Unit/Issued by
IQTEA/ Anders Staaf

Date
2026-04-20

Ref. No/Order No
CAB-250127-94851-362:012

Unit/Appoint
OEMDG/ Thomas Eklund

Classification
UNCLASSIFIED

Issue
1.12

# Security Target – Saab SPNP Information Exchange Gateway 1.0.1

# DOCUMENT HISTORY

| Issue | Status | Issue date | Revision description | Edited by |
|---|---|---|---|---|
| 1.0 | Approved | 2025-02-18 | First version | Anders Staaf |
| 1.1 | Approved | 2025-03-11 | Updated after comments from the evaluator | Anders Staaf |
| 1.2 | Approved | 2025-05-13 | Addressed the certifier's comments | Anders Staaf |
| 1.3 | Approved | 2025-08-18 | Minor updates | Anders Staaf |
| 1.4 | Approved | 2025-10-27 | Updated according to ADV | Anders Staaf |
| 1.5 | Approved | 2025-11-14 | Name changed from TacEdge IEG to SPNP IEG | Anders Staaf |
| 1.6 | Approved | 2025-11-18 | New role added to FMT_SMR.1: User Administrator | Anders Staaf |
| 1.7 | Approved | 2025-11-20 | Evaluator comments are addressed. | Anders Staaf |
| 1.8 | Approved | 2025-11-26 | Evaluator comments are addressed. | Anders Staaf |
| 1.9 | Approved | 2025-11-27 | Updated after comments from Saab | Anders Staaf |
| 1.10 | Approved | 2026-01-27 | Updated after testing | Anders Staaf |
| 1.11 | Approved | 2026-03-09 | Addressed certifier comments. | Anders Staaf |
| 1.12 | Approved | 2026-04-20 | Addressed certifier comments. | Anders Staaf |

# Contents

1 ST Introduction ....6
1.1 ST Reference ....6
1.2 TOE Reference ....6
1.3 Document Overview ....6
1.4 Conventions ....6
1.5 TOE Overview ....7
1.5.1 SPNP IEG Scenarios ....7
1.6 TOE Description ....10
1.6.1 System Overview ....10
1.6.2 SPNP IEG Applications and Services Supported ....10
1.6.3 TOE States ....11
1.6.4 Roles ....11
1.6.5 Physical Scope ....11
1.6.6 Logical Scope ....13
1.6.7 Features Excluded from the TOE ....14
2 Conformance Claims ....15
2.1 CC Conformance Claim ....15
2.2 PP Conformance Claims ....15
2.3 Package Conformance Claims ....15
3 Security Problem Definition ....16
3.1 Introduction ....16
3.2 Threats ....16
3.3 Organizational Security Policies ....17
3.4 Assumptions ....17
4 Security Objectives ....18
4.1 Introduction ....18
4.2 Security Objectives for the TOE ....18
4.3 Security Objectives for the Operational Environment ....19
4.4 Security Objectives Rationale ....20
4.4.1 Security Objectives Coverage ....20
4.4.2 Security Objectives Sufficiency ....21
5 Extended Components Definition ....23

5.1 FPT_DSK_EXT Extended: Protection of Data on Disk ....23
5.1.1 Family Behaviour: ....23
5.1.2 Component Leveling: ....23
5.1.3 Management: ....23
5.1.4 Audit: ....23
5.1.5 Protection of Data on Disk – FPT_DSK_EXT.1 Extended ....23
6 Security Requirements ....24
6.1 TOE Security Functionality ....24
6.2 Security Functional Requirements ....24
6.2.1 Security Audit – FAU ....25
6.2.2 Cryptographic Support – FCS ....26
6.2.3 User Data Protection – FDP ....29
6.2.4 Identification and Authentication – FIA ....31
6.2.5 Security Management – FMT ....31
6.2.6 Protection of the TSF – FPT ....34
6.2.7 TOE access – FTA ....35
6.2.8 Trusted Path/Channels – FTP ....35
6.3 Security Assurance Requirements ....36
6.4 Security Requirements Rationale ....37
6.4.1 Security Functional Requirements Dependencies ....37
6.4.2 Security Assurance Dependencies Analysis ....39
6.4.3 Security Functional Requirements Coverage ....40
6.4.4 Security Functional Requirements Sufficiency ....42
6.4.5 Justification of the Chosen Evaluation Assurance Level ....43
7 TOE Summary Specification ....44
7.1 TOE Security Functions ....44
7.1.1 Security Audit ....45
7.1.2 Cryptographic Support ....45
7.1.3 User Data Protection ....46
7.1.4 Identification and Authentication ....47
7.1.5 Security Management ....47
7.1.6 Protection of the TSF ....47
7.1.7 TOE access banners ....48
Appendix A – Abbreviations and Acronyms ....49

Appendix B - Referenced Documents .....50

# 1 ST Introduction

## 1.1 ST Reference

| | |
|---|---|
| **Title:** | Security Target – Saab SPNP Information Exchange Gateway |
| **Version:** | 1.12 |
| **Date:** | 2026-04-20 |
| **Editor:** | Anders Staaf, Combitech AB |

## 1.2 TOE Reference

| | |
|---|---|
| **Target of Evaluation:** | SPNP Information Exchange Gateway |
| **Version:** | 1.0.1 |
| **Date:** | 2026-01-16 |
| **Developer:** | Saab AB |

**Note**: SPNP Information Exchange Gateway is also called SPNP IEG or only IEG.

The TOE is the hardware and software of an Information Exchange Gateway.

## 1.3 Document Overview

Chapter 1 gives a description of the ST and the TOE. This description serves as an aid to understanding the security requirements and the security functions.

Chapter 2 states the conformance claims made.

Chapter 3 describes the security problem definition of the TOE. This includes assumptions about the environment of the TOE, threats against the TOE, TOE environment and organizational security policies that are to be employed to ensure the security of the TOE.

Chapter 4 describes the security objectives stated with the intent of the security functions. The security objectives are divided into two groups of security objects, for the TOE and for the TOE operational environment.

Chapter 5 defines the extended components which are then detailed in Section 6.

Chapter 6 specified the IT security functional and assurance requirements that must be satisfied by the TOE.

Chapter 7 describes how the security functional requirements are implemented in the TOE.

## 1.4 Conventions

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations, when performed on requirements that derive from CC Part 2, are identified in this ST in the following manner:

- Selection: Indicated by surrounding brackets, e.g., [selected item].

- Assignment: Indicated by surrounding brackets and italics, e.g., [*assigned item*].
- Refinement: Refined components are identified by using **bold** for additional information, or ~~strikeout~~ for deleted text.
- Iteration: Indicated by assigning a number in parenthesis to the end of the functional component identifier as well as by modifying the functional component title to distinguish between iterations, e.g., 'FDP_ACC.1(1), Subset access control (administrators)' and 'FDP_ACC.1(2) Subset access control (devices)'.

## 1.5 TOE Overview

The purpose of the SPNP Information Exchange Gateway systems (IEG) product is to form the basis of a product that can provide secure bi-directional information sharing communication between security domains of equal or different security class. The SPNP IEG supports security levels of Svensk Hemlig/Konfidentiell/Begränsad Hemlig and NATO SECRET/CONFIDENTIAL/RESTRICTED.

Interoperability, multi-national and multi-domain communication within NATO requires a large amount of IEG systems, that also drives business opportunities. As the SPNP IEG supports both network centric as well as data centric functionality for both the central and tactical scenarios, it has a great advantage over other existing technologies.

The SPNP IEG will be a critical enabler for NATO-led missions to share information about situational awareness, sensor and effector information at the tactical level. IEGs are designed to protect their own domain, and only information and services that need to be exchanged are allowed across the IEG to the other security domain. The SPNP IEG supports any land, naval and air/AEW scenario to enable cross domain communication.

The SPNP IEG will be Common Criteria EAL4+ certified, which is a prerequisite to achieve NATO accreditation.

SPNP IEG provides a common Saab technology platform that could complement, or even integrate, existing Saab network-centric security gateway solutions such as GARM (link 16 security filter) and TactiGuardXD (SIP security filter) and enhance those with the new data centric functionality by leveraging the SPNP IEG.

### 1.5.1 SPNP IEG Scenarios

NATO Federated Mission Network (FMN) improves and streamlines defence and security capabilities by leveraging technology and digitalising battlefield operations. Tactical mission networks collaborative combat requires nations to share and exchange information in real time, improving situational awareness and enabling faster and more coordinated military operations. It can include everything from shared intelligence and joint logistics to rapid communication and coordination of forces.

Information Exchange Gateway (IEG) is the NATO-selected solution for sharing information between different security levels and/or possibly operation or management domains. IEG ensures that information is shared securely between domains in multi-national FMN missions. It requires a trust model between security domains sharing information.

Security domains can be defined at the following levels;

- Strategic level, IEG will support the political consultation process enabling better NATO-national planning and more effective operations.
- Operational level, IEG support day-to-day operational planning and management
- Tactical level, IEG enables improved presentation of information and intelligence to commanders, coalition-wide sharing and understanding of commander's intent, distributed collaborative working and the networked integration of sensors, decision-makers and effectuators.

