.	CAVP Cert #
FCS_CKM.1	Asymmetric Key Generation: 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;	CN Series Common Crypto Library	ARM Cortex A9	ECDSA KeyGen(FIPS 186-4) ECDSA KeyVer(FIPS186-4)	A3451
FCS_CKM.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”;	CN Series Common Crypto Library	ARM Cortex A9	KAS-ECC Sp800 56A/3 (NIST SP 800-56A Revision 3)	A3451
FCS_COP.1/ DataEncryption	encryption/decryption in accordance with a specified cryptographic algorithm AES used in [CTR] mode and cryptographic key sizes [128 bits, 256 bits]	CN Series Common Crypto Library	ARM Cortex A9	AES-CTR	A3451

SFR	Algorithm	Implementation name	Operational Environment	CAVP Alg.	CAVP Cert #
FCS_COP.1/ SigGen	cryptographic signature services (generation and verification): RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [2048 bits or greater]	CN Series Common Crypto Library	ARM Cortex A9	RSA SigGen (FIPS186-4) RSA SigVer (FIPS186-4)	A3451
FCS_COP.1/ SigGen	cryptographic signature services (generation and verification): Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [256 bits or greater]	CN Series Common Crypto Library	ARM Cortex A9	ECDSA SigGen (FIPS186-4) ECDSA SigVer (FIPS186-4)	A3451
FCS_COP.1/ Hash	cryptographic hashing services in accordance with a specified cryptographic algorithm [SHA-256, SHA-384, SHA-512]	CN Series Common Crypto Library	ARM Cortex A9	SHA-256 SHA2-384 SHA2-512	A3451
FCS_COP.1/ KeyedHash	keyed-hash message authentication in accordance with a specified cryptographic algorithm [HMAC-SHA-256, HMAC-SHA-512]	CN Series Common Crypto Library	ARM Cortex A9	HMAC-SHA2-256 HMAC-SHA2-512	A3451
FCS_RBG_EXT.1	deterministic random bit generation services using [selection: Hash_DRBG [SHA-256]	CN Series Common Crypto Library	ARM Cortex A9	Hash DRBG	A3451

2.4 Physical Scope

13 The physical boundary of the TOE is the encryptor hardware and firmware. Table 5. shows the TOE models. All TOE models use the same embedded software (version shown in Table 1) and share the same hardware architecture. Table 5 columns are as follows:

a) **Model.** The TOE model number.

b) **CPU & ASIC.** The CPU and ASIC for the TOE model.

c) **Hardware.** The part numbers associated with the hardware enclosure and supported power supply.

d) **Power.** Type of power supply for each hardware part number for a given model.

e) **Protocol / FPGA Bitstream.** The supported protocols and related FPGA bitstream, including whether TIM is supported.

f) **AES Modes.** The supported AES Modes.

g) **I/F.** The supported local/network port interfaces.

h) **LCD/Keypad.** Whether the model includes an LCD and Keypad.

Table 5: TOE models

Model	CPU & ASIC	Hardware	Power	Protocol / FPGA Bitstream	AES Modes	I/F	LCD/ Keypad
CN4010	ARM Cortex A9	A4010B	DC (Plug Pack)	1G Ethernet 1G Ethernet TIM	CTR	RJ45	No
CN4020	ARM Cortex A9	A4020B	DC (Plug Pack)	1G Ethernet 1G Ethernet TIM		SFP	No
CN6010	ARM Cortex A9	A6010B A6011B A6012B	AC/AC Dual DC/DC Dual AC/DC Dual	1G Ethernet 1G Ethernet TIM		RJ45 SFP	Yes
CN6110	ARM Cortex A9	A6110B A6111B A6112B	AC/AC Dual DC/DC Dual AC/DC Dual	1G Ethernet 1G Ethernet TIM 10G Ethernet 10G Ethernet TIM		RJ45 SFP+	Yes
CN6140	ARM Cortex A9	A6140B	AC/AC Dual	1Gx1 Ethernet Single Port 1Gx4 Ethernet Multi Port		SFP+	Yes

Model	CPU & ASIC	Hardware	Power	Protocol / FPGA Bitstream	AES Modes	I/F	LCD/ Keypad
		A6141B	DC/DC Dual	1Gx1 Ethernet TIM Single Port 1Gx4 Ethernet TIM Multi Port			
				10Gx1 Ethernet Single Port 10Gx2 Ethernet Multi Port			
		A6142B	AC/DC Dual	10Gx1 Ethernet TIM Single Port 10Gx4 Ethernet TIM Multi Port			
				10Gx4 Ethernet Multi Port			
CN9120	ARM Cortex A9	A9120B A9121B A9122B	AC/AC Dual DC/DC Dual AC/DC Dual	100G Ethernet		QSFP 28	Yes

2.4.1 TOE Delivery

14 The encryptor device is delivered with the embedded software via commercial courier. The TOE embedded software may also be downloaded via the Senetas Distributed by Thales customer portal.

