

# SDoT Security Gateway

## Security Target Lite

Document name: ST\_Lite\_SDoTSGW6.2i\_SDoTFilter\_V2.0.docx

Version number: V 2.0

Version date: 08.07.2021

Author: INFODAS GmbH

Number of pages: 105

Issued by: INFODAS GmbH  
Rhonestraße 2  
50765 Cologne, Germany

Legal: All rights reserved.  
Passing on and duplication of this document as well as utilisation and communication of its contents are only permitted with the express consent of INFODAS GmbH.  
Contraventions will be prosecuted in court and will result in damages.

## Table of Contents

Table of Contents.....	i
List of Figures .....	v
List of Tables.....	vi
Abbreviations.....	vii
General.....	x
<b>1 ST Introduction (ASE_INT.1).....</b>	<b>13</b>
1.1 ST Reference .....	13
1.2 TOE reference.....	13
1.3 TOE overview.....	13
1.3.1 TOE definition and operational usage .....	13
1.3.2 Major Security Features of the TOE .....	14
1.3.3 TOE Type.....	17
1.3.4 Required non-TOE Hardware (HW)/Software (SW)/Firmware (FW) .....	18
1.4 TOE description .....	19
1.4.1 TOE Description – Physical Scope.....	19
1.4.2 TOE Description – Logical Scope .....	19
<b>2 Conformance claims (ASE_CCL.1).....</b>	<b>23</b>
2.1 CC conformance claim .....	23
2.2 PP Claim.....	23
2.3 Package Claim .....	23
2.4 Conformance Rationale .....	23
<b>3 Security Problem Definition (ASE_SPD.1) .....</b>	<b>24</b>
3.1 Introduction.....	24
3.2 Assets .....	24
3.2.1 Primary Assets .....	24
3.2.2 Secondary Assets.....	24
3.3 Subjects and external entities.....	25
3.4 Threats .....	25
3.5 Assumptions .....	27
3.6 Organisational Security Policies.....	29
<b>4 Security Objectives (ASE_OBJ.2).....</b>	<b>31</b>

4.1	Security Objectives for the TOE .....	31
4.2	Security Objectives for the Operational Environment .....	34
4.3	Rationale between SPD and security objectives.....	37
4.4	Rationale Threats .....	42
4.4.1	T.REVEAL_TO_LOW .....	42
4.4.2	T.MALICIOUS_CODE .....	43
4.4.3	T.AUTH .....	43
4.4.4	T.WRONG_LABEL.....	44
4.4.5	T.INSERT .....	44
4.4.6	T.MISCONFIG .....	44
4.4.7	T.AUDIT_CONTROL.....	44
4.4.8	T.AUDIT_COLLAPSE .....	45
4.4.9	T.AUDIT_ACCESS.....	45
4.5	Rationale OSPs.....	45
4.5.1	OSP.PROTOCOLS .....	45
4.5.2	OSP.FLOW_CONTROL.....	45
4.5.3	OSP.AUDIT .....	46
4.5.4	OSP.CONFIG_AUDIT .....	46
4.5.5	OSP.DUAL_CONTROL.....	46
4.6	Rationale Assumptions .....	46
4.6.1	A.DIFF_NET.....	46
4.6.2	A.TRUSTW_ONLY .....	46
4.6.3	A.HIGH_PROTECTION.....	46
4.6.4	A.ACCESS .....	47
4.6.5	A.TRUSTW_STAFF.....	47
4.6.6	A.AUDIT .....	47
4.6.7	A.ROLE_SEPARATION .....	47
4.6.8	A.HSM.....	47
4.6.9	A.PKI .....	47
4.6.10	A.NTP_SERVER .....	47
4.6.11	A.USER_IDENT .....	47

4.6.12	A.L4_PLATFORM.....	47
4.6.13	A.DEDICATED_ADMIN_NET .....	48
4.6.14	A.HIGH_AVAILABILITY.....	48
4.6.15	A.BOOT .....	48
<b>5</b>	<b>Definition of Security Function Policies (SFPs).....</b>	<b>49</b>
<b>6</b>	<b>Extended components definition (ASE_ECD.1).....</b>	<b>55</b>
6.1	Class FPT: Protection of the TSF .....	55
6.1.1	TSF integrity checks (FPT_INC).....	55
<b>7</b>	<b>Statement of security requirements (ASE_REQ.2).....</b>	<b>56</b>
7.1	Security functional requirements.....	56
7.1.1	User Data Protection (FDP) .....	58
7.1.2	Trusted path/channels (FTP) .....	71
7.1.3	Identification and authentication (FIA).....	71
7.1.4	Cryptographic support (FCS).....	72
7.1.5	Security management (FMT).....	75
7.1.6	Protection of the TSF (FPT) .....	78
7.1.7	Security audit (FAU) .....	79
7.2	Dependency Rationale.....	83
7.3	Security assurance requirements rationale .....	87
7.4	Security Functional Requirements Rationale.....	89
7.4.1	OT.FILTER.....	92
7.4.2	OT.PRE_FILTER .....	92
7.4.3	OT.LABELS .....	92
7.4.4	OT.SANITISED_DATA .....	92
7.4.5	OT.BANDWIDTH.....	92
7.4.6	OT.PROTOCOLS.....	92
7.4.7	OT.PROTOCOL_DENY .....	93
7.4.8	OT.USER_AUTHENTICATION .....	93
7.4.9	OT.ROLE_SEPARATION.....	93
7.4.10	OT.FOUR_EYES .....	93
7.4.11	OT.SECURE_CHANNEL .....	93
7.4.12	OT.AUDIT_CHANGE_LOG.....	94

---

7.4.13	OT.AUDIT .....	94
7.4.14	OT.AUDIT_PROTECT .....	94
7.4.15	OT.AUDIT_LOG_AVAILABILITY .....	94
7.4.16	OT.PROTECTION .....	94
7.4.17	OT.INIT .....	95
7.4.18	OT.DEFAULT .....	95
7.4.19	OT.WARNING .....	95
<b>8</b>	<b>TOE Summary Specification (ASE_TSS.1) .....</b>	<b>96</b>
8.1	TOE Security Functions .....	96
8.1.1	SF_LBL: Labelling Mechanism .....	96
8.1.2	SF_FR: Filtering Mechanism .....	96
8.1.3	SF_CP: Channel Protection .....	97
8.1.4	SF_DP: Data Protection .....	98
8.1.5	SF_AA: Authentication and Authorisation .....	98
8.1.6	SF_AT: Audit Trail .....	99
8.1.7	SF_SP: Self Protection .....	100
8.2	TOE Summary Specification Rationale .....	101
<b>9</b>	<b>Bibliography .....</b>	<b>103</b>

## List of Figures

<i>Figure 1: SDoT Security Gateway</i> .....	15
<i>Figure 2: Logical scope of the TOE</i> .....	20

## List of Tables

<i>Table 1 Main functionalities of each compartment.....</i>	17
<i>Table 2 Required non-TOE HW/SW/FW components of SDoT Security Gateway.....</i>	18
<i>Table 3 SDoT Security Gateway scope of delivery.....</i>	19
<i>Table 4 Primary assets.....</i>	24
<i>Table 5 Secondary assets.....</i>	25
<i>Table 6 Subjects.....</i>	25
<i>Table 7 Threats.....</i>	27
<i>Table 8 Assumptions.....</i>	29
<i>Table 9 OSPs.....</i>	30
<i>Table 10 Security Objectives for the TOE.....</i>	33
<i>Table 11 Security Objectives for the Operational Environment.....</i>	36
<i>Table 12 Security Objective for the TOE coverage.....</i>	38
<i>Table 13 Security Objective for the Operational Environment Coverage.....</i>	41
<i>Table 14 audit access control SFP.....</i>	49
<i>Table 15 admin access control SFP.....</i>	49
<i>Table 16 policy admin access control SFP.....</i>	49
<i>Table 17 dual control admin SFP.....</i>	50
<i>Table 18 dual control policy admin SFP.....</i>	50
<i>Table 19 data labelling SFP.....</i>	51
<i>Table 20 check label SFP.....</i>	52
<i>Table 21 data to low SFP.....</i>	53
<i>Table 22 pre-filtering SFP.....</i>	54
<i>Table 23 supported protocol SFP.....</i>	54
<i>Table 24 clean protocol SFP.....</i>	54
<i>Table 25 SFRs of the TOE.....</i>	58
<i>Table 26 auditable events.....</i>	80
<i>Table 27 Dependencies between the Security Functional Requirements (SFRs) for the TOE.....</i>	87
<i>Table 28 Security Assurance Requirements (SARs).....</i>	88
<i>Table 29 Coverage of the Security Objectives for the TOE by SFRs.....</i>	91
<i>Table 30 TSS Rationale Overview.....</i>	102

## Abbreviations

ADatP-3	Allied Data Publication-3
ADEXP	ATS Data Exchange Presentation
ASCII	American Standard Code for Information Interchange
ASE	Assurance Class in the CC Standard referring to the <b>Security Target Evaluation</b>
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 " <b>C</b> onformance <b>cl</b> 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 functional class " <b>S</b> ecurity <b>A</b> udit"
FCO	SFRs belonging to the functional class " <b>C</b> ommunication"
FDP	SFRs belonging to the functional class " <b>U</b> ser <b>D</b> ata <b>P</b> rotection"
FIA	SFRs belonging to the functional class " <b>I</b> dentification and <b>a</b> uthentication"
FMT	SFRs belonging to the functional class " <b>S</b> ecurity <b>m</b> anagement"
FPT	SFRs belonging to the functional class " <b>P</b> rotection of the <b>T</b> 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 <b>introduction</b> " 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 <b>objectives</b> " of the assurance class ASE
OSP	Organisational Security Policy
RAM	Random Access Memory
REQ	Refers to the assurance family "Security <b>requirements</b> " 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 “ <b>S</b> ecurity <b>p</b> roblem <b>d</b> 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 “ <b>T</b> OE <b>s</b> ummary <b>s</b> 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
Public	

### Revision History:

Version	Date	Application Note	Author
V 0.1	28.06.2019	First draft before submission of certification request	INFODAS GmbH
V 0.2	01.07.2019	QA version	INFODAS GmbH
V 0.3	09.07.2019	Version after QA	INFODAS GmbH
V 0.4	24.07.2019	- Added Assumption A.DEDICATED_ADMIN_NET - Editorial Changes	INFODAS GmbH
V 0.5	06.08.2019	- Editorial Changes in Application Notes of FDP_ACF.1.2/LabelCheck and FAU_STG.2. - Editorial Changes in 8.1.2.1.	INFODAS GmbH
V 0.6	04.09.2019	- Added FCS_CKM and FCS_COP SFRs for software based cryptographic operations of the TOE. - The optional SDoT Workstation removed. Following to that, the optional user role of the human labeller, the objective OE.LABEL_MAN and the assumption A.LABEL_MAN were obsolete and removed. - SFR FCO_NRO.2 and corresponding objective removed, since the TOE only supports TLS connection to clients and application systems but does not enforce TLS. - First comments of evaluation lab regarding ASE_INT.1 considered. - First comments of BSI before Kick-Off meeting considered - editorial changes	INFODAS GmbH
V 0.7	05.09.2019	QA	INFODAS GmbH

