MPIC v3.5

Security Target

Version 1.11

May 2025

Document prepared by

www.lightshipsec.com

Document History

Version	Date	Author	Description
0.1	1 October 2024	T. Condly	Initial Draft.
1.0	11 October 2024	T. Condly	Draft for evaluation.
1.1	16 October 2024	T. Condly	Addressed Evaluator ORs.
1.2	23 October 2024	T. Condly	Added TD0886.
1.3	28 November 2024	T. Condly	Updated vendor logo, CAVP, and audit description.
1.4	12 December 2024	T. Condly	Addressed Evaluator OR.
1.5	22 January 2025	T. Condly	Addressed Validator ORs.
1.6	3 February 2025	T. Condly	Addressed Validator ORs.
1.7	7 February 2025	T. Condly	QA Updates.
1.8	4 March 2025	T. Condly	Added TD 0900.
1.9	25 March 2025	T. Condly	TSS updates.
1.10	28 April 2025	T. Condly	Added TD0909.
1.11	18 May 2025	T. Condly	Addressed Validator ORs.

Table of Contents

List of Tables

1 Introduction

1.1 Overview

1 This Security Target (ST) defines the CAE MPIC Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

2 The CAE MPIC is a standalone physical Network Device, used to transmit data from the hardware panels to a software-based flight simulation, processed by one or more Daughter Boards (DB). The simulation data is processed by the DB's and then feedback is transmitted back to the hardware panels via the MPIC. It comes in a range of form factors (see Table 5). The different form factors can be installed in combination or independently to Network data. All form factors provide a basic set of security functions such as, a secure remote management path, identification and authentication services to trusted administrators, and secure auditing of administrator actions. The form factors are not security relevant and the claimed SFRs are supported across all TOE models.

3 The MPIC-PCMIP form factor differs as it has a standard type slot for extensions compared to the custom interface on the MPIC. The MPIC-EMB differs as it is designed to be embedded and not mounted into systems. The MPIC-ILAC differs as its main function is to supply variable AC voltage to the cockpit integral lighting. The MPIC-SBC differs as its main function is to provide faster ethernet computing with a second ethernet port and a 48 pin daughterboard connector for demanding autopilot simulation.

1.2 Identification

Table 1: Evaluation identifiers

Target of Evaluation	CAE MPIC Build: 3.5.10
Security Target	CAE MPIC v3.5 Security Target, v1.11, May 2025

1.3 Conformance Claims

4 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	Source	Applicability Rational
TD0682	Addressing Ambiguity in FCS_SSHS_EXT.1 Tests	PKG_SSH	Applicable
TD0695	Choice of 128 or 256 bit size in AES-CTR in SSH Functional Package.	PKG_SSH	Applicable
TD0732	FCS_SSHS_EXT.1.3 Test 2 Update	PKG_SSH	Applicable
TD0777	Clarification to Selections for Auditable Events for FCS_SSH_EXT.1	PKG_SSH	Applicable
TD0909	Updates to FCS_SSH_EXT.1.1 App Note in SSH FP 1.0	PKG_SSH	Applicable
TD0836	NIT Technical Decision: Redundant Requirements in FPT_TST_EXT.1	NDcPP	Applicable.
TD0868	NIT Technical Decision: Clarification of time frames in FCS_IPSEC_EXT.1.7 and FCS_IPSEC_EXT.1.8	NDcPP	N/A – IPSEC is not claimed.
TD0879	NIT Decision: Correction of Chapter Headings in CPP_ND_V3.0E	NDcPP	Applicable
TD0880	NIT Decision: Removal of Duplicate Selection in FMT_SMF.1.1	NDcPP	Applicable
TD0886	Clarification to FAU_STG_EXT.1 Test 6	NDcPP	Applicable
TD0899	NIT Technical Decision: Correction of Renegotiation Test for TLS 1.2	NDcPP	N/A – TLS is not claimed.
TD0900	NIT Technical Decision: Clarification to Local Administrator Access in FIA_UIA_EXT.1.3	NDcPP	Applicable