2.4.2 Guidance Documents

15 The TOE includes the following guidance documents (PDF) which are made available via the Senetas Distributed by Thales customer portal:

a) Senetas Distributed by Thales CN4000/CN6000/CN9000 Series Ethernet Encryptors Firmware Version 5.5.0 Operational User Guidance (AGD_OPE.1) v1.1, 13 December 2024

b) Senetas Corporation CN4010 Encryptor All Operational Modes, Rev 55-24-010, October 2024

c) Senetas Corporation CN4020 Encryptor All Operational Modes, Rev 55-24-010, October 2024

d) Senetas Corporation CN6010 Encryptor All Operational Modes, Rev 55-24-010, October 2024

e) Senetas Corporation CN6110 Encryptor All Operational Modes, Rev 55-24-010, October 2024

f) Senetas Corporation CN6140 Encryptor All Operational Modes, Rev 55-24-010, October 2024

g) Senetas Corporation CN9120 Encryptor Ethernet Mode, Rev 55-24-010, October 2024

2.4.3 Non-TOE Components

16 The TOE operates with the following components in the environment:

a) **Audit Server.** Remote syslog server.

2.4.4 Functions not included in the TOE Evaluation

a) Point-to-point and Point-to-Multipoint Layer2 Encryption

b) CM7

c) RESTful SNMP MIB Interface

d) Keypad Hardware panel

e) SNMPv3

3 Security Problem Definition

17 The Security Problem Definition is reproduced from section 4 of the NDcPP.

3.1 Threats

Table 6: Threats

Identifier	Description
T.UNAUTHORIZED_ ADMINISTRATOR_ ACCESS	Threat agents may attempt to gain Administrator access to the Network Device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between Network Devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_ CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_ COMMUNICATION_ CHANNELS	Threat agents may attempt to target Network Devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the Network Device itself.
T.WEAK_ AUTHENTICATION_ ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints, e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.
T.UPDATE_ COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
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

Identifier	Description
	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. Threat agents may also be able to take advantage of weak administrative passwords to gain privileged access to the device.
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

Table 7: Assumptions

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

Identifier	Description
A.NO_THRU_ TRAFFIC_ PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).
A.TRUSTED_ ADMINISTRATOR	The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE’s trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
A.REGULAR_ UPDATES	The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_ CREDENTIALS_ SECURE	The Administrator’s credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.RESIDUAL_ INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

3.3 Organizational Security Policies

Table 8: Organizational Security Policies

Identifier	Description
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

18 The security objectives are reproduced from section 5 of the NDcPP.

Table 9: Security Objectives for the Operational Environment

Identifier	Description
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.NO_GENERAL_ PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
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.

5 Security Requirements

5.1 Conventions

19 This document uses the following font conventions to identify the operations defined by the CC:

a) **Assignment.** Indicated with italicized text.

b) **Refinement.** Indicated with bold text and strikethroughs.

c) **Selection.** Indicated with underlined text.

d) **Assignment within a Selection:** Indicated with italicized and underlined text.

e) **Iteration.** Indicated by adding a string starting with "/" (e.g. "FCS_COP.1/Hash").

20 **Note:** Operations performed within the Security Target are denoted within brackets []. Operations shown without brackets are reproduced from the NDcPP.

5.2 Extended Components Definition

21 The Extended Components are defined in Appendix C of the NDcPP.

Table 10: Extended Components

Requirement	Title	Source	Applicable TDs
FAU_STG_EXT.1	Protected Audit Event Storage	NDcPP	
FCS_RBG_EXT.1	Random Bit Generation	NDcPP	
FCS_SSH_EXT.1	SSH Protocol	PKG_SSH	TD0777
FCS_SSHS_EXT.1	SSH Protocol – Server	PKG_SSH	TD0682, TD0732
FIA_PMG_EXT.1	Password Management	NDcPP	
FIA_UIA_EXT.1	User Identification and Authentication	NDcPP	
FPT_SKP_EXT.1	Protection of TSF Data (for reading of all symmetric keys)	NDcPP	
FPT_APW_EXT.1	Protection of Administrator Passwords	NDcPP	
FPT_TST_EXT.1	TSF Testing	NDcPP	
FPT_TUD_EXT.1	Trusted Update	NDcPP	
FPT_STM_EXT.1	Reliable Time Stamps	NDcPP	
FTA_SSL_EXT.1	TSF-initiated Session Locking	NDcPP	