V 0.8	17.09.2019	<ul style="list-style-type: none"> <li>- Changes due to ASE comments from 2019-09-09 of evaluation lab</li> <li>- FDP_IFF.1/Validation and its dependency added</li> <li>- Added description of HA-variant in 1.4</li> <li>- further editorial changes due to changes in V 0.6 which went unnoticed by the author</li> </ul>	INFODAS GmbH
V 0.9	20.09.2019	QA	INFODAS GmbH
V 1.0	25.10.2019	<ul style="list-style-type: none"> <li>- Added assumption A.HIGH_AVAILABILITY.</li> <li>- Changes due to ASE comments from 2019-10-01 of evaluation lab</li> </ul>	INFODAS GmbH
V 1.1	04.11.2019	Minor Changes in A.HSM due to comment from evaluation lab	INFODAS GmbH
V1.2	02.12.2019	Minor Changes from the BSI crypto comments	INFODAS GmbH
V1.3	21.01.2020	<p>Minor corrections in Table 29 and Table 30.</p> <p>Added some explanation in sec. 1.4 that the information flow from LOW to HIGH is not security relevant.</p>	INFODAS GmbH
V1.4	26.02.2020	<p>Minor corrections in the following SFRs</p> <ul style="list-style-type: none"> <li>- FDP_ACF.1/Admin</li> <li>- FTP_TRP.1</li> <li>- FMT_MSA.1</li> <li>- FMT_SMF.1</li> <li>- FAU_ARP.1</li> <li>- FDP_ACC/LabelCheck and FDP_ACF/LabelCheck are now integrated as information flow in FDP_IFC.1.1/DataToLow respectively in FDP_IFF.1.1/DataToLow.</li> <li>- FPT_TST was removed and replaced with the new defined family FPT_INC.1.</li> </ul> <p>The following SFRs were removed:</p> <ul style="list-style-type: none"> <li>- FIA_ATD.1</li> <li>- FDP_ITC.2</li> </ul> <p>Added the following SFRs:</p> <ul style="list-style-type: none"> <li>- FDP_ACC.1/AdminAccess</li> <li>- FDP_ACC.1/PolicyAdminAccess</li> <li>- FDP_ACF.1/AdminAccess</li> <li>- FDP_ACF.1/PolicyAdminAccess</li> </ul>	INFODAS GmbH

		Added the following tables and SFPs in Sec. 5 - <i>Table 15 admin access control SFP</i> - <i>Table 16 policy admin access control SFP</i>	
V1.5	11.03.2020	- Minor correction in Extended Component Definition of FPT_INC.1.	INFODAS GmbH
V1.6	18.05.2020	- Fixed names of Compartments to correspond to the Subsystems of the TOE in TDS - Minor correction in Table 3 regarding the manuals to correspond to the manuals delivered for AGD - A.BOOT and OE.BOOT added	INFODAS GmbH
V1.7	19.11.2020	Minor correction in FAU_GEN.1 and in SF_AT due to evaluation results in the context of ADV.	INFODAS GmbH
V1.8	12.02.2021	Further corrections due to comments from evaluation lab from 2020-12-01 and due to comments related to the AGD evaluation	INFODAS GmbH
V 1.9	29.03.2021	Minor changes due to comments from the lab. Minimal information added in Table 3.	INFODAS GmbH
V 1.91	19.05.2021	Another instance of this document created from the full version for publication (ST-lite) in accordance with [AIS_35] and supporting document [MC_ST_LITE].	INFODAS GmbH
V 2.0	09.07.2021	Minor adaptations due to minor changes in the non-lite version of the Security Target	

## 1 ST Introduction (ASE\_INT.1)

1 This chapter provides an unambiguous identification of the main characteristics of this Security  
2 Target and the TOE in scope of the security certification process. This security target was created  
3 considering [AIS\_41] of BSI.

### 1.1 ST Reference

4 **Title:** SDoT Security Gateway Security Target Lite

5 **Version:** V 2.0

6 **Date:** 08.07.2021

7 **Author:** INFODAS GmbH

### 1.2 TOE reference

8 **Product name:** SDoT Security Gateway

9 **TOE name (long):** SDoT Security Gateway, SDoT Filter SW

10 **TOE name (short):** SDoT Filter SW

11 **TOE version:** 6.2i

12 **Developer name:** INFODAS GmbH

13 **Certification ID:** BSI-DSZ-CC-1129

### 1.3 TOE overview

14 The TOE version 6.2i refers to the use case for the deployment to the international free market.  
15 Hereby, 6.2i describes a mnemonic convention which exact configuration is identified as the  
16 following revision: 6.2.15252.29203. This Security Target defines the security objectives for, and  
17 security requirements of the SDoT Filter SW (TOE), which is a component of the product SDoT  
18 Security Gateway of INFODAS GmbH. Further, this security target defines the security objectives of  
19 the operational environment for the TOE. The following subsections give an overview of the TOE, its  
20 usage and major security features, the TOE type, and lists all required non-TOE Hardware, non-TOE  
21 Software/Firmware.

#### 1.3.1 TOE definition and operational usage

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

28 SDoT Security Gateway includes the TOE which provides the filtering functionalities to check  
29 security labels for the transmission of data between the two differently classified networks and  
30 provides mechanisms to validate structured data objects against a rule set. The SDoT Security  
31 Gateway comprises the SDoT Filter Platform (HW with HSM, FW, OS) and the SDoT Filter SW which

32 is the TOE. The SDoT Security Gateway includes an SDoT Administration for Administration of the  
33 SDoT Filter. More information about the non-TOE parts of SDoT Security Gateway will be given in  
34 1.3.4. Therefore, the TOE is an application delivered together with a set of software and hardware  
35 components to the customer. The underlying micro kernel operating system with its separation  
36 mechanism is part of the TOE environment. All hardware and software which are needed to securely  
37 operate the TOE in accordance with the TOE assumptions, and in accordance to the assumptions of  
38 the TOE operational environment, are in scope of delivery, see Table 3. The hardware parts and  
39 software parts besides the TOE are partially customized for SDoT Security Gateway to make sure  
40 that the TOE operates properly as intended with the dedicated delivery parts only.

### 1.3.2 Major Security Features of the TOE

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

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

55 The TOE includes seven compartments for different purposes. These are

- 56 • FI\_GUI,
- 57 • FI\_HGH,
- 58 • FI\_CFG,
- 59 • FI\_H2L,
- 60 • FI\_L2H,
- 61 • FI\_LOW, and
- 62 • FI\_ADT.

63 The security mechanisms of the TOE are implemented on the compartments FI\_GUI, FI\_CFG,  
64 FI\_H2L, and FI\_ADT. The TOE enforces the information flow policy which ensures that only data  
65 with either a correct label, or structured data with classified information which must be checked  
66 against a corresponding rule set, can then be forwarded to the lower classified network (LOW). The  
67 TOE collects and checks audit data to identify any occurring policy violation. The TOE performs  
68 management functions on configuration data in FI\_CFG. Identification and authentication of  
69 administrators and auditor of the TOE is provided by the FI\_GUI which communicates via TLS  
70 connection to the SDoT Administration.

71 The compartment FI\_H2L is responsible for the main filtering functionality of the TOE. The only  
 72 possibility to send data from the higher classified network (HIGH) to the lower classified network  
 73 (LOW) is through the compartment FI\_H2L. The FI\_H2L communicates with the compartments  
 74 FI\_HGH and FI\_LOW through the L4Re OS. Hence, FI\_H2L does neither have a direct connection to  
 75 the higher classified network (HIGH) nor to the lower classified network, but instead, FI\_H2L  
 76 communicates with FI\_HGH for connection to network HIGH. For the same reason, FI\_H2L  
 77 communicates with FI\_LOW for connection to network LOW. The following figure depicts the TOE  
 78 with its IT environment which build together the SDoT Security Gateway.

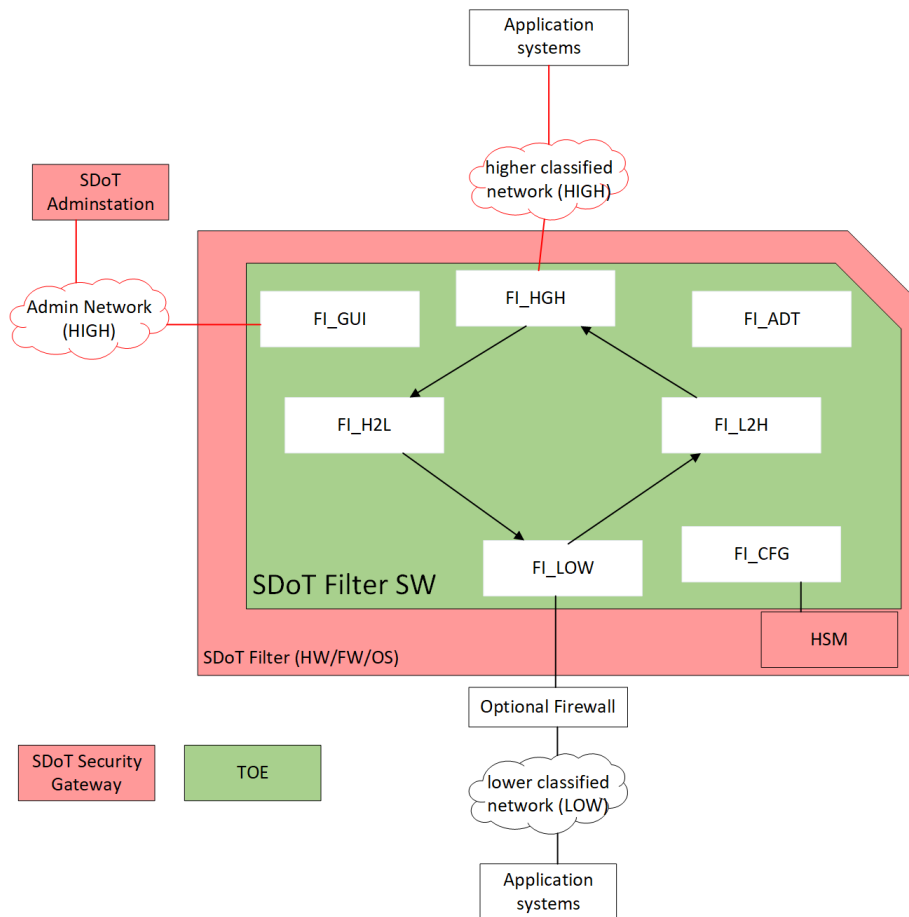


Figure 1: SDoT Security Gateway

79 The information flow from the network LOW to the network HIGH is under control of the  
 80 compartment FI\_L2H which has no direct link to the network HIGH and LOW. For the communication  
 81 to network LOW the compartment FI\_L2H uses FI\_LOW and similarly, the FI\_HGH is used for  
 82 communication to the network HIGH. All protocol data which is sent from the network LOW to the  
 83 network HIGH is filtered by the compartment FI\_L2H.

