Security Target Lite

for

TactiGuard PG

Record of Changes

Revision	Date	Changed By	Change Description
0.1	2026-03-27	ASPE	Lite version of TactiGuard PG – Security Target (SVP-35), version 11.
1	2026-03-27	ASPE	Updated according to review sheet (M-files: SVP-426). Released.
2	2026-05-01	ASPE	Updated according to review sheet (M-files: SVP-443). Released.
2.1	2026-05-04	ASPE	Updated due to Jira observation PGCCP-452 (Version number).
3	2026-05-05	ASPE	Updated according to review sheet (M-files: SVP-448). Released.
3.1	2026-05-18	ASPE	Updated due to Jira observation PGCCP-461.
4	2026-05-18	ASPE	Updated according to review sheet (M-files: SVP-456). Released.
4.1	2026-05-20	ASPE	Updated du e to Jira observation PGCCP-460 and PGCCP-462.
5	2026-05-21	ASPE	Updated according to review sheet (M-files: SVP-457).
5.1	2026-05-22	ASPE	Updated du e to Jira observation PGCCP-465.
6	2026-05-26	ASPE	Updated according to review sheet (M-files: SVP-459).
6.1	2026-05-28	ASPE	Updated due to Jira observation PGCCP-466.
7	2026-05-29	ASPE	Updated according to review sheet (M-files: SVP-460).
7.1	2026-05-29	ASPE	Updated due to Jira observation PGCCP-467.
8	2026-05-29	ASPE	Updated according to review sheet (M-files: SVP-462).

Table of Contents **Page**

1 Introduction

1.1 Purpose

This document is the Security Target Lite for the TactiGuard PG product named in this document as Target of Evaluation (TOE).

1.2 References

Ref. No	Title	ID
1.	Common Criteria Part 1: Introduction and general model Part 2: Security functional components Part 3: Security assurance components Part 4: Framework for the specification of evaluation methods and activities Part 5: Pre-defined packages of security requirements November 2022, CC:2022 Revision 1	CCMB-2022-11-001 CCMB-2022-11-002 CCMB-2022-11-003 CCMB-2022-11-004 CCMB-2022-11-005
2.	TactiGuard PG - Configuration Parameters	M-files: SVP-46
3.	TactiGuard PG - PG Protocol	M-files: SVP-47
4.	TactiGuard PG - Installation Guidance	M-files: SVP-48
5.	Security Target for L4Re Secure Separation Kernel CC 1.0.2 Microkernel BSI Certification ID: BSI-DSZ-CC-1177-v2-2026 Kernkonzept GmbH	M-files: SVP-453
6.	L4Re Configuration Guidance Kernkonzept GmbH	M-files: SVP-183
7.	TactiGuard PG - User Guidance	M-files: SVP-71
8.	TactiGuard PG - Manufacturing Procedure	M-files: SVP-237

Table 1 References.

1.3 Terms & definitions

Word/abbreviation/acronym	Explanation
BLACK information	Unclassified information or Classification lower than RED classification. The actual classification is dependent by the actual use or deployment of TOE.
CC	Common Criteria.
Compartment	A Compartment is a process controlled by the Microkernel, where each process is separated from each other. IPC based communication can be used for communication between the processes.
Doc	Document.
EAL	Evaluation Assurance Level.
IP	Internet Protocol.
IPC	Inter Process Communication.
M&A	Management and Authentication.
NIC	Network Interface Card.
NTP	Network Time Protocol.
OS	Operating System.
OSP	Organizational Security Policies.
PG	Parameter Guard.
PP	Protection Profile.
RED information	Classified information. The actual classification is dependent on the actual use or deployment of TOE.
RTC	Real-time Clock.

Word/abbreviation/acronym	Explanation
SF	Security Function.
SFP	Security Functional Policy.
SFR	Security Functional Requirement.
SHA	Secure Hash Algorithms
ST	Security Target.
SW	Software.
TOE	Target of Evaluation.
TSF	TOE Security Function.
TSF data	Data for the operation of TOE upon which the enforcement of the SFR relies.
UDP	User Datagram Protocol.

Table 2 Terms and abbreviations.

2 TOE Introduction

2.1 ST Reference

The security target is identified as:

Title:	Security Target (ST) for TactiGuard PG
Version:	18
Authors:	ASPE
Publication Date:	2026-05-29
Doc. Number:	SVP-35

2.2 TOE Reference

The TOE is identified as:

Name:	TactiGuard PG
Stock Number:	111499
Version:	1.0.1

2.3 TOE Overview

Common security practice is to separate a system into sub-systems with different classification level. Higher classified sub-system might need to exchange information with lower or non-classified subsystem and requires a security mechanism with high assurance for that purpose.

In Figure 1 an example is provided, where a user on the higher classified system needs to perform configuration of a radio located on the lower or non-classified system. The parameter settings entered by the user is lower or non-classified information and shall be transmitted to the lower or non-classified system, such that leakage of classified information to the lower or non-classified sub-system is prevented. The TactiGuard PG is the trusted product with high assurance requirements for that purpose.

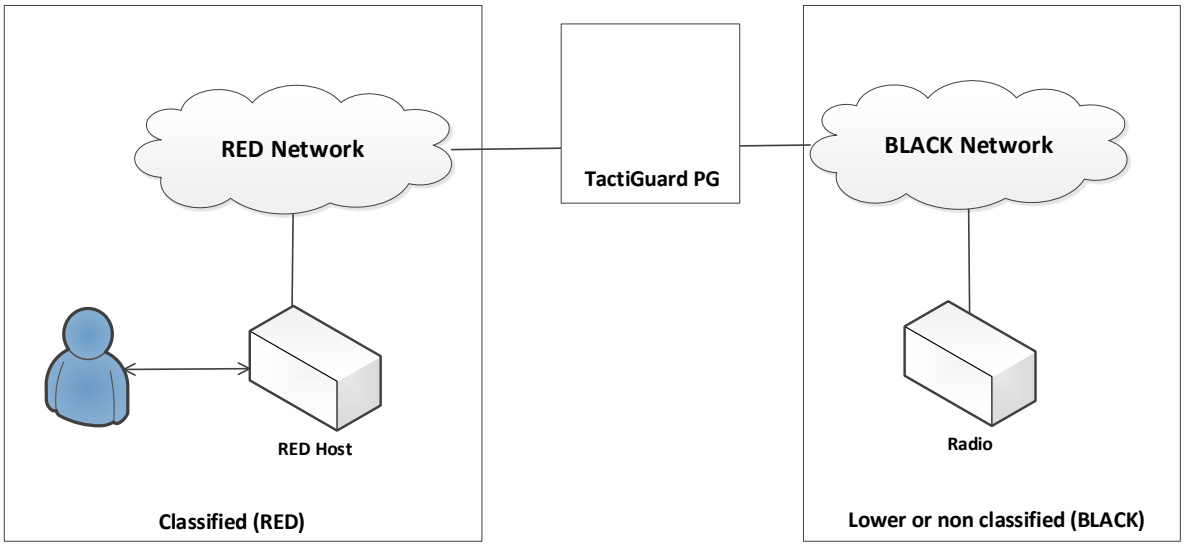

Figure 1 TOE usage example for configuration of a Radio on lower or non-classified system from the classified system.

In general the Hosts located on a RED network shall be able to send Configuration Parameters to Hosts located on a BLACK network. To be sure that only BLACK configuration values are transmitted to the BLACK network a security mechanism is required.