1.4 Terminology

Table 3: Terminology

Term	Definition
CC	Common Criteria
NDcPP	collaborative Protection Profile for Network Devices
PP	Protection Profile
TOE	Target of Evaluation
TSF	TOE Security Functionality

2 TOE Description

2.1 Type

5 The TOE is a network device that transmits data between the hardware panels to a software-based flight simulator.

2.2 Usage

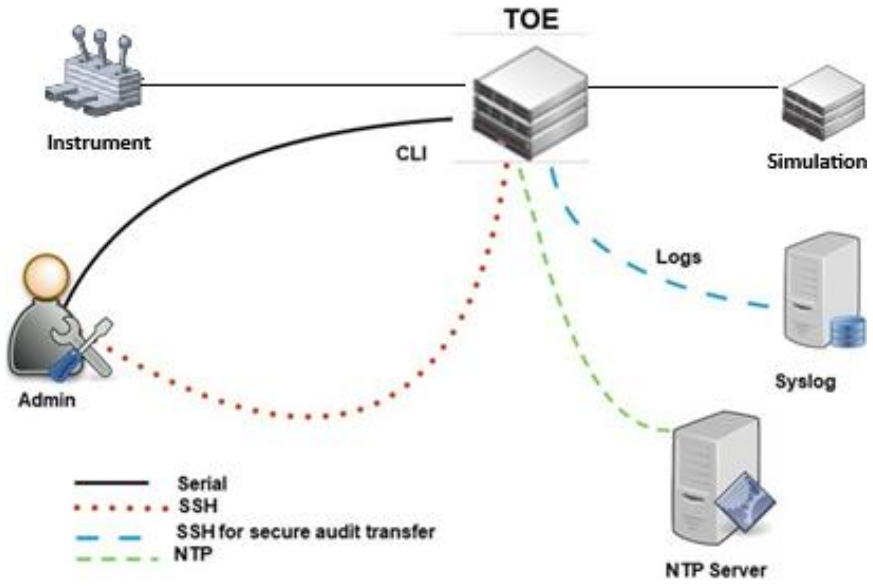
2.2.1 Deployment

6 The TOE is deployed as a network device and is a key network infrastructure component in software-based flight simulators. The TOE protects authorized communications as described in section 2.3 Security Functions / Logical Scope below.

2.2.2 Interfaces

7 The TOE management interfaces are shown in Figure 1.

Figure 1: TOE Interfaces



8 The TOE interfaces are as follows:

a) **CLI.** CLI via Serial and CLI via remote SSH connection

b) **Logs.** The TOE uses a Syslog server.

c) **NTP.** The TOE synchronizes time via NTP.

d) **Instrument.** The TOE transmits simulation data between the software-based simulator and the hardware panels.

e) **Simulation.** The TOE transmits simulation data between the software-based simulator and the hardware panels.

2.3 Security Functions / Logical Scope

9 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.

d) **Identification and Authentication.** The TOE ensures that all users must be authenticated before accessing its functions and data.

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 be locked for a Security Administrator defined time period.

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 and destroy cryptographic keys. Relevant Cryptographic Algorithm Validation Program (CAVP) certificates are shown in Table 4.

Table 4: CAVP Certificates

Algorithm Capability	Certificate
AES-CTR	A2558
ECDSA Key Gen (186-4) ECDSA Sig Gen (186-4) ECDSA Sig Ver (186-4)	
RSA Key Gen (186-4) RSA Sig Gen (186-4)	

Algorithm Capability	Certificate
RSA Sig Ver (186-4)	
SHA-1, SHA-256, SHA-512	
HMAC-SHA-256, HMAC-SHA-512	
KAS-ECC	
CTR_DRBG (AES)	

