SDoT Security Gateway - SDoT Filter SW
Security Target - Lite

Document name:	ST_SDoTSGW6.2a_SecurityTarget.docx
Version number:	V 1.11
Version date:	25.09.2023
Author:	INFODAS GmbH
Number of pages:	103

Issued by: INFODAS GmbH
Rhonestraße 2
50765 Cologne, Germany

Table of Contents

List of Figures

List of Tables

Abbreviations

ADatP-3	Allied Data Publication–3
ADEXP	ATS Data Exchange Presentation
ASCII	American Standard Code for Information Interchange
ASE	**A**ssurance Class in the CC Standard referring to the **S**ecurity Target **E**valuation
ASTERIX	All Purpose Structured EUROCONTROL Surveillance Information Exchange
CA	Certification Authority
CC	Common Criteria for Information Technology Security Evaluation
CCL	Refers to the assurance family "**C**onformance **cl**aims" in the assurance class ASE
CD	Compact Disc
CEM	Common Criteria for Information Technology Security Evaluation, Evaluation methodology
CPU	Central Processing Unit
DVD	Digital Versatile Disc
EAL	Evaluation Assurance Level
FAU	SFRs belonging to the **f**unctional class "Security **Au**dit"
FCO	SFRs belonging to the **f**unctional class "**Co**mmunication"
FDP	SFRs belonging to the **f**unctional class "User **D**ata **P**rotection"
FIA	SFRs belonging to the **f**unctional class "**I**dentification and **a**uthentication"
FMT	SFRs belonging to the **f**unctional class "Security **m**anagemen**t**"
FPT	SFRs belonging to the **f**unctional class "**P**rotection of the **T**SF"
FSD	Field Structured Data
FW	Firmware
GUI	Graphical User Interface

H2L	High-to-Low
HDD	Hard Disk Drive
HMAC	Hash Message Authentication Code
HSM	Hardware Security Module
HTTP / S	Hypertext Transfer Protocol / Secure
HW	Hardware
ICAP	Internet Content Adaptation Protocol
INT	Refers to the assurance family "ST introduction" of the assurance class ASE
IO	Input-Output
IP	Internet Protocol
JSON	Java Script Object Notification
L2H	Low-to-high
L4	Implementation of microkernel L4
L4Linux	Modified kernel of Linux running on top of L4
L4Re	L4 Runtime environment
LCD	Liquified Crystal Display
Net SPIF	Network Security Policy Information File
NTP	Network Time Protocol
OBJ	Refers to the assurance family "Security objectives" of the assurance class ASE
OSP	Organisational Security Policy
RAM	Random Access Memory
REQ	Refers to the assurance family "Security requirements" of the assurance class ASE
RNG	Random Number Generator
RTF	Rich Text Format

SAR	Security Assurance Requirement
SDoT	Security Inter-Domain Transition
SFP	Security Function Policy
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SMTP MTA	SMTP Message/Mail Transfer Agent
SPD	Refers to the assurance family "**S**ecurity **p**roblem **d**efinition" of the assurance class ASE
SPIF	Security Policy Information File
SSD	Solid State Drive
ST	Security Target
SW	Software
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
TSS	Refers to the assurance family "**T**OE **s**ummary **s**pecification" of the assurance class ASE
UDP	User Datagram Protocol
UEFI	Unified Extensible Firmware Interface
XML	Extensible Markup Language
XSD	XML Schema Definition

General

Distribution List:

Recipient	Number of copies
atsec	1
CSA	1

Revision History:

Version	Date	Application Note	Author
V 0.1	03.11.2022	First draft generated from Security Target of SGW 6.2a of the NITES certification	INFODAS GmbH
V 0.9	04.11.2022	First draft after internal QA for submission with SCCS application form	INFODAS GmbH
V 1.0	07.03.2023	First final Version - Cert ID added - Minor corrections due to lab feedback in chapter 7.3	INFODAS GmbH
V 1.1	21.08.2023	Revised title, page header and TOE name long due to the request for change by CSA.	INFODAS GmbH
V 1.11	25.08.2023	Lite Version of the ST	INFODAS GmbH

1 ST Introduction (ASE_INT.1)

This chapter provides an unambiguous identification of the main characteristics of this Security Target and the TOE in scope of the security certification process. Some information in TOE overview and in TOE description contain confidential information which are sanitised in the public version of this security target (ST Lite). This security target was created considering [AIS_41] of BSI.

1.1 ST Reference

Title: SDoT Security Gateway - SDoT Filter SW Security Target

Version: V 1.11

Date: 25.09.2023

Author: INFODAS GmbH

1.2 TOE reference

Product name: SDoT Security Gateway

TOE name (long): SDoT Security Gateway - SDoT Filter SW

TOE name (short): SDoT Filter SW

TOE version: 6.2a

Developer name: INFODAS GmbH

Certification ID: CSA_CC_22008

1.3 TOE overview

The TOE version 6.2a refers to the use case for the deployment to the Singapore market. Hereby, 6.2a describes a mnemonic convention which exact configuration is identified as the following revision: 6.2.15566.31149. This Security Target defines the security objectives for, and security requirements of the SDoT Filter SW (TOE), which is a component of the product SDoT Security Gateway of INFODAS GmbH. Further, this security target defines the security objectives of the operational environment for the TOE. The following subsections give an overview of the TOE, its usage and major security features, the TOE type, and lists all required non-TOE Hardware, non-TOE Software/Firmware.

1.3.1 TOE definition and operational usage

The product SDoT Security Gateway provides a secure interconnection between two IP networks which could have different types of security classifications. For a secure exchange of data between these networks the SDoT Security Gateway serves as protection to not let confidential data, within a potentially higher classified network (HIGH), unintentionally flow to a lower classified network (LOW) which is not authorised to get hold of confidential information from the higher classified network.

SDoT Security Gateway includes the TOE which provides the filtering functionalities to check security labels for the transmission of data between the two differently classified networks and provides mechanisms to validate structured data objects against a pre-defined rule set. The SDoT

Security Gateway comprises the SDoT Filter Platform (HW with HSM, FW, OS) and the SDoT Filter SW which is the TOE. The SDoT Security Gateway includes an SDoT Adminstation for Administration of the SDoT Filter. More information about the non-TOE parts of SDoT Security Gateway will be given in 1.3.4. Therefore, the TOE is an application delivered together with a set of software and hardware components to the customer. The underlying micro kernel operating system with its separation mechanism is part of the TOE environment. All hardware and software which are needed to securely operate the TOE in accordance to the TOE assumptions, and in accordance to the assumptions of the TOE operational environment, are in scope of delivery, see Table 3. The hardware parts and software parts besides the TOE are partially customized for SDoT Security Gateway to make sure that the TOE operates properly as intended with the dedicated delivery parts only.

1.3.2 Major Security Features of the TOE

The TOE implements the functions of the SDoT Security Gateway which are responsible to filter incoming data. Depending on the network classification of the destinated network the TOE either uses labels which are cryptographically signed, or the incoming data objects are structured data containing classified information and are then validated against a corresponding and pre-defined rule set. Cryptographic support for labelling and random numbers is securely provided by the dedicated HSM within the physical environment of the TOE.

The TOE is running on a L4Re operating system which provides the capability to run independent systems in isolated parts, called compartments. Splitting the system into compartments makes it possible to implement logically separated subsystems of the TOE. The system hosting the TOE uses an UEFI-based secure boot mechanism to ensure that only authentic software is running on the system. Therefore, the TOE runs on a platform system which provides strong separation, and isolation mechanisms for each compartment. Further, the platform provides an instrument for restricting the communication between each compartment by means of controlling and monitoring capabilities.

The TOE includes seven compartments for different purposes. These are

- FI_GUI,
- FI_HGH,
- FI_CFG,
- FI_H2L,
- FI_L2H,
- FI_LOW, and
- FI_ADT.

The security mechanisms of the TOE are implemented on the compartments FI_GUI, FI_CFG, FI_H2L, and FI_ADT. The TOE enforces the information flow policy which ensures that only data with either a correct label, or structured data with classified information which must be checked against a corresponding and pre-defined rule set, can then be forwarded to the lower classified network (LOW). The TOE collects and checks audit data to identify any occurring policy violation. The TOE performs management functions on configuration data in FI_CFG. Identification and authentication of administrators and auditor of the TOE is provided by the FI_GUI which communicates via TLS connection to the SDoT Adminstation.

The compartment FI_H2L is responsible for the main filtering functionality of the TOE. The only possibility to send data from the higher classified network (HIGH) to the lower classified network (LOW) is through the compartment FI_H2L. The FI_H2L communicates with the compartments FI_HGH and FI_LOW through the L4Re OS. Hence, FI_H2L does neither have a direct connection to the higher classified network (HIGH) nor to the lower classified network, but instead, FI_H2L communicates with FI_HGH for connection to network HIGH. For the same reason, FI_H2L communicates with FI_LOW for connection to network LOW. The following figure depicts the TOE with its IT environment which build together the SDoT Security Gateway.

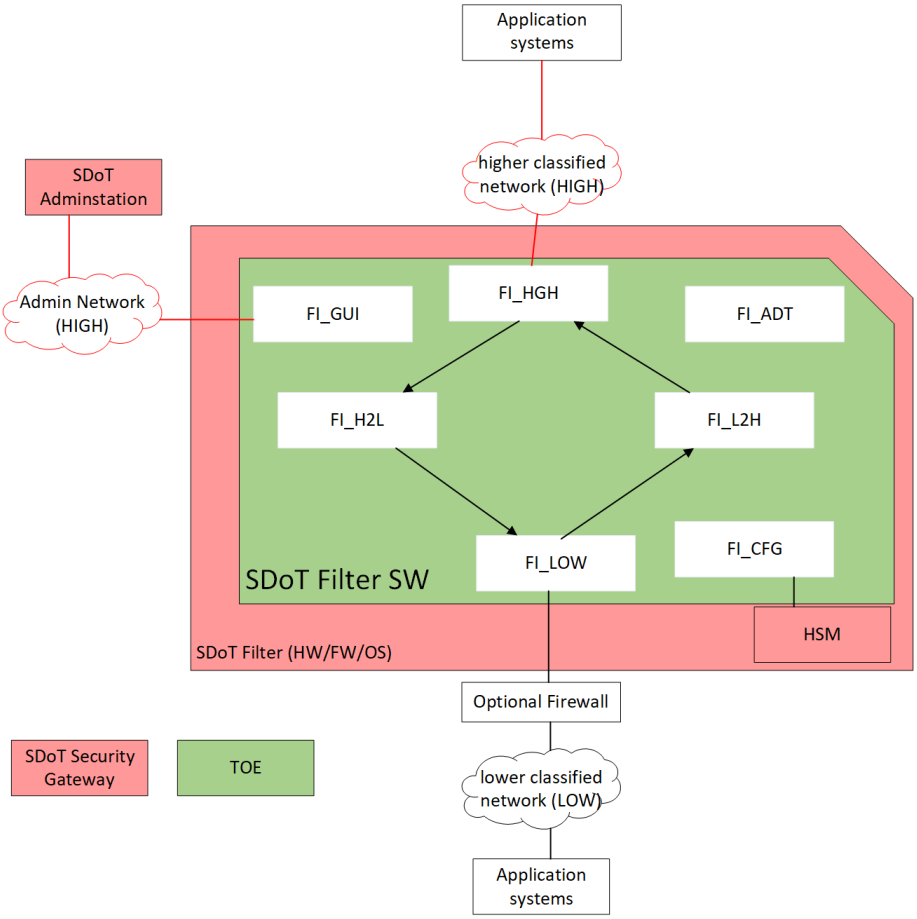

Figure 1: SDoT Security Gateway

The information flow from the network LOW to the network HIGH is under control of the compartment FI_L2H which has no direct link to the network HIGH and LOW. For the communication to network LOW the compartment FI_L2H uses FI_LOW and similarly, the FI_HGH is used for communication to the network HIGH. All protocol data which is sent from the network LOW to the network HIGH is filtered by the compartment FI_L2H.

Outside of the TOE the SDoT Security Gateway provides security mechanisms which include the SDoT Adminstation and a dedicated HSM. These parts outside of the TOE are the operational environment of the TOE. Further, it is recommended that the operator of the TOE considers to use a firewall which is located between the SDoT Security Gateway and the lower classified network LOW.

90 The SDoT Adminstation allows the administrator, policy-admin or the auditor to fulfil their
91 responsibility and role as such. The SDoT Adminstation is connected to the TOE via the compartment
92 FI_GUI through a dedicated higher classified administration network in the HIGH domain.

93 The following table outlines the main functionalities of each compartment:

Compartment	Description
FI_GUI	• Provides the GUIs for administrating and auditing purposes of the TOE. • Establishes the administrative TLS connection to the SDoT Adminstation.
FI_HGH	• Includes proxies for SMTP, HTTP, UDP and TCP for communication with the TOE environment within the network HIGH.
FI_CFG	• Responsible for the communication with the HSM for cryptographic purposes. • Provides functionalities for the administration of the TOE.
FI_H2L	• This compartment is responsible for pre-filtering all incoming data from the network HIGH. • It automatically validates the data against the pre-defined rule set. • Attaches the security label which is cryptographically generated by the HSM or writes relevant information into a header of the used data transfer protocol ICAP after successful validation. Remark: If the security label which contains a classification of the information within the transmitted data object is not needed in the LOW network, then the computationally intensive generation of a security label is not necessarily needed. In this case, the SDoT Filter can be configured such that the internally determined classification information is stored into the ICAP header for performance reasons, i.e. a security label is not generated. • Filters the data in accordance with its classification written in the label or on the ICAP header.
FI_L2H	For forwarding data from network LOW to network HIGH the TOE can be configured with three different options within this compartment. **Description of first option:** • Pre-filtering of incoming data from network LOW, • Automatic validation of data against a pre-defined policy,

	• Attaches a security label or writes relevant information into a header of the used data transfer protocol ICAP after successful validation, • Filters the data in accordance with its classification written in the label or on the ICAP header. **Description of second option:** • Security labels are generated based on the security level of network LOW **Description of third option:** • Data messages are directly forwarded to network HIGH
FI_LOW	• Includes proxies for SMTP, HTTP, UDP and TCP for communication with the TOE environment within the network LOW.
FI_ADT	• Includes mechanisms for logging security relevant events.

Table 1 Main functionalities of each compartment

94 **The major security features of the TOE are summarised as follows:**

95 • The TOE validates security labels attached to data and forwards the data after
96 successful validation from the network HIGH to the network LOW or denies the data to
97 be forwarded in case the label is not correct.

98 • The TOE validates structured data against configured rule sets.

99 • The TOE only accepts connections on configured ports. For each port, only correct
100 communication according to the configured protocol is accepted by the TOE.

101 • The TOE provides strong binding between data and the corresponding security labels
102 with digital signatures. The digital signatures are provided by the HSM which does not
103 belong to the TOE

104 • The TOE re-builds (sanitisation) and converts (canonicalization) forwarded security
105 labels

106 • The TOE provides secure auditing mechanisms of logs and secure administration
107 capabilities.

108 • The TOE provides mechanisms for authentication.

1.3.3 TOE Type

109 The TOE is a software security filter, which is part of a security gateway (hardware and software) of
110 INFODAS GmbH.

1.3.4 Required non-TOE Hardware (HW)/Software (SW)/Firmware (FW)

111 Besides the required HSM the product SDoT Security Gateway comprises several hardware
112 components running a dedicated L4Re operating system. Besides the TOE the SDoT Security
113 Gateway consists of the following parts:

114 • Underlying platform (hardware and operating system) of the TOE

115 • HSM for cryptographic support in terms of labelling mechanisms, random numbers
116 and secure storage

117 • SDoT Adminstation including hardware and software parts

118 • Smartcard Reader for authentication purposes at the SDoT Adminstation

119 • Smartcards for cryptographic support and authentication

120 Besides the hardware and operating systems, there are several software components which belong
121 to the TOE environment (cf. Figure 1 and Figure 2). The following table provides an overview of all
122 required non-TOE hardware and non-TOE software components which are needed to securely
123 operate the TOE. In addition, all components required by SDoT Security Gateway for its secure use
124 are listed below.

Required non-TOE HW/SW/FW components of SDoT Security Gateway	
Underlying Platform of the TOE:	
Hardware	Hardware of server appliance in a 1U, 19" rackmount with HSM, CPU, RAM, HDDs, LC display, and physical interfaces.
Firmware/OS	Installed on the server appliance: UEFI Boot loader, HSM FW, L4Re microkernel OS, L4/Linux, BusyBox
SDoT Adminstation	Machine (laptop computer) of the renowned manufacturer GETAC with CentOS.
Installation CD/DVD	Software of SDoT Filter and SDoT Adminstation
Smartcard Reader	Smartcard Reader of renowned manufacturer Reiner SCT of type CyberJack Secoder or CyberJack RFID
Smartcards	Smartcard with certificate for initialisation purposes and empty user smartcards which must be initialised for authentication purposes.

Table 2 Required non-TOE HW/SW/FW components of SDoT Security Gateway

1.4 TOE description

125 The following table shows the delivery parts of the SDoT Security Gateway where the TOE belongs
126 to. Following to that, the subsections provide a description of the physical and logical boundaries of
127 the TOE.

Name	Description	Medium
HW, FW, OS, HSM of SDoT Security Gateway	Comprises all Hardware and FW/OS Parts on which the TOE is running	Hardware with installed HSM and FW/OS of SDoT Security Gateway
SDoT Adminstation	Laptop Computer for remote administration of the SDoT Filter	Hardware with installed FW/OS for administration purposes
TOE Installation ISO	Software for installation of the TOE on the SDoT Security Gateway	DVD
SDoT Adminstation ISO	Software for installation of the SDoT Adminstation SW	DVD
Guidance Documentation	Manual for SDoT Filter, V1.3 Manual for Adminstation, V1.5 Product Information – Requirements for Secure Operation, V1.3	All guidance documents are provided digitally via encrypted email attachment in Portable Document Format or via the infodas download portal.
Smartcards	Provides key material for first initialisation and further Smartcards for authentication purposes on the SDoT Stations	Smartcard

Table 3 SDoT Security Gateway scope of delivery

1.4.1 TOE Description – Physical Scope

128 The TOE is a software component of the SDoT Security Gateway. Therefore, there are no physical
129 parts of the SDoT Security Gateway in scope of the TOE. The reader may refer to Table 3 above for
130 information about the physical parts of the SDoT Security Gateway.