The main objective is to secure that no classified information is released to the lower or non-classified networks, when the Configuration Parameters are sent.

The BLACK hosts, their Configuration Parameters and the allowed numerical values are known. Hence, it is possible to have a Whitelist of possible parameters to set and their allowed values in a static table from which they can be compared. In this way only very constrained information is send from the RED Hosts to the BLACK network and provides a strong contents filtering mechanism.

2.3.1 Usage and major security features of TOE

TOE performs the filtering based on a very constrained use of host ID, parameter ID and value(s), such that simple numerical comparison and range check can be applied. The Whitelist is defined in accordance with the syntax defined in Configuration Parameter for TactiGuard PG [2].

TOE can pass all information on from BLACK to RED network without restrictions.

The TOE is running on a Microkernel which provides separation of compartments, allowing multiple sub-systems to run in isolation. The Microkernel also provides mechanisms for controlling the communication between compartments. Together this allows for a strong separation of sub-systems into logically separate components.

The TOE and Microkernel are installed together on a computer and booted securely by utilising the Secure Boot of the Computer according to the Installation Guidance [4].

An authorised user with role Administrator or Configurator defines the allowed parameters to be sent from the RED System to the BLACK system by writing the allowed values in the Whitelist.

Only transmission of data in accordance with the defined transport protocol shall be transmitted, called Session Protocol [3]. Attempts of non-compliant communication are denied and audit events for the attempt will be stored.

An authorised user with role Administrator, Configurator or Auditor can read the audit event log.

TOE provides the following features:

- TOE provides access control, such that audit events can be read and configuration of Whitelist can be performed.
- TOE makes sure that the only allowed transport of parameters is in accordance with the Session Protocol.
- TOE makes sure that the request is transmitted if and only if the request is in the Whitelist.
- TOE stores audit information for all requests.

2.3.2 TOE Type

Software for Data Transfer and Content Filtering.

Main Objective: Confidentiality of RED System (Prevention of leak from RED to BLACK System).

2.3.3 Required non-TOE hardware/software

Required non-TOE hardware/software:

- External Computer and USB Storage providing the following:
  - Editing the Whitelist.
  - Copy Whitelist to attached USB storage, such that the Whitelist can be imported into TOE.
- Server with x86_64 CPU, disk storage, 2 Network Interface Cards (NIC) and optional an additional NIC and provides the following functionality:
  - The two NICs are respectively used for the BLACK and RED network connection.
  - Optional NIC (BLUE) for monitoring purpose.
  - Secure boot for secure start.
  - Real-time Clock (RTC).
  - The Server executes the Microkernel and TOE.
- Microkernel executes on the Server and provides the following functionality:
  - Domain separation between Compartments.
  - Controlled information flow between Compartments to prevent bypass of TOE.
  - Access control to hardware devices, such as NIC and disk storage.
  - Secure start up.
- Linux, providing the following functionality:
  - Access to hardware device from a Compartment.

- Access to communication between Compartments.
- Ability to, optionally, send a copy of audit events to an external log collector.

- Time source on either RED or BLACK network supporting Network Time Protocol (NTP).

The following figure provides an overview over the required items and their interconnections.

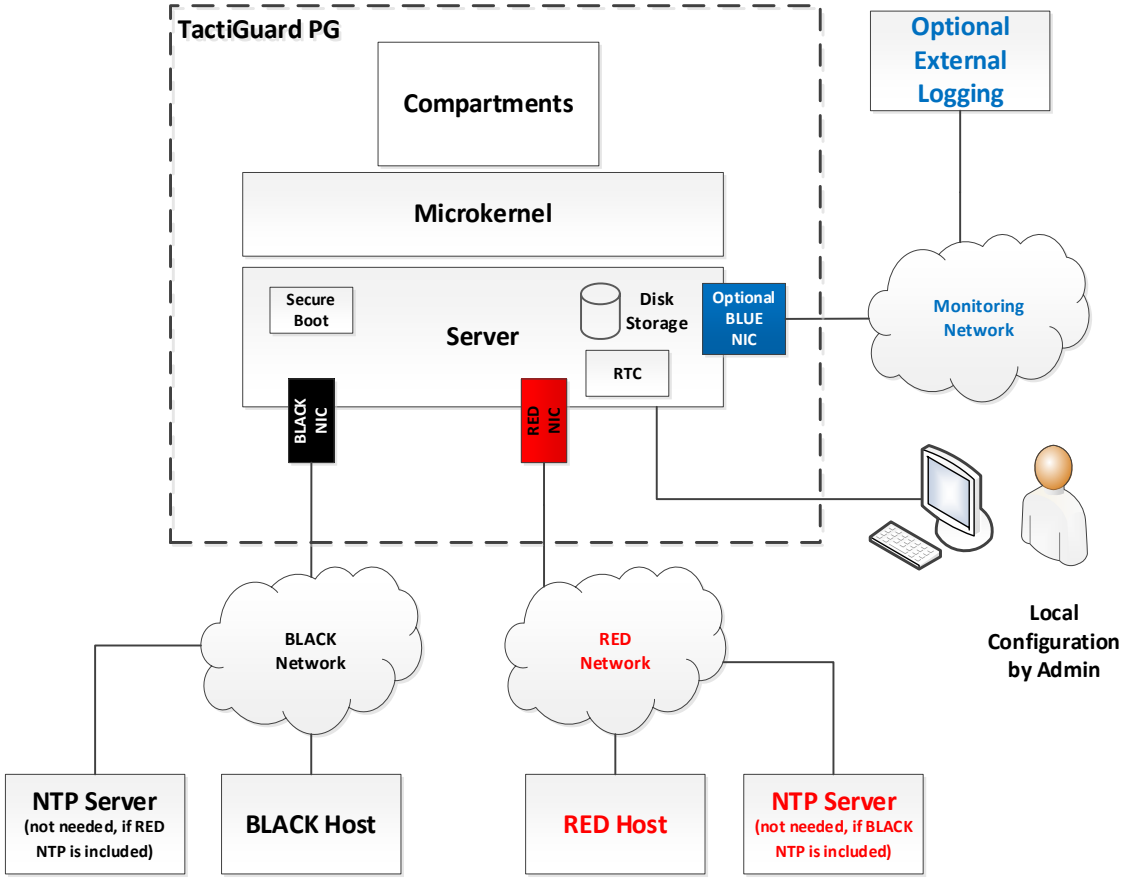

Figure 2 Overview of the complete solution. Compartments is comprised of native applications and Linux virtual machines which execute the TOE and TOE-supporting functionality.
TactiGuard PG is the Cross Domain appliance.

2.4 TOE Description

2.4.1 TOE Life Cycle

The following steps defines the overall life cycle of TOE:

1) At Saab Danmark TOE Development.

2) At Saab Danmark Manufacturing is performed in accordance with Manufacturing Procedure [8].

3) An Installer perform the installation of TOE in accordance with Installation Guidance [4].

4) TOE is operated by the user roles Administrator, Configurator and Auditor in its target operational environment according to the User Guidance [7].

5) Saab Danmark performs Maintenance of TOE.

