Nokia LightSpan Access Node MF Common Criteria Security Target

Version 0.96

Contents

1 Introduction 7
1.1 Security Target Reference 7
1.2 TOE Identification 7
1.3 TOE Type 7
1.4 TOE Overview 7
1.5 TOE Description 8
1.5.1 Architecture Description 8
1.5.2 Physical scope 10
1.5.3 Evaluated configuration 11
1.5.4 Logical Scope 11
1.5.5 Delivery method 14
2 Conformance claims 15
2.1 Common Criteria Conformance Claims 15
3 Security Problem Definition 16
3.1 Threat Environment 16
3.2 Threats 16
3.3 Organizational security policies 17
3.4 Assumptions 17
4 Security objectives 19
4.1 Security Objectives for the TOE 19
4.2 Security Objectives for the Operational Environment 20
4.3 Rationale for the Security Objectives 20
4.3.1 Coverage 20
4.3.2 Sufficiency 21
5 Extended components definition 26
5.1 Security Audit (FAU) 26
5.1.1 Protected Audit Event Storage (FAU_STG_EXT) 26
5.2 Cryptographic Support (FCS) 27
5.2.1 NTP Protocol (FCS_NTP_EXT) 27
5.2.2 TLS Client Protocol (FCS_TLSC_EXT) 28
5.2.3 TLS Server Protocol (FCS_TLSS_EXT) 32
5.2.4 SSH Protocol (FCS_SSH_EXT) 35
5.3 Identification and Authentication (FIA) 37

5.3.1 Password Management (FIA_PMG_EXT) ... *37*
5.3.2 User Identification and Authentication (FIA_UIA_EXT) ... *38*
5.4 PROTECTION OF THE TSF (FPT) ... 39
5.4.1 Protection of TSF Data (FPT_SKP_EXT) ... *39*
5.4.2 Protection of Administrator Passwords (FPT_APW_EXT) ... *39*
5.4.3 Time stamps (FPT_STM_EXT) ... *40*
5.4.4 Trusted Update (FPT_TUD_EXT) ... *40*
5.5 TOE ACCESS (FTA) ... 41
5.5.1 TSF-initiated Session Locking (FTA_SSL_EXT) ... *41*
6 Security requirements for the TOE ... 43
6.1 SECURITY FUNCTIONAL REQUIREMENTS FOR THE TOE ... 43
6.1.1 Security Audit (FAU) ... *43*
6.1.2 Cryptographic Support (FCS) ... *46*
6.1.3 User data protection (FDP) ... *55*
6.1.4 Identification and Authentication (FIA) ... *55*
6.1.5 Security Management (FMT) ... *56*
6.1.6 Protection of the TSF (FPT) ... *57*
6.1.7 TOE Access (FTA) ... *58*
6.1.8 Trusted Path/Channels (FTP) ... *58*
6.2 SECURITY REQUIREMENTS DEPENDENCY ANALYSIS ... 60
6.3 SECURITY ASSURANCE REQUIREMENTS FOR THE TOE ... 64
6.4 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE ... 66
6.4.1 Coverage ... *66*
6.4.2 Sufficiency ... *68*
6.4.3 Security assurance requirements rationale ... *69*
7 TOE Summary Specification ... 71
7.1 SECURITY AUDIT ... 71
7.2 CRYPTOGRAPHIC SUPPORT ... 71
7.3 IDENTIFICATION AND AUTHENTICATION ... 72
7.4 SECURITY FUNCTION MANAGEMENT ... 73
7.5 PROTECTION OF THE TSF ... 75
7.6 TOE ACCESS ... 75
7.7 TRUSTED PATH / CHANNELS ... 75
7.7.1 Administrative traffic ... *76*
7.7.2 Communication to other server ... *76*

7.8 MANAGEMENT ACCESS 76
8 Glossary of terms and abbreviations 77
9 References 80

Figures

Figure 1 Lightspan node deployment model 7
Figure 2 High-level architecture 9
Figure 3 Lightspan Management Protocols 10

Tables

Table 1 Security Objectives for the TOE....19
Table 2 Security Objectives for the Operational Environment....20
Table 3 Mapping of security objectives to threats and policies....21
Table 4 Mapping of security objectives for the Operational Environment to assumptions, threats and policies....21
Table 5 Sufficiency of objectives countering threats....22
Table 6 Sufficiency of objectives holding assumptions 25
Table 7 Sufficiency of objectives enforcing Organizational Security Policies 25
Table 8 Security Functional Requirements and Auditable Events 46
Table 9 TOE SFR dependency analysis....64
Table 10 SARs 65
Table 11 Mapping of security functional requirements to security objectives....68
Table 12 Mapping of security objectives to security functional requirements....69
Table 13 Supported SSH Authentication and Encryption Schemes (AS-NE)....72
Table 14 Supported SSH Authentication and Encryption Schemes (Shelf-NE/LT-NE)....72

Change History

Version	Change Description	Author	Date
0.1	Initial draft version	Rasma Araby (atsec)	2025-01-17
0.2	Included information about SFRs	Rasma Araby (atsec)	2025-01-29
0.3	Added further refinements to the SFRs	Rasma Araby (atsec)	2025-01-31
0.4	Added information about TLS cipher suites	Rasma Araby (atsec)	2025-02-21
0.5	Addressed evaluator comments	Rasma Araby (atsec)	2025-04-14
0.6	Added further details about SFRs	Rasma Araby (atsec)	2025-04-29
0.7	Addressed evaluator comments	Rasma Araby (atsec)	2025-05-09
0.8	Addressed evaluator comments	Fanni Gózon (atsec)	2025-05-16
0.9	Addressed evaluator comments	Rasma Araby (atsec)	2025-06-04
0.91	Added details about the delivery mechanism	Rasma Araby (atsec)	2025-11-07
0.92	Added selection details in the SFRs, updated the list of guidance documentation and updated the TOE version	Rasma Araby (atsec)	2026-06-05
0.93	Adjusted details about supported SSH ciphersuites	Rasma Araby (atsec)	2026-06-25
0.94	Added the version number of the supplementary guide	Rasma Araby (atsec)	2026-07-10
0.95	Addressed evaluator comments	Rasma Araby (atsec)	2026-07-13
0.96	Addressed certifier comments	Rasma Araby (atsec)	2026-08-27

1 Introduction

1.1 Security Target Reference

ST Title: Nokia (Nokia Lightspan Access Node MF) Common Criteria Security Target

ST Version: Version 0.96

Date: 2026-08-27

Developer: Nokia

Keywords: Access Node, Network Device

1.2 TOE Identification

The TOE is the Nokia Lightspan Access Node MF (Lightspan) software version 25.12. The TOE software is running on the devices identified below:

- Lightspan Access Node MF-2 running Lightspan 25.12 (SW-build 2512.636)

1.3 TOE Type

The TOE type is an Access Node designed to support massive-scale access networks.

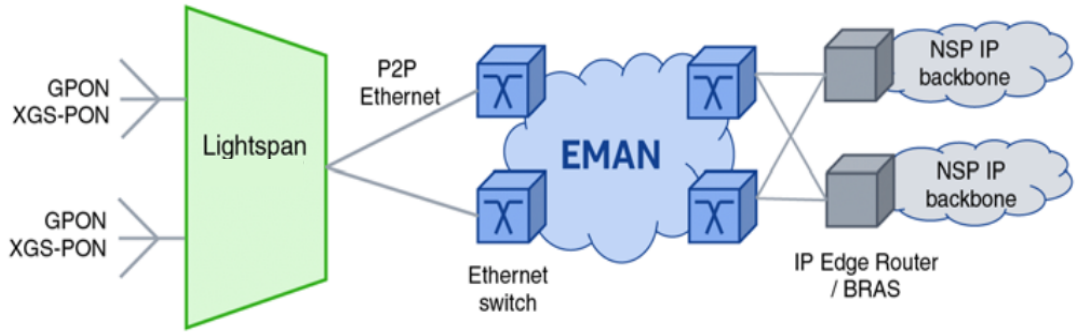
1.4 TOE Overview

The Nokia Lightspan Access Node MF is a network device that serves as the connection point between the end-user's equipment (like home routers or business gateways) and the core network of a telecom provider. The Optical Network Unit (ONU) in conjunction with the Lightspan Fiber Access Node (OLT) form a fiber access network capable of delivering high quality voice, video, and data services to both single-family or multi-dwelling residential subscribers and business subscribers. The TOE software runs on the dedicated Lightspan Access Node MF-2 hardware.

The TOE supports deployment in a Fiber To The Home (FTTH) architecture based on Gigabit Passive Optical Network (GPON) or 10 Gigabit symmetrical and asymmetrical PON (XGS-PON dual rate). The Nokia Lightspan Access Node MF uses a modular hardware architecture based on Line Termination (LT) and Network Termination (NT) cards.

In the FTTH architecture, the Optical Line Termination (OLT) supports Central Office or Cabinet deployment providing GPON or XGS-PON access towards the customer premises and with 1/10/100 Gigabit Ethernet capable links to the aggregation network.

The Lightspan Access Node MF supports the management model (NETCONF/YANG) and other requirements for an OLT defined in Broadband Forum TR-156 and the associated YANG Modules defined in Broadband Forum TR-383 and TR-385. The Lightspan network architecture is shown in Figure 1 Lightspan node deployment model.



The TOE provides the following security functions:

- Security Audit: The TOE provides audit record generation and storage. Audit records can be stored locally or remotely
- Cryptographic Support: All cryptographic operations, including algorithms and key generation used by the TOE are provided by cryptographic module OpenSSL
- Identification and Authentication: The TOE identifies individual administrative users by user name and authenticates them by passwords or public key. Authentication of administrators is enforced at all management interfaces, i.e. NETCONF (SSH or TLS), CLI (SSH). The TOE can be configured to use local authentication and authorization or remote RADIUS server (RFC 2865).
- Security Function Management: The user privileges are applied for every management user access to the database of the TOE. The rules are applied irrespective of the management protocol (CLI, NETCONF) or the underlying security protocol (SSH, TLS). The TOE provides user privileges level access authorization.
- Protection of the TSF: The TOE protects critical security data, including keys and passwords. The TOE enforces trusted updates to the TOE software and reliable timestamps.
- TOE Access: The TOE allows configuration of a disconnection time for idle CLI or NETCONF session connections. The TOE can lock out users when a certain threshold of failed attempt is reached. The TOE displays an administrator-specified advisory notice and consent warning message regarding use of the TOE.
- Trusted Path / Channels: The TOE secures administrative traffic and establishes TLS sessions with external log servers in the operational environment.
- Management access: The TOE provides separation of management traffic from control and data traffic.

1.5 TOE Description

Lightspan Access Node MF can be deployed with numerous interfaces and in different network environments. In a basic deployment, Lightspan Access Node MF is used to provide High-Speed Internet (HSI), Video, and Voice over IP (VoIP) services to subscribers using Gigabit Passive Optical Network (GPON) or 10 Gigabit symmetrical and asymmetrical PON (XGS-PON dual rate).

The PON LT connects via fiber interfaces to the PON and physically terminates into the ONU (Optical Network Units) that provides the user interfaces for all services.

The PON (GPON/XGS-PON) interface is an optical interface that provides the ability to transport data between the Optical Line Termination (OLT) and the Optical Network Unit (ONU). Each PON interface is shared by up to 128 ONUs. Some ONUs are used to connect individual residential or business subscribers - the Single Family Unit (SFU) or Single Business Unit (SBU); others connect more residential or business subscribers - the Multi-Dwelling Unit (MDU) and Multi-Tenant Unit (MTU).

In the architecture of large Lightspan nodes, there are multiple Network Elements (NE) each managed or controlled individually from the access controller. Each LT-card has one NE, and on the Network Termination (NT) cards there may be even more than one NE. Depending on the shelf type, the number of supported LT and NT cards may vary, but the overall management architecture remains the same.

Having multiple NEs in one system is important to assure the scalability of the management and control interface between Lightspan node and access controller.

1.5.1 Architecture Description

The TOE consists of several standalone Network Elements (NE). These NEs are:

- a shelf Network Element (SHELF-NE) providing common equipment, software, alarm and log management.

- an Aggregation Switch (AS) of the IHUB Network Element (AS-NE) providing the switching and routing functionalities.
- multiple (O)LT Network Elements (LT-NE) providing xPON or P2P transport and forwarding functionality.

The figure below shows the high-level functional architecture of the main functional capabilities (from the viewpoint of its forwarding capabilities) and the mapping to the NE implementation of the TOE.

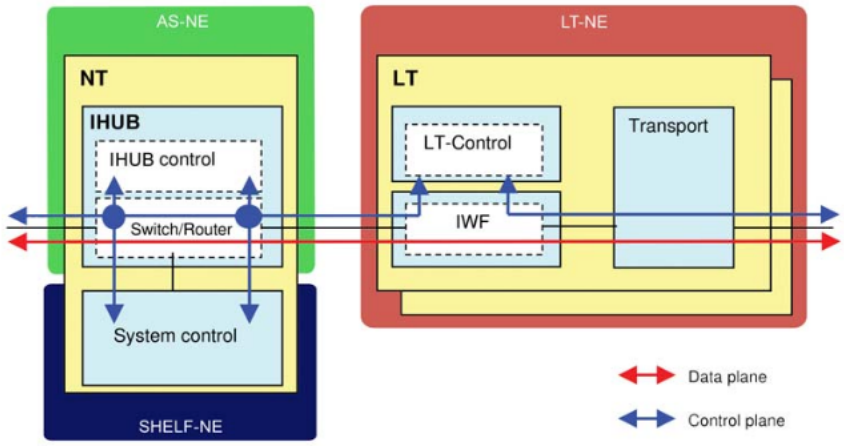


Figure 2 High-level architecture

The NT board consists of an IHUB subsystem and a System Control subsystem.

- The IHUB subsystem consists of a switch/router device and IHUB control software (SW).
- The System Control subsystem implements the management plane of the system (both the NT board and the LT boards) and part of the control plane (subscriber management in particular).

LT boards typically have an InterWorking Function (IWF), a Transport subsystem and an LT-Control subsystem.

- The transport subsystem terminates the physical layer of the subscriber interfaces. It varies with the type of access technology used (Ethernet, PON).
- The IWF processes the packets in the fast path. It is capable of handling frames at L2 and L3, including sophisticated filtering and traffic management, all at the line rate of the transport medium.
- The LT-Control subsystem takes care of the slow path control plane and internal Operations And Maintenance applications.

Every instance of these NEs (LT-NE, AS-NE and SHELF-NE) has its dedicated management connections. Each Network Element (NE) is managed through protocols listed in the figure below. Small nodes are modelled as one NE. Larger nodes, such as Lightspan Access Node MF are modelled as multiple NE.