1.4.2 TOE Description – Logical Scope

131 Figure 1 shows an overview of the separated compartments which are part of the TOE. The following
132 Figure 2 shows the logical scope of the TOE within the compartments and gives an overview of non-
133 TOE components of the product:

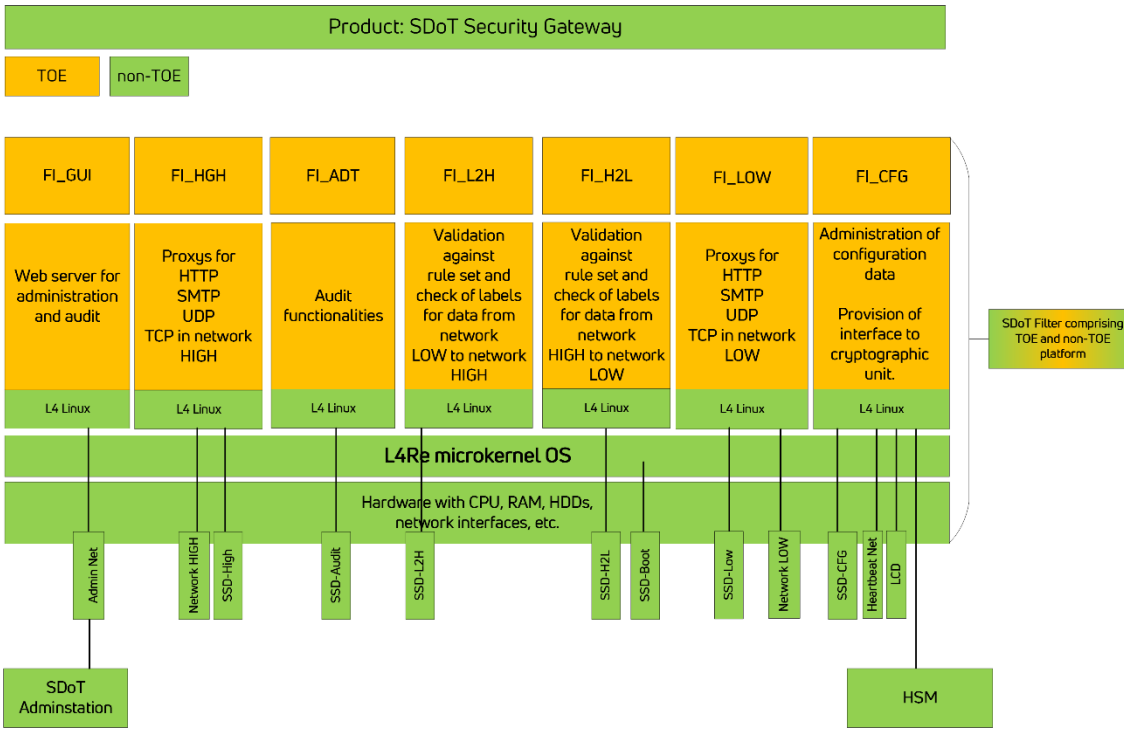

Figure 2: Logical scope of the TOE

As shown in Figure 2 the system platform required by the TOE provides multiple environments for the implementation of compartments with strong separation mechanisms. Each compartment represents an isolated security domain with its own underlying L4Linux. The microkernel architecture provides control mechanisms to restrict the communication between the compartments.

For a better overview of the SDoT Security Gateway a short description of all components is given in the following.

SDoT Adminstation (non-TOE):

The SDoT Adminstationis is based on a CentOS architecture. The functionalities for local administration and local auditing of the SDoT Adminstations are provided by a GUI through a common browser. Configuration parameters and audit data are managed within the administration GUI, and respectively by the audit GUI of the SDoT Adminstation.

The cryptographic support is provided by a smartcard called "data smartcard" which is inserted into the integrated reader of the corresponding SDoT Adminstation. A further smartcard called "user smartcard" is used with a dedicated smartcard reader and is included in the scope of delivery.

The SDoT Adminstation is connected to the TOE via a dedicated administration network in the HIGH domain and can only be used by administrators, policy-admins and auditors. The policy-admin can attach labels and sign rule sets. The digital signature is generated in the smartcard of the policy-admin. The rule set must then be configured by two different admins via the Administration GUI for dual control.

SDoT Filter SW (TOE)

In the following, the compartments which build the TOE are outlined:

156 **COMPARTMENT FI_GUI**

157 The web-based Administration GUI and Audit GUI are displayed by a common web browser installed
158 on the SDoT Adminstation (non-TOE). With Administration GUI and Audit GUI the configuration data
159 and audit data of the TOE can be managed. Further, the FI_GUI establishes the TLS connection for
160 administrative purposes with the SDoT Adminstation.

161 **COMPARTMENT FI_CFG**

162 This is where the main configuration is managed, and monitoring tasks are performed. This is the
163 only compartment with a connection to the HSM which provides hardware support for some
164 cryptographic mechanisms used by the TOE. The administration agent is called by the web server
165 of FI_GUI after a TLS connection was initiated from the SDoT Adminstation.

166 The TOE supports a functionality called HA-variant (High Availability variant) of the SDoT Security
167 Gateway. Here, a cluster of redundantly designed SDoT Filters (nodes) are operated, whereby each
168 of these nodes fully implements the TOE. The node that currently accepts and processes the
169 incoming data in operational mode is called the master node. The other nodes are called slave nodes.

170 From an operational point of view, high availability is an important aspect for uninterruptible
171 operation, but it is not providing any security function.

172 Heartbeat communication is completely decoupled from the data flow between the HIGH and LOW
173 networks, since this communication only takes place between the administration agents in the resp.
174 FI_CFG of the two nodes (point-to-point connection), there are no network coupling elements in
175 between, and no other network interface is connected in the FI_CFG.

176 If the master node fails or if the connectivity of the master node with IT systems of the HIGH network
177 is lost, the system automatically switches to a functioning slave node. For this purpose, the
178 administration agents (in FI_CFG) of the nodes monitor each other by cyclically requesting status
179 information of the other agents via the heartbeat connection. If the master node fails or is no longer
180 accessible, one of the slave nodes becomes the master node.

181 **COMPARTMENT FI_ADT**

182 This compartment provides functions for logging security relevant events. Only the audit agent
183 within FI_ADT has access to logged audit data in the audit storage. Further, the audit agent monitors
184 the audit storage capacity to avoid any potential overflow of the audit storage. The FI_ADT
185 communicated with the FI_GUI which establishes the TLS connection for displaying the relevant
186 information on the SDoT Adminstation.

187 The audit agent is responsible to record security relevant events on the TOE, related to writing
188 entries into the audit trail. The audit agent in FI_ADT is responsible to generate alarms, i.e. e-mails.
189 The SMTP-MTA of the TOE sends then the e-mails to a list of receivers. The list is configurable and
190 stored in the FI_CFG which protects the integrity with checksums stored in the HSM.

191 Further, the audit agent covers the following tasks:

192 • Generate new audit trails if the current audit trail exceeds a pre-defined size,

193 • Generate new audit trails daily,

194 • Monitor the storage capacity of the storage device to prevent an audit trail overflow.

195 **COMPARTMENT FI_H2L**

All data which are sent from the higher classified network HIGH to the lower classified network LOW are processed by the so called "H2L SchemaValidator" which is a process within the compartment FI_H2L.

COMPARTMENT FI_L2H

In general, forwarding data from LOW to HIGH is not a security critical functionality since the main objective of the TOE is to prevent unwanted data flow in the opposite direction, from HIGH to LOW. Only the direction from HIGH to LOW is security relevant and addressed as SFR in section 7. The main asset are data within the higher classified network HIGH which have to be protected.

COMPARTMENT FI_HGH

The FI_HGH provides proxy support for the following types of protocols:

- SMTP
- HTTP
- UDP
- TCP

The proxies perform the following tasks which controls all data flow in the higher classified network HIGH.

- Accept data from higher classified network HIGH and forwarding the data to FI_H2L.
- Forwarding data to the higher classified network HIGH which comes from FI_L2H.

Also, the above-mentioned proxies support the non-TOE functionality for mutually authenticated TLS connection with IT systems of the operational environment of the TOE within the network HIGH.

COMPARTMENT FI_LOW

The FI_LOW includes provides proxy support for the following types of protocols:

- SMTP
- HTTP
- UDP
- TCP

The proxies perform the following tasks which controls all data flow in the lower classified network HIGH.

- Accept data from lower classified network LOW and forwarding the data to FI_L2H.
- Forwarding data to the lower classified network LOW which comes from FI_H2L.

Also, the above-mentioned proxies support the non-TOE functionality for mutually authenticated TLS connection with IT systems of the operational environment of the TOE within the network LOW.

2 Conformance claims (ASE_CCL.1)

2.1 CC conformance claim

228 This Security Target claims conformance to

229 • Common Criteria for Information Technology Security Evaluation, Part 1: Intro-duction
230 and general model, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002 (cf.
231 [CC_Part1])

232 • Common Criteria for Information Technology Security Evaluation, Part 2: Security
233 functional components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002 (cf.
234 [CC_Part2])

235 • Common Criteria for Information Technology Security Evaluation, Part 3: Security
236 assurance components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003 (cf.
237 [CC_Part3])

238 in the following way

239 • Part 2 extendet

240 • Part 3 conformant

241 The Common Criteria for Information Technology Security Evaluation, Evaluation methodology,
242 Version 3.1, Revision 5, April 2017, CCMB-2017-04-004 (cf. [CEM]) must be considered.

2.2 PP Claim

243 This Security Target does not claim conformance to any existing Protection Profile nor to any
244 existing security functional requirement package.

2.3 Package Claim

245 The assurance packages claimed by the TOE is EAL4 augmented by ALC_FLR.2 which adds flaw
246 reporting procedures, and AVA_VAN.5 which adds advanced methodical vulnerability analysis to
247 the Evaluation Assurance Level EAL4.

2.4 Conformance Rationale

248 Since the current Security Target does not claim conformance to any existing Protection Profile, a
249 Conformance Rationale is not necessary.

3 Security Problem Definition (ASE_SPD.1)

3.1 Introduction

250 This chapter introduces the relevant assets which are protected by the TOE and/or its operational
251 environment. Following to that, the subjects and external entities interacting with the TOE are
252 described. Table 8 outlines the assumptions which describe the security attributes of the TOE
253 operational environment to achieve the intended level of security. Possible threats which have to be
254 effectively averted by the TOE, its operational environment or a combination of both are listed in
255 Table 7. The relevant organisational security policies (OSPs) are described in Table 9.

3.2 Assets

256 In this section the primary assets and secondary assets of the TOE are introduced and categorised
257 into its protective objectives; integrity (I), authenticity (A), and confidentiality (C).

3.2.1 Primary Assets

258 The following primary assets are protected by the TOE and/or its operational environment:

#	Assets	Description	Protective Objective
1.	DATA_IN_HIGH	All confidential data within the higher classified network (HIGH) shall be protected against unauthorised transmission.	C, I, A

Table 4 Primary assets

3.2.2 Secondary Assets

259 For an effective protection of the primary assets the following secondary assets must also be
260 protected by the TOE and/or its operational environment:

#	Assets	Description	Protective Objective
1.	CONF_SW_DATA	The integrity of the configuration data and program files of the TOE shall be protected against unauthorised access.	I
2.	AUTH_DATA	Unauthorised access to the TOE shall be prevented. The confidentiality, integrity and authenticity of access data, identification and authentication data shall be protected.	C, I, A

3.	AUDIT_DATA	The confidentiality and integrity of all data of the audit trail shall be protected. Unauthorised access shall be effectively prevented.	C, I
4.	KEY_DATA	The confidentiality and integrity of cryptographic key data shall be protected.	C, I

Table 5 Secondary assets

3.3 Subjects and external entities

261 External entities and subjects that may act as threat agent and perform operations on objects are
262 the following:

#	Subjects and External Entities	Description
1.	Human Attacker	This threat agent could be in both higher classified network HIGH and in the lower classified network LOW with the intention to leak classified data from HIGH to LOW.
2.	Non-educated human user	This threat agent resides within the higher classified network HIGH. The non-educated human user may unintentionally misconfigure the TOE.
3.	IT environment	The IT environment defines all components outside of the TOE and outside of the SDoT Security Gateway.
4.	Administrator, and Auditor of the SDoT Adminstation	Authorised persons with access to the SDoT Adminstation, which is connected through a dedicated higher classified network to the SDoT Security Gateway, to administrate, and perform audit task.

Table 6 Subjects

3.4 Threats

263 Any user of the TOE may act as threat agent.

264 This section describes the threats which must be countered by the TOE independently, by its
265 operational environment, or in combination of the two.

#	Threats	Description
1.	T.REVEAL_TO_LOW	**Adverse action:** The threat agent tries to forward confidential information from the network HIGH to a user (human or IT-system) within the lower classified network. **Threat agent:** Human Attacker

		Asset: DATA_IN_HIGH, CONF_SW_DATA, AUTH_DATA, AUDIT_DATA, KEY_DATA
2.	T.MALICIOUS_CODE	**Adverse action:** A human attacker within the higher classified network (HIGH) bypasses the security functionality of the TOE by importing malicious code into the TOE so that confidential data can pass the filtering system of the TOE. **Threat agent:** Human Attacker **Asset:** DATA_IN_HIGH, CONF_SW_DATA
3.	T.AUTH	**Adverse action:** An attacker tries to get unauthorised access to the TOE by bypassing the TOEs authentication mechanisms. The attacker may pretend to be an authorised user of the TOE. **Threat agent:** Human attacker **Asset:** DATA_IN_HIGH, CONF_SW_DATA, KEY_DATA, AUDIT_DATA
4.	T.WRONG_LABEL	**Adverse action:** A human attacker or a non-educated human user in network HIGH replaces security labels (human attacker) or accidentally replaces security labels (non-educated human user), and then passes intentionally (human attacker) or unintentionally (non-educated human user) confidential data, which was initially labelled HIGH, and then be revealed in network LOW. **Threat agent:** Human attacker and/or non-educated human user having access to labelling mechanisms of the TOE **Asset::** DATA_IN_HIGH, CONF_SW_DATA
5.	T.INSERT	**Adverse action:** A human attacker or a non-educated human user inserts confidentially classified information into non-confidential data, after the data was already labelled and classified as non-confidential. Data could then be forwarded to the lower classified network, which may include confidential information. **Threat agent:** Human attacker and non-educated human user having access to the TOE. **Asset: :** DATA_IN_HIGH, CONF_SW_DATA
6.	T.MISCONFIG	**Adverse action:** A non-educated administrator or non-educated policy admin may configure the TOE in an un-intended way, that confidential data pass the filter mechanisms of the TOE. The same holds for careless administrators or policy admins. **Threat agent:** Administrators and Auditor of the SDoT°Adminstations **Asset: :** DATA_IN_HIGH, CONF_SW_DATA

7.	T.AUDIT_CONTROL	**Adverse action:** A human attacker or an IT system, modifies the audit records of the TOE, so that security incidents or illegal actions can remain undetected. **Threat agent:** Human attacker, IT environment **Asset:** AUDIT_DATA
8.	T.AUDIT_COLLAPSE	**Adverse action:** A human attacker or an IT system within the network manipulates the audit trail of the TOE, to produce an audit overflow or produce a huge amount of audit data, to make an analysis of audit logs become increasingly unfeasible. **Threat agent:** Human attacker, IT environment **Asset:** DATA_IN_HIGH, AUDIT_DATA
9.	T.AUDIT_ACCESS	**Adverse action:** A human attacker or an IT system within the network environment of the higher classified network HIGH gets hold of confidential information from data records of the audit trail. **Threat agent:** Human attacker, IT environment **Asset:** DATA_IN_HIGH, AUDIT_DATA

Table 7 Threats

3.5 Assumptions

266 This section of the SPD describes the security aspects of the operational environment in which the
267 TOE is assumed to be operated.

#	Assumptions	Description
1.	A.DIFF_NET	It is assumed that the TOE is connected to two networks with different need to know principles or classifications. The TOE will not fulfil its purpose if the two networks to which the TOE is connected have the same confidentiality classification. Hence, one of the two networks shall have a high classified security domain within a network called 'HIGH' and another one shall have a lower classified security domain within a network called 'LOW'.
2.	A.TRUSTW_ONLY	It is assumed that if other components besides the TOE connect the networks HIGH and LOW, these do not violate the security policy of the TOE.
3.	A.HIGH_PROTECTION	All physical parts of the SDoT Security Gateway, which includes the TOE, are located within the higher classified security domain. This includes all tasks performed, on the SDoT Adminstation of the SDoT Security Gateway.

4.	A.ACCESS	It is assumed that all access to the TOE, and its physical environment, is restricted to authorised persons only. These include administrators and auditor, and human users.
5.	A.TRUSTW_STAFF	It is assumed that all privileged users of the TOE, its underlying platform, and operational environment within the higher classified security domain network HIGH are well trained and follow all policies.
6.	A.AUDIT	An authorised and well-trained auditor shall examine the audit logs in pre-defined time periods which must be in accordance with a security policy defined by the organisation operating the TOE.
7.	A.ROLE_SEPARATION	Since the TOE is not able to separate the roles of privileged users to its individual human characteristics, it is assumed that the organisation operating the TOE defines in its security policy that no individual human user owns the administrator role and the auditor role in the same time.
8.	A.HSM	It is assumed that the TOE is operated with IT systems which are capable of properly assigning labels to the corresponding data. Only appropriate data are signed with labels. The labelling mechanism is sufficiently cryptographically supported by hardware related security mechanisms. Except for the ECDSA key generation for TLS connection to the SDoT Adminstation, the generation of cryptographic keys are not in scope of the TOE and it is assumed that state-of-the-art cryptographic mechanisms are used. The HSM and Smartcards which are in scope of delivery of the SDoT Security Gateway ensure that adequate cryptographic operations are used. Further, the Random Bit Generator of the HSM is used to securely obtain random numbers. Random numbers from HSM are directly used without further post-processing by software. If TLS is used for communication to external systems, the digital signature for TLS used by the web server and communication proxies are generated by the HSM. Further, keys used for audit data protection are generated by the HSM.
9.	A.PKI	It is assumed that a trustworthy PKI is available to the TOE.
10	A.NTP_SERVER	It is assumed that the operator of the TOE uses a reliable NTP server for generating trustworthy time stamps.

