Trusted Security Filter

TSF 401

Security Target Lite

DUAL USE CONTROLLED

Export controlled and subject to export authorization of Norway

Classification **OPEN**	Document Title	Radical – Business Id	Revision	DTC	Language	Entity Cage Code	Thales Cage Code	PAGE
Export Control **DUAL USE CONTROLLED**	**TSF 401** **Security Target Lite**	**3AQ 33330 AAAB**	**001**	**938**	**EN**	**N4244**	**0026**	**1 of 68**

DOCUMENT CHANGE HISTORY

Revision	Date	Description
001	28.11.2025	This is the first release of the document.

Table of Contents

List of Figures

List of Tables

1. SECURITY TARGET INTRODUCTION (ASE_INT)

The Target of Evaluation (TOE) of this Security Target (ST) is the Trusted Security Filter - TSF 401.

1.1 SECURITY TARGET REFERENCE

Title: TSF 401 Security Target Lite
Reference: 3AQ 33330 AAAB 938
Version: 001
Author: Thales Norway AS
Date: Nov 27th 2025

1.2 TOE REFERENCE

TOE name: TSF 401
TOE version: SW: 1.0.0
Product ID: 3AQ 30600 AAXX

Assurance level: EAL 5 augmented with ALC_FLR.3 (Systematic flaw remediation)

1.3 REFERENCED DOCUMENTS

[1]	CCMB-2022-11-001	Common Criteria for Information Technology Security Evaluation, Version Nov 2022 rev 1, Part 1 (also known as part 1 of the ISO/IEC 15408 Evaluation Criteria).
[2]	CCMB-2022-11-002	Common Criteria for Information Technology Security Evaluation, Version Nov 2022 rev 1, Part 2 (also known as part 2 of the ISO/IEC 15408 Evaluation Criteria).
[3]	CCMB-2022-11-003	Common Criteria for Information Technology Security Evaluation, Version Nov 2022 rev 1, Part 3 (also known as part 3 of the ISO/IEC 15408 Evaluation Criteria).
[4]	SDIP-27 Level A	NATO Tempest Requirements and Evaluation Procedures
[5]	FIPS PUB 197	Specification of the Advanced Encryption Standard (AES)
[6]	NIST 800-38E	Recommendation for Block Cipher Modes of Operation: The XTS-AES for Confidentiality on Storage Device

Table 1: Referenced documents

1.4 TOE OVERVIEW

The Trusted Security Filter - TSF 401 - is a Cross Domain Solution (CDS) that allows secure data transfer between different security levels. The TSF 401 can be used to transfer data between networks, for example with a security classification span from SECRET to UNCLASSIFIED.

The main purpose of the TSF 401 is to inspect and filter data addressed from one security domain to another and only allow transfer of data that complies with the filter specification.

The TSF 401 has two separate and independent channels and is capable of filtering in both directions on the main channel, or operate as diode allowing all traffic in one direction and blocking all traffic in the opposite direction. The secondary channel can be used as diode or for interface redundancy.

When operating as a diode the TSF 401 has the capacity to transmit up to 20 Gbit/s by using the two simultaneous channels of 10 Gbit/s each. When a channel is configured to operate as a filter, the capacity is up to 10 Gbit/s in the filter direction using offset-based filtering. In addition to offset-based filtering, the TSF 401 supports parsing for more advanced content checking of payloads with dynamic content.

Figure 1 illustrates the TSF 401 as a CDS between networks.

Figure 1: System example

Each of the two networks may consist of one or more end systems of different types. The end systems may be connected to the same subnet as the TSF 401, or they can be on different subnets, accessed via a router.

Major security features:

- Secure installation of filter definition files
- Secure storage of filter definition files
- HW enforced filtering mechanisms
- Protected audit log
- Endorsed cryptographic functions for disc encryption and SW/FW image protection
- Cryptographic Ignition Key (CIK)
- Secure certificate management and signature verification
- Secure boot, including self-tests of security critical functions
- Secure SW installation/update
- Software upgradeable from local USB or central management
- Tamper detection and response
- Zeroise switch
- Alarm and audit management from local HMI and central management
- Secure communication with a central management system

- Role based access control
- Designed to comply with TEMPEST requirements according to SDIP-27 level A.

1.5 TOE DESCRIPTION

Figure 2 shows the TSF 401 and its supporting tools. The supporting tools are outside the scope of the Common Criteria (CC) evaluation. The TOE is the TSF 401 main system with all SW, FW and HW modules. This includes the security filter mechanism, network services, internal management and management of filter files, trust anchors and certificates.

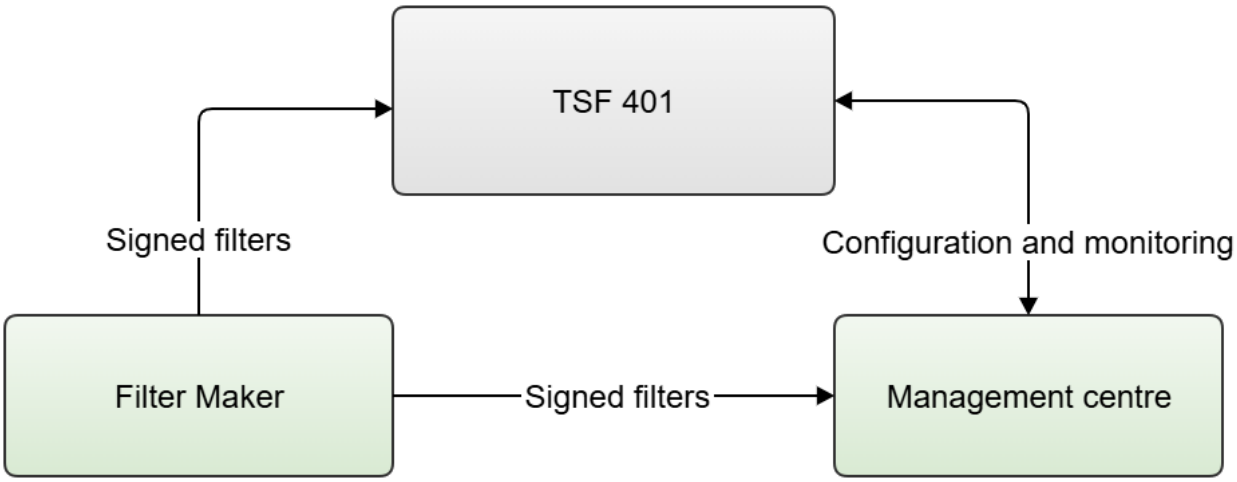

Figure 2: TSF 401 - System overview

- The **TSF 401** is a CDS that provides secure data transfer between security domains of different security levels.
- The **Filter Maker** is used for producing and signing the filter definition files.
- The Management Centre is a central system for remote management and monitoring of TSF 401s.

The TSF 401 has two Ethernet interfaces on the High side and two Ethernet interfaces on the Low side. Filter function:

- One channel with fully configurable two-way filtering
  - Independent filtering each way (High to Low and Low to High)
  - Filters can be configured to work as a Diode allowing all traffic from Low to High and block all traffic from High to Low and vice versa.
- Two extra network interfaces that can be used in the following way:
  - For interface redundancy – active failover if link on the main interface fails; or
  - Configured as a diode.

The interfaces are called Red1 and Red2 on High side, and Black1 and Black2 on Low side.

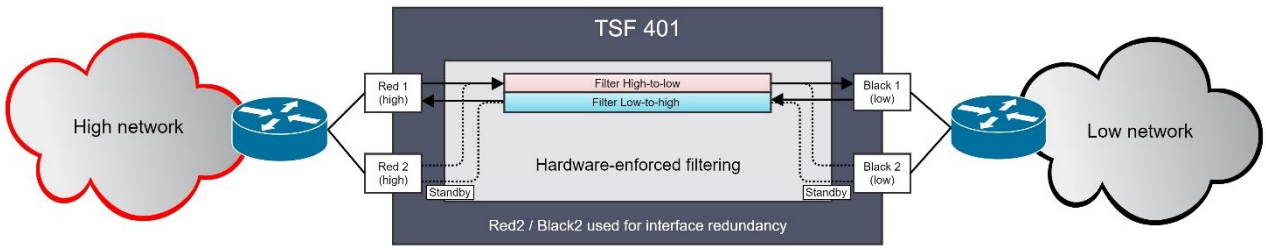

Figure 3: TSF 401 data paths with secondary interfaces in redundancy mode

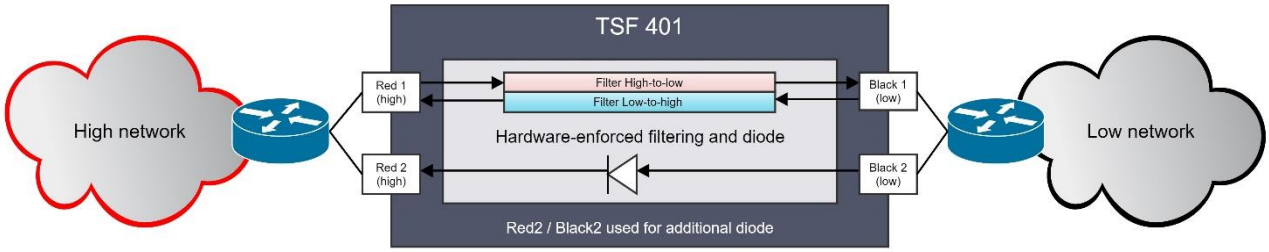

Figure 4: TSF 401 data paths with secondary interfaces in diode mode.

The default setting of the filter is “No traffic”, meaning that all traffic through the filter is blocked in both directions. This is the state of the system until a signed filter definition file is validated, installed and selected.

When a filter definition file is active, the TSF 401 only forwards data that complies with the filter specification. Non-compliant data is discarded and metadata is aggregated and available in the management centre.

1.5.1 TSF 401 – LOGICAL ARCHITECTURE

The TSF 401 architecture can be divided into the Control and signalling plane and the Data plane. Figure 5 illustrates the logical architecture of the TSF 401 with services mapped to logical domains and whether they belong to the control plane or data plane. The two channels are managed by a single Control and signalling plane.

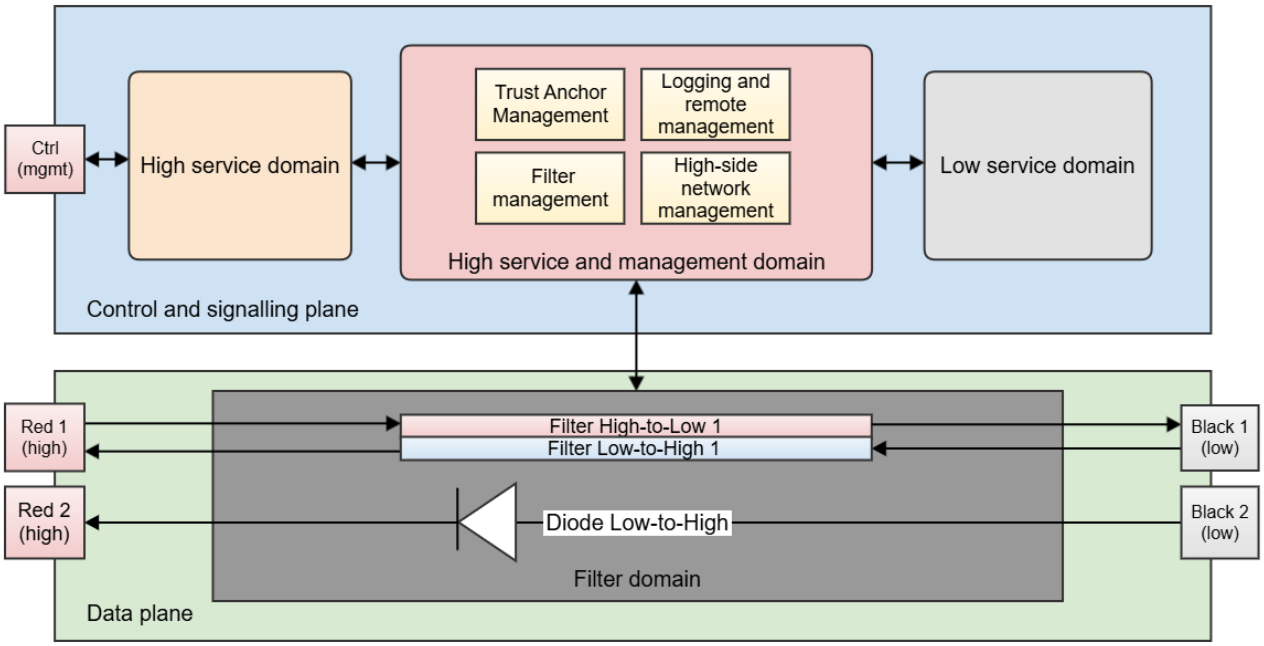

Figure 5: TSF 401 logical architecture

The TSF 401 consists of the following logical modules:

High side (Red):

- Human-Machine-Interface (HMI)
- High side network services
- Trust Anchor management
- Filter management
- Audit logs and remote management support
- High side network management

Low side (Black):

- Low side services

Filter domain:

- Offset-based filter High-to-Low
- Parser High-to-Low
- Offset-based filter Low-to-High
- Parser Low-to-High
- Diode

1.5.1.1 Data plane – Processing of user data through the filter

The filter function is implemented in the Data plane. User data traffic through the filter addressed to end systems in the High or Low network is processed through the data plane with the filter functions.