5.3 Functional Requirements

Table 11: Summary of SFRs

Requirement	Title
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Association
FAU_STG_EXT.1	Protected Audit Event Storage
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_RBG_EXT.1	Random Bit Generation
FCS_SSH_EXT.1	SSH Protocol
FCS_SSHS_EXT.1	SSH Protocol – Server
FIA_PMG_EXT.1	Password Management
FIA_UIA_EXT.1	User Identification and Authentication
FIA_UAU.7	Protected Authentication Feedback
FMT_MOF.1/Functions	Management of Security Functions Behaviour
FMT_MOF.1/ManualUpdate	Management of Security Functions Behaviour
FMT_MOF.1/Services	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_SMR.2	Restrictions on Security Roles
FPT_SKP_EXT.1	Protection of TSF Data (for reading of all symmetric keys)

Requirement	Title
FPT_APW_EXT.1	Protection of Administrator Passwords
FPT_TST_EXT.1	TSF Testing
FPT_TUD_EXT.1	Trusted Update
FPT_STM_EXT.1	Reliable Time Stamps
FTA_SSL_EXT.1	TSF-initiated Session Locking
FTA_SSL.3	TSF-initiated Termination
FTA_SSL.4	User-initiated Termination
FTA_TAB.1	Default TOE Access Banners
FTP_ITC.1	Inter-TSF trusted channel
FTP_TRP.1/Admin	Trusted Path

5.3.1 Security Audit (FAU)

FAU_GEN.1 Audit Data Generation

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

a. Start-up and shut-down of the audit functions;

b. All auditable events for the <u>not specified</u> 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).*
- <u>[Resetting passwords (name of related Administrator account shall be logged),</u>];

d. *Specifically defined auditable events listed in ~~**Table 2**~~ **Table 12**.*

Table 12: Audit Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	None.

Requirement	Auditable Events	Additional Audit Record Contents
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_RBG_EXT.1	None.	None.
FCS_SSH_EXT.1	• [Failure to establish SSH connection] • [Establishment of SSH connection] • [Termination of SSH connection session] • [Dropping of packet(s) outside defined size limits]	• [Reason for failure and Non-TOE endpoint of attempted connection (IP Address)] • [Non-TOE endpoint of connection (IP Address)] • [Non-TOE endpoint of connection (IP Address)] • [Packet size]
FCS_SSHS_EXT.1	No events specified	
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of identification and authentication mechanisms.	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_MOF.1/Services	None.	None.
FMT_MTD.1/CoreData	None.	None.

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

Requirement	Auditable Events	Additional Audit Record Contents
	• Failure of the trusted path functions.	

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

a. Date and time of the event, type of event, subject identity ~~(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 2~~** **Table 12***.

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.

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 [*2 log files with 1 record each*].

FAU_STG_EXT.1.5 The TSF shall [drop new audit data, overwrite previous audit records according to the following rule: [*overwrite oldest first*]] 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].

5.3.2 Cryptographic Support (FCS)

FCS_CKM.1 Cryptographic Key Generation

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

- ECC schemes using ‘NIST curves’ [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4;

] ~~and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].~~

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: [selection:

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

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

FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method

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

  ]

that meets the following: *No Standard*.

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

FCS_COP.1.1/DataEncryption The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in [CTR] mode and cryptographic key sizes [128 bits, 256 bits] that meet the following: AES as specified in ISO 18033-3, [CTR as specified in ISO 10116].

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

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

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

]

and cryptographic key sizes [

- For RSA: modulus 2048 bits or greater,
- For ECDSA: 256 bits or greater

]

that meet the following: [

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

].

FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)

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

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

FCS_COP.1.1/KeyedHash The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm [HMAC-SHA-256, HMAC-SHA-512] and cryptographic key sizes *[assignment: key size (in bits) used in HMAC]* **and message digest sizes [256, 512] bits** that meet the following: *ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”*.

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 [HASH_DRBG [SHA-256]].

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

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] and [*no other standard*].

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

- “publickey” (RFC 4252): [
  - 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 bytes*] 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),

] and no other mechanisms.

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

- 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: [

- ecdh-sha2-nistp256 (RFC 5656),
- ecdh-sha2-nistp384 (RFC 5656),
- ecdh-sha2-nistp521 (RFC 5656),

] and no other mechanisms.

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

- RFC 5656 (Section 4)

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

FCS_SSH_EXT.1.8 The TSF shall ensure that [

- a rekey of the session keys,

] occurs when any of the following thresholds are met:

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

FCS_SSHS_EXT.1 SSH Server Protocol

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

- ecdsa-sha2-nistp256 (RFC 5656),

].

5.3.3 Identification and Authentication (FIA)

FIA_PMG_EXT.1 Password Management

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

a. Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: ["!", "@", "#", "$", "%", "^", "&", "*", "(",”)”,”<”,”>”,”?”];

b. Minimum password length shall be *configurable to between [8] and [29] characters.*

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 The TSF shall provide the following remote authentication mechanisms [public key] and local authentication mechanisms [password-based].