11	A.USER_IDENT	It is assumed that all privileged users within the higher classified network are properly identified and authenticated against the related IT systems before any actions can be performed.
12	A.L4_PLATFORM	The TOE runs on a L4Re which is a minimalised operating system with a microkernel architecture providing kernel separation properties. The L4Re is providing an own compartment for each logical separated part of the TOE. Within each compartment an own L4Linux, which is a para-virtualised Linux kernel within the provided hypervisor of L4Re, is running without privileges, and execute the processes of the TOE. Further, it is assumed that the process separation properties of the L4Linux Kernel are properly used.
13	A.DEDICATED_ADMIN_NET	It is assumed that the TOE is connected to the SDoT Adminstation only through a dedicated network for administration purposes. The dedicated admin network is a physically isolated network within the network domain HIGH.
14	A.HIGH_AVAILABILITY	It is assumed that if the operator of the TOE decides to use the optional functionality, namely the HA variant of the SDoT Filter, the operator will provide a physically separated network. The physically separated network is the only connection via the Heartbeat interface of the SDoT Filter designed to operate a cluster of redundant SDoT Filters.
15	A.BOOT	It is assumed that the TOE uses the secure start-up and initialisation mechanisms provided by the UEFI based secure boot process of the SDoT Filter platform. Further, it is assumed that the administrators follow the Guidance Documents to not modify the pre-configured BIOS-settings.

Table 8 Assumptions

3.6 Organisational Security Policies

268 This section describes the Organisational Security Policies (OSPs). The TOE, its operational
269 environment, or a combination of the two shall comply with the following OSPs as security rules,
270 procedures or guidelines imposed (or presumed to be imposed) now and/or in future by an actual or
271 hypothetical organisation in the operational environment (cf. A6.3 of [CC_Part1]).

#	OSPs	Description
1.	OSP.PROTOCOLS	Only protocols which are supported by the filtering function of the TOE are used for communication between the higher classified network HIGH and the lower classified network LOW.

2.	OSP.FLOW_CONTROL	Only data which is classified as low can pass the filtering mechanism of the compartment FI_H2L.
3.	OSP.AUDIT	All message data send from the higher classified network HIGH to the lower classified network LOW shall be registered in the audit trail. All significant attributes of the data are kept in the audit trail. Data which were rejected to be forwarded from network HIGH to network LOW shall be stored in the audit trail. The auditor shall have the possibility to completely access and reconstruct data in the audit trail.
4.	OSP.CONFIG_AUDIT	All changes to the configuration of the TOE shall be identifiable and subject of the audit.
5.	OSP.DUAL_CONTROL	For all changes on the TOE configuration, dual control shall be required. There shall be no change to the TOE configuration possible, if only one administrator made the change. Only configurations which are approved by two administrators of the TOE can be accepted.

Table 9 OSPs

4 Security Objectives (ASE_OBJ.2)

272 This chapter describes the security objectives for the TOE and the security objectives for the
273 operational TOE environment.

4.1 Security Objectives for the TOE

274 The TOE must comply with the following security objectives

#	Objective for the TOE	Description
1.	OT.FILTER	The TOE shall filter all data sent from the higher classified network HIGH and distinguish whether the data can be forwarded to the lower classified network low or not. The TOE shall be able to determine the security attributes and security classification of the data either by checking the attached security label or by cross-checking against a pre-defined rule set for structured data.
2.	OT.PRE_FILTER	The TOE shall provide mechanisms which make it possible to apply a pre-filtering method, before any message data is sent to the main filter of the TOE. The pre-filtering mechanism cannot modify any security label or data message. *Application Note: This security objective shall enable the administrators of the TOE to demand more stringent rules on message data to be passed from network HIGH to LOW. For example, the administrator could configure the pre-filtering mechanism in such a way, that automatically labelled messages will be blocked and not forwarded to the main filter.*
3.	OT.LABELS	The TOE shall provide labelling mechanisms with cryptographic support from the HSM for unambiguous classification of data. For filtering decisions, the TOE shall only consider those security labels which are in accordance to the following: Labels have been generated by an authorised user only Labels are strongly bound to the resp. data and any attempt to modify a label leads to an invalid label and the data will be rejected by the TOE The TOE can unambiguously identify the security level of the data object documented in the corresponding label.

		The TOE can determine whether the level of security of the data was manually assigned by a human user or automatically by an IT system.
4.	OT.SANITISED_DATA	The TOE shall make sure that all data within the higher classified network is sanitised in accordance with the related security policy of the TOE operator. All unnecessary information will be erased from the data resp. from the messages.
5.	OT.BANDWIDTH	The TOE shall provide the functionality to limit the bandwidth for the transfer of message data from the higher classified network HIGH to the lower classified network LOW.
6.	OT.PROTOCOLS	The TOE shall only support the proxies / relays for the following types of communication protocols between the higher classified network HIGH and the lower classified network LOW: SMTP, HTTP, UDP, and TCP.
7.	OT.PROTOCOL_DENY	The TOE shall deny all types of protocol communication which do not comply with the protocols listed in OT.PROTOCOLS
8.	OT.USER_AUTHENTICATION	The TOE shall authenticate all privileged users of the TOE before any actions on the TOE can be performed.
9.	OT.ROLE_SEPARATION	The TOE shall be able to separate the role of the administrators and auditor of the TOE.
10.	OT.FOUR_EYES	Changes to configuration data of the TOE shall only be possible by strictly following the dual control mechanisms enforced by the TOE and supported by the operational environment.
11.	OT.SECURE_CHANNEL	The TOE shall be able to establish a secure communication channel which enables the users (stations) to communicate securely with the provided TSFs of the TOE.
12.	OT.AUDIT_CHANGE_LOG	The TOE shall log all changes to configuration data which enables the auditor to track all changes and identify the user.
13.	OT.AUDIT	The TOE shall be able to track all message data transferred from the network HIGH to network LOW and keep the information in an audit trail. Data which were rejected to be forwarded to network LOW shall be registered for later investigation purposes.

14.	OT.AUDIT_PROTECT	The TOE shall use cryptographic keys stored in the HSM to cryptographically protect the audit records against manipulation of the audit storage records. Further, the TOE shall provide mechanisms to protect audit records against event loss or saturation of the storage device. It shall not be possible to modify any audit record in the audit trail. Only the authorised auditor can review the audit data.
15.	OT.AUDIT_LOG_AVAILABILITY	The TOE shall provide the audit data to authorised auditors.
16.	OT.PROTECTION	The TOE shall protect its own configuration data and program files against attempts of bypassing, deactivating or manipulating the configuration and program files. The TOE shall prevent that any data, which were initially classified to reside within the network HIGH, will be maliciously passed to the lower classified network LOW due to manipulation of configuration data and program files.
17.	OT.INIT	After the initialisation process the TOE shall be constantly in a secure state. If this is for any reason not possible the TOE shall block all network traffic trying to pass the filter mechanism of the TOE.
18.	OT.DEFAULT	The default settings of all configurable items of the TOE shall always be set to a secure state.
19.	OT.WARNING	Upon detection of a security relevant event the TOE shall send warning messages to privileged users.

Table 10 Security Objectives for the TOE

4.2 Security Objectives for the Operational Environment

275 The operational environment must comply with the following security objectives

#	Objective for the Operational Environment	Description
1.	OE.DIFF_NET	The TOE shall be connected to two networks with different classifications. The two networks are classified as HIGH and LOW.
2.	OE.TRUSTW_ONLY	If besides the TOE, there are other connections between the two networks HIGH and LOW, these are established using trustworthy components only and do not violate the security policy of the TOE.
3.	OE.HIGH_PROTECTION	The TOE and all physical parts outside the TOE which are scope of the delivery of the SDoT Security Gateway shall be connected within the higher classified network HIGH only.
4.	OE.ACCESS	All access to the TOE and its physical operational environment is restricted to authorised persons only. These include the auditor, administrators and human users.
5.	OE.TRUSTW_STAFF	The operational environment shall make sure that all privileged users of the TOE are trusted by the organisation operating the TOE.
6.	OE.AUDIT_ENFORCE	The operational environment shall ensure that the audit data is regularly checked by an authorised and well-trained auditor in accordance with the security policy defined by the organisation operating the TOE.
7.	OE.ROLE_SEPARATION	The operational environment shall ensure that the roles of the administrator and the auditor are owned by different persons.
8.	OE.HSM	The operational environment shall ensure that the TOE is operated with IT systems which are capable of properly assigning labels to the corresponding data. Only appropriate data are signed with labels. The labelling mechanism is sufficiently cryptographically supported by hardware related security mechanisms. Since generation of cryptographic keys are not in scope of the TOE the operational environment shall ensure that state-of-the-art cryptographic mechanisms are used. The HSM and Smartcards which are in scope of delivery of the SDoT Security Gateway ensure that adequate cryptographic

		operations are used. Further, the output from the Random Bit Generator of the HSM shall be used directly without further post-processing by software. If TLS is used for communication to external systems the operational environment shall ensure that the digital signature for TLS used by the web server and communication proxies is generated by the HSM. Further, it shall be ensured that keys used for audit data protection is generated by the HSM.
9.	OE.PKI	The operator of the TOE shall use a trustworthy PKI for digital signing certificates (CSRs) and generating and administrating CAs and CRLs.
10	OE.NTP_SERVER	The operator of the TOE shall use a trustworthy NTP server which is capable to reliably synchronise the time between all components in the operational environment of the TOE.
11	OE.USER_IDENT	The operational environment shall identify and authenticate all privileged users within the higher classified network HIGH before any actions can be performed.
12	OE.L4_PLATFORM	The operational environment regarding the operating system on which the TOE is running shall be an L4Re microkernel OS where each logically separated part of the TOE runs in a dedicated compartment. Within each compartment an own L4Linux, which is a para-virtualised Linux kernel within the provided hypervisor of L4Re, shall be used without privileges, and execute the processes of the TOE. The process separation properties of the L4Linux Kernel are shall be properly used.
13	OE.DEDICATED_ADMIN_NET	The TOE shall be connected to the SDoT Adminstation only through a dedicated network for administration purposes. The dedicated admin network shall be an isolated network within the higher classified domain HIGH.
14	OE.HIGH_AVAILABILITY	The operational environment shall ensure that if the operator of the TOE decides to use the optional functionality, namely the HA variant of the SDoT Filter, the operator will provide a physically separated network. The physically separated network shall be the only connection via the Heartbeat interface of the SDoT Filter designed to operate a cluster of redundant SDoT Filters.
15	OE.BOOT	The TOE shall use the secure start-up and initialisation mechanisms provided by the UEFI based secure boot process of the SDoT Filter platform. Further, the

		administrators shall follow the Guidance Documents to not modify the pre-configured BIOS-settings.

Table 11 Security Objectives for the Operational Environment

4.3 Rationale between SPD and security objectives

276 The following two tables provides the security objectives coverage for the TOE and the security objectives coverage for the operational environment of the TOE.

	Objectives for the TOE	OT.FILTER	OT.PRE_FILTER	OT.LABELS	OT.SANITISED_DATA	OT.BANDWIDTH	OT.PROTOCOLS	OT.PROTOCOL_DENY	OT.USER_AUTHENTICATION	OT.ROLE_SEPARATION	OT.FOUR_EYES	OT.AUDIT_CHANGE_LOG	OT.SECURE_CHANNEL	OT.AUDIT	OT.AUDIT_PROTECT	OT.AUDIT_LOG_AVAILABILITY	OT.PROTECTION	OT.INIT	OT.DEFAULT	OT.WARNING
Threats																				
T.REVEAL_TO_LOW		x	x	x	x	x	x	x	x		x	x		x		x			x	x
T.MALICIOUS_CODE																	x	x		
T.AUTH									x				x							
T.WRONG_LABEL				x																
T.INSERT				x																
T.MISCONFIG										x	x	x			x					
T.AUDIT_CONTROL									x	x					x					
T.AUDIT_COLLAPSE															x					

	Objectives for the TOE	OT.FILTER	OT.PRE_FILTER	OT.LABELS	OT.SANITISED_DATA	OT.BANDWIDTH	OT.PROTOCOLS	OT.PROTOCOL_DENY	OT.USER_AUTHENTICATION	OT.ROLE_SEPARATION	OT.FOUR_EYES	OT.AUDIT_CHANGE_LOG	OT.SECURE_CHANNEL	OT.AUDIT	OT.AUDIT_PROTECT	OT.AUDIT_LOG_AVAILABILITY	OT.PROTECTION	OT.INIT	OT.DEFAULT	OT.WARNING
T.AUDIT_ACCESS									x				x							
OSPs																				
OSP.PROTOCOLS							x	x												
OSP.FLOW_CONTROL		x																		
OSP.AUDIT														x	x	x				
OSP.CONFIG_AUDIT									x			x								
OSP.DUAL_CONTROL											x									

Table 12 Security Objective for the TOE coverage

	Objectives for the Operational Environment	OE.DIFF_NET	OE.TRUSTW_ONLY	OE.HIGH_PROTECTION	OE.ACCESS	OE.TRUSTW_STAFF	OE.AUDIT_ENFORCE	OE.ROLE_SEPARATION	OE.HSM	OE.PKI	OE.USER_IDENT	OE.L4_PLATFORM	OE.NTP_SERVER	OE.DEDICATED_ADMIN_NET	OE.HIGH_AVAILABILITY	OE.BOOT
Threats																
T.REVEAL_TO_LOW		x	x	x		x										
T.MALICIOUS_CODE				x												x
T.AUTH																
T.WRONG_LABEL																
T.INSERT																
T.MISCONFIG				x												
T.AUDIT_CONTROL					x											
T.AUDIT_COLLAPSE																
T.AUDIT_ACCESS					x		x									
OSPs																

	Objectives for the Operational Environment	OE.DIFF_NET	OE.TRUSTW_ONLY	OE.HIGH_PROTECTION	OE.ACCESS	OE.TRUSTW_STAFF	OE.AUDIT_ENFORCE	OE.ROLE_SEPARATION	OE.HSM	OE.PKI	OE.USER_IDENT	OE.L4_PLATFORM	OE.NTP_SERVER	OE.DEDICATED_ADMIN_NET	OE.HIGH_AVAILABILITY	OE.BOOT
OSP.PROTOCOLS																
OSP.FLOW_CONTROL																
OSP.AUDIT							x									
OSP.CONFIG_AUDIT																
OSP.DUAL_CONTROL																
Assumptions																
A.DIFF_NET		x														
A.TRUSTW_ONLY		x	x													
A.HIGH_PROTECTION				x												
A.ACCESS					x											
A.TRUSTW_STAFF						x										

	Objectives for the Operational Environment	OE.DIFF_NET	OE.TRUSTW_ONLY	OE.HIGH_PROTECTION	OE.ACCESS	OE.TRUSTW_STAFF	OE.AUDIT_ENFORCE	OE.ROLE_SEPARATION	OE.HSM	OE.PKI	OE.USER_IDENT	OE.L4_PLATFORM	OE.NTP_SERVER	OE.DEDICATED_ADMIN_NET	OE.HIGH_AVAILABILITY	OE.BOOT
A.AUDIT							x									
A.ROLE_SEPARATION								x								
A.HSM									x							
A.PKI										x						
A.USER_IDENT											x					
A.L4_PLATFORM												x				
A.NTP_SERVER													x			
A.DEDICATED_ADMIN_NET														x		
A.HIGH_AVAILABILITY															x	
A.BOOT																x

Table 13 Security Objective for the Operational Environment Coverage

277 In the following subsections a more detailed justification of the security objectives coverage related
278 to the SPD is given.

4.4 Rationale Threats

279 The following subsections provide a rational on how threats are encountered by the TOE or by the
280 operational environment of the TOE.

4.4.1 T.REVEAL_TO_LOW

281 Potential leakage of confidential information from the network HIGH to a user (human or IT-System)
282 within the lower classified network is countered by a combination of several objectives for the TOE
283 and objectives for the operational environment of the TOE.

284 OT.FILTER addresses T.REVEAL_TO_LOW with the corresponding filtering mechanism which filters
285 all data sent between the higher classified network and the lower classified network. OT.FILTER
286 makes sure that only data are passing the filtering mechanism of the TOE which is classified to have
287 at least the same security level of the lower classified network LOW or less than LOW.

288 OT.PRE_FILTER provides additional filtering mechanisms to further mitigate the risk of
289 T.REVEAL_TO_LOW by blocking inappropriate messages before they can even reach the main
290 filtering component of the TOE.

291 OT.SANITISED_DATA counters T.REVEAL_TO_LOW by ensuring that no confidential information
292 can pass the filtering mechanism to the lower classified network in accordance with the security rule
293 set of the TOE operator. All unnecessary information will be removed from the data resp. from the
294 message and are not visible to the user.

295 OT.USER_AUTHENTICATION addresses T.REVEAL_TO_LOW by ensuring that only authorised and
296 authenticated users can access and change configuration of the TOEs security related
297 functionalities.

298 OT.LABELS provides the meta-information and therefore the security label which supports
299 OT.FILTER by its filtering decision.

300 Further, it ensures that the attached label are unambiguously assignable to the respective data.

301 OT.INIT counters T.REVEAL_TO_LOW in the case where after TOE initialisation a secure state cannot
302 be achieved. Here, the TOE will block all traffic and no higher classified confidential information can
303 be passed from the higher classified network to the lower classified network.

304 OT.PROTOCOLS counters T.REVEAL_TO_LOW by ensuring that only data sent with communication
305 protocols, which are supported by the TOE, are passed through the filtering mechanism of the TOE.
306 All other communication attempts are rejected by the TOE with OT.PROTOCOL_DENY.

307 OT.BANDWIDTH adds a further countermeasure. It enables an upper limit for data to be transferred,
308 and thus, a limitation of the bandwidth of any possibly remaining information leakage in case of any
309 information disclosure.

310 OT.FOUR_EYES ensures that no single administrator or policy-admin of the TOE is able to
311 maliciously misconfigure the TOE, which may lead to any security flaw or leakage of confidential
312 information.

313 OT.AUDIT_CHANGE_LOG enables the auditor to track all changes to the TOE configuration, and
314 identify the corresponding user. This objective for the TOE addresses T.REVEAL_TO_LOW by

motivating the user to not make any light-minded change to the TOE configuration, and avoid any misconfiguration of the TOE.

OT.AUDIT addresses T.REVEAL_TO_LOW by making possible to the auditor to detect illegally transferred data or any attempt to send data illegally from the higher classified network to the lower classified network.

OT.AUDIT_LOG_AVAILABILITY provides the audit logs to the auditor so that potential incidents can be identified and analysed.

OT.DEFAULT ensures that any potential unsecure state must be configured manually and intentionally by the administrators. This avoids any unintentionally unsecure state via default settings of the TOE.