2.4 Physical Scope

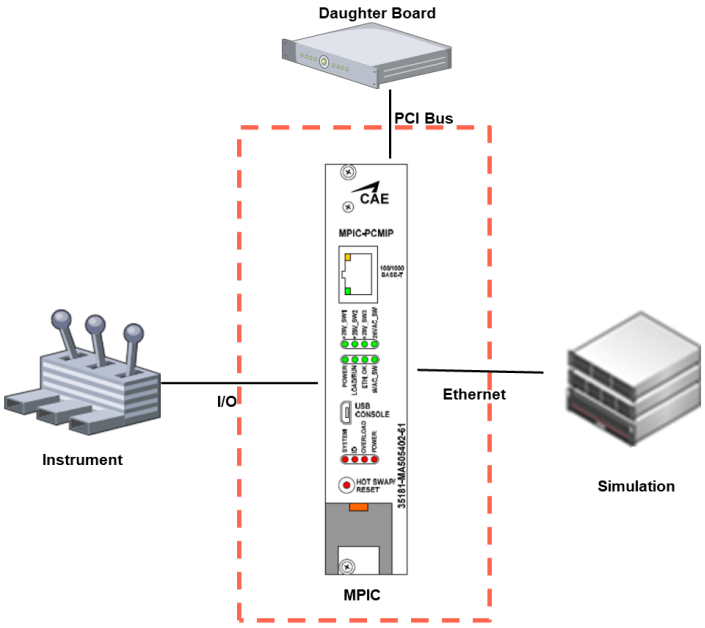
10 The physical boundary of the TOE includes all software and hardware shown in Table 5. The TOE is delivered via commercial courier.

Table 5: TOE Models

Type/Model	CPU	Part Number	Software	Differences
MPIC	i.MX6 ARM Cortex-A9 (ARMv7-A) with CAAM	MA505400.61.2.268	cae-mx6qmpic-3.5.10 MPICLinuxDistributionXR 3.5	Form Factor
MPIC-PCMIP	i.MX6 ARM Cortex-A9 (ARMv7-A) with CAAM	MA505402.61.2.268		
MPIC-EMB	i.MX6 ARM Cortex-A9 (ARMv7-A) with CAAM	MA505404.61.2.268		
MPIC-EMB	i.MX6 ARM Cortex-A9 (ARMv7-A) with CAAM (quad-core)	MA505404.62.2.268		
MPIC-ILAC	i.MX6 ARM Cortex-A9 (ARMv7-A) with CAAM	MA563540.61.2.268		
MPIC-SBC	i.MX6 ARM Cortex-A9 (ARMv7-A) with CAAM (quad-core)	MA563510.61.2.268		

11 An example deployment of the TOE is depicted in Figure 2.

Figure 2: TOE Deployment



2.4.1 Guidance Documents

12 The TOE includes the following guidance documents (PDF):

a) CAE MPIC v3.5 Common Criteria Guide, v1.2

b) Getting Started with MPIC, Developer's Guide – TPD 20365 Rev 9, 07 October 2024

2.4.2 Non-TOE Components

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

a) **Audit Server.** The TOE sends audit events to syslog server.

b) **NTP Server.** The TOE synchronizes time via NTP.

c) **Instrument.** The TOE transmits simulation data between the software-based simulator and the hardware panels.

d) **Simulator.** The TOE transmits simulation data between the software-based simulator and the hardware panels.

2.4.3 Functions not included in the TOE Evaluation

14 The function that falls outside of the scope of this evaluation is the transmission of data between the hardware panel to the DB's and simulation. The data that traverses the TOE do not originate from the TOE and are not destined for the TOE directly. The TOE converts electrical signals from input to PCI bus signals, ethernet packets and vice versa. These signals are processed by DB's to update the simulation and hardware instruments.

3 Security Problem Definition

15 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.

Identifier	Description
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. 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

16 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. Note: For vNDs the TOE includes only the contents of the its own VM, and does not include other VMs or the VS.
OE.NO_THRU_ TRAFFIC_ PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For vNDs, this includes the VS Administrator responsible for configuring the VMs that implement ND functionality. 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

5.1 Conventions

17 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").

18 **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

19 Refer to the Extended Components Definitions in sections of the PP and Functional Package as follows:

a) NDcPP – Appendix C.

b) PKG_SSH – No extended components definition identified.