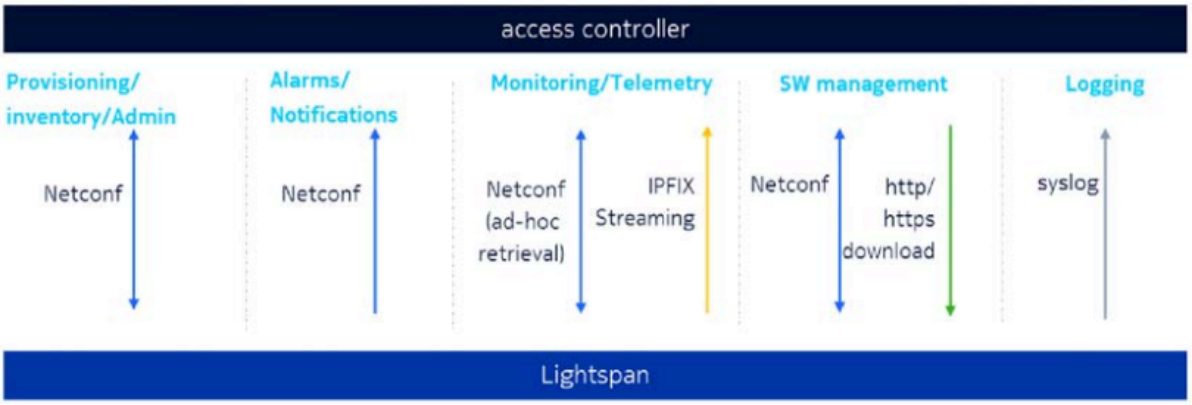


Figure 3 Lightspan Management Protocols

1.5.2 Physical scope

This section list the physical scope of the TOE. The TOE is limited to the software components listed in section 1.5.1. The unique identifier for software components is provided in section 1.2 TOE Identification.

Relevant guidance documents that are part of the TOE are listed in the table below.

Guidance documentation	Identification/Reference
Lightspan Security Hardening guide	3JL-43000-ACAA-RJZZA
Customer Release Note	3TJ-00170-MAAA-FMZZB
Lightspan Access Node MF Release 25.12 System Description	3HH-13800-IAAA-TQZZA 22
Software package guide for 25.12	3HH-14266-AAAA-RJZZA 32
User Safety and Installation Manual for MF-2	3HH-90465-AAAA-RJZZA 21
Customer Documentation Package (package containing all the provided OAM Manuals): • Lightspan MF-2 Reference Configurations • Lightspan MF-2/LMNT-B OAM Manual • Lightspan MF-2/LMNT-B IHUB OAM Manual • Lightspan MF-2/LMNT-B Alarms • Lightspan MF-2/LMNT-B IHUB Alarms • LMNT-B eCLI Command Guide	3HH-92611-FAAA

The following components can be found in the operating environment of the TOE on systems other than those hosting the TOE:

- Audit server
- RADIUS server

- Access Controller

1.5.3 Evaluated configuration

In order to make the TOE securely managed, the operator must make sure that:

- A dedicated management access model is applied.
- The secure variants of the management interfaces are used:
    - NETCONF over SSH or TLS
    - CLI over SSH
    - Syslog over TLS
- The external log server should be the primary means of archiving audit records.
- A secure administrator authentication method is used. Refer to 'authentication' section in the OAM manuals.
- The only CLI that the administrators are using is the embedded YANG eCLI.
- Unused management interfaces are closed.
- All unused network service ports are closed.
- The debug port for troubleshooting is closed.
- The access control lists to limit access to the management IP address are configured.
- The default user accounts are managed.
- The default user passwords are changed.
- The strong encryption algorithms, key exchange algorithms and authentication algorithms are used.
- The 'system lockout' is configured to prevent brute force attacks.
- The 'idle timeout' is configured.
- The device Certificates are managed.
- The software download verification (verifying the authenticity of SW downloaded explicitly) is done during the software upgrade or migration process.

1.5.4 Logical Scope

Security features are provided by the TOE are described in the sections below.

1.5.4.1 Security Audit

The TOE provides log record generation and storage. The TOE supports the usage of a remote syslog collector as a centralized aggregation point for log analysis. Audit records are generated for all security-relevant events.

While the TOE can store audit records locally, in the evaluated configuration an external log server is used as the primary means of archiving audit records.

When the local audit storage exceeds a maximum size, the TOE overwrites the oldest audit records.

By default, the severity (log level) ‘warning’ will be set to applications and syslog output channel. This means that the log records with severity ‘warning’ or higher will be sent as syslog messages to the log collector.

1.5.4.2 Cryptographic Support

All cryptographic operations, including algorithms and key generation used by the TOE are provided by cryptographic module (OpenSSL).

Trusted paths for the TOE administrator are provided by SSH or TLS: NETCONF over SSH, NETCONF over TLS or CLI over SSH. For administrative sessions, the TOE always acts as a server.

Trusted channels between the TOE and external entities, such as a syslog server, are provided by TLS connections.

1.5.4.3 Identification and Authentication

The TOE identifies individual administrative users by user name and authenticates them by passwords or public key. Both authentication methods are allowed by default. The administrator can configure the allowed authentication methods for users of the system. The administrator can create any user and have the user assigned to specific access-groups in line with the intended privilege levels of the created user.

The TOE supports a configurable password policy to define the minimum length of the password, the minimum number of digital numbers, the minimum number of special characters and define if both upper- and lower-case alphabetic characters shall or shall not be present.

Authentication of administrators is enforced at all management interfaces, i.e. NETCONF (SSH or TLS), CLI (SSH).

The TOE can be configured to use local authentication and authorization or remote RADIUS server (RFC 2865). RADIUS is only supported when password-based authentication is used. Public key authentication will be performed only locally. Such users must be created locally.

In case the user is created locally, authentication and authorization is applied based on the configuration of the user profile (RADIUS versus local). By default, local authentication and authorization is performed.

1.5.4.4 Security Function Management

The user privileges are applied for every management user access to the database (configuration and/or state) of the TOE. The rules are applied irrespective of the management protocol (CLI, NETCONF) or the underlying security protocol (SSH, TLS).

The TOE provides user privileges level access authorization, Role Based Access Control (RBAC) based on a simplification of the RFC8341 Network Configuration Access Control Model (NACM). For ease-of-use and simplification, predefined domains (groups) with assigned rules (read-only/read-write/execute) have instantiated on the Lightspan Access Node.

eCLI supports Role Based Access Control (RBAC): eCLI users are assigned to one or more "usergroups" which restrict CLI access to particular domains related to those "usergroups".

The default "admin" user is shared between cli-users and NETCONF users. More users can be created, and in general, cli-users and NETCONF-users should be separated

To control or manage the TOE, the administrator should primarily use the Access Controller, if available in the operating environment of the TOE. NETCONF is one of the major protocols between the Access Controller (Altiplano) and the Lightspan Access Node. NETCONF is supported either over SSH or over TLS. It is used for:

- Configuration, Provisioning, Inventory, Administration
- Notifications and Alarms
- Ad-hoc retrieval of some limited data in context of Monitoring or Telemetry, but not for bulk data collection. For the latter IPFIX streaming is more appropriate.
- Software and database management, in order to instruct software downloads, software activation, database downloads and so on.

Several CLI options are supported, each one optimized and targeted to specific cases in the variety of situations and deployments. In the evaluated configuration, the only CLI that the administrators are using is the embedded YANG eCLI.

Embedded YANG eCLI (YANG eCLI): This CLI provides unlimited access to the management objects in the Lightspan Access Node. It is fully derived from YANG and hence is subjected to changes according to the YANG model changes. This CLI is only to be used in absence of an Access Controller like Altiplano.

Access to this CLI is possible locally via serial CRAFT or LEMI interface on the TOE as well as via a remote SSH connection. After successful identification and authentication, the administrator has access to the TOE, but the administrator's access is limited to the domains being assigned according to RBAC.

1.5.4.5 Protection of the TSF

The TOE is designed to protect critical security data, including keys and passwords. The TOE also provides a mechanism to provide trusted updates to the TOE software and reliable timestamps in order to support TOE functions, including accurate audit recording.

1.5.4.6 TOE Access

The system provides the ability of an administrator user to configure a disconnection time for idle CLI or NETCONF session connections. It is possible to configure the maximum idle time.

A user or IP can be locked out from accessing the TOE when a certain threshold of failed attempt is reached. This threshold is the 'max-retry-attempts' and it can be configured by the administrator. The max-retry-attempts is the cumulative number of failed login attempts that must happen in order to trigger a lockout.

Before establishing an administrative user session, the TSF displays an administrator-specified advisory notice and consent warning message regarding use of the TOE.

1.5.4.7 Trusted Path / Channels

The security functionality provided by the TOE in order to protect the confidentiality and integrity of network connections are described below.

1.5.4.7.1 Administrative traffic

The TOE secures administrative traffic (i.e., administrators connecting to the TOE in order to configure and maintain it) as follows:

- The connection between the TOE and Persistent Management Agent (PMA), a component in Access Controller, is based on TLS. Management traffic is NETCONF over TLS (RFC 7589).
- The TOE can also secure administrative traffic by SSH. SSH can be configured to secure NETCONF and CLI interfaces.

1.5.4.7.2 Communication to other server

The TOE offers the establishment of TLS sessions with external log servers in the operational environment for protection of audit records in transfer. The TOE acts as a TLS client.

1.5.4.8 Management access

The TOE provides separation of management traffic from control and data traffic. The TOE provides a specific management VLAN, which enforces traffic separation.

1.5.5 Delivery method

The Lightship MF-2 appliance is shipped to the customers via common carrier. It contains pre-installed software. However, the customers are instructed to re-install the software from the Nokia SW Distribution Platform (SWDP) (https://customer.nokia.com/support/s/).

All instructions on how to download the TOE are provided in the Installation Manual.

The TOE documentation package(s) can be downloaded (as zip-files) or consulted (as html) on the Nokia On Line Customer Support (OLCS) platform via the Nokia Support Portal at https://customer.nokia.com/support/s/

2 Conformance claims

2.1 Common Criteria Conformance Claims

This ST is CC Part 2 extended and CC Part 3 conformant.

This ST claims conformance to CC:2022, Revision 1, November 2022.

This ST claims conformance to the EAL3 package of security assurance requirements, augmented with ALC_FLR.2, as specified in CC:2022

This ST does not claim conformance to any protection profile.

3 Security Problem Definition

3.1 Threat Environment

This section describes the threat model for the TOE and identifies the individual threats that are assumed to exist in the TOE environment. The assets to be protected by the TOE are as follows.

- Communications with the TOE: for administering the TOE (administration traffic), for sending and receiving authentication information sent to external servers (authentication traffic), and for sending audit records to an external audit server (audit traffic).
- The current version of the TOE and trusted updates to its firmware.
- TSF data stored by the TOE (e.g. user credentials, digital certificates, configuration files).

The threat agents having an interest in manipulating the data model can be categorized as either:

- Unauthorized individuals (“attackers”) which are unknown to the TOE and its runtime environment.

3.2 Threats

T.UNAUTHORIZED_ADMINISTRATOR_ACCESS
Threat agents may attempt to gain Administrator access to the TOE by nefarious means such as masquerading as an Administrator to the device, 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. 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 TOE that does not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols 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 TOE 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 TOE 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 TOE 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 TOE 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.MANAGEMENT_TRAFFIC

Threat agents may attempt to gain access to the administration traffic through the user traffic. This could allow an attacker to perform malicious actions that compromise the security functionality of the TOE and the network on which it resides.

3.3 Organizational security policies

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.

3.4 Assumptions

A.PHYSICAL_PROTECTION

The TOE 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.

A.LIMITED_FUNCTIONALITY

The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).

A.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.

A.NO_THRU_TRAFFIC_PROTECTION

A standard/generic TOE does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the TOE to protect data that originates on or is destined to the device itself, to include administrative data and audit data.

A.TRUSTED_ADMINISTRATOR

The administrator(s) for the TOE 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 TOE is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.

A.REGULAR_UPDATES

The TOE 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 TOE are protected by the platform on which they reside.

A.NTP_SOURCE

The TOE is assumed to have reliable NTP sources available in the operational environment.

A.PLATFORM_ENTROPY

The platform provides seed material of sufficient quality and quantity to initialize and reseed the TOE's deterministic random bit generator.

4 Security objectives

4.1 Security Objectives for the TOE

Security Objective	Description
O.ADMIN_ACCESS	The TOE must ensure that only identified and authenticated users gain access to administrative functions and protected resources.
O.ADMIN_SESSION	The TOE must protect interactive administrator's sessions by allowing the termination of sessions by an administrator, and forcing the termination of a session after a specified period of inactivity .
O.CRYPTOGRAPHY	The TOE must use standardized cryptographic algorithms, which must provide sufficient strength through the use of appropriate key sizes and modes. Key generation algorithms must use a standardized Deterministic Random Bit Generator (DRBG) seeded with an amount of entropy equal or greater of the strength of the cryptographic keys generated.
O.COMMUNICATION_CHANNELS	The TOE must protect critical network traffic from disclosure and modification using standardized secure tunnelling protocols. These protocols must use strong cryptographic algorithms and authentication methods for each endpoint. Critical network traffic includes transfer of TSF data to and from the TOE, administrators performing security management activities, and communication with external IT entities used by the TOE to support the TSF (e.g. an external authentication server).
O.TRUSTED_UPDATES	The TOE must verify the integrity and authenticity of software or firmware updates before being installed through one or more authentication methods using strong cryptographic algorithms.
O.AUDIT	The TOE must record security relevant actions of users on the TOE. The information recorded in these security events must be in sufficient detail to help an administrator of the TOE detect attempted security violations or potential misconfiguration of the TOE security features.
O.TSF_DATA_PROTECTION	The TOE must protect the network device software, firmware, and TSF data (administrator credentials, credentials used for secure channels, etc.) from unauthorized disclosure and modification.
O.ACCESS_BANNER	The TSF must display an initial banner before users log into the TOE. The initial banner must contain restrictions of use, legal agreements, or any other appropriate information to which users make consent by accessing the TOE.
O.MANAGEMENT_TRAFFIC	The TOE must separate administration traffic from the user traffic.

Table 1 Security Objectives for the TOE

4.2 Security Objectives for the Operational Environment

Security Objective	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	Administrators are trusted to follow and apply all guidance documentation in a trusted manner.
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 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.
OE.NTP_SOURCE	The TOE has reliable NTP sources available in the operational environment.
OE.PLATFORM_ENTROPY	The platform provides seed material of sufficient quality and quantity to initialize and reseed the TOE's deterministic random bit generator.

Table 2 Security Objectives for the Operational Environment

4.3 Rationale for the Security Objectives

4.3.1 Coverage

The following table provides a mapping of TOE objectives to threats and policies, showing that each objective counters or enforces at least one threat or policy, respectively.