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

FIA_UAU.7 Protected Authentication Feedback

FIA_UAU.7.1 The TSF shall provide only *obscured feedback* to the **administrative** user while the authentication is in progress **at the local console**.

5.3.4 Security Management (FMT)

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 [audit functionality when Local Audit Storage Space is full] to *Security Administrators.*

FMT_MOF.1/ManualUpdate Management of security functions behaviour

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

FMT_MOF.1/Services Management of Security Functions Behaviour

FMT_MOF.1.1/Services The TSF shall restrict the ability to start and stop the functions services to Security Administrators.

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*.

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.*

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- *Ability to administer the TOE remotely;*
- *Ability to configure the access banner;*
- *Ability to configure the 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 start and stop services;
  - 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 set the time which is used for time-stamps;
  - Ability to administer the TOE locally;
  - Ability to configure the local session inactivity time before session termination or locking;
  - Ability to manage the trusted public keys database;]

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.

5.3.5 Protection of the TSF (FPT)

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.

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.

FPT_TST_EXT.1 TSF testing

FPT_TST_EXT.1.1 The TSF shall run a suite of the following self-tests [

- During initial start-up (on power on) to verify the integrity of the TOE firmware and software;

]

- to demonstrate the correct operation of the TSF: [*Firmware integrity tests, Known Answer Tests*] and if failure detected [*enter a Secure shutdown state and Halt (“Secure Halt”)*].

FPT_TST_EXT.1.2 The TSF shall respond to [all failures] by [[*preventing the module being configured and passing any data over the Network data output interface*]].

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 [the most recently installed version of the TOE firmware/software;].

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.

FPT_STM_EXT.1 Reliable Time Stamps

FPT_STM_EXT.1.1 The TSF shall be able to provide reliable time stamps for its own use.

FPT_STM_EXT.1.2 The TSF shall [allow the Security Administrator to set the time].

5.3.6 TOE Access (FTA)

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.

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*.

FTA_SSL.4 User-initiated Termination

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

FTA_TAB.1 Default TOE Access Banners

FTA_TAB.1.1 Before establishing ~~a~~ **an administrative user** session the TSF shall display **a Security Administrator-specified** advisory **notice and consent** warning message regarding ~~unauthorised~~ use of the TOE.

5.3.7 Trusted path/channels (FTP)

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall **be capable of using [SSH] to** provide a **trusted** communication channel between itself and ~~another trusted IT product~~ **authorized IT entities supporting the following capabilities: audit server, [no other capabilities]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from ~~modification or~~ 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 [

- *Syslog Server via SSH*

].

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** ~~users~~ 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** ~~users~~ to initiate communication via the trusted path.

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

5.4 Assurance Requirements

22 The TOE security assurance requirements are summarized in Table 13.

Table 13: Assurance Requirements

Assurance Class	Components	Description
Security Target Evaluation	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 User Guidance
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

23 In accordance with section 7.1 of the NDcPP, the following refinement is made to ASE:

a) **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.**

6 TOE Summary Specification

24 The following describes how the TOE fulfils each SFR included in section 5.3.

6.1 Security Audit

6.1.1 FAU_GEN.1

25 The TOE generates the audit records specified at FAU_GEN.1 containing fields that include the timestamp, IP address (if applicable), action, user (if applicable) and a contextual message indicating success or failure of the action.

26 The following information is logged as a result of the Security Administrator generating/importing or deleting cryptographic keys:

a) **Importing user public key**: Action and key reference.

b) **Deleting user public key**: Action and key reference.

c) **Generating host key**: Action and key reference.

6.1.2 FAU_GEN.2

27 The TOE includes the user identity in audit events resulting from actions of identified users.

6.1.3 FAU_STG_EXT.1

28 Log files are transferred via SSH (see FCS_SSH_EXT.1 & FCS_SSHS_EXT.1) to the audit server in real time.

29 Logs are stored locally in rotating log files as follows:

a) **audit.** Up to 4000 records are stored before they are rotated. Only one live log is kept.

b) **event.** Up to 4000 records are stored before they are rotated. Only one live log is kept.

30 Administrators may view audit records and no capability to modify the audit records is provided. Local audit logs are persistent.

31 The log rotation behaviour is configurable and can be set to either drop new records or overwrite oldest records first. Audit records can be deleted manually.