NATO defines five scenarios for interconnecting their Communication Information System (CIS) with associated requirements for the SPNP IEG;

- Scenario A: NATO to NATO Enclaves
- Scenario B: NATO to NATO Nations
- Scenario C:
  - C1: NATO to NATO Lead Mission at NATO SECRET/Mission SECRET level
  - C2: NATO Lead Mission to NATO Nations at NATO SECRET/Mission SECRET level
  - C3: NATO Lead Mission to International Organisations at NATO RESTRICTED / NATO UNCLASSIFIED level
  - C4: NATO Lead Mission to Non-NATO Nations CIS/International Organisations at NATO SECRET/Mission SECRET level
  - C5: NATO Lead Mission to Other Mission at NATO SECRET/Mission SECRET level
- Scenario D: NATO to Non-NATO Nations /International Organisations at NATO SECRET level
- Scenario E: NATO to Public Networks e.g. Internet

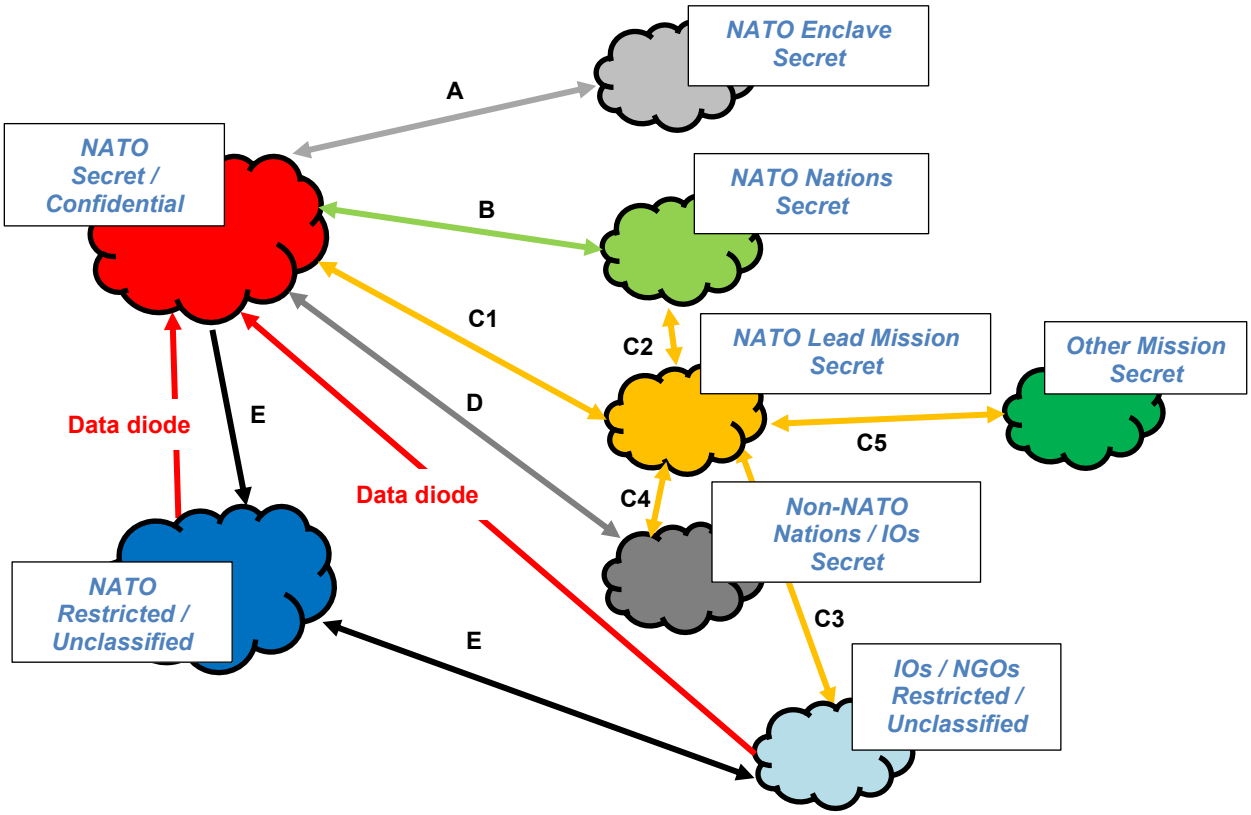



*Figure 1, NATO IEG scenarios*

## 1.6 TOE Description

### 1.6.1 System Overview

The TOE is a fully programmable network element that runs on a hardware platform that includes a hardware programmable data plane pipeline. The network element hardware, software and build environment constitutes the Programmable Trusted Network Element, PTNE.

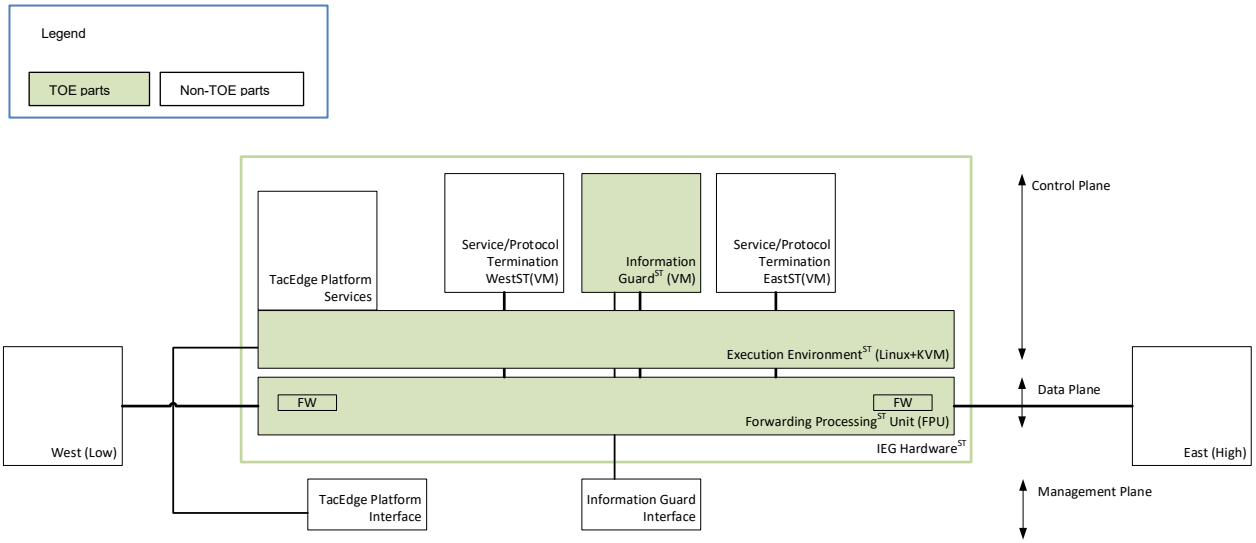



*Figure 2, TOE structure*

The TOE includes the following parts:

**Forwarding Processing Unit (FPU)** – Decides what to do with packets arriving on an inbound interface. This may result in dropping the packet, forwarding it to other ports or to the control plane. The FPU includes firewalls on both the West (high) and the East (low) sides.

**Execution Environment (CPU)** – Running Linux with KVM hypervisor.

**Information Guard** – Virtual machines used as a programmable information guards. One is for information flow low-to-high and one is for information flow high-to-low.

Management and configuration for the FPU, Execution Environment, and the Information Guard is done through Execution Environment functionality.

The virtual machines execute on the Linux KVM hypervisor. Two of the virtual machines, West and East parser/proxy are not included in the TOE.

### 1.6.2 SPNP IEG Applications and Services Supported

SPNP IEG supports several applications and services with associated protocols details. Transport/protocol specific control messages like SMTP, XMPP, REST, SOAP, HTTP/HTTPS headers and actual payload data content like XML, REST, JSON, MTF, NVG being exchanged are supported. Examples of applications supported are:

- Email (SMTP)

Parsing and proxy functionality for the services and protocols mentioned are not evaluated or tested in the evaluated configuration.

### 1.6.3 TOE States

The TOE supports two states: Operational state and Maintenance state. In Maintenance state no user data will flow through the TOE.

### 1.6.4 Roles

The TOE supports the following roles:

**User** - Uses the TOE as gateway but have no TSF privileges

**Operator** - Only allowed to read the TOE configuration

**Administrator** - Authorized for software installation and detailed configuration, except access to the security log.

**Security officer** - The security officer role is the only role that should be given access to the security log. The Security officer is also allowed to read the TOE configuration.

**User Administrator** - The User Administrator handles user management, adding and removing users, updating user configuration and reading the TOE configuration.

### 1.6.5 Physical Scope

The TOE is based on a hardware platform from APS Networks, APS BF2156X-1T. The hardware platform includes Intel Tofino Technology hosting a P4 programmable data plane pipeline.

An overview showing interfaces and major components is found in Figure 2.

TOE software is developed for the Intel Barefoot Tofino ASIC, referred to in this document as FPU, and the Intel x86 CPU, referred to in this document as CPU.