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



88 The SDoT Administration allows the administrator, policy-admin or the auditor to fulfil their  
89 responsibility and role as such. The SDoT Administration is connected to the TOE via the compartment  
90 FI\_GUI through a dedicated higher classified administration network in the HIGH domain.

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

Compartment	Description
FI_GUI	<ul style="list-style-type: none"> <li>Provides the GUIs for administrating and auditing purposes of the TOE.</li> <li>Establishes the administrative TLS connection to the SDoT Administration.</li> </ul>
FI_HGH	<ul style="list-style-type: none"> <li>Includes proxies for SMTP, HTTP, UDP and TCP for communication with the TOE environment within the network HIGH.</li> </ul>
FI_CFG	<ul style="list-style-type: none"> <li>Responsible for the communication with the HSM for cryptographic purposes.</li> <li>Provides functionalities for the administration of the TOE.</li> </ul>
FI_H2L	<ul style="list-style-type: none"> <li>This compartment is responsible for pre-filtering all incoming data from the network HIGH.</li> <li>It automatically validates the data against the pre-defined rule set.</li> <li>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.</li> </ul> <p>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.</p> <ul style="list-style-type: none"> <li>Filters the data in accordance with its classification written in the label or on the ICAP header.</li> </ul>
FI_L2H	<p>For forwarding data from network LOW to network HIGH the TOE can be configured with three different options within this compartment.</p> <p><b>Description of first option:</b></p> <ul style="list-style-type: none"> <li>Pre-filtering of incoming data from network LOW,</li> <li>Automatic validation of data against a pre-defined policy,</li> </ul>

	<ul style="list-style-type: none"> <li>Attaches a security label or writes relevant information into a header of the used data transfer protocol ICAP after successful validation,</li> <li>Filters the data in accordance with its classification written in the label or on the ICAP header.</li> </ul> <p><b>Description of second option:</b></p> <ul style="list-style-type: none"> <li>Security labels are generated based on the security level of network LOW</li> </ul> <p><b>Description of third option:</b></p> <ul style="list-style-type: none"> <li>Data messages are directly forwarded to network HIGH</li> </ul>
FI_LOW	<ul style="list-style-type: none"> <li>Includes proxies for SMTP, HTTP, UDP and TCP for communication with the TOE environment within the network LOW.</li> </ul>
FI_ADT	<ul style="list-style-type: none"> <li>Includes mechanisms for logging security relevant events.</li> </ul>

Table 1 Main functionalities of each compartment

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

- 93           • The TOE validates security labels attached to data and forwards the data after  
94           successful validation from the network HIGH to the network LOW or denies the data to  
95           be forwarded in case the label is not correct.
- 96           • The TOE validates structured data against configured rule sets.
- 97           • The TOE only accepts connections on configured ports. For each port, only correct  
98           communication according to the configured protocol is accepted by the TOE.
- 99           • The TOE provides strong binding between data and the corresponding security labels  
100           with digital signatures. The digital signatures are provided by the HSM which does not  
101           belong to the TOE
- 102           • The TOE re-builds (sanitisation) and converts (canonicalization) forwarded security  
103           labels
- 104           • The TOE provides secure auditing mechanisms of logs and secure administration  
105           capabilities.
- 106           • The TOE provides mechanisms for authentication.

### 1.3.3 TOE Type

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

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

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

- 112 • Underlying platform (hardware and operating system) of the TOE
- 113 • HSM for cryptographic support in terms of labelling mechanisms, random numbers  
114 and secure storage
- 115 • SDoT Administration including hardware and software parts
- 116 • Smartcard Reader for authentication purposes at the SDoT Administration
- 117 • Smartcards for cryptographic support and authentication

118 Besides the hardware and operating systems, there are several software components which belong  
119 to the TOE environment (cf. Figure 1 and Figure 2). The following table provides an overview of all  
120 required non-TOE hardware and non-TOE software components which are needed to securely  
121 operate the TOE. In addition, all components required by SDoT Security Gateway for its secure use  
122 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 Administration	Machine (laptop computer) of the renowned manufacturer GETAC with CentOS.
Installation CD/DVD	Software of SDoT Filter and SDoT Administration
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

123 The following table shows the delivery parts of the SDoT Security Gateway where the TOE belongs  
124 to. Following to that, the subsections provide a description of the physical and logical boundaries of  
125 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, V1.5 Manual for Adminstation, V1.0 Product Information – Requirements for Secure Operation, V1.2	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

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

### 1.4.2 TOE Description – Logical Scope

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

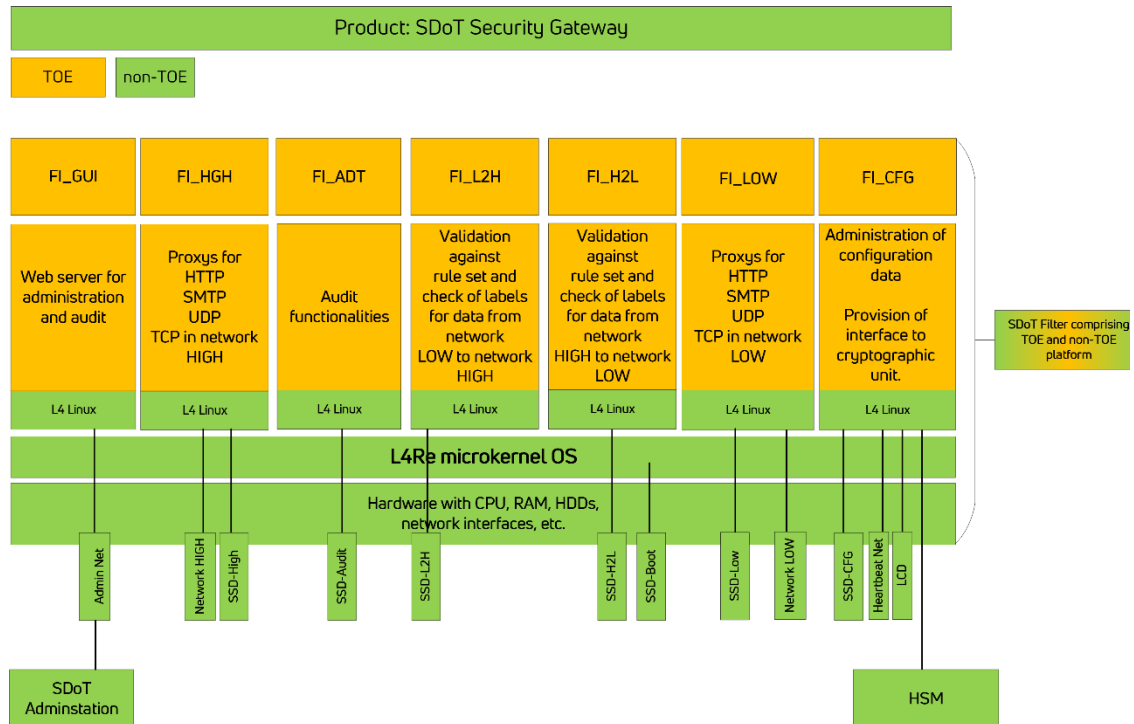


Figure 2: Logical scope of the TOE

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

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

#### 139 **SDoT Administration (non-TOE):**

140 The SDoT Administration is based on a CentOS architecture. The functionalities for local  
 141 administration and local auditing of the SDoT Administrations are provided by a GUI through a  
 142 common browser. Configuration parameters and audit data are managed within the administration  
 143 GUI, and respectively by the audit GUI of the SDoT Administration.

#### 144 **SDoT Filter SW (TOE)**

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

#### 146 **COMPARTMENT FI\_GUI**

147 The web-based Administration GUI and Audit GUI are displayed by a common web browser installed  
 148 on the SDoT Administration (non-TOE). With Administration GUI and Audit GUI the configuration data  
 149 and audit data of the TOE can be managed. Further, the FI\_GUI establishes the TLS connection for  
 150 administrative purposes with the SDoT Administration.

**151 COMPARTMENT FI\_CFG**

152 This is where the main configuration is managed, and monitoring tasks are performed. This is the  
153 only compartment with a connection to the HSM which provides hardware support for some  
154 cryptographic mechanisms used by the TOE.

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

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

**161 COMPARTMENT FI\_ADT**

162 This compartment provides functions for logging security relevant events. Only the audit agent  
163 within FI\_ADT has access to logged audit data in the audit storage. Further, the audit agent monitors  
164 the audit storage capacity to avoid any potential overflow of the audit storage. The FI\_ADT  
165 communicated with the FI\_GUI which establishes the TLS connection for displaying the relevant  
166 information on the SDoT Administration.

167 The audit agent is responsible to record security relevant events on the TOE, related to writing  
168 entries into the audit trail. The audit agent in FI\_ADT is responsible to generate alarms, i.e. e-mails.  
169 The SMTP-MTA of the TOE sends then the e-mails to a list of receivers. The list is configurable and  
170 stored in FI\_CFG which protects the integrity with checksums stored in the HSM.

171 Further, the audit agent covers the following tasks:

- 172 • Generate new audit trails if the current audit trail exceeds a pre-defined size,
- 173 • Generate new audit trails daily,
- 174 • Monitor the storage capacity of the storage device to prevent an audit trail overflow.

**175 COMPARTMENT FI\_H2L**

176 All data which are sent from the higher classified network HIGH to the lower classified network LOW  
177 are processed by FI\_H2L.

**178 COMPARTMENT FI\_L2H**

179 In general, forwarding data from LOW to HIGH is not a security critical functionality since the main  
180 objective of the TOE is to prevent unwanted data flow in the opposite direction, from HIGH to LOW.  
181 The main asset are data within the higher classified network HIGH which have to be protected.

**182 COMPARTMENT FI\_HGH**

183 The FI\_HGH provides proxy support for the following types of protocols:

- 184 • SMTP
- 185 • HTTP
- 186 • UDP
- 187 • TCP

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

- 190           • Accept data from higher classified network HIGH and forwarding the data to FI\_H2L.
- 191           • Forwarding data to the higher classified network HIGH which comes from FI\_L2H.
- 192 Also, the above-mentioned proxies support the non-TOE functionality for mutually authenticated  
193 TLS connection with IT systems of the operational environment of the TOE within the network HIGH.
- 194 **COMPARTMENT FI\_LOW**
- 195 The FI\_LOW includes provides proxy support for the following types of protocols:
- 196           • SMTP
- 197           • HTTP
- 198           • UDP
- 199           • TCP
- 200 The proxies perform the following tasks which controls all data flow in the lower classified network  
201 HIGH.
- 202           • Accept data from lower classified network LOW and forwarding the data to FI\_L2H.
- 203           • Forwarding data to the lower classified network LOW which comes from FI\_H2L.
- 204 Also, the above-mentioned proxies support the non-TOE functionality for mutually authenticated  
205 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

206 This Security Target claims conformance to

- 207 • Common Criteria for Information Technology Security Evaluation, Part 1: Intro-duction  
208 and general model, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002 (cf.  
209 [CC\_Part1])
- 210 • Common Criteria for Information Technology Security Evaluation, Part 2: Security  
211 functional components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002 (cf.  
212 [CC\_Part2])
- 213 • Common Criteria for Information Technology Security Evaluation, Part 3: Security  
214 assurance components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003 (cf.  
215 [CC\_Part3])

216 in the following way

- 217 • Part 2 extendet
- 218 • Part 3 conformant

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

### 2.2 PP Claim

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

### 2.3 Package Claim

223 The assurance packages claimed by the TOE is EAL4 augmented by ALC\_FLR.2 which adds flaw  
224 reporting procedures to the Evaluation Assurance Level EAL4.