OT.WARNING addresses T.REVEAL_TO_LOW by reducing the risk of any sending of confidential information, intentionally or accidentally to the lower classified network since, this is a security relevant event, and the TOE sends warning messages to the user.

OE.DIFF_NET, OE.TRUSTW_STAFF and OE.TRUSTW_ONLY support OT.FILTER by ensuring that all data to be sent between the higher classified and the lower classified networks have to pass the filtering mechanism since, there are only trustworthy connection between the higher classified and the lower classified networks. Further, the organisation operating the TOE ensures that only trustworthy personnel have privileged user roles.

Further, OE.DEDICATED_ADMIN_NET supports OT.FILTER to ensure that the TOE is only configured through a dedicated admin network which is additionally supports to secure the configuration of the TOE.

OE.HIGH_PROTECTION supports OT.FILTER to further address T.REVEAL_TO_LOW by ensuring that all filtering tasks performed by the TOE is done within the higher classified network, before sending any data to the lower classified network.

4.4.2 T.MALICIOUS_CODE

OT.PROTECTION addresses T.MALICIOUS_CODE by directly requiring the TOE to protect all configuration data against any attempt to bypass, deactivate, or manipulate the configuration of the TOE.

OT.INIT ensures that the TOE is in a secure state after the initialisation process. Periodically performed integrity checks help to verify the current state and help detect any unsigned code.

OE.HIGH_PROTECTION addresses T.MALICIOUS_CODE by requiring the TOE to be located within the HIGH domain. Further, OE.BOOT helps to mitigate the risk of T.MALICIOUS_CODE in the presence of secure boot mechanisms which only allows authentic software to be executed. Additionally, OE.BOOT requires the administrators to keep the securely pre-configures settings of the used BIOS.

4.4.3 T.AUTH

OT.USER_AUTHENTICATION counters T.AUTH by means of requiring all users of the TOE with special privileges within the higher classified network to be authenticated before any action on the TOE is possible. OT.SECURE_CHANNEL supports OT.USER_AUTHENTICATION by providing a secure channel for privileged users to communicate with the TOE.

4.4.4 T.WRONG_LABEL

353 OT.LABELS counters T.WRONG_LABEL by ensuring that the TOE only uses labels

354 • which have been generated by an authorised user only,

355 • are strongly bound to the resp. data and any attempt to modify a label leads to an
356 invalid label and the data will be rejected by the TOE,

357 • The TOE can unambiguously identify the categorisation of the security level of the
358 label

359 • The TOE can determine whether the categorisation of the level of security of the data
360 was manually within the network HIGH or automatically by an IT system.

361 Further, it counters T.WRONG_LABEL by requiring the TOE to use security labels which have a
362 strong bond between the label and the corresponding data resp. the message.

4.4.5 T.INSERT

363 OT.LABELS counters T.INSERT, by requiring that labels generated by the TOE have a strong bound
364 to the corresponding data. Any modification of the data will make the label and the data invalid for
365 the TOE.

4.4.6 T.MISCONFIG

366 OT.FOUR_EYES addresses T.MISCONFIG by avoiding that an administrator or policy-admin could
367 unintentionally misconfigure the TOE by means of enforcing the dual control mechanism.

368 OT.PROTECTION counters the T.MISCONFIG by ensuring that the TOE cannot be misconfigured in a
369 way, that data can pass the filtering mechanism of the TOE from the higher classified network to the
370 lower classified network.

371 OT.ROLE_SEPARATION limits the privileges of a single user, i.e. administrator is not able to
372 misconfigure the TOE in a way that the configuration change is not logged and not detected by the
373 auditor.

374 OT.AUDIT_CHANGE_LOG ensures that each configuration change is logged into the audit trail and
375 the identity of the user who is triggering any configuration change is logged. This may limit errors
376 due to misconfiguration of the TOE to a minimum and encourage the user to be more careful. The
377 auditor can analyse the audit trail and detect any possible misconfiguration and replace by a safe
378 and good known configuration.

379 OT.AUDIT_PROTECT ensures that logged configurations are cryptographically protected against
380 manipulation.

381 OE.HIGH_PROTECTION reduces the risk that the TOE will be attacked from the lower classified
382 network. The TOE is physically and organisationally located within the higher classified network.

4.4.7 T.AUDIT_CONTROL

383 OT.AUDIT_PROTECT counters the threat by protecting the audit data against any attempt of
384 bypassing, deactivating, or manipulating the audit data.

385 OT.ROLE_SEPARATION ensures that only the auditor is able to remove records from the audit trail.

386 OE.ACCESS counters the threat by ensuring that only auditors and administrators have physical
387 access to the TOE.

388 OT.USER_AUTHENTICATION supports OT.ROLE_SEPARATION by ensuring that the auditor is
389 authenticated before the auditor can take any action.

4.4.8 T.AUDIT_COLLAPSE

390 OT.AUDIT_PROTECT counters T.AUDIT_COLLAPSE directly by preventing audit overflows.
391 OT.AUDIT_PROTECT requires the TOE to provide mechanisms to protect audit records against event
392 loss or saturation of the storage device.

4.4.9 T.AUDIT_ACCESS

393 OE.AUDIT_ENFORCE requires that the audit trail is regularly checked by the authorised auditor so
394 that records are regularly reduced. This mitigates the threat T.AUDIT_ACCESS because the amount
395 of confidential audit records is kept manageable.

396 OT.ROLE_SEPARATION counters T.AUDIT_ACCESS by ensuring that a privileged user with other
397 user role than the auditor cannot move audit records.

398 OT.USER_AUTHENTICATION counters the threat T.AUDIT_ACCESS by ensuring that the auditor is
399 authorised to read and move audit records. OT.SECURE_CHANNEL supports
400 OT.USER_AUTHENTICATION by providing a secure channel for authorised auditors to communicate
401 with the TOE.

402 OE.ACCESS supports to counter the threat by making sure that only authorised users have access
403 to the TOE. Hence, only authorised auditors have access to any audit data.

4.5 Rationale OSPs

404 The following describes how OSPs are enforced by the TOE or by the operational environment of
405 the TOE.

4.5.1 OSP.PROTOCOLS

406 The security objective for the TOE OT.PROTOCOLS corresponds to OSP.PROTOCOLS by requiring
407 the TOE to only process the pre-defined list of supported protocols as listed by OT.PROTOCOLS. All
408 other protocols will not be accepted and is provided by OT.PROTOCOL_DENY.

4.5.2 OSP.FLOW_CONTROL

409 OT.FILTER ensures that only data which is corresponding to the classification of the lower classified
410 network can pass the filtering mechanism of the TOE. Therefore, OT.FILTER is addressed by the
411 organisational security policy OSP.FLOW_CONTROL.

4.5.3 OSP.AUDIT

412 The objective OT.AUDIT requires the TOE to log all information regarding origin, destination, time of
413 transfer of data and the result of filtering decision which makes it possible to retrace all data passed
414 the filtering mechanism of the TOE.

415 OE.AUDIT_ENFORCE requires that the audit trail is regularly examined by an authorised auditor.
416 OT.AUDIT_LOG_AVAILABILITY supports OE.AUDIT_ENFORCE by providing the audit data to the
417 authorised auditor.

418 Further, OT.AUDIT_PROTECT ensures the integrity of audit data and enforces that records are not
419 lost.

4.5.4 OSP.CONFIG_AUDIT

420 The objective OT.AUDIT_CHANGE_LOG requires that all changes to configuration data are logged.
421 The auditor shall be able to track all changes and identify the user who made any change. Also, the
422 identification of the user is realised by OT.USER_AUTHENTICATION. The combination of both
423 objectives implements the policy.

4.5.5 OSP.DUAL_CONTROL

424 OT.FOUR_EYES implements this policy by requiring that all changes are performed by two
425 administrators. There is no possibility that only one administrator can make changes without the
426 confirmation of a second administrator.

4.6 Rationale Assumptions

427 In this section the correspondence between the assumptions, and the objectives for the TOE, or its
428 operational environment is demonstrated.

4.6.1 A.DIFF_NET

429 The security objective for the operational environment of the TOE OE.DIFF_NET corresponds to the
430 assumption A.DIFF_NET by requiring the TOE to be connected between two networks, which have
431 different security classifications. One network has a higher classification than the other.

4.6.2 A.TRUSTW_ONLY

432 OE.TRUSTW_ONLY requires that the TOE is the only connection between the higher classified
433 network, and the lower classified network. OE.DIFF_NET supports OE.TRUSTW_ONLY because it
434 requires that the TOE is connected to two differently classified networks.

4.6.3 A.HIGH_PROTECTION

435 This assumption is directly covered by the objective OE.HIGH_PROTECTION which requires the TOE
436 to be physically and organisationally located and operated within the domain of the higher classified
437 network.

4.6.4 A.ACCESS

438 This assumption is directly covered by the objective OE.ACCESS which requires that all access to
439 the TOE and its physical operational environment is restricted to authorised users only.

4.6.5 A.TRUSTW_STAFF

440 OE.TRUSTW_STAFF covers the assumption A.TRUSTW_STAFF by requiring that all users of the
441 TOE are trusted by the organisation operating the TOE.

4.6.6 A.AUDIT

442 The assumption A.AUDIT is covered by OE.AUDIT_ENFORCE because the operational environment
443 of the TOE ensures that audit data is regularly checked by an authorised auditor.

4.6.7 A.ROLE_SEPARATION

444 OE.ROLE_SEPARATION upholds this assumption because this objective requires the operational
445 environment to ensure that each privileged user of the TOE has exactly one privileged user role.

4.6.8 A.HSM

446 OE.HSM addresses A.HSM which ensures that all needed cryptographic support is derived from the
447 cryptographic units which are delivered together with the TOE.

4.6.9 A.PKI

448 The assumption A.PKI is covered by the objective OE.PKI which requires the operator of the TOE to
449 use a trustworthy PKI.

4.6.10 A.NTP_SERVER

450 The assumption A.NTP_SERVER is covered by the objective OE.NTP_SERVER which requires the
451 operator of the TOE to use a trustworthy NTP server.

4.6.11 A.USER_IDENT

452 The assumption A.USER_IDENT is covered by the objective OE.USER_IDENT which requires to
453 identify and authenticate all privileged users within the higher classified network HIGH before any
454 actions can be performed.

4.6.12 A.L4_PLATFORM

455 The assumption A.L4_PLATFORM is covered by the objective OE.L4_PLATFORM which requires the
456 TOE to run on a L4Re microkernel OS which provides dedicated logical separation mechanisms for
457 each compartment.

4.6.13 A.DEDICATED_ADMIN_NET

458 The assumption A.DEDICATED_ADMIN_NET is covered by the objective
459 OE.DEDICATED_ADMIN_NET which requires that the TOE is connected to the SDoT Adminstation
460 only through a dedicated network for administration purposes. Further, the objective requires that
461 the dedicated admin network is a physically isolated network within the higher classified network
462 HIGH.

4.6.14 A.HIGH_AVAILABILITY

463 The assumption A.HIGH_AVAILABILITY is addressed by OE.HIGH_AVAILABILITY which requires that
464 if the TOE will be operated in the HA-variant, the operational environment ensures that the
465 physically separated network via the Heartbeat interface is the only used connection.

4.6.15 A.BOOT

466 The assumption A.BOOT is directly addressed by OE.BOOT which requires that the TOE uses the
467 secure start-up and boot mechanisms provided by the underlying platform. Further, the
468 administrators of the TOE are required to use the securely pre-configured BIOS settings.

5 Definition of Security Function Policies (SFPs)

audit access control SFP		
Type	**Name**	**Remark**
Subject and/or users	User trying to have access to the audit trail	See FDP_ACF.1.1/AuditAccess
Object	Audit records	
Security Attribute	user_role	
Operation	Read audit_records	See FDP_ACF.1.2/AuditAccess
	Delete audit_records	
Condition	user_role = auditor	

Table 14 audit access control SFP

admin access control SFP		
Type	**Name**	**Remark**
Subject and/or users	User trying to gain access to the TOE general configuration	See FDP_ACF.1.1/AdminAccess
Object	General TOE configuration	
Security Attribute	user_role	
Operation	Read general TOE configuration	See FDP_ACF.1.2/AdminAccess
Condition	user_role = administrator	

Table 15 admin access control SFP

policy admin access control SFP		
Type	**Name**	**Remark**
Subject and/or users	User trying to gain access to the configuration of TOE functionalities which automatically perform checks regarding the security level of a message.	See FDP_ACF.1.1/PolicyAdminAccess
Object	TOE parameter of TOE functionalities which automatically perform checks regarding the security level of a message.	
Security Attribute	user_role	
Operation	Read the TOE corresponding parameter	See FDP_ACF.1.2/PolicyAdminAccess
Condition	user_role = policy admin	

Table 16 policy admin access control SFP

dual control admin SFP		
Type	**Name**	**Remark**
Subject and/or users	User trying to modify the TOE general configuration	The TOE enforces dual control mechanisms which ensures that changes to the general TOE configuration must be confirmed by a second administrator.
Object	general TOE configuration	-
Security Attribute	user_role	User role
Operation	modify, add or delete general TOE configuration	See FDP_ACF.1.2/Admin
Condition	user_role = administrator	

Table 17 dual control admin SFP

dual control policy admin SFP		
Type	**Name**	**Remark**
Subject and/or users	User having access to change the configuration of TOE functionalities which automatically perform checks regarding the security level of a message	The TOE enforces dual control mechanisms for any changes made by a policy admin which must be confirmed by another policy admin.
Object	TOE parameter	TOE Parameter of TOE functionalities which automatically perform checks regarding the security level of incoming data a message.
Security Attribute	user_role	See FDP_ACF.1.2/PolicyAdmin
Operation	modify, add or delete TOE parameter	See FDP_ACF.1.2/PolicyAdmin
Condition	user_role = policy admin	

Table 18 dual control policy admin SFP

data validation SFP		
Type	**Name**	**Remark**
Subject	Parser process	Internal parser processes of the TOE
Information	Message	Message to be validated against a labelled rule set.

Security Attribute	data_label_type label_class_info rule_set_label_class_info data_security_label ICAP_class_info	Security label type. The classification information (label_class_info) to be stored into the label of Message. (rule_set_label_class_info) contains the classification information stored in the label of the corresponding rule set. If the validation of Message is successful, then either a security label will be attached (data_security_label) or the classification information of Message is written into the ICAP header (ICAP_class_info) of Message.
Operation	Message validation	See FDP_IFF.1/Validation
Condition	Message passes as described in FDP_IFF.1/Validation	-

Table 19 data labelling SFP

check label SFP		
Type	**Name**	**Remark**
Subject	Check label process	Internal process of the TOE which is responsible for the verification of attached security labels.
Information	data_content	Data to be transmitted
	security_label	Security label of data_content.
Security Attribute (security_label)	data_security_label	Content of security label
	data_security_label.signature	Signature of security label
	data_security_label.policy_id	Policy identifier stored in security label A policy contains a set of classifications. What is tested must be included in this set.
	Data_security_label.classification	Type of classification stored in security label The classifications are defined fixed values in the SPIF, whereas the label is checked.
	Data_security_label.categories	Type of category stored in security label
Security Attribute (LabelCA.CONF)	Data_Label.CA	CA(s) used to validate signatures of Security label.
	SPIF.policy_id	Policy identifier of SPIF

Security Attribute (SPIF.CONF)	SPIF.valid_classification	Valid classification within the SPIF
	SPIF.valid_categories	Valid categories within the SPIF A category is a restriction or extension of the classification, e.g. "releasable to" or "Need to Know", or no label may be accepted from certain object/persons.
	SPIF.invalid_combination	Invalid combinations between classifications and categories
Operation	further processing of label or rejection if check of security label fails.	-
Condition	Verification of data_security_label.signature is successful and data_security_label is well-formed and data_security_label.policy_id = SPIF.policy_id and data_security_label.classification $\in$ {SPIF.valid_classification} and {data_security_label.categories} $\subseteq$ {SPIF.valid_categories} and {data_security_label.classification x data_security_label.categories} $\notin$ { SPIF.invalid_combination }	{data_security_label.classification x data_security_label.categories} = {(classification, category_1), ..., (classification, category_N), N $\in \mathbb{N}$} The structure of a security label is described in sec. 8.1.1 and technically more detailed in [Kon_Label].

Table 20 check label SFP

data to low SFP		
Type	**Name**	**Remark**

Subject	Filter	Filtering functionality of the TOE
	user_low_net	User/Users in the lower classified network LOW
	user_role_sender	The role of the user sending the data
Information	data_content	Data sent from higher classified network HIGH to the lower classified network LOW.
Security Attribute	security_level_low.CONF	The security level of the lower classified network LOW
	data_security_level	The attribute security level of the data sent from the higher classified network HIGH to the lower classified network LOW is derived from the attached security label or from the ICAP header of received data, see°FDP_IFF.1/Validation and FDP_IFF.1/PreFilter.
	mode.CONF	Configuration of the mode of operation of the TOE whether maintenance mode or operational mode
	band_limit.CONF	Limit of bandwidth for data transmission
	data_bandwidth	Bandwidth of data transmission
Authentication Method	-	-
Operation	forward data to user in the lower classified network LOW user_low_net	-
Condition	data_security_level ≤ security_level_low.CONF	-

Table 21 data to low SFP

pre-filtering SFP		
Type	**Name**	**Remark**
Subject	Pre-filter	Pre filtering component of the TOE
Information	data_security_label	Incoming security labels of data to be transmitted.

Security Attribute	data_security_label.attributes	The attributes of data_security_label whether the data was labelled automatically and externally or internally
	label_types allowed_attributes.CONF	The part of the TOE configuration which determines the allowed type (allowed_attributes.CONF) of the security label (label_types) whether they can pass the filtering function.
Operation	See application note of FDP_IFF.1.4/PreFilter	-
Condition	See FDP_IFF.1.2/PreFilter, FDP_IFF.1.3/PreFilter	-

Table 22 pre-filtering SFP

supported protocol SFP		
Type	**Name**	**Remark**
Subject	next_step.DATA	Component of the TOE which would process the protocol data unit in the next step
Information	data_units.PROTOCOL	Protocol data units which are sent from the higher classified network HIGH to the lower classified network LOW
Security Attribute	protocol	-
Operation	see FDP_IFF.1.2/Supported-Protocol	-
Condition	see FDP_IFF.1.2/Supported-Protocol	-

Table 23 supported protocol SFP

clean protocol SFP		
Type	**Name**	**Remark**
Subject	next_step.DATA	See *Table 23*
Information	data_units.PROTOCOL	See *Table 23*
Security Attribute	protocol	-
Operation	See FDP_IFF.1.2/CleanProtocol	-
Condition	See FDP_IFF.1.2/CleanProtocol	-

Table 24 clean protocol SFP

6 Extended components definition (ASE_ECD.1)

6.1 Class FPT: Protection of the TSF

6.1.1 TSF integrity checks (FPT_INC)

469 **Family Behaviour**

470 The family defines the requirements for the self-testing of the TSF with respect to integrity checks
471 of TSF data. Examples are the integrity of general TOE configuration data and TSF executable code.
472 The actions to be taken by the TOE as the result of self-testing are defined in other families.