20 Extended components are identified by an "EXT" appended to the SFR identifier.

5.3 Functional Requirements

Table 10: Summary of SFRs

Requirement	Title	Source	Type
FAU_GEN.1	Audit Data Generation	NDcPP	Mandatory
FAU_GEN.2	User Identity Association	NDcPP	Mandatory
FAU_STG_EXT.1	Protected Audit Event Storage	NDcPP	Mandatory
FCS_CKM.1	Cryptographic Key Generation	NDcPP	Mandatory
FCS_CKM.2	Cryptographic Key Establishment	NDcPP	Mandatory
FCS_CKM.4	Cryptographic Key Destruction	NDcPP	Mandatory
FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/Decryption)	NDcPP	Mandatory
FCS_COP.1/SigGen	Cryptographic Operation (Signature Generation and Verification)	NDcPP	Mandatory
FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)	NDcPP	Mandatory
FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)	NDcPP	Mandatory

Requirement	Title	Source	Type
FCS_NTP_EXT.1	NTP Protocol	NDcPP	Selection
FCS_RBG_EXT.1	Random Bit Generation	NDcPP	Mandatory
FCS_SSH_EXT.1	SSH Protocol	PKG_SSH	Mandatory
FCS_SSHC_EXT.1	SSH Protocol – Client	PKG_SSH	Selection
FCS_SSHS_EXT.1	SSH Protocol – Server	PKG_SSH	Selection
FIA_AFL.1	Authentication Failure Handling	NDcPP	Selection
FIA_PMG_EXT.1	Password Management	NDcPP	Selection
FIA_UIA_EXT.1	User Identification and Authentication	NDcPP	Mandatory
FIA_UAU.7	Protected Authentication Feedback	NDcPP	Selection
FMT_MOF.1/Functions	Management of Security Functions Behaviour	NDcPP	Selection
FMT_MOF.1/ManualUpdate	Management of Security Functions Behaviour	NDcPP	Mandatory
FMT_MOF.1/Services	Management of Security Functions Behaviour	NDcPP	Selection
FMT_MTD.1/CoreData	Management of TSF Data	NDcPP	Mandatory
FMT_MTD.1/CryptoKeys	Management of TSF Data	NDcPP	Selection
FMT_SMF.1	Specification of Management Functions	NDcPP	Mandatory
FMT_SMR.2	Restrictions on Security Roles	NDcPP	Mandatory
FPT_SKP_EXT.1	Protection of TSF Data (for reading of all symmetric keys)	NDcPP	Mandatory
FPT_APW_EXT.1	Protection of Administrator Passwords	NDcPP	Selection
FPT_TST_EXT.1	TSF Testing	NDcPP	Mandatory
FPT_TUD_EXT.1	Trusted Update	NDcPP	Mandatory
FPT_STM_EXT.1	Reliable Time Stamps	NDcPP	Mandatory
FTA_SSL_EXT.1	TSF-initiated Session Locking	NDcPP	Mandatory
FTA_SSL.3	TSF-initiated Termination	NDcPP	Mandatory
FTA_SSL.4	User-initiated Termination	NDcPP	Mandatory
FTA_TAB.1	Default TOE Access Banners	NDcPP	Mandatory
FTP_ITC.1	Inter-TSF trusted channel	NDcPP	Mandatory
FTP_TRP.1/Admin	Trusted Path	NDcPP	Mandatory

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 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 2***~~ ***Table 11****.*

Table 11: Audit 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.

Requirement	Auditable Events	Additional Audit Record Contents
FCS_NTP_EXT.1	• Configuration of a new time server • Removal of configured time server	Identity if new/removed time server
FCS_RBG_EXT.1	None.	None.
FCS_SSH_EXT.1	[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 attempted connection (IP Address)]
	[Termination of SSH connection session]	[Non-TOE endpoint of attempted connection (IP Address)]
	[Dropping of packet(s) outside defined size limits]	[Packet size]
FCS_SSHC_EXT.1	No events specified	N/A
FCS_SSHS_EXT.1	No events specified	N/A
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of 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.
FMT_MTD.1/CryptoKeys	None.	None.
FMT_SMF.1	All management activities of TSF data.	None.