6.2 Cryptographic Support

Table 14: CAVP SFR Mapping

SFR	Algorithm Capability	CAVP
FCS_CKM.1 Cryptographic Key Generation	ECDSA KeyGen (FIPS Pub 186-4) (P-256, P-384, P-521)	A3451
FCS_CKM.2 Cryptographic Key Establishment	Elliptic Curve-based Schemes (NIST SP 800-56A Rev 3)	

FCS_COP.1/DataEncryption Cryptographic Operation (AES Data Encryption/Decryption)	AES CTR (128 and 256 bits)	
FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)	RSA SigGen (FIPS 186-4) (modulus 2048 bits) RSA SigVer (FIPS 186-4) (modulus 2048 bits)	
	ECDSA SigGen (FIPS 186-4) (256, 384, 521 bits) ECDSA SigVer (FIPS 186-4) (256, 384, 521 bits)	
FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)	SHA-256, SHA-384, SHA-512 (256, 384, and 512 bits respectively)	
FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)	HMAC-SHA-256, HMAC-SHA-512 (256, and 512 bits respectively)	
FCS_RBG_EXT.1	HASH_DRBG:SHA-256 (256 bits)	

32

6.2.1 FCS_CKM.1

33 The TOE supports key generation for the following asymmetric schemes:

a) **ECC P-256/P-384/P-521.** Used in SSH authentication and key exchange.

6.2.2 FCS_CKM.2

34 The TOE supports the following key establishment schemes:

a) **ECC schemes.** Used in SSH key exchange. TOE is both sender and receiver.

35 Table 15 below identifies the scheme being used by each service.

Table 15: Key Agreement Mapping

Scheme	SFR	Service
ECC	FCS_SSHS_EXT.1	Administration / Syslog

6.2.3 FCS_CKM.4

36 During the zeroisation process the encryptor will reboot destroying plaintext keys held in volatile storage. Keys stored in plaintext in volatile storage are overwritten with zeros after use.

37 Key destruction of keys in non-volatile storage is initiated by the Security Administrator via the CLI / SSH administrative interfaces.

38 Table 17 shows the origin, storage location and destruction details for cryptographic keys. Unless otherwise stated, the keys are generated by the TOE.

6.2.4 FCS_COP.1/DataEncryption

39 The TOE provides symmetric encryption and decryption capabilities using 128 and 256 bit AES in CTR mode. AES is implemented in SSH.

40 The relevant NIST CAVP certificate numbers are listed Table 4.

6.2.5 FCS_COP.1/SigGen

41 The TOE provides cryptographic signature generation and verification services using:

a) RSA Signature Algorithm with key size of 2048 bits,

b) ECDSA Signature Algorithm with key sizes of 256, 384 and 521 bits

42 The RSA signature verification services are used in firmware integrity checks.

43 The ECDSA signature verification services are used in the SSH protocol.

44 The relevant NIST CAVP certificate numbers are listed in Table 4.

6.2.6 FCS_COP.1/Hash

45 The TOE provides cryptographic hashing services using SHA-256, SHA-384 and SHA-512.

46 SHA is implemented in the following parts of the TSF:

a) SSH;

b) Digital signature verification as part of trusted update validation; and

c) Hashing of passwords in non-volatile storage.

47 The relevant NIST CAVP certificate numbers are listed in Table 4.

6.2.7 FCS_COP.1/KeyedHash

48 The TOE provides keyed-hashing message authentication services HMAC-SHA-256, and HMAC-SHA-512.

49 HMAC is implemented in SSH.

50 The characteristics of the HMACs used in the TOE are given in Table 16.

Table 16: HMAC Characteristics

Algorithm	Block Size	Key Size	Digest Size
HMAC-SHA-256	512 bits	256 bits	256 bits
HMAC-SHA-512	1024 bits	512 bits	512 bits

51 The relevant NIST CAVP certificate numbers are listed in Table 4.

6.2.8 FCS_RBG_EXT.1

52 The TOE contains a HASH_DRBG that is seeded from a SP 800-90B compliant hardware based TRNG. Entropy from the noise source is conditioned and used to seed the DRBG with 256 bits of full entropy.

53 Additional detail is provided the proprietary Entropy Description.

6.2.9 FCS_SSH_EXT.1

54 The TOE implements an SSH server for remote administration.

55 The TOE implements SSH in compliance with RFCs 4251, 4252, 4253, 4254, 4344, 5656, and 6668.

56 The TOE SSH client supports public keys for user authentication using ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521.

57 The TOE examines the size of each received SSH packet. If the packet is greater than 256KB, it is automatically dropped.

58 The TOE utilizes AES-CTR-128 and AES-CTR-256 for SSH encryption.

59 The TOE supports host keys using ecdsa-sha2-256

60 The TOE provides data integrity for SSH connections via hmac-sha2-256, hmac-sha2-512.

61 The TOE supports the following shared secret establishment algorithms, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521.

62 The TOE uses SSH KDF defined in RFC 5656 (Section 4)

63 The TOE will re-key SSH connections after 1 hour or after an aggregate of 1 gig of data has been exchanged (whichever occurs first).

64 The TOE authenticates the identity of the SSH client using a local database associating each user with its corresponding public key.