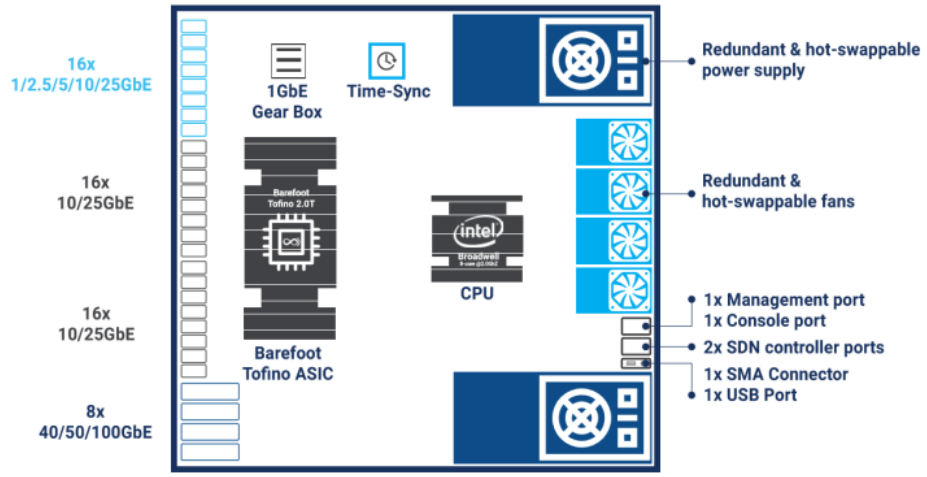



*Figure 3, TOE hardware overview*

#### 1.6.5.1 External Interfaces

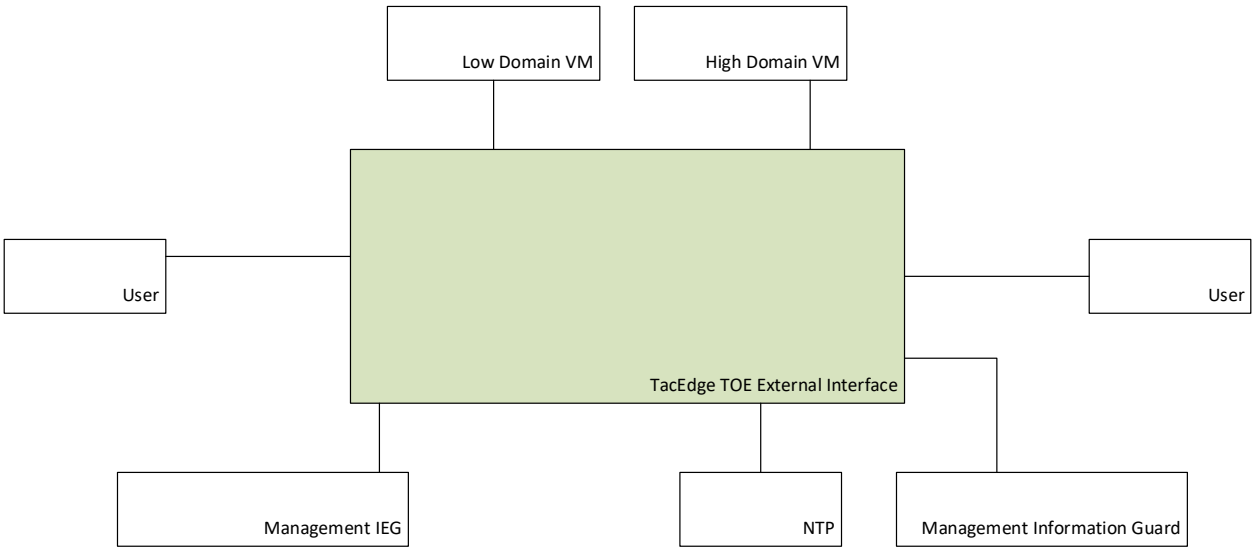



*Figure 4, TOE external interfaces*

- **Data Plane Interface**

Secure bi-directional information sharing communication of user data.

- **Low domain parser/proxy interface**

Interface to low domain parser/proxy VM.

- **High domain parser/proxy interface**

Interface to high domain parser/proxy VM.

- **Management platform interface**

The Administrator manages the TOE platform using a web-based GUI.

- **Management information guard interface**

The Administrator manages the TOE information guard using a web-based GUI.

- **Reliable time interface**

Reliable time is received from an NTP server.

An external syslog server is supported but not evaluated or tested in the evaluated configuration.

#### 1.6.5.2 Non-TOE Hardware/Software/Firmware

The TOE includes all software and hardware for SPNP IEG. It depends on the following external components:

- Web browser used for the management interfaces
    - Mozilla Firefox, 134.0.2 or later

- NTP server compliant with RFC 5905

#### 1.6.5.3 Guidance

SPNP IEG Installation Instructions for PTNE.CCC.1.0.0, T-MCI-0538, issue A, 2025-10-31, Saab.

SPNP IEG User Manual for PTNE.CCC.1.0.0, T-MCI-0543, issue A, 2025-10-31, Saab

Guidance – Saab SPNP Information Exchange Gateway 1.0, CAB-250827-120034-454, issue 0.2, 2025-11-13, Combitech

#### 1.6.5.4 Delivery

The TOE is delivered by courier with the software installed. Updated software is installed by re-installation of the TOE using a secured USB.

### 1.6.6 Logical Scope

The TOE provides the following security functionality:

#### 1.6.6.1 Security Audit

Security related event logs are generated from various sources and collected locally in a circular log record trail. Only the Security Officer has access to the event log storage. The event logs can be exported by the Security Officer in Syslog format to an external log server. External Syslog server is, however, not included in the evaluation.

#### 1.6.6.2 User Data Protection

User data flowing through the TOE is controlled according to information flow control policies for the Firewalls and the Information Guard. Rulesets for the information flow control policies are programmable throw the Management information guard interface and the Management platform interface.

#### 1.6.6.3 Identification and Authentication

Users, Administrators, Operators, Security Officers, and User Administrators have to identify and authenticate before accessing the TOE.

#### 1.6.6.4 Security management

Administrators, Operators, Security Officers, and User Administrators manage the TOE through a web-based GUI.

#### 1.6.6.5 Protection of the TSF

The integrity of the Virtual Machines is verified at startup. A secure state is preserved when critical errors are identified. The secure state disables user data traffic. The TOE is able to provide reliable time stamps. Reliable time is received from a NTP server. The hard disk is encrypted with a key stored in a hardware TPM.

#### 1.6.6.6 Trusted Path

The Management information guard interface and the Management platform interface communication is provided using HTTPS/TLS. TLS v1.2 and v1.3 are supported.

### 1.6.7 Features Excluded from the TOE

The following features will not be included in the evaluation:

- Management API
- HTTPS certificate support
- Syslog interface
- SNMP
- USB installation interface

# 2 Conformance Claims

## 2.1 CC Conformance Claim

This Security Target is conformant to Common Criteria version 2022, revision 1

- CCMB-2022-11-001, Common Criteria version CC:2022 revision 1, part 1
- CCMB-2022-11-002, Common Criteria version CC:2022 revision 1, part 2
- CCMB-2022-11-003, Common Criteria version CC:2022 revision 1, part 3
- CCMB-2022-11-004, Common Criteria version CC:2022 revision 1, part 4
- CCMB-2022-11-005, Common Criteria version CC:2022 revision 1, part 5
- ISO/IEC 15408-1, Information security, cybersecurity and privacy protection - Evaluation criteria for IT security, fourth edition, 2022-08 - Part 1
- ISO/IEC 15408-2, Information security, cybersecurity and privacy protection - Evaluation criteria for IT security, fourth edition, 2022-08 - Part 2
- ISO/IEC 15408-3, Information security, cybersecurity and privacy protection - Evaluation criteria for IT security, fourth edition, 2022-08 - Part 3
- ISO/IEC 15408-4, Information security, cybersecurity and privacy protection - Evaluation criteria for IT security, fourth edition, 2022-08 - Part 4
- ISO/IEC 15408-5, Information security, cybersecurity and privacy protection - Evaluation criteria for IT security, fourth edition, 2022-08 - Part 5

The TOE is conformant to: CC Part2 extended and CC Part3 conformant.

## 2.2 PP Conformance Claims

This Security Target does not claim compliance to any Protection Profile.

## 2.3 Package Conformance Claims

This Security Target claims conformance to assurance requirement package EAL4 augmented by ALC_FLR.1.

# 3 Security Problem Definition

## 3.1 Introduction

The security problem definition described below includes threats, organizational security policies and assumptions on the TOE operational environment.

## 3.2 Threats

Threats are described by an adverse action performed by defined threat agents on the assets that the TOE has to protect. The assets and their protection needed, the threat agents and their attack potential, and the threat adverse actions are described below.

The TOE is intended to protect information on the security levels of Svensk Hemlig/Konfidentiell/Begränsad Hemlig and NATO SECRET/CONFIDENTIAL/RESTRICTED.

| Identifier | Description |
|---|---|
| T.DATA_ACCESS | Threat agents may attempt to bypass the information flow control policy by sending information which may result in exploitation and/or compromise of protected resources, through the TOE. |
| T.UNAUTHORIZED_ ADMINISTRATOR_ACCESS | Threat agents may attempt to gain administrator access to the TOE by nefarious means. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the TOE 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.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_FAILURE | Threat agents could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device. |

*Table 1, Threats against the TOE*

### 3.3 Organizational Security Policies

Organizational security policies, OSPs, for the TOE are stated according to Table 2.

| Name | OSP |
|---|---|
| P.ACCOUNTABILITY | The TOE administrators must be accountable for their actions. |
| P.ACCESS_BANNER | The TOE must display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which administrators consent by accessing the TOE. |

*Table 2, Organizational Security Policies for the TOE*

### 3.4 Assumptions

Assumptions on the TOE operational environment are made according to Table 3.

| Name | Assumptions on the TOE operational environment |
|---|---|
| A.PHYSICAL_ PROTECTION | The TOE and its administrator management network are assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the TOE's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the TOE and the data it contains. |
| A.TRUSTED_ ADMINISTRATOR | The Security 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 to lack malicious intent when administering the device. |
| A.LIMITED_ FUNCTIONALITY | The TOE 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.RELIABLE_TIME | The TOE operational environment is assumed to provide a reliable time source. |

*Table 3, Assumptions on the TOE environment*

# 4 Security Objectives

## 4.1 Introduction

The statement of security objectives defines the security objectives for the TOE and its environment. The security objectives are intended to address all security environment aspects identified. The security objectives reflect the stated intent and are suitable to counter all identified threats and cover all identified organizational security policies and assumptions. The following categories of objectives are identified:

- The security objectives for the TOE shall be clearly stated and traced back to aspects of identified threats to be countered by the TOE and/or organizational security policies to be met by the TOE.
- The security objectives for the environment shall be clearly stated and traced back to aspects of identified threats countered by the TOE environment, organizational security policies or assumptions.