473 Application Note: The other families of the class FPT do not provide a family which only refers to
474 periodic integrity checks during start-up, during operation or upon request of an authorised user. In
475 the following, the family FPT_INC TSF Integrity Checks will be defined in accordance with the style
476 used in the Common Criteria Part 2, cf. sections 6 and 7 in [CC_Part2].

477 **Component Levelling**

478 FPT_INC.1 TSF Integrity, provides the ability to verify the integrity of TSF data and TSF itself. This
479 test may be performed at start-up, periodically, at the request of the authorised user, or when other
480 conditions are met.

481 **Management FPT_INC.1**

482 a) management of the conditions under which TSF integrity checks occurs, such as during initial
483 start-up, regular interval, or under specified conditions;

484 b) management of the time interval if appropriate.

485 **Audit: FPT_INC.1**

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

488 a) Execution of the TSF integrity checke and the results of the checks.

FPT_INC.1	**TSF Integrity**	
	Hierarchical to:	No other components.
	Dependencies:	No dependencies.
FPT_INC.1.1	The TSF shall run a suite of integrity checks [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions[assignment: conditions under which integrity check should occur]*] to demonstrate the integrity of [selection: *[assignment: parts of TSF data, parts of TSF], the TSF, the TSF data*].	
FPT_INC.1.2	The TSF shall provide authorised users with the capability to verify the integrity of [selection: *[assignment: parts of TSF data], TSF data*].	
FPT_INC.1.3	The TSF shall provide authorised users with the capability to verify the integrity of [selection: *[assignment: parts of TSF], TSF*].	

7 Statement of security requirements (ASE_REQ.2)

489 This section defines the security functional requirements according to [CC_Part2] and the security
490 assurance requirements (SARs) from [CC_Part3], which apply for the TOE.

7.1 Security functional requirements

491 The following table outlines the Security Functional Requirements (SFRs) for the TOE:

#	User Data Protection (FDP)	
1.	FDP_ACC.1/AuditAccess	Subset access control
2.	FDP_ACC.1/Admin	Subset access control
3.	FDP_ACC.1/PolicyAdmin	Subset access control
4.	FDP_ACC.1.1/AdminAccess	Subset access control
5.	FDP_ACC.1.1/PolicyAdminAccess	Subset access control
6.	FDP_ACF.1/AuditAccess	Security attribute based access control
7.	FDP_ACF.1/Admin	Security attribute based access control
8.	FDP_ACF.1/PolicyAdmin	Security attribute based access control
9.	FDP_ACF.1.1/AdminAccess	Security attribute based access control
10.	FDP_ACF.1.1/PolicyAdminAccess	Security attribute based access control
11.	FDP_IFC.1/DataToLow	Subset information flow control
12.	FDP_IFC.1/PreFilter	Subset information flow control
13.	FDP_IFC.1/Supported-Protocol	Subset information flow control
14.	FDP_IFC.1/CleanProtocol	Subset information flow control
15.	FDP_IFC.1/Validation	Subset information flow control
16.	FDP_IFF.1/DataToLow	Simple security attributes
17.	FDP_IFF.1/PreFilter	Simple security attributes
18.	FDP_IFF.1/Supported-Protocol	Simple security attributes
19.	FDP_IFF.1/CleanProtocol	Simple security attributes

20.	FDP_IFF.1/Validation	Simple security attributes
21.	FDP_IFF.3	Limited illicit information flow
	Trusted path (FTP)	
22.	FTP_TRP.1	Trusted path
	Identification and authentication (FIA)	
23.	FIA_UAU.2	User authentication before any action
24.	FIA_UID.2	Timing of identification
	Cryptographic support (FCS)	
25.	FCS_CKM.1/ECDSA	Cryptographic operation
26.	FCS_CKM.2	Cryptographic operation
27.	FCS_CKM.4	Cryptographic operation
28.	FCS_COP.1/RSA	Cryptographic operation
29.	FCS_COP.1/ECDSA	Cryptographic operation
30.	FCS_COP.1/AES	Cryptographic operation
31.	FCS_COP.1/HMAC	Cryptographic operation
32.	FCS_COP.1/SHA2	Cryptographic operation
	Security management (FMT)	
33.	FMT_MSA.1	Management of security attributes
34.	FMT_MSA.3	Static attribute initialisation
35.	FMT_MTD.1/Admin	Management of TSF data
36.	FMT_MTD.1/AuditAccess	Management of TSF data
37.	FMT_MTD.1/AuditDelete	Management of TSF data
38.	FMT_MTD.1/PolicyAdmin	Management of TSF data
39.	FMT_MTD.3	Secure TSF data
40.	FMT_SMF.1	Specification of management functions
41.	FMT_SMR.2	Security management roles

	Protection of the TSF (FPT)	
42.	FPT_STM.1	Reliable time stamps
43.	FPT_INC.1	TSF integrity
44.	FPT_TDC.1	Inter-TSF basic TSF data consistency
	Security audit (FAU)	
45.	FAU_ARP.1	Security audit automatic response
46.	FAU_GEN.1	Audit data generation
47.	FAU_GEN.2	User identity association
48.	FAU_SAA.1	Security audit analysis
49.	FAU_SAR.1	Security audit review
50.	FAU_SAR.2	Restricted audit review
51.	FAU_STG.2	Guarantees of audit data availability
52.	FAU_STG.3	Action in case of possible audit data loss
53.	FAU_STG.4	Prevention of audit data loss

Table 25 SFRs of the TOE

492 The following styles of marking operations are applied:

493 • Assignments are denoted in **bold.**

494 • Selections are marked in *italic underlined.*

495 • Iterations are marked by adding a "/" and short name to the SFR identification.

496 • Refinements indicating additions are marked in ***bold and italic underlined.***

497 • Refinements indicating removals are marked as ~~crossed out.~~

7.1.1 User Data Protection (FDP)

FDP_ACC	**Access control policy**
FDP_ACC.1/AuditAccess	Subset access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/AuditAccess	The TSF shall enforce the **audit access control SFP** on **subjects and/or users having access to the audit trail of the TOE to perform the operations Read or Delete of audit_records.**

Application Note: In this SFR the general term "subject" as given in [CC_Part2] in the second assignment of this SFR is refined to "subjects and/or users".

FDP_ACC.1/AdminAccess	Subset access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/AdminAccess	The TSF shall enforce the **admin access control SFP** on **subjects and/or users having access to the general configuration of the TOE to read configuration items.**

Application Note: In this SFR the general term "subject" as given in [CC_Part2] in the second assignment of this SFR is refined to "subjects and/or users".

FDP_ACC.1/PolicyAdminAccess	Subset access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/PolicyAdminAccess	The TSF shall enforce the **policy admin access control SFP** on **subjects and/or users having access to the rule set configuration of the TOE to read configuration items.**

Application Note: In this SFR the general term "subject" as given in [CC_Part2] in the second assignment of this SFR is refined to "subjects and/or users".

FDP_ACC.1/Admin	Subset access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1Security attribute based access control
FDP_ACC.1.1/Admin	The TSF shall enforce the **dual control admin SFP** on **subjects and/or users having access to change the general configuration of the TOE.**

Application Note: In this SFR the general term "subject" as given in [CC_Part2] in the second assignment of this SFR is refined to "subjects and/or users".

FDP_ACC.1/PolicyAdmin	Subset access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1/PolicyAdmin	The TSF shall enforce the **dual control policy admin SFP** on **subjects and/or users having access to change the**

	configuration of TOE functionalities which automatically perform checks regarding the security level of incoming structured data.

Application Note: In this ST the general term "subject" as given in [CC_Part2] in the second assignment of this SFR is refined to "subjects and/or users".

FDP_ACF	**Access control functions**
FDP_ACF.1/AuditAccess	Security attribute based access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/AuditAccess	The TSF shall enforce the **audit access control SFP** to objects based on the following: 1. **Subject and/or users: User trying to have access to the audit trail** 2. **Object: audit trail** 3. **Security Attributes: user role (notation: user_role)**
FDP_ACF.1.2/AuditAccess	The TSF shall enforce the following rules to determine if an operation among controlled ***subjects and/or users*** and controlled objects is allowed: **operation: read/delete audit_records** **condition: user_role = auditor.**
FDP_ACF.1.3/AuditAccess	The TSF shall explicitly authorise access of ***subjects and/or users*** to objects based on the following additional rules: **none.**
FDP_ACF.1.4/AuditAccess	The TSF shall explicitly deny access of ***subjects and/or users*** to objects based on the following additional rules: **none.**

Application Note: In this SFR the general term "subject" as given in [CC_Part2] is refined to "subjects and/or users".

FDP_ACF.1/AdminAccess	Security attribute based access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/AdminAccess	The TSF shall enforce the **admin access control SFP** to objects based on the following: 1. **Subject and/or users: User trying to gain access to the TOE general configuration** 2. **Object: general TOE configuration** 3. **Security Attributes: user role (notation: user_role).**
FDP_ACF.1.2/AdminAccess	The TSF shall enforce the following rules to determine if an operation among controlled ***subjects and/or users*** and controlled objects is allowed: **operation: read general TOE configuration** **condition: To gain access to the general TOE configuration the following condition must be met:** **user_role = administrator.**
FDP_ACF.1.3/AdminAccess	The TSF shall explicitly authorise access of ***subjects and/or users*** to objects based on the following additional rules: **none.**
FDP_ACF.1.4/AdminAccess	The TSF shall explicitly deny access of ***subjects and/or users*** to objects based on the following additional rules: **none.**

Application Note: In this SFR the general term "subject" as given in [CC_Part2] is refined to "subjects and/or users".

FDP_ACF.1/PolicyAdminAccess	Security attribute based access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/PolicyAdminAccess	The TSF shall enforce the **policy admin access control SFP** to objects based on the following: 1. **Subject and/or users: User trying to gain access to the configuration of TOE functionalities which automatically perform checks regarding the security level of a message.** 2. **Object: TOE parameter of TOE functionalities which automatically perform checks regarding the security level of a message.** 3. **Security Attributes: user role (notation: user_role).**

FDP_ACF.1.2/PolicyAdminAccess	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **operation: read the corresponding TOE parameter** **condition: To gain access to the corresponding TOE parameter the following condition must be met: user_role = policy admin.**
FDP_ACF.1.3/PolicyAdminAccess	The TSF shall explicitly authorise access of ***subjects and/or users*** to objects based on the following additional rules: **none.**
FDP_ACF.1.4/PolicyAdminAccess	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **none.**

Application Note: In this SFR the general term "subject" as given in [CC_Part2] is refined to "subjects and/or users".

FDP_ACF.1/Admin	Security attribute based access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/Admin	The TSF shall enforce the **dual control admin SFP** to objects based on the following: 1. **Subject and/or users: User trying to modify the TOE general configuration** 2. **Object: general TOE configuration** 3. **Security Attributes: user role (notation: user_role).**
FDP_ACF.1.2/Admin	The TSF shall enforce the following rules to determine if an operation among controlled ***subjects and/or users*** and controlled objects is allowed: **operation: modify, add or delete general TOE configuration** **condition: The operation is performed by two different users with user_role = administrator.**
FDP_ACF.1.3/Admin	The TSF shall explicitly authorise access of ***subjects and/or users*** to objects based on the following additional rules: **none.**

FDP_ACF.1.4/Admin	The TSF shall explicitly deny access of ***subjects and/or users*** to objects based on the following additional rules: **none.**

Application Note: In this SFR the general term "subject" as given in [CC_Part2] is refined to "subjects and/or users".

FDP_ACF.1/PolicyAdmin	Security attribute based access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/PolicyAdmin	The TSF shall enforce the **dual control policy admin SFP** to objects based on the following: 1. **Subject and/or users: User having access to change the configuration of TOE functionalities which automatically perform checks regarding the security level of a message.** 2. **Object: TOE parameter of TOE functionalities which automatically perform checks regarding the security level of a message.** 3. **Security Attributes: user role (notation: user_role).**
FDP_ACF.1.2/PolicyAdmin	The TSF shall enforce the following rules to determine if an operation among controlled ***subjects and/or users*** and controlled objects is allowed: **operation: modify, add or delete TOE parameter** **condition: The operation is performed by two different users with user_role = policy admin.**
FDP_ACF.1.3/PolicyAdmin	The TSF shall explicitly authorise access of ***subjects and/or users*** to objects based on the following additional rules: **none.**
FDP_ACF.1.4/PolicyAdmin	The TSF shall explicitly deny access of ***subjects and/or users*** to objects based on the following additional rules: **none.**

Application Note: In this SFR the general term "subject" as given in [CC_Part2] is refined to "subjects and/or users".

FDP_IFC	**Information flow control policy**
FDP_IFC.1/DataToLow	Subset information flow control

Hierarchical to:	No other components.
Dependencies:	FDP_IFF.1 Simple security attributes
FDP_IFC.1.1/DataToLow	The TSF shall enforce the **check label SFP and data to low SFP** on **all data sent from the higher classified network to the lower classified network.**
FDP_IFC.1/PreFilter	Subset information flow control
Hierarchical to:	No other components.
Dependencies:	FDP_IFF.1 Simple security attributes
FDP_IFC.1.1/PreFilter	The TSF shall enforce the **pre-filtering SFP** on **all labelled data sent from the higher classified network to the lower classified network before forwarded to the main filtering component of the TOE.**

Application Note: The main filtering component of the TOE enforces the data to low SFP, i.e. the component implementing FDP_IFC.1.1/DataToLow.

FDP_IFC.1/Supported-Protocol	Subset information flow control
Hierarchical to:	No other components.
Dependencies:	FDP_IFF.1 Simple security attributes
FDP_IFC.1.1/Supported-Protocol	The TSF shall enforce the **supported protocol SFP** on **all protocol data between the higher classified network HIGH and the lower classified network LOW. Hence, in both directions. The TSF shall allow or deny protocols.**
FDP_IFC.1/CleanProtocol	Subset information flow control
Hierarchical to:	No other components.
Dependencies:	FDP_IFF.1 Simple security attributes
FDP_IFC.1.1/CleanProtocol	The TSF shall enforce the **clean protocol SFP** on **all protocol data sent from the higher classified network HIGH to the lower classified network LOW.**
FDP_IFC.1/Validation	Subset information flow control
Hierarchical to:	No other components.
Dependencies:	FDP_IFF.1 Simple security attributes

FDP_IFC.1.1/Validation	The TSF shall enforce the **data validation SFP** on **all unlabelled data sent from the higher classified network to the lower classified network before forwarded to the main filtering component of the TOE.**
FDP_IFF FDP_IFF.1/DataToLow	**Information flow control functions** Simple security attributes
Hierarchical to:	No other components.
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation
FDP_IFF.1.1/DataToLow	The TSF shall enforce the **check label SFP and data to low SFP** based on the following types of ***subjects and/or users*** and information security attributes: **The security attributes for checking security labels are listed in table Table 20 check label SFP. Regarding the security attributes for the security function policy of the information flow for data to be passed to the lower classified network are described in Table 21 data to low SFP.**
FDP_IFF.1.2/DataToLow	The TSF shall permit an information flow between a controlled ***subjects and/or users*** and controlled information via a controlled operation if the following rules hold: **The controlled information flow for checking security labels are listed in table Table 20 check label SFP. Regarding the security attributes for the security function policy of the information flow for data to be passed to the lower classified network are described in Table 21 data to low SFP.**
FDP_IFF.1.3/DataToLow	The TSF shall enforce **the following additional rules:** **If** **security_level_low.CONF not unambigiously determinable (netSPIF LOW not configured)** **or** **data_security_level not unambigiously determinable (malfunction of previous process step)** **Then** **No information flow is permitted**

FDP_IFF.1.4/DataToLow	The TSF shall explicitly authorise an information flow based on the following rules: **none**
FDP_IFF.1.5/DataToLow	The TSF shall explicitly deny an information flow based on the following rules: **If** **data_bandwidth would exceed band_limit.CONF** **or** **mode.CONF = maintenance** **Then** **No information flow is allowed**

Application Note: In this SFR the general term "subject" as given in [CC_Part2] is refined to "subjects and/or users".

FDP_IFF.1/PreFilter	Simple security attributes
Hierarchical to:	No other components.
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation
FDP_IFF.1.1/PreFilter	The TSF shall enforce the **pre-filtering SFP** based on the following types of subject and information security attributes:

Subject	Security Attribute
Pre-filter	data_security_label label_types allowed_attributes.CONF
Information	**Security Attribute**
data_security label	data_security_label.attributes

FDP_IFF.1.2/PreFilter	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **{data_security_label.attributes} ∈ {allowed_attributes.CONF}**

Application Note:

Controlled Subject: Main filtering component of the TOE

Controlled information: all data in a message

Controlled operation: forward controlled information to a controlled subject

FDP_IFF.1.3/PreFilter	The TSF shall enforce the **none.**
FDP_IFF.1.4/PreFilter	The TSF shall explicitly authorise an information flow based on the following rules: **none.**
FDP_IFF.1.5/PreFilter	The TSF shall explicitly deny an information flow based on the following rules: **none.**

Application Note:

Above attributes are related to each other in the following way:

Processing = {automatically, manually}

Origin = {external, internal}

Label_types = processing x origin = {(automatic, external), (automatic, internal), (manual, external)}

data_security_label.attributes = (p, o) ∈ {Label_types}, #p ∈ {processing}, o ∈ {origin}

all_possible.CONF = power set(Label_types) # set of all subsets of Label_ Types

allowed_attributes.CONF ∈ {all_possible.CONF}

FDP_IFF.1/Supported-Protocol	Simple security attributes
Hierarchical to:	No other components.
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation
FDP_IFF.1.1/Supported-Protocol	The TSF shall enforce the **supported protocol SFP** based on the following types of subject and information security attributes:

Subject	**Security Attribute**
next_step.DATA	**-**
Information	**Security Attribute**
data_units.PROTOCOL	**protocol**

FDP_IFF.1.2/Supported-Protocol	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **Operation: Forward data message to next_step.DATA** **Condition: data_units.PROTOCOL ∈ {supported.PROTOCOL}**

Application Note:

{supported.PROTOCOL} := set of communication protocols supported by the TOE.