6.2.10 FCS_SSHS_EXT.1

65 The TOE uses host keys using ecdsa-sha2-256.

6.3 Identification and Authentication

6.3.1 FIA_PMG_EXT.1

66 The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower case letters, numbers, and special characters “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, ”<”, ”>”, ”?”.

67 The minimum password length is settable by the Administrator and is configurable between 8 to 29 characters.

6.3.2 FIA_UIA_EXT.1

68 The TOE requires all users to be successfully identified and authenticated. The TOE warning banner is displayed prior to authentication.

69 Administrative access to the TOE is facilitated through several interfaces:

a) **CLI.** Administrative CLI via direct serial connection.

b) **SSH CLI.** Administrative CLI via SSH.

70 The TOE prompts the user locally for a password credential. The TOE is administered remotely via SSH with public keys. Only after the administrative user presents the correct authentication credentials will they be granted access to the TOE administrative functionality. No TOE administrative access is permitted until an administrator is successfully identified and authenticated.

71 The process for administering the TOE locally is as follows. The user is first prompted to provide a username. After the user provides the username, the user is prompted to provide the administrative credential associated with the user account (e.g. password).

72 For administering the TOE remotely, the user must provide the username and public key credentials simultaneously.

73 The TOE then either grants administrative access (if the combination of username and credential is correct) or indicates that the login was unsuccessful. The TOE does not provide a reason for failure in the cases of a login failure.

6.3.3 FIA_UAU.7

74 For all authentication at the local CLI the TOE provides no feedback when the administrative password is entered so that the password is obscured.

6.4 Security Management

6.4.1 FMT_MOF.1/Functions

75 The TOE restricts the ability to modify audit functionality when Local Audit Storage is full to Security Administrators.

76 The Security Administrator may modify the audit functionality by “enabling wrapping” which will cause the TOE to overwrite previous audit records starting with the oldest first when storage is full, or by “disabling wrapping” which will cause the TOE to drop new audit data when storage is full.

6.4.2 FMT_MOF.1/ManualUpdate

77 The TOE restricts the ability to enable the functions to perform manual updates to Security Administrators.

6.4.3 FMT_MOF.1.1/Services

78 The TOE restricts the ability to start and stop the services to Security Administrators.

79 The Security Administrator may start and stop the SSH service.

6.4.4 FMT_MTD.1/CoreData

80 Users are required to login before being provided with access to any administrative functions. Access to TSF data and functions is restricted to Security Administrators as described by FMT_SMR.2 below.

6.4.5 FMT_MTD.1/CryptoKeys

81 The TOE restricts the ability to manage the cryptographic keys to Security Administrators.

82 The Administrator is able to manage the import and deletion of the trusted public keys database for the purpose of remote SSH authentication.

6.4.6 FMT_SMF.1

83 The TOE provides the following management capabilities:

a) Ability to administer the TOE remotely (SSH)

b) Ability to configure the access banner via CLI or SSH CLI

c) Ability to configure the remote session inactivity time before session termination

   i) The CLI / SSH CLI timeout value is set via the CLI or SSH CLI

d) Ability to update the TOE and to verify the updates via CLI or SSH CLI

e) Ability to start and stop services

f) 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);

g) Ability to modify the behaviour of the transmission of audit data to an external IT entity

h) Ability to manage the cryptographic keys

i) Ability to set the time which is used for time-stamps

j) Ability to administer the TOE locally

k) Ability to configure the local session inactivity time before session termination or locking

l) Ability to manage the trusted public keys database

6.4.7 FMT_SMR.2

84 The TOE defines four roles for accessing the TSFs:

a) **Administrators**: is a Security Administrator and can change defaults, query, modify, delete and clear the CI entries and User accounts, clear the audit log, view the audit log, set the system time and initiate the firmware update via CLI or Keypad. This account is used to access the CLI and SSH CLI.

b) **Supervisors**: can change defaults, query, modify, delete and clear the CI entries, view the User accounts table and audit log and set the system time.

c) **Operators**: can query the CI and User Account tables only, and view the audit log.

d) **Upgraders**: can remotely upgrade the firmware via USB query the CI and User Account tables and view the audit log.

85 Management of TSF data is restricted to Security Administrators.

6.5 Protection of the TSF

6.5.1 FPT_SKP_EXT.1

86 Keys are protected as described in Table 17. In all cases, plaintext private keys cannot be viewed through an interface designed specifically for that purpose.