## 4.2 Security Objectives for the TOE

The following security objectives for the TOE are defined.

| Security Objective | Description |
|---|---|
| O.RESTRICTED_ACCESS | The TOE shall mediate the flow of all user data and upheld the information flow control policy between the high and low domain networks governed by the TOE. |
| O.IDENTIFICATION_ AUTHENTICATION | The TOE shall be able to identify and authenticate authorized administrators[1] prior to allowing access to TOE security management functions. |
| O.TRUSTED_PATH | The TOE shall protect confidentiality and integrity and ensure the authenticity of data passed between itself and an authorized administrator using strong encryption. |
| O.STORAGE_ ENCRYPTION | The TOE shall encrypt TSF Data stored in non-volatile storage devices. |
| O.AUDIT | The TOE shall be able to provide an audit trail of security relevant events including reliable time and identification of the subject that caused the event. An authorized administrator shall be allowed to read and manage the security event trail. |
| O.SECURE_STATE | The TOE shall protect the assets against security breaches caused by critical failures in the TOE or components in the operational environment upon which the TOE depends by entering a secure state. |

[1] Authorized administrators include all roles except User, specified in FMT_SMR.1.

| Security Objective | Description |
|---|---|
| O.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. |

*Table 4, Security objectives for the TOE*

## 4.3 Security Objectives for the Operational Environment

| Security Objective | Description |
|---|---|
| OE.PHYSICAL_PROTECTION | The TOE is physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the TOE's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the TOE and the data it contains. |
| OE.TRUSTED_ ADMINISTRATOR | The Security Administrator(s) for the TOE are trusted and act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are to lack malicious intent when administering the device. |
| OE.NO_GENERAL_ PURPOSE | The TOE provides networking functionality as its core function and does not provide functionality/services that could be deemed as general-purpose computing. For example, the device does not provide a computing platform for general purpose applications (unrelated to networking functionality). |
| OE.RELIABLE_TIME | The TOE operational environment provides a reliable time source. |

*Table 5, Security objectives for the TOE operational environment*

## 4.4 Security Objectives Rationale

### 4.4.1 Security Objectives Coverage

This section provides tracings of the security objectives for the TOE to threats, OSPs, and assumptions.

| | T.DATA_ACCESS | T.UNAUTHORIZED_ADMINISTRATOR_ACCESS | T.WEAK_CRYPTOGRAPHY | T.UNDETECTED_ACTIVITY | T.SECURITY_FUNCTIONALITY_FAILURE | P.ACCOUNTABILITY | P.ACCESS_BANNER | A.PHYSICAL_ PROTECTION | A.TRUSTED_ ADMINISTRATOR | A.LIMITED_ FUNCTIONALITY | A.RELIABLE_TIME |
|---|---|---|---|---|---|---|---|---|---|---|---|
| O.RESTRICTED_ ACCESS | X | | | | | | | | | | |
| O.IDENTIFICATION_ AUTHENTICATION | | X | | | | X | | | | | |
| O.TRUSTED_PATH | | X | X | | | | | | | | |
| O.STORAGE_ ENCRYPTION | | X | | | | | | | | | |
| O.AUDIT | | | | X | | X | | | | | |
| O.SECURE_STATE | | | | | X | | | | | | |
| O.ACCESS_BANNER | | | | | | | X | | | | |
| OE.PHYSICAL_ PROTECTION | | | | | | | | X | | | |
| OE.TRUSTED_ ADMINISTRATOR | | | | | | | | | X | | |
| OE.LIMITED_ FUNCTIONALITY | | | | | | | | | | X | |
| OE.RELIABLE_TIME | | X | | | | X | | | | | X |

*Table 6, Security objectives coverage*

### 4.4.2 Security Objectives Sufficiency

The following rationale provides justification that the security objectives for the environment are suitable to cover each individual assumption or threat to the environment, that each security objective for the environment that traces back to a threat or an assumption about the environment of use.

| Threat/OSP/Assumption | Objective | Rationale |
|---|---|---|
| T.DATA_ACCESS | O.RESTRICTED_ ACCESS | The threat is mitigated by mediating the flow of all user data and upheld the information flow control policy between the high and low domain networks governed by the TOE. |
| T.UNAUTHORIZED_ ADMINISTRATOR_ACCESS | O.IDENTIFICATION_AUTHENTIC ATION | The threat is mitigated by using a trusted path, identify and authenticate authorized administrators prior to allowing access to TOE security management functions, and hold the TSF data stored in non-volatile memory encrypted. |
| | O.TRUSTED_PATH | |
| | O.STORAGE_ENCRYPT ION | |
| T.WEAK_CRYPTOGRAPHY | O.TRUSTED_PATH | The threat is mitigated by using strong encryption. |
| T.UNDETECTED_ACTIVITY | O.AUDIT | The threat is mitigated by providing an audit trail of security relevant events where the audit records include reliable time and identification of the subject that caused the event. |
| | OE.RELIABLE_TIME | |
| T.SECURITY_ FUNCTIONALITY_FAILURE | O.SECURE_STATE | The threat is mitigated by entering a secure state when critical failures occur in the TOE or in components in its operational environment. |
| P.ACCOUNTABILITY | O.IDENTIFICATION_AUTHENTIC ATION | The threat is mitigated by providing an audit trail of security relevant events where the audit records include reliable time and identification of the subject that caused the event. |
| | O.AUDIT | |
| | OE.RELIABLE_TIME | |

| Threat/OSP/Assumption | Objective | Rationale |
|---|---|---|
| P.ACCESS_BANNER | O.ACCESS_BANNER | The OSP is met by the objective verbatim. |
| A.PHYSICAL_PROTECTION | OE.PHYSICAL_PROTECTION | The assumption is covered by the objective verbatim. |
| A.TRUSTED_ADMINISTRATOR | OE.TRUSTED_ADMINISTRATOR | The assumption is covered by the objective verbatim. |
| A.LIMITED_FUNCTIONALITY | OE.LIMITED_FUNCTIONALITY | The assumption is covered by the objective verbatim. |
| A.RELIABLE_TIME | OE.RELIABLE_TIME | The assumption is covered by the objective verbatim. |

*Table 7, Security objectives sufficiency*

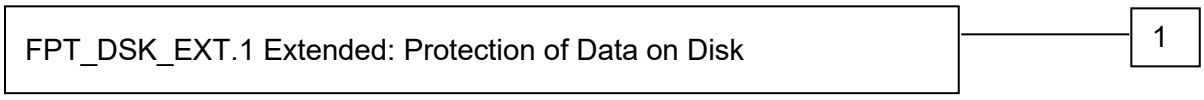
# 5 Extended Components Definition

## 5.1 FPT_DSK_EXT Extended: Protection of Data on Disk

### 5.1.1 Family Behaviour:

This family is to mandate the encryption of all protected data written to the storage.

### 5.1.2 Component Leveling:




The FPT_DSK_EXT family consists of one component: FPT_DSK_EXT.1 Extended: Protection of Data on Disk, which defines requirements for the TSF to encrypt all the Confidential TSF data stored on the Field-Replaceable Nonvolatile Storage Devices in order to avoid storing these data in plaintext on the devices.

### 5.1.3 Management:

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

a) There are no management actions foreseen.

### 5.1.4 Audit:

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.

### 5.1.5 Protection of Data on Disk – FPT_DSK_EXT.1 Extended

Hierarchical to: No other components.

Dependencies: FCS_COP.1 Cryptographic operation

**FPT_DSK_EXT.1.1** The TSF shall [selection: *perform encryption in accordance with FCS_COP.1, use a self-encrypting Field-Replaceable Nonvolatile Storage Device that is separately FIPS 140-2/3 certified.*] such that any Nonvolatile Storage Device contains no plaintext confidential TSF Data.

**FPT_DSK_EXT.1.2** The TSF shall encrypt all protected data without user intervention.

Rationale:

Protection of Data on Disk is to specify that encryption of any confidential data without user intervention, and the Common Criteria does not provide a suitable SFR for the Protection of Data on Disk.

This extended component protects the TSF data on disk, and it is therefore placed in the FPT class with a single component.

# 6 Security Requirements

## 6.1 TOE Security Functionality

The TOE functional and assurance security requirements are specified below.

## 6.2 Security Functional Requirements

| SFR | Name |
|---|---|
| FAU_GEN.1 | Audit data generation |
| FAU_STG.1 | Audit data storage location |
| FCS_CKM.1(a) | Cryptographic key generation (TLS) |
| FCS_CKM.1(b) | Cryptographic key generation (SSD Encryption/Decryption) |
| FCS_CKM.6(a) | Timing and event of cryptographic key destruction (TLS) |
| FCS_CKM.6(b) | Timing and event of cryptographic key destruction (SSD Encryption/Decryption) |
| FCS_COP.1(a) | Cryptographic operation (TLS) |
| FCS_COP.1(b) | Cryptographic operation (SSD Encryption/Decryption) |
| FCS_RBG.1 | Random bit generation (RBG) |
| FCS_RBG.3 | Random bit generation (internal seeding – single source) |
| FDP_IFC.1(a) | Subset information flow control (Information Guard) |
| FDP_IFF.1(a) | Simple security attributes (Information Guard) |
| FDP_IFC.1(b) | Subset information flow control (Firewall) |
| FDP_IFF.1(b) | Simple security attributes (Firewall) |
| FIA_UAU.2 | User authentication before any action |
| FIA_UID.2 | User identification before any action |
| FMT_MSA.1(a) | Management of security attributes (Information Guard) |
| FMT_MSA.1(b) | Management of security attributes (Firewall) |
| FMT_MSA.3(a) | Static attribute initialization (Information Guard) |
| FMT_MSA.3(b) | Static attribute initialization (Firewall) |
| FMT_MTD.1(a) | Management of TSF data (Administrator) |
| FMT_MTD.1(b) | Management of TSF data (Operator) |
| FMT_MTD.1(c) | Management of TSF data (Security officer) |
| FMT_MTD.1(d) | Management of TSF data (User Administrator) |
| FMT_SMF.1 | Specification of Management Functions |
| FMT_SMR.1 | Security roles |
| FPT_DSK_EXT.1 | Protection of Data on Disk |
| FPT_FLS.1 | Failure with preservation of secure state |

| SFR | Name |
|---|---|
| FPT_STM.1 | Reliable time stamps |
| FPT_TST.1 | TSF self-testing |
| FTA_TAB.1 | TOE access banners |
| FTP_TRP.1 | Trusted path |
| FTP_ITC.1 | Inter-TSF trusted channel |

*Table 8, Security Functional Requirements*

### 6.2.1 Security Audit – FAU

#### 6.2.1.1 Audit data generation – FAU_GEN.1

Hierarchical to: No other components.
Dependencies: FPT_STM.1 Reliable time stamps

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

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

b) All auditable events for the [not specified] level of audit;

c) [*auditable events specified in Table 9*.