Objective	Threats / OSPs
O.ADMIN_ACCESS	T.UNAUTHORIZED_ADMINISTRATOR_ACCESS

Objective	Threats / OSPs
O.ADMIN_SESSION	T.UNAUTHORIZED_ADMINISTRATOR_ACCESS
O.CRYPTOGRAPHY	T.WEAK_CRYPTOGRAPHY
O.COMMUNICATION_CHANNELS	T.UNTRUSTED_COMMUNICATION_CHANNELS T.WEAK_AUTHENTICATION_ENDPOINTS
O.TRUSTED_UPDATES	T.UPDATE_COMPROMISE
O.AUDIT	T.UNDETECTED_ACTIVITY
O.TSF_DATA_PROTECTION	T.SECURITY_FUNCTIONALITY_COMPROMISE
O.ACCESS_BANNER	P.ACCESS_BANNER
O.MANAGEMENT_TRAFFIC	T.MANAGEMENT_TRAFFIC

Table 3 Mapping of security objectives to threats and policies

The following table provides a mapping of the objectives for the Operational Environment to assumptions, threats and policies, showing that each objective holds, counters or enforces at least one assumption, threat or policy, respectively .

Objective	Assumptions / Threats / OSPs
OE.PHYSICAL	A.PHYSICAL_PROTECTION
OE.NO_GENERAL_PURPOSE	A.LIMITED_FUNCTIONALITY
OE.NO_THRU_TRAFFIC_PROTECTION	A.NO_THRU_TRAFFIC_PROTECTION
OE.TRUSTED_ADMIN	A.TRUSTED_ADMINISTRATOR
OE.UPDATES	A.REGULAR_UPDATES
OE.ADMIN_CREDENTIALS_SECURE	A.ADMIN_CREDENTIALS_SECURE
OE.RESIDUAL_INFORMATION	A.RESIDUAL_INFORMATION
OE.NTP_SOURCE	A.NTP_SOURCE
OE.PLATFORM_ENTROPY	A.PLATFORM_ENTROPY T.WEAK_CRYPTOGRAPHY

Table 4 Mapping of security objectives for the Operational Environment to assumptions, threats and policies

4.3.2 Sufficiency

The following rationale provides justification that the security objectives are suitable to counter each individual threat and that each security objective tracing back to a threat, when achieved, actually contributes to the removal, diminishing or mitigation of that threat.

Threat	Rationale for security objectives
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	The threat of gaining administrator access to the network device by nefarious means such as masquerading as an administrator to the device, replaying an administrative session, or performing man-in-the-middle attacks is countered by O.ADMIN_ACCESS and O.ADMIN_SESSION.
T.WEAK_CRYPTOGRAPHY	The threat of exploiting weak cryptographic algorithms or performing cryptographic exhaust against the key space, because of poorly chosen encryption algorithms, modes, or key sizes is countered by O.CRYPTOGRAPHY. OE.PLATFORM_ENTROPY ensures the platform provides seed material of sufficient quality and quantity.
T.UNTRUSTED_COMMUNICATION_CHANNELS	The threat of losing confidentiality and integrity of the critical network traffic, and potentially a compromise of the network device itself because of not using standardized secure tunneling protocols is countered by O.COMMUNICATION_CHANNELS.
T.WEAK_AUTHENTICATION_ENDPOINTS	The threat of having critical network traffic exposed because of using protocols that use weak methods to authenticate the endpoints is countered by O.COMMUNICATION_CHANNELS.
T.UPDATE_COMPROMISE	The threat of using a compromised update of the software or firmware tampered by an attacker is countered by O.TRUSTED_UPDATES.
T.UNDETECTED_ACTIVITY	The threat of access, change, and/or modify the security functionality of the network device without administrator awareness is countered by O.AUDIT.
T.SECURITY_FUNCTIONALITY_COMPROMISE	The threat of compromising credentials and device data enabling continued access to the network device and its critical data is countered by O.TSF_DATA_PROTECTION.
T.MANAGEMENT_TRAFFIC	The threat of gaining access to the management traffic is countered by O.MANAGEMENT_TRAFFIC.

Table 5 Sufficiency of objectives countering threats

The following rationale provides justification that the security objectives for the environment are suitable to cover each individual assumption, that each security objective for the environment that traces back to an assumption about the environment of use of the TOE, when achieved, actually contributes to the environment achieving consistency with the assumption, and that if all security objectives for the environment that trace back to an assumption are achieved, the intended usage is supported.

Assumption	Rationale for security objectives
A.PHYSICAL_PROTECTION	The assumption: The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/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. is upheld by: OE.PHYSICAL: Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
A.LIMITED_FUNCTIONALITY	The assumption: The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example the device should not provide computing platform for general purpose applications (unrelated to networking functionality). is upheld by: 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.
A.RESIDUAL_INFORMATION	The assumption: 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. is upheld by: OE.RESIDUAL_INFORMATION: The 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.
A.NO_THRU_TRAFFIC_PROTECTION	The assumption: A standard/generic TOE does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the TOE 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 TOE, destined for another network entity, is not covered by the ND cPP. It is assumed

Assumption	Rationale for security objectives
	that this protection will be covered by cPPs and PP-Modules for particular types of TOE (e.g., firewall). is upheld by: 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.
A.TRUSTED_ADMINISTRATOR	The assumption: The Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device. is upheld by: OE.TRUSTED_ADMIN: TOE Administrators are trusted to follow and apply all guidance documentation in a trusted manner.
A.REGULAR_UPDATES	The assumption: The TOE 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. is upheld by: 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.
A.ADMIN_CREDENTIALS_SECURE	The assumption: The Administrator's credentials (private key) used to access the network device are protected by the platform on which they reside. is upheld by: 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.
A.NTP_SOURCE	The assumption: The TOE is assumed to have reliable NTP sources available in the operational environment.

Assumption	Rationale for security objectives
	Is upheld by: OE.NTP_SOURCE: the operational environment provides the TOE with reliable NTP sources.
A.PLATFORM_ENTROPY	The assumption: The platform provides seed material of sufficient quality and quantity to initialize and reseed the TOE's deterministic random bit generator. Is upheld by: OE.PLATFORM_ENTROPY: the platform provides seed material of sufficient quality and quantity.

Table 6 Sufficiency of objectives holding assumptions

The following rationale provides justification that the security objectives are suitable to cover each individual organizational security policy (OSP), that each security objective that traces back to an OSP, when achieved, actually contributes to the implementation of the OSP, and that if all security objectives that trace back to an OSP are achieved, the OSP is implemented.

OSP	Rationale for security objectives
P.ACCESS_BANNER	The organizational security policy that requires an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE is enforced by O.ACCESS_BANNER.

Table 7 Sufficiency of objectives enforcing Organizational Security Policies

5 Extended components definition

This Security Target defines its own extended components based on the extended components defined in the collaborative Protection Profile for Network Devices, version 3.0e ([NDcPPv3.0e]):

- FCS_TLSC_EXT.1 TLS Client Protocol
- FCS_TLSC_EXT.2 TLS Client Support for Mutual Authentication
- FCS_TLSS_EXT.1 Extended: TLS Server Protocol
- FCS_TLSS_EXT.2 TLS Server Support for Mutual Authentication

It also uses the following extended components defined in the collaborative Protection Profile for Network Devices, version 3.0e ([NDcPPv3.0e]):

- FAU_STG_EXT.1 Extended: Protected Audit Event Storage
- FCS_NTP_EXT.1 Extended: Protocol
- FIA_PMG_EXT.1 Extended: Password Management
- FIA_UIA_EXT.1 Extended: User Identification and Authentication
- FPT_SKP_EXT.1 Extended: Protection of TSF Data (for reading of all symmetric keys)
- FPT_APW_EXT.1 Protection of Administrator Passwords
- FPT_STM_EXT.1 Extended: Reliable Time Stamps
- FPT_TUD_EXT.1 Extended: Trusted Update
- FTA_SSL_EXT.1 Extended: TSF-initiated Session Locking

This Security Target also uses the following extended component defined in the Functional Package for Secure Shell, version 2.0 ([PKG_SSHv2.0]):

- FCS_SSH_EXT.1 Extended: SSH Protocol

For completeness of the ST, the extended components definitions are repeated below.

5.1 Security Audit (FAU)

5.1.1 Protected Audit Event Storage (FAU_STG_EXT)

Family Behaviour

This component defines the requirements for the TSF to be able to securely transmit audit data between the TOE and an external IT entity. This is a new family defined for the FAU class.

Component Levelling



FAU_STG_EXT.1 Protected audit event storage requires the TSF to use a trusted channel implementing a secure protocol.

Management: FAU_STG_EXT.1

The following actions could be considered for the management functions in FMT:

- The TSF shall have the ability to configure the cryptographic functionality.

Audit: FAU_STG_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. There are no auditable events foreseen.

FAU_STG_EXT.1 Protected Audit Event Storage

Hierarchical to: No other components

Dependencies:

- FAU_GEN.1 Audit data generation
- FTP_ITC.1 Inter-TSF Trusted Channel

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 [selection:

- The TOE shall consist of a single standalone component that stores audit data locally,
- The TOE shall be a distributed TOE that stores audit data on the following TOE components: [assignment: identification of TOE components],
- The TOE shall be a distributed TOE with storage of audit data provided externally for the following TOE components: [assignment: list of TOE components that do not store audit data locally and the other TOE components to which they transmit their generated audit data].

FAU_STG_EXT.1.3 The TSF shall maintain a [selection: log file, database, buffer, [assignment: other local logging method]] 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 [selection: persistent, non- persistent] audit records locally with a minimum storage size of [assignment: number of records and/or file/buffer size(s)].

FAU_STG_EXT.1.5 The TSF shall [selection: drop new audit data, overwrite previous audit records according to the following rule: [assignment: rule for overwriting previous audit records], [assignment: other action]] 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 [selection: none, manual export, ability to view locally].

5.2 Cryptographic Support (FCS)

5.2.1 NTP Protocol (FCS_NTP_EXT)

Family Behaviour

The component in this family addresses the ability for a TOE to protect NTP time synchronization traffic. This is a new family defined for the FCS class.

Component Levelling



FCS_NTP_EXT.1 NTP Protocol requires NTP to be implemented as specified

Management: FCS_NTP_EXT.1

The following actions could be considered for the management functions in FMT:

a. Ability to configure NTP

Audit: FCS_NTP_EXT.1

The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:

a. There are no auditable events foreseen.

FCS_NTP_EXT.1 NTP Protocol

Hierarchical to: No other components

Dependencies:

- FCS_COP.1 Cryptographic operation
- [FCS_DTLSC_EXT.1 DTLSC Client Protocol or FCS_IPSEC_EXT.1 IPsec]

FCS_NTP_EXT.1.1 The TSF shall use only the following NTP version(s) [selection: NTP v3 (RFC 1305), NTP v4 (RFC 5905)].

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

- Authentication using [selection: SHA1, SHA256, SHA384, SHA512, AES-CBC-128, AES-CBC-256] as the message digest algorithm(s);
- [selection: IPsec, DTLS] to provide trusted communication between itself and an NTP time source.

].

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.

5.2.2 TLS Client Protocol (FCS_TLSC_EXT)

Family Behaviour

The component in this family addresses the ability for a client to use TLS to protect data between the client and a server using the TLS protocol. This is a new family defined for the FCS class.

Component Levelling



FCS_TLSC_EXT.1 TLS Client Protocol requires that the client side of TLS be implemented as specified.

FCS_TLSC_EXT.2 TLS Client Support for Mutual Authentication requires that the client side of the TLS implementation include mutual authentication.

Management: FCS_TLSC_EXT.1, FCS_TLSC_EXT.2

The following actions could be considered for the management functions in FMT:

a. There are no management activities foreseen.

Audit: FCS_TLSC_EXT.1, FCS_TLSC_EXT.2

The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:

a. Failure of TLS session establishment

b. TLS session establishment

c. TLS session termination

FCS_TLSC_EXT.1 TLS Client Protocol

Hierarchical to: No other components

Dependencies:

- FCS_CKM.1 Cryptographic Key Generation
- FCS_CKM.2 Cryptographic Key Establishment
- 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_TLSC_EXT.1.1 The TSF shall implement [selection: TLS 1.3 (RFC 8446), TLS 1.2 (RFC 5246)] supporting the following ciphersuites:

[selection:

- Select supported ciphersuites for TLS 1.2 from:
  - TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
  - TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 8422
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 8422
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 8422
  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 8422
  - TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
  - TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
  - TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
  - TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
  - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289

- Select supported ciphersuites for TLS 1.3 from:
  - TLS_AES_128_GCM_SHA256
  - TLS_AES_256_GCM_SHA384
  - TLS_AES_128_CCM_SHA256
  - TLS_AES_128_CCM_8_SHA256

] and no other ciphersuites.

FCS_TLSC_EXT.1.2 The TSF shall verify that the presented identifier matches [selection: the reference identifier per RFC 6125 Section 6, IPv4 address in the CN or in the SAN, IPv6 address in the CN or in the SAN, IPv4 address in the SAN, IPv6 address in the SAN, the identifier per RFC 5280 Appendix A using [selection: id-at-commonName, id-at-countryName, id-at-dnQualifier, id-at-generationQualifier, id-at-givenName, id-at-initials, id-at-localityName, id-at-name, id-at-organizationalUnitName, id-at-organizationName, id-at-pseudonym, id-at-serialNumber, id-at-stateOrProvinceName, id-at-surname, id-at-title] and no other attribute types].

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

- without any administrator override mechanism
- except with the following administrator override: If the TSF fails to determine the revocation status the TSF shall allow the administrator to provide override authorization to establish the connection on a per certificate basis.

].

FCS_TLSC_EXT.1.4 The TSF shall [selection: not present the Supported Groups Extension, present the Supported Groups Extension with the following curves/groups: [selection: secp256r1, secp384r1, secp521r1, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192] and no other curves/groups] in the Client Hello.

FCS_TLSC_EXT.1.5 The TSF shall [selection:

- present the signature_algorithms extension with support for the following algorithms:

[selection:

- rsa_pkcs1 with sha256(0x0401),
- rsa_pkcs1with sha384(0x0501),
- rsa_pkcs1 with sha512(0x0601),
- ecdsa_secp256r1 with sha256(0x0403),
- ecdsa_secp384r1 with sha384(0x0503),
- ecdsa_secp521r1 with sha512(0x0603),
- rsa_pss_rsae with sha256(0x0804),
- rsa_pss_rsae with sha384(0x0805),
- rsa_pss_rsae with sha512(0x0806),

- rsa_pss_pss with sha256(0x0809),
- rsa_pss_pss with sha384(0x080a),
- rsa_pss_pss with sha512(0x080b)
-] and no other algorithms;

- present the signature_algorithms_cert extension with the following Signature Schemes:

[selection:

- rsa_pkcs1 with sha256(0x0401),
- rsa_pkcs1with sha384(0x0501),
- rsa_pkcs1 with sha512(0x0601),
- ecdsa_secp256r1 with sha256(0x0403),
- ecdsa_secp384r1 with sha384(0x0503),
- ecdsa_secp521r1 with sha512(0x0603),
- rsa_pss_rsae with sha256(0x0804),
- rsa_pss_rsae with sha384(0x0805),
- rsa_pss_rsae with sha512(0x0806),
- rsa_pss_pss with sha256(0x0809),
- rsa_pss_pss with sha384(0x080a),
- rsa_pss_pss with sha512(0x080b)
-] and no other SignatureSchemes

].