### 2.4 Conformance Rationale

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



### 3 Security Problem Definition (ASE\_SPD.1)

#### 3.1 Introduction

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

#### 3.2 Assets

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

##### 3.2.1 Primary Assets

235 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

236 For an effective protection of the primary assets the following secondary assets must also be  
237 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

238 External entities and subjects that may act as threat agent and perform operations on objects are  
239 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 Administration	Authorised persons with access to the SDoT Administration, 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

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

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

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

		<b>Asset:</b> DATA_IN_HIGH, CONF_SW_DATA, AUTH_DATA, AUDIT_DATA, KEY_DATA
2.	T.MALICIOUS_CODE	<p><b>Adverse action:</b> 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.</p> <p><b>Threat agent:</b> Human Attacker</p> <p><b>Asset:</b> DATA_IN_HIGH, CONF_SW_DATA</p>
3.	T.AUTH	<p><b>Adverse action:</b> 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.</p> <p><b>Threat agent:</b> Human attacker</p> <p><b>Asset:</b> DATA_IN_HIGH, CONF_SW_DATA, KEY_DATA, AUDIT_DATA</p>
4.	T.WRONG_LABEL	<p><b>Adverse action:</b> 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.</p> <p><b>Threat agent:</b> Human attacker and/or non-educated human user having access to labelling mechanisms of the TOE</p> <p><b>Asset::</b> DATA_IN_HIGH, CONF_SW_DATA</p>
5.	T.INSERT	<p><b>Adverse action:</b> 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.</p> <p><b>Threat agent:</b> Human attacker and non-educated human user having access to the TOE.</p> <p><b>Asset: :</b> DATA_IN_HIGH, CONF_SW_DATA</p>
6.	T.MISCONFIG	<p><b>Adverse action:</b> 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.</p> <p><b>Threat agent:</b> Administrators and Auditor of the SDoT°Adminstations</p> <p><b>Asset: :</b> DATA_IN_HIGH, CONF_SW_DATA</p>

7.	T.AUDIT_CONTROL	<p><b>Adverse action:</b> A human attacker or an IT system, modifies the audit records of the TOE, so that security incidents or illegal actions can remain undetected.</p> <p><b>Threat agent:</b> Human attacker, IT environment</p> <p><b>Asset:</b> AUDIT_DATA</p>
8.	T.AUDIT_COLLAPSE	<p><b>Adverse action:</b> 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.</p> <p><b>Threat agent:</b> Human attacker, IT environment</p> <p><b>Asset:</b> DATA_IN_HIGH, AUDIT_DATA</p>
9.	T.AUDIT_ACCESS	<p><b>Adverse action:</b> 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.</p> <p><b>Threat agent:</b> Human attacker, IT environment</p> <p><b>Asset:</b> DATA_IN_HIGH, AUDIT_DATA</p>

Table 7 Threats

### 3.5 Assumptions

243 This section of the SPD describes the security aspects of the operational environment in which the  
244 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 Administration 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	<p>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.</p> <p>Except for the ECDSA key generation for TLS connection to the SDoT Administration, 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.</p> <p>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.</p> <p>Further, keys used for audit data protection are generated by the HSM.</p>
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 Administration 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

245 This section describes the Organisational Security Policies (OSPs). The TOE, its operational  
 246 environment, or a combination of the two shall comply with the following OSPs as security rules,  
 247 procedures or guidelines imposed (or presumed to be imposed) now and/or in future by an actual or  
 248 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)

249 This chapter describes the security objectives for the TOE and the security objectives for the  
250 operational TOE environment.

### 4.1 Security Objectives for the TOE

251 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.  <i>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.</i>
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

252 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	<p>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.</p> <p>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</p>

		<p>operations are used. Further, the output from the Random Bit Generator of the HSM shall be used directly without further post-processing by software.</p> <p>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.</p>
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 shall be properly used.
13	OE.DEDICATED_ADMIN_NET	The TOE shall be connected to the SDoT Administration 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

253 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
<b>Threats</b>																				
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
<b>Threats</b>																
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									
<b>OSPs</b>																



	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																
<b>Assumptions</b>																
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

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

#### 4.4 Rationale Threats

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

##### 4.4.1 T.REVEAL\_TO\_LOW

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

261 OT.FILTER addresses T.REVEAL\_TO\_LOW with the corresponding filtering mechanism which filters  
262 all data sent between the higher classified network and the lower classified network. OT.FILTER  
263 makes sure that only data are passing the filtering mechanism of the TOE which is classified to have  
264 at least the same security level of the lower classified network LOW or less than LOW.

265 OT.PRE\_FILTER provides additional filtering mechanisms to further mitigate the risk of  
266 T.REVEAL\_TO\_LOW by blocking inappropriate messages before they can even reach the main  
267 filtering component of the TOE.

268 OT.SANITISED\_DATA counters T.REVEAL\_TO\_LOW by ensuring that no confidential information  
269 can pass the filtering mechanism to the lower classified network in accordance with the security rule  
270 set of the TOE operator. All unnecessary information will be removed from the data resp. from the  
271 message and are not visible to the user.

272 OT.USER\_AUTHENTICATION addresses T.REVEAL\_TO\_LOW by ensuring that only authorised and  
273 authenticated users can access and change configuration of the TOEs security related  
274 functionalities.

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

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

278 OT.INIT counters T.REVEAL\_TO\_LOW in the case where after TOE initialisation a secure state cannot  
279 be achieved. Here, the TOE will block all traffic and no higher classified confidential information can  
280 be passed from the higher classified network to the lower classified network.

281 OT.PROTOCOLS counters T.REVEAL\_TO\_LOW by ensuring that only data sent with communication  
282 protocols, which are supported by the TOE, are passed through the filtering mechanism of the TOE.  
283 All other communication attempts are rejected by the TOE with OT.PROTOCOL\_DENY.

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

287 OT.FOUR\_EYES ensures that no single administrator or policy-admin of the TOE is able to  
288 maliciously misconfigure the TOE, which may lead to any security flaw or leakage of confidential  
289 information.

290 OT.AUDIT\_CHANGE\_LOG enables the auditor to track all changes to the TOE configuration, and  
291 identify the corresponding user. This objective for the TOE addresses T.REVEAL\_TO\_LOW by

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

294 OT.AUDIT addresses T.REVEAL\_TO\_LOW by making possible to the auditor to detect illegally  
295 transferred data or any attempt to send data illegally from the higher classified network to the lower  
296 classified network.

297 OT.AUDIT\_LOG\_AVAILABILITY provides the audit logs to the auditor so that potential incidents can  
298 be identified and analysed.

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

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

305 OE.DIFF\_NET, OE.TRUSTW\_STAFF and OE.TRUSTW\_ONLY support OT.FILTER by ensuring that all  
306 data to be sent between the higher classified and the lower classified networks have to pass the  
307 filtering mechanism since, there are only trustworthy connection between the higher classified and  
308 the lower classified networks. Further, the organisation operating the TOE ensures that only  
309 trustworthy personnel have privileged user roles.

310 Further, OE.DEDICATED\_ADMIN\_NET supports OT.FILTER to ensure that the TOE is only configured  
311 through a dedicated admin network which is additionally supports to secure the configuration of the  
312 TOE.

313 OE.HIGH\_PROTECTION supports OT.FILTER to further address T.REVEAL\_TO\_LOW by ensuring  
314 that all filtering tasks performed by the TOE is done within the higher classified network, before  
315 sending any data to the lower classified network.

#### 4.4.2 T.MALICIOUS\_CODE

316 OT.PROTECTION addresses T.MALICIOUS\_CODE by directly requiring the TOE to protect all  
317 configuration data against any attempt to bypass, deactivate, or manipulate the configuration of the  
318 TOE.

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

321 OE.HIGH\_PROTECTION addresses T.MALICIOUS\_CODE by requiring the TOE to be located within  
322 the HIGH domain. Further, OE.BOOT helps to mitigate the risk of T.MALICIOUS\_CODE in the  
323 presence of secure boot mechanisms which only allows authentic software to be executed.  
324 Additionally, OE.BOOT requires the administrators to keep the securely pre-configures settings of  
325 the used BIOS.

#### 4.4.3 T.AUTH

326 OT.USER\_AUTHENTICATION counters T.AUTH by means of requiring all users of the TOE with  
327 special privileges within the higher classified network to be authenticated before any action on the  
328 TOE is possible. OT.SECURE\_CHANNEL supports OT.USER\_AUTHENTICATION by providing a  
329 secure channel for privileged users to communicate with the TOE.

#### 4.4.4 T.WRONG\_LABEL

- 330 OT.LABELS counters T.WRONG\_LABEL by ensuring that the TOE only uses labels
- 331
- which have been generated by an authorised user only,
  - 332 • are strongly bound to the resp. data and any attempt to modify a label leads to an
  - 333 invalid label and the data will be rejected by the TOE,
  - 334 • The TOE can unambiguously identify the categorisation of the security level of the
  - 335 label
  - 336 • The TOE can determine whether the categorisation of the level of security of the data
  - 337 was manually within the network HIGH or automatically by an IT system.
- 338 Further, it counters T.WRONG\_LABEL by requiring the TOE to use security labels which have a
- 339 strong bond between the label and the corresponding data resp. the message.

#### 4.4.5 T.INSERT

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

#### 4.4.6 T.MISCONFIG

- 343 OT.FOUR\_EYES addresses T.MISCONFIG by avoiding that an administrator or policy-admin could
- 344 unintentionally misconfigure the TOE by means of enforcing the dual control mechanism.
- 345 OT.PROTECTION counters the T.MISCONFIG by ensuring that the TOE cannot be misconfigured in a
- 346 way, that data can pass the filtering mechanism of the TOE from the higher classified network to the
- 347 lower classified network.
- 348 OT.ROLE\_SEPARATION limits the privileges of a single user, i.e. administrator is not able to
- 349 misconfigure the TOE in a way that the configuration change is not logged and not detected by the
- 350 auditor.
- 351 OT.AUDIT\_CHANGE\_LOG ensures that each configuration change is logged into the audit trail and
- 352 the identity of the user who is triggering any configuration change is logged. This may limit errors
- 353 due to misconfiguration of the TOE to a minimum and encourage the user to be more careful. The
- 354 auditor can analyse the audit trail and detect any possible misconfiguration and replace by a safe
- 355 and good known configuration.
- 356 OT.AUDIT\_PROTECT ensures that logged configurations are cryptographically protected against
- 357 manipulation.
- 358 OE.HIGH\_PROTECTION reduces the risk that the TOE will be attacked from the lower classified
- 359 network. The TOE is physically and organisationally located within the higher classified network.