| SFR | Auditable Event | Additional Information |
|---|---|---|
| FAU_GEN.1 | --- | --- |
| FAU_STG.1 | Warning or failure to store log events locally | Log partition full,<br>log partition almost full,<br>unrotated log file,<br>log partition not mounted |
| FCS_CKM.1(a), (b) | --- | --- |
| FCS_CKM.6(a), (b) | --- | --- |
| FCS_COP.1(a), (b) | --- | --- |
| FCS_RBG.1 | --- | --- |
| FCS_RBG.3 | --- | --- |
| FDP_IFC.1(a) | --- | --- |
| FDP_IFF.1(a) | --- | --- |
| FDP_IFC.1(b) | --- | --- |
| FDP_IFF.1(b) | --- | --- |
| FIA_UAU.2 | Authentication success or failure | Subject identity |
| FIA_UID.2 | Identification success or failure | Subject identity |
| FMT_MSA.1(a) | Configuration change | Changed configuration item |
| FMT_MSA.1(b) | Configuration change | Changed configuration item |
| FMT_MSA.3(a) | --- | --- |

| SFR | Auditable Event | Additional Information |
|---|---|---|
| FMT_MSA.3(b) | --- | --- |
| FMT_MTD.1(a) | Configuration change | Changed configuration item |
| FMT_MTD.1(b) | Configuration change | Changed configuration item |
| FMT_MTD.1(c) | Configuration change | Changed configuration item |
| FMT_MTD.1(d) | Configuration change | Changed configuration item |
| FMT_SMF.1 | Configuration change | Changed configuration item |
| FMT_SMR.1 | Role administration | User added,<br>user removed,<br>changed user role |
| FPT_DSK_EXT.1 | --- | --- |
| FPT_FLS.1 | Hardware or software related error/warning | Change of state,<br>reason of error/warning |
| FPT_STM.1 | NTP not synchronized | Lost synchronization,<br>Restart of NTP daemon |
| FPT_TST.1 | Test failure | Reason for failure |
| FTA_TAB.1 | --- | --- |
| FTP_TRP.1 | Trusted path failure | Reason for the failure |
| FTP_ITC.1 | Trusted channel failure | Reason for the failure |

*Table 9, Auditable events*

].

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each auditable event type, based on the auditable event definitions of the functional components included in the PP, PP-Module, functional package or ST, [*information specified in Table 9*].

### 6.2.1.2 Audit data storage location – FAU_STG.1

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation
FTP_ITC.1 Inter-TSF trusted channel

**FAU_STG.1.1** The TSF shall be able to store generated audit data on the [TOE itself].

## 6.2.2 Cryptographic Support – FCS

### 6.2.2.1 Cryptographic key generation – FCS_CKM.1 (a) TLS

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or

FCS_COP.1 Cryptographic operation]
FCS_CKM.3 Cryptographic key access
[FCS_RBG.1 Random bit generation, or
FCS_RNG.1 Generation of random numbers]
FCS_CKM.6 Timing and event of cryptographic key destruction

**FCS_CKM.1.1(a)** The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*as specified in Table 10*] and specified cryptographic key sizes [*as specified in Table 10*] that meet the following: [*standards as specified in Table 10*].

| Algorithm | Key Size | Standard |
|---|---|---|
| RSA | 2048, 4096 bits | FIPS 186-4, Appendix B |
| AES | 128, 256 bits | FIPS 197 |
| ChaCha20-Poly1305 | 256 bits | RFC8439 |
| TLS key generation via ECDHE | AES 128, 256 bits | SP 800-135 Rev.1 |
| TLS key generation via ECDHE | HMAC 160, 256, 384 bits | SP 800-135 Rev.1 |

*Table 10, Key generation, TLS*

### 6.2.2.2 Cryptographic key generation – FCS_CKM.1 (b) SSD Encryption/Decryption

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.3 Cryptographic key access
[FCS_RBG.1 Random bit generation, or
FCS_RNG.1 Generation of random numbers]
FCS_CKM.6 Timing and event of cryptographic key destruction

**FCS_CKM.1.1(b)** The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*as specified in Table 11*] and specified cryptographic key sizes [*as specified in Table 11*] that meet the following: [*standards as specified in Table 11*].

| Algorithm | Key Size | Standard |
|---|---|---|
| AES | 256 bits | FIPS 197 |

*Table 11, Key generation, SSD encryption*

### 6.2.2.3 Timing and event of cryptographic key destruction – FCS_CKM.6 (a) TLS

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

**FCS_CKM.6.1(a)** The TSF shall destroy [*TLS session and ephemeral keys*] when [no longer needed].

**FCS_CKM.6.2(a)** The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method [*volatile memory power off*] that meets the following: [*no standard*].

### 6.2.2.4 Timing and event of cryptographic key destruction – FCS_CKM.6 (b) SSD Encryption/Decryption

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

**FCS_CKM.6.1(b)** The TSF shall destroy [*the SSD encryption/decryption key created in volatile memory*] when [*transferred to a hardware TPM*].

**FCS_CKM.6.2(b)** The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method [*volatile memory power off*] that meets the following: [*no standard*].

### 6.2.2.5 Cryptographic operation – FCS_COP.1 (a) TLS

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.3 Cryptographic key access

**FCS_COP.1.1(a)** The TSF shall perform [*cryptographic operations as specified in Table 12*] in accordance with a specified cryptographic algorithm [*as specified in Table 12*] and cryptographic key sizes [*as specified in Table 12*] that meet the following: [*standards as specified in Table 12*].

| Operation | Algorithm | Key/Hash Bit Size | Standard |
|---|---|---|---|
| Encryption, decryption | AES (CBC mode) | 256, 384 bits | FIPS 197<br>SP800-38A<br>SP800-38D |
| | AES (GCM mode) | | |
| | ChaCha20-Poly1305 | 256 bits | RFC8439 |
| Cryptographic Signature | RSA Digital Signature Algorithm<br>RSASSA-PKCS1-v1_5 | 2048, 4096 bits | PKCS #1 v2.2<br>FIPS 186-4 |
| Hashing | SHA-256, SHA-384 | 256, 384 bits | FIPS 180-4 |
| Keyed Hash Message Authentication Code | HMAC-SHA-256, HMAC-SHA-384 | 256, 384 bits | RFC 2104 |

*Table 12, Cryptographic operations, TLS*

### 6.2.2.6 Cryptographic operation – FCS_COP.1 (b) SSD Encryption/Decryption

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation, or
FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.3 Cryptographic key access

**FCS_COP.1.1(b)** The TSF shall perform [*encryption, decryption*] in accordance with a specified cryptographic algorithm [*AES-GCM*] and cryptographic key sizes [*256*] that meet the following: [*FIPS 197, SP800-38D*].

### 6.2.2.7 Random bit generation (RBG) – FCS_RBG.1

Hierarchical to: No other components.

Dependencies: [FCS_RBG.2 Random bit generation (external seeding), or
FCS_RBG.3 Random bit generation (internal seeding – single source)]
FPT_FLS.1 Failure with preservation of secure state
FPT_TST.1 TSF self-testing

**FCS_RBG.1.1** The TSF shall perform deterministic random bit generation services using [*CSPRNG*] in accordance with [*no standards*] after initialization with a seed.

**FCS_RBG.1.2** The TSF shall use a [TSF noise source [*environmental noise collected from device drivers*] for initialized seeding.

**FCS_RBG.1.3** The TSF shall update the RBG state by [reseeding] using a [TSF noise source [*environmental noise collected from device drivers*] in the following situations: [on the condition: [*Reboot*]] in accordance with [*no standards*].

### 6.2.2.8 Random bit generation (internal seeding – single source) – FCS_RBG.3

Hierarchical to: No other components.

Dependencies: FCS_RBG.1 Random bit generation (RBG)

**FCS_RBG.3.1** The TSF shall be able to seed the RBG using a [TSF hardware-based noise source] [*environmental noise collected from device drivers*] with a minimum of [*256*] bits of min-entropy.

## 6.2.3 User Data Protection – FDP

### 6.2.3.1 Subset information flow control – FDP_IFC.1(a) - Information Guard

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

**FDP_IFC.1.1(a)** The TSF shall enforce the [*Information Guard information flow control SFP*] on [

*Subjects:* *Originator entity, destination entity*

*Information:* *User data aimed to pass through the TOE*

*Operations:* *User data sent from the originator entity mediated by the TOE and aimed at the destination entity.*

].

#### 6.2.3.2 Simple security attributes – FDP_IFF.1(a) - Information Guard

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute

**FDP_IFF.1.1(a)** The TSF shall enforce the [*Information Guard information flow control SFP*] based on the following types of subject and information security attributes: [

*Subjects:*
*Originator entity, attribute: Category tags*
*Destination entity, attribute: Category tags*

*Information:*
*User data aimed to pass through the TOE, attributes:*
*- Information classification*
*- Category tags*

].

**FDP_IFF.1.2(a)** The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

*Originator entity and destination entity category tags comply with the information classification and category tags according to the Security Policy defined in the Security Policy Information File, SPIF*].

**FDP_IFF.1.3(a)** The TSF shall enforce ~~the~~ [*no additional information flow control SFP rules*].

**FDP_IFF.1.4(a)** The TSF shall explicitly authorize an information flow based on the following rules: [*None*].

**FDP_IFF.1.5(a)** The TSF shall explicitly deny an information flow based on the following rules: [*None*].

**Application note:** For information about Security Policies and SPIF, see https://www.xmlspif.org.

#### 6.2.3.3 Subset information flow control – FDP_IFC.1(b) - Firewall

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

**FDP_IFC.1.1(b)** The TSF shall enforce the *[Firewall information flow control SFP*] on [

*Subjects:* *Source entity, destination entity*

*Information:* *IP protocol packets*

*Operations:* *All operations that cause controlled information to flow to and from controlled subjects covered by the SFP]*.