FCS_TLSC_EXT.1.6 The TSF [selection: provides, does not provide] the ability to configure the list of supported ciphersuites as defined in FCS_TLSC_EXT.1.1.

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

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

FCS_TLSC_EXT.1.8 The TSF shall [selection: not use PSKs, only use PSKs in TLS 1.3 session resumption with forward secrecy].

FCS_TLSC_EXT.1.9 The TSF shall [selection: support TLS 1.2 secure renegotiation through use of the "renegotiation_info" TLS extension in accordance with RFC 5746, reject [selection: TLS 1.2, TLS 1.3] renegotiation attempts].

FCS_TLSC_EXT.2 TLS Client Support for Mutual Authentication

Hierarchical to: No other components

Dependencies:

- FCS_CKM.1Cryptographic Key Generation
- FCS_CKM.2 Cryptographic Key Establishment
- 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_TLSC_EXT.1 TLS Client Protocol without mutual authentication

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

5.2.3 TLS Server Protocol (FCS_TLSS_EXT)

Family Behaviour

The component in this family addresses the ability for a server to use TLS to protect data between a client and the server using the TLS protocol. This is a new family defined for the FCS class.

Component Levelling



FCS_TLSS_EXT.1 TLS Server Protocol requires that the server side of TLS be implemented as specified.

FCS_TLSS_EXT.2: TLS Server Support for Mutual Authentication requires the mutual authentication be included in the TLS implementation.

Management: FCS_TLSS_EXT.1, FCS_TLSS_EXT.2

The following actions could be considered for the management functions in FMT:

a. There are no management activities foreseen.

Audit: FCS_TLSS_EXT.1, FCS_TLSS_EXT.2

The following actions should be considered for audit if FAU_GEN Security audit

data generation is included in the PP/ST:

a. Failure of TLS session establishment
b. TLS session establishment
c. TLS session termination

FCS_TLSS_EXT.1 TLS Server Protocol

Hierarchical to: No other components

Dependencies:

- FCS_CKM.1 Cryptographic Key Generation
- FCS_CKM.2 Cryptographic Key Establishment
- 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_TLSS_EXT.1.1 The TSF shall implement [selection: TLS 1.3 (RFC 8446), TLS 1.2 (RFC 5246)] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites: [selection:

- Select supported ciphersuites for TLS 1.2 from:
    - TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
    - TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
    - TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
    - TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
    - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 8422
    - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 8422
    - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 8422
    - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 8422
    - TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
    - TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
    - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
    - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
    - TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
    - TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
    - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
    - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
    - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
    - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
    - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
    - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
    - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
    - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
    - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
    - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- Select supported ciphersuites for TLS 1.3 from:
    - TLS_AES_128_GCM_SHA256
    - TLS_AES_256_GCM_SHA384
    - TLS_AES_128_CCM_SHA256
    - TLS_AES_128_CCM_8_SHA256

] and no other ciphersuites.

FCS_TLSS_EXT.1.2 The TSF shall authenticate itself using X.509 certificate(s) using [selection: RSA with key size [selection: 2048, 3072, 4096] bits; ECDSA over NIST curves [selection: secp256r1, secp384r1, secp521r1] and no other curves].

FCS_TLSS_EXT.1.3 The TSF shall perform key exchange using: [selection:

- RSA key establishment with key size [selection: 2048, 3072, 4096] bits;
- EC Diffie-Hellman key agreement over NIST curves [selection: secp256r1, secp384r1, secp521r1] and no other curves;
- Diffie-Hellman parameters [selection: of size 2048 bits, of size 3072 bits, of size 4096 bits, of size 6144 bits, of size 8192 bits, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192]

].

FCS_TLSS_EXT.1.4 The TSF shall support [selection: no session resumption, session resumption based on session IDs according to RFC 5246 (TLS 1.2), session resumption based on session tickets according to RFC 5077 (TLS 1.2), session resumption according to RFC 8446 (TLS 1.3)].

FCS_TLSS_EXT.1.5 The TSF [selection: provides, does not provide] the ability to configure the list of supported ciphersuites as defined in FCS_TLSS_EXT.1.1.

FCS_TLSS_EXT.1.6 The TSF shall prohibit the use of the following extensions:

Early data extension

FCS_TLSS_EXT.1.7 The TSF shall [selection: not use PSKs, only use PSKs in TLS 1.3 session resumption with forward secrecy].

FCS_TLSS_EXT.1.8 The TSF shall [selection: support secure renegotiation in accordance with RFC 5746 by always including the “renegotiation_info” TLS extension in TLS 1.2 ServerHello messages, reject [selection: TLS 1.2, TLS 1.3] renegotiation attempts].

FCS_TLSS_EXT.2 TLS Server Support for Mutual Authentication

Hierarchical to: No other components

Dependencies:

- FCS_CKM.1 Cryptographic Key Generation
- FCS_CKM.2 Cryptographic Key Establishment
- 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_TLSS_EXT.1 TLS Server Protocol without mutual authentication

FCS_TLSS_EXT.2.1 The TSF shall support TLS communication with mutual authentication of TLS clients using X.509v3 certificates and shall [selection:

- reject the connection if the client either does not provide a client certificate at all or the client certificate cannot be successfully validated by the TOE (except for override mechanisms that might be defined in FCS_TLSS_EXT.2.2) ('hard fail')
- accept the connection even if the client does not provide a client certificate at all, as long as a fall-back authentication is performed using one of the other authentication mechanisms defined in this cPP before any other TSF-mediated action is performed via this channel ('soft fail')

].

FCS_TLSS_EXT.2.2 When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the client certificate is invalid. The TSF shall also [selection:

- not implement any administrator override mechanism

- require administrator authorization to establish the connection if the TSF fails to determine the revocation status of the presented client certificate

].

FCS_TLSS_EXT.2.3 The TSF shall not establish a trusted channel if the identifier contained in a certificate does not match an expected identifier for the client. If the identifier is a Fully Qualified Domain Name (FQDN), then the TSF shall match the identifiers according to RFC 6125, otherwise the TSF shall parse the identifier from the certificate and match the identifier against the expected identifier of the client as described in the TSS.

FCS_TLSS_EXT.2.4 The TSF shall present a [selection: TLS 1.2, TLS 1.3] Certificate Request message containing the following algorithms: [selection:

- rsa_pkcs1 with sha256(0x0401),
- rsa_pkcs1 with sha384(0x0501),
- rsa_pkcs1 with sha512(0x0601),
- ecdsa_secp256r1 with sha256(0x0403),
- ecdsa_secp384r1 with sha384(0x0503),
- ecdsa_secp521r1 with sha512(0x0603),
- rsa_pss_rsae with sha256(0x0804),
- rsa_pss_rsae with sha384(0x0805),
- rsa_pss_rsae with sha512(0x0806),
- rsa_pss_pss with sha256(0x0809),
- rsa_pss_pss with sha384(0x080a),
- rsa_pss_pss with sha512(0x080b)

] and no other algorithms.

5.2.4 SSH Protocol (FCS_SSH_EXT)

Family Behavior

This family defines requirements for implementation of the SSH protocol that goes beyond the level of detail specified for trusted communications in CC Part 2.

Component Leveling



FCS_SSH_EXT.1, SSH Protocol, requires the TSF to specify the details of its SSH protocol implementation.

Management: FCS_SSH_EXT.1

No specific management functions are identified.

Audit: FCS_SSH_EXT.1

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP, PP-Module, FP, or ST:

- Failure to establish SSH connection
- Establishment of SSH connection

- Termination of SSH connection
- Dropping of packets outside defined size limits

FCS_SSH_EXT.1 SSH Protocol

Hierarchical to: No other components.

Dependencies to:

- FCS_CKM.1 Cryptographic Key Generation
- FCS_CKM.2 Cryptographic Key Derivation
- FCS_COP.1 Cryptographic Operation
- FCS_RBG.1 Random Bit Generation

FCS_SSH_EXT.1.1 The TOE shall implement SSH acting as a [selection: client, server] that complies with RFCs 4251, 4252, 4253, 4254, [selection: 4256, 4344, 5647, 5656, 6187, 6668, 8268, 8308, 8332, no other RFCs] and [no other standard].

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

- password, complying with [selection: RFC 4252, RFC 4256 keyboard-interactive methods]
- "publickey" (RFC 4252): [selection:
    - rsa-sha2-512 (RFC 8332)
    - ecdsa-sha2-nistp384 (RFC 5656)
    - ecdsa-sha2-nistp521 (RFC 5656)
    - x509v3-ecdsa-sha2-nistp384 (RFC 6187)
    - x509v3-ecdsa-sha2-nistp521 (RFC 6187)

]

] and no other methods.

FCS_SSH_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [assignment: number of bytes between 35 KB and 1 GB (inclusive)] in an SSH transport connection are dropped.

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

- AEAD_AES_256_GCM (RFC 5647)
- aes256-gcm@openssh.com (RFC 5647)

] and no other mechanisms.

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

- AEAD_AES_256_GCM (RFC 5647)
- implicit

] and no other mechanisms.

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

- diffie-hellman-group15-sha512 (RFC 8268)
- diffie-hellman-group16-sha512 (RFC 8268)

- diffie-hellman-group17-sha512 (RFC 8268)
- diffie-hellman-group18-sha512 (RFC 8268)
- ecdh-sha2-nistp384 (RFC 5656)
- ecdh-sha2-nistp521 (RFC 5656)

] and no other mechanisms.

FCS_SSH_EXT.1.7 The TSF shall use an SSH key derivation function (KDF) as defined in [selection:

- 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 [selection:

- a rekey of the session keys
- connection termination

] occurs when any of the following thresholds are met:

- [assignment: length of time lesser than or equal to one hour] connection time
- no more than [assignment: number of bytes less than or equal to one gigabyte] of transmitted data, or
- no more than [assignment: number of bytes less than or equal to one gigabyte] of received data.

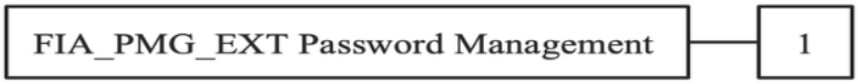
5.3 Identification and Authentication (FIA)

5.3.1 Password Management (FIA_PMG_EXT)

Family Behaviour

The TOE defines the attributes of passwords used by administrative users to ensure that strong passwords and passphrases can be chosen and maintained. This is a new family defined for the FIA class.

Component Levelling



FIA_PMG_EXT.1 Password management requires the TSF to support passwords with varying composition requirements, minimum lengths, maximum lifetime, and similarity constraints.

Management: FIA_PMG_EXT.1

There are no management functions foreseen.

Audit: FIA_PMG_EXT.1

There are no auditable events foreseen.

FIA_PMG_EXT.1 Password Management

Hierarchical to: No other components

Dependencies: No other components

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: [selection: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", [assignment: other characters]];

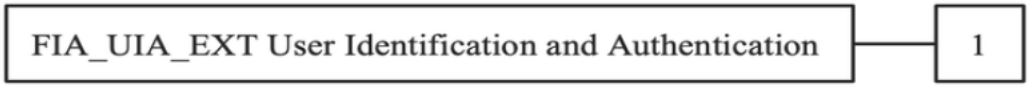
b. Minimum password length shall be configurable to between [assignment: minimum number of characters supported by the TOE] and [assignment: number of characters greater than or equal to 15] characters.

5.3.2 User Identification and Authentication (FIA_UIA_EXT)

Family Behaviour

The TSF allows certain specified actions before the non-TOE entity goes through the identification and authentication process. This is a new family defined for the FIA class.

Component Levelling



FIA_UIA_EXT.1 User Identification and Authentication requires Administrators (including remote Administrators) to be identified and authenticated by the TOE, providing assurance for that end of the communication path. It also ensures that every user is identified and authenticated before the TOE performs any mediated functions.

Management: FIA_UIA_EXT.1

The following actions could be considered for the management functions in FMT:

a. Ability to configure the list of TOE services available before an entity is identified and authenticated

Audit: FIA_UIA_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. All use of the identification and authentication mechanism

b. Provided user identity, origin of the attempt (e.g. IP address)

FIA_UIA_EXT.1 User Identification and Authentication

Hierarchical to: No other components

Dependencies: FTA_TAB.1 Default TOE Access Banners

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;
- [selection: no other actions, automated generation of cryptographic keys, [assignment: list of services, actions performed by the TSF in response to non-TOE requests]].

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 [selection: Web GUI password, SSH password, SSH public key, X.509 certificate, [assignment: other authentication mechanism]] and local authentication mechanisms [selection: none, password-based, [assignment: other authentication mechanism]].

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

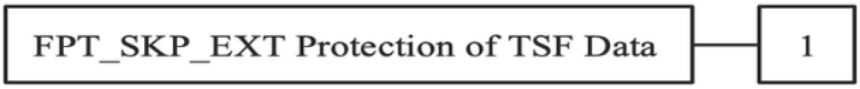
5.4 Protection of the TSF (FPT)

5.4.1 Protection of TSF Data (FPT_SKP_EXT)

Family Behaviour

Components in this family address the requirements for managing and protecting TSF data, such as cryptographic keys. This is a new family modelled after the FPT class.

Component Levelling



Protection of TSF Data (for reading all symmetric keys), requires preventing symmetric keys from being read by any user or subject. It is the only component of this family.

Management: FPT_SKP_EXT.1

The following actions could be considered for the management functions in FMT:

a. There are no management activities foreseen.

Audit: FPT_SKP_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. There are no auditable events foreseen.

FPT_SKP_EXT.1 Protection of TSF Data (for reading of all symmetric keys)

Hierarchical to: No other components

Dependencies: No other components

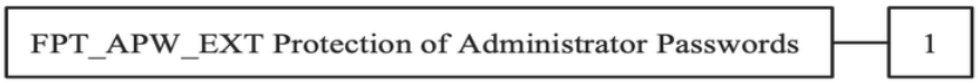
FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

5.4.2 Protection of Administrator Passwords (FPT_APW_EXT)

Family Behaviour

Components in this family ensure that the TSF will protect plaintext credential data such as passwords from unauthorized disclosure. This is a new family defined for the FPT class.

Component Levelling



FPT_APW_EXT.1 Protection of Administrator passwords requires that the TSF prevent plaintext credential data from being read by any user or subject.