Requirement	Auditable Events	Additional Audit Record Contents
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.	None
	Termination of the trusted channel.	None
	Failure of the trusted channel functions	Reason for Failure
FTP_TRP.1/Admin	Initiation of the trusted path.	None
	Termination of the trusted path.	None
	Failure of the trusted path functions.	Reason for Failure

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 11****.*

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 [non-persistent] audit records locally with a minimum storage size of [*7MB and 800MB*].

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

- RSA schemes using cryptographic key sizes of [*2048 bits, 3072 bits, 4096 bits*] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3;
- ECC schemes using ‘NIST curves’ [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4;

- FFC Schemes using ‘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].

] 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: [

- 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].

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

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-1, SHA-256, SHA-512] ~~and cryptographic key sizes [*assignment: cryptographic key sizes*]~~ and **message digest sizes [160, 256, 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 *[256 bits, 512 bits]* **and message digest sizes [256, 512] bits** that meet the following: *ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"*.

FCS_NTP_EXT.1 NTP Protocol

FCS_NTP_EXT.1.1 The TSF shall use only the following NTP version(s) [NTP v4 (RFC 5905)].

FCS_NTP_EXT.1.2 The TSF shall update its system time using [

- Authentication using [SHA1] as the message digest algorithm(s);

].

FCS_NTP_EXT.1.3 The TSF shall not update NTP timestamp from broadcast and/or multicast addresses.

FCS_NTP_EXT.1.4 The TSF shall support configuration of at least three (3) NTP time sources in the Operational Environment.

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 [[*two*] platform-based noise sources] 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 [client, server] in accordance with that complies with RFCs 4251, 4252, 4253, 4254, [4344, 5656, 6668, 8268, 8308, 8332, 8709] 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),
    - ssh-ed25519 (RFC 8709),

    ]

] and no other methods.

FCS_SSH_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [*256 kilobytes)*] 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: [

- 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),
- diffie-hellman-group18-sha512 (RFC 8268),
- 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 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.

FCS_SSHC_EXT.1 SSH Protocol - Client

FCS_SSHC_EXT.1.1 The TSF shall authenticate its peer (SSH server) using: [

- using a local database by associating each host name with a public key corresponding to the following list: [
    - ssh-rsa (RFC 4253),
    - ecdsa-sha2-nistp256 (RFC 5656),
    - ecdsa-sha2-nistp384 (RFC 5656),
    - ecdsa-sha2-nistp521 (RFC 5656),

  ],

]

] as described in RFC 4251 section 4.1.

FCS_SSHS_EXT.1 SSH Server Protocol

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

- ssh-rsa (RFC 4253),
- ecdsa-sha2-nistp256 (RFC 5656),

].

5.3.3 Identification and Authentication (FIA)

FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when an Administrator configurable positive integer within [*1-1000*] 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].

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 [15] and [1024] 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 [SSH password, SSH public key] and [no other mechanism]. The TSF shall provide the following local authentication mechanisms [password-based].

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

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 [transmission of audit data to an external IT entity] 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 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 NTP;
    - Ability to administer the TOE locally;
    - Ability to configure authentication failure parameters for FIA_AFL.1;
    - 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;
- Prior to providing any cryptographic service and [on-demand] to verify correct operation of cryptographic implementation necessary to fulfil the TSF;
- [no other] self-tests.

to demonstrate the correct operation of the TSF.

FPT_TST_EXT.1.2 The TSF shall respond to [all failures] by [[*making any operation supported by the failed function unavailable*]].

Application Note: This SFR modified by TD0836.

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.

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 [synchronise time with an NTP server].

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 [***audit server communications***].

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

21 The TOE security assurance requirements are summarized in Table 12.

Table 12: 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

22 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

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

6.1 Security Audit

6.1.1 FAU_GEN.1

24 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.

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

a) **Generate SSH key-pair**. Action and key reference.

b) **Import of SSH public key**. Action and key reference.

c) **Deletion of SSH public key**. Action and key reference.

6.1.2 FAU_GEN.2

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

6.1.3 FAU_STG_EXT.1

27 Log files are transferred in real time via SSH tunnel (see FCS_SSHC_EXT.1) to the external audit server. Only authorized administrators may view audit records and no capability to modify the audit records is provided.