2.4.2 Physical Scope of TOE

The output from the TOE development phase (Lifecycle step 1 in section 2.4.1) consists of the following internal delivery items:

No.	Type	Identified	Release
1	SW	TactiGuard PG	File name: tactiguard-pg-1.0.1.tar.gz Version: 1.0.1
2	Doc	Installation Guidance for TactiGuard PG M-files: SVP-48 Saab Danmark A/S	File name: TactiGuard PG – Installation Guidance.pdf Version: 4
3	Doc	User Guidance for TactiGuard PG M-files: SVP-71 Saab Danmark A/S	File name: TactiGuard PG – User Guidance.pdf Version: 4

Table 3 Development delivery items.

The Development delivery items are input for Manufacturing, as described in section 2.4.3. Verification of correct versions for software (item no. 1 in above table) and documentation (item no. 2 and 3 from Table 3) is performed according to the Manufacturing Procedure [8] inside the Secure Development Environment.

The output from the Manufacturing (Lifecycle step 2 in section 2.4.1) is defined by the following table:

No.	Form of delivery	Identified	Contains
1	Manufactured software digital archive	tactiguard-pg-<stock number>-<version>.iso	Software for installation on supported hardware, including TactiGuard PG (item no. 1 from Table 3).
2	Manufactured documentation digital archive	tactiguard-pg-doc-<stock number>-<version>.zip	Documentation supporting the TactiGuard PG, including Installation (item no. 2 from Table 3) and User Guidance (item no. 3 from Table 3).

Table 4 Manufacturing delivery item.

The stock number and version will be resolved during the Manufacturing for a given server. A SHA-256 hash value is created for each of the Manufactured digital archive during Manufacturing for a given server.

The integrity and authenticity of the Manufactured digital archives, and hence the TOE, shall be verified using two hash values, which are delivered via a separate secured (authenticity) channel. The secure channel is agreed upon with the individual customer. The Installer performs the verification before installation.

The Manufactured digital archives shall be protected for confidentiality by encryption or organisational means. The selection on these means is flexible, such that particular customer's preferred protections can be utilised.

2.4.3 Logical Scope of TOE

The logical scope is shown in the following figure.

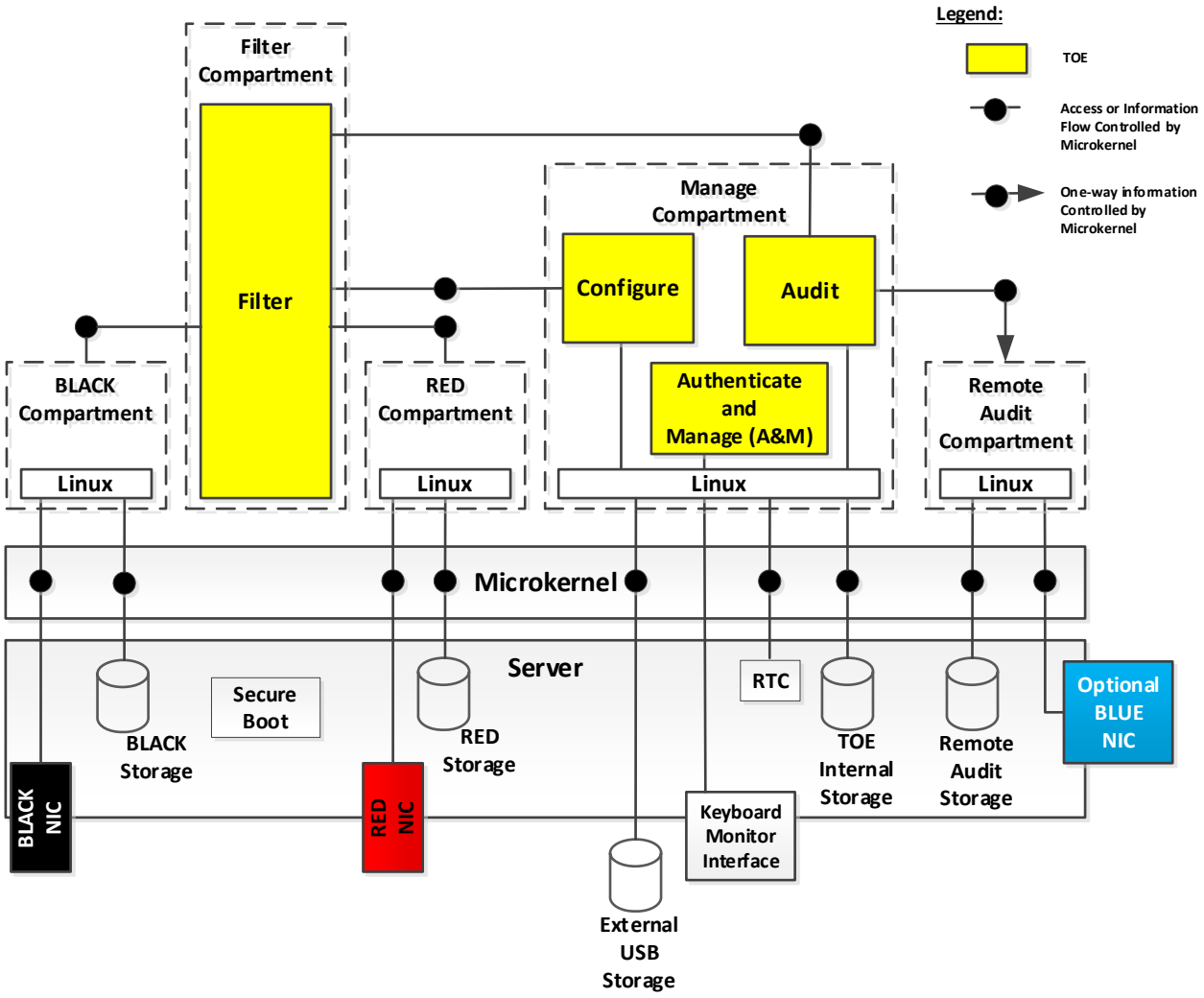

Figure 3 TOE overview.

All compartments are executed within its own security domain and all compartments, except the Filter compartment, has its own underlying Linux providing access to drivers and supporting functionality.

- Configure: Responsible for managing the lifetime of TOE. This includes loading the configuration from storage and providing it to the Filter component.

- Audit: Responsible for receiving and storing audit events from TOE, and optionally forwarding a copy to an external log collector. The actual transmission of events to an external log collector is out of scope of the TOE and will be provided by Linux.

- Filter: Responsible for performing the actual filtering of messages going from the RED Compartment to the BLACK Compartment and forwarding messages going from the BLACK Compartment to the RED Compartment. Multiple instances of Filter may exist, such that concurrent filtering can occur as shown in Figure 4.

- Authenticate and Manage (A&M): Responsible for authenticating administrative users and providing Local Access to configure or audit the TOE. Authentication is performed before any configuration action can take place. Authenticate and Manage provides a text-based user interface (TUI) for the user interaction.

The underlying Microkernel enforces separation of Compartments and information flow control between them. A Build Configuration for the Microkernel defines the Compartments in the system. The possible information flow and access to hardware devices are defined by the execution context of each defined Compartment and hereby part of TOE.

During Manufacturing the following is configured:

- Only BLACK Compartment has access to the BLACK NIC, which is Build Configured and enforced by the Microkernel.

- Only RED Compartment has access to the RED NIC, which is Build Configured and enforced by the Microkernel.