Management: FPT_APW_EXT.1

The following actions could be considered for the management functions in FMT:

a. There are no management functions foreseen.

Audit: FPT_APW_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. There are no auditable events foreseen.

FPT_APW_EXT.1 Protection of Administrator Passwords

Hierarchical to: No other components

Dependencies: No other components

FPT_APW_EXT.1.1 The TSF shall store administrative passwords in non-plaintext form.

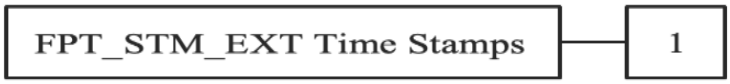
FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext administrative passwords.

5.4.3 Time stamps (FPT_STM_EXT)

Family Behaviour

Components in this family extend FPT_STM requirements by describing the source of time used in timestamps. This is a new family defined for the FPT class.

Component Levelling



FPT_STM_EXT.1 Reliable Time Stamps is hierarchic to FPT_STM.1: it requires that the TSF provide reliable time stamps for TSF and identifies the source of the time used in those timestamps.

Management: FPT_STM_EXT.1

The following actions could be considered for the management functions in FMT:

a. Management of the time

b. Administrator setting of the time

Audit: FPT_STM_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. Discontinuous changes to the time

FPT_STM_EXT.1 Reliable Time Stamps

Hierarchical to: No other components

Dependencies: No other components

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 [selection: allow the Administrator to set the time, synchronise time with an NTP server, obtain time from the underlying virtualization system].

5.4.4 Trusted Update (FPT_TUD_EXT)

Family Behaviour

Components in this family address the requirements for updating the TOE firmware and/or software. This is a new family defined for the FPT class.

Component Levelling



FPT_TUD_EXT.1 Trusted Update requires management tools be provided to update the TOE firmware and software, including the ability to verify the updates prior to installation.

Management: FPT_TUD_EXT.1,

The following actions could be considered for the management functions in FMT:

a. Ability to update the TOE and to verify the updates

b. Ability to update the TOE and to verify the updates using the digital signature capability (FCS_COP.1/SigGen) and [selection: no other functions, [assignment: other cryptographic functions (or other functions) used to support the update capability]]

c. Ability to update the TOE, and to verify the updates using [selection: digital signature, no other mechanism] capability prior to installing those updates

Audit: FPT_TUD_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. Initiation of the update process

b. Any failure to verify the integrity of the update

FPT_TUD_EXT.1 Trusted Update

Hierarchical to: No other components

Dependencies: FCS_COP.1/SigGen Cryptographic operation (for Cryptographic Signature and Verification), or FCS_COP.1/Hash Cryptographic operation (for cryptographic hashing)

FPT_TUD_EXT.1.1 The TSF shall provide Administrators the ability to query the currently executing version of the TOE firmware/software and [selection: the most recently installed version of the TOE firmware/software; no other TOE firmware/software version].

FPT_TUD_EXT.1.2 The TSF shall provide Administrators the ability to manually initiate updates to TOE firmware/software and [selection: support automatic checking for updates, support automatic updates, no other update mechanism].

FPT_TUD_EXT.1.3 The TSF shall provide means to authenticate firmware/software updates to the TOE using a [selection: X.509 certificate, digital signature] prior to installing those updates.

5.5 TOE Access (FTA)

5.5.1 TSF-initiated Session Locking (FTA_SSL_EXT)

Family Behaviour

Components in this family address the requirements for TSF-initiated and user-initiated locking, unlocking, and termination of interactive sessions. The extended FTA_SSL_EXT family is based on the FTA_SSL family.

Component Levelling



FTA_SSL_EXT.1 TSF-initiated session locking, requires system initiated locking of an interactive session after a specified period of inactivity. It is the only component of this family.

Management: FTA_SSL_EXT.1

The following actions could be considered for the management functions in FMT:

a. Specification of the time of user inactivity after which lock-out occurs for an individual user.

Audit: FTA_SSL_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. Any attempts at unlocking an interactive session.

FTA_SSL_EXT.1 TSF-initiated Session Locking

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [selection:

- lock the session - disable any activity of the Administrator's data access/display devices other than unlocking the session, and requiring that the Administrator re-authenticate to the TSF prior to unlocking the session;
- terminate the session]

after a Administrator-specified time period of inactivity.

6 Security requirements for the TOE

This section descriptions the security functional and assurance requirements for the TOE. The notation, formatting, and conventions used are defined below.

Application notes have been added by the ST authors to provide the reader with additional understanding or to clarify the ST author's intent; they are italicized and usually appear immediately preceding or following the element needing clarification.

CC component operations are identified in the following way:

- Assignments and selections are typeset in **bold text.**
- Refinements are identified by **bold underlined** text for any additions.
- Deletions are incorporated directly into the text and are not specifically marked in the ST.

6.1 Security functional requirements for the TOE

This section describes the security functional requirements for the TOE.

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 Audit Data Generation

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

a) Start-up and shutdown of the audit functions;

b) All auditable events for the **not specified** level of audit; and

c) All 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 8.**

FAU_GEN.1.2 The TSF shall record within the audit data 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 ST**, information specified in column three of Table 8**.

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.

Requirement	Auditable Events	Additional Audit Record Contents
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.6	None.	None.
FCS_COP.1/SSH DataEncryption	None.	None.
FCS_COP.1/TLS DataEncryption	None.	None.
FCS_COP.1/SigGen	None.	None.
FCS_COP.1/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.
FCS_NTP_EXT.1	Configuration of a new time server Removal of configured time server	Identity if new/removed time server
FCS_RBG.1	None.	None.
FCS_RBG.2	None.	None.
FCS_SSH_EXT.1/AS-NE	Failure to establish SSH connection	Reason for failure
FCS_SSH_EXT.1/Shelf-NE/LT-NE	Failure to establish SSH connection	Reason for failure
FCS_TLSC_EXT.1	Failure to establish a TLS Session	Reason for failure
FCS_TLSC_EXT.2	None.	None.
FCS_TLSS_EXT.1	Failure to establish a TLS Session	Reason for failure
FCS_TLSS_EXT.2	Failure to authenticate the client	Reason for failure
FDP_IFC.1	None.	None.
FDP_IFF.1	None.	None.
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded	Origin of the attempt (e.g., IP address)

Requirement	Auditable Events	Additional Audit Record Contents
FIA_PMG_EXT.1/Shelf-NE/LT-NE	None.	None.
FIA_PMG_EXT.1/AS-NE	None.	None.
FIA_UAU.7	None.	None.
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FMT_MSA.1	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.
FMT_SMR.2	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_STM_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	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.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTA_SSL_EXT.1	Any attempts at unlocking of an interactive session.	None.
FTA_TAB.1	None.	None.

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

Table 8 Security Functional Requirements and Auditable Events

6.1.1.2 FAU_GEN.2 User identity association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.1.3 FAU_STG_EXT.1 Protected Audit Event Storage

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

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

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

FAU_STG_EXT.1.3 The TSF shall maintain a **log file** of audit records in the event that an interruption of communication with the remote audit server occurs.

FAU_STG_EXT.1.4 The TSF shall be able to store **persistent** audit records locally with a minimum storage size of **10MBs**.

FAU_STG_EXT.1.5 The TSF shall **overwrite previous audit records according to the following rule: the oldest log file is deleted** 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 **manual export, ability to view locally**.

Application note: The maximum allowed size of log file storage is 10 MBs.

6.1.2 Cryptographic Support (FCS)

6.1.2.1 FCS_CKM.1 Cryptographic Key Generation

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

- **RSA schemes using cryptographic key sizes of 2048 bits or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3;**
- **ECC schemes using 'NIST curves' P-256, P-384, P-521 that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4.**

6.1.2.2 FCS_CKM.2 Cryptographic Key Establishment

FCS_CKM.2.1 The TSF shall **perform** cryptographic key **establishment** in accordance with a specified cryptographic key **establishment** method:

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

6.1.2.3 FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_CKM.6.1 The TSF shall destroy **private keys** when **no longer needed**.

FCS_CKM.6.2 The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method

- **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.**

Application note: Private keys used for SSH and TLS connections.

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

FCS_COP.1.1/SSH 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, 192 bits, 256 bits** that meet the following: **AES as specified in ISO 18033-3, CTR as specified in ISO 10116.**

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

FCS_COP.1.1/TLS DataEncryption The TSF shall perform **encryption/decryption** in accordance with a specified cryptographic algorithm **AES used in GCM mode, cryptographic algorithm ChaCha20—Poly1305** and cryptographic key sizes **128 bits**, **256 bits** that meet the following: **AES as specified in ISO 18033-3, ChaCha20—Poly1305 as specified in RFC 7539**, **GCM as specified in ISO 19772**.

6.1.2.6 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.**

Application note: This SFR is for SSH and TLS.

6.1.2.7 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 **message digest** sizes **256, 384, 512 bits** that meet the following: **ISO/IEC 10118-3:2004**.

Application note: This SFR is for SSH and TLS.

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

FCS_COP.1.1/KeyedHash The TSF The TSF shall perform **keyed-hash message authentication** in accordance with a specified cryptographic algorithm **HMAC-SHA-256, HMAC-SHA-384** and cryptographic key sizes **256, 384 and message digest sizes 256, 384 bits** that meet the following: **ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"**.

Application note: This SFR is for SSH and TLS.

6.1.2.9 FCS_NTP_EXT.1 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 AES-128-CMAC 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.

6.1.2.10 FCS_RBG.1 Random bit generation (RBG)

FCS_RBG.1.1 The TSF shall perform deterministic random bit generation services using **CTR_DRBG (AES)** in accordance with **ISO/IEC 18031:2025** after initialization with a seed.

FCS_RBG.1.2 The TSF shall use a **TSF interface for seeding** for initialized seeding.

FCS_RBG.1.3 The TSF shall update the DRBG state by **reseeding** using a **TSF interface for seeding** in the following situations: **after 65536 generate operations or 7 minutes since the previous initialization or reseeding** in accordance with **ISO/IEC 18031: 2025.**

6.1.2.11 FCS_RBG.2 Random bit generation (external seeding)

FCS_RGB.2.1 The TSF shall be able to accept a minimum of **256 bits** from a TSF interface for the purpose of seeding.

6.1.2.12 FCS_SSH_EXT.1/AS-NE SSH Protocol

FCS_SSH_EXT.1.1/AS-NE The TOE shall implement SSH acting as a **server** that complies with RFCs 4251, 4252, 4253, 4254, **RFC 5656, RFC 8332, RFC 4256, RFC 6187, RFC 6668, no other RFCs** and [no other standard].

FCS_SSH_EXT.1.2/AS-NE The TSF shall ensure that the SSH protocol implementation supports the following authentication methods:

- **password complying with RFC 4252**
- **"publickey" (RFC 4252):**
    - **rsa-sha2-512 (RFC 8332)**
    - **ecdsa-sha2-nistp521 (RFC 5656)**
    - **ecdsa-sha2-nistp256 (RFC 5656)**
    - **rsa-sha2-256 (RFC 8332)**

] and no other methods.

FCS_SSH_EXT.1.3/AS-NE The TSF shall ensure that, as described in RFC 4253, packets greater than **256 KB** in an SSH transport connection are dropped.

FCS_SSH_EXT.1.4/AS-NE The TSF shall protect data in transit from unauthorised disclosure using following mechanisms:

- **aes128-ctr**
- **aes192-ctr**
- **aes256-cbc**

and no other mechanisms.

FCS_SSH_EXT.1.5/AS-NE The TSF shall protect data in transit from modification, deletion, and insertion using:

- **hmac-sha2-256**
- **hmac-sha2-512**

and no other mechanisms.

FCS_SSH_EXT.1.6/AS-NE The TSF shall establish a shared secret with its peer using:

- **diffie-hellman-group 14-sha256**
- **diffie-hellman-group 16-sha512**

and no other mechanisms.

FCS_SSH_EXT.1.7/AS-NE The TSF shall use an SSH key derivation function (KDF) as defined in

- **RFC 4253, Section 7.2**

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

FCS_SSH_EXT.1.8/AS-NE The TSF shall ensure that

- **connection termination**

occurs when any of the following thresholds are met:

- **30 minutes** connection time **without open channels**
- no more than **one gigabyte** of transmitted data, or

- no more than **one gigabyte** of received data.

6.1.2.13 FCS_SSH_EXT.1/Shelf-NE/LT-NE SSH Protocol

FCS_SSH_EXT.1.1/Shelf-NE/LT-NE The TOE shall implement SSH acting as a **server** that complies with RFCs 4251, 4252, 4253, 4254, **6668, 8268, 8308, no other RFCs** and [no other standard].

FCS_SSH_EXT.1.2/Shelf-NE/LT-NE The TSF shall ensure that the SSH protocol implementation supports the following authentication methods:

- **password complying with RFC 4252**
- **"publickey" (RFC 4252):**
    - **rsa-sha2-512 (RFC 8332)**
    - **ecdsa-sha2-nistp384 (RFC 5656)**
    - **ecdsa-sha2-nistp521 (RFC 5656)**

] and no other methods.

FCS_SSH_EXT.1.3/Shelf-NE/LT-NE The TSF shall ensure that, as described in RFC 4253, packets greater than **256 KB** in an SSH transport connection are dropped.

FCS_SSH_EXT.1.4/Shelf-NE/LT-NE The TSF shall protect data in transit from unauthorised disclosure using following mechanisms:

- **aes128-ctr**
- **aes192-ctr**
- **aes256-ctr**

and no other mechanisms.

FCS_SSH_EXT.1.5/Shelf-NE/LT-NE The TSF shall protect data in transit from modification, deletion, and insertion using:

- **hmac-sha2-256**
- **hmac-sha2-512**

and no other mechanisms.

FCS_SSH_EXT.1.6/Shelf-NE/LT-NE The TSF shall establish a shared secret with its peer using:

- **diffie-hellman-group18-sha512**
- **diffie-hellman-group14-sha256**
- **diffie-hellman-group-exchange-sha256**

and no other mechanisms.

FCS_SSH_EXT.1.7/Shelf-NE/LT-NE The TSF shall use an SSH key derivation function (KDF) as defined in

- **RFC 4253, Section 7.2**

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

FCS_SSH_EXT.1.8/Shelf-NE/LT-NE The TSF shall ensure that

- **connection termination**

occurs when any of the following thresholds are met:

- **10 minutes** connection time **without open channels**

- no more than **one gigabyte** of transmitted data, or
- no more than **one gigabyte** of received data.