FDP_IFF.1.3/Supported-Protocol	The TSF shall enforce the **none.**
FDP_IFF.1.4/Supported-Protocol	The TSF shall explicitly authorise an information flow based on the following rules: **none.**
FDP_IFF.1.5/Supported-Protocol	The TSF shall explicitly deny an information flow based on the following rules: **data_units.PROTOCOL ∉{supported.PROTOCOL}.**
FDP_IFF.1/CleanProtocol	Simple security attributes
Hierarchical to:	No other components.
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation
FDP_IFF.1.1/CleanProtocol	The TSF shall enforce the **clean protocol SFP** based on the following types of subject and information security attributes: **Subject** / **Security Attribute** **next_step.DATA** / **-** **Information** / **Security Attribute** **data_units.PROTOCOL** / **protocol** **Protocol data of the protocol data units which are sent from the higher classified network HIGH to the lower classified network LOW.**
FDP_IFF.1.2/CleanProtocol	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **Operation: forward data_units.PROTOCOL to next processing step next_step.DATA.** **Condition: no confidential information in protocol data.**
FDP_IFF.1.3/CleanProtocol	The TSF shall enforce the **none.**
FDP_IFF.1.4/CleanProtocol	The TSF shall explicitly authorise an information flow based on the following rules: **none.**

FDP_IFF.1.5/CleanProtocol	The TSF shall explicitly deny an information flow based on the following rules: **none.**
FDP_IFF.1/Validation	Simple security attributes
Hierarchical to:	No other components.
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation
FDP_IFF.1.1/Validation	The TSF shall enforce the **data validation SFP** based on the following types of subject and information security attributes:

Subject	Security Attribute
Parser process	-
Information	**Security Attribute**
Message	data_label_type label_class_info rule_set_label_class_info data_security_label ICAP_class_info

1. Subject: Internal parser processes of the TOE
2. Information: Message to be validated against a labelled rule set.
3. Security Attributes

   Security label type (data_label_type) of Message to be validated. The classification information (label_class_info) to be stored into the label of Message. (rule_set_label_class_info) contains the classification information stored in the label of the corresponding rule set. If the validation of Message is successful, then either a security label will be attached (data_securety_label) or the classification information of Message is written into the ICAP header (ICAP_class_info) of Message.

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

	data inspection against a labelled rule set describing structure and allowed contents of a message of structured type XML, ADEXP, FSD (like NMEA, Link 16), ASTERIX, FORMDATA or JSON is successful] then (data_label_type = (automatic, internal)[1] and (label_class_info = rule_set_label_class_info[1] or ICAP_class_info = rule_set_label_class_info)))

Application Note:

data_label_type ∈ {(automatic, external), (automatic, internal), (manual, external)}

Controlled subject: Parser process

Controlled information: Message

Operation: attach a security label to received data or store the classification information into the ICAP header of the structured data. If the security label containing the classification information is not needed in the lower classified network LOW the internal and computationally intensive generation of a security label is not necessary. In this case, the TOE can be configured such that the internally determined classification information is stored into the ICAP header of the data, i.e. a security label is not generated for performance reasons.

FDP_IFF.1.3/Validation	The TSF shall enforce the **sanitisation of the representation of the message data.**
FDP_IFF.1.4/Validation	The TSF shall explicitly authorise an information flow based on the following rules: **none.**

[1] Attach a security label

FDP_IFF.1.5/Validation	The TSF shall explicitly deny an information flow based on the following rules: **none.**
FDP_IFF	**Information flow control functions**
FDP_IFF.3	Limited illicit information flows
Hierarchical to:	No other components.
Dependencies:	FDP_IFC.1 Subset information flow control
FDP_IFF.3.1	The TSF shall enforce the **data to low SFP** to limit the capacity of **data flow capability from the higher classified network HIGH to the lower classified network LOW** to a **maximum capacity to be configured by the administrator of the TOE.**

7.1.2 Trusted path/channels (FTP)

FTP_TRP	**Trusted path**
FTP_TRP.1	Trusted path
Hierarchical to:	No other components
Dependencies:	No dependencies
FTP_TRP.1.1	The TSF shall provide a communication path between itself and *local, remote* users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *modification, disclosure.*
FTP_TRP.1.2	The TSF shall permit *local users, remote users* to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for **user authentication, TOE management and audit review.**

Application Note:

The TLS channel is established using the cryptographic library openSSL, see [Crypt_Filter]. The currently used TLS version is TLS 1.2 with the following allowed cipher suits:

- *ECDHE-ECDSA-AES128-GCM-SHA256*
- *ECDHE-ECDSA-AES256-GCM-SHA384*

7.1.3 Identification and authentication (FIA)

FIA_UAU	**User authentication**
FIA_UAU.2	User authentication before any action
Hierarchical to:	FIA_UAU.1 Timing of authentication
Dependencies:	FIA_UID.2 Timing of identification
FIA_UAU.2.1	The TSF shall require each ***privileged*** user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
FIA_UID	**Timing of identification**
FIA_UID.2	Timing of identification
Hierarchical to:	FIA_UID.1 Timing of identification
Dependencies:	No dependencies
FIA_UID.2.1	The TSF shall require each ***privileged*** user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application Note:

This SFR intends to identify the privileged user via the TLS connection to the SDoT Adminstation before the privileged user can take any further TSF mediated action. The SDoT Adminstation is part of the TOE operational environment where the privileged user is authenticated and identified via its smartcard.

7.1.4 Cryptographic support (FCS)

FCS_CKM	**Cryptographic key management**
FCS_CKM.1/ECDSA	Cryptographic key generation
Hierarchical to:	No other components
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.1.1/ECDSA	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **EC key pair**

	generation and specified cryptographic key sizes **256, 384 or 512 Bit** that meet the following: **SP800-56AR3.**
FCS_CKM.2	Cryptographic key distribution
Hierarchical to:	No other components
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation FCS_CKM.4 Cryptographic key destruction]
	The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **ECDHE** that meets the following: **IEEE 1363 (ECKAS-DH1).**
FCS_CKM.4	Cryptographic key destruction
Hierarchical to:	No other components
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **overwriting the key with zeros** that meets the following: **none**.
FCS_COP	**Cryptographic operation**
FCS_COP.1/RSA	Cryptographic operation
Hierarchical to:	No other components
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/RSA	The TSF shall perform **digital signature verification** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **between 2048 Bit and 8192 Bit** that meet the following: **RSASSA PKCS#1 as specified in RFC 3447**.
FCS_COP.1/ECDSA	Cryptographic operation
Hierarchical to:	No other components
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or

	FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/ECDSA	The TSF shall perform **digital signature verification** in accordance with a specified cryptographic algorithm **ECDSA** and cryptographic key sizes **256 Bit, 384 Bit and 512 Bit** that meet the following: **signature verification as specified in ANSI X9.62 with keys based on the ECC domain parameters secp256r1, secp384r1, brainpoolP256r1, brainpoolP384r1, and brainpoolP512r1 with sha2 according to curve size as sub function**.
FCS_COP.1/AES	Cryptographic operation
Hierarchical to:	No other components
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/AES	The TSF shall perform **encryption and decryption** in accordance with a specified cryptographic algorithm **AES in GCM mode** and cryptographic key sizes **128 Bit and 256 Bit** that meet the following: **FIPS 197 and SP800-38D.**
FCS_COP.1/HMAC	Cryptographic operation
Hierarchical to:	No other components
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/HMAC	The TSF shall perform **hash-based message authentication code** in accordance with a specified cryptographic algorithm **HMAC-SHA-384, SHA-256,** and cryptographic key sizes **384 Bit and 256 Bit** that meet the following: **RFC 2104**.
FCS_COP.1/SHA2	Cryptographic operation
Hierarchical to:	No other components
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/SHA2	The TSF shall perform **digest computation** in accordance with a specified cryptographic algorithm **SHA-2** and cryptographic key

	sizes **256 Bit, 384 Bit and 512 Bit** that meet the following: **FIPS 180-4**.

7.1.5 Security management (FMT)

FMT_MSA	**Management of security attributes**
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.1Specification of Management Functions
FMT_MSA.1.1	The TSF shall enforce the **dual control policy admin SFP** to restrict the ability to **query, modify, delete** the security attribute **of the rule set** to **the policy admin.**
FMT_MSA.3	Static attribute initialisation
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 **dual control admin SFP, dual control policy admin SFP, data validation SFP, check label SFP, supported protocol SFP, clean protocol 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~~ **no one** to specify alternative initial values to override the default values when an object or information is created.
FMT_MTD	**Management of TSF data**
FMT_MTD.1/Admin	Management of TSF data
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1/Admin	The TSF shall restrict the ability to *modify* the **general TOE configuration data** to **administrators of the TOE.**
FMT_MTD.1/AuditAccess	Management of TSF data

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1/ AuditAccess	The TSF shall restrict the ability to **access** the **audit trail** to **auditors.**
FMT_MTD.1/AuditDelete	Management of TSF data
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1/ AuditDelete	The TSF shall restrict the ability to **delete or move** the **audit data** to **auditors.**
FMT_MTD.1/PolicyAdmin	Management of TSF data
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1/ PolicyAdmin	The TSF shall restrict the ability to **modify** the **TOE configuration data regarding TOE functionalities which manage the policy of the received data, whether to automatically decide about the security level** to **the policy admins.**
FMT_MTD.3	Secure TSF data
Hierarchical to:	No other components.
Dependencies:	FMT_MTD.1 Management of TSF data
FMT_MTD.3.1	The TSF shall ensure that only secure values are accepted for **the general TOE configuration data.**
FMT_SMF	**Specification of Management Functions**
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:

	The general TOE configuration management: - Define receiver of notifications regarding security events - Enable/disable functionality for automatic labelling - Define the rules which control the pre-filtering operation - Setting of the maximum bandwidth - Define rules for monitoring audited events regarding security violations. Management of TOE parameter - Setting the configuration aspects of TOE functions that perform checks on the security level of a given message, i.e. setting of a rule set. - Show monitoring Status of the TSF Operation mode management: - Change the mode of the TOE from operational to maintenance - Change the mode of the TOE from maintenance to operational Parameter management of the labelling mechanism - Set parameters for the control of the labelling mechanism of the TOE - Communicate with HSM for generation of Keys - Import and export of certificates from, and export of parameters to the HSM Audit functions and audit trail management: - Create audit record archives of the TOE to be able to export the archive.

Application Note:

Management of User IDs, credentials for authentication, authorised user roles are provided by a CA of the TOE environment. Identification and authentication mechanisms for human users are provided by certificates. All human users must verify their identity with a PIN-protected smartcard on the resp. station. User accounts are set by the administrators to get access to TOE functionalities through the station.

FMT_SMR	Security management roles
FMT_SMR.2	Restriction on security roles
Hierarchical to:	FMT_SMR.1 Security roles

Dependencies:	FIA_UID.2 Timing of identification
FMT_SMR.2.1	The TSF shall maintain the roles: **policy-admin, administrator and auditor.**
FMT_SMR.2.2	The TSF shall be able to associate users with roles.
FMT_SMR.2.3	The TSF shall ensure that the conditions **administrator and auditor roles are strictly separated, without** **possibility of simultaneously logged in administrator and auditor user,** are satisfied.

Application Note:

Users are associated to the respective roles with a CA outside the TOE.

7.1.6 Protection of the TSF (FPT)

FPT_STM	**Time stamp**
FPT_STM.1	Reliable time stamps
Hierarchical to:	No other components
Dependencies:	No dependencies
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps.

Application Note:

The reliability is achieved by synchronising with an NTP-Server which is an assumption to the operational environment of the TOE. Nonetheless, the TOE implements the protocol for time synchronisation.

FPT_INC	**TSF integrity checks**
FPT_INC.1	TSF integrity
Hierarchical to:	No other components
Dependencies:	No dependencies
FPT_INC.1.1	The TSF shall run a suite of integrity checks *during initial start-up, periodically during normal operation* to demonstrate the integrity of **general configuration data, rule sets, SPIF, NetSPIF, and stored TSF executable code.**

FPT_INC.1.2	The TSF shall provide authorised users with the capability to verify the integrity of **general configuration data, rule sets, SPIF, and NetSPIF.**
FPT_INC.1.3	The TSF shall provide authorised users with the capability to verify the integrity of **stored TSF executable code.**
FPT_TDC	**Inter-TSF TSF data consistency**
FPT_TDC.1	Inter-TSF basic TSF data consistency
Hierarchical to:	No other components
Dependencies:	No dependencies
FPT_TDC.1.1	The TSF shall provide the capability to consistently interpret **security labels with its classification** when shared between the TSF and another trusted IT product.
FPT_TDC.1.2	The TSF shall use **check label SFP** when interpreting the TSF data from another trusted IT product.

7.1.7 Security audit (FAU)

FAU_ARP	**Security audit automatic response**
FAU_ARP.1	Security alarms
Hierarchical to:	No other components
Dependencies:	FAU_SAA.1 Potential violation analysis
FAU_ARP.1.1	The TSF shall take **the following actions:** - **send an e-mail to a configurable list of recipients** - **report into the audit-trail** - **place an indicator of any potential security violation on the Audit GUI** - **enter the maintenance mode** upon detection of a potential security violation.
FAU_GEN	**Security audit data generation**
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 *not Specified* level of audit; and c) **See Table 26.**
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the ~~PP/~~ST, **the information in Table 26**

Application Note:

For all the auditable events for the basic level of audit, see 8.1.6.1

The following table gives an overview of auditable events and information available in the audit trail.

Auditable events in the TOE	*Available information in audit record*
Changes to the TOE configuration and parameters	*Value of changed TOE configuration and parameter before and after the change was made, i.e.* - *start and stop of the TOEs system* - *change of operation mode* - *administration activities* - *authentication against the TOE*
Processing data messages	*The following audit data are recorded while processing the data of a message:* - *origin,* - *destination,* - *time of transfer,* - *result of the filter decision,* - *the data which can uniquely identify the message.*

Rejecting data messages	*complete data message;* *Note: this is configurable, and the default configuration is "no message data"*

Table 26 auditable events

FAU_GEN.2	User identity association
Hierarchical to:	No other components
Dependencies	FAU_GEN.1 Audit data generation FIA_UID.2 Timing of identification
FAU_GEN.2.1	For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.
FAU_SAA	**Security audit analysis**
FAU_SAA.1	Potential violation analysis
Hierarchical to:	No other components
Dependencies	FAU_GEN.1 Audit data generation
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: a) Accumulation or combination of **auditable events:** **- Underflow of audit storage capacity** **- Exceeding the set bandwidth** **- Upcoming expiration of certificates** **- Errors during self-tests.** known to indicate a potential security violation; b) **none**
FAU_SAR	**Security audit review**
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 **auditors** with the capability to read **all audit information** from the audit records.
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
FAU_SAR.2	Restricted audit review
Hierarchical to:	No other components
Dependencies:	FAU_SAR.1 Audit review
FAU_SAR.2.1	The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read access.
FAU_STG	**Security audit event storage**
FAU_STG.2	Guarantees of audit data availability
Hierarchical to:	FAU_STG.1 Protected audit trail storage
Dependencies:	FAU_GEN.1 Audit data generation
FAU_STG.2.1	The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG.2.2	The TSF shall be able to *prevent* unauthorised modifications to the stored audit records in the audit trail.

Application Note:

The TOE protects the authenticity and integrity of the audit records with an HMAC using sha384 in accordance to RFC 2104.

FAU_STG.2.3	The TSF shall ensure that **all** stored audit records will be maintained when the following conditions occur: *audit storage exhaustion, failure, attack*
FAU_STG.3	Action in case of possible audit data loss
Hierarchical to:	No other components
Dependencies:	FAU_STG.1 Protected audit trail storage
FAU_STG.3.1	The TSF shall **inform a configurable list of recipients (E-Mail Addresses of administrators and auditors) by an alarm message and the auditor by an audit record and an alarm counter on the audit GUI** if the audit trail exceeds **80% of the total capacity of the audit trail storage device.**

FAU_STG.4	Prevention of audit data loss
Hierarchical to:	FAU_STG.3 Action in case of possible audit data loss
Dependencies:	FAU_STG.1 Protected audit trail storage
FAU_STG.4.1	The TSF shall *prevent audited events, except those taken by the authorised user with special rights* and **inform a configurable list of recipients (E-Mail Addresses of administrators and auditors) and preserve a secure state (maintenance mode) which informs the administrator and the auditor by an audit record in which no data is forwarded from network HIGH to network LOW** if the audit trail is full.

7.2 Dependency Rationale

498 The dependency rationale for Security Functional Requirements shows that the basis for mutual
499 support including the internal consistency between in sec. 7.1 defined Security Functional
500 Requirements are satisfied. The following table provides an overview showing that all dependencies
501 between the chosen Security Functional Components are analysed, and non-dissolved
502 dependencies are sufficiently explained.

#	SFR	Dependencies	Support of the Dependencies
1.	FDP_ACC.1	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1
2.	FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	Fulfilled by FDP_ACC.1 Fulfilled by FMT_MSA.3
3.	FDP_IFC.1	FDP_IFF.1 Simple security attributes	Fulfilled by FDP_IFF.1
4.	FDP_IFF.1	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	Fulfilled by FDP_IFC.1 Fulfilled by FMT_MSA.3
5.	FDP_IFF.3	FDP_IFC.1 Subset information flow control	Fulfilled by FDP_IFC.1
6.	FTP_TRP.1	No dependencies	n.a.

#	SFR	Dependencies	Support of the Dependencies
7.	FIA_UAU.2	FIA_UID.1 Timing of identification	Fulfilled by FIA_UID.2 which is hierarchical
8.	FIA_UID.2	No dependencies	n.a.
9.	FCS_CKM.1/ECDSA	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_COP.1/ECDSA and FCS_CKM.4
10.	FCS_CKM.2	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation FCS_CKM.4 Cryptographic key destruction]	Fulfilled by FCS_CKM.1/ECDSA
11.	FCS_CKM.4	[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]	Fulfilled by FCS_CKM.1/ECDSA
12.	FCS_COP.1/RSA	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Fulfilled by the HSM in the operational environment. The HSM securely generates the RSA key pair.
13.	FCS_COP.1/AES	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Fulfilled by the HSM in the operational environment. The HSM provides the AES key used by the TOE for Audit data encryption.