The logical components for processing of user data traffic through the filter are assigned to a filter domain that constitutes the separation between the High and Low networks.

The data flows between the High and the Low networks are sent over either channel 1 or channel 2. Data cannot cross between the two channels, i.e., packets received on Red1 can only be forwarded to Black1, not to Red2 or Black2. External network devices (routers, switches) are responsible for routing the data packets to the correct TSF 401 interface.

All filter logic is implemented in hardware through Field Programmable Gate Array (FPGA) logic, and all decisions to drop or pass traffic across the domains are made in the FPGA.

1.5.1.2 Control and signalling plane

The Control and signalling plane is responsible for the internal TSF 401 management, which includes communication with remote management centres, configuration of TSF 401 interfaces and network services, status monitoring, SW update, Trust Anchor management and filter management.

Management of the TSF 401 is available through the local Human Machine Interface (HMI), or remotely using the management interface, which can be set to the Ctrl interface, Red1 interface or Off. The Ctrl interface is a separate physical management interface that enables the use of a separate management network.

The Control and signalling plane handles filter management, such as loading, verifying, activating and deleting filter definition files.

The Control and signalling plane is responsible for the configuration of the two channels. This includes configuration of the Red and Black interfaces and ensuring that verified filters are deployed in the correct channel.

1.5.2 SECURITY FILTER MECHANISM

The filtering mechanism is implemented as a core filter enforcer that controls all data released through the filter from High to Low side and Low to High side. The filter enforcer, both offset-based and parser, is implemented in FPGA. The active filter can be selected from installed filter definition files during operation. A typical filter limits data exchange to a specified set of application messages. All other traffic/messages are stopped. The filter definition file is a set of rules for inspection of protocol parameters and message content. A filter allows only selected packets matching the rules to pass through the filter.

1.5.3 SECURITY FEATURES

Secure installation of filter definition files:

The TOE has mechanisms to ensure that only authorized filter definition files are installed. Filter definition files are signed using the signing function available in Filter Maker. The signature is verified when the filter definition file is installed and when it is selected to be active on the device.

Endorsed cryptographic functions:

The TOE has endorsed cryptographic functions for protecting the integrity of the security critical information, such as SW/FW and filter definition files, and protecting the integrity and confidentiality of key material. The TOE generates internal keys with endorsed cryptographic methods. The cryptographic functions include random number generation, key generation of internal keys, Cryptographic Ignition Key (CIK) handling, disc encryption, SW/FW image protection and secure communication with a central management system. The secure channel to the management centre uses a Transport Layer Security (TLS) certificate-based authentication method.

Audit log:

The TOE records auditable events in an audit log protected from modification. The audit log can be viewed by authorized users and collected by a management server.

Self-test:

The TOE has a secure boot process with security critical self-tests that verify correct operation of security critical functions. There are also periodic tests and operational tests to verify security critical functions during operation. If a failure is detected, the device reboots and will halt operation if the fail situation persists.

Root of trust – Certificate management and signature verification:

The TOE has a number of Device Trust Anchors (DTAs) installed. These are used to secure the integrity and root of trust. The DTAs ensure that only authenticated SW/FW packages and filter definition files can be installed and they prevent that unauthenticated certificates are installed. This ensures that the TSF 401 cannot operate with filter definition files generated by unauthorized sources.

The root of trust certificate chain is verified when the device boots. All new certificates loaded to the device are verified with a digital signature. The signed filter definition files and SW updates are checked and only installed if the signature can be verified.

Secure installation of SW/FW:

The SW/FW package load process can be activated remotely from the management centre or locally from the Human Machine Interface (HMI). The package is either installed from the management centre or installed from a USB stick. The SW/FW packages are signed and the signature is verified against the certificate chain.

Tamper and zeroise:

The tamper and zeroise handling can be activated both with power on and off.

Zeroise can be activated locally using the zeroise switch, with power on or off, or remotely from the management centre. After zeroise, the TSF 401 will be able to boot, but the operator must be physically present and perform initial configuration.

The main objective of the tamper response is to ensure the integrity of the TSF 401 and its configuration.

The Crypto Destruct interface enables external tamper activation and is enabled/disabled (default disabled) from the local HMI or the management centre.

TEMPEST:

The TOE is TEMPEST approved according to SDIP-27 level A.

Access control:

The TOE supports role-based access control with three operator roles:

- Operator – Operational role with read access
- Network Operator – Operational role with access to network functions
- Security Operator – Administrative role with specific privileges for managing the security critical operations

1.5.4 INTERFACES TO EXTERNAL SYSTEMS

Table 2 details the interfaces to external systems.

Interfaces	Protocols
Low Network Interface	IPv4 (RFC 791) IPv6 (RFC 8200) 2 x Ethernet 10 Gbit/s (SFP+ connectors), or 2 x Ethernet 1 Gbit/s (SFP connectors) Connection of Low side networks
High Network Interface	IPv4 (RFC 791)

	IPv6 (RFC 8200) 2 x Ethernet 10 Gbit/s (SFP+ connectors), or 2 x Ethernet 1 Gbit/s (SFP connectors) Connection of High side networks
Management Interface	IPv4 OR IPv6 Ethernet interface 1Gbit/s (SFP connector) Connection of management centre on High side
USB interface	USB-C interface for loading configuration file from management centre, DTAs, SW updates and filter definition files

Table 2: Interfaces to external systems

Figure 6 and Figure 7 shows the external interfaces of the TSF 401.

Figure 6: External interfaces – Front

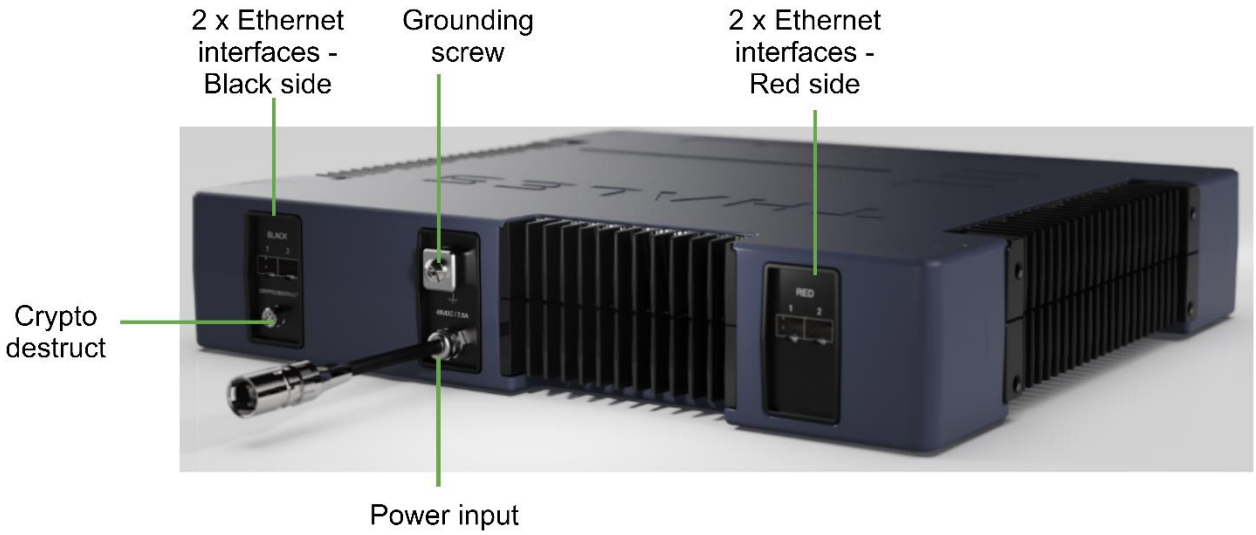

Figure 7: External interfaces – Rear

- The High and Low sides have two Ethernet interfaces for user traffic between networks
- Power input 48 VDC - Adapter converting from AC to 48 VDC fixed to HW with 2.5-meter cable
- Crypto destruct interface – For connection of an external sensor for activating tamper mechanisms
- Key fill – Disabled (not in use)
- Zeroise switch
- Cryptographic Ignition Key (CIK) interface with a plug-in CIK device. Removing the CIK disables the external communication interfaces and TSF 401 reboots. The TSF 401 cannot be used without the CIK.
- Keypad and display
- The management module has a USB-C interface and an Ethernet interface on the front panel
- Power button
- Light-Emitting Diodes (LEDs) organised in a LED panel:
    - Power on – Green LED
    - Tamper activated – Red LED
    - Multicolour LEDs for link status of each interface connector
    - Alarm LED:
        - Active alarm: Blinking red
        - Acknowledged alarm: Red
        - Battery voltage low: Yellow

1.6 TOE ENVIRONMENT

The following section describes the main security features provided by the TOE environment:

Physical protection

The TOE environment is required to provide physical protection of the TOE, according to the supported classification level, ensuring that only authorised personnel are allowed physical access to the TOE.

Operator authentication control

Operators shall be identified and authenticated before they are granted access to data and services.

Platform integrity control

The TSF 401 has a number of Device Trust Anchors installed. These are used to secure the integrity and root of trust. The Device Trust Anchors (DTA) key pairs are generated using an approved solution for generation of keys and for signing. The signing algorithm used to sign DTA bundles and SW/FW packages is a quantum secure signing algorithm. The private keys used for signing DTAs, filter TAs, SW/FW packages and filter definition files shall be stored outside the TOE in a secure location.

Software integrity control

Production of the SW/FW packages requires that the individual FPGA and SW images are signed and encrypted. In addition, the complete SW/FW package that includes all images is signed.

Physical environment

The TSF 401 shall be installed in temperature-controlled environments. Power input is 48 VDC and the device may be installed in standard 19'' racks.

Management centre

There is a trusted channel from the management centre to the TOE. The channel is protected by mutual authentication and integrity protection of the management data. The implementation of the trusted channel is considered part of the TOE environment.

2. CONFORMANCE CLAIMS (ASE_CCL)

2.1 CC CONFORMANCE CLAIM

Conformance	Common Criteria for Information Technology Security Evaluation Part 2 conformant: Security Functional Components, ref [2] Part 3 conformant: Security Assurance Components, ref [3]
Assurance level	EAL5 augmented with ALC_FLR.3 (Systematic flaw remediation)

2.2 PP CONFORMANCE CLAIM

This Security Target has no Protection Profile conformance claim.

3. SECURITY PROBLEM DEFINITION (ASE_SPD)

3.1 GENERAL

This section provides the statement of the TOE Security Problem Definition (SPD), which identifies and explains all:

a) Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects.

b) Assets that must be protected by the TOE Security Functions (TSF).

> **Note:** In this document, TSF is the abbreviation for TOE Security Function. TOE or TSF 401 is used for the device and product name.

c) Known and presumed threat agents that may execute attacks on the TOE.

d) Known and presumed threats countered either by the TOE or by the security environment.

3.2 ASSUMPTIONS

The following conditions are assumed to exist in the operational environment.

A.PHYSICAL	The system comprising the TOE and the High network is installed in a physically protected area, minimum approved for information classified High. This also applies to the channel from the management centre. The Low network is installed in a physical area minimum approved for protection of the information classified Low.
A.TRAINING	All TOE operators are trained in the correct use of the TOE.
A.CLEARANCE	All TOE operators have a minimum clearance for the security level High, and is authorised for all information handled by the system.
A.MAN_AUTHORISED	Only operators with special authorisation are allowed to configure and manage the system including the TOE.
A.USAGE	The TOE is installed in a protected environment according to the classification level of the High network and installation guidelines for the TOE.
A.ORGANIZATION	Filter files are assessed and approved for use by relevant authorities before they are signed, and signed filter files can be trusted to be correct, only specifying traffic to be allowed through the TOE.
A.HSP	The endorsed cryptographic functions delivered by the High Security Platform (HSP) of the TOE are trusted. These functions are evaluated by the Norwegian National Security Authority (NSM) and NATO security authorities.