6.1.2.14 FCS_TLSC_EXT.1 TLS Client Protocol

FCS_TLSC_EXT.1.1 The TSF shall implement **TLS 1.3 (RFC 8446), TLS 1.2 (RFC 5246)** supporting the following ciphersuites:

- **TLS 1.2:**
  - **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289**
  - **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289**
  - **ECDHE-RSA-CHACHA20-POLY1305 as defined in RFC 7905**
- **TLS 1.3:**
  - **TLS_AES_128_GCM_SHA256 as defined in RFC 8446**
  - **TLS_AES_256_GCM_SHA384 as defined in RFC 8446**
  - **TLS_CHACHA20_POLY1305_SHA256 as defined in RFC 8446**

and no other ciphersuites.

FCS_TLSC_EXT.1.2 The TSF shall verify that the presented identifier matches **IPv4 address in the CN or in the SAN, IPv6 address in the CN or in the SAN**.

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

- **without any administrator override mechanism**.

FCS_TLSC_EXT.1.4 The TSF shall **present the Supported Groups Extension with the following curves/groups: secp256r1, secp384r1, secp521r1, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, x448, x25519 and no other curves/groups** in the Client Hello.

FCS_TLSC_EXT.1.5 The TSF shall

- present the signature_algorithms extension with support for the following algorithms:

  TLS v1.3
  - **rsa_pkcs1 with sha256(0x0401),**
  - **rsa_pkcs1with sha384(0x0501),**
  - **rsa_pkcs1 with sha512(0x0601),**
  - **ecdsa_secp256r1 with sha256(0x0403),**
  - **ecdsa_secp384r1 with sha384(0x0503),**
  - **ecdsa_secp521r1 with sha512(0x0603),**
  - **rsa_pss_rsae with sha256(0x0804),**
  - **rsa_pss_rsae with sha384(0x0805),**
  - **rsa_pss_rsae with sha512(0x0806),**
  - **rsa_pss_pss with sha256(0x0809),**
  - **rsa_pss_pss with sha384(0x080a),**
  - **rsa_pss_pss with sha512(0x080b),**
  - **ed25519 (0x0807),**

- **ed448 (0x0808),**
- **SHA224 ECDSA (0x0303),**
- **SHA224 RSA (0x0301),**

TLS v1.2

- **ecdsa_secp256r1_sha256 (0x0403)**
- **ecdsa_secp384r1_sha384 (0x0503)**
- **ecdsa_secp521r1_sha512 (0x0603)**
- **ed25519 (0x0807)**
- **ed448 (0x0808)**
- **rsa_pss_pss_sha256 (0x0809)**
- **rsa_pss_pss_sha384 (0x080a)**
- **rsa_pss_pss_sha512 (0x080b)**
- **rsa_pss_rsae_sha256 (0x0804)**
- **rsa_pss_rsae_sha384 (0x0805)**
- **rsa_pss_rsae_sha512 (0x0806)**
- **rsa_pkcs1_sha256 (0x0401)**
- **rsa_pkcs1_sha384 (0x0501)**
- **rsa_pkcs1_sha512 (0x0601)**
- **SHA224 ECDSA (0x0303)**
- **SHA224 RSA (0x0301)**
- **SHA224 DSA (0x0302)**
- **SHA256 DSA (0x0402)**
- **SHA384 DSA (0x0502)**
- **SHA512 DSA (0x0602)**
- and no other algorithms.

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

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

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

FCS_TLSC_EXT.1.8 The TSF shall **not use PSKs**.

FCS_TLSC_EXT.1.9 The TSF shall **reject TLS 1.2, TLS 1.3 renegotiation attempts**.

6.1.2.15 FCS_TLSC_EXT.2 TLS Client Support for Mutual Authentication

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

6.1.2.16 FCS_TLSS_EXT.1 TLS Server Protocol

FCS_TLSS_EXT.1.1 The TSF shall implement **TLS 1.3 (RFC 8446), TLS 1.2 (RFC 5246)** and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites: [selection:

- **TLS 1.2:**
  - **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289**
  - **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289**
  - **ECDHE-RSA-CHACHA20-POLY1305**
- **TLS 1.3:**
  - **TLS_AES_128_GCM_SHA256**
  - **TLS_AES_256_GCM_SHA384**
  - **TLS_CHACHA20_POLY1305_SHA256**

] and no other ciphersuites.

FCS_TLSS_EXT.1.2 The TSF shall authenticate itself using X.509 certificate(s) using RSA with key size **2048, 3072, 4096** bits and no other curves.

FCS_TLSS_EXT.1.3 The TSF shall perform key exchange using:

- **RSA key establishment with key size 2048, 3072, 4096 bits;**
- **EC Diffie-Hellman key agreement over NIST curves secp256r1, secp384r1, secp521r1 and no other curves.**

FCS_TLSS_EXT.1.4 The TSF shall support **no session resumption**.

FCS_TLSS_EXT.1.5 The TSF p**rovides** the ability to configure the list of supported ciphersuites as defined in FCS_TLSS_EXT.1.1.

FCS_TLSS_EXT.1.6 The TSF shall prohibit the use of the following extensions:

- Early data extension

FCS_TLSS_EXT.1.7 The TSF shall **not use PSKs**.

FCS_TLSS_EXT.1.8 The TSF shall **reject TLS 1.2, TLS 1.3 renegotiation attempts**.

6.1.2.17 FCS_TLSS_EXT.2 TLS Server Support for Mutual Authentication

FCS_TLSS_EXT.2.1 The TSF shall support TLS communication with mutual authentication of TLS clients using X.509v3 certificates and shall

- **reject the connection if the client either does not provide a client certificate at all or the client certificate cannot be successfully validated by the TOE (except for override mechanisms that might be defined in FCS_TLSS_EXT.2.2) ('hard fail').**

FCS_TLSS_EXT.2.2 When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the client certificate is invalid. The TSF shall also

- **not implement any administrator override mechanism**.

FCS_TLSS_EXT.2.3 The TSF shall not establish a trusted channel if the identifier contained in a certificate does not match an expected identifier for the client. If the identifier is a Fully Qualified Domain Name (FQDN), then the TSF shall match the identifiers according to RFC 6125, otherwise the TSF shall parse the identifier from the certificate and match the identifier against the expected identifier of the client as described in the TSS.

FCS_TLSS_EXT.2.4 The TSF shall present a **TLS 1.2, TLS 1.3** Certificate Request message containing the following algorithms:

TLS v 1.3

- **rsa_pkcs1 with sha256(0x0401),**
- **rsa_pkcs1 with sha384(0x0501),**
- **rsa_pkcs1 with sha512(0x0601),**
- **ed25519 (0x0807),**
- **ed448 (0x0808),**
- **ecdsa_secp256r1 with sha256(0x0403),**
- **ecdsa_secp384r1 with sha384(0x0503),**
- **ecdsa_secp521r1 with sha512(0x0603),**
- **rsa_pss_rsae with sha256(0x0804),**
- **rsa_pss_rsae with sha384(0x0805),**
- **rsa_pss_rsae with sha512(0x0806),**
- **rsa_pss_pss with sha256(0x0809),**
- **rsa_pss_pss with sha384(0x080a),**
- **rsa_pss_pss with sha512(0x080b),**
- **SHA224 ECDSA (0x0303),**
- **SHA224 RSA (0x0301)**

TLS v 1.2

- **ecdsa_secp256r1_sha256 (0x0403),**
- **ecdsa_secp384r1_sha384 (0x0503),**
- **ecdsa_secp521r1_sha512 (0x0603),**
- **ed25519 (0x0807),**
- **ed448 (0x0808),**
- **rsa_pss_pss_sha256 (0x0809),**
- **rsa_pss_pss_sha384 (0x080a),**
- **rsa_pss_pss_sha512 (0x080b),**
- **rsa_pss_rsae_sha256 (0x0804),**
- **rsa_pss_rsae_sha384 (0x0805),**
- **rsa_pss_rsae_sha512 (0x0806),**
- **rsa_pkcs1_sha256 (0x0401),**
- **rsa_pkcs1_sha384 (0x0501),**
- **rsa_pkcs1_sha512 (0x0601),**
- **SHA224 ECDSA (0x0303),**
- **SHA224 RSA (0x0301),**
- **SHA224 DSA (0x0302),**

- **SHA256 DSA (0x0402),**
- **SHA384 DSA (0x0502),**
- **SHA512 DSA (0x0602)**

and no other algorithms.

6.1.3 User data protection (FDP)

6.1.3.1 FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the **Management information flow control SFP** on

- **Subjects: network interfaces**
- **Information: IP packets**
- **Operations: permit or deny communication.**

6.1.3.2 FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the **Management information flow control SFP** based on the following types of subject and information security attributes:

- **Subject security attributes: Receiving/transmitting VLAN interface**
- **Security information attributes: Management VLAN ID in packet header.**

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **VLAN interfaces are configured to be in the Management VLAN.**

FDP_IFF.1.3 The TSF shall enforce the **information flow so that only packets containing Management VLAN ID in the packet header are forwarded to the Management VLAN interface.**

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: **none.**

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: **communication from VLAN interfaces that do not match the Management VLAN ID is dropped.**

6.1.4 Identification and Authentication (FIA)

6.1.4.1 FIA_AFL.1 Authentication Failure Handling (Refinement)

FIA_AFL.1.1 The TSF shall detect when an Administrator configurable positive integer within **1 to 64** unsuccessful authentication attempts occur related to **Administrators attempting to authenticate remotely using a password.**

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **prevent the offending Administrator from successfully establishing a remote session using any authentication method that involves a password until an Administrator defined time period has elapsed**.

6.1.4.2 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**.

6.1.4.3 FIA_PMG_EXT.1/Shelf-NE/LT-NE Password Management

FIA_PMG_EXT.1.1/Shelf-NE/LT-NE 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 **20** characters.

6.1.4.4 FIA_PMG_EXT.1/AS-NE Password Management

FIA_PMG_EXT.1.1/AS-NE 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 **5** and **50** characters.

6.1.4.5 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 **password, SSH public key, X.509 certificate** 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.

6.1.5 Security Management (FMT)

6.1.5.1 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce **Management information flow control SFP** to restrict the ability to **change_default** security attributes **Management VLAN ID** to **Administrator**.

6.1.5.2 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 **Administrators**.

6.1.5.3 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 **Administrators**.

6.1.5.4 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 **Administrators**.

6.1.5.5 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 **Administrators**.

6.1.5.6 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 manage the cryptographic keys;**
- **Ability to configure the cryptographic functionality;**
- **Ability to configure the list of supported TLS ciphers;**
- **Ability to re-enable an Administrator account;**
- **Ability to configure NTP;**
- **Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;**
- **Ability to administer the TOE locally;**
- **Ability to configure the local session inactivity time before session termination or locking;**
- **Ability to configure the authentication failure parameters for FIA_AFL.1;**
- **Ability to manage the trusted public keys database.**

6.1.5.7 FMT_SMR.2 Restrictions on security roles

FMT_SMR.2.1 The TSF shall maintain the roles:

- **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 Administrator role shall be able to administer the TOE remotely**

are satisfied.

6.1.6 Protection of the TSF (FPT)

6.1.6.1 FPT_APW_EXT.1 Protection of Administrator Passwords

FPT_APW_EXT.1.1 The TSF shall store administrative passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext administrative passwords.

6.1.6.2 FPT_SKP_EXT.1 Protection of TSF Data (for reading of all symmetric keys)

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

6.1.6.3 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**.

6.1.6.4 FPT_TUD_EXT.1 Trusted Update

FPT_TUD_EXT.1.1 The TSF shall provide **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 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.

6.1.7 TOE Access (FTA)

6.1.7.1 FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1 The TSF shall terminate **a remote** interactive session after a **Administrator-configurable time interval of session inactivity**.

6.1.7.2 FTA_SSL.4 User-initiated Termination

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

6.1.7.3 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 Administrator-specified time period of inactivity.

6.1.7.4 FTA_TAB.1 Default TOE Access Banners

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

6.1.8 Trusted Path/Channels (FTP)

6.1.8.1 FTP_ITC.1 Inter-TSF Trusted Channel

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

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

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **transmission of syslog records to syslog audit server.**

6.1.8.2 FTP_TRP.1/Admin Trusted Path

FTP_TRP.1.1/Admin The TSF shall **be capable of using SSH, TLS to** provide a communication path between itself and **authorized remote Administrators** that **are** logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **disclosure and provides detection of modification of the channel data.**

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

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

6.2 Security Requirements Dependency Analysis

The following table demonstrates the dependencies of the SFRs modelled in CC Part 2, the extended component definition in this Security Target, [NDcPPv3.0E] and ([PKG_SSHv2.0]):, and how the SFRs for the TOE resolve those dependencies.

Security functional requirement	Dependencies	Resolution
FAU_GEN.1	FPT_STM.1	FPT_STM_EXT.1
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 Satisfied by FIA_UIA_EXT.1, which specifies the relevant Administrator identification timing
FAU_STG_EXT.1	FAU_GEN.1 FTP_ITC.1	FAU_GEN.1 FTP_ITC.1
FCS_CKM.1	[FCS_CKM.2 or FCS_CKM.5 or FCS_COP.1 [FCS_RBG.1 or FCS_RNG.1] FCS_CKM.6	FCS_CKM.2 FCS_COP.1 FCS_RBG.1 FCS_CKM.6
FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5]	FCS_CKM.1
FCS_CKM.6	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
FCS_COP.1/Hash	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5] FCS_CKM.6	FCS_CKM.1 FCS_CKM.6
FCS_COP.1/KeyedHash	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5]	FCS_CKM.1 FCS_CKM.6

Security functional requirement	Dependencies	Resolution
	FCS_CKM.6	
FCS_COP.1/SigGen	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5] FCS_CKM.6	FCS_CKM.1 FCS_CKM.6
FCS_COP.1/SSH DataEncryption	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5] FCS_CKM.6	FCS_CKM.1 FCS_CKM.6
FCS_COP.1/TLS DataEncryption	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5] FCS_CKM.6	FCS_CKM.1 FCS_CKM.6
FCS_NTP_EXT.1	FCS_COP.1 [FCS_DTLSC_EXT.1 or FCS_IPSEC_EXT.1]	FCS_COP.1/DataEncryption FCS_COP.1/SigGen FCS_COP.1/Hash FCS_COP.1/KeyedHash FCS_DTLSC_EXT.1 and FCS_IPSEC_EXT.1 are not applicable in this ST
FCS_RBG.1	[FCS_RBG.2 or FCS_RBG.3] FPT_FLS.1 FPT_TST.1	FCS_RBG.2 No, FPT_FLS.1 OE.PLATFORM_ENTROPY ensures sufficient quality and quantity of seed material). No, FPT_TST.1 (OE.PLATFORM_ENTROPY ensures sufficient quality and quantity of seed material).
FCS_RBG.2	FCS_RBG.1	FCS_RBG.1
FCS_SSH_EXT.1/AS-NE	FCS_CKM.1 FCS_CKM.2	FCS_CKM.1 FCS_CKM.2