#### 4.4.7 T.AUDIT\_CONTROL

- 360 OT.AUDIT\_PROTECT counters the threat by protecting the audit data against any attempt of
- 361 bypassing, deactivating, or manipulating the audit data.

- 362 OT.ROLE\_SEPARATION ensures that only the auditor is able to remove records from the audit trail.  
363 OE.ACCESS counters the threat by ensuring that only auditors and administrators have physical  
364 access to the TOE.  
365 OT.USER\_AUTHENTICATION supports OT.ROLE\_SEPARATION by ensuring that the auditor is  
366 authenticated before the auditor can take any action.

#### 4.4.8 T.AUDIT\_COLLAPSE

- 367 OT.AUDIT\_PROTECT counters T.AUDIT\_COLLAPSE directly by preventing audit overflows.  
368 OT.AUDIT\_PROTECT requires the TOE to provide mechanisms to protect audit records against event  
369 loss or saturation of the storage device.

#### 4.4.9 T.AUDIT\_ACCESS

- 370 OE.AUDIT\_ENFORCE requires that the audit trail is regularly checked by the authorised auditor so  
371 that records are regularly reduced. This mitigates the threat T.AUDIT\_ACCESS because the amount  
372 of confidential audit records is kept manageable.  
373 OT.ROLE\_SEPARATION counters T.AUDIT\_ACCESS by ensuring that a privileged user with other  
374 user role than the auditor cannot move audit records.  
375 OT.USER\_AUTHENTICATION counters the threat T.AUDIT\_ACCESS by ensuring that the auditor is  
376 authorised to read and move audit records. OT.SECURE\_CHANNEL supports  
377 OT.USER\_AUTHENTICATION by providing a secure channel for authorised auditors to communicate  
378 with the TOE.  
379 OE.ACCESS supports to counter the threat by making sure that only authorised users have access  
380 to the TOE. Hence, only authorised auditors have access to any audit data.

### 4.5 Rationale OSPs

- 381 The following describes how OSPs are enforced by the TOE or by the operational environment of  
382 the TOE.

#### 4.5.1 OSP.PROTOCOLS

- 383 The security objective for the TOE OT.PROTOCOLS corresponds to OSP.PROTOCOLS by requiring  
384 the TOE to only process the pre-defined list of supported protocols as listed by OT.PROTOCOLS. All  
385 other protocols will not be accepted and is provided by OT.PROTOCOL\_DENY.

#### 4.5.2 OSP.FLOW\_CONTROL

- 386 OT.FILTER ensures that only data which is corresponding to the classification of the lower classified  
387 network can pass the filtering mechanism of the TOE. Therefore, OT.FILTER is addressed by the  
388 organisational security policy OSP.FLOW\_CONTROL.

### 4.5.3 OSP.AUDIT

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

392 OE.AUDIT\_ENFORCE requires that the audit trail is regularly examined by an authorised auditor.  
393 OT.AUDIT\_LOG\_AVAILABILITY supports OE.AUDIT\_ENFORCE by providing the audit data to the  
394 authorised auditor.

395 Further, OT.AUDIT\_PROTECT ensures the integrity of audit data and enforces that records are not  
396 lost.

### 4.5.4 OSP.CONFIG\_AUDIT

397 The objective OT.AUDIT\_CHANGE\_LOG requires that all changes to configuration data are logged.  
398 The auditor shall be able to track all changes and identify the user who made any change. Also, the  
399 identification of the user is realised by OT.USER\_AUTHENTICATION. The combination of both  
400 objectives implements the policy.

### 4.5.5 OSP.DUAL\_CONTROL

401 OT.FOUR\_EYES implements this policy by requiring that all changes are performed by two  
402 administrators. There is no possibility that only one administrator can make changes without the  
403 confirmation of a second administrator.

## 4.6 Rationale Assumptions

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

### 4.6.1 A.DIFF\_NET

406 The security objective for the operational environment of the TOE OE.DIFF\_NET corresponds to the  
407 assumption A.DIFF\_NET by requiring the TOE to be connected between two networks, which have  
408 different security classifications. One network has a higher classification than the other.

### 4.6.2 A.TRUSTW\_ONLY

409 OE.TRUSTW\_ONLY requires that the TOE is the only connection between the higher classified  
410 network, and the lower classified network. OE.DIFF\_NET supports OE.TRUSTW\_ONLY because it  
411 requires that the TOE is connected to two differently classified networks.

### 4.6.3 A.HIGH\_PROTECTION

412 This assumption is directly covered by the objective OE.HIGH\_PROTECTION which requires the TOE  
413 to be physically and organisationally located and operated within the domain of the higher classified  
414 network.

#### 4.6.4 A.ACCESS

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

#### 4.6.5 A.TRUSTW\_STAFF

417 OE.TRUSTW\_STAFF covers the assumption A.TRUSTW\_STAFF by requiring that all users of the  
418 TOE are trusted by the organisation operating the TOE.

#### 4.6.6 A.AUDIT

419 The assumption A.AUDIT is covered by OE.AUDIT\_ENFORCE because the operational environment  
420 of the TOE ensures that audit data is regularly checked by an authorised auditor.

#### 4.6.7 A.ROLE\_SEPARATION

421 OE.ROLE\_SEPARATION upholds this assumption because this objective requires the operational  
422 environment to ensure that each privileged user of the TOE has exactly one privileged user role.

#### 4.6.8 A.HSM

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

#### 4.6.9 A.PKI

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

#### 4.6.10 A.NTP\_SERVER

427 The assumption A.NTP\_SERVER is covered by the objective OE.NTP\_SERVER which requires the  
428 operator of the TOE to use a trustworthy NTP server.

#### 4.6.11 A.USER\_IDENT

429 The assumption A.USER\_IDENT is covered by the objective OE.USER\_IDENT which requires to  
430 identify and authenticate all privileged users within the higher classified network HIGH before any  
431 actions can be performed.

#### 4.6.12 A.L4\_PLATFORM

432 The assumption A.L4\_PLATFORM is covered by the objective OE.L4\_PLATFORM which requires the  
433 TOE to run on a L4Re microkernel OS which provides dedicated logical separation mechanisms for  
434 each compartment.



#### 4.6.13 A.DEDICATED\_ADMIN\_NET

435 The assumption A.DEDICATED\_ADMIN\_NET is covered by the objective  
436 OE.DEDICATED\_ADMIN\_NET which requires that the TOE is connected to the SDoT Administration  
437 only through a dedicated network for administration purposes. Further, the objective requires that  
438 the dedicated admin network is a physically isolated network within the higher classified network  
439 HIGH.

#### 4.6.14 A.HIGH\_AVAILABILITY

440 The assumption A.HIGH\_AVAILABILITY is addressed by OE.HIGH\_AVAILABILITY which requires that  
441 if the TOE will be operated in the HA-variant, the operational environment ensures that the  
442 physically separated network via the Heartbeat interface is the only used connection.

#### 4.6.15 A.BOOT

443 The assumption A.BOOT is directly addressed by OE.BOOT which requires that the TOE uses the  
444 secure start-up and boot mechanisms provided by the underlying platform. Further, the  
445 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	<p>Verification of data_security_label.signature is successful</p> <p>and</p> <p>data_security_label is well-formed</p> <p>and</p> <p>data_security_label.policy_id = SPIF.policy_id</p> <p>and</p> <p>data_security_label.classification <math>\in</math> {SPIF.valid_classification}</p> <p>and</p> <p>{data_security_label.categories} <math>\subseteq</math> {SPIF.valid_categories}</p> <p>and</p> <p>{data_security_label.classification x data_security_label.categories} <math>\notin</math> {SPIF.invalid_combination}</p>	<p>{data_security_label.classification x data_security_label.categories} = {(classification, category_1), ..., (classification, category_N), N <math>\in</math> <math>\mathbb{N}</math>}</p> <p>The structure of a security label is described in sec. 8.1.1 and technically more detailed in [Kon_Label].</p>

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

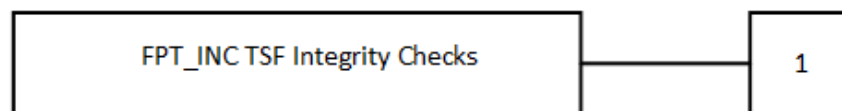
#### 6.1.1 TSF integrity checks (FPT\_INC)

##### 446 Family Behaviour

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

450 Application Note: The other families of the class FPT do not provide a family which only refers to  
451 periodic integrity checks during start-up, during operation or upon request of an authorised user. In  
452 the following, the family FPT\_INC TSF Integrity Checks will be defined in accordance with the style  
453 used in the Common Criteria Part 2, cf. sections 6 and 7 in [CC\_Part2].

##### 454 Component Levelling



455 FPT\_INC.1 TSF Integrity, provides the ability to verify the integrity of TSF data and TSF itself. This  
456 test may be performed at start-up, periodically, at the request of the authorised user, or when other  
457 conditions are met.

##### 458 Management FPT\_INC.1

- 459 a) management of the conditions under which TSF integrity checks occurs, such as during initial  
460 start-up, regular interval, or under specified conditions;
- 461 b) management of the time interval if appropriate.

##### 462 Audit: FPT\_INC.1

463 The following actions should be auditable if FAU\_GEN Security audit data generation is included in  
464 the PP/ST:

- 465 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: *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: *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: *parts of TSF*], TSF].



## 7 Statement of security requirements (ASE\_REQ.2)

466 This section defines the security functional requirements according to [CC\_Part2] and the security  
467 assurance requirements (SARs) from [CC\_Part3], which apply for the TOE.

### 7.1 Security functional requirements

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

#	User Data Protection (FDP)		
1.	FDP_ACC.1/AuditAccess	Subset control	access
2.	FDP_ACC.1/Admin	Subset control	access
3.	FDP_ACC.1/PolicyAdmin	Subset control	access
4.	FDP_ACC.1.1/AdminAccess	Subset control	access
5.	FDP_ACC.1.1/PolicyAdminAccess	Subset control	access
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
<b>Trusted path (FTP)</b>		
22.	FTP_TRP.1	Trusted path
<b>Identification and authentication (FIA)</b>		
23.	FIA_UAU.2	User authentication before any action
24.	FIA_UID.2	Timing of identification
<b>Cryptographic support (FCS)</b>		
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
<b>Security management (FMT)</b>		
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

469 The following styles of marking operations are applied:

- 470
- Assignments are denoted in **bold**.
  - 471 • Selections are marked in *italic underlined*.
  - 472 • Iterations are marked by adding a "/" and short name to the SFR identification.
  - 473 • Refinements indicating additions are marked in ***bold and italic underlined***.
  - 474 • Refinements indicating removals are marked as ~~crossed-out~~.