Table 17: Keys

Key	Algorithm	Storage	Zeroization
SSH Private Keys	ECDSA	Flash – plaintext	SSH Private Keys are stored in plaintext in non-volatile storage are overwritten with zeros when destroyed.
SSH Public Keys	ECDSA	Flash-plaintext	SSH public keys are cleared from storage by Security Administrator initiated functions. Keys stored in plaintext in non-volatile storage are overwritten with zeros when destroyed.
SSH Session Keys	AES / ECDH	RAM – plaintext	OpenSSL ensures that keys (including re-keyed keys) are overwritten with zeroes when no longer required.
System Master Key (KEK)	AES-CFB	Flash-plaintext	The SMK is overwritten with zeroes when the erase button has been pressed

6.5.2 FPT_APW_EXT.1

87 Passwords are protected as describe in Table 18. In all cases plaintext passwords cannot be viewed through an interface designed specifically for that purpose.

Table 18: Passwords

Key/Password	Generation/ Algorithm	Storage
Locally stored administrator passwords	User generated	Flash - SHA-256 hash encrypted with an AES-CFB 256 bit key

6.5.3 FPT_TST_EXT.1

88 At startup, the TOE undergoes the following tests:

a) Firmware Integrity Tests

b) Cryptographic Kown Answer Tests

89 These tests ensure the correct operation of the cryptographic functionality of the TOE, and verify that the correct TOE image is being used. The cryptographic functionality will not be available if the tests fail, and any operation of the TOE supported by this functionality will not be available. If any tests fail, the device enter a Secure shutdown state and Halt (“Secure Halt”). Thereby preventing the module being configured and passing any data over the Network data output interface. Attempt to recover by power-cycle. If the Secure Halt condition persists the module cannot be recovered and must be returned to the factory.

6.5.4 FPT_TUD_EXT.1

90 The current firmware version may be queried using any administrative interface.

91 The Security Administrator manually initiates TOE updates from the Local or SSH CLI. TOE update files must first be available to the TOE by plugging in a USB containing the upgrade image. The TOE does not support delayed activation.

92 TOE update files are digitally signed (RSA) and the signature is verified using a hardcoded public key prior to installation of the update. If verification fails, the update is aborted, and an error message is displayed.

6.5.5 FPT_STM_EXT.1

93 The TOE allows the Security Administrator to set the time manually.

94 The TOE makes use of time for the following:

a) Audit record timestamps

b) Session timeouts (lockout enforcement)

6.6 TOE Access

6.6.1 FTA_SSL_EXT.1

95 The Security Administrator may configure the TOE to terminate an inactive local interactive session following a specified period of time. This is applicable to the local CLI. Idle timeout for the local CLI can be configured between 3 to 60 minutes.

6.6.2 FTA_SSL.3

96 The Security Administrator may configure the TOE to terminate an inactive remote interactive session following a specified period of time. This is applicable to the SSH CLI.

6.6.3 FTA_SSL.4

97 Administrative users may terminate their own sessions at any time by either calling the “logout” command at the local CLI and remote SSH CLI.

6.6.4 FTA_TAB.1

98 The TOE displays an administrator configurable message to users prior to login at the CLI, SSH CLI.

6.7 Trusted Path/Channels

6.7.1 FTP_ITC.1

99 The TOE supports secure communication with the following IT entities:

a) Audit server per FCS_SSH_EXT.1 & FCS_SSHS_EXT.1

100 The trusted channel is initiated by the external IT entity and the TOE acts as the server.

101 The TOE is the initiator of communication via the trusted channel.

6.7.2 FTP_TRP.1/Admin

102 The TOE provides the following trusted paths for remote administration:

a) SSH CLI. Administrative CLI via SSH per FCS_SSH_EXT.1 & FCS_SSHS_EXT.1

7 Rationale

7.1 Conformance Claim Rationale

103 The following rationale is presented with regard to the PP conformance claims:

a) **TOE type.** As identified in section 2.1, the TOE is network device, consistent with the NDcPP.

b) **Security problem definition.** As shown in section 3, the threats, OSPs and assumptions are reproduced directly from the NDcPP.

c) **Security objectives.** As shown in section 4, the security objectives are reproduced directly from the NDcPP.

d) **Security requirements.** As shown in section 5, the security requirements are reproduced directly from the NDcPP. No additional requirements have been specified.

7.2 Security Objectives Rationale

104 All security objectives are drawn directly from the NDcPP.

7.3 Security Requirements Rationale

105 All security requirements are drawn directly from the NDcPP. Table 19 presents a mapping between threats and SFRs as presented in the NDcPP.