Security functional requirement	Dependencies	Resolution
	FCS_COP.1 FCS_RBG.1	FCS_COP.1/SSH DataEncryption FCS_COP.1/SigGen FCS_COP.1/Hash FCS_COP.1/KeyedHash FCS_RBG.1
FCS_SSH_EXT.1/Shelf-NE/LT-NE	FCS_CKM.1 FCS_CKM.2 FCS_COP.1 FCS_RBG.1	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/SSH DataEncryption FCS_COP.1/SigGen FCS_COP.1/Hash FCS_COP.1/KeyedHash FCS_RBG.1
FCS_TLSC_EXT.1	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/DataEncryption FCS_COP.1/SigGen FCS_COP.1/Hash FCS_COP.1/KeyedHash FCS_RBG_EXT.1	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/TLS DataEncryption FCS_COP.1/SigGen FCS_COP.1/Hash FCS_COP.1/KeyedHash Satisfied by FCS_RBG.1
FCS_TLSC_EXT.2	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/DataEncryption FCS_COP.1/SigGen FCS_COP.1/Hash FCS_COP.1/KeyedHash FCS_RBG_EXT.1 FCS_TLSC_EXT.1	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/TLS DataEncryption FCS_COP.1/SigGen FCS_COP.1/Hash FCS_COP.1/KeyedHash Satisfied by FCS_RBG.1 FCS_TLSC_EXT.1
FCS_TLSS_EXT.1	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/DataEncryption FCS_COP.1/SigGen FCS_COP.1/Hash FCS_COP.1/KeyedHash FCS_RBG_EXT.1	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/TLS DataEncryption FCS_COP.1/SigGen FCS_COP.1/Hash FCS_COP.1/KeyedHash Satisfied by FCS_RBG.1

Security functional requirement	Dependencies	Resolution
FCS_TLSS_EXT.2	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/DataEncryption FCS_COP.1/SigGen FCS_COP.1/Hash FCS_COP.1/KeyedHash FCS_RBG_EXT.1 FCS_TLSS_EXT.1	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/TLS DataEncryption FCS_COP.1/SigGen FCS_COP.1/Hash FCS_COP.1/KeyedHash Satisfied by FCS_RBG.1 FCS_TLSS_EXT.1
FDP_IFC.1	FDP_IFF.1	Yes, FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	Yes, FDP_IFC.1 No, FMT_MSA.3 (restrictive values are enforced, alternative values cannot be specified)
FIA_AFL.1	FIA_UAU.1	Satisfied by FIA_UIA_EXT.1, which specifies the relevant Administrator identification timing
FIA_PMG_EXT.1/AS-NE	No dependencies	
FIA_PMG_EXT.1/Shelf-NE/LT-NE	No dependencies	
FIA_UAU.7	FIA_UAU.1	Satisfied by FIA_UIA_EXT.1, which specifies the relevant Administrator identification timing
FIA_UIA_EXT.1	FTA_TAB.1	FTA_TAB.1
FMT_MOF.1/ManualUpdate	FMT_SMR.1 FMT_SMF.1	FMT_SMR.2 FMT_SMF.1
FMT_MOF.1/Services	FMT_SMR.1 FMT_SMF.1	FMT_SMR.2 FMT_SMF.1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_IFC.1 FMT_SMR.1 FMT_SMF.1
FMT_MTD.1/CoreData	FMT_SMR.1	FMT_SMR.2

Security functional requirement	Dependencies	Resolution
	FMT_SMF.1	FMT_SMF.1
FMT_MTD.1/CryptoKeys	FMT_SMR.1 FMT_SMF.1	FMT_SMR.2 FMT_SMF.1
FMT_SMF.1	No dependencies	
FMT_SMR.2	FIA_UID.1	Satisfied by FIA_UIA_EXT.1, which specifies the relevant Administrator identification timing
FPT_APW_EXT.1	No dependencies	
FPT_SKP_EXT.1	No dependencies	
FPT_STM_EXT.1	No dependencies	
FPT_TUD_EXT.1	FCS_COP.1/SigGen or FCS_COP.1/Hash	FCS_COP.1/SigGen FCS_COP.1/Hash
FTA_SSL_EXT.1	FIA_UAU.1	Satisfied by FIA_UIA_EXT.1, which specifies the relevant Administrator identification timing
FTA_SSL.3	FMT_SMR.1	FMT_SMR.2
FTA_SSL.4	No dependencies	
FTA_TAB.1	No dependencies	
FTP_ITC.1	No dependencies	
FTP_TRP.1/Admin	No dependencies	

Table 9 TOE SFR dependency analysis

The security functional requirements in this Security Target do not introduce dependencies on any security assurance requirement; neither do the security assurance requirements in this Security Target introduce dependencies on any security functional requirement.

6.3 Security assurance requirements for the TOE

The security assurance requirements (SARs) for the TOE are the Evaluation Assurance Level 3 which is defined in [CC] part 5 and assurance components are specified in [CC] part 3

Security assurance Class	Security assurance requirement	Source
ADV: Development	ADV_ARC.1 Security architecture description	CC Part 3

Security assurance Class	Security assurance requirement	Source
	ADV_FSP.3 Functional specification with complete summary	CC Part 3
	ADV_TDS.2 Architectural design	CC Part 3
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	CC Part 3
	AGD_PRE.1 Preparative procedures	CC Part 3
ALC: Life-cycle support	ALC_CMC.3 Authorization controls	CC Part 3
	ALC_CMS.3 Implementation representation CM coverage	CC Part 3
	ALC_DEL.1 Delivery procedures	CC Part 3
	ALC_DVS.1 Identification of security measures	CC Part 3
	ALC_LCD.1 Developer defined life-cycle model	CC Part 3
	ALC_FLR.2 Flaw reporting procedures	CC Part 3
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims	CC Part 3
	ASE_ECD.1 Extended components definition	CC Part 3
	ASE_INT.1 ST introduction	CC Part 3
	ASE_OBJ.2 Security objectives	CC Part 3
	ASE_REQ.2 Derived security requirements	CC Part 3
	ASE_SPD.1 Security problem definition	CC Part 3
	ASE_TSS.1 TOE summary specification	CC Part 3
ATE: Test	ATE_COV.2 Analysis of coverage	CC Part 3
	ATE_DPT.1 Testing: basic design	CC Part 3
	ATE_FUN.1 Functional testing	CC Part 3
	ATE_IND.2 Independent testing – sample	CC Part 3
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis	CC Part 3

Table 10 SARs

6.4 Security functional requirements rationale

6.4.1 Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective.

Security functional requirements	Objectives
FAU_GEN.1	O.AUDIT
FAU_GEN.2	O.AUDIT
FAU_STG_EXT.1	O.AUDIT
FCS_CKM.1	O.CRYPTOGRAPHY
FCS_CKM.2	O.CRYPTOGRAPHY
FCS_CKM.6	O.CRYPTOGRAPHY
FCS_COP.1/Hash	O.CRYPTOGRAPHY
FCS_COP.1/KeyedHash	O.CRYPTOGRAPHY
FCS_COP.1/SigGen	O.CRYPTOGRAPHY
FCS_COP.1/SSH DataEncryption	O.CRYPTOGRAPHY
FCS_COP.1/TLS DataEncryption	O.CRYPTOGRAPHY
FCS_NTP_EXT.1	O.AUDIT
FCS_RBG.1	O.CRYPTOGRAPHY
FCS_RBG.2	O.CRYPTOGRAPHY
FCS_SSH_EXT.1/AS-NE	O.COMMUNICATION_CHANNELS
FCS_SSH_EXT.1/Shelf-NE/LT-NE	O.COMMUNICATION_CHANNELS
FCS_TLSC_EXT.1	O.COMMUNICATION_CHANNELS
FCS_TLSC_EXT.2	O.COMMUNICATION_CHANNELS
FCS_TLSS_EXT.1	O.COMMUNICATION_CHANNELS
FCS_TLSS_EXT.2	O.COMMUNICATION_CHANNELS
FDP_IFC.1	O.MANAGEMENT_TRAFFIC

Security functional requirements	Objectives
FDP_IFF.1	O.MANAGEMENT_TRAFFIC
FIA_AFL.1	O.ADMIN_ACCESS, O.ADMIN_SESSION
FIA_PMG_EXT/AS-NE	O.ADMIN_ACCESS
FIA_PMG_EXT/Shelf-NE/LT-NE	O.ADMIN_ACCESS
FIA_UAU.7	O.ADMIN_ACCESS
FIA_UIA_EXT.1	O.ADMIN_ACCESS
FMT_MOF.1/ManualUpdate	O.ADMIN_ACCESS, O.TRUSTED_UPDATES
FMT_MOF.1/Services	O.ADMIN_ACCESS
FMT_MSA.1	O.MANAGEMENT_TRAFFIC
FMT_MTD.1/CoreData	O.ADMIN_ACCESS, O.TSF_DATA_PROTECTION
FMT_MTD.1/CryptoKeys	O.ADMIN_ACCESS, O.TSF_DATA_PROTECTION
FMT_SMF.1	O.ADMIN_ACCESS, O.AUDIT, O.TRUSTED_UPDATES, O.TSF_DATA_PROTECTION
FMT_SMR.2	O.ADMIN_ACCESS, O.AUDIT, O.TRUSTED_UPDATES, O.TSF_DATA_PROTECTION
FPT_APW_EXT.1	O.TSF_DATA_PROTECTION
FPT_SKP_EXT.1	O.TSF_DATA_PROTECTION
FPT_STM_EXT.1	O.AUDIT
FPT_TUD_EXT.1	O.TRUSTED_UPDATES
FTA_SSL_EXT.1	O.ADMIN_SESSION
FTA_SSL.3	O.ADMIN_SESSION
FTA_SSL.4	O.ADMIN_SESSION

Security functional requirements	Objectives
FTA_TAB.1	O.ACCESS_BANNER
FTP_ITC.1	O.COMMUNICATION_CHANNELS
FTP_TRP.1/Admin	O.COMMUNICATION_CHANNELS

Table 11 Mapping of security functional requirements to security objectives

6.4.2 Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives.

Security objectives	Rationale
O.ADMIN_ACCESS	FIA_UIA_EXT.1 defines that the display of the banner is the only action allowed prior to identification and authentication. FIA_UAU.7 requires that password feedback be obscured during authentication. FIA_AFL.1 specifies the actions on reaching a threshold number of consecutive password failures. FIA_PMG_EXT/Shelf-NE/LT-NE and FIA_PMG_EXT/AS-NE provide password management capabilities. The following SFRs restrict security management functionality to security administrators: FMT_MOF.1/ManualUpdate for Trusted Updates of the TOE, FMT_MOF.1/Services for starting and stopping services, FMT_MTD.1/CryptoKeys for management of cryptographic keys, and FMT_MTD.1/CoreData for management of TSF data. FMT_SMF.1 and FMT_SMR.2 specify the security management functionality associated with this objective.
O.ADMIN_SESSION	FTA_SSL.3 addresses the termination of remote sessions after a specified period of inactivity. FTA_SSL.4 addresses the termination of the session by the administrator. FTA_SSL_EXT.1 addresses the termination for local interactive sessions. FIA_AFL.1 specifies the actions on reaching a threshold number of consecutive password failures.
O.CRYPTOGRAPHY	FCS_CKM.1 defines the required standards and key sizes for key generation, while FCS_CKM.2 defines the required standards for key distribution. FCS_COP.1/SSH DataEncryption, FCS_COP.1/TLS DataEncryption, FCS_COP.1/SigGen, FCS_COP.1/Hash, FCS_COP.1/KeyedHash define the cryptographic algorithms, modes, key sizes and standards. FCS_RBG.1, FCS_RBG.2 define the Deterministic Random Bit Generator (DRBG) and the minimum entropy required for key generation. FCS_CKM.6 defines the timing and event of cryptographic key destruction.

Security objectives	Rationale
O.COMMUNICATION_CHANNELS	FTP_ITC.1 and FTP_TRP.1/Admin define trusted communication channels with external IT entities and remote administrators, respectively. Trusted communication channels are secured by the protocols mentioned below. Secure transport protocols are defined in FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSS_EXT.1, FCS_TLSS_EXT.2, FCS_SSH_EXT.1/AS-NE and FCS_SSH_EXT.1/Shelf-NE/LT-NE.
O.TRUSTED_UPDATES	FPT_TUD_EXT.1 specifies the behavior of the verification and installation of software updates by the TOE administrator. FMT_MOF.1/ManualUpdate restricts the ability to perform manual updates to Administrators. FMT_SMF.1 and FMT_SMR.2 specify the security management functionality associated with this objective.
O.AUDIT	FAU_GEN.1 defines the events that the TOE is required to audit. Those events are related to other security functional requirements showing which event contributes to make users accountable for their actions with respect to the requirement. FAU_GEN.2 requires that the events are associated with the identity of the user that caused the event. FAU_STG_EXT.1 defines protected audit event storage requirements. FMT_SMF.1 and FMT_SMR.2 specify the security management functionality associated with this objective. FPT_STM_EXT.1 provides reliable timestamps for generating audit records. FCS_NTP_EXT.1 provides NTP time sources.
O.TSF_DATA_PROTECTION	FPT_SKP_EXT.1 addresses the protection of cryptographic key material, whereas FPT_APW_EXT.1 addresses the protection of administrator passwords. FMT_MTD.1/CoreData, FMT_MTD.1/CryptoKeys, FMT_SMF.1 and FMT_SMR.2 specify security management functionality associated with this objective and its corresponding access constraints.
O.ACCESS_BANNER	FTA_TAB.1 addresses the display of the banner before a session is established.
O.MANAGEMENT_TRAFFIC	FDP_IFC.1 and FDP_IFF.1 define Management information flow control SFP for separation of management traffic. FMT_MSA.1 specify management functionality associated with this objective.

Table 12 Mapping of security objectives to security functional requirements

6.4.3 Security assurance requirements rationale

The chosen assurance level, EAL3, ensures the TOE to be resistant to an attacker possessing an Enhanced-basic attack potential, commensurate with the threat environment that is experienced by typical consumers of the TOE.

EAL3 is augmented with ALC_FLR.2 to assist in ensuring that discovered security flaws are tracked and are corrected by the developer and that TOE users are aware of how to report a security flaw and receive corrective fixes.

7 TOE Summary Specification

7.1 Security audit

The TOE records audit events for authentication attempts, administrative operations, as well as all of the events identified in Table 8. Each audit record contains the date and time of the event, type of event, subject identity (user, device or process) and outcome (success or failure).

The TOE writes audit records can be stored locally. When the local audit storage exceeds a maximum size, the TOE overwrites the oldest audit records. The TOE can be configured to transmit the audit records to a specified, external Syslog server. Communication between the TOE and the external Syslog server must be configured and enabled in the evaluation configuration.