- Only Remote Audit Compartment has access to the BLUE NIC, which is Build Configured and enforced by the Microkernel. The communication between TOE and Remote Audit Compartment is one-way, such that potential attacks from the BLUE network is mitigated. Remote Audit Compartment is responsible for the forwarding of audit event to the remote logging server on the BLUE monitoring network and is optional functionality.

- The Remote Audit Compartment functionality can, as an alternative, be located at the RED Compartment. The communication from Manage Compartment is still one-way to the RED Compartment, such that potential attacks from the RED network is mitigated. The Remote Audit Compartment will in this case not exist in Figure 3.

- External USB Storage is used for the import of the Whitelist. Only Management Compartment has access to External USB Storage, and is enforced by the Microkernel.

- TOE Internal Storage is used for storage of Whitelist (configuration data of TOE), Audit (internal audit event log) and M&A Data (Management and Authentication data of TOE). Only Management has access to TOE Internal Storage. The access to Internal Storage is enforced by the Microkernel.

- Real-time Clock (RTC) is used for providing time to Linux at the Manage Compartment for the Audit time stamps.

- RED, BLACK and Remote Audit Storage are used for each compartment and access to the storage is enforced by the Microkernel.

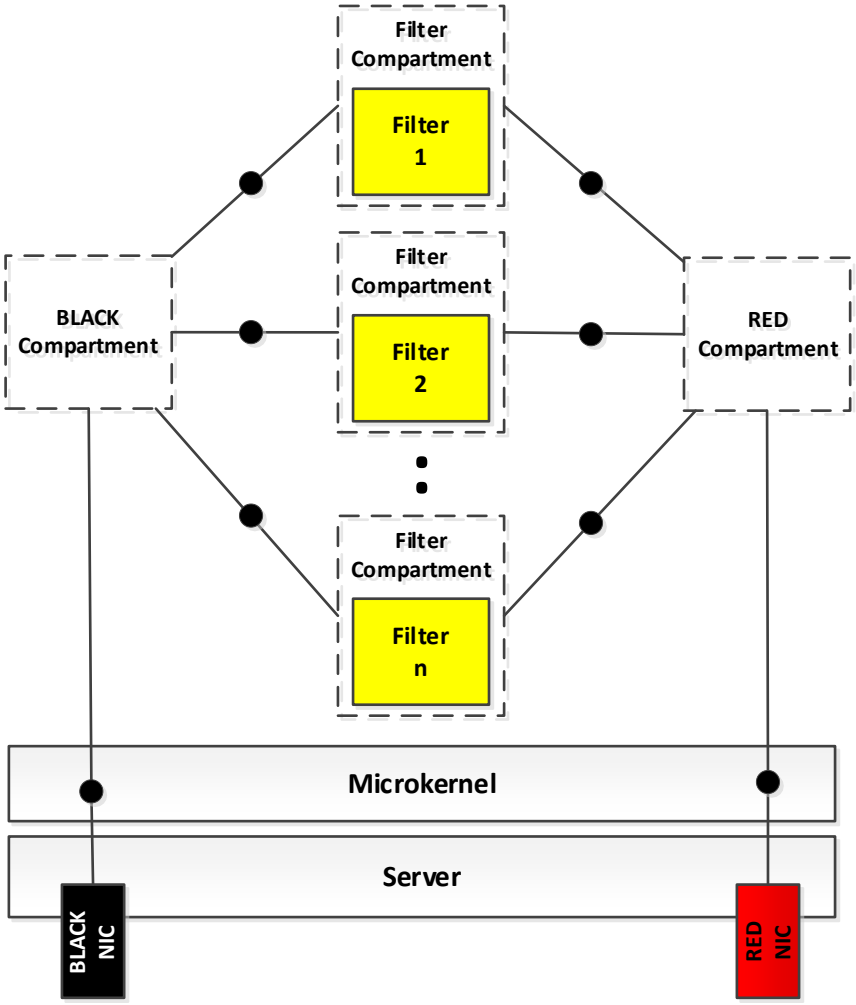

Figure 4 Multiple filter compartments.

The Server has multiple CPU cores, some of which are assigned to RED, BLACK, Management and Remote Audit Compartments. An upper bound of 9 Filter instances may exist, to provide concurrent filtering. At manufacturing time, the actual number of filter instance are set and is dependent on the number of free cores and available RAM.

Network communication paths, to each instance of the Filter Compartment, are defined in RED and BLACK Compartments, at manufacturing time, by assigning a UDP port number to each Filter Compartment instance.

The Administrator or Configurator role may, at runtime, assign a Whitelist to each Filter Compartment instance. Each Filter Compartment is thereby assigned its own CPU core, UDP port number and Whitelist.

The maximum number of Filter Compartments is 9.

3 Conformance Claims

3.1 CC Conformance Claim

The ST is Common Criteria CC:2022 R1 Part 2 conformant and Part 3 conformant; no extended components have been defined.

3.2 PP Claim

The ST does not claim conformance to any registered Protection Profile.

3.3 Package Claim

The ST claims conformance to the EAL4 assurance package augmented with ALC_FLR.3 as defined in Part 5 of the Common Criteria CC:2022 R1.

Note: The intended Evaluation Assurance is EAL5, but the certification claim is EAL4, due to the EUCC Certification Scheme.

3.4 Conformance Rationale

No conformance rationale is necessary for this evaluation since this ST does not claim conformance to a Protection Profile.

4 Security Problem Definition

The purpose of the security problem definition is to define the scope and nature of the security problem the TOE is intended to address.

The environment to which the TOE shall cope with is defined as a number of assets, threat agents, threats, assumptions and policies.

The security problem definition consists of identified assumptions about the environment, threats to assets and organizational security policies.

To facilitate easy definition of threats, organisational security policies, assumptions, security objectives and security requirements, the subjects, objects and operations to be used in the ST are defined first.

The personnel that interact with the TOE are:

Subjects	
Short name	**Description**
S.ADMIN	Authenticated authorised administrator of the TOE.
S.CONFIGURATOR	Authenticated authorised Whitelist configurator of the TOE.
S.AUDITOR	Authenticated authorised auditor with read only rights for reading audit events provided by TOE.
S.INSTALLER	Installer of TOE.

Table 5 Personnel subjects.

The systems (equipment) that interact with the TOE are:

Subjects	
Short name	**Description**
S.RED_HOST	Host located on the RED network.
S.BLACK_HOST	Host located on the BLACK network.

Table 6 Equipment subjects.

The (data) objects for the TOE:

Objects	
Short name	**Description**
O.PARAMETER	Parameter addressing and values to be set on resources located on black network.

Table 7 Objects.

TOE will operate upon:

Operations	
Short name	**Description**
Send	Send O.PARAMETER from S.RED_HOST to S.BLACK_HOST.

Table 8 Operations.

4.1 Threats

4.1.1 Assets

Assets	
Short name	**Description**
AS.RED_INFORMATION	Classified information located on the RED System.

Table 9 Assets.

4.1.2 Threat Agents

The following subjects are capable to effectuate threats for the TOE (i.e. Threat Agents):

Threat Agents	
Short name	**Description**
TA.EXTERNAL	Personnel or resources of the BLACK System with no authorized access to the RED System. These threat agents may try to access the Classified Information (AS.RED_INFORMATION).
TA.MONITORING	Personnel or resources of the Monitoring Network with no authorized access to the RED System. These threat agents may try to access the Classified Information (AS.RED_INFORMATION).
TA.INTERNAL_RESOURCE	Internal resources of the RED System, which are not authorised to send information through TOE. These threat agents may try to send Classified Information (AS.RED_INFORMATION) such that they can be released outside the RED System.
TA.HOST	Authorized Hosts on the RED network (S.RED_HOST) allowed to send Parameter(s) via the TOE may unintentionally release classified information (AS.RED_INFORMATION) to the BLACK network.
TA.NON_TOE	Non-TOE Compartment executing on the Microkernel.
TA.ADMIN	Authenticated authorized administrator of the TOE.