3.3 IDENTIFICATION OF ASSETS

The assets the TOE shall protect are the following:

AS.AUDIT	The audit log generated by the TOE. The audit log consists of timestamped security events.
AS.CERTIFICATES	The TOE stores Device Trust Anchors (DTAs) and certificates used for authentication and verification of the chain of trust.
AS.CODE_IMAGES	Code images (compiled SW and FW images) for the TOE. The code images are encrypted and authenticated (signed). If they are manipulated, the TOE will reject the new image and boot with the old one.
AS.CONFIG	Configuration state of the TOE, including operators and operator metadata, security policies, date and time and configuration parameters.
AS.FILTER	Filter definition files that are stored on the TOE and used for filtering traffic between High and Low networks.
AS.INFO_HIGH	Data from the High network not specified to be allowed transferred to the Low network.
AS.INFO_LOW	Data from the Low network not specified to be allowed transferred to the High network.
AS.KEYS	Cryptographic key material stored on the TOE.

3.4 THREAT AGENTS

The following Threat Agents (TA) are defined:

TA.INTERNAL	Personnel that have authorised access to the installation of the TOE and/or the High network and who has intent to perform unauthorised actions. This personnel may be trained specifically to perform unauthorised actions. They may inject unauthorised software/firmware into the site/network. They may be supported by entities with unlimited resources.
TA.EXTERNAL	Personnel that do not have access to the installation of the TOE and/or the High network, who has the intent to divulge classified information. This personnel may have unlimited resources.

TA.USER	Users with access to the TOE with no intent to perform unauthorised actions who may unintentionally perform unauthorised actions.
TA.ADMIN	Authenticated authorized security operators of the TOE. These threat agents may unintentionally perform unauthorized actions or misuse the device causing an unintentional leak or modification of information and the configuration of security critical functions.
TA.MALFUNCTIONS	Hardware or software failures or transmission errors that may cause information to be modified or leaked by accident.

3.5 THREATS

This section identifies threats that are met by the TOE. Threats are performed by an attacker against a TOE asset.

T.INFO_HIGH_LOW	Information on the High network not allowed to be transferred to the Low network may be transferred to the Low network.
Threat agents	TA.ADMIN and/or TA.MALFUNCTIONS. In addition, the following must be present: TA.EXTERNAL
Asset	AS.INFO_HIGH
Unwanted outcome	Unauthorised personnel get access to information on the High network.
Attack methods	Personnel (TA.ADMIN) unintentionally configures or installs the TOE in a way that enables transfer of information from the High network to the Low network. Persons (TA.EXTERNAL) pick up the High information from the Low network outside the physically protected area for High information.
T.INFO_LOW_HIGH	Information on the Low network not allowed to be transferred to the High network may be transferred to the High network.
Threat agents	TA.ADMIN and/or TA.MALFUNCTIONS. In addition, the following must be present: TA.EXTERNAL
Asset	AS.INFO_HIGH
Unwanted outcome	The integrity and/or availability of the information on the High network is compromised.
Attack methods	Personnel (TA.ADMIN) or (TA.EXTERNAL) unintentionally or intentionally configures or installs the TOE in a way that enables transfer of information

	from the Low network to the High network that compromises the integrity and/or availability of the information on the High network.
T.TAMPERING	A security critical part of the TOE is subjected to physical attack that may compromise security functions or information.
Threat agents	TA.INTERNAL combined with TA.EXTERNAL
Asset	AS.INFO_HIGH, AS.AUDIT, AS.CODE_IMAGES, AS.CONFIG, AS.KEYS
Unwanted outcome	Unauthorised personnel get access to information on the High network or security critical information on the TOE.
Attack method	A person (TA.INTERNAL) modifies the TOE to transfer information from the High network to the Low network or extracts information from the TOE. Persons (TA.EXTERNAL) pick up the High network information from the Low network outside the physically protected area of the High network.
T.MISUSE	An attacker attempts to transfer information from the High network to the Low network by use of data messages.
Threat agents	TA.INTERNAL combined with TA.EXTERNAL
Asset	AS.INFO_HIGH
Unwanted outcome	Unauthorised personnel get access to information classified High.
Attack method	A person (TA.INTERNAL) introduces/modifies software and/or hardware in the High network to pick up information classified High and transfers this information to the Low network via the TOE. Persons (TA.EXTERNAL) pick up the information classified High from the Low network outside the physically protected area for High information. This threat increases if this can continue undetected.
T.TEMPEST	Electromagnetic emanations may divulge classified information.
Threat agents	TA.EXTERNAL possibly in combination with TA.INTERNAL
Asset	AS.INFO_HIGH or AS.INFO_LOW
Unwanted outcome	Unauthorised personnel get access to information from the High network or the Low network.
Attack method	Information on the High network or the Low network is electromagnetically emanated to where it can be intercepted.

T.UNAUTHORISED_USE	Authorised persons on the High network may perform unauthorised use of the High system's applications and management system.
Threat agents	TA.INTERNAL or TA.USER. In addition, the following must be present: TA.EXTERNAL.
Asset	AS.INFO_HIGH
Unwanted outcome	Unauthorised personnel get access to information from the High network.
Attack method	Authorised persons intentionally (TA.INTERNAL) or unintentionally (TA.USER) perform unauthorised use of the High system's applications and management, so that this leads to transfer of information from the High network to the Low network. Persons (TA.EXTERNAL) pick up the High information from the Low network outside the physically protected area for High information.
T.ILLEGAL_CONFIG	An attacker attempts to: • Modify or destroy authorised filter definition files on the TOE. • Modify or destroy keys used for signing or verifying filter definition files on the TOE. • Install unauthorised filter definition files on the TOE. • Inject malicious code on the TOE. • Install or modify software or firmware on the TOE. by unauthorised access through the management interfaces.
Threat agents	TA.INTERNAL combined with TA.EXTERNAL
Asset	AS.CONFIG, AS.CODE_IMAGES, AS.INFO_HIGH, AS.INFO_LOW, AS.CERTIFICATES, AS.FILTER, AS.KEYS
Unwanted outcome	Unauthorised personnel get access to information from the High network, succeed in a denial-of-service attack, exploits vulnerability in the High network from the Low network and compromises integrity and availability of the information and functions in the High network.
Attack method	A person (TA.INTERNAL) manipulates a filter definition file or SW in the TOE through the management interface with the intent to transfer information from the High to the Low network, or to prevent the TOE from transferring data by sending control information to malware in the High network. Persons (TA.EXTERNAL) pick up the High information from the Low network outside the physically protected area for High information, or the

	data is prevented from being transferred between the High and Low networks.
T.ABUSE.CERTIFICATE	Abuse installation of certificates. An attacker attempts to install certificate(s) without verification, modify existing certificate chains, or add a new certification chain.
Threat agents	TA.INTERNAL combined with TA.EXTERNAL
Asset	AS.INFO_HIGH, AS.CODE_IMAGES, AS,CONFIG, AS.FILTER, AS.KEYS, AS.CERTIFICATES
Unwanted outcome	Unauthorised personnel get access to information from the High network. The TOE receives unauthorized modified filter definition files, certificates, software or firmware.
Attack method	A person (TA.INTERNAL or TA.EXTERNAL) installs a certificate through the management interface (High side) without verification, e.g., bypassing the verification process, modifies existing certificate chains or adds a new certification chain and is able to install a modified filter definition file or modified software or firmware in such a way that not allowed information from the High network is transmitted to the Low network. Persons (TA.EXTERNAL) pick up the High information from the Low network outside the physically protected area of the High information.

3.6 ORGANISATIONAL SECURITY POLICIES (OSP)

This section describes the Organizational Security Policies (OSPs) that shall be enforced by the TOE and TOE environment.

OSP.ACCESS	Each operator`s abilities to use the TOE functions must be limited by the TOE, and be in accordance with the security policy.
OSP.ACCOUNTABILITY	The operators of the TOE shall be held accountable for their actions within the system.
OSP.IDENTIFICATION_AUTHENTICATION	All operators must be identified and authenticated prior to accessing any controlled resources with the exception of read access to public objects. Identification shall be as Operator, Security Operator or Network Operator.
OSP.RESIST_MODERATE	The TOE shall resist attackers with moderate attack potential.
OSP.ANTI_TAMPER	The TOE shall be inspected for tampering upon reception and periodically during operation. The TOE must be constructed in such a way that any tampering or tampering attempt is clearly detectable.

OSP.MAINTENANCE	Only appropriately trained and authorized personnel shall perform maintenance of the TOE. The maintenance procedures shall be documented.

4. SECURITY OBJECTIVES (ASE_OBJ)

4.1 TOE IT SECURITY OBJECTIVES

O.ACCESS_CONTROL	The TOE shall restrict the access to its services, depending on the operator role. The TOE shall provide the roles Operator, Network Operator and Security Operator. The different Operator roles are assigned access to specific TOE functionality.
O.ALARM_FAILURE	If a hardware or software failure is detected in the TOE, the TOE shall raise an alarm and reboot.
O.AUDIT	The TOE shall have a protected audit log residing in permanent memory that is not possible to modify by the user. The audit log can be viewed and collected by an external management server or log server on the High network or separate management network.
O.CHECK_OPERATION	The TOE shall verify that TSFs operate correctly. The TOE shall verify the integrity of TOE SW/FW during installation and boot, and verify the integrity of internal TSF data and key material during start-up and operation. Periodic Single Event Upset monitoring is performed to verify the TOE integrity during operation. Security critical functions shall be tested by a combination of power-up tests, periodic tests and continuous tests.
O.CIK	The TOE shall implement a removable Cryptographic Ignition Key (CIK) that protects the internal keys and SW/FW images. When the CIK is removed the TOE will reboot, and the boot process is halted until the correct CIK is present.
O.ENDORSED_CRYPTO	The TOE shall have endorsed cryptographic functions to verify and authenticate SW update files, filter files, updated DTA files and for encryption of internal keys, SW/FW images and filter files stored on the TOE. The TOE shall generate cryptographic strong keys using an endorsed Random Number Generator (RNG). The TOE shall securely manage cryptographic keys. Keys shall be destructed when they are no longer in use.
O.DOMAIN_SEPARATION	The TOE shall be internally separated into a Red (High) and Black (Low) domain to separate services belonging to the High side and Low side. The TOE shall provide separate interfaces for: - High side user data - Low side user data

	- Management functions, such as configuration, audit log export, SW updates and filter loading The TOE shall restrict information flow between the internal domains and validate the information before it is exchanged between the domains.
O.FILTER	Only specified data shall be allowed to pass through the filter mechanism from High to Low and from Low to High network when a filter is selected.
O.FILTER_LOAD	The TOE shall have a mechanism to load filter files. Only filter files verified and authenticated by a digital signature shall be allowed. Filter files that fail verification shall be rejected.
O.FILTER_THRESHOLD	The TOE shall perform flow monitoring of messages handled by the filter and shall generate an audit if the specified threshold for a given message type defined in the filter definition is exceeded.
O.NO_CONFIG	The filter files shall not be configurable inside the TOE. The TOE Security Operator shall be able to select between predefined verified and approved filter files.
O.PROTECTED_CODE	The TOE shall only allow valid and authenticated software and firmware to be loaded to the device.
O.SECURE_CHANNEL	The TOE shall establish a secure channel between the TOE and a management server for remote monitoring and management, and for loading SW/FW and filter files.
O.TAMPER	The TOE shall automatically activate tamper mechanisms if a secure state cannot be maintained. All key material, filter files, management data and user data contained inside the TOE shall be destructed, and the TOE shall be made inoperable. The TOE will no longer boot with the standard SW/FW.
O.ZEROISE	The TOE shall provide a zeroise mechanism which will destruct all filter files, key material and user data contained inside the TOE, and reset the TOE to its initial factory state. It shall be possible for anyone with physical access to the TOE to zeroise the device, and to zeroise from a remote management centre.

4.2 TOE NON-IT SECURITY OBJECTIVES

NO.SEALING	The TOE shall be physically sealed in such a way that it is clearly evident if it has been opened/tampered with.
NO.TEMPEST	The TOE shall meet the requirements in SDIP-27 Level A, ref. [4].