SFR coverage:

- FAU_GEN.1
- FAU_GEN.2
- FAU_STG_EXT.1

7.2 Cryptographic support

All cryptographic operations, including algorithms and key generation used by the TOE are provided by cryptographic module (OpenSSL). OpenSSL implements the Transport Layer Security (TLS) protocol and cryptographic algorithms. The following table summarizes the cryptographic algorithms implemented in OpenSSL.

OpenSSL includes a Deterministic Random Bit Generator (DRBG) used for key generation and random data (e.g. shared secrets). The DRBG uses the CTR_DRBG with AES-256-CTR algorithm.

For Shelf-NE/LT-NE, seed material originates from a hardware-based entropy source, a physical hardware random-number generator, and is passed to seed the OpenSSL DRBG. For AS-NE, seed material is obtained from a software-based noise source that combines CPU cycle/count register values, nanosecond-resolution clock values, and bounded task-delay jitter, and is then used to seed the OpenSSL DRBG.

The TOE implements TLS version 1.2 and TLS version 1.3 provided by OpenSSL (Shelf-Ne/LT-NE: OpenSSL 3.0.9, AS-NE: OpenSSL 1.1.1) to establish a secure channel for NETCONF (NETCONF over TLS). The TOE acts as a server.

The TOE offers the establishment of TLS sessions with external log servers in the operational environment for protection of audit records in transfer. The TOE acts as a TLS client.

The TOE as a TLS client and the TLS server supports the following cipher suites:

- TLS 1.2:
    - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
    - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
    - ECDHE-RSA-CHACHA20-POLY1305
- TLS 1.3:
    - TLS_AES_128_GCM_SHA256
    - TLS_AES_256_GCM_SHA384
    - TLS_CHACHA20_POLY1305_SHA256

The TOE also implements SSH to allow establishment of secure communication over NETCONF or CLI.

Security protocol	Encryption algorithm	Authentication algorithm	Key exchange algorithms	Authentication mechanism

SSH	aes128-ctr aes192-ctr aes256-ctr	hmac-sha2-256 hmac-sha2-512	diffie-hellman-group 14-sha256 diffie-hellman-group 16-sha512	Username/password, Keybased

Table 13 Supported SSH Authentication and Encryption Schemes (AS-NE)

Security protocol	Encryption algorithm	Authentication algorithm	Key exchange algorithms	Authentication mechanism
SSH	aes128-ctr aes192-ctr aes256-ctr	hmac-sha2-256 hmac-sha2-512	diffie-hellman-group 18-sha512 diffie-hellman-group 14-sha256 diffie-hellman-group- exchange-sha256	Username/password, Keybased

Table 14 Supported SSH Authentication and Encryption Schemes (Shelf-NE/LT-NE)

SFR coverage:

- FCS_CKM.1
- FCS_CKM.2
- FCS_CKM.6
- FCS_COP.1/SSH DataEncryption
- FCS_COP.1/TLS DataEncryption
- FCS_COP.1/Hash
- FCS_COP.1/KeyedHash
- FCS.COP.1/SigGen
- FCS_NTP_EXT.1
- FCS_RBG.1
- FCS_RBG.2
- FCS_SSH_EXT.1/AS-NE
- FCS_SSH_EXT.1/Shelf-NE/LT-NE
- FCS_TLSC_EXT.1
- FCS_TLSC_EXT.2
- FCS_TLSS_EXT.1
- FCS_TLSS_EXT.2

7.3 Identification and Authentication

The TOE identifies individual administrative users by user name and authenticates them by passwords or public key. Both authentication methods are allowed by default. The administrator can configure the allowed authentication methods for users of the system. The administrator can create any user and have the user assigned to specific access-groups in line with the intended privilege levels of the created user. Authentication of administrators is enforced at all management interfaces, i.e. NETCONF (SSH or TLS), CLI (SSH).

The TOE can be configured to use local authentication and authorization or remote RADIUS server (RFC 2865). RADIUS is only supported when password-based authentication is used. Public key authentication will be performed only locally. Such users must be created locally.

Authorization through RADIUS is supported through Nokia-Lightspan VSA's by conveying the entitled RBAC user-groups via the respective VSA in the AccessAccept message. The VSA is used to assign the permissions (= privileges) to the administrator being authenticated. A dedicated Nokia-Lightspan-User-Group is required for each of the User Groups (VSA value) for which the administrator is granted permissions. In case of multiple groups, the VSA must be repeated for each user Group.

In case the user is created locally, authentication and authorization is applied based on the configuration of the user profile (RADIUS or local authentication). By default, local authentication and authorization is performed.

The TOE supports a configurable password policy to define the minimum length of the password, the minimum number of digital numbers, the minimum number of special characters and define if both upper- and lower-case alphabetic characters shall or shall not be present. The following special characters are supported: **"!", "@", "#", "$", "%", "^", "&", "*", "(", ")".**

The initial and default values of the password policy is one number, one lower case letter, one uppercase letter, and one special character and minimum length of password eight characters.

The TOE provides only obscured feedback to the administrative user while the authentication is in progress at the local console.

A user or IP can be locked out from accessing the TOE when a certain threshold of failed attempt is reached. This threshold is the 'max-retry-attempts' and it can be configured. The max-retry-attempts is the cumulative number of failed login attempts that must happen in order to trigger a lockout. The default threshold of failed attempts is 3 attempts. The range of configurable threshold values is 1 to 64. The lockout duration can be configured either as dynamic or fixed. Default value '0' enables dynamic lockout type. Initial value of dynamic lockout duration is 2 minutes and every subsequent failure increase the lockout-duration for 2 minutes. Maximum lockout duration is restricted to 15 minutes.

SFR coverage:

- FIA_AFL.1
- FIA_UAU.7
- FIA_PMG_EXT.1/AS-NE
- FIA_PMG_EXT.1/Shelf-NE/AS-NE
- FIA_UIA_EXT.1

7.4 Security Function Management

The user privileges are applied for every management user access to the database (configuration and/or state) of the TOE. The rules are applied irrespective of the management protocol (CLI, NETCONF) or the underlying security protocol (SSH, TLS). The TOE provides user privileges level access authorization, Role Based Access Control (RBAC) based on a simplification of the RFC8341 Network Configuration Access Control Model (NACM). For ease-of-use and simplification, predefined domains (groups) with assigned rules (read-only/read-write/execute) have instantiated on the Lightspan Access Node.

The system offers predefined groups for the following domains:

- System logging
- Equipment
- Software management
- Transport
- L2 Forwarding

- Multicast
- QoS
- Subscriber
- Notifications
- Alarms
- OAM

The default "admin" user is shared between cli-users and NETCONF users. More users can be created, and in general, cli-users and NETCONF-users should be separated

To control or manage the TOE, the administrator should primarily use the Access Controller. NETCONF is one of the major protocols between the Access Controller (Altiplano) and the Lightspan Access Node. NETCONF is supported either over SSH or over TLS.

Several CLI options are supported, each one optimized and targeted to specific cases in the variety of situations and deployments. In the evaluated configuration, the only CLI that the administrators are using is the embedded YANG eCLI

Embedded YANG eCLI (YANG eCLI): This CLI provides unlimited access to the management objects in the Lightspan Access Node. It is fully derived from YANG and hence is subjected to changes according to the YANG model changes. This CLI is only to be used in absence of an Access Controller like Altiplano.

Access to this CLI is possible locally via serial CRAFT or LEMI interface on the TOE as well as via a remote SSH connection. After successful identification and authentication, the administrator has access to the TOE, but the operator’s access is limited to the domains being assigned according to RBAC.

The TOE restricts the ability to start and stop the functions services to administrators. The administrator is able to start and stop the following services:

- bridge-vpls
- bridge
- cross-connect
- oam
- protection
- security
- traffic-management
- layer3
- ipv4
- ipv6
- mirror
- Pseudowire
- TransportLSP

SFR coverage:

- FMT_MOF.1/ManualUpdate
- FMT_MOF.1/Services
- FMT_MTD.1/CoreData
- FMT_MTD.1/CryptoKeys
- FMT_SMF.1
- FMT_SMR.2

7.5 Protection of the TSF

The TOE is designed to protect critical security data, including keys and passwords.

Sensitive cryptographic keys are stored in the TOE's configuration files. The TOE does not offer an interface to retrieve the contents of its configuration files. Passwords are stored in a salted hashed format:

- Shelf-NE and LT-NE: SHA-512
- AS-NE: bcrypt. bcrypt generates a unique 128-bit salt. It is based on the Blowfish encryption algorithm and uses an adaptive hashing function.

The TOE can retrieve the time from an NTP server. The TOE implements NTPv4 client (RFC5905). NTP servers are configured manually via the NETCONF management interface or are dynamically discovered via DHCP.

The TOE also provides a mechanism to provide trusted updates to the TOE software. The higher release software needs to be downloaded to the Lightspan Access Node. This requires that first the non-active software release is removed such that the higher software release can be hosted. After successful download, the software upgrade is then performed by "activating" this higher software release. If there would be a failure during such upgrade, the TOE will automatically roll-back.

The software of the Lightspan Access Node MF is signed by Nokia when they are delivered to the customer. The TOE can validate the signature of the software before it is activated. A corrupted or unauthorized software will fail this verification and hence validates the integrity and authenticity. The certificate is signed using sha512WithRSAEncryption algorithm and contains the name of the release as the common name. The signed certificate can be viewed on the management interface and can be independently verified for authenticity by the administrators by requesting a copy of the signed certificate of the release from Nokia.

SFR coverage:

- FPT_APW_EXT.1
- FPT_SKP_EXT.1
- FPT_STM_EXT.1
- FPT_TUD_EXT.1

7.6 TOE Access

The system provides the ability of an administrator user to configure a disconnection time for idle CLI or NETCONF session connections. It is possible to configure the maximum idle time. The administrative users can also actively terminate their session connections (log out).

Before establishing an administrative user session, the TSF can be configured to display a administrator-specified advisory notice and consent warning message regarding use of the TOE.

The TOE also allows configuration of the access banners. The access banners are displayed before establishment of the administrative user session.

SFR coverage:

- FTA_SSL.3
- FTA_SSL.4
- FTA_SSL_EXT.1
- FTA_TAB.1

7.7 Trusted Path / Channels

The security functionality provided by the TOE in order to protect the confidentiality and integrity of network connections are described below.

7.7.1 Administrative traffic

The TOE secures administrative traffic (i.e., administrators connecting to the TOE in order to configure and maintain it) as follows:

- The connection between the TOE and Persistent Management Agent (PMA), a component in Access Controller, is based on TLS. Management traffic is NETCONF over TLS (RFC 7589). The TOE initiates a TCP connection to the PMA. The PMA responds by initiating TLS to the TOE. As part of the TLS session initiation, the TOE and the PMA authenticate each other. The mutual authentication takes place using X.509 certificates. The TOE TLS implementation is based on OpenSSL (Shelf-Ne/LT-NE: OpenSSL 3.0.9, AS-NE: OpenSSL 1.1.1). Supported TLS ciphers are listed in section 7.2.
- The TOE can also secure administrative traffic by SSH. SSH can be configured to secure NETCONF and CLI interfaces. Supported SSH authentication and encryption schemes are provided in Table 13 and Table 14.

SFR coverage:

- FTP_TRP.1/Admin Trusted Path

7.7.2 Communication to other server

The TOE offers the establishment of TLS sessions with external log servers in the operational environment for protection of audit records in transfer. The TOE acts as a TLS client. TLS communication can be configured with either mutual authentication or one-way authentication. The Syslog server is always authenticated by the TOE.

SFR coverage:

- FTP_ITC.1

7.8 Management access

The TOE provides separation of management traffic from the control and data traffic. The TOE provides a specific management VLAN, which enforces traffic separation. Any management access to the Lightspan Access Node via a VLAN which is not the management VLAN is not possible. Such traffic is dropped.

The TOE uses a dedicated external management VLAN (4093). The management IP address and management protocols are only accessible via the external management VLAN. The management IP address is dynamically assigned via DHCP or a fixed IP address configured from OLT for PON-fed nodes.

SFR coverage:

- FDP_IFC.1
- FDP_IFF.1
- FMT_MSA.1

8 Glossary of terms and abbreviations

Term/ Abbreviation	Definition
adversary	a person or other agent, not authorized to access the TOE or one of its peers but is able to exercise significant powers on the black network over which the TOE and its peers communicate, that mounts a network attack from the black network with the objective of violating one of the security policies
25GS-PON	25 Gigabit symmetrical and asymmetrical PON
AS-NE	NE on the NT-card
BRAS	Broadband Remote Access Server
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
DRBG	Deterministic Random Bit Generator
eCLI	embedded Command Line Interface
EMAN	Ethernet Metropolitan Area Network/
FTTH	Fiber To The Home
GPON	Gigabit Passive Optical Network
HSI	High-Speed Internet
IP	Internet Protocol
IPFIX	Internet Protocol Flow Information Export
L2 Forwarding	Layer 2 Forwarding Protocol
LEMI	Local Ethernet Management Interface
Local console	Access to the TOE via serial CRAFT or LEMI interface
LT	Line Termination
LT-NE	Line Termination Network Element
MDU	Multi-Dwelling Unit
MTU	Multi-Tenant Unit

Term/ Abbreviation	Definition
NACM	Network Configuration Access Control Model
NE	Network Element
NETCON	Network Configuration
NSP	Network Services Platform
NT	Network Termination
NTP	Network Time Protocol
OAM	Operations Administration and Maintenance
OLCS	On Line Customer Support
OLT	Optical Line Termination
ONU	Optical Network Units)
OpenSSL	Open Secure Sockets Layer
P2P	Peer to Peer
PMA	Persistent Management Agent
PMA	Persistent Management Agent
PON	Passive Optical Network
QoS	Quality of Service
RADIUS	Remote Authentication Dial in User System
RBAC	Role Based Access Control
RSA	Rivest-Shamir-Adleman Algorithm
SBU	Single Business Unit
SFU	Single Family Unit
SHA	Secure Hash Algorithm
SHELF-NE	The NEs on the NTs
SSH	Secure Shell
SSL	Secure Sockets Layer

Term/ Abbreviation	Definition
SW	Software
SWDP	SW Distribution Platform
Syslog	System Log
TLS	Transport Layer Security
VLAN	Virtual Local Area Network
VoIP	Video, and Voice over IP
VSA	Virtual System Administrator
XGS-PON	10 Gigabit symmetrical and asymmetrical PON
YANG	Yet Another Next Generation

9 References

Ref #	Title
[1]	Common Criteria for Information Technology Security Evaluation, Part 1-5, CC:2022, Revision 1, November 2022
[2]	Common Methodology for Information Technology Security Evaluation, CEM:2022, Revision 1, November 2022
[3]	Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.1, 2024-07-22
[4]	Information Security, Cybersecurity and Privacy Protection - Evaluation Criteria for IT Security, Part 1-5, ISO/IEC 15408-1:2022, August 2022