#### 6.2.3.4 Simple security attributes – FDP_IFF.1(b) - Firewall

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute

**FDP_IFF.1.1(b)** The TSF shall enforce the [*Firewall information flow control SFP*] based on the following types of subject and information security attributes: [

*Subject attributes:*
*- Source physical port*

*- Destination physical port*
*- Source logical port*
*- Destination logical port*
*- Source MAC address*
*- Destination MAC address*
*- Source IP address*
*- Destination IP address*
*- VLAN*

*Information attributes:*
*- Ethernet protocol*
*- IP protocol*]

**FDP_IFF.1.2(b)** The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

*An information flow is permitted if no denying access control rule is defined for any of the subject and information attributes or any combination of those attributes.*

**]**.

**FDP_IFF.1.3(b)** The TSF shall enforce ~~the~~ [*no additional information flow control SFP rules*].

**FDP_IFF.1.4(b)** The TSF shall explicitly authorize an information flow based on the following rules: [*None*].

**FDP_IFF.1.5(b)** The TSF shall explicitly deny an information flow based on the following rules:

[*None*].

### 6.2.4 Identification and Authentication – FIA

#### 6.2.4.1 User authentication before any action – FIA_UAU.2

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

**FIA_UAU.2.1** The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

#### 6.2.4.2 User identification before any action – FIA_UID.2

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies

**FIA_UAU.2.1** The TSF shall require each user to be successfully identified before allowing any TSF-mediated actions on behalf of that user.

### 6.2.5 Security Management – FMT

#### 6.2.5.1 Management of security attributes – FMT_MSA.1(a) - Information Guard

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

**FMT_MSA.1.1** The TSF shall enforce the [*Information Guard information flow control SFP*] to restrict the ability to [*change_default, query, modify, delete*, [*export, import*]] the security attributes [*all security attributes*] to [*the Administrator*].

#### 6.2.5.2 Management of security attributes – FMT_MSA.1(b) - Firewall

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

**FMT_MSA.1.1** The TSF shall enforce the [*Firewall information flow control SFP*] to restrict the ability [*change_default, query, modify, delete*, [*export, import*]] the security attributes [*all security attributes*] to [*the Administrator*].

#### 6.2.5.3 Static attribute initialization – FMT_MSA.3(a) - Information Guard

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

**FMT_MSA.3.1** The TSF shall enforce the [*Information Guard information flow control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

#### 6.2.5.4 Static attribute initialization – FMT_MSA.3(b) - Firewall

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

**FMT_MSA.3.1** The TSF shall enforce the [*Firewall information flow control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

#### 6.2.5.5 Management of TSF data – FMT_MTD.1(a) - Administrator

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

**FMT_MTD.1.1(a)** The TSF shall restrict the ability to [change_default, query, modify, delete, clear, [*export, import, send ping*]] the [*all TSF data except the security log]* to [*the Administrator*].

#### 6.2.5.6 Management of TSF data – FMT_MTD.1(b) - Operator

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

**FMT_MTD.1.1(b)** The TSF shall restrict the ability to [query, modify, [*export, send ping*]] the [*following TSF data from*

- *Status pages:*

- *View (GET) System Status*
- *View Chassis, Temperatures, Fan Speeds*
- *View Port Status, LACP Status, Transceivers, Packet Counters, Drop Counters*
- *View MAC Entries*
- *View IGMP Snooping Status*
- *View Routing Drop Counters, ARP Cache*
- *View External Access IP address*
- *View NTP Status*
- *Export Platform Diagnostics (encrypted file)*
- *Perform Management and Data Plane Ping*

- *Management Pages:*
  - *View Configuration for External Access, Data Plane Access, HTTPS Certificate*
  - *View Syslog Configuration*
  - *View NTP Configuration*
  - *View SNMP Configuration*
  - *View Radius Configuration*
- *Data Plane Pages:*
  - *View Physical Ports Configuration*
  - *View Logical Ports Configuration*
  - *View VLAN Configuration and VLAN Status*
  - *View Switching ACL Rules and Default Policy*
  - *View Port Mirroring Configuration*
  - *View IGMP Snooping Configuration*
  - *View Routing Configuration*
  - *View Routing ACL Rules and Default Policy*
  - *View DHCP Server Configuration*
  - *View Secure Bypass Configuration*
- *Virtual Machines Pages:*
  - *View Media Files*
  - *View VM Configurations*
- *About Pages:*
  - *View Third-Party Licenses*
- *Account Pages:*
  - *Change User Password*

] ~~to~~ **for the** [*the Operator*].

**Application note**: No operations on TSF data are restricted to the Operator only. The Operator is restricted to the operations listed above. The Administrator has capability to manage all TSF data, i.e., also the operations listed above.

### 6.2.5.7 Management of TSF data – FMT_MTD.1(c) – Security Officer

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

**FMT_MTD.1.1(c)** The TSF shall restrict the ability to [query, modify, delete, clear] the [event log] to [*the Security officer*].

### 6.2.5.8 Management of TSF data – FMT_MTD.1(d) – User Administrator

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

**FMT_MTD.1.1(d)** The TSF shall restrict the ability to [query, modify, delete, clear] the [TSF data regarding user management] to [*the User Administrator*].

#### 6.2.5.9 Specification of Management Functions – FMT_SMF.1

Hierarchical to: No other components.

Dependencies: No dependencies.

**FMT_SMF.1.1** The TSF shall be capable of performing the following management functions: [
*- Query TOE status information;*
*- Apply configuration changes;*
*- Handle user identification, authentication, and role parameters*
*- Export/import configuration items*
*- Restart the TOE.*
].

#### 6.2.5.10 Security roles – FMT_SMR.1

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

**FMT_SMR.1.1** The TSF shall maintain the roles [*User, Operator, Administrator, Security officer, User Administrator*].

**FMT_SMR.1.2** The TSF shall be able to associate users with roles.

#### 6.2.5.11 Protection of Data on Disk – FPT_DSK_EXT.1 Extended

Hierarchical to: No other components.

Dependencies: FCS_COP.1 Cryptographic operation

**FPT_DSK_EXT.1.1** The TSF shall [*perform encryption in accordance with FCS_COP.1*] such that any Nonvolatile Storage Device contains no plaintext confidential TSF Data.

**FPT_DSK_EXT.1.2** The TSF shall encrypt all protected data without user intervention.

### 6.2.6 Protection of the TSF – FPT

#### 6.2.6.1 Failure with preservation of secure state – FPT_FLS.1

Hierarchical to: No other components.

Dependencies: No dependencies.

**FPT_FLS.1.1** The TSF shall preserve a secure state when the following types of failures occur: [

- Controller not able to function
- Driver communicating with switching function in dataplane (FPU) not functioning

].

#### 6.2.6.2 Reliable time stamps – FPT_STM.1

Hierarchical to: No other components.

Dependencies: No dependencies.

**FPT_STM.1.1** The TSF shall be able to provide reliable time stamps.

#### 6.2.6.3 TSF self-testing – FPT_TST.1

Hierarchical to: No other components.

Dependencies: No dependencies.

**FPT_TST.1.1** The TSF shall run a suite of the following self-tests [during initial start-up] to demonstrate the correct operation of [[*TSF software and configuration*]: [*Integrity verification*]].

**FPT_TST.1.2** The TSF shall provide authorized users with the capability to verify the integrity of [ [*no parts of TSF data*]].

**FPT_TST.1.3** The TSF shall provide authorized users with the capability to verify the integrity of [ [*no parts of the TSF*]].

### 6.2.7 TOE access – FTA

#### 6.2.7.1 Default TOE access banners – FTA_TAB.1

Hierarchical to: No other components.

Dependencies: No dependencies.

**FTA_TAB.1.1** Before establishing a user session, the [TSF] shall display an [*text describing restrictions of use, legal agreements, or any other appropriate information to which administrators consent by accessing the TOE*] message.

### 6.2.8 Trusted Path/Channels – FTP

#### 6.2.8.1 Inter-TSF trusted channel – FTP_ITC.1

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

**FTP_ITC.1.3** The TSF shall initiate communication via the trusted channel for [cross-domain communications by implementing mTLS].

#### 6.2.8.2 Trusted path – FTP_TRP.1

Hierarchical to: No other components.

Dependencies: No dependencies.

**FTP_TRP.1.1** The TSF shall provide a communication path between itself and [local] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].

**FTP_TRP.1.2** The TSF shall permit [local users] to initiate communication via the trusted path.

**FTP_TRP.1.3** The TSF shall require the use of the trusted path for [initial user authentication, [management of TOE]].

## 6.3 Security Assurance Requirements

The security assurance requirements according to Table 13 have been chosen. The comprise EAL4 augmented by ALC_FLR.1.

| Assurance Class | SAR | Name |
|---|---|---|
| ADV: Development | ADV_ARC.1 | Security architecture description |
| | ADV_FSP.4 | Complete functional specification |
| | ADV_IMP.1 | Implementation representation of the TSF |
| | ADV_TDS.3 | Basic modular design |
| AGD: Guidance documents | AGD_OPE.1 | Operational user guidance |
| | AGD_PRE.1 | Preparative procedures |
| ALC: Life-cycle support | ALC_CMC.4 | Production support, acceptance procedures and automation |
| | ALC_CMS.4 | Problem tracking CM coverage |
| | ALC_DEL.1 | Delivery procedures |
| | ALC_DVS.1 | Identification of security controls |
| | ALC_FLR.1 | Basic flaw remediation |
| | ALC_LCD.1 | Developer defined life-cycle processes |
| | ALC_TAT.1 | Well-defined development tools |
| ASE: Security Target evaluation | ASE_CCL.1 | Conformance claims |
| | ASE_ECD.1 | Extended components definition |
| | ASE_INT.1 | ST introduction |
| | ASE_OBJ.2 | Security objectives |
| | ASE_REQ.2 | Derived security requirements |
| | ASE_SPD.1 | Security problem definition |
| | ASE_TSS.1 | TOE summary specification |
| ATE: Tests | ATE_COV.2 | Analysis of coverage |
| | ATE_DPT.1 | Testing: basic design |
| | ATE_FUN.1 | Functional testing |

| Assurance Class | SAR | Name |
|---|---|---|
| | ATE_IND.2 | Independent testing – sample |
| AVA: Vulnerability assessment | AVA_VAN.3 | Focused vulnerability analysis |