Table 10 Threat Agents.

4.1.3 Identification of Threats

Threats	
Short name	**Description**
T.EXTERNAL_ATTACK	TA.EXTERNAL may manipulate or attack TOE, such that RED Information (AS.RED_INFORMATION) could leak to the BLACK Network.
T.MONITORING_ATTACK	TA.MONITORING may manipulate or attack TOE, such that RED Information (AS.RED_INFORMATION) could leak to the BLACK Network..
T.INTERNAL_LEAK	TA.INTERNAL_RESOURCE may bypass TOE, such that RED Information (AS.RED_INFORMATION) could leak to the BLACK Network.
T.MISUSE	TA.INTERNAL_RESOURCE or TA.HOST may send RED Information (AS.RED_INFORMATION) via TOE to the BLACK Network.
T.NON_TOE	TA.NON_TOE might influence the internal communication between Compartments of TOE. Furthermore, unauthorised access to hardware devices, e.g. access to BLACK NIC and RED NIC.
T.LOCAL_ATTACK	A local attacker may compromise the installed TOE by malicious installation and configuration of TOE.

Table 11 Threats.

4.2 Organizational Security Policies (OSPs)

OSP	
Policy	**Description**
P.SEPARATION	Classified information shall not be released to lower classified or non-classified systems.

Table 12 Organizational Security Policies.

4.3 Assumptions

The following are threats handled as assumptions, since it is not the TOE's responsibility to counter these threats.

Assumptions	
Assumption	**Description**
A.RED_SYSTEM	RED System is secured according to security measures for the contained information, e.g. Classified Information (AS.RED_INFORMATION).
A.BLACK_SYSTEM	BLACK System is secured according to security measures for the contained information.
A.SECURE_LOCATION	TOE is located in a secure area during storage and operation.
A.SECURE_PLATFORM	TOE is executing on a securely configured BIOS and a security certified Microkernel [5] providing separation of Compartments, Information Flow (including one-way communication between compartments) and Access Control to hardware devices. The configuration of the Microkernel shall be in accordance with the provided guidance for the Microkernel [6] and be in accordance with the defined compartments and information flow as defined in Figure 3. Linux provides supporting device drivers, network stack, reliable time, libraries and, for RED and BLACK OS, a firewall. Server provides trusted Secure Boot. Cryptography and hashing are not in the scope of the TOE. SHA-256 is used and is provided by a library adhering to the FIPS 180-4 standard.

Table 13 Assumptions.

5 Security Objectives

The high-level solution is divided into a two parts solution, one part is the TOE, and the second part is the operational environment of TOE. Each part of the high-level solution has its own set of objectives to address the security problem.

5.1 TOE Security Objectives

TOE Security Objectives	
Objective	**Description**
OT.ALLOWED_PROTOCOL	The transfer between RED System and BLACK System shall only allow PG Session Protocol to be used. All other non-conformant protocols shall be denied.
OT.FILTERED	Data transferred from RED System to BLACK System shall be in accordance with the filtered parameter ID and its value(s) as specified by the Whitelist.
OT.AUDITING	The TOE must record defined security-relevant events and present it to authorized users. The information recorded for security-relevant events must contain the time and date the event happened to help the authorized user detect attempted security violations or potential misconfiguration of the TOE security features that would leave the IT assets open to compromise.
OT.MANAGE	The TOE must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms and must ensure that only authorized users are able to access such functionality.

Table 14 TOE Security Objectives.

5.2 Operational Environment Security Objectives

This section defines the Security Objectives of the TOE and its environment. The Security Objectives reflect the stated intent to counter all identified threats. They comply with all organizational security policies identified and uphold all assumptions.

Operational Environment Security Objectives	
Objective	**Description**
OE.RED_SYSTEM	The RED System consisting of RED network and its hosts shall be secured according to the value of the RED systems information, such that authenticity of information from the TA.HOST is ensured.
OE.BLACK_SYSTEM	The BLACK System consisting of BLACK network and its hosts shall be secured according to the value of the BLACK systems information.
OE.SECURE_LOCATION	The TOE shall be stored and installed within controlled access facilities.
OE.INSTRUCTED_ADMIN	Trusted users (S.ADMIN, S.CONFIGURATOR and S.AUDITOR) are assigned, instructed and shall act as such to manage and monitor the TOE.
OE.INSTRUCTED_INSTALLER	Trusted users (S.INSTALLER) are assigned, instructed and shall act as such to install the TOE.
OE.SECURE_PLATFORM	TOE is executing on a securely configured BIOS and a security certified Microkernel [5] providing separation of Compartments, Information Flow (including one-way communication between compartments) and Access Control to hardware devices. The configuration of the Microkernel shall be in accordance with the provided guidance for the Microkernel [6] and be in accordance with the defined compartments and information flow as defined in Figure 3. Linux provides supporting device drivers, network stack, reliable time, libraries and, for RED and BLACK OS, a firewall. Server provides trusted Secure Boot. Cryptography and hashing are not in the scope of the TOE. SHA-256 is used and is provided by a library adhering to the FIPS 180-4 standard.

Table 15 Operational Environment Security Objectives.

5.3 Security Objectives Rationale

5.3.1 Security Objective Coverage

This section provides tracings between objectives for the TOE and what threats are being countered by the objective(s) and what OSPs being enforced by the security objectives.

Also the tracing between each security objective for the operational environment and the threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective is shown.

Threats & Assumptions / Objectives	T.EXTERNAL_ATTACK	T.MONITORING_ATTACK	T.INTERNAL_LEAK	T.MISUSE	T.NON_TOE	T.LOCAL_ATTACK	A.RED_SYSTEM	A.BLACK_SYSTEM	A.SECURE_LOCATION	A.SECURE_PLATFORM	P.SEPARATION
OT.ALLOWED_PROTOCOL	X		X								
OT.FILTERED			X	X							X
OT.AUDITING						X					
OT.MANAGE						X					X
OE.RED_SYSTEM			X	X			X				
OE.BLACK_SYSTEM	X							X			
OE.SECURE_LOCATION									X		
OE.INSTRUCTED_INSTALLER									X	X	
OE.INSTRUCTED_ADMIN							X	X	X		
OE.SECURE_PLATFORM	X	X	X		X	X				X	X

Table 16 Security Objective Coverage.

5.4 Security Objectives Sufficiency

5.4.1 Threats

5.4.1.1 T.EXTERNAL_ATTACK

Attacker potential from BLACK network is limited by OE.BLACK_SYSTEM. Direct attack from the BLACK network is prevented by first line of defence by the OE.SECURE_PLATFORM such that attack only has access according to the defined information flow. Second line of defence is OT.ALLOWED_PROTOCOL.

5.4.1.2 T.MONITORING_ATTACK

Direct attack from the MONITORING network is prevented by the one-way communication (OE.SECURE_PLATFORM) with the Remote Audit Compartment, which provides access to the Monitoring Network.