4.3 ENVIRONMENT IT SECURITY OBJECTIVES

OE.AUDIT	The audit log is continuously transferred to an external log server or management centre at regular intervals. The TOE environment shall review the audit logs generated and exported from the TOE to detect security violations and hold authorized users accountable for their actions related to the TOE, detect TOE malfunction or identify threat agents trying to access the TOE.
OE.CERTIFICATES	The IT environment shall be able to sign filter files, SW update files and trust anchors for verification and authentication when they are loaded to the TOE.
OE.MAINTENANCE_INTERVALS	The TOE environment shall perform maintenance activities as specified and within the intervals required by the TOE user documentation.
OE.MGMT_ACCESS	Only authorised and trained personnel shall have access to configure and manage the TOE.
OE.ORGANIZATION	The TOE environment shall evaluate and approve filter files before they are signed so that only approved filters can be loaded to the TOE.

4.4 ENVIRONMENT NON-IT SECURITY OBJECTIVES

NOE.ACCESS_CTRL	Only authorised personnel shall be given physical access to the system comprising the TOE and the High network.
NOE.AUDIT	Authorised managers of the TOE must ensure that the TOE audit log is used and managed effectively. The TOE audit log shall be inspected regularly. Appropriate and timely action shall be taken on detection of security breaches.
NOE.CLEARANCE	All users (operators of the TOE) shall have clearance for at least the highest security level of the information handled by the system High network.
NOE.INSTALL	The TOE shall be installed and configured according to the installation guidelines and user manuals for the TOE.

NOE.MAN_TRAIN	The TOE managers shall be fully trained to use and interpret the TOE equipment.
NOE.PHYS_PROT	The site where the TOE is installed shall have physical protection. The level of protection shall be approved for minimum the security level of the High network.

4.5 SECURITY OBJECTIVES FOR THE TOE RATIONALE

This section demonstrates that threats, assumptions and organizational security policies are covered by the security objectives.

4.5.1 RATIONALE FOR THREATS AND ASSUMPTIONS

Table 3 shows that all threats and assumptions are met by at least one security objective. The rationale for threats and assumptions is described in the subsections below.

Threats - Assumptions / Objectives	T.INFO_HIGH_LOW	T-INFO_LOW_HIGH	T.TAMPERING	T.MISUSE	T.TEMPEST	T.UNAUTHORISED_USE	T.ILLEGAL_CONFIG	T.ABUSE_CERTIFICATE	A.PHYSICAL	A.TRAINING	A.CLEARANCE	A.MAN_AUTHORISED	A.USAGE	A.ORGANIZATON	A.HSP
O.ACCESS_CONTROL							x	x							
O.ALARM_FAILURE	x	x													
O.AUDIT				x											
O.CHECK_OPERATION	x	x					x								
O.CIK							x								
O.ENDORSED_CRYPTO				x			x								x
O.DOMAIN_SEPARATION	x	x		x			x								
O.FILTER_THRESHOLD				x											
O.FILTER	x	x		x											
O.FILTER_LOAD				x		x	x	x							
O.NO_CONFIG	x	x				x									
O.PROTECTED_CODE						x	x	x							
O.SECURE_CHANNEL						x	x								
O.TAMPER			x				x								
O.ZEROISE							x								
NO.SEALING			x												
NO.TEMPEST					x										
OE.AUDIT				x											
OE.CERTIFICATES						x		x							
OE.MAINTENANCE_INTERVALS			x												

OE.MGMT_ACCESS						x						x			
OE.ORGANIZATION														x	
NOE.ACCESS_CTRL			x						x		x				
NOE.AUDIT				x											
NOE.CLEARANCE											x				
NOE.INSTALL					x				x	x			x		
NOE.MAN_TRAIN	x	x		x						x					
NOE.PHYS_PROT			x						x						

Table 3: Rationale for threats and assumptions

4.5.1.1 T.INFO_HIGH_LOW

The TOE controls the separation of High and Low information and the information flowing from the High to the Low network and Low to High network (O.FILTER). The filter file is not configurable after it is installed in the TOE (O.NO_CONFIG). A traffic control module ensures data validation of configuration, management and signalling data between High and Low internal domains (O.DOMAIN_SEPARATION). A failure in domain separation will be detected during power-up and normal operation (O.CHECK_OPERATION). A local alarm indication is given by detection of hardware or software failure (O.ALARM_FAILURE). The TOE managers are fully trained to handle and interpret the TOE equipment (NOE.MAN_TRAIN).

4.5.1.2 T.INFO_LOW_HIGH

The TOE controls the separation of High and Low information and the information flowing from the Low to the High network and High to Low network (O.FILTER). The filter file is not configurable after it is installed in the TOE (O.NO_CONFIG). A traffic control module ensures data validation of configuration, management and signalling data between High and Low internal domains (O.DOMAIN_SEPARATION). A failure in domain separation will be detected during power-up and normal operation (O.CHECK_OPERATION). A local alarm indication is given by detection of hardware or software failure (O.ALARM_FAILURE). The TOE managers are fully trained to handle and interpret the TOE equipment (NOE.MAN_TRAIN).

4.5.1.3 T.TAMPERING

To prevent tampering the TOE is installed in a physically protected area (NOE.PHYS_PROT) with access control (NOE.ACCESS_CONTROL). The TOE is sealed so that it is easy to see if the seal has been broken (NO.SEALING). Periodic manual inspection will detect possible tampering (OE.MAINTENANCE_INTERVALS). The TOE has tampering detection mechanisms for making security critical information unavailable (O.TAMPER).

4.5.1.4 T.MISUSE

Filter files are verified and authenticated when they are loaded to the TOE (O.FILTER_LOAD). Filter files are stored encrypted until a filter file is selected in the TOE (O.ENDORSED_CRYPTO). All messages passing through the TOE, from the High network to the Low network and/or Low to High network, are checked by the filtering mechanism (O.FILTER). The TOE will count all messages that are allowed to pass through the filter and generate an audit event if the count for a message type exceeds the threshold (O.FILTER_THRESHOLD). The TOE stores events on rejected messages in the audit log (O.AUDIT). The TOE manager is trained (NOE.MAN_TRAIN) to inspect the filter statistics and audit log to discover attempts to misuse covert channels (NOE.AUDIT) and (OE.AUDIT). The TOE validates messages between the

internal domains so that only predefined information elements with well-defined message formats are allowed to pass between the High and Low internal domains (O.DOMAIN_SEPARATION).

4.5.1.5 **T.TEMPEST**

The TOE shall be installed according to installation guidelines (NOE.INSTALL), and comply with the TEMPEST installation guidelines (NO.TEMPEST).

4.5.1.6 **T.UNAUTHORISED_USE**

The management traffic requires certificate-based authentication between the TOE and management server (OE.CERTIFICATES) and uses cryptographic techniques for establishing a secure communication channel with the TOE (O.SECURE_CHANNEL). TOE managers need special authorisation to handle the configuration and management part of the TOE (OE.MGMT_ACCES). Filter files and SW installed in the TOE are not possible to modify from TOE management (O.FILTER_LOAD), (O.NO_CONFIG), (O.PROTECTED_CODE).

4.5.1.7 **T.ILLEGAL_CONFIG**

TOE managers must be authenticated to gain access to the TOE management and only the role Security Operator is allowed to import data (O.ACCESS_CONTROL). The TOE filter files and SW/FW images are protected against manipulation within the TOE (O.ENDORSED_CRYPTO). The TOE has a secure channel between the TOE and a management server for remote monitoring and management, and for loading SW/FW and filter files (O.SECURE_CHANNEL).

The TOE generates cryptographic keys for internal use only and cryptographic keys are generated and administered according to endorsed cryptographic management (O.ENDORSED_CRYPTO). Internal system keys are protected by the CIK (O.CIK). The TOE verifies the integrity of key material (O.CHECK_OPERATION).

Cryptographic keys and filter files are erased upon tamper detection (O.TAMPER) and if zeroise is activated (O.ZEROISE). The filter files are authenticated and verified when loaded into the TOE and before activation (O.FILTER_LOAD). SW/FW images are protected so that only valid, verified and authenticated SW/FW packages can be installed in the TOE (O.PROTECTED_CODE). The integrity of the SW/FW is verified during start-up and operation (O.CHECK_OPERATION). Filter files are authenticated and verified when they are installed, during start-up and when a filter file is selected to be the active filter (O.CHECK_OPERATION). The information flow of management and configuration data is controlled between the High and Low internal domains (O.DOMAIN_SEPARATION).

4.5.1.8 **T.ABUSE_CERTIFICATE**

TOE managers must be authenticated and only the role Security Operator is allowed to load trust anchors, filter files and SW/FW (O.ACCESS_CONTROL). Only verified and authenticated trust anchors, SW/FW and filter files are allowed to be loaded to the TOE (O.FILTER_LOAD) and (O.PROTECTED_CODE). Private keys for verification and authentication of trust anchors, filter files and SW/FW images are stored and protected to the level of the High network (OE.CERTIFICATES).

4.5.1.9 **A.PHYSICAL**

The TOE must be installed according to the installation guidelines (NOE.INSTALL). Only authorised persons shall be given physical access to the system comprising the TOE and the connected networks (NOE.ACCESS_CTRL). The TOE must be installed in a physically protected area, minimum approved for the highest security level of information handled in the system (NOE.PHYS_PROT).

4.5.1.10 A.TRAINING

The TOE managers are fully trained to handle and interpret the TOE (NOE.MAN_TRAIN). The TOE managers or personnel responsible for installing the TOE (technicians) are trained to install the TOE according to the installation guidelines (NOE.INSTALL).

4.5.1.11 A.CLEARANCE

Only authorised personnel shall be given physical access to the system comprising the TOE and the connected networks (NOE.ACCESS_CTRL) and (NOE.CLEARANCE).

4.5.1.12 A.MAN_AUTHORISED

Special authorisation is required to grant access to handle configuration and management of the TOE (OE.MANAGEMENT_ACCESS).

4.5.1.13 A.USAGE

The TOE must be installed and configured according to the installation guidelines and configured/used according to the user manuals (NOE.INSTALL).

4.5.1.14 A.ORGANIZATION

The filter files that are signed have gone through an approval process to verify that the specified traffic is allowed to pass through the filter (OE.ORGANIZATION).

4.5.1.15 A.HSP

The cryptographic support functions of the High Security Platform (HSP) used in the TOE will be subject to security evaluation by Norwegian National Security Authorities (NSM) and NATO security authorities, which ensures that only endorsed crypto algorithms, key types and sizes and standards are used (O.ENDORSED_CRYPTO).

4.5.2 RATIONALE FOR ORGANIZATIONAL SECURITY POLICIES

Table 4 shows that all Organizational Security Policies (OSPs) are met by at least one security objective. The rationale for OSPs is described in the subsections below.

OSPs / Objectives	OSP.ACCESS	OSP.ACCOUNTABILITY	OSP.IDENTIFICATION_AUTHENTICATION	OSP.RESIST_MODERATE	OSP.ANTI_TAMPER	OSP.MAINTENANCE
O.ACCESS_CONTROL	x		x			
O.AUDIT		x				

O.CHECK_OPERATION				x		
O.DOMAIN_SEPARATION				x		
O.FILTER_LOAD				x		
O.PROTECTED_CODE				x		x
O.SECURE_CHANNEL				x		
O.TAMPER				x	x	
O.ZEROISE						
NO.SEALING					x	
OE.AUDIT		x				
OE.MAINTENACE_INTERVALS					x	x
OE.MGMT_ACCESS	x		x			x
NOE.ACCESS_CTRL			x		x	x
NOE.AUDIT		x		x		
NOE.CLEARANCE			x			x
NOE.MAN_TRAIN						x

Table 4: Rationale for OSPs

4.5.2.1 **OSP.ACCESS**

The TOE addresses each user's (Operators, Network Operators and Security Operators) abilities to use the TOE functions in accordance with the security function policies. The TOE requires the TOE to restrict the access to its services, depending on the user's role and privileges (O.ACCESS_CONTROL) and (OE.MGMT_ACCESS).

4.5.2.2 **OSP.ACCOUNTABILITY**

The TOE requires the users (Operators, Network Operators and Security Operators) to be held accountable for their actions within the TOE. The TOE is required to verify the user's role and associate security relevant events actions with the roles, and record the actions performed by the role in the audit log (O.AUDIT) and (OE.AUDIT). The TOE audit log shall be inspected regularly (NOE.AUDIT).