Table 19: NDcPP SFR Rationale

Identifier	SFR Rationale
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	• The Administrator role is defined in FMT_SMR.2 and the relevant administration capabilities are defined in FMT_SMF.1 and FMT_MTD.1/CoreData, with optional additional capabilities in FMT_MOF.1/Services and FMT_MOF.1/Functions • The actions allowed before authentication of an Administrator are constrained by FIA_UIA_EXT.1, and include the advisory notice and consent warning message displayed according to FTA_TAB.1 • The requirement for the Administrator authentication process is described in FIA_UIA_EXT.1 • Locking of Administrator sessions is ensured by FTA_SSL_EXT.1 (for local sessions), FTA_SSL.3 (for remote sessions), and FTA_SSL.4 (for all interactive sessions) • The secure channel used for remote Administrator connections is specified in FTP_TRP.1/Admin • (Malicious actions carried out from an Administrator session are separately addressed by T.UNDETECTED_ACTIVITY) • If the TOE provides remote administration using a password-based authentication mechanism, FIA_AFL.1

Identifier	SFR Rationale
	provides actions on reaching a threshold number of consecutive password failures.
T.WEAK_CRYPTOGRAPHY	• Requirements for key generation and key distribution are set in FCS_CKM.1 and FCS_CKM.2 respectively • Requirements for use of cryptographic schemes are set in FCS_COP.1/DataEncryption, FCS_COP.1/SigGen, FCS_COP.1/Hash, and FCS_COP.1/KeyedHash • Requirements for random bit generation to support key generation and secure protocols (see SFRs resulting from T.UNTRUSTED_COMMUNICATION_CHANNELS) are set in FCS_RBG_EXT.1 • Management of cryptographic functions is specified in FMT_SMF.1
T.UNTRUSTED_COMMUNICATION_CHANNELS	• The general use of secure protocols for identified communication channels is described at the top level in FTP_ITC.1 and FTP_TRP.1/Admin; for distributed TOEs the requirements for inter-component communications are addressed by the requirements in FPT_ITT.1 • Requirements for the use of secure communication protocols are set for allowed protocols in FCS_DTLSC_EXT.1, FCS_DTLSC_EXT.2, FCS_DTLSS_EXT.1, FCS_DTLSS_EXT.2, FCS_HTTPS_EXT.1, FCS_IPSEC_EXT.1, FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSS_EXT.1, FCS_TLSS_EXT.2 • Requirements for the use of secure communication protocols implemented by the packages specified in Section 2.2 may be found in the respective package's document. • Optional and selection-based requirements for use of public key certificates to support secure protocols are defined in FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3
T.WEAK_AUTHENTICATION_ENDPOINTS	• The use of appropriate secure protocols to provide authentication of endpoints (as in the SFRs addressing T.UNTRUSTED_COMMUNICATION_CHANNELS) are ensured by the requirements in FTP_ITC.1 and FTP_TRP.1/Admin; for distributed TOEs the authentication requirements for endpoints in inter-component communications are addressed by the requirements in FPT_ITT.1 • Additional possible special cases of secure authentication during registration of distributed TOE components are addressed by FCO_CPC_EXT.1 and FTP_TRP.1/Join.

Identifier	SFR Rationale
T.UPDATE_COMPROMISE	• Requirements for protection of updates are set in FPT_TUD_EXT.1 • Additional optional use of certificate-based protection of signatures can be specified using FPT_TUD_EXT.2, supported by the X.509 certificate processing requirements in FIA_X509_EXT.1, FIA_X509_EXT.2 and FIA_X509_EXT.3 • Requirements for management of updates are defined in FMT_SMF.1 and (for manual updates) in FMT_MOF.1/ManualUpdate, with optional requirements for automatic updates in FMT_MOF.1/AutoUpdate
T.UNDETECTED_ACTIVITY	• Requirements for basic auditing capabilities are specified in FAU_GEN.1 and FAU_GEN.2, with timestamps provided according to FPT_STM_EXT.1 and if applicable, protection of NTP channels in FCS_NTP_EXT.1. • Requirements for protecting audit records stored on the TOE are specified in FAU_STG.1. • Requirements for secure storage and transmission of local audit records to an external IT entity via a secure channel are specified in FAU_STG_EXT.1 and FAU_STG_EXT.1. • .Optional additional requirements for dealing with potential loss of locally stored audit records are specified in FAU_STG_EXT.2, and FAU_STG_EXT.3.
T.SECURITY_FUNCTIONALITY_COMPROMISE	• Protection of secret/private keys against compromise is specified in FPT_SKP_EXT.1 • Secure destruction of keys is specified in FCS_CKM.4 • If (optionally) management of keys is provided by the TOE then this is specified in FMT_SMF.1 and confining this functionality to Security Administrators is required by FMT_MTD.1/CryptoKeys • If optional local administration using a password-based authentication mechanism is provided by the TOE, FIA_UAU.7 provides protection of password entry by providing only obscured feedback at the local console. • If the TOE provides password-based authentication mechanisms, requirements for password lengths and available characters are set in FIA_PMG_EXT.1. Requirements for secure storage of passwords are set in FPT_APW_EXT.1
T.SECURITY_FUNCTIONALITY_FAILURE	• Requirements for running self-test(s) are defined in FPT_TST_EXT.1
P.ACCESS_BANNER	• An advisory notice and consent warning message is required to be displayed by FTA_TAB.1