28 All logs are non-persistent and stored locally in rotating log files as follows:

a) **/var/log/syslog.** The TOE maintains a log partition with a maximum disk space of 800MB. The TOE periodically rotates four log files to maintain approximately 50% capacity, or 400MB, to ensure that the space never becomes full. When a log file rotates, it is renamed and a new file is created. Once four log files have been created, the TOE deletes the oldest log file upon the generation of a new log, and continues logging.

b) **/var/log/auth.log.** The TOE maintains a log partition with a maximum disk space of 800MB. The TOE periodically rotates four log files to maintain approximately 50% capacity, or 400MB, to ensure that the space never becomes full. When a log file rotates, it is renamed and a new file is created. Once four log files have been created, the TOE deletes the oldest log file upon the generation of a new log, and continues logging.

c) **/var/audit/audit.log**. Rotates four log files. When each log file reaches a maximum size of 7MB, the old file gets renamed and a new file is created. When all four log files are full, the TOE removes the oldest log file first and continues logging.

6.2 Cryptographic Support

6.2.1 FCS_CKM.1

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

a) **RSA Schemes.** Key sizes of 2048, 3072 and 4096 bits. Used in SSH authentication.

b) **ECC Schemes.** Key sizes of 256, 384 and 521 bits. Used in SSH authentication and key exchange.

c) **FFC Schemes using safe primes.** Key sizes 2048, 3072, and 4096. Used in SSH Key exchange.

6.2.2 FCS_CKM.2

30 The TOE supports the following key establishment schemes:

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

b) **FFC schemes using safe primes.** Used in SSH key exchange. TOE is both sender and receiver. The following Diffie Helman groups are supported:

i) Group 14 per RFC 3526 section 3

ii) Group 16 per RFC 3526 section 5

iii) Group 18 per RFC 3526 section 7

31 Table 13 below identifies the scheme being used by each service.

Table 13: Key Agreement Mapping

Scheme	SFR	Service
ECC	FCS_SSHS_EXT.1	Administration
	FCS_SSHC_EXT.1	Audit Server
FFC Safe Primes	FCS_SSHS_EXT.1	Administration
	FCS_SSHC_EXT.1	Audit Server

6.2.3 FCS_CKM.4

32 Table 15 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

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

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

6.2.5 FCS_COP.1/SigGen

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

a) RSA Signature Algorithm with key sizes of 2048, 3072, 4096

b) ECDSA Signature Algorithm with NIST curves P-256, P-384, P-521

36 The RSA and ECDSA signature verification services are used for the SSH protocol and TOE firmware integrity checks.

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

6.2.6 FCS_COP.1/Hash

38 The TOE provides cryptographic hashing services using SHA-1, SHA-256, and SHA-512.

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

a) SSH; (SHA-1, SHA-256, and SHA-512)

b) Digital signature verification as part of trusted update validation; (SHA-256)

c) Hashing of passwords in non-volatile storage; (SHA-512)

d) NTP symmetric keys. (SHA-1)

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

6.2.7 FCS_COP.1/KeyedHash

41 The TOE provides keyed-hashing message authentication services using HMAC-SHA-256 and HMAC-SHA-512.

42 HMAC is implemented in SSH.

43 The characteristics of the HMACs used in the TOE are given in Table 14.

Table 14: 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

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

6.2.8 FCS_NTP_EXT.1

45 The TOE implements NTPv4 as per RFC 5905. The TOE supports SHA-1 authentication. The TOE allows configuration of up to three NTP servers.

6.2.9 FCS_RBG_EXT.1

46 The TOE contains a CTR_DRBG that is seeded by CPU and other hardware provided entropy sources. Entropy from the noise is conditioned and used to seed the DRBG with 256 bits of full entropy.

47 Additional details are provided the proprietary Entropy Description.

6.2.10 FCS_SSH_EXT.1, FCS_SSHC_EXT.2, FCS_SSHS_EXT.1

48 The TOE implements an SSH client for transmission of audit logs to the audit server and SSH server for remote administration.

49 The TOE implements SSH in compliance with RFCs 4251, 4252, 4253, 4254, 4344, 5656, 6668, 8268, 8308, 8332, and 8709.

50 The TOE SSH client supports public key authentication using the following algorithms: ssh-rsa, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, and ecdsa-sha2-nistp521.