4.5.2.3 **OSP.IDENTIFICATION_AUTHENTICATION**

The TOE addresses identification and authentication of all users by category (Operators, Network Operators and Security Operators) prior to accessing any controlled resources (O.ACCESS_CONTROL). Configuration and management of the TOE is restricted to authorized and trained personnel (OE.MGMT_ACCESS). Physical access is subject to authorization (NOE.ACCESS_CTRL). All users shall be authorized for the level of the information handled by the system High network (NOE_CLEARANCE).

4.5.2.4 **OSP.RESIST_MODERATE**

The TOE has security functions to resist attacks from attackers with moderate attack potential. If a secure state cannot be maintained the device tamper mechanisms will be activated (O.TAMPER). The TOE is resistant against attacks by verification of the integrity and authenticity of filter files (O.FILTER_LOAD),

SW/FW images (O.PROTECTED_CODE) and loading of certificates/trust anchors, filter files and SW/FW updates through the management interfaces (O.SECURE_CHANNEL). Security critical functions are tested by a combination of power-up tests, periodic tests and continuous tests (O.CHECK_OPERATION). The audit log is inspected regularly for detection of attacks (NOE.AUDIT). The internal high and low service and management domains in the TOE are separated to protect from attacks using a potential bypass channel (O.DOMAIN_SEPARATION).

4.5.2.5 **OSP.ANTI_TAMPER**

The TOE shall be constructed in such a way that any tampering can be easily detected by the TOE and observed by operators (NO.SEALING). Regular physical inspection is required (OE.MAINTENANCE_INTERVALS). Physical access to the TOE shall be restricted (NOE.ACCESS_CTRL). The TOE ensures detection and response if modification is attempted by physical means (O.TAMPER).

4.5.2.6 **OSP.MAINTENANCE**

The TOE requires that only trained and authorized personnel perform maintenance on the TOE (OE.MGMT_ACCESS and NOE.MAN_TRAIN). The TOE prevents unauthorized software updates (O.PROTECTED_CODE), while the TOE environment is required to provide secure facilities and authorize personnel to gain physical access (NOE.ACCESS_CTRL and NOE.CLEARANCE). Maintenance personnel shall perform maintenance activities as specified and within the intervals required by TOE user documentation (OE.MAINTENANCE_INTERVALS).

5. EXTENDED COMPONENTS DEFINITION (ASE_ECD)

The following explicit components have been included in this Security Target because the Common Criteria components are found to be insufficient.

5.1 EXPLICIT FUNCTIONAL COMPONENT

Explicit component	**Identifier**	**Rationale**
FAU_GEN_EXT.1	Identification of roles: Operator, Network Operator and Security Operator.	The security audit data generation SFR is explicitly added to include a requirement for role association instead of individual user identification (replaces FAU_GEN.2). The TSF associates auditable events to identified roles.
Hierarchical to:	No other components.	
Dependencies:	FAU_GEN.1 Audit data generation	
FAU_GEN_EXT.1.1	For audit events resulting from actions of identified roles, the TSF shall be able to associate each auditable event with the role that caused the event.	

Explicit component	**Identifier**	**Rationale**
FMT_SMR_EXT.1	Security roles	Replaces the FMT_SMR.1 which has a requirement to identify individual users. This explicit component identifies security roles with no identification of individual users to roles.
Hierarchical to:	No other components.	
Dependencies:	FIA_UID.1 Timing of identification	
FMT_SMR_EXT.1.1	The TSF shall maintain the roles [*assignment: the authorized identified roles*].	

6. SECURITY REQUIREMENTS

This section contains the security requirements applicable for the TOE. These requirements consist of Security Functional Requirements (SFRs) from Common Criteria (CC) part 2, and Security Assurance Requirements (SARs) from CC part 3.

6.1 TOE SECURITY FUNCTIONAL REQUIREMENTS

The Table 5 lists the Security Functional Requirements (SFRs) included in this ST.

Functional class	Component	Name
FAU – Security Audit	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_GEN_EXT.1	Role identity association
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Security audit review
	FAU_STG.1	Audit data storage location
	FAU_STG.2	Protected audit trail storage
	FAU_STG.5	Prevention of audit data loss
FCS – Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.6	Timing and event of cryptographic key destruction.
	FCS_COP.1	Cryptographic operation
	FCS_RNG.1	Random number generation.
FDP – User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute-based access control
	FDP_IFC.2	Complete information flow control
	FDP_IFF.1	Simple security attributes
	FDP_IFF.6	Illicit information flow monitoring
	FDP_ITC.2	Import of user data with security attributes

FIA – Identification and Authentication	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.6	Re-authentication
	FIA_UID.1	Timing of identification
FMT – Security Management	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR_EXT.1	Security roles
FPT – Protection of the TOE Security Functions (TSFs)	FPT_FLS.1	Failure with preservation of secure state
	FPT_PHP.3	Resistance to physical attack
	FPT_STM.1	Reliable time stamps
	FPT_TDC.1	Inter-TSF basic TSF data consistency
	FPT_TST.1	TSF self-testing
FTP – Trusted path/channels	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted path

Table 5: Security functional requirements

6.1.1 SECURITY FUNCTIONAL POLICIES

The following Security Functional Policies (SFPs) are defined:

6.1.1.1 Traffic_Data information flow control policy

The Traffic_Data information flow control policy regulates how the TOE shall allow or prevent user traffic data through the filter mechanism between two networks. The SFP is defined by FDP_IFC.2/Traffic_Data and FDP_IFF.1/Traffic_Data. The Traffic_Data information flow control policy is monitored for illicit information defined by FDP_IFF.6.

6.1.1.2 Internal information flow control policy

The Internal information flow control policy regulates how the TOE maintains the internal domain separation and how the TOE shall allow or prevent data between internal domains. The SFP is defined by FDP_IFC.2/Internal and FDP_IFF.1/Internal. The Internal information flow control policy is monitored for illicit information defined by FDP_IFF.6.

6.1.1.3 Configuration Access Control Policy

The Configuration access control policy regulates the access to Security Configuration including authentication of the role Security Operator. The SFP is defined by FDP_ACC.1 and FDP_ACF.1. The Configuration access control policy is referenced in FDP_ITC.2, ensuring a secure import of filter files and software update files.

6.1.2 CLASS FAU: SECURITY AUDIT

FAU_ARP.1	**Security alarms**
FAU_ARP.1.1	The TSF shall take [*an action to raise a local alarm, reboot, halt operation*] upon detection of a potential security violation.
Hierarchical to:	No other components.
Dependencies:	FAU_SAA.1 Potential violation analysis.

FAU_GEN.1	**Audit data generation**
FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions b) All auditable events for the [*not specified*] level of audit; and c) [*Exceeding threshold values*].
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, 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, [*additional relevant information*].
Hierarchical to:	No other components.
Dependencies:	FPT_STM.1 Reliable time stamps.

FAU_GEN.EXT 1	**Role association**
FAU_GEN_EXT .1.1	For audit events resulting from actions of identified roles, the TSF shall be able to associate each auditable event with the role that caused the event.
Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation

FAU_SAA.1	**Potential violation analysis**
FAU_SAA.1.1	The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.
FAU_SAA.1.2	The TSF shall enforce the following rules for monitoring audited events: • Accumulation or combination of [*tampering protection, zeroise, self-tests*] known to indicate a potential security violation. • [*none*]
Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation.

FAU_SAR.1	**Security audit review**
FAU_SAR.1.1	The TSF shall provide [*TOE operators*] with the capability to read [*all audits*] from the audit data.
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation.

FAU_STG.1	**Audit data storage location**
FAU_STG.1.1	The TSF shall be able to store generated audit data on the [*TOE itself, transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1*]. **Note:** FTP_ITC.1 is implemented by a TLS connection between the TOE and management entity provided by software libraries in the environment.
Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation FTP_ITC.1 Inter-TSF trusted channel

FAU_STG.2	**Protected audit trail storage**
FAU_STG.2.1	The TSF shall protect the stored audit records from unauthorised deletion.
FAU_ STG.2.2	The TSF shall be able to [*prevent*] unauthorised modifications to the stored audit data in the audit trail.
Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation.

FAU_STG.5	**Prevention of audit data loss**
FAU_STG.5.1	The TSF shall [*overwrite the oldest audit records*], [*export to external management/log server*] if the audit data storage is full.
Hierarchical to:	FAU_STG.4 Action in case of possible audit data loss
Dependencies:	FAU_STG.2 Protected audit data storage FAU_GEN.1 Audit data generation

6.1.3 CLASS FCS: CRYPTOGRAPHIC SUPPORT

FCS_CKM.1	**Cryptographic key generation**
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*AES*] and specified cryptographic key sizes [*256*] that meet the following: *[FIPS Publication 197 Advanced Encryption Standard (AES)]*.
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.3	**Cryptographic key access**
FCS_CKM.3.1	The TSF shall perform [*decryption of keys*] in accordance with a specified cryptographic key access method [*key unwrapping*] that meets the following: [EKMS 324 – AES Key Wrap].
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.6	**Timing and event of cryptographic key destruction**
FCS_CKM.6.1	The TSF shall destroy [*internally generated cryptographic keys (including keys decrypting filter files)*] when [*no longer needed*, [*expired, tampering*]].
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 [*overwriting*] that meets the following: [*endorsed cryptographic destruction method*].
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_COP.1	**Cryptographic operation**
FCS_COP.1.1	The TSF shall perform [- *verification of digital signatures for certificates (DTAs), SW updates and filter files* - *disc encryption* - *protection of SW/FW images* - *authentication of management server*] in accordance with a specified cryptographic algorithm

	[- digital signatures: *SPHINCS+ and RSA* *- disc encryption: AES-XTS* *- SW/FW images: Encrypted with AES-GCM - Signed with RSA signatures* *- management communication: Transport Layer Security (TLS) protocol*] and cryptographic key sizes [*256*] that meet the following: [- *FIPS Publication 197 Advanced Encryption Standard (AES)* *- NIST 800-38E]*.
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 CKM.5 Cryptographic key derivation] FCS_CKM.3 Cryptographic key access

FCS_RNG.1	**Random number generation**
FCS_RNG.1.1	The TSF shall provide a [*true*] random number generator that implements: [*National Security Authority (NSM) and NATO requirements*].
FCS_RNG.1.2	The TSF shall provide [*bits*] that meet [*NSM and NATO requirements*].
Hierarchical to:	No other components.
Dependencies:	No dependencies.

6.1.4 CLASS FDP: USER DATA PROTECTION

FDP_ACC.1	**Subset access control**
FDP_ACC.1.1	The TSF shall enforce the [*Configuration access control policy*] on [*TOE managers injecting Security configuration files and modifying and querying dynamic parameters*].
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute-based access control

FDP_ACF.1	**Security attribute-based access control**

FDP_ACF.1.1	The TSF shall enforce the [*Configuration access control policy*] to objects based on the following: [Subjects and attributes: *TOE Manager roles (Security Operator, Network Operator, Operator), passwords.* *Objects and attributes: Filter files, software update files, DTAs and filter TAs – Digital signature* *Dynamic parameters: Initial values (factory settings), network service parameters, management interface and traffic interface parameters*].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*Only Security Operator shall be authorised to inject filter files and software update files, DTAs, and filter TAs. Security Operator/Network Operator can change dynamic parameters. Prior to accepting the filter files, software update files, DTAs and filter TAs the following verification shall be done: Integrity and authenticity shall be verified by means of a digital signature*].
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*At first start-up after delivery or after zeroise it shall be possible to perform pairing of TOE and management server based on digital certificates (TLS)*].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*The TOE shall deny injection of filter files, software update files, DTAs and filter TAs from all interfaces other than the management interfaces (Red1 interface, Ctrl interface, USB interface) and deny access to use of HMI for security management to all others than the Security Operator)*].
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA**.**3 Static attribute

FDP_IFC.2/Traffic_Data	**Complete information flow control**
FDP_IFC.2.1	The TSF shall enforce the [*Traffic_data information flow control SFP*] on [*subjects:* • *Filter domain* • *Red1 and 2 interfaces* • *Black1 and 2 interfaces* *information:* • *Data from High network to Low network and*

	• *Data from Low network to High network* *through the filter*] and all operations that cause that information to flow to and from subjects covered by the SFP.
FDP_IFC.2.2	The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.
Hierarchical to:	FDP_IFC.1 Subset information flow control
Dependencies:	FDP_IFF.1 Simple security attributes