#	SFR	Dependencies	Support of the Dependencies
14.	FCS_COP.1/ECDSA	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_CKM.1/ECDSA and FCS_CKM.4
15.	FCS_COP.1/HMAC	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Fulfilled by the HSM in the operational environment which provides the key for the HMAC calculation for the Audit trail.
16.	FCS_COP.1/SHA2	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	n.a.
17.	FMT_MSA.1	[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	[Fulfilled by FDP_ACC.1 and FDP_IFC.1] Fulfilled by FMT_SMR.2 which is hierarchical to FMT_SMR.1 Fulfilled by FMT_SMF.1
18.	FMT_MSA.3	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	Fulfilled by FMT_MSA.1 Fulfilled by FMT_SMR.2 which is hierarchical to FMT_SMR.1

#	SFR	Dependencies	Support of the Dependencies
19.	FMT_MTD.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	Fulfilled by FMT_SMR.2 which is hierarchical to FMT_SMR.1 Fulfilled by FMT_SMF.1
20.	FMT_MTD.3	FMT_MTD.1 Management of TSF data	Fulfilled by FMT_MTD.1
21.	FMT_SMF.1	No dependencies	n.a.
22.	FMT_SMR.2	FIA_UID.2 Timing of identification	Fulfilled by FIA_UID.2
23.	FPT_STM.1	No dependencies	n.a.
24.	FPT_INC.1	No dependencies	n.a.
25.	FPT_TDC.1	No dependencies	n.a.
26.	FAU_ARP.1	FAU_SAA.1 Potential violation analysis	Fulfilled by FAU_SAA.1
27.	FAU_GEN.1	FPT_STM.1 Reliable time stamps	Fulfilled by FPT_STM.1
28.	FAU_GEN.2	FAU_GEN.1 Audit data generation FIA_UID.2 Timing of identification	Fulfilled by FAU_GEN.1 Fulfilled by FIA_UID.2
29.	FAU_SAA.1	FAU_GEN.1 Audit data generation	Fulfilled by FAU_GEN.1
30.	FAU_SAR.1	FAU_GEN.1 Audit data generation	Fulfilled by FAU_GEN.1
31.	FAU_SAR.2	FAU_SAR.1 Audit review	Fulfilled by FAU_SAR.1
32.	FAU_STG.2	FAU_GEN.1 Audit data generation	Fulfilled by FAU_GEN.1

#	SFR	Dependencies	Support of the Dependencies
33.	FAU_STG.3	FAU_STG.1 Protected audit trail storage	Fulfilled by FAU_STG.2 which is hierarchical to FAU_STG.1
34.	FAU_STG.4	FAU_STG.3 Action in case of possible audit data loss FAU_STG.1 Protected audit trail storage	Fulfilled by FAU_STG.3 Fulfilled by FAU_STG.2 which is hierarchical to FAU_STG.1

Table 27 Dependencies between the Security Functional Requirements (SFRs) for the TOE

7.3 Security assurance requirements rationale

503 The assurance level for evaluation of the TOE, its life cycle and operating environment are chosen
504 as the pre-defined assurance level EAL4 augmented with the following assurance component in
505 accordance with [CC_Part3]:

506 • ALC_FLR.2 Flaw reporting procedures.

507 • AVA_VAN.5 Advanced methodical vulnerability analysis

508 This corresponds to a total assurance level EAL4+.
509 The Level EAL4 augmented with ALC_FLR.2 and AVA_VAN.5 was chosen to permit INFODAS GmbH
510 as a developer to gain maximum assurance from positive security engineering based on good
511 commercial development practices which, though rigorous, do not require substantial specialist
512 knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be
513 economically to retrofit the existing product line of INFODAS GmbH.
514 The selection of the component ACL_FLR.2 provides additional assurance of the TOE that potential
515 security flaws can be tracked and corrected by the developer. Further, the selection of AVA_VAN.5
516 provides more confidence that the TOE can resist even higher attack potential than is actually
517 required by EAL 4.
518 Augmented assurance components are marked in **bold** in the following table:

Assurance class	Assurance Family	Assurance Component
Development	ADV_ARC	ADV_ARC.1 Security architecture description
	ADV_FSP	ADF_FSP.4 Complete functional specification
	ADV_IMP	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS	ADV_TDS.3 Basic modular design
	AGD_OPE	AGD_OPE.1 Operational user guidance

Guidance documents	AGD_PRE	AGD_PRE.1 Preparative procedures
Life-cycle support	ALC_CMC	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL	ALC_DEL.1 Delivery procedures
	ALC_DVS	ALC_DVS.1 Identification of security measures
	ALC_FLR	**ALC_FLR.2 Flaw reporting procedures**
	ALC_LCD	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT	ALC_TAT.1 Well-defined development tools
Security target evaluation	ASE_CCL	ASE_CCL.1 Conformance claims
	ASE_ECD	ASE_ECD.1 Extended components definition
	ASE_INT	ASE_INT.1 ST introduction
	ASE_OBJ	ASE_OBJ.2 Security objectives
	ASE_REQ	ASE_REQ.2 Derived security requirements
	ASE_SPD	ASE_SPD.1 Security problem definition
	ASE_TSS	ASE_TSS.1 TOE summary specification
Tests	ATE_COV	ATE_COV.2 Analysis of coverage
	ATE_DPT	ATE_DPT.1 Testing: basic design
	ATE_FUN	ATE_FUN.1 Functional testing
	ATE_IND	ATE_IND.2 Independent testing – sample
Vulnerability assessment	**AVA_VAN**	**AVA_VAN.5 Advanced methodical vulnerability analysis**

Table 28 Security Assurance Requirements (SARs)

7.4 Security Functional Requirements Rationale

519 The following subsections provide an overview regarding the coverage of Security Objectives for the TOE by Security Functional Requirements and a rational of the
520 chosen Security Assurance Requirements. The following table shows an overview for the tracing of SFRs back to the security objectives for the TOE.

SFRs	OT.FILTER	OT.PRE_FILTER	OT.LABELS	OT.PROTOCOLS	OT.SANITISED_DATA	OT.BANDWIDTH	OT.PROTOCOL_DENY	OT.USER_AUTHENTICATION	OT.ROLE_SEPARATION	OT.FOUR_EYES	OT.SECURE_CHANNEL	OT.AUDIT_CHANGE_LOG	OT.AUDIT	OT.AUDIT_PROTECT	OT.AUDIT_LOG_AVAILABILITY	OT.PROTECTION	OT.INIT	OT.DEFAULT	OT.WARNING
FDP_ACC.1/AuditAccess									x						x	x			
FDP_ACC.1/AdminAccess									x										
FDP_ACC.1/PolicyAdmin Access									x										
FDP_ACC.1/Admin										x									
FDP_ACC.1/PolicyAdmin										x									
FDP_ACF.1/AuditAccess									x						x	x			
FDP_ACF.1/AdminAccess									x										
FDP_ACF.1/PolicyAdmin Access									x										
FDP_ACF.1/Admin										x									
FDP_ACF.1/PolicyAdmin										x									
FDP_IFC.1/DataToLow	x		x						x								x		
FDP_IFC.1/PreFilter		x																	
FDP_IFC.1/Supported-Protocol				x			x												
FDP_IFC.1/CleanProtocol					x														

SFRs	OT.FILTER	OT.PRE_FILTER	OT.LABELS	OT.PROTOCOLS	OT.SANITISED_DATA	OT.BANDWIDTH	OT.PROTOCOL_DENY	OT.USER_AUTHENTICATION	OT.ROLE_SEPARATION	OT.FOUR_EYES	OT.SECURE_CHANNEL	OT.AUDIT_CHANGE_LOG	OT.AUDIT	OT.AUDIT_PROTECT	OT.AUDIT_LOG_AVAILABILITY	OT.PROTECTION	OT.INIT	OT.DEFAULT	OT.WARNING
FDP_IFC.1/Validation			x																
FDP_IFF.1/DataToLow	x		x			x			x								x		
FDP_IFF.1/PreFilter		x																	
FDP_IFF.1/Supported-Protocol				x			x												
FDP_IFF.1/CleanProtocol					x														
FDP_IFF.1/Validation			x																
FDP_IFF.3						x													
FTP_TRP.1											x								
FIA_UAU.2								x											
FIA_UID.2								x											
FCS_CKM.1/ECDSA											x								
FCS_CKM.2											x								
FCS_CKM.4											x								
FCS_COP.1/RSA			x								x								
FCS_COP.1/ECDSA			x								x								
FCS_COP.1/AES											x			x					
FCS_COP.1/HMAC														x					
FCS_COP.1/SHA2			x								x			x					
FMT_MSA.1			x																
FMT_MSA.3																		x	
FMT_MTD.1/Admin										x									

SFRs	OT.FILTER	OT.PRE_FILTER	OT.LABELS	OT.PROTOCOLS	OT.SANITISED_DATA	OT.BANDWIDTH	OT.PROTOCOL_DENY	OT.USER_AUTHENTICATION	OT.ROLE_SEPARATION	OT.FOUR_EYES	OT.SECURE_CHANNEL	OT.AUDIT_CHANGE_LOG	OT.AUDIT	OT.AUDIT_PROTECT	OT.AUDIT_LOG_AVAILABILITY	OT.PROTECTION	OT.INIT	OT.DEFAULT	OT.WARNING
FMT_MTD.1/AuditAccess									x										
FMT_MTD.1/AuditDelete									x					x					
FMT_MTD.1/PolicyAdmin										x									
FMT_MTD.3																x			
FMT_SMF.1		x	x			x			x							x			x
FMT_SMR.2									x										
FPT_STM.1												x	x						
FPT_INC.1																x			
FPT_TDC.1	x																		
FAU_ARP.1																	x		x
FAU_GEN.1												x	x						
FAU_GEN.2												x	x						
FAU_SAA.1																			x
FAU_SAR.1															x				
FAU_SAR.2									x						x				
FAU_STG.2														x					
FAU_STG.3														x					
FAU_STG.4														x					

Table 29 Coverage of the Security Objectives for the TOE by SFRs

7.4.1 OT.FILTER

OT.FILTER is fulfilled by FDP_IFC.1/DataToLow and FDP_IFF.1/DataToLow. These SFRs make sure that only data which comply to the data to low SFP are possible to be sent from the higher classified network to the lower classified network. Further, FPT_TDC.1 ensures the consistent interpretation of security labels sent between the TOE and other trusted IT systems.

7.4.2 OT.PRE_FILTER

The security objective OT.PRE_FILTER are addressed by FDP_IFC.1/PreFilter, FDP_IFF.1/PreFilter which enforce the pre-filtering SFP and assure that only message data corresponding to configurable pre-conditions are forwarded to the main filtering component of the TOE. FMT_SMF.1 provides administrators to configure the pre-filtering conditions used by OT.PRE_FILTER.

7.4.3 OT.LABELS

FDP_IFC.1/Validation and FDP_IFF.1/Validation ensure that the TOE checks the strong bound of a security label to the corresponding message data. FDP_IFC.1/Validationand FDP_IFF.1/Validation provide the test strategy which must be performed before a security label is attached to the data. FMT_MSA.1 provides a restriction regarding the manual labelling mechanism. FMT_SMF.1 ensures that configuration mechanisms to set the rules for automatic labelling of the TOE are provided.

FDP_IFC.1/DataToLow and FDP_IFF.1/DataToLow address the security objective for the TOE by ensuring that security labels are not considered as such, if the security label was not generated by an authorised user; if the categorisation respectively the level of security cannot be unambiguously identified by the TOE; and if the TOE is not able to determine whether the categorisation of the security label was decided manually or automatically. Further, FDP_IFC.1/DataToLow and FDP_IFF.1/DataToLow are responsible to ensure that the security label has a strong bond to the corresponding data, resp. decide which user can perform an import of a security label.

FCS_COP.1/RSA, FCS_COP.1/ECDSA and FCS_COP.1/SHA2 provide the cryptographic operation for checking the security label whether it corresponds to OT.LABELS.

7.4.4 OT.SANITISED_DATA

FDP_IFC.1/CleanProtocol and FDP_IFF.1/CleanProtocol are addressing OT.SANITISED_DATA by enforcing the TOE to apply clean protocol SFP, and assure that data which is categorised to be confidential, is not sent to the lower classified network.

Further, OT.SANITISED_DATA is addressed by FDP_IFC.1/Validation and FDP_IFF.1/Validation by enforcing the data validation SFP, which controls the internal parser process of the TOE.

7.4.5 OT.BANDWIDTH

This security objective is directly required to be fulfilled by FDP_IFF.3 and FDP_IFF.1/DataToLow. Further, FMT_SMF.1 directly requires the TOE to provide mechanisms to set up the bandwidth limits.

7.4.6 OT.PROTOCOLS

The objective OT.PROTOCOLS addresses those communication protocols which must be supported by the TSF. No other protocols than those listed by OT.PROTOCOLS shall be supported. This will be

ensured by the TSF according to the SFRs FDP_IFC.1/Supported-Protocol and FDP_IFF.1/Supported-Protocol.

7.4.7 OT.PROTOCOL_DENY

The security objective to the TOE OT.PROTOCOL_DENY requires the TOE to not accept all types of protocol communication which do not comply with protocols listed in OT.PROTOCOLS.

FDP_IFC.1/Supported-Protocol and FDP_IFF.1/Supported-Protocol enforces the supported protocol SFP to ensure that all attempts to build up a connection with different protocol types other than listed in OT.PROTOCOLS will be denied by the TSF.

7.4.8 OT.USER_AUTHENTICATION

The security objective OT.USER_AUTHENTICATION aims to ensure that all users of the TOE are authenticated before any other action can be performed.

This objective is mainly achieved by FIA_UID.2 and FIA_UAU.2 which require that all users are identified and authenticated considering the application note in FIA_UID.2.

7.4.9 OT.ROLE_SEPARATION

The security objective OT.ROLE_SEPARATION aims to ensure that the TOE is able to separate the role of all administrators and auditor or the TOE. This is achieved by the following SFRs:

FMT_SMR.2 assures that the roles of policy-admin, administrator and auditor are separated and there is no possibility of simultaneous log-in. FMT_SMF.1 provides functionalities which give access to general configuration of user IDs, credentials for authentication and authorised user roles.

FMT_MTD.1/AuditAccess, FMT_MTD.1/AuditDelete, FDP_ACF.1/AuditAccess, FDP_ACC.1/AuditAccess with FAU_SAR.2 achieve the security objective by assuring that only the role of the auditor is able to read or delete audit records from the audit trail.

FMT_MTD.1/Admin, FMT_MTD.1/PolicyAdmin, FDP_ACC.1/Admin, FDP_ACF.1/Admin, FDP_ACC.1/PolicyAdmin, FDP_ACF.1/PolicyAdmin, FDP_ACC.1/AdminAccess, FDP_ACF.1/AdminAccess, FDP_ACC.1/PolicyAdminAccess, and FDP_ACF.1/PolicyAdminAccess achieve the security objective by assuring that only the role of the respective policy-/administrator is able to read or delete/modify rule sets/general TOE configuration data.

7.4.10 OT.FOUR_EYES

This objective is achieved by the combination FDP_ACF.1/Admin and FDP_ACC.1/Admin resp. FDP_ACF.1/PolicyAdmin and FDP_ACC.1/PolicyAdmin. Beforementioned SFRs ensure that the dual control admin SFP, dual control policy admin SFP, FDP_ACC.1/AdminAccess, FDP_ACF.1/AdminAccess, FDP_ACC.1/PolicyAdminAccess, and FDP_ACF.1/PolicyAdminAccess are enforced by the TOE.

FMT_MTD.1/Admin and FMT_MTD.1/PolicyAdmin that only the administrator resp. the policy-admin can make the corresponding change.

7.4.11 OT.SECURE_CHANNEL

This objective aims that the TOE can establish a secure communication channel and is directly addressed by FTP_TRP.1.

FCS_CKM.1/ECDSA addresses the provision cryptographic keys used by the secure channel while FCS_CKM.2 provides the key distribution method used by the TOE. FCS_CKM.4 ensures that keys are zeroized when no longer needed. FCS_COP.1/ECDSA, FCS_COP.1/RSA, FCS_COP.1/AES and FCS_COP.1/SHA2 provide the cryptographic algorithms used for establishing the TLS connection.

7.4.12 OT.AUDIT_CHANGE_LOG

This security objective aims that the TOE logs all changes to configuration data where the auditor can track all changes and identify the user. FAU_GEN.1 is achieving this objective by requiring the TOE to provide audit records for all changes made on the TOE configuration with time data and user data. FAU_GEN.2 ensures that each individual user who made any change is tracked. FPT_STM.1 ensures that the TOE obtains reliable time stamps which added to the audit record.

7.4.13 OT.AUDIT

The security objective aims that the TOE can track all message data transferred from the network HIGH to network LOW and keep the information in an audit trail. The data which were rejected to be forwarded to network LOW shall be stored for later investigation purposes. FAU_GEN.1 directly addresses this security objective by requiring the TOE to log all messages and corresponding metadata as identified in Table 26. FAU_GEN.2 ensures that each individual user who made any change is tracked. FPT_STM.1 ensures that the TOE obtains reliable time stamps which added to the audit record.

7.4.14 OT.AUDIT_PROTECT

This security objective is achieved by FMT_MTD.1/AuditDelete which ensures that only the auditor can delete or move audit records from the audit trail. FAU_STG.2 provides the protection of stored audit records from modification and from unauthorised removal from the audit trail. Further, FAU_STG.2 requires that stored audit records are maintained if the audit storage is full or a failure of the storage occurs.

FCS_COP.1/HMAC and FCS_COP.1/AES address the cryptographic algorithms used to protect the integrity and confidentiality of the audit records.

FAU_STG.3 and FAU_STG.4 reduce the risk of losing audit records by providing alerting mechanisms to be able to detect exhaustions of the storage.

7.4.15 OT.AUDIT_LOG_AVAILABILITY

This security objective aims to provide the audit data to authorised auditors. This is achieved by FDP_ACC.1/AuditAccess and FDP_ACF.1/AuditAccess which require that only auditors have access to audit records. Further, FAU_SAR.1 requires that the TOE provides mechanisms that auditors can read the audit records and FAU_SAR.2 ensures that only users who have been granted access have read access to the records.

7.4.16 OT.PROTECTION

The security objective OT.PROTECTION aims that the TOE protects its own configuration data against attempts of bypassing , deactivating or manipulating the configuration data. This objective is addressed by several SRFs. The combination of these SFRs ensures that this objective is achieved.