### 7.1.1.1 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 <b>audit access control SFP</b> on subjects and/or users having access to the audit trail of the TOE to perform the operations Read or Delete of <b>audit_records</b> .

*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 <b>admin access control SFP</b> on <b>subjects and/or users having access to the general configuration of the TOE to read configuration items.</b>

*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 <b>policy admin access control SFP</b> on <b>subjects and/or users having access to the rule set configuration of the TOE to read configuration items.</b>

*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.1 Security attribute based access control
FDP_ACC.1.1/Admin	The TSF shall enforce the <b>dual control admin SFP</b> on <b>subjects and/or users having access to change the general configuration of the TOE.</b>

*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 <b>dual control policy admin SFP</b> on <b>subjects and/or users having access to change the</b>

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 <b>audit access control SFP</b> to objects based on the following: <ol style="list-style-type: none"> <li><b>Subject and/or users: User trying to have access to the audit trail</b></li> <li><b>Object: audit trail</b></li> <li><b>Security Attributes: user role (notation: user_role)</b></li> </ol>
FDP_ACF.1.2/AuditAccess	The TSF shall enforce the following rules to determine if an operation among controlled <u>subjects and/or users</u> and controlled objects is allowed: <b>operation: read/delete audit_records</b> <b>condition: user_role = auditor.</b>
FDP_ACF.1.3/AuditAccess	The TSF shall explicitly authorise access of <u>subjects and/or users</u> to objects based on the following additional rules: <b>none.</b>
FDP_ACF.1.4/AuditAccess	The TSF shall explicitly deny access of <u>subjects and/or users</u> to objects based on the following additional rules: <b>none.</b>

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

*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	<p>The TSF shall enforce the <b>policy admin access control SFP</b> to objects based on the following:</p> <ol style="list-style-type: none"> <li>1. <b>Subject and/or users:</b> User trying to gain access to the configuration of TOE functionalities which automatically perform checks regarding the security level of a message.</li> <li>2. <b>Object:</b> TOE parameter of TOE functionalities which automatically perform checks regarding the security level of a message.</li> <li>3. <b>Security Attributes:</b> user role (notation: <code>user_role</code>).</li> </ol>

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

*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	<p>The TSF shall enforce the <b>dual control admin SFP</b> to objects based on the following:</p> <ol style="list-style-type: none"> <li>1. <b>Subject and/or users: User trying to modify the TOE general configuration</b></li> <li>2. <b>Object: general TOE configuration</b></li> <li>3. <b>Security Attributes: user role (notation: user_role).</b></li> </ol>
FDP_ACF.1.2/Admin	<p>The TSF shall enforce the following rules to determine if an operation among controlled <i><b>subjects and/or users</b></i> and controlled objects is allowed:</p> <p><b>operation: modify, add or delete general TOE configuration</b></p> <p><b>condition: The operation is performed by two different users with user_role = administrator.</b></p>
FDP_ACF.1.3/Admin	<p>The TSF shall explicitly authorise access of <i><b>subjects and/or users</b></i> to objects based on the following additional rules: <b>none.</b></p>

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 <b>check label SFP and data to low SFP</b> on <b>all data sent from the higher classified network to the lower classified network.</b>
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 <b>pre-filtering SFP</b> on <b>all labelled data sent from the higher classified network to the lower classified network before forwarded to the main filtering component of the TOE.</b>

*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 <b>supported protocol SFP</b> on <b>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.</b>
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 <b>clean protocol SFP</b> on <b>all protocol data sent from the higher classified network HIGH to the lower classified network LOW.</b>
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 <b>data validation SFP</b> on <b>all unlabelled data sent from the higher classified network to the lower classified network before forwarded to the main filtering component of the TOE.</b>
<b>FDP_IFF</b>	<b>Information flow control functions</b>
FDP_IFF.1/DataToLow	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	<p>The TSF shall enforce the <b>check label SFP and data to low SFP</b> based on the following types of <i><u>subjects and/or users</u></i> and information security attributes:</p> <p><b>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.</b></p>
FDP_IFF.1.2/DataToLow	<p>The TSF shall permit an information flow between a controlled <i><u>subjects and/or users</u></i> and controlled information via a controlled operation if the following rules hold:</p> <p><b>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.</b></p>
FDP_IFF.1.3/DataToLow	<p>The TSF shall enforce the following additional rules:</p> <p style="padding-left: 40px;"><b>If</b></p> <p style="padding-left: 80px;"><b>security_level_low.CONF not unambiguously determinable (netSPIF LOW not configured)</b></p> <p style="padding-left: 80px;"><b>or</b></p> <p style="padding-left: 80px;"><b>data_security_level not unambiguously determinable (malfunction of previous process step)</b></p> <p style="padding-left: 40px;"><b>Then</b></p> <p style="padding-left: 80px;"><b>No information flow is permitted</b></p>

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	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 <b>none</b> .
FDP_IFF.1.4/PreFilter	The TSF shall explicitly authorise an information flow based on the following rules: <b>none</b> .
FDP_IFF.1.5/PreFilter	The TSF shall explicitly deny an information flow based on the following rules: <b>none</b> .

*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 <b>supported protocol SFP</b> based on the following types of subject and information security attributes: <table border="1" data-bbox="663 1525 1351 1787"> <thead> <tr> <th>Subject</th> <th>Security Attribute</th> </tr> </thead> <tbody> <tr> <td>next_step.DATA</td> <td>-</td> </tr> <tr> <th>Information</th> <th>Security Attribute</th> </tr> <tr> <td>data_units.PROTOCOL</td> <td>protocol</td> </tr> </tbody> </table>	Subject	Security Attribute	next_step.DATA	-	Information	Security Attribute	data_units.PROTOCOL	protocol
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: <p><b>Operation: Forward data message to next_step.DATA</b></p> <p><b>Condition: data_units.PROTOCOL ∈ {supported.PROTOCOL}</b></p>								

*Application Note:*

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

FDP_IFF.1.3/Supported-Protocol	The TSF shall enforce the <b>none</b> .								
FDP_IFF.1.4/Supported-Protocol	The TSF shall explicitly authorise an information flow based on the following rules: <b>none</b> .								
FDP_IFF.1.5/Supported-Protocol	The TSF shall explicitly deny an information flow based on the following rules: <b>data_units.PROTOCOL</b> $\notin$ <b>{supported.PROTOCOL}</b> .								
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	<p>The TSF shall enforce the <b>clean protocol SFP</b> based on the following types of subject and information security attributes:</p> <table border="1"> <thead> <tr> <th>Subject</th> <th>Security Attribute</th> </tr> </thead> <tbody> <tr> <td>next_step.DATA</td> <td>-</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th>Information</th> <th>Security Attribute</th> </tr> </thead> <tbody> <tr> <td>data_units.PROTOCOL</td> <td>protocol</td> </tr> </tbody> </table> <p><b>Protocol data of the protocol data units which are sent from the higher classified network HIGH to the lower classified network LOW.</b></p>	Subject	Security Attribute	next_step.DATA	-	Information	Security Attribute	data_units.PROTOCOL	protocol
Subject	Security Attribute								
next_step.DATA	-								
Information	Security Attribute								
data_units.PROTOCOL	protocol								
FDP_IFF.1.2/CleanProtocol	<p>The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:</p> <p><b>Operation: forward data_units.PROTOCOL to next processing step next_step.DATA.</b></p> <p><b>Condition: no confidential information in protocol data.</b></p>								
FDP_IFF.1.3/CleanProtocol	The TSF shall enforce the <b>none</b> .								
FDP_IFF.1.4/CleanProtocol	The TSF shall explicitly authorise an information flow based on the following rules: <b>none</b> .								