FDP_IFC.2/Internal	**Complete information flow control**
FDP_IFC.2.1	The TSF shall enforce the [*Internal information flow control SFP*] on [*subjects:* • *High domain – Management High* • *Low domain – Management Low* • *TCM module* • *Ctrl interface and Red1 interface, USB-HMI (management interfaces)* *information:* • *Management and signalling data from High network to the High and Low domain of the TOE and* • *Management and signalling data from the High domain to the Low domain*] and all operations that cause that information to flow to and from subjects covered by the SFP.
FDP_IFC.2.2	The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.
Hierarchical to:	FDP_IFC.1 Subset information flow control
Dependencies:	FDP_IFF.1 Simple security attributes

FDP_IFF.1/Traffic_Data	**Simple security attributes**

FDP_IFF.1.1	The TSF shall enforce the [*Traffic_data information flow control SFP*] based on the following types of subject and information security attributes: [*Subjects: Security attributes* • *Filter domain and traffic interfaces: Filter rule set* *information: Security attributes* • *Data from High network to Low network: Properties matching the filter rule set* • *Data from Low network to High network: Properties matching the filter rule set*].
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: [*the filter rule set defined in the filter file*].
FDP_IFF.1.3	The TSF shall enforce [*no additional information flow control SFP rules*].
FDP_IFF.1.4	The TSF shall explicitly authorize an information flow based on the following rules: [*the filter rule set defined in the filter file*].
FDP_IFF.1.5	The TSF shall explicitly deny an information flow based on the following rules: [[*the filter rule set defined in the filter file*].
Hierarchical to:	No other components.
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute

FDP_IFF.1/Internal	**Simple security attributes**
FDP_IFF.1.1	The TSF shall enforce the [*Internal information flow control SFP*] based on the following types of subject and information security attributes: [*subjects: High domain and Ctrl and Red1 interfaces, USB-HMI (management interfaces) – Management and network services: TLS certificate verification – Digital signatures* *Low domain – Management and network services: Pre-defined message formats and rate limitation.* *TCM module: Pre-defined message formats and rate limitation from High to Low internal domains* Information: *Management, configuration and signalling data to the TOE High domain and Low domain from High network/management, and from internal High domain to internal Low domain*].

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: [*definition of the message format and rate limitation through the TCM module*].
FDP_IFF.1.3	The TSF shall enforce [*information flow control of management, configuration and signalling data between internal domains*].
FDP_IFF.1.4	The TSF shall explicitly authorize an information flow based on the following rules: [*predefined message format and rate limitation*].
FDP_IFF.1.5	The TSF shall explicitly deny an information flow based on the following rules: [the message does not match the predefined format and/or exceeds rate].
Hierarchical to:	No other components.
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute

FDP_IFF.6	**Illicit information flow monitoring**
FDP_IFF.6.1	The TSF shall enforce the [*Traffic_data information flow control SFP and Internal information flow control policy*] to monitor the [*information flows not allowed through the filter mechanism, and information flows of management, configuration and signalling data between internal domains*] when it exceeds the [*threshold values and filter rules through filter mechanism, and rate limitation and format requirements through Traffic Control Module between internal domains*].
Hierarchical to:	No other components.
Dependencies:	FDP_IFC.1 Subset information flow control is covered as FDP_IFC.2 is included.

FDP_ITC.2	**Import of user data with security attributes**
FDP_ITC.2.1	The TSF shall enforce the [*Configuration access control policy*] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.2.2	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3	The TSF shall ensure that the protocol used provides for unambiguous association between the security attributes and the user data received.
FDP_ITC.2.4	The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.
FDP_ITC.2.5	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE [*none*].

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency

6.1.5 CLASS FIA: IDENTIFICATION AND AUTHENTICATION

FIA_UAU.4	**Single-use authentication mechanisms**
FIA_UAU.4.1	The TSF shall prevent reuse of authentication data related to [*the first time a user logs on, or after a password reset].*
Hierarchical to:	No other components.
Dependencies:	No dependencies.

FIA_UAU.6	**Re-authentication**
FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions: *[- power on* *- after zeroisation* *- after restart* *- after a period of inactive time (auto lock and logout)* *- when security and network parameters are configured]*
Hierarchical to:	No other components.
Dependencies:	No dependencies

FIA_UID.1	**Timing of identification**
FIA_UID.1.1	The TSF shall allow: [- *Self-tests* *- View alarms* *- Identification by role and password (Operator, Network Operator, Security Operator)*

	- Crypto destruct and zeroise *- Change backup battery* *- Replace Small Form Factor Pluggable connectors: Requires network operator password to make the TOE operational after replacing a connector]* on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any TSF-mediated actions on behalf of that user. **Note:** The TOE requires the CIK to be inserted before any of the operations above, except for activation of crypto destruct/zeroise, change of battery and Small Form Factor Pluggable connectors.
Hierarchical to:	No other components.
Dependencies:	No dependencies

6.1.6 CLASS FMT: SECURITY MANAGEMENT

FMT_MSA.1	**Management of security attributes**
FMT_MSA.1.1	The TSF shall enforce the [*Configuration access control SFP*] to restrict the ability to [*modify, delete*] the security attributes [*digital signatures of SW update files, DTAs and filter TAs, filter files, manage security password and time settings*] to [*Security Operator*].
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR_EXT.1 Security roles FMT_SMF.1 Specification of Management Functions

FMT_MSA.3	**Static attribute initialization**
FMT_MSA.3.1	The TSF shall enforce the [*Configuration access control policy SFP*] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [*none*] to specify alternative initial values to override the default values when an object or information is created.
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR_EXT.1 Security roles

FMT_MTD.1	**Management of TSF data**
FMT_MTD.1.1	The TSF shall restrict the ability to [modify, change] the [*filter files, trust anchors, SW updates, security password, time settings*] to [*the Security Operator role*].
Hierarchical to:	No other components.
Dependencies:	FMT_SMR_EXT.1 Security roles FMT_SMF.1 Specification of Management Functions

FMT_SMF.1	**Specification of management functions**
FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: [*Selecting no traffic or filter operation, inject filter files, select active filter, adjust time and date, SW update, install DTAs and filter TAs, manage passwords and audit data*].
Hierarchical to:	No other components.
Dependencies:	No dependencies.

FMT_SMR_EXT.1	**Security roles**
FMT_SMR._EXT. 1.1	The TSF shall maintain the roles [*Operator, Network Operator, Security Operator*].
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification

6.1.7 CLASS FPT: PROTECTION OF THE TOE SECURITY FUNCTIONS (TSF)

FPT_FLS.1	**Failure with preservation of secure state**
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: [*self-test fails (critical alarms), tampering detected, zeroise, complete loss of power, battery lid open, SFP connector missing, missing or wrong CIK*].
Hierarchical to:	No other components.
Dependencies:	No dependencies.

FPT_PHP.3	**Resistance to physical attack**
FPT_PHP.3.1	The TSF shall resist [*physical tampering: open the TOE, open battery lid, remove SFP connectors, temperature limits exceeded*] to the [*entire device*] such that the SFRs are always enforced.
Hierarchical to:	No other components.
Dependencies:	No dependencies.

FPT_STM.1	**Reliable time stamps**
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps. **Note:** The reliable time stamps are used for audits according to FAU_GEN.1.
Hierarchical to:	No other components.
Dependencies:	No dependencies.

FPT_TDC.1	**Inter-TSF basic TSF data consistency**
FPT_TDC.1.1	The TSF shall provide the capability to consistently interpret [*filter files, DTAs, filter TAs, SW updates, time settings*] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2	The TSF shall use [*the following rules:* - *Verification of digital signatures* - *Verification of integrity through checksum* - *Filter rules for user traffic data*] when interpreting the TSF data from another trusted IT product.
Hierarchical to:	No other components.
Dependencies:	No dependencies.

FPT_TST.1	**TSF self-testing**
FPT_TST.1.1	The TSF shall run a suite of the following self-tests: [*During initial start-up: All cryptographic and security critical functions, RAM, HW* *During normal operation: Random Generator test, Single event upset scanning*

	At request of user: Interface and display tests] and *At the conditions* [*when injecting a filter file and when activating/selecting a filter file*]] to demonstrate the correct operation of [*the TSF*]: [*verification of digital signature of filter files*].
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of [*TSF data*].
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of [*TSF*].
Hierarchical to:	No other components.
Dependencies:	No dependencies.

6.1.8 CLASS FTP: TRUSTED PATH/CHANNELS

FTP_ITC.1	**Inter-TSF trusted channel**
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 [*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 [*No functions*].
Hierarchical to:	No other components.
Dependencies:	No dependencies.

FTP_TRP.1	**Trusted path**
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	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 and network and security parameter configuration*].
Hierarchical to:	No other components.
Dependencies:	No dependencies.

6.2 TOE SECURITY ASSURANCE REQUIREMENTS

The assurance level of the TOE is EAL5 augmented with ALC_FLR.3 - Systematic flaw remediation. The assurance components are summarised in Table 6.

Assurance class	Assurance component name	Assurance family
ADV: Development	Security architecture description	ADV_ARC.1
	Complete semi-formal functional specification with additional error information	ADV_FSP.5
	Implementation representation of the TSF	ADV_IMP.1
	Well-structured internals	ADV_INT.2
	Semi-formal modular design	ADV_TDS.4
AGD: Guidance documents	Operational user guidance	AGD_OPE.1
	Preparative procedures	AGD_PRE.1
ALC: Life Cycle Support	Production support, acceptance procedures and automation	ALC_CMC.4
	Development tools CM coverage	ALC_CMS.5
	Delivery procedures	ALC_DEL.1
	Identification of security measures	ALC_DVS.1
	Systematic flaw remediation	ALC_FLR.3
	Developer defined life-cycle model	ALC_LCD.1
	Compliance with implementation standards	ALC_TAT.2
ASE: Security Target Evaluation	Conformance claims	ASE_CCL.1
	Extended components definition	ASE_ECD.1
	ST introduction	ASE_INT.1
	Security objectives	ASE_OBJ.2
	Derived security requirements	ASE_REQ.2
	Security problem definition	ASE_SPD.1

	TOE summary specification	ASE_TSS.1
ATE: Tests	Analysis of coverage	ATE_COV.2
	Testing: modular design	ATE_DPT.3
	Functional testing	ATE_FUN.1
	Independent testing – sample	ATE_IND.2
AVA: Vulnerability assessment	Methodical vulnerability analysis	AVA_VAN.4

Table 6: Security assurance requirements - EAL5

6.3 SECURITY REQUIREMENTS RATIONALE

Table 7 identifies which SFRs satisfy the security objectives in chapter 4. All security objectives are satisfied by at least one SFR and all SFRs meet at least one objective.

SFRs / OBJECTIVES	O.ACCESS_CONTROL	O.ALARM_FAILURE	O.AUDIT	O.CHECK_OPERATION	O.CIK	O.ENDORSED_CRYPTO	O.DOMAIN_SEPARATION	O.FILTER_THRESHOLD	O.FILTER	O.FILTER_LOAD	O.NO_CONFIG	O.PROTECTED_CODE	O.SECURE_CHANNEL	O.TAMPER	O. ZEROISE	NO.SEALING
FAU_ARP.1		x		x												
FAU_GEN.1			x					x								
FAU_GEN_EXT.1			x													
FAU_SAA.1				x										x	x	
FAU_SAR.1			x													
FAU_STG.1			x										x			
FAU_STG.2			x										x			
FAU_STG.5			x										x			
FCS_CKM.1						x										
FCS_CKM.3						x										
FCS_CKM.6					x	x								x	x	
FCS_COP.1				x		x				x		x	x			
FCS_RNG.1						x										
FDP_ACC.1	x									x	x	x	x			
FDP_ACF.1	x					x				x		x	x			
FDP_IFC.2									x							
FDP_IFF.1							x		x		x					
FDP_IFF.6							x	x	x							
FDP_ITC.2	x									x		x	x			

SFRs \ OBJECTIVES	O.ACCESS_CONTROL	O.ALARM_FAILURE	O.AUDIT	O.CHECK_OPERATION	O.CIK	O.ENDORSED_CRYPTO	O.DOMAIN_SEPARATION	O.FILTER_THRESHOLD	O.FILTER	O.FILTER_LOAD	O.NO_CONFIG	O.PROTECTED_CODE	O.SECURE_CHANNEL	O.TAMPER	O. ZEROISE	NO.SEALING
FIA_UAU.4	x															
FIA_UAU.6	x															
FIA_UID.1	x															
FMT_MSA.1	x										x			x	x	
FMT_MSA.3											x	x				
FMT_MTD.1	x															
FMT_SMF.1	x															
FMT_SMR_EXT.1	x															
FPT_FLS.1				x					x							
FPT_PHP.3														x		x
FPT_STM.1			x													
FPT_TDC.1				x						x		x	x			
FPT_TST.1																
FTP_ITC.1			x							x		x	x			
FTP_TRP.1	x															

Table 7: Rationale for security functional requirements

FAU_ARP.1 Security alarms

The TOE will raise a local alarm indication if a TOE hardware or software failure is detected (O.ALARM_FAILURE). The TOE will halt operation or reboot if a critical alarm occurs. Power-up tests, periodic and continuous tests detect if there is a potential security violation (O.CHECK_OPERATION).