5.4.1.3 T.INTERNAL_LEAK

In general attacks from the internal RED network are prevented by the secure RED Network, OE.RED_SYSTEM. TOE is protecting itself by the first line of defence by the OT.ALLOWED_PROTOCOL and second line of defence by OT.FILTERED, where Whitelist based filtering is performed.

Bypass of TOE is prevented by correct configuration of the OE.SECURE_PLATFORM during Development and Manufacturing life cycle step (see definition in section 2.4.1) such that defined information flow is performed.

5.4.1.4 T.MISUSE

In general attacks from the internal RED network are prevented by the secure RED Network, OE.RED_SYSTEM. RED information could be send and will not be allowed due to the Whitelist based filtering (OT.FILTERED).

5.4.1.5 T.NON_TOE

OE.SECURE_PLATFORM enforces the controlled information flow between Compartments. Furthermore, OE.SECURE_PLATFORM enforces the access control to hardware devices. The definition of system is defined by a Configuration file and used by OE.SECURE_PLATFORM.

5.4.1.6 T.LOCAL_ATTACK

Only authorized users get access to TOE for configuration (OT.MANAGE). All access to TOE is written to the audit event log (OT.AUDITING), such that unauthorized attempts may be investigated and detected.

Installation of TOE uses securely configured BIOS and secure boot (OE.SECURE_PLATFORM), such that authentic TOE is installed.

5.4.2 Assumptions

5.4.2.1 A.RED_SYSTEM

A.RED_SYSTEM is directly covered by OE.RED_SYSTEM, securely managed by OE.INSTRUCTED_ADMIN.

5.4.2.2 A.BLACK_SYSTEM

A.BLACK_SYSTEM is directly covered by OE.BLACK_SYSTEM, securely managed by OE.INSTRUCTED_ADMIN.

5.4.2.3 A.SECURE_LOCATION

A.SECURE_LOCATION is directly covered by OE.SECURE_LOCATION, securely installed by OE.INSTRUCTED_INSTALLER and managed by OE.INSTRUCTED_ADMIN.

5.4.2.4 A.SECURE_PLATFORM

A.SECURE_PLATFORM is directly covered by OE.SECURE_PLATFORM, securely installed by OE.INSTRUCTED_INSTALLER.

5.4.3 Policy

5.4.3.1 P.SEPARATION

Only allowed information flow is enforced by the OT.FILTERED.

Separation policy is supported by Compartments for TOE (OT.MANAGE) and enforced by Filtering (OT.FILTERED) and OE.SECURE_PLATFORM.

6 Extended Components Definition

No additional extended components are needed and therefore none are defined.

7 Security Requirements

To provide an overview of the used Security Functional Policies (SFP), the following descriptions are provided:

- SFP.USER_ADMIN – Policy for handling users and their access to the TOE, such as getting an overview of the users, create users, delete users and modify the settings for a user.
- SFP.SESSION_PROTOCOL – Is an information flow policy where only the session protocol is accepted. It provides a first line of defence, before the actual filtering is performed by SFP.FILER.
- SFP.FILTER – Policy for performing a well-defined filtering based on parameter ID and its value range. Definition of the filtering is according to a Whitelist, which can be defined outside of TOE and imported into TOE according to SFP.IMPORT_WHITELIST.
- SFP.IMPORT_WHITELIST – Policy for importing a Whitelist from the outside into TOE.

7.1 Security Functional Requirements (SFRs)

Conventions used for the SFRs:

- Assignment: Indicated with italicized text;
- Selection: Indicated with underlined text;
- Assignment within a Selection: Indicated with italicized and underlined text;
- Iteration: Indicated by appending the SFR with parentheses that contain a text string that is unique for each iteration.

7.1.1 FAU: Security audit

7.1.1.1 Security audit data generation (FAU_GEN)

Audit events:

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	Start-up and shutdown of the audit functions.	None.
FAU_SAR.1	Reading of information from the audit records.	None.
FAU_STG.1	None.	None.
FAU_STG.2	None.	None.
FAU_STG.5	Actions taken due to the audit data storage failure.	None.
FDP_ACC.1	None.	None.
FDP_ACF.1	All requests to perform an operation on an object covered by the SFP.	None.
FDP_IFC.1 (Session)	None.	None.
FDP_IFC.1 (Filter)	None.	None.
FDP_IFF.1 (Session)	The specific security attributes used in making an information flow enforcement decision.	None.
FDP_IFF.1 (Filter)	The specific security attributes used in making an information flow enforcement decision.	None.
FDP_ITC.1	All attempts to import user data, including any security attributes.	None.
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken and the subsequent, if appropriate, restoration to the normal state.	None.
FIA_ATD.1	None.	None.
FIA_UAU.2	All use of the authentication mechanism.	None.
FIA_UAU.5	The final decision on authentication.	None.
FIA_UAU.6	All re-authentication attempts.	None.
FIA_UAU.7	None.	None.
FIA_UID.2	None.	None.
FMT_MOF.1	All modifications in the behaviour of the functions in the TSF.	None.

Requirement	Auditable Events	Additional Audit Record Contents
FMT_MSA.1	All modifications of the values of security attributes.	None.
FMT_MSA.3	None.	None.
FMT_SMF.1	Use of the management functions.	None.
FMT_SMR.1	Modifications to the group of users that are part of a role.	None.

Table 17 TOE Security Functional Requirements and Auditable Events.

7.1.1.1.1 FAU_GEN.1 Audit data generation

Hierarchical to:

- No other components.

Dependencies:

- FPT_STM.1 Reliable time stamps.

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

a) Start-up and shutdown of the audit functions;
b) All auditable events for the [not specified] level of audit; and
c) [*None*].

Note: The dependency to FPT_STM.1 is resolved by OE.SECURE_PLATFORM.

7.1.1.2 Security audit review (FAU_SAR)

7.1.1.2.1 FAU_SAR.1 Audit review

Hierarchical to:

- No other components.

Dependencies:

- FAU_GEN.1 Audit data generation.

FAU_SAR.1.1 The TSF shall provide [*ADMIN, CONFIGURATOR or AUDITOR*] with the capability to read [*All audit information*] from the audit data.

FAU_SAR.1.2 The TSF shall provide the audit data in a manner suitable for the user to interpret the information.

7.1.1.3 Security audit data storage (FAU_STG)

7.1.1.3.1 FAU_STG.1 Audit data storage location

Hierarchical to:

- No other components.

Dependencies:

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

FAU_STG.1.1 The TSF shall be able to store generated audit data on the [[*Storage attached to TOE, optional Remote Logging on separate physical monitoring network*].]

Note: The dependency to FTP_ITC.1 is resolved by OE.SECURE_PLATFORM. Secure storage is local only, but may be optionally exported towards remote monitoring network.

7.1.1.3.2 FAU_STG.2 Protected audit data storage

Hierarchical to:

- No other components.

Dependencies:

- FAU_GEN.1 Audit data generation.

FAU_STG.2.1 The TSF shall protect the stored audit data in the audit trail from unauthorized deletion.

FAU_STG.2.2 The TSF shall be able to [prevent] unauthorized modifications to the stored audit data in the audit trail.

7.1.1.3.3 FAU_STG.5 Prevention of audit data loss

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.

FAU_STG.5.1 The TSF shall [overwrite the oldest stored audit records] if the audit data storage is full.