FPT_INC.1 provides mechanisms to perform integrity checks and detect malicious code or misconfigured TOE configuration.

FMT_SMF.1 ensures that management functions are provided to set the TOE into maintenance mode/operational mode.

FDP_ACF.1/Admin and FDP_ACC.1/Admin, together, assure that any change to general configuration parameter has to be done by two administrators with dual control technique. In addition, FMT_MTD.3 ensures that only secure values are accepted for general TOE configuration data.

7.4.17 OT.INIT

OT.INIT has the objective that after initialisation process the TOE is constantly in a secure state. The SFRs FDP_IFC.1/DataToLow and FDP_IFF.1/DataToLow fulfil this objective by enforcing the data to low SFP. FAU_ARP.1, enables the TOE to detect potential insecure states, and if so, enter the maintenance mode.

7.4.18 OT.DEFAULT

This security objective for the TOE has the intention of achieving that all default settings of all configurable items of the TOE are always set to a secure state. The SFR FMT_MSA.3 implements the security objective by requiring that the TSF enforces all defined SFPs to provide restrictive default values for security attributes that are used to enforce the respective SFP. Further, no user can specify alternative values to replace the default values by creating an object or information.

7.4.19 OT.WARNING

The objective of OT.WARNING is that when a security relevant event was detected, the TSF sends warnings to the user. FAU_SAA.1 and FAU_ARP.1 assure that the TSF monitors audited events in accordance with the defined set of rules. The auditor will be informed when potential security violating acts were monitored. FMT_SMF.1 assures the configuration capability of the addressees of the warning notification.

8 TOE Summary Specification (ASE_TSS.1)

This section describes the security mechanisms of the TOE and how these meet the SFRs.

8.1 TOE Security Functions

8.1.1 SF_LBL: Labelling Mechanism

The TOE provides mechanisms to perform labelling tasks. The following describes the main security properties of SF_LBL.

8.1.1.1 SF_LBL.1

The TOE enforces data validation SFP on all data which have to be labelled by the TOE. The TOE performs a syntax analysis on incoming structured data. The generated security label is of the type (automatic, internal) as required by FDP_IFF.1/Validation.

Only supported structures of the data will be processed by the H2L SchemaValidator respectively the L2H SchemaValidator. The supported formats are XML, ADEXP, FSD, ASTERIX, FORMDATA, and JSON. All other formats will be rejected by the TOE.

8.1.1.2 SF_LBL.2

The security labels have a strong binding to the corresponding data. Any modification of the data or the related security label will invalidate both data and security label. This will lead to a rejection and the data will not pass the TOE. This feature is achieved with XML signatures which are following strict rules in terms of syntax and processing mechanisms, see [XML_SYN].The structure of the security label is based on the NATO standard (see [ADaTP_4774], [ADaTP_4778]).

8.1.1.3 SF_LBL.3

The TOE provides configuration mechanisms to define the parameters regarding the automatic labelling of the message data, in the case where a labelling generation is initiated by the TOE, with cryptographic support of the HSM. The HSM is part of the delivery of the SDoT Security Gateway but resides outside of the TOE. The verification of security labels is performed by the TOE.

8.1.1.4 SFRs addressed by SF_LBL

The security function SF_LBL addresses the requirements of the following SFRs: FDP_IFF.1/Validation Subset access control, FDP_IFC.1/DataToLow Subset information flow control, FDP_IFF.1/DataToLow Simple security attributes , FDP_IFF.1/Validation Security attribute based access control, Security attribute based access control, FMT_SMF.1 Specification of Management Functions, FCS_COP.1/ECDSA, FCS_COP.1/RSA and FCS_COP.1/SHA2.

8.1.2 SF_FR: Filtering Mechanism

The TOE provides filtering mechanisms which is the main security functionality of the TOE. The following subsections will describe the main security properties of SF_FR.

8.1.2.1 SF_FR.1

The TOE enforces the data to low SFP for all data messages which is sent from the higher classified network to the lower classified network. The main filtering mechanism of the TOE forwards incoming data messages from the higher classified network based on the classification of the data.

8.1.2.2 SF_FR.2

The TOE enforces the pre-filtering SFP for all data messages before the data is forwarded to the main filtering component of the TOE.

8.1.2.3 SF_FR.3

The TOE enforces the supported protocol SFP for all protocol data units between the higher classified network and the lower classified network for both directions. In accordance with FDP_IFF.1/Supported-Protocol the only supported communication protocols are the following: SMTP, HTTP, UDP, and TCP.

8.1.2.4 SF_FR.4

If the TOE is in maintenance mode, all incoming message data will be blocked resp. cannot pass the filtering component of the TOE. The auditing and logging functionalities are not affected during the maintenance mode.

8.1.2.5 SF_FR.5

There is no confidential information stored longer than needed in the memory. The memory is zeroised after the message data and all security critical data was processed by the TOE.

8.1.2.6 SF_FR.6

The TOE provides mechanisms to consistently interpret security labels regarding the security categorisation of the labels which are shared between the TOE and other trusted IT-Systems of the operational environment of the TOE. All security labels which do not have a known structure or any other unknown attribute with regards to the security classification are rejected by the TOE.

8.1.2.7 SFRs addressed by SF_FR

The security function SF_FR addresses the requirements of the following SFRs: FDP_IFC.1/DataToLow Subset information flow control, FDP_IFC.1/PreFilter Subset information flow control, FDP_IFC.1/Supported-Protocol Subset information flow control, FDP_IFF.1/DataToLow Simple security attributes, FMT_SMF.1 Specification of Management Functions, FDP_IFF.1/PreFilter Simple security attributes, FPT_TDC.1 Inter-TSF basic TSF data consistency, and FDP_IFF.1/Supported-Protocol Simple security attributes.

8.1.3 SF_CP: Channel Protection

The TOE supports several mechanisms to provide security functionalities related to covert channel protection. The following security properties of the TOE are included:

8.1.3.1 SF_CP.1

The TOE enforces the clean protocol SFP on all protocol data units which are sent from network HIGH to the lower classified network. Only if the protocol data does not contain confidential information, the TOE will forward then the data between the differently classified networks.

8.1.3.2 SF_CP.2

The TOE controls the bandwidth which can be configured by the operator of the TOE. The TOE will then block all incoming and outgoing connections, if these exceed the configured bandwidth. The TOE can limit the capacity of information flow from the higher classified network to the network LOW.

8.1.3.3 SFRs addressed by SF_CP

The security function SF_CP addresses the requirements of the following SFRs:
FDP_IFC.1/CleanProtocol Subset information flow control, FDP_IFF.1/DataToLow Simple security attributes, FDP_IFF.1/CleanProtocol Simple security attributes, FDP_IFF.1/CleanProtocol Subset information flow control, FDP_IFF.3 Limited illicit information flows, and FMT_SMF.1 Specification of Management Functions.

8.1.4 SF_DP: Data Protection

The TOE includes the following security functions to provide data protection mechanisms.

The TOE enforces check label SFP on all data messages with attached external security labels. In a first step security labels are extracted from the data message for all data coming from the higher classified network.

8.1.4.1 SFRs addressed by SF_DP

The security function SF_DP addresses the requirements of the following SFRs:
FDP_IFC.1/DataToLow Subset information flow control, FDP_IFF.1/DataToLow Simple security attributes

8.1.5 SF_AA: Authentication and Authorisation

The TOE includes security functionalities to provide authentication and authorisation mechanisms which addresses the related SFRs. The TOE supports a secure channel initiated by the SDoT Adminstation within a dedicated network.

Only users which have the explicit permission to read the audit records of the TOE have access to the audit records. Only the user with the user role "Auditor" can access the GUI for auditing purposes. After successful identification and authentication of the auditor, the GUI grants access to the audit functionalities. The TOE enforces the audit access control SFP on all users trying to have access to the audit trail and the auditing functionalities of the TOE.

Likewise, the TOE enforces the dual control admin SFP for all users trying to modify the general TOE configuration. In this context, the TOE enforces the dual control policy admin SFP for all users trying to change the TOE configuration regarding the TOE functionalities for automatically deciding about the security level of a given message data.

The TOE enforces that only the role of the auditor can read, move or delete audit records from the audit trail of the TOE. The TOE enforces that only two different administrators can make changes to the TOE configuration. One administrator temporarily stores the configuration data regarding any modification of configuration parameters of the TOE. Afterwards, a different administrator must confirm or reject the proposed changes. The changes will only apply, if the second administrator has confirmed the proposed modification of configuration data by the first administrator.

The same procedure applies to the role of the policy-admin where the TOE enforces the dual control policy admin SFP.

8.1.5.1 SFRs addressed by SF_AA

FAU_SAR.2 Restricted audit review, FDP_ACC.1/AuditAccess Subset access control, FDP_ACC.1/Admin Subset access control, FDP_ACC.1/PolicyAdmin Subset access control, FDP_ACC.1/AdminAccess Subset access control, FDP_ACC.1/PolicyAdminAccess Subset access control, FDP_ACF.1/AuditAccess Security attribute based access control, FDP_ACF.1/AdminAccess Security attribute based access control, FDP_ACF.1/PolicyAdminAccess Security attribute based access control, FDP_ACF.1/Admin Security attribute based access control, FDP_ACF.1/PolicyAdmin Security attribute based access control, FDP_IFF.1/DataToLow Simple security attributes, FIA_UAU.2 User authentication before any action, FIA_UID.2 Timing of identification, FMT_MSA.1, Management of security attributes, FMT_MTD.1/Admin Management of TSF data, FMT_MTD.1/AuditAccess Management of TSF data, FMT_MTD.1/AuditDelete Management of TSF data, FMT_MTD.1/PolicyAdmin Management of TSF data, FMT_SMF.1 Specification of Management Functions, FTP_TRP.1 Trusted path , FMT_SMR.2 Restriction on security roles, FTP_TRP.1Trusted Path FCS_CKM.1/ECDSA, , FCS_COP.1/AES, FCS_COP.1/ECDSA, and FCS_COP.1/SHA2.

8.1.6 SF_AT: Audit Trail

The TOE includes security functionalities to meet the requirements addressed in the related SFRs as listed in 8.1.6.2.

Upon detection of a potential security violation the TOE takes the following actions:

a. The TOE sends an e-mail to a configurable list of addressees

b. Generates an audit entry into the audit trail

c. Indicates the potential security violation on the audit GUI

For each auditable event resulting from an action of the authenticated human user, the TOE associates the audit record unambiguously with the user role who performed any auditable action. The TOE stores the DN of the certificate of the user role who caused the auditable event.

8.1.6.1 Auditable Events

In the following, the main auditable events are listed.

- Not available in ST-Lite Version

8.1.6.2 SFRs addressed by SF_AT

FAU_ARP.1 Security audit automatic response, FAU_GEN.1 Audit data generation, FAU_GEN.2 User identity association, FAU_SAA.1 Potential violation analysis, FAU_SAR.1 Audit review, FAU_SAR.2 Restricted audit review, FAU_STG.2 Guarantees of audit data availability, FAU_STG.3 Action in case of possible audit data loss, FAU_STG.4 Prevention of audit data loss, FDP_ACC.1/AuditAccess Subset access control, FDP_IFF.1/DataToLow Simple security attributes, FDP_IFF.3 Limited illicit information flows, FIA_UAU.2 User authentication before any action, FIA_UID.2 Timing of identification, FMT_MSA.1 Management of security attributes, FMT_MSA.3 Static attribute initialisation, FMT_MTD.1/AuditAccess, Management of TSF data, FMT_MTD.1/AuditDelete, Management of TSF data, FMT_SMF.1 Specification of Management Functions, FMT_SMR.2 Restriction on security roles, FPT_STM.1 Reliable time stamps, FCS_COP.1/HMAC, FCS_COP.1/SHA2 and FCS_COP.1/AES.

8.1.7 SF_SP: Self Protection

The TOE includes several functionalities to provide self-protection mechanisms. The TOE enforces the policy dual control admin SFP on all users attempting to change the general TOE configuration The TOE enforces that two different users of role administrator are required to be able to change (modify, insert, delete) the general TOE configuration.

The TOE ensures that no message flow from HIGH to LOW network is possible in maintenance mode. The TOE provides restrictive default values for the following security attributes that are used to enforce the SFPs:

- parameters of the general TOE configuration
- the part of the TOE configuration that determines what types of security labels are allowed
- rule sets for automatic data inspection
- valid classifications, valid categories, invalid combinations between classifications and categories within the policy (SPIF)
- permissible classifications and categories which can pass the filtering mechanisms of the TOE towards the lower classified network (NetSPIF)

The default values of these security attributes are set during the installation phase. In this phase, it is not possible to change the default values.

The TOE preserves the secure state, by switching into maintenance mode, when the following types of failures occur:

- software failure
- hardware failure
- power outage
- out of memory error
- audit trail full

8.1.7.1 SFRs addressed by SF_SP

FDP_ACC.1/Admin Subset access control, FDP_ACF.1/Admin Security attribute based access control, FDP_IFF.1/DataToLow Simple security attributes, FMT_MSA.3 Static attribute initialisation, FMT_MTD.1/Admin Management of TSF data, FPT_INC.1 TSF integrity, FMT_MTD.3 Secure TSF data, and FMT_SMF.1 Specification of Management Functions.

8.2 TOE Summary Specification Rationale

The following table provides an overview of the demonstration in 8.1 regarding the coverage of the SFRs by the TSFs.

#	SFRs	TSFs
1.	FDP_ACC.1/AuditAccess	SF_AA
2.	FDP_ACC.1/Admin	SF_AA, SF_SP
3.	FDP_ACC.1/PolicyAdmin	SF_AA
4.	FDP_ACC.1/AdminAccess	SF_AA,
5.	FDP_ACC.1/PolicyAdminAccess	SF_AA,
6.	FDP_ACF.1/AuditAccess	SF_AA
7.	FDP_ACF.1/Admin	SF_AA, SF_SP
8.	FDP_ACF.1/PolicyAdmin	SF_AA
9.	FDP_ACF.1/AdminAccess	SF_AA,
10.	FDP_ACF.1/PolicyAdminAccess	SF_AA,
11.	FDP_IFC.1/DataToLow	SF_FR, SF_LBL, SF_DP
12.	FDP_IFC.1/PreFilter	SF_FR
13.	FDP_IFC.1/Supported-Protocol	SF_FR
14.	FDP_IFC.1/CleanProtocol	SF_CP
15.	FDP_IFC.1/Validation	SF_LBL
16.	FDP_IFF.1/DataToLow	SF_FR, SF_CP, SF_AA, SF_SP, SF_LBL, SF_DP
17.	FDP_IFF.1/PreFilter	SF_FR
18.	FDP_IFF.1/Supported-Protocol	SF_FR
19.	FDP_IFF.1/CleanProtocol	SF_CP
20.	FDP_IFF.1/Validation	SF_LBL
21.	FDP_IFF.3	SF_CP, SF_AT
22.	FTP_TRP.1	SF_AA
23.	FIA_UAU.2	SF_AA, SF_AT
24.	FIA_UID.2	SF_AA, SF_AT
25.	FCS_CKM.1/ECDSA	SF_AA
26.	FCS_CKM.4	SF_AA
27.	FCS_CKM.2	SF_AA
28.	FCS_COP.1/AES	SF_AA, SF_AT
29.	FCS_COP.1/ECDSA	SF_LBL, SF_AA
30.	FCS_COP.1/HMAC	SF_AT
31.	FCS_COP.1/RSA	SF_LBL
32.	FCS_COP.1/SHA2	SF_LBL, SF_AA, SF_AT
33.	FMT_MSA.1	SF_AA, SF_AT
34.	FMT_MSA.3	SF_SP, SF_AA
35.	FMT_MTD.1/Admin	SF_AA, SF_SP
36.	FMT_MTD.1/AuditAccess	SF_AA
37.	FMT_MTD.1/AuditDelete	SF_AA
38.	FMT_MTD.1/PolicyAdmin	SF_AA

39.	FMT_MTD.3	SF_SP
40.	FMT_SMF.1	SF_LBL, SF_FR, SF_CP, SF_AA, SF_AT, , SF_SP
41.	FMT_SMR.2	SF_AA
42.	FPT_STM.1	SF_AT
43.	FPT_INC.1	SF_SP
44.	FPT_TDC.1	SF_FR
45.	FAU_ARP.1	SF_AT
46.	FAU_GEN.1	SF_AT
47.	FAU_GEN.2	SF_AT
48.	FAU_SAA.1	SF_AT
49.	FAU_SAR.1	SF_AT
50.	FAU_SAR.2	SF_AA, SF_AT
51.	FAU_STG.2	SF_AT
52.	FAU_STG.3	SF_AT
53.	FAU_STG.4	SF_AT

Table 30 TSS Rationale Overview

9 Bibliography

Criteria and methodology interpretation

[CC_Part1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002

[CC_Part2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002

[CC_Part3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003

[CEM] Common Criteria for Information Technology Security Evaluation, Evaluation methodology, Version 3.1, Revision 5, April 2017, CCMB-2017-04-004[AIS_41] Application Notes and Interpretation of the Scheme (AIS), AIS 41, Version 2, 31.01.11, Certification body of the BSI in the context of the certification scheme

Technical references

[Crypt_Filter] SDoT Filter, Cryptographic Mechanisms, V0.5, 06.08.2019, INFODAS GmbH

[Kon_Label] SDoT Produktfamilie International - Konzeptpapier zum Labelling, INFODAS GmbH

[Kon_Filter] SDoT Security Gateway International, Konzeptpapier Filtermechanismen, INFODAS GmbH

[ADaTP_4774] „Confidentiality Metadata Label Syntax", Edition A Version 1, Dec 2017, NATO STANDARDIZATION Organization

[ADaTP_4778] „Metadata Binding Mechanism", Edition A Version 1, Oct 2018, NATO STANDARDIZATION Organization

[RFC3986] IETF RFC 3986, "Uniform Resource Identifier (URI): Generic Syntax", at http://tools.ietf.org/html/rfc3986

[XML] XML SPIF Homepage. URL: http://www.xmlspif.org/

[XML_SYN] World Wide Web Consortium standard 'XML Signature Syntax and Processing Version 1.1', W3C Recommendation 11 April 2013, at http://www.w3.org/TR/xmldsig-core1/

[XML_SPEC] Extensible Markup Language (XML) 1.0 (Fifth Edition) W3C Recommendation, 26 November 2008, http://www.w3.org/TR/xml/.