FAU_GEN.1 Audit data generation

The TOE registers auditable events indicating type of event and outcome of the event from the TOE (O.AUDIT). The TOE monitors the rate of flow through the filter and issues an audit event if the threshold is exceeded (O.FILTER_THRESHOLD).

FAU_GEN_EXT.1 Role association

For audit events resulting from actions of identified roles (Operators, Network Operators and Security Operators), the TOE shall be able to associate each auditable event with the role of the user that caused the event (O.AUDIT).

FAU_SAA.1 Potential violation analysis

The TOE has automatic and manual functions for tamper activation (O.TAMPER) and zeroise (O.ZEROISE). The TOE performs self-tests that can detect potential security violations and operational integrity check of SW/FW, including Periodic Single Event Upset monitoring (O.CHECK_OPERATION).

FAU_SAR.1 Security audit review

The TOE provides the capability to read the information from the audit records (O.AUDIT).

FAU_STG.1 Audit data storage location

The TOE protects the stored audit log (O.AUDIT) and transmits the audit log to an external management/log server (O.SECURE_CHANNEL).

FAU_STG.2 Protected audit trail storage

The audit log is protected from unauthorised modification (O.AUDIT) and the TOE transmits the audit log to an external management/log server (O.SECURE_CHANNEL).

FAU_STG.5 Prevention of audit data loss

The TOE overwrites the oldest records when the audit log is full (O.AUDIT) and transmits the audit log to an external management/log server (O.SECURE_CHANNEL).

FCS_CKM.1 Cryptographic key generation

The TOE generates cryptographic keys for internal use. The key generation method is based on endorsed cryptographic methods (O.ENDORSED_CRYPTO).

FCS_CKM.3 Cryptographic key access

The TOE uses a key wrap function to encrypt/decrypt all internal keys in the system (O.ENDORSED_CRYPTO). All cryptographic keys are stored in encrypted form (wrapped) and only temporarily decrypted (unwrapped) when needed by a cryptographic operation.

FCS_CKM.6 Timing and event of cryptographic key destruction

Key material is destructed according to endorsed cryptographic methods (O.ENDORSED_CRYPTO). Keys are made inaccessible in the event of activation of tamper mechanisms (O.TAMPER) and zeroise (O.ZEROISE). When the CIK is removed the cryptographic keys are made inaccessible (O.CIK).

FCS_COP.1 Cryptographic operation

The TOE performs verification of digital signatures of imported filter files (O.FILTER_LOAD) and software update files (O.PROTECTED_CODE). During start-up and use the TOE checks the integrity of SW/FW and key material (O.CHECK_OPERATION). The TOE uses disc encryption and protects the SW/FW images, filter files and internal keys stored on the TOE, and internal keys are in addition protected using key wrapping (O.ENDORSED_CRYPTO). The TOE uses TLS to establish a secure channel between the TOE and a management server (O.SECURE.CHANNEL).

FCS_RNG.1 Random number generation

Internal keys are generated by an approved Random Number Generator (RNG) used for providing random numbers for cryptographic purposes (O.ENDORSED_CRYPTO).

FDP_ACC.1 Subset access control

The TOE performs access control of TOE managers (O.ACCESS_CONTROL) and security configuration files in order to ensure secure import of security configuration files (O.FILTER_LOAD) and (O.PROTECTED_CODE). TOE managers cannot modify security configuration files stored on the TOE (O.NO_CONFIG). Access from remote management server is verified and authenticated (O.SECURE_CHANNEL).

FDP_ACF.1 Security attribute-based access control

The TOE manager must log in to the TOE with a role and password (O.ACCESS_CONTROL).The TOE performs verification and authentication of filter files (O.FILTER_LOAD) and SW/FW images ((O.PROTECTED_CODE) when they are installed and at every boot. The TOE security configuration files are stored encrypted on the TOE (O.ENDORSED_CRYPTO). The access from remote management server is verified and authenticated (O.SECURE_CHANNEL).

FDP_IFC.2 Complete information flow control

The TOE enforces the filter mechanism on all messages sent between the High network and the Low network when a filter file is active (O.FILTER).

FDP_IFF.1 Simple security attributes

The TOE enforces the information flow control SFP based on the attributes of the messages checked by the filter (O.FILTER). The TOE has an information flow control SFP that is non-configurable when filters have been loaded into the TOE (O.NO.CONFIG). The TOE protects the system from potential bypass of information related to management functions so that only predefined information elements are allowed between the High and Low internal domains (O.DOMAIN_SEPARATION).

FDP_IFF.6 Illicit information flow monitoring

Messages not complying with the filter specification are rejected and counted (O.FILTER). The TOE enforces a threshold of legitimate messages (O.FILTER_THRESHOLD). The Traffic Control Module (TCM) is a message filter that controls and restricts information between the internal domains (O.DOMAIN_SEPARATION).

FDP_ITC.2 Import of user data with security attributes

The TOE enforces the configuration access control policy (O.ACCESS_CONTROL) when importing filter files (O.FILTER_LOAD) and software updates (O.PROTECTED_CODE) from outside the TOE (O.SECURE_CHANNEL).

FIA_UAU.4 Single-use authentication mechanisms

The TOE manager must set passwords when initiating the TOE the first time and after password reset (O.ACCESS_CONTROL).

FIA_UAU.6 Re-authentication

The TOE requires password for reauthentication of Network Operator when network parameters are configured and of Security Operator when security parameters are configured, and after power on, zeroise, restart and after an inactive time limit (O.ACESS_CONTROL).

FIA_UID.1 Timing of identification

The TOE allows viewing alarms without password, all other menu items require password (O.ACCESS_CONTROL). Crypto destruct, zeroise, change of battery does not need password. Replacing SFP connectors requires Network Operator password before the TOE becomes operational.

FMT_MSA.1 Management of security attributes

The security attributes are non-configurable when installed on the TOE (O.NO.CONFIG). Management of security attributes is limited to the Security Operator (O.ACCESS_CONTROL).

FMT_MSA.3 Static attribute initialization

The default security attributes are non-configurable (O.NO.CONFIG) and (O.PROTECTED_CODE).

FMT_MTD.1 Management of TSF data

Filter files, trust anchors and SW updates, and configuration of security management data, can only be modified or changed by the Security Operator (O.ACCESS_CONTROL).

FMT_SMF.1 Specification of management functions

The security management functions available for the Security Operator (O.ACCESS_CONTROL) are selecting no traffic or filter operation, inject filter files, select active filter, adjust time and date, SW update, install DTAs and filter TAs, manage passwords and audit data.

FMT_SMR_EXT.1 Security roles

The TOE maintains roles with access control for the TOE managers (O.ACCESS_CONTROL).

FPT_FLS.1 Failure with preservation of secure state

The TOE is designed to fail in a safe manner. This includes failure as a result of self-test (O.CHECK_OPERATION) and failure that compromises the High/Low protection (O.FILTER). The TOE checks integrity during initiation, installation and operation and is rendered in a secure state in case of failures (O.CHECK_OPERATION).

FPT_PHP.3 Resistance to physical attack

The TOE has tampering mechanisms (O.TAMPER) and physical sealing (NO.SEALING) to protect the TOE against tampering.

FPT_STM.1 Reliable time stamps

Auditable events are stored with reliable time stamps (O.AUDIT).

FPT_TDC.1 Inter-TSF basic TSF data consistency

The TOE ensures consistent interpretation of TSF data when sent between TOE and other trusted IT system, when filter files are installed (O.FILTER_LOAD), SW updates are installed (O.PROTECTED_CODE) and TSF data is sent between management centre and TOE (O.SECURE_CHANNEL). The TOE ensures consistent interpretation of the TSF data through verification of digital signatures and self-tests (O.CHECK_OPERATION).

FPT_TST.1 TSF self-testing

Security critical functions are tested by a combination of power-up tests, periodic tests, and/or continuous tests, and the TOE checks the integrity of TSF data during operation and has periodic single event upset monitoring (O.CHECK_OPERATION).

FTP_ITC.1 Inter-TSF trusted channel

The TOE provides a trusted channel through a dedicated management interface using TLS for management purposes (O.SECURE_CHANNEL). The trusted channel is used for management configuration and for import of filter files (O.FILTER_LOAD), SW update files (O.PROTECTED_CODE) and collection of the audit log (O.AUDIT).

FTP_TRP.1 Trusted path

There is a trusted path from the local HMI to the TOE for authentication of the local user (O.ACCESS_CONTROL).

6.4 SFR DEPENDENCIES

Table 8 lists SFR dependencies and if the dependency SFRs are included.

SFR	Dependency	Included
FAU_ARP.1	FAU_SAA.1	YES
FAU_GEN.1	FPT_STM.1	YES
FAU_GEN_EXT.1	FAU_GEN.1	YES
FAU_SAA.1	FAU_GEN.1	YES
FAU_SAR.1	FAU_GEN.1	YES
FAU_STG.1	FAU_GEN.1	YES
	FTP_ITC.1	YES
FAU_STG.2	FAU_GEN.1	YES
FAU_STG.5	FAU_STG.2	YES
	FAU_GEN.1	YES
FCS_CKM.1	FCS_CKM.2 or	NO
	FCS_CKM.5 or	NO
	FCS_COP.1	YES
	FCS_CKM.3	YES
	FCS_RBG.1 or	NO

	FCS_RNG.1	YES
	FCS_CKM.6	YES
FCS_CKM.3	FDP_ITC.1 or	NO
	FDP_ITC.2 or	YES
	FCS_CKM.1 or	YES
	FCS_CKM.5	NO
FCS_CKM.6	FDP_ITC.1 or	NO
	FDP_ITC.2 or	YES
	FCS_CKM.1	YES
FCS_COP.1	FCS_ITC.1 or	NO
	FDP_ITC.2 or	YES
	FCS_CKM.1 or	YES
	FCS_CKM.5	NO
	FCS_CKM.3	YES
FCS_RNG.1	None	
FDP_ACC.1	FDP_ACF.1	YES
FDP_ACF.1	FDP_ACC.1	YES
	FMT_MSA.3	YES
FDP_IFC.2	FDP_IFF.1	YES
FDP_IFF.1	FDP_IFC.1	YES[1]
	FMT MSA.3	YES
FDP_IFF.6	FDP_IFC.1	YES[2]
FDP_ITC.2	FDP_ACC.1 or	YES
	FDP_IFC.1	YES[3]
	FTP_ITC.1 or	YES

[1] FDP_IFF.1 has a dependency to FDP_IFC.1, which is covered by FDP_IFC.2.

[2] FDP_IFF.6 has a dependency to FDP_IFC.1, which is covered by FDP_IFC.2.

[3] FDP_ITC.2 has a dependency to FDP_IFC.1, which is covered by FDP_IFC.2.

	FTP_TRP.1	YES
	FPT_TDC.1	YES
FIA_UAU.4	None	
FIA_UAU.6	None	
FIA_UID.1	None	
FMT_MSA.1	FDP_ACC.1 or	YES
	FDP_IFC.1	NO
	FMT_SMR_EXT.1	YES
	FMT_SMF.1	YES
FMT_MSA.3	FMT_MSA.1	YES
	FMT_SMR_EXT.1	YES
FMT_MTD.1	FMT_SMR_EXT.1	YES
	FMT_SMF.1	YES
FMT_SMF.1	None	
FMT_SMR_EXT.1	FIA_UID.1	YES
FPT_FLS.1	None	
FPT_PHP.3	None	
FPT_STM.1	None	
FPT_TDC.1	None	
FPT_TST.1	None	
FTP_ITC.1	None	
FTP_TRP.1	None	

Table 8: SFR dependencies

7. TOE SUMMARY SPECIFICATION

7.1 TOE SECURITY FUNCTIONS

This section describes the security functions provided by the TOE to meet the SFRs specified in chapter 6.1.