*Table 13, Security Assurance Requirements*

## 6.4 Security Requirements Rationale

### 6.4.1 Security Functional Requirements Dependencies

| Requirement | Direct explicit dependencies | Dependencies met by | Comment |
|---|---|---|---|
| FAU_GEN.1 | FPT_STM.1 | FPT_STM.1 | |
| FAU_STG.1 | FAU_GEN.1<br>FTP_ITC.1 | FAU_GEN.1 | FTP_ITC.1: Event log export is not included in the evaluation. |
| FCS_CKM.1(a) | [FCS_CKM.2 or FCS_CKM.5 or FCS_COP.1]<br>FCS_CKM.3<br>[FCS_RBG.1 or FCS_RNG.1]<br>FCS_CKM.6 | FCS_COP.1(a)<br>FCS_RBG.<br>FCS_CKM.6(a) | FCS_CKM.3: Cryptographic keys are not used outside of the TOE. |
| FCS_CKM.1(b) | [FCS_CKM.2 or FCS_CKM.5 or FCS_COP.1]<br>FCS_CKM.3<br>[FCS_RBG.1 or FCS_RNG.1]<br>FCS_CKM.6 | FCS_COP.1(b)<br>FCS_RBG.<br>FCS_CKM.6(b) | FCS_CKM.3: Cryptographic keys are not used outside of the TOE. |
| FCS_CKM.6(a) | [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] | FCS_CKM.1(a) | |
| FCS_CKM.6(b) | [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] | FCS_CKM.1(b) | |
| FCS_COP.1(a) | [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5]<br>FCS_CKM.3 | FCS_CKM.1(a) | FCS_CKM.3: Cryptographic keys are not used outside of the TOE. |
| FCS_COP.1(b) | [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5] | FCS_CKM.1(b) | FCS_CKM.3: Cryptographic keys are not used outside of the TOE. |

| Requirement | Direct explicit dependencies | Dependencies met by | Comment |
|---|---|---|---|
| | FCS_CKM.3 | | |
| FCS_RBG.1 | [FCS_RBG.2 or FCS_RBG.3]<br>FPT_FLS.1<br>FPT_TST.1 | FCS_RBG.3<br>FPT_FLS.1<br>FPT_TST.1 | |
| FCS_RBG.3 | FCS_RBG.1 | FCS_RBG.1 | |
| FDP_IFC.1(a) | FDP_IFF.1 | FDP_IFF.1 (a) | |
| FDP_IFF.1(a) | FDP_IFC.1<br>FMT_MSA.3 | FDP_IFC.1 (a)<br>FMT_MSA.3 (a) | |
| FDP_IFC.1(b) | FDP_IFF.1 | FDP_IFF.1 (b) | |
| FDP_IFF.1(b) | FDP_IFC.1<br>FMT_MSA.3 | FDP_IFC.1 (b)<br>FMT_MSA.3 (b) | |
| FIA_UAU.2 | FIA_UID.1 | FIA_UID.2 | FIA_UID.2 is hierarchical to FIA_UID.1 |
| FIA_UID.2 | No dependencies | --- | --- |
| FMT_MSA.1(a) | [FDP_ACC.1 or FDP_IFC.1]<br>FMT_SMR.1<br>FMT_SMF.1 | FDP_IFC.1(a)<br>FMT_SMR.1<br>FMT_SMF.1 | |
| FMT_MSA.1(b) | [FDP_ACC.1 or FDP_IFC.1]<br>FMT_SMR.1<br>FMT_SMF.1 | FDP_IFC.1(b)<br>FMT_SMR.1<br>FMT_SMF.1 | |
| FMT_MSA.3(a) | FMT_MSA.1<br>FMT_SMR.1 | FMT_MSA.1(a)<br>FMT_SMR.1 | |
| FMT_MSA.3(b) | FMT_MSA.1<br>FMT_SMR.1 | FMT_MSA.1(b)<br>FMT_SMR.1 | |
| FMT_MTD.1(a), (b), (c), (d) | FMT_SMR.1<br>FMT_SMF.1 | FMT_SMR.1<br>FMT_SMF.1 | |
| FMT_SMF.1 | No dependencies | --- | --- |
| FMT_SMR.1 | FIA_UID.1 | FIA_UID.2 | FIA_UID.2 is hierarchical to FIA_UID.1 |
| FPT_DSK_EXT.1 | FCS_COP.1 | FCS_COP.1 | |
| FPT_FLS.1 | No dependencies | --- | --- |
| FPT_STM.1 | No dependencies | --- | --- |
| FPT_TST.1 | No dependencies | --- | --- |
| FTA_TAB.1 | No dependencies | --- | --- |

| Requirement | Direct explicit dependencies | Dependencies met by | Comment |
|---|---|---|---|
| FTP_TRP.1 | No dependencies | --- | --- |
| FTP_ITC.1 | No dependencies | --- | --- |

*Table 14, SFR dependencies*

According to Table 14 all applicable dependencies are met.

### 6.4.2 Security Assurance Dependencies Analysis

The chosen evaluation assurance level EAL4 augmented by ALC_FLR.1. Since all dependencies are met internally by the EAL package only the augmented the assurance components dependencies are analyzed.

| Assurance Component | Dependencies | Comment |
|---|---|---|
| ALC_FLR.1 | No dependencies | --- |

*Table 15, Security Assurance Dependencies Analysis*

According to Table 15 all dependencies are met.

### 6.4.3 Security Functional Requirements Coverage

| | O.RESTRICTED_ACCESS | O.IDENTIFICATION_AUTHENTICATION | O.TRUSTED_PATH | O.STORAGE _ENCRYPTI ON | O.AUDIT | O.SECURE_STATE | O.ACCESS_BANNER |
|---|---|---|---|---|---|---|---|
| FAU_GEN.1 | | | | | X | | |
| FAU_STG.1 | | | | | X | | |
| FCS_CKM.1(a) | | | X | | | | |
| FCS_CKM.1(b) | | | | X | | | |
| FCS_CKM.6(a) | | | X | | | | |
| FCS_CKM.6(b) | | | | X | | | |
| FCS_COP.1(a) | | | X | | | | |
| FCS_COP.1(b) | | | | X | | | |
| FCS_RBG.1 | | | X | X | | | |
| FCS_RBG.3 | | | X | X | | | |
| FDP_IFC.1(a) | X | | | | | | |
| FDP_IFF.1(a) | X | | | | | | |
| FDP_IFC.1(b) | X | | | | | | |
| FDP_IFF.1(b) | X | | | | | | |
| FIA_UAU.2 | | X | | | | | |
| FIA_UID.2 | | X | | | | | |
| FMT_MSA.1(a) | X | | | | | | |
| FMT_MSA.1(b) | X | | | | | | |
| FMT_MSA.3(a) | X | | | | | | |
| FMT_MSA.3(b) | X | | | | | | |
| FMT_MTD.1(a) | X | | | | | | |
| FMT_MTD.1(b) | X | | | | | | |
| FMT_MTD.1(c) | | | | | X | | |
| FMT_MTD.1(d) | | X | | | | | |
| FMT_SMF.1 | X | | | | X | X | |
| FMT_SMR.1 | | X | | | | | |

| | O.RESTRICTED_ACCESS | O.IDENTIFICATION_AUTHENTICATION | O.TRUSTED_PATH | O.STORAGE_ENCRYPTION | O.AUDIT | O.SECURE_STATE | O.ACCESS_BANNER |
|---|---|---|---|---|---|---|---|
| FPT_DSK_EXT.1 | | | | X | | | |
| FPT_FLS.1 | | | | | | X | |
| FPT_STM.1 | | | | | X | | |
| FPT_TST.1 | | | | | | X | |
| FTA_TAB.1 | | | | | | | X |
| FTP_TRP.1 | | | X | | | | |
| FTP_ITC.1 | | | X | | | | |

*Table 16, Security Functional Requirements Coverage*

### 6.4.4 Security Functional Requirements Sufficiency

| Objective | SFR | Rationale |
|---|---|---|
| O.RESTRICTED_ACCESS | FDP_IFC.1(a)<br>FDP_IFF.1(a)<br>FDP_IFC.1(b)<br>FDP_IFF.1(b)<br>FMT_MSA.1(a)<br>FMT_MSA.1(b)<br>FMT_MSA.3(a)<br>FMT_MSA.3(b)<br>FMT_MTD.1(a)<br>FMT_MTD.1(b)<br>FMT_SMF.1 | The TOE mediates the flow of all user data and upheld the information flow control policies between the high and low domain networks governed by the TOE. The Administrator and Operator have privileges to manage the information flow control policies. |
| O.IDENTIFICATION_AUTHENTICATION | FIA_UAU.2<br>FIA_UID.2<br>FMT_MTD.1(d)<br>FMT_SMR.1 | The TOE identifies and authenticates authorized administrators prior to allowing access to TOE security management functions. The TOE users are connected to roles. The User Administrator is allowed to add, remove, and configure user accounts. |
| O.TRUSTED_PATH | FCS_CKM.1(a)<br>FCS_CKM.6(a)<br>FCS_COP.1(a)<br>FCS_RBG.1<br>FCS_RBG.3<br>FTP_TRP.1<br>FTP_ITC.1 | The TOE protects confidentiality and integrity and ensure the authenticity of data passed between itself and an authorized administrator and between itself and another trusted IT product, using strong encryption. |
| O.STORAGE _ENCRYPTI ON | FCS_CKM.1(b)<br>FCS_CKM.6(b)<br>FCS_COP.1(b)<br>FCS_RBG.1<br>FCS_RBG.3<br>FPT_DSK_EXT.1 | The TOE encrypts TSF Data stored in non-volatile storage devices. |
| O.AUDIT | FAU_GEN.1<br>FAU_STG.1<br>FMT_MTD.1(c)<br>FMT_SMF.1<br>FPT_STM.1 | The TOE provides an audit trail of security relevant events including reliable time and identification of the subject that caused the event. An authorized administrator shall be allowed to manage the security event trail. |
| O.SECURE_STATE | FMT_SMF.1<br>FPT_FLS.1<br>FPT_TST.1 | The TOE protects the assets against security breaches caused by critical failures in the TOE or components in the operational |

| Objective | SFR | Rationale |
|---|---|---|
| | | environment upon which the TOE depends on entering a secure state. The Administrator is allowed to restart the TOE after the failure has been fixed. |
| O.ACCESS_BANNER | FTA_TAB.1 | The TOE displays an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which administrators consent by accessing the TOE. |

*Table 17, Security Functional Requirements Sufficiency*

### 6.4.5 Justification of the Chosen Evaluation Assurance Level

The assurance level EAL4 augmented with ALC_FLR.1 has been chosen as appropriate for an Information Exchange Gateway supporting security levels of Svensk Hemlig/Konfidentiell/Begränsad Hemlig and NATO SECRET/CONFIDENTIAL/RESTRICTED.