FDP_IFF.1.5/CleanProtocol	The TSF shall explicitly deny an information flow based on the following rules: <b>none</b> .								
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	<p>The TSF shall enforce the <b>data validation SFP</b> based on the following types of subject and information security attributes:</p> <table border="1"> <thead> <tr> <th>Subject</th> <th>Security Attribute</th> </tr> </thead> <tbody> <tr> <td>Parser process</td> <td>-</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th>Information</th> <th>Security Attribute</th> </tr> </thead> <tbody> <tr> <td>Message</td> <td>data_label_type label_class_info rule_set_label_class_info data_security_label ICAP_class_info</td> </tr> </tbody> </table> <ol style="list-style-type: none"> <li>1. <b>Subject:</b> Internal parser processes of the TOE</li> <li>2. <b>Information:</b> Message to be validated against a labelled rule set.</li> <li>3. <b>Security Attributes</b> 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_security_label) or the classification information of Message is written into the ICAP header (ICAP_class_info) of Message.</li> </ol>	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
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								
FDP_IFF.1.2/Validation	<p>The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:</p> <p><b>(Message passes if</b></p> <p>[</p>								

```

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_info1
        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**.

<sup>1</sup> Attach a security label

FDP_IFF.1.5/Validation	The TSF shall explicitly deny an information flow based on the following rules: <b>none</b> .
<b>FDP_IFF</b>	<b>Information flow control functions</b>
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 <b>data to low SFP</b> to limit the capacity of <b>data flow capability from the higher classified network HIGH to the lower classified network LOW</b> to a <b>maximum capacity to be configured by the administrator of the TOE</b> .

### 7.1.2 Trusted path/channels (FTP)

<b>FTP_TRP</b>	<b>Trusted path</b>
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 <u>local, remote</u> users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from <u>modification, disclosure</u> .
FTP_TRP.1.2	The TSF shall permit <u>local users, remote users</u> to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for <b>user authentication, TOE management and audit review</b> .

*Application Note:*

*The TLS channel is established using the cryptographic library openssl, see [Crypt\_Filter]. The currently used TLS version is TLS 1.2.*

### 7.1.3 Identification and authentication (FIA)

<b>FIA_UAU</b>	<b>User authentication</b>
----------------	----------------------------



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 <i>privileged</i> user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
<b>FIA_UID</b>	<b>Timing of identification</b>
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 <i>privileged</i> 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 Administration before the privileged user can take any further TSF mediated action. The SDoT Administration is part of the TOE operational environment where the privileged user is authenticated and identified via its smartcard.*

#### 7.1.4 Cryptographic support (FCS)

<b>FCS_CKM</b>	<b>Cryptographic key management</b>
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 <b>EC key pair generation</b> and specified cryptographic key sizes <b>384 or 512 Bit</b> that meet the following: <b>SP800-56AR3</b> .
<b>FCS_CKM.2</b>	<b>Cryptographic key distribution</b>
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 <b>ECDHE</b> that meets the following: <b>IEEE 1363 (ECKAS-DH1)</b> .
<b>FCS_CKM.4</b>	<b>Cryptographic key destruction</b>
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]
<b>FCS_CKM.4.1</b>	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method <b>overwriting the key with zeros</b> that meets the following: <b>none</b> .
<b>FCS_COP</b>	<b>Cryptographic operation</b>
<b>FCS_COP.1/RSA</b>	<b>Cryptographic operation</b>
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]
<b>FCS_COP.1.1/RSA</b>	The TSF shall perform <b>digital signature verification</b> in accordance with a specified cryptographic algorithm <b>RSA</b> and cryptographic key sizes <b>between 2048 Bit and 8192 Bit</b> that meet the following: <b>RSASSA PKCS#1 as specified in RFC 3447</b> .
<b>FCS_COP.1/ECDSA</b>	<b>Cryptographic operation</b>
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]
<b>FCS_COP.1.1/ECDSA</b>	The TSF shall perform <b>digital signature verification</b> in accordance with a specified cryptographic algorithm <b>ECDSA</b> and cryptographic key sizes <b>256 Bit, 384 Bit and 512 Bit</b> 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 <b>encryption and decryption</b> in accordance with a specified cryptographic algorithm <b>AES in GCM mode</b> and cryptographic key sizes <b>128 Bit and 256 Bit</b> that meet the following: <b>FIPS 197 and SP800-38D</b> .
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 <b>hash-based message authentication code</b> in accordance with a specified cryptographic algorithm <b>HMAC-SHA-384, SHA-256</b> , and cryptographic key sizes <b>384 Bit and 256 Bit</b> that meet the following: <b>RFC 2104</b> .
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 <b>digest computation</b> in accordance with a specified cryptographic algorithm <b>SHA-2</b> and cryptographic key sizes <b>256 Bit, 384 Bit and 512 Bit</b> that meet the following: <b>FIPS 180-4</b> .

## 7.1.5 Security management (FMT)

<b>FMT_MSA</b>	<b>Management of security attributes</b>
FMT_MSA.1	Management of security attributes
Hierarchical to:	No other components
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MSA.1.1	The TSF shall enforce the <b>dual control policy admin SFP</b> to restrict the ability to <b>query, modify, delete</b> the security attribute <b>of the rule set to the policy admin</b> .
<b>FMT_MSA.3</b>	<b>Static attribute initialisation</b>
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 <b>dual control admin SFP, dual control policy admin SFP, data validation SFP, check label SFP, supported protocol SFP, clean protocol SFP</b> to provide <i>restrictive</i> default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow <del>the</del> <b>no one</b> to specify alternative initial values to override the default values when an object or information is created.
<b>FMT_MTD</b>	<b>Management of TSF data</b>
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 <i>modify</i> the <b>general TOE configuration data to administrators of the TOE</b> .
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 <b>access</b> the <b>audit trail</b> to <b>auditors</b> .
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 <b>delete or move</b> the <b>audit data</b> to <b>auditors</b> .
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 <b>modify</b> the <b>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</b> .
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 <b>the general TOE configuration data</b> .
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:  <b>The general TOE configuration management:</b>

- 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.*

<b>FMT_SMR</b>	<b>Security management roles</b>
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: <b>policy-admin, administrator and auditor.</b>
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 <b>administrator and auditor roles are strictly separated, without possibility of simultaneously logged in administrator and auditor user,</b> 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)

<b>FPT_STM</b>	<b>Time stamp</b>
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.*

<b>FPT_INC</b>	<b>TSF integrity checks</b>
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 <i>during initial start-up, periodically during normal operation</i> to demonstrate the integrity of <b>general configuration data, rule sets, SPIF, NetSPIF, and stored TSF executable code.</b>
FPT_INC.1.2	The TSF shall provide authorised users with the capability to verify the integrity of <b>general configuration data, rule sets, SPIF, and NetSPIF.</b>

FPT_INC.1.3	The TSF shall provide authorised users with the capability to verify the integrity of <b>stored TSF executable code</b> .
<b>FPT_TDC</b>	<b>Inter-TSF TSF data consistency</b>
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 <b>security labels with its classification</b> when shared between the TSF and another trusted IT product.
FPT_TDC.1.2	The TSF shall use <b>check label SFP</b> when interpreting the TSF data from another trusted IT product.

### 7.1.7 Security audit (FAU)

<b>FAU_ARP</b>	<b>Security audit automatic response</b>
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 <b>the following actions</b> : <ul style="list-style-type: none"> <li>- <b>send an e-mail to a configurable list of recipients</b></li> <li>- <b>report into the audit-trail</b></li> <li>- <b>place an indicator of any potential security violation on the Audit GUI</b></li> <li>- <b>enter the maintenance mode</b></li> </ul> upon detection of a potential security violation.
<b>FAU_GEN</b>	<b>Security audit data generation</b>
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:



FAU\_GEN.1.2

- a) Start-up and shutdown of the audit functions;
- b) All auditable events for *not Specified* level of audit; and
- c) **See Table 26.**

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.*

<i>Auditable events in the TOE</i>	<i>Available information in audit record</i>
<i>Changes to the TOE configuration and parameters</i>	<p><i>Value of changed TOE configuration and parameter before and after the change was made, i.e.</i></p> <ul style="list-style-type: none"> <li>- <i>start and stop of the TOEs system</i></li> <li>- <i>change of operation mode</i></li> <li>- <i>administration activities</i></li> <li>- <i>authentication against the TOE</i></li> </ul>
<i>Processing messages data</i>	<p><i>The following audit data are recorded while processing the data of a message:</i></p> <ul style="list-style-type: none"> <li>- <i>origin,</i></li> <li>- <i>destination,</i></li> <li>- <i>time of transfer,</i></li> <li>- <i>result of the filter decision,</i></li> <li>- <i>the data which can uniquely identify the message.</i></li> </ul>
<i>Rejecting messages data</i>	<p><i>complete data message;</i> <i>Note: this is configurable, and the default configuration is "no message data"</i></p>

*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.
<b>FAU_SAA</b>	<b>Security audit analysis</b>
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 <b>auditable events</b> : - <b>Underflow of audit storage capacity</b> - <b>Exceeding the set bandwidth</b> - <b>Upcoming expiration of certificates</b> - <b>Errors during self-tests.</b> known to indicate a potential security violation; b) <b>none</b>
<b>FAU_SAR</b>	<b>Security audit review</b>
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 <b>auditors</b> with the capability to read <b>all audit information</b> 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.
<b>FAU_SAR.2</b>	<b>Restricted audit review</b>

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.
<b>FAU_STG</b>	<b>Security audit event storage</b>
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 <i>prevent</i> 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 <b>all</b> stored audit records will be maintained when the following conditions occur: <u>audit storage exhaustion, failure, attack</u>
<b>FAU_STG.3</b>	<b>Action in case of possible audit data loss</b>
Hierarchical to:	No other components
Dependencies:	FAU_STG.1 Protected audit trail storage
FAU_STG.3.1	The TSF shall <b>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</b> if the audit trail exceeds <b>80% of the total capacity of the audit trail storage device</b> .
<b>FAU_STG.4</b>	<b>Prevention of audit data loss</b>
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 <u>prevent audited events, except those taken by the authorised user with special rights</u> and <b>inform a configurable list of</b>

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

475 The dependency rationale for Security Functional Requirements shows that the basis for mutual  
476 support including the internal consistency between in sec. 7.1 defined Security Functional  
477 Requirements are satisfied. The following table provides an overview showing that all dependencies  
478 between the chosen Security Functional Components are analysed, and non-dissolved  
479 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.
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]	Fulfilled by FCS_COP.1/ECDSA and FCS_CKM.4

#	SFR	Dependencies	Support of the Dependencies
		FCS_CKM.4 Cryptographic key destruction	
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.
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

#	SFR	Dependencies	Support of the Dependencies
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
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

#	SFR	Dependencies	Support of the Dependencies
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
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	Fulfilled by FAU_STG.3 Fulfilled by FAU_STG.2

#	SFR	Dependencies	Support of the Dependencies
		FAU_STG.1 Protected audit trail storage	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

480 The assurance level for evaluation of the TOE, its life cycle and operating environment are chosen  
481 as the pre-defined assurance level EAL4 augmented with the following assurance component in  
482 accordance with [CC\_Part3]:

- 483 • ALC\_FLR.2 Flaw reporting procedures.

484 This corresponds to a total assurance level EAL4+.

485 The Level EAL4 augmented with ALC\_FLR.2 was chosen to permit INFODAS GmbH as a developer  
486 to gain maximum assurance from positive security engineering based on good commercial  
487 development practices which, though rigorous, do not require substantial specialist knowledge,  