7.1.1 SF.ACCESS_CONTROL

The TOE supports three roles determining the user's privilege level:

- Security Operator – Administrative role with privileges for managing the security management configuration, such as adjusting the real-time clock, inject filter files, software updates, DTA and filter TA management).
- Operator – Operational role with read access
- Network Operator – Operational role with privileges for managing network functions

The TOE roles are created as part of the implementation. Passwords are set in the initial configuration process.

The TOE allows the Security Operator to manage device settings:

- Change passwords
- Set time
- Configuration of security parameters
- Software update
- Filter management
- DTA management

The TOE enforces role-based authentication consisting of a role password, and a removable Cryptographic Ignition Key (CIK). The CIK is common for all users and a valid CIK must be inserted for the device to be operational. Only one local user can be logged in at a time, but it is possible to log in from external management and local HMI at the same time.

7.1.2 SF.ANTI_TAMPER

The TOE has protective measures to detect and resist tampering attempts. The TOE stores evidence of tampering attempts in the audit log, and is constructed in such a way that physical tampering attempts are evident upon visual inspection. When the TOE detects tampering, the tampering mechanisms are activated, security critical information is erased, and the system will not go back to its normal operational state. The TOE has physical sealing to detect tampering.

7.1.3 SF.AUDIT

The TOE maintains an audit log recording all security related events. Each audit entry contains an event name, time, date and a reference to the role (Operator, Network Operator or Security Operator) logged in at the time of the occurrence. The audit log is collected by the management centre or other log server over a secure channel.

7.1.4 SF.CONFIGURATION_ACCESS_CONTROL

The configuration access control function provides secure import of configuration data by means of access control and certificate-based verification of integrity and authenticity for configuration files:

- Verification of imported filter files
- Verification of imported SW update files
- Verification of imported DTAs and filter TAs

The security function ensures that security configuration file import can only be initiated after a TOE operator has explicitly authorized the operation.

The TOE performs integrity checks when filter files, SW update files, DTAs and filter TAs are imported and when booting. Filter files are integrity checked when a filter file is selected to be the active filter.

Management data between the management centre and the TOE is protected by TLS.

7.1.5 SF.CRYPTO

The TOE provides endorsed cryptographic functions for protecting the security critical information on the TOE. The TOE generates keys for internal use. The TOE implements a random number generator for generating internal keys.

7.1.6 SF.DOMAIN_SEPARATION

The TOE restricts information flow between the Red (High) and Black (Low) internal domains and validates the information before it is exchanged between the internal domains. The TOE validates messages between the internal domains so that only predefined information elements with well-defined message formats are allowed to pass through the Traffic Control Module (TCM) between the High and Low internal domains.

7.1.7 SF.FAIL_SECURE

The TOE is designed to handle failures without violating the trusted functionality. If the TOE fails, it will restart, or enter a failure mode disabling all functionality, rendering the TOE in a secure state.

7.1.8 SF.FILTER_THRESHOLD

The TOE can monitor the rate of flow of legal messages through the filter mechanism. A threshold value for each legal message type can be set in the filter definition files. The threshold value cannot be changed in the TOE. The TOE generates an audit event when the rate of flow exceeds the threshold value.

7.1.9 SF.INFORMATION_FLOW_CONTROL

The TOE controls the separation of High and Low information and the information flowing from the High to the Low network and Low to High network. The flow control rules are based on:

- All messages between the High and Low networks are checked in the filtering mechanism
- The TOE manager can select between installed sets of predefined filter files
- Messages that do not comply with the SFP are rejected
- The number of rejected messages are counted and available in the management centre

7.1.10 SF.SECURITY_STATES

The TOE implements a state machine for internal security states. The state machine enforces restrictions on information flow and the allowed operations for each of the internal states. The TOE is designed to handle

failures without violating the trusted functionality. If the TOE fails, it will restart or enter a failure mode disabling all functionality.

7.1.11 SF.SELF_TEST

The self-test function detects errors in security critical functions. Whenever the TOE boots, the internal integrity is verified and self-tests are performed. During operation periodic self-tests detect filter errors and hardware or software errors. The TOE will raise a local alarm and reboot if critical errors are detected.

7.1.12 SF.ZEROISE

The TOE has a zeroise mechanism which will destruct all crypto material and user data contained inside the TOE. After a zeroise it is possible to boot the system.

Anyone with physical access, or privileged remote access (from the management centre), to the TOE can activate the zeroise function.

7.2 TOE SUMMARY SPECIFICATION RATIONALE

Table 9 shows how TOE Security Functions (SF) satisfy SFRs.

TOE security functions	SFRs	Description
SF.ACCESS_CONTROL	FMT_SMF.1 FMT_MTD.1 FMT_SMR_EXT.1 FIA_UAU.4 FIA_UAU.6 FIA_UID.1	The security function implements access control to the security management functions for the TOE (FMT_SMF.1, FMT_MTD.1). Users are required to set the password at initiation of the device and first-time login (FIA_UAU.4). The TOE provides distinct roles (Security Operator, Network Operator and Operator) (FMT_SMR_EXT.1), for controlling access to TOE functionality. Each role has a set of associated security attributes that includes privileges, password, and status (password change needed or lockout state) (FIA_UAU.6). After a CIK has been inserted, but prior to user authentication, the TOE provides a limited set of functionality to the user, including zeroise and crypto destruct (FIA_UID.1).
SF.ANTI_TAMPER	FPT_PHP.3 FCS_CKM.6 FAU_SAA.1 FMT_MSA.1	The TOE implements anti-tampering mechanisms that are always available (FPT_PHP.3). Key material is destructed upon tamper activation (FCS_CKM.6). Potential security violations are detected and result in tampering, reboot or halt operation (FAU_SAA.1). There is no opportunity to modify, change filter files after a Zeroise as they are erased (FMT_MSA.1).

SF.AUDIT	FAU_GEN.1 FAU_GEN_EXT.1 FAU_SAR.1 FAU_STG.1 FAU_STG.2 FAU_STG.5 FMT_MTD.1 FPT_STM.1 FTP_ITC.1	The TOE audit function records auditable events in an audit log (FAU_GEN.1). The TOE audits all security related operations and associates the operations with the active role (FAU_GEN_EXT.1). The TOE permits authorized users to inspect the audit log (FAU_SAR.1). The stored events cannot be modified or deleted. (FAU_STG.1). The audit log can be collected by an external management/log server. The TOE audit trail cannot be modified and is protected from deletion (FAU_STG.2). The audit mechanism overwrites the oldest stored audit records when the audit storage is full (FAU_STG.5). The TOE has a built-in real-time clock used for time stamping audit events (FPT_STM.1). The management system collects the audit log via a trusted channel protected by TLS (FTP_ITC.1).
SF.CONFIGURATION_ACCESS_CONTROL	FTP_ITC.1 FTP_TRP.1 FDP_ITC.2 FCS_COP.1 FDP_ACC.1 FDP_ACF.1 FPT_TDC.1 FMT_MSA.1 FMT_MSA.3	Security configuration files are imported into the TOE from a secure dedicated interface from remote management (FTP_ITC.1) or by local users (FTP_TRP.1). The TOE performs secure configuration by verified and authenticated import of security configuration files (FDP_ITC.2). The TOE enforces access control on TOE managers installing security configuration files (FDP_ACC.1). The TOE provides security attribute-based access control on subjects, objects and dynamic parameters of the TOE (FDP_ACF.1). The TOE interprets the security configuration files in a consistent manner (FPT_TDC.1). The ability to change security attributes is restricted (FMT_MSA.1 and FMT_MSA.3). The TOE uses endorsed cryptographic functions for cryptographic operations (FCS_COP.1).
SF.CRYPTO	FCS_CKM.1. FCS_CKM.3 FCS_CKM.6 FCS_COP.1 FCS_RNG.1	The TOE generates keys according to endorsed cryptographic methods (FCS_CKM.1). TOE uses a key wrap function to encrypt/decrypt all internal keys (FCS_CKM.3). Key material is destructed according to endorsed cryptographic methods (FCS_CKM.6).

		The TOE verifies and authenticates security configuration files when they are installed, and provides confidentiality protection of security critical information stored on the TOE (FCS_COP.1). The TOE contains a random number generator for generating internal keys (FCS_RNG.1).
SF.DOMAIN_SEPARATION	FDP_IFF.1 FDP_IFF.6	The security function provides separate internal domains for configuration, management and signalling data between High and Low internal domains to restrict the information flow between the domains to well defined information elements with rate limitation (FDP_IFF.1) and (FDP_IFF.6).
SF.FAIL_SECURE	FPT_FLS.1	The fail secure function preserves a secure state after failure by shutting down the Ethernet interfaces and rebooting the unit (FPT_FLS.1).
SF.FILTER_THRESHOLD	FAU_GEN.1 FDP_IFF.6	The TOE filter threshold function monitors the rate of flow through the filter and generates an audit if the threshold is exceeded (FAU_GEN.1) and (FDP_IFF.6).
SF.INFORMATION_FLOW_CONTROL	FDP_IFC.2 FDP_IFF.1 FDP_IFF.6 FPT_FLS.1	The TOE information flow control controls all information flows through the filter (FDP_IFC.2/Traffic data) determined by the filter specification (FDP_IFF.1) and all information between internal high and low domains through management interface (FDP_IFC.2/Internal. The TOE monitors the number of rejected messages (FDP_IFF.6). When a filter failure is detected, the TOE stops all traffic through the filter (FPT_FLS.1).
SF.SECURITY_STATES	FIA_UID.1 FDP_ACC.1 FDP_ACF.1 FIA_UAU.6 FPT_FLS.1 FDP_IFC.2 FDP_IFF.1	The security function handles transitions between security states as well as power states. The security function has complete control over all interfaces and available functionality (FIA_UID.1, FDP_ACC.1, FDP_ACF.1, FDP_IFC.2, FDP_IFF.1). The security function forces users to reauthenticate after specific state transitions, including CIK in/out events, restart and power state changes (FIA_UAU.6). The security function preserves a secure state if a failure occurs (FPT_FLS.1).
SF.SELF_TEST	FAU_ARP.1 FAU_SAA.1 FCS_COP.1	The TOE raises an alarm in case of an error in the filter function or other security violations (FAU_ARP.1).

	FPT_TST.1 FPT_TDC.1 FPT_FLS.1	Self-testing detects potential security violations (FAU_SAA.1). The TOE verifies the signature of filter files when they are installed and activated during operation (FCS_COP.1) The self-test function performs power-on self-tests and periodic tests during operation to detect abnormal situations (FPT_TST.1) and to verify security critical functionality (FPT_TDC.1) and takes action when failures are detected (FPT_FLS.1).
SF.ZEROISE	FAU_SAA.1 FCS_CKM.6 FMT_MSA.1	The TOE erases key material (FCS_CKM.6) when the device is zeroised (FAU_SAA.1). There is no opportunity to modify, change filter files after a Zeroise as they are erased (FMT_MSA.1).

Table 9: Security functions satisfy SFRs

8. NOTES

8.1 ACRONYMS AND ABBREVIATIONS

CC	Common Criteria
CDS	Cross Domain Solution
CIK	Cryptographic Ignition Key
DTA	Device Trust Anchor
EAL	Evaluation Assurance Level
FW	Firmware
FPGA	Field Programmable Gate Array
HMI	Human Machine Interface
HSP	High Security Platform
HW	Hardware
IP	Internet Protocol
IT	Information Technology
LED	Light Emitting Diode
NSM	Norwegian National Security Authority
OSP	Organizational Security Policy
RNG	Random Number Generator
SF	Security Function
SFP	Security Functional Policy
SFR	Security Functional Requirement
ST	Security Target
SW	Software
TA	Threat Agent
TA	Trust Anchor

TCM	Traffic Control Module
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSF 401	Trusted Security Filter 401 (product name)

8.2 DEFINITIONS

High domain (red)	The domain on High side towards the higher classified network
Low domain (black)	The domain on Low side towards the lower classified network.
Security configuration files	Filter files, SW updates, SW/FW images, DTAs, filter TAs, initial configuration files.
Endorsed crypto	Cryptographic methods, algorithms, key types, sizes and standards that are endorsed and evaluated by NSA and NATO security authorities.
HSP	High Security Platform is a HW/SW/FW platform with common functionality and features that are shared with other products.
Random Generator test	A number of operational tests of the Random Number Generation function.
Single event upset scanning	Single event upset monitoring that runs periodically to verify the integrity of the programmable logic. The function detects any configuration change in the programmable logic. Action is taken in case of failure events or tamper detection.