51 The TOE SSH server supports both password-based and public key-based authentication using the following algorithms:

- Peer Authentication - ssh-rsa and ecdsa-sha2-nistp256.
- User Authentication – ssh-rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, ssh-ed25519.

52 The TOE establishes user identity by referencing the authorized keys file when presented with a public key authentication attempt.

53 The TOE supports the following key exchange algorithms: diffie-hellman-group14-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, ecdh-sha2-nistp256, ecdh-sha2-nistp384, and ecdh-sha2-nistp521.

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

55 The TOE utilises aes-ctr-128 and aes-ctr-256 for SSH encryption.

56 The TOE provides data integrity for SSH connections via hmac-sha2-256 and hmac-sha2-512.

57 The TOE derives cryptographic session keys via shared secret using SSH KDF as defined in RFC 4253 (Section 7.2) and RFC 5656 (Section 4).

58 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).

6.3 Identification and Authentication

6.3.1 FIA_AFL.1

59 The TOE is capable of tracking authentication failures of remote administrators.

60 When a user account has sequentially failed the configured number of allowed authentication attempts, the account will be locked for a Security Administrator defined period of time.

61 Failure of public key authentication directs the user to the password authentication method, incrementing the failure counter. After the failed number of allowed authentication attempts, the account will be locked for a Security Administrator defined period of time.

62 The local console does not implement the lockout mechanism.

6.3.2 FIA_PMG_EXT.1

63 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 “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”.

64 The minimum password length is settable by the Administrator and can range from 15 to 1024 characters.

6.3.3 FIA_UIA_EXT.1

65 The TOE requires all users to be successfully identified and authenticated. The TOE warning banner is displayed prior to authentication. No actions are allowed before administrator authentication.

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

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

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

67 Administrator credentials are the same for each user regardless of which interface is accessed. Both password-based and public key authentication are supported on the Bash CLI. Only password-based authentication is supported for local (serial) authentication. Once successfully authenticated, Administrators are presented with the command line.

6.3.4 FIA_UAU.7

68 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

69 The TOE does not permit access to any functions (other than the warning/consent banner and authentication interface) prior to login.

70 The TOE defines a single role, which is that of the Security Administrator. The Security Administrator is able to start and stop the trusted path / trusted channels via the CLI. The Security Administrator is able to modify the behaviour of the transmission of audit data to an external IT entity in the following capacity:

a) Enable and disable the syslog service.

b) Configure the reference identifier of the remote server.

c) Configure the public key used to authenticate to the remote server using the algorithms specified in FCS_SSHC_EXT.1.

6.4.2 FMT_MOF.1/ManualUpdate

71 The TOE restricts the ability to perform software updates to Security Administrators.

6.4.3 FMT_MOF.1/Services

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

73 The list of services Security Administrators can start and stop include the following:

- syslog
- ntp.

74 The Security Administrator is able to start and stop services over the CLI.

6.4.4 FMT_MTD.1/CoreData

75 Administrators are required to login before being provided with access to any administrative functions.

6.4.5 FMT_MTD.1/CryptoKeys

76 The TOE restricts the ability to manage all SSH keys to Security Administrators. Administrators can generate and delete SSH Host keys and SSH public keys. Administrators also have the ability to import and delete external host keys used for remote syslog communications.

6.4.6 FMT_SMF.1

77 The TOE provides the following management capabilities:

- Ability to administer the TOE locally and remotely.
- Ability to configure the access banner.
- Ability to configure the session inactivity time before session termination or locking.
- Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates.
- Ability to configure the authentication failure parameters for FIA_AFL.1.

- Ability to start and stop services.
- 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 NTP.
- Ability to manage the trusted public keys database.

78 Each management capability is available to administrators authenticated both locally and remotely via SSH.

6.4.7 FMT_SMR.2

79 The following user accounts are available, which are all Security Administrators:

a) **admin.** This account is used to access the CLI and SSH CLI.