7.1.2 FDP: User data protection

7.1.2.1 Access control policy (FDP_ACC)

7.1.2.1.1 FDP_ACC.1 Subset access control

Hierarchical to:

- No other components.

Dependencies:

- FDP_ACF.1 Security attribute-based access control

FDP_ACC.1.1 The TSF shall enforce the [*SFP.USER_ADMIN*] on [
List of subjects: Users
Objects: Usernames, passwords and role assignments
Operation: View, Create, Delete, Modify
].

7.1.2.2 Access control functions (FDP_ACF)

7.1.2.2.1 FDP_ACF.1 Security attribute-based access control

Hierarchical to:
- No other components.

Dependencies:
- FDP_ACC.1 Subset access control
- FMT_MSA.3 Static attribute

FDP_ACF.1.1 The TSF shall enforce the [*SFP.USER_ADMIN*] to objects based on the following:
[*List of subjects: Users*
Objects: Usernames, passwords and role assignments
Attribute: user_role].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*user_role is ADMIN*].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [*None*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*None*].

7.1.2.3 Information flow control policy (FDP_IFC)

7.1.2.3.1 FDP_IFC.1 (Session) Subset information flow control

Hierarchical to:
- No other components.

Dependencies:
- FDP_IFF.1 (Session) Simple security attributes

FDP_IFC.1.1 (Session) The TSF shall enforce the [*SFP.SESSION_PROTOCOL*] on [

Subjects:
- *Hosts connected through RED network interfaces*
- *Hosts connected through BLACK network interfaces*

Information:

- *PG session protocol [3]*

Operations:

- *Send protocol message*]

7.1.2.3.2 FDP_IFC.1 (Filter) Subset information flow control

Hierarchical to:

- No other components.

Dependencies:

- FDP_IFF.1 (Filter) Simple security attributes

FDP_IFC.1.1 (Filter) The TSF shall enforce the [*SFP.FILTER*] on [

Subjects:

- *Hosts connected through RED network interfaces*
- *Hosts connected through BLACK network interfaces*

Information:

- *{Host IDs, parameter IDs} in Whitelist*
- *Acceptable range of values in Whitelist*

Operations:

- *Send host ID, parameter ID and value*]

7.1.2.4 Information flow control functions (FDP_IFF)

7.1.2.4.1 FDP_IFF.1 (Session) Simple security attributes

Hierarchical to:

- No other components.

Dependencies:

- FDP_IFC.1 (Session) Subset information flow control
- FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 (Session) The TSF shall enforce the [*SFP.SESSION_PROTOCOL*] based on the following types of subject and information security attributes: [
Subject:

- *Hosts connected through RED network interfaces and*
- *Hosts connected through BLACK network interfaces*

Information:

- *PG session protocol [3]*

].

FDP_IFF.1.2 (Session) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*None*].

FDP_IFF.1.3 (Session) The TSF shall enforce the [*None*].

FDP_IFF.1.4 (Session) The TSF shall explicitly authorise an information flow based on the following rules: [*Transmission in accordance with Session Protocol*].

FDP_IFF.1.5 (Session) The TSF shall explicitly deny an information flow based on the following rules: [*All other transmission than accepted by FDP_IFF.1.4 (Session)*].

7.1.2.4.2 FDP_IFF.1 (Filter) Simple security attributes

Hierarchical to:

- No other components.

Dependencies:

- FDP_IFC.1 (Filter) Subset information flow control.
- FMT_MSA.3 Static attribute initialization.

FDP_IFF.1.1 (Filter) The TSF shall enforce the [*SFP.FILTER*] based on the following types of subject and information security attributes: [
Subject:

- *Hosts connected through RED network interfaces and*
- *Hosts connected through BLACK network interfaces*

Information:

- *{Host IDs, parameter IDs} in Whitelist*
- *Acceptable range of values in Whitelist*

].

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

FDP_IFF.1.3 (Filter) The TSF shall enforce the [*None*].

FDP_IFF.1.4 (Filter) The TSF shall explicitly authorise an information flow based on the following rules: [*host ID and parameter ID is in Whitelist and the value is within allowed range for sending information from RED System to BLACK System*].

FDP_IFF.1.5 (Filter) The TSF shall explicitly deny an information flow based on the following rules: [*host ID or parameter ID not in Whitelist or value(s) outside allowed range*].

7.1.2.5 Import from outside of the TOE (FDP_ITC)

7.1.2.5.1 FDP_ITC.1 Import of user data without security attributes

Hierarchical to:

- No other components.

Dependencies:

- [FDP_ACC.1 Subset access control, ~~or FDP_IFC.1 Subset information flow control~~]
- FMT_MSA.3 Static attribute initialization

FDP_ITC.1.1 The TSF shall enforce the [*SFP.IMPORT_WHITELIST*] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [*Imported whitelist must be accepted by user_role ADMIN or CONFIGURATOR*].

Note: ADMIN or CONFIGURATOR shall be instructed to perform a review before the accept is made.

7.1.3 FIA: Identification and authentication

7.1.3.1 Authentication failures (FIA_AFL)

7.1.3.1.1 FIA_AFL.1 Authentication failure handling

Hierarchical to:

- No other components.

Dependencies:

- FIA_UAU.1 Timing of authentication.

FIA_AFL.1.1 The TSF shall detect when [3] unsuccessful authentication attempts occur related to [*login*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [surpassed], the TSF shall [*deny a new login attempt for additional 1 minute*].

7.1.3.2 User attribute definition (FIA_ATD)

7.1.3.2.1 FIA_ATD.1 User attribute definition

Hierarchical to:
- No other components.

Dependencies:
- No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [*usernames, passwords and role assignments*].

7.1.3.3 User authentication (FIA_UAU)

7.1.3.3.1 FIA_UAU.2 User authentication before any action

Hierarchical to:
- FIA_UAU.1 Timing of authentication.

Dependencies:
- FIA_UID.1 Timing of identification.

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

7.1.3.3.2 FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to:
- No other components.

Dependencies:
- No dependencies.

FIA_UAU.5.1 The TSF shall provide [*authentication based on user name and password*] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [*the TOE locally verifies the password hash matches the stored password hash associated with the provided username*].

Note: Hash function covered by OE.SECURE_PLATFORM, where user name is used as salt.

7.1.3.3.3 FIA_UAU.6 Re-authenticating

Hierarchical to:
- No other components.

Dependencies:

- No dependencies.

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions [*Logout by user, Time-out*].

7.1.3.3.4 FIA_UAU.7 Protected authentication feedback

Hierarchical to:

- No other components.

Dependencies:

- FIA_UAU.1 Timing of authentication.

FIA_UAU.7.1 The TSF shall provide only [*the authentication mechanism that failed the authentication*] to the user while the authentication is in progress.

7.1.3.4 User identification (FIA_UID)

7.1.3.4.1 FIA_UID.2 User identification before any action

Hierarchical to:

- FIA_UID.1 Timing of identification.

Dependencies:

- No dependencies.

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

7.1.4 FMT: Security management

7.1.4.1 Management of functions in TSF (FMT_MOF)

7.1.4.1.1 FMT_MOF.1 Management of security functions behavior

Hierarchical to:

- No other components.

Dependencies:

- FMT_SMR.1 Security roles
- FMT_SMF.1 Specification of Management Functions Component relationships

FMT_MOF.1.1 The TSF shall restrict the ability to [enable] the functions [*imported Whitelist configuration of the TOE*] to [*ADMIN or CONFIGURATOR*].