# 7 TOE Summary Specification

This section presents information to how the TOE meets the functional requirements described in previous sections of this ST.

## 7.1 TOE Security Functions

Each of the security requirements and the associated descriptions correspond to security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements. Table 18 lists the security functions and their associated SFRs.

| TOE Security Function | SFR |
|---|---|
| Security audit | FAU_GEN.1 |
| | FAU_STG.1 |
| Cryptographic support | FCS_CKM.1(a) (b) |
| | FCS_CKM.6(a) (b) |
| | FCS_COP.1(a) (b) |
| | FCS_RBG.1 |
| | FCS_RBG.3 |
| User data protection | FDP_IFC.1(a) |
| | FDP_IFF.1(a) |
| | FDP_IFC.1(b) |
| | FDP_IFF.1(b) |
| Identification and authentication | FIA_UAU.2 |
| | FIA_UID.2 |
| Security management | FMT_MSA.1(a) |
| | FMT_MSA.1(b) |
| | FMT_MSA.3(a) |
| | FMT_MSA.3(b) |
| | FMT_MTD.1(a) |
| | FMT_MTD.1(b) |
| | FMT_MTD.1(c) |
| | FMT_MTD.1(d) |
| | FMT_SMF.1 |
| | FMT_SMR.1 |
| Protection of the TSF | FPT_DSK_EXT.1 |
| | FPT_FLS.1 |

| TOE Security Function | SFR |
|---|---|
| | FPT_STM.1 |
| | FPT_TST.1 |
| TOE access banners | FTA_TAB.1 |
| Trusted path | FTP_TRP.1<br>FTP_ITC.1 |

*Table 18, TOE Security Functions*

### 7.1.1 Security Audit

Records of security related events are written to a local log trail in persistent memory. The log records are structured according to the Syslog Protocol (RFC 5424). The oldest log entry is overwritten if the log trail gets full. A warning is logged and shown at the management GUI when 25% of the log trail space remains. A warning is also produced if the log trail turns around.

Only the Security officer can access and manage the log records.

### 7.1.2 Cryptographic Support

The TOE supports cryptographic operations for the functions described below. OpenSSL v3.0.7 is used by the TOE.

#### 7.1.2.1 Random Bit Generation

The TSF uses Linux */dev/random* functions to generate random numbers for key generation. It also uses OpenSSL *rand* function that on a Linux deployment uses Linux random functions. The entropy source is environmental noise collected from device drivers. The /*dev/random* function is blocked until enough entropy is collected, typically during boot. The functions provide 256 bits security.

#### 7.1.2.2 Trusted Path

A trusted path using HTTPS/TLS is established to the administrative web GUI.

Only TLS v1.2 (RFC5246) and TLS v1.3 (RFC8446) are supported with the following cipher suites:

TLS v1.2:
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_256_CCM_8
TLS_RSA_WITH_AES_256_CCM

TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_128_CCM_8
TLS_RSA_WITH_AES_128_CCM
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256

TLS v1.3:
TLS_AES_256_GCM_SHA384
TLS_AES_128_GCM_SHA256
TLS_AES_128_CCM_SHA256

The cryptographic keys used for TLS are stored in volatile memory and destroyed at power off.

#### 7.1.2.3 Trusted Channel

A trusted channel using mTLS is established to other trusted IT products. X.509 certificates and private RSA 2048- or 4096-bits keys according to RFC 5280 are used.

#### 7.1.2.4 SSD Encryption/Decryption

The SSD disk storage used for TSF data is encrypted. No user data is stored at the SSD.

The AES key used for the encryption/decryption is created at installation in volatile memory and stored and protected by a hardware TPM module.

### 7.1.3 User Data Protection

Information flow control policies determine if incoming/outgoing packages shall be dropped or forwarded. Policies are applied at two levels:

- West (low) and East (high) firewall
- Information guard

The information guard supports a Security Policy Information Framework, SPIF. XML-based formats and syntax is used for security policies and confidentiality metadata used by the SPIF. The security policies semantics creates a common security policy based on agreed NATO Security Policy and supporting directives. The complete, up to date SPIF for the NATO Security Policy is held in the NATO Metadata Registry & Repository (NMRR). XML scheme for SPIF can be found at this URL: http://www.xmlspif.org/schema/xmlspif.xsd. Example of a NATO type SPIF: http://www.xmlspif.org/wp-content/uploads/2009/03/policy-nato-style.xml. This SPIF is used in the evaluated configuration. For the corresponding NATO standards, see ref [4], [5], and [6].

### 7.1.4 Identification and Authentication

Management of the TOE is performed by the roles: Administrator, Security officer, Operator, and User Administrator. Persons authorized for these roles are identified and authenticated by the TOE before access to the management functions is allowed.

### 7.1.5 Security Management

The Operator is only allowed to read TOE configuration. The Administrator is allowed to read and access all configuration and management functions except manage the security event log. The Security officer is allowed to read TOE configuration and is the only role allowed to read and manage the security event log. The User administrator is allowed to read TOE configuration and to manage user's configuration. The Security officer role cannot be combined with the Administrator nor the User Administrator roles.

The security attributes that the rules in the information flow control policies are based on can be managed by the Administrator. Default values are restricted, which means that all packages are dropped until otherwise is configured.

### 7.1.6 Protection of the TSF

The TOE supports two states: Operational state and Maintenance state. Operational state has two substates, Operational nominal and Operational degraded. In Operational nominal no Warnings or Errors has been detected. In Operational degraded state at least one Warning or Error has been detected. The switch will transition to Operational nominal when all Warnings and Errors have been resolved.

Examples of Warnings are:

- Faulty power supply
- Log partition full
- Unrotated log file detected
- NTP not synchronized
- Unexpected application crash
- Security manager functionality reported integrity violation
- Disk issue detected

Examples of Errors:

- Log partition not mounted
- Ethernet interface missing
- Platform manager functionality failed to monitor one or more components
- Fan issue detected

Two Errors are considered severe. When one of these Errors appear, the switch will transition to Maintenance state and attempt to reset the switching function in the dataplane (FPU).

Severe Errors are:

- Controller not able to function

- Driver communicating with switching function in dataplane not functioning

The switch will remain in Maintenance state until all Severe Errors have been resolved.

Warnings, Errors and Severe Errors are logged.

### 7.1.7 TOE access banners

A text describing restrictions of use, legal agreements, or any other appropriate information to which administrators consent by accessing the TOE is displayed when logging in to the TOE.

# Appendix A – Abbreviations and Acronyms

For Common Criteria abbreviations and acronyms, please see CC:2022 part 1, part 2, and part 3.

| Acronym or Abbreviation | Explanation |
|---|---|
| API | Application Program Interface |
| BMC | Board Management Controller |
| C2 | Command and Control |
| FMN | NATO Federated Mission Networking |
| FPU | Floating Point Unit |
| FW | Firewall |
| GUI | Graphical User Interface |
| IEG | Information Exchange Gateway |
| KVM | Kernel-based Virtual Machine, Linux based hypervisor for virtual machines |
| MIME | Multipurpose Internet Mail Extensions |
| MIP | Multilateral Interoperability Programme's (MIP) standard for interoperability of Command and Control (C2) systems at all levels |
| NMRR | NATO Metadata Registry & Repository |
| NTP | Network Time Protocol |
| PTNE | Programmable Trusted Network Element |
| PTT | Push To Talk |
| PTV | Push To Video |
| SIP | Session Initiation Protocol |
| SNMP | Simple Network Management Protocol |
| SMTP | Simple Mail Transfer Protocol is an Internet standard communication protocol for electronic mail transmission |
| SPIF | Security Policy Information Framework |
| SPNP | Saab Programmable Networking Platform |
| SSD | Solid State Drive |
| TPM | Trusted Platform Module (TPM) is an international standard for a secure crypto processor, a dedicated microcontroller designed to secure hardware through integrated cryptographic keys |
| VM | Virtual Machine |
| XML | Extensible Markup Language (XML) is a markup language and file format for storing, transmitting, and reconstructing arbitrary data |
| XMPP | Extensible Messaging and Presence Protocol is an open communication protocol designed for instant messaging |

*Table 19, Abbreviations and acronyms*

# Appendix B - Referenced Documents

[1] Common Criteria for Information Technology Security Systems, Part 1: Introduction and general model, Version 3.1, Revision 4, CCMB-2012-09-001, September 2012

[2] Common Criteria for Information Technology Security Systems, Part 2: Security functional requirements, Version 3.1, Revision 4, CCMB-2012-09-002, September 2012

[3] Common Criteria for Information Technology Security Systems, Part 3: Security assurance requirements, Version 3.1, Revision 4, CCMB-2012-09-003, September 2012

[4] NATO STANDARD, ADatP-4774, CONFIDENTIALITY METADATA LABEL SYNTAX, Edition A Version 1, DECEDMBER 2017

[5] NATO STANDARD, ADatP-4778, METADATA BINDING MECHANISM, Edition A Version 1, OCTOBER 2018

[6] NATO STANDARD, ADatP-5636, NATO CORE METADATA SPECIFICATION (NCMS), Edition A Version 1, NOVEMBER 2022