80 Management of TSF data is restricted to Security Administrators.

6.5 Protection of the TSF

6.5.1 FPT_SKP_EXT.1

81 Keys are protected as described in Table 15. In all cases, plaintext keys cannot be viewed through an interface designed specifically for that purpose.

Table 15: Keys

Key	Algorithm	Storage	Zeroization
SSH Private Keys	RSA/ECDSA	Flash - plaintext	Keys are destroyed when generating new keys by deleting the previous file and creating a new file. Initiated via CLI command by the Security Administrator.
SSH Ephemeral Keys	AES / DH / ECDH	RAM – plaintext	OpenSSL ensures that keys (including re-keyed keys) are overwritten with zeroes when no longer required.
NTP Key	SHA-1	Flash - plaintext	Keys are destroyed by manually specifying the index of the key to delete. Initiated via CLI command by the Security Administrator.

6.5.2 FPT_APW_EXT.1

82 Passwords are protected as describe in

83 Table 16. In all cases plaintext passwords cannot be viewed through an interface designed specifically for that purpose.

Table 16: Passwords

Key/Password	Generation/ Algorithm	Storage
Locally stored administrator passwords	User generated	Flash - SHA-512 hash

6.5.3 FPT_TST_EXT.1

84 At startup, or when initiated by a Security Administrator, the TOE undergoes the following tests:

a) Firmware integrity test: Checks that the packages and cryptographic modules of the TOE have not been modified including but not limited to:

i) Openssl-fips

ii) Openssl

iii) Openssh

iv) cae-commands

v) cae-commands-extended

b) OpenSCAP tests: Security test of the firmware using OpenSCAP.

c) FIPS Test Suite: Cryptographic key generation and known answers tests to ensure the correctness of the cryptographic module.

85 These tests ensure the correct operation of the cryptographic functionality of the TOE, the FIPS module and 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.

6.5.4 FPT_TUD_EXT.1

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

87 The Security Administrator manually initiates TOE updates from the Bash CLI.

88 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. If the verification succeeds the update is applied and the TOE must be manually restarted to use the new version.

89 TOE updates are obtained by physical delivery from CAE to the onsite location.

6.5.5 FPT_STM_EXT.1

90 The TOE makes use of secure NTP to maintain date and time. The TOE can configure at least three different time servers, using SHA1 pre-shared keys for authentication, while also rejecting unsolicited broadcast and/or multicast time updates.

91 The TOE makes use of time for the following:

a) Audit record timestamps

b) Session timeouts

c) Lockout enforcement (authentication failure limit exceeded).

6.6 TOE Access

6.6.1 FTA_SSL_EXT.1

92 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.

6.6.2 FTA_SSL.3

93 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 Bash CLI.

6.6.3 FTA_SSL.4

94 Administrative users may terminate their own sessions at any time by using the “exit” command.

6.6.4 FTA_TAB.1

95 The TOE displays an administrator configurable message to users prior to login at the local CLI and Bash CLI.

6.7 Trusted Path/Channels

6.7.1 FTP_ITC.1

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

a) Audit server: The TOE connects to an external trusted audit server as a client via SSH per FCS_SSHC_EXT.1. SSH utilizes the following algorithms:

   i) Encryption: aes128-ctr, aes256-ctr

   ii) Authentication: ssh-rsa, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nitp521

   iii) Data integrity MAC: hmac-sha2-256, hmac-sha2-512

   iv) Key Exchange: ecdh-sha2-nistp256, diffie-hellman-group14- sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, ecdh-sha2-nistp384, ecdh-sha2-nistp521

6.7.2 FTP_TRP.1/Admin

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

a) **CLI.** Administrative CLI via SSH per FCS_SSHS_EXT.1.

7 Rationale

7.1 Conformance Claim Rationale

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

a) **TOE type.** As identified in section 2.1, the TOE is a 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

99 All security objectives are drawn directly from the NDcPP.

7.3 Security Requirements Rationale

100 All security requirements are drawn directly from the NDcPP. Table 17 presents a mapping between threats and SFRs as presented in the NDcPP.

Table 17: 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 provides actions on reaching a threshold number of consecutive password failures.

Identifier	SFR Rationale
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