7.1.4.2 Management of security attributes (FMT_MSA)

7.1.4.2.1 FMT_MSA.1 Management of security attributes

Hierarchical to:
- No other components.

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

FMT_MSA.1.1 The TSF shall enforce the [*SFP.USER_ADMIN*] to restrict the ability to [query, modify, delete, create] the security attributes [*usernames, passwords and role assignments*] to [*ADMIN*].

7.1.4.2.2 FMT_MSA.3 Static attribute initialization

Hierarchical to:
- No other components.

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

FMT_MSA.3.1 The TSF shall enforce the [*SFP.USER_ADMIN, SFP.IMPORT_WHITELIST, SFP.FILTER*] 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.

7.1.4.3 Specification of Management Functions (FMT_SMF)

7.1.4.3.1 FMT_SMF.1 Specification of Management Functions

Hierarchical to:
- No other components.

Dependencies:
- No dependencies.

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

User management:
- *Create user and assign role and password*

- *Change password*
- *Change role assignment*
- *Delete user*

Whitelist import:

- *Import whitelist from USB memory device*
- *Review imported whitelist*
- *Accept and store whitelist for use by SFP.FILTER*

].

7.1.4.4 Security management roles (FMT_SMR)

7.1.4.4.1 FMT_SMR.1 Security roles

Hierarchical to:

- No other components.

Dependencies:

- FIA_UID.1 Timing of identification.

FMT_SMR.1.1 The TSF shall maintain the roles [*ADMIN, CONFIGURATOR and AUDITOR*].

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

7.2 Security Assurance Requirements (SARs)

The certification assurance level claimed for the TOE is EAL4 and augmented with ALC_FLR.3. See note in section 3.3.

7.3 Security Requirements Rationale

Security Objective / **Security Functional Requirement (SFR)**	OT.ALLOWED_PROTOCOL	OT.FILTERED	OT. AUDITING	OT.MANAGE
FAU_GEN.1			**X**	
FAU_SAR.1			**X**	

Security Objective / **Security Functional Requirement (SFR)**	OT.ALLOWED_PROTOCOL	OT.FILTERED	OT. AUDITING	OT.MANAGE
FAU_STG.1			**X**	
FAU_STG.2			**X**	
FAU_STG.5			**X**	
FDP_ACC.1				**X**
FDP_ACF.1				**X**
FDP_IFC.1 (Session)	**X**			
FDP_IFC.1 (Filter)		**X**		
FDP_IFF.1 (Session)	**X**			
FDP_IFF.1 (Filter)		**X**		
FDP_ITC.1				**X**
FIA_AFL.1				**X**
FIA_ATD.1				**X**
FIA_UAU.2				**X**
FIA_UAU.5				**X**
FIA_UAU.6				**X**
FIA_UAU.7				**X**
FIA_UID.2				**X**
FMT_MOF.1	**X**	**X**		**X**
FMT_MSA.1				**X**
FMT_MSA.3	**X**	**X**		**X**

Security Objective / Security Functional Requirement (SFR)	OT.ALLOWED_PROTOCOL	OT.FILTERED	OT. AUDITING	OT.MANAGE
FMT_SMF.1	**X**	**X**		**X**
FMT_SMR.1				**X**

Table 18 Security Requirements Rationale.

7.3.1 OT.ALLOWED_PROTOCOL

The allowed session protocol is enforced by FDP_IFC.1 (Session) and FDP_IFF.1 (Session). Default values are restrictive (FMT_MSA.3) and can be changed by updating the Whitelist configuration (FMT_MOF.1) by the defined Management Function (FMT_SMF.1).

7.3.2 OT.FILTERED

The objective OT.FILTERED is defined by the information flow policy FDP_IFC.1 (Filter) and implemented by the rules defined by FDP_IFF.1 (Filter). Whitelist of acceptable send has a restrictive initial value (FMT_MSA.3), e.g. an empty Whitelist. The Whitelist configuration can be changed according to FMT_MOF.1 with the defined Management Function (FMT_SMF.1).

7.3.3 OT.AUDITING

All auditable events are stored locally (FAU_STG.1, FAU_STG.2 and FAU_STG.5) for each send operation and defined by FAU_GEN.1 with a reliable time stamp (OE.SECURE_PLATFORM). They can be viewed (FAU_SAR.1) by an authorized user.

7.3.4 OT.MANAGE

Before a user can manage or view the audit events, he/she needs to be authenticated (FIA_AFL.1, FIA_ATD.1, FIA_UAU.2, FIA_UAU.5, FIA_UAU.6, FIA_UAU.7 and FIA_UID.2).

The authentication is based on username and password validation against stored credentials (OE.SECURE_PLATFORM).

Management is performed for users (FDP_ACC.1 and FDP_ACF.1) and the Whitelist configuration is performed by importing the Whitelist (FDP_ITC.1) of the Filter Function (FMT_SMF.1). Restrictive security attributes are defined (FMT_MSA.3) such that user role ADMIN can perform Management

functions (FMT_MSA.1, FMT_MOF.1, FMT_SMF.1 and FMT_SMR.1) and CONFIGURATOR can import, review and activate Whitelist (FMT_MOF.1 and FMT_SMF.1).

8 TOE Summary Specification

The TOE Summary specification defines the instantiation of the security requirements for the TOE.

The following subsection describes the TOE Security Functions (TSF) and their correspondence to the stated security requirements.

8.1 TOE Security Functions

An overview of all TOE Security Functions and which Security Requirements they fulfill is given in the following table. Further descriptions of TSFs are given in subsections below.

TOE Security Function (TSF) / **Security Functional Requirement (SFR)**	SF-1 Filtering	SF-2 Management	SF-3 Auditing
FAU_GEN.1			**X**
FAU_SAR.1			**X**
FAU_STG.1			**X**
FAU_STG.2			**X**
FDP_ACC.1		**X**	
FDP_ACF.1		**X**	
FDP_IFC.1 (Session)	**X**		
FDP_IFC.1 (Filter)	**X**		
FDP_IFF.1 (Session)	**X**		
FDP_IFF.1 (Filter)	**X**		

TOE Security Function (TSF) / Security Functional Requirement (SFR)	SF-1 Filtering	SF-2 Management	SF-3 Auditing
FDP_ITC.1	**X**	**X**	
FIA_AFL.1		**X**	
FIA_ATD.1		**X**	
FIA_UAU.2		**X**	
FIA_UAU.5		**X**	
FIA_UAU.6		**X**	
FIA_UAU.7		**X**	
FIA_UID.2		**X**	
FMT_MOF.1		**X**	
FMT_MSA.1		**X**	
FMT_MSA.3		**X**	
FMT_SMF.1		**X**	
FMT_SMR.1		**X**	

Table 19 TOE Security Functions

8.1.1 SF-1 Filtering

Filtering is performed by the following information flow control of TOE:

- Only the allowed Session Protocol communication to/from TOE.
- Resource address and parameter is in Whitelist and the value is within allowed range for sending information from RED System to BLACK System. All information can be send from BLACK System to RED System without restriction.

The Whitelist starts with restrictive values, which is not allowing any communication by an empty Whitelist.

8.1.2 SF-2 Management

Access control of users and management of users and passwords. The Whitelist defining the filtering (SF-1) is managed.

8.1.3 SF-3 Auditing

TOE is generating security events for later investigation and stored locally.