488 skills, and other resources. EAL4 is the highest level at which it is likely to be economically to retrofit  
489 the existing product line of INFODAS GmbH.

490 The selection of the component ACL\_FLR.2 provides additional assurance of the TOE that potential  
491 security flaws can be tracked and corrected by the developer.

492 Augmented assurance components are marked in **bold** in the following table:

Assurance class	Assurance Family	Assurance Component
<b>Development</b>	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
<b>Guidance documents</b>	AGD_OPE	AGD_OPE.1 Operational user guidance
	AGD_PRE	AGD_PRE.1 Preparative procedures
<b>Life-cycle support</b>	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.3 Focused vulnerability analysis

Table 28 Security Assurance Requirements (SARs)

## 7.4 Security Functional Requirements Rationale

493 The following subsections provide an overview regarding the coverage of Security Objectives for the TOE by Security Functional Requirements and a rationale of the  
494 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

495 OT.FILTER is fulfilled by FDP\_IFC.1/DataToLow and FDP\_IFF.1/DataToLow. These SFRs make sure  
496 that only data which comply to the data to low SFP are possible to be sent from the higher classified  
497 network to the lower classified network. Further, FPT\_TDC.1 ensures the consistent interpretation  
498 of security labels sent between the TOE and other trusted IT systems.

#### 7.4.2 OT.PRE\_FILTER

499 The security objective OT.PRE\_FILTER are addressed by FDP\_IFC.1/PreFilter, FDP\_IFF.1/PreFilter  
500 which enforce the pre-filtering SFP and assure that only message data corresponding to  
501 configurable pre-conditions are forwarded to the main filtering component of the TOE. FMT\_SMF.1  
502 provides administrators to configure the pre-filtering conditions used by OT.PRE\_FILTER.

#### 7.4.3 OT.LABELS

503 FDP\_IFC.1/Validation and FDP\_IFF.1/Validation ensure that the TOE checks the strong bound of a  
504 security label to the corresponding message data. FDP\_IFC.1/Validation and FDP\_IFF.1/Validation  
505 provide the test strategy which must be performed before a security label is attached to the data.  
506 FMT\_MSA.1 provides a restriction regarding the manual labelling mechanism. FMT\_SMF.1 ensures  
507 that configuration mechanisms to set the rules for automatic labelling of the TOE are provided.

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

515 FCS\_COP.1/RSA, FCS\_COP.1/ECDSA and FCS\_COP.1/SHA2 provide the cryptographic operation  
516 for checking the security label whether it corresponds to OT.LABELS.

#### 7.4.4 OT.SANITISED\_DATA

517 FDP\_IFC.1/CleanProtocol and FDP\_IFF.1/CleanProtocol are addressing OT.SANITISED\_DATA by  
518 enforcing the TOE to apply clean protocol SFP, and assure that data which is categorised to be  
519 confidential, is not sent to the lower classified network.

520 Further, OT.SANITISED\_DATA is addressed by FDP\_IFC.1/Validation and FDP\_IFF.1/Validation by  
521 enforcing the data validation SFP, which controls the internal parser process of the TOE.

#### 7.4.5 OT.BANDWIDTH

522 This security objective is directly required to be fulfilled by FDP\_IFF.3 and FDP\_IFF.1/DataToLow.  
523 Further, FMT\_SMF.1 directly requires the TOE to provide mechanisms to set up the bandwidth  
524 limits.

#### 7.4.6 OT.PROTOCOLS

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

527 ensured by the TSF according to the SFRs FDP\_IFC.1/Supported-Protocol and  
528 FDP\_IFF.1/Supported-Protocol.

#### 7.4.7 OT.PROTOCOL\_DENY

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

531 FDP\_IFC.1/Supported-Protocol and FDP\_IFF.1/Supported-Protocol enforces the supported  
532 protocol SFP to ensure that all attempts to build up a connection with different protocol types other  
533 than listed in OT.PROTOCOLS will be denied by the TSF.

#### 7.4.8 OT.USER\_AUTHENTICATION

534 The security objective OT.USER\_AUTHENTICATION aims to ensure that all users of the TOE are  
535 authenticated before any other action can be performed.

536 This objective is mainly achieved by FIA\_UID.2 and FIA\_UAU.2 which require that all users are  
537 identified and authenticated considering the application note in FIA\_UID.2.

#### 7.4.9 OT.ROLE\_SEPARATION

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

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

543 FMT\_MTD.1/AuditAccess, FMT\_MTD.1/AuditDelete, FDP\_ACF.1/AuditAccess,  
544 FDP\_ACC.1/AuditAccess with FAU\_SAR.2 achieve the security objective by assuring that only the  
545 role of the auditor is able to read or delete audit records from the audit trail.

546 FMT\_MTD.1/Admin, FMT\_MTD.1/PolicyAdmin, FDP\_ACC.1/Admin, FDP\_ACF.1/Admin,  
547 FDP\_ACC.1/PolicyAdmin, FDP\_ACF.1/PolicyAdmin, FDP\_ACC.1/AdminAccess,  
548 FDP\_ACF.1/AdminAccess, FDP\_ACC.1/PolicyAdminAccess, and FDP\_ACF.1/PolicyAdminAccess  
549 achieve the security objective by assuring that only the role of the respective policy-/administrator  
550 is able to read or delete/modify rule sets/general TOE configuration data.

#### 7.4.10 OT.FOUR\_EYES

551 This objective is achieved by the combination FDP\_ACF.1/Admin and FDP\_ACC.1/Admin resp.  
552 FDP\_ACF.1/PolicyAdmin and FDP\_ACC.1/PolicyAdmin. Beforementioned SFRs ensure that the  
553 dual control admin SFP, dual control policy admin SFP, FDP\_ACC.1/AdminAccess,  
554 FDP\_ACF.1/AdminAccess, FDP\_ACC.1/PolicyAdminAccess, and FDP\_ACF.1/PolicyAdminAccess  
555 are enforced by the TOE.

556 FMT\_MTD.1/Admin and FMT\_MTD.1/PolicyAdmin that only the administrator resp. the policy-  
557 admin can make the corresponding change.

#### 7.4.11 OT.SECURE\_CHANNEL

558 This objective aims that the TOE can establish a secure communication channel and is directly  
559 addressed by FTP\_TRP.1.

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

#### 7.4.12 OT.AUDIT\_CHANGE\_LOG

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

#### 7.4.13 OT.AUDIT

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

#### 7.4.14 OT.AUDIT\_PROTECT

576 This security objective is achieved by FMT\_MTD.1/AuditDelete which ensures that only the auditor  
577 can delete or move audit records from the audit trail. FAU\_STG.2 provides the protection of stored  
578 audit records from modification and from unauthorised removal from the audit trail. Further,  
579 FAU\_STG.2 requires that stored audit records are maintained if the audit storage is full or a failure  
580 of the storage occurs.

581 FCS\_COP.1/HMAC and FCS\_COP.1/AES address the cryptographic algorithms used to protect the  
582 integrity and confidentiality of the audit records.

583 FAU\_STG.3 and FAU\_STG.4 reduce the risk of losing audit records by providing alerting  
584 mechanisms to be able to detect exhaustions of the storage.

#### 7.4.15 OT.AUDIT\_LOG\_AVAILABILITY

585 This security objective aims to provide the audit data to authorised auditors. This is achieved by  
586 FDP\_ACC.1/AuditAccess and FDP\_ACF.1/AuditAccess which require that only auditors have access  
587 to audit records. Further, FAU\_SAR.1 requires that the TOE provides mechanisms that auditors can  
588 read the audit records and FAU\_SAR.2 ensures that only users who have been granted access have  
589 read access to the records.

#### 7.4.16 OT.PROTECTION

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

593 FPT\_INC.1 provides mechanisms to perform integrity checks and detect malicious code or  
594 misconfigured TOE configuration.

595 FMT\_SMF.1 ensures that management functions are provided to set the TOE into maintenance  
596 mode/operational mode.

597 FDP\_ACF.1/Admin and FDP\_ACC.1/Admin, together, assure that any change to general  
598 configuration parameter has to be done by two administrators with dual control technique. In  
599 addition, FMT\_MTD.3 ensures that only secure values are accepted for general TOE configuration  
600 data.

#### **7.4.17 OT.INIT**

601 OT.INIT has the objective that after initialisation process the TOE is constantly in a secure state. The  
602 SFRs FDP\_IFC.1/DataToLow and FDP\_IFF.1/DataToLow fulfil this objective by enforcing the data  
603 to low SFP. FAU\_ARP.1, enables the TOE to detect potential insecure states, and if so, enter the  
604 maintenance mode.

#### **7.4.18 OT.DEFAULT**

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

#### **7.4.19 OT.WARNING**

610 The objective of OT.WARNING is that when a security relevant event was detected, the TSF sends  
611 warnings to the user. FAU\_SAA.1 and FAU\_ARP.1 assure that the TSF monitors audited events in  
612 accordance with the defined set of rules. The auditor will be informed when potential security  
613 violating acts were monitored. FMT\_SMF.1 assures the configuration capability of the addressees  
614 of the warning notification.



## 8 TOE Summary Specification (ASE\_TSS.1)

615 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

616 The TOE provides mechanisms to perform labelling tasks. The following describes the main security  
617 properties of SF\_LBL.

##### 8.1.1.1 SF\_LBL.1

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

621 The supported formats are XML, ADEXP, FSD, ASTERIX, FORMDATA, and JSON. All other formats  
622 will be rejected by the TOE.

##### 8.1.1.2 SF\_LBL.2

623 The security labels have a strong binding to the corresponding data. Any modification of the data or  
624 the related security label will invalidate both data and security label. This will lead to a rejection and  
625 the data will not pass the TOE. This feature is achieved with XML signatures which are following  
626 strict rules in terms of syntax and processing mechanisms, see [XML\_SYN].The structure of the  
627 security label is based on the NATO standard (see [ADaTP\_4774], [ADaTP\_4778]).

##### 8.1.1.3 SF\_LBL.3

628 The TOE provides configuration mechanisms to define the parameters regarding the automatic  
629 labelling of the message data, in the case where a labelling generation is initiated by the TOE, with  
630 cryptographic support of the HSM. The HSM is part of the delivery of the SDoT Security Gateway  
631 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

632 The security function SF\_LBL addresses the requirements of the following SFRs:  
633 FDP\_IFF.1/Validation Subset access control, FDP\_IFC.1/DataToLow Subset information flow  
634 control, FDP\_IFF.1/DataToLow Simple security attributes, FDP\_IFF.1/Validation Security attribute  
635 based access control, Security attribute based access control, FMT\_SMF.1 Specification of  
636 Management Functions, FCS\_COP.1/ECDSA, FCS\_COP.1/RSA and FCS\_COP.1/SHA2.

#### 8.1.2 SF\_FR: Filtering Mechanism

637 The TOE provides filtering mechanisms which is the main security functionality of the TOE. The  
638 following subsections will describe the main security properties of SF\_FR.

#### 8.1.2.1 SF\_FR.1

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

#### 8.1.2.2 SF\_FR.2

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

#### 8.1.2.3 SF\_FR.3

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

#### 8.1.2.4 SF\_FR.4

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

#### 8.1.2.5 SF\_FR.5

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

#### 8.1.2.6 SF\_FR.6

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

#### 8.1.2.7 SFRs addressed by SF\_FR

657 The security function SF\_FR addresses the requirements of the following SFRs:  
658 FDP\_IFC.1/DataToLow Subset information flow control, FDP\_IFC.1/PreFilter Subset information  
659 flow control, FDP\_IFC.1/Supported-Protocol Subset information flow control,  
660 FDP\_IFF.1/DataToLow Simple security attributes, FMT\_SMF.1 Specification of Management  
661 Functions, FDP\_IFF.1/PreFilter Simple security attributes, FPT\_TDC.1 Inter-TSF basic TSF data  
662 consistency, and FDP\_IFF.1/Supported-Protocol Simple security attributes.

### 8.1.3 SF\_CP: Channel Protection

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

### 8.1.3.1 SF\_CP.1

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

### 8.1.3.2 SF\_CP.2

668 The TOE controls the bandwidth which can be configured by the operator of the TOE. The TOE will  
669 then block all incoming and outgoing connections, if these exceed the configured bandwidth. The  
670 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

671 The security function SF\_CP addresses the requirements of the following SFRs:  
672 FDP\_IFC.1/CleanProtocol Subset information flow control, FDP\_IFF.1/DataToLow Simple security  
673 attributes, FDP\_IFF.1/CleanProtocol Simple security attributes, FDP\_IFF.1/CleanProtocol Subset  
674 information flow control, FDP\_IFF.3 Limited illicit information flows, and FMT\_SMF.1 Specification  
675 of Management Functions.

### 8.1.4 SF\_DP: Data Protection

676 The TOE includes the following security functions to provide data protection mechanisms.  
677 The TOE enforces check label SFP on all data messages with attached external security labels. In a  
678 first step security labels are extracted from the data message for all data coming from the higher  
679 classified network. In a next step the TOE imports a message with security label if the following  
680 holds:

#### 8.1.4.1 SFRs addressed by SF\_DP

681 The security function SF\_DP addresses the requirements of the following SFRs:  
682 FDP\_IFC.1/DataToLow Subset information flow control, FDP\_IFF.1/DataToLow Simple security  
683 attributes

### 8.1.5 SF\_AA: Authentication and Authorisation

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

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

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

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

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

704 **Note:** The TLS channel is established using the cryptographic library openssl, see [Crypt\_Filter].  
705 The currently used TLS version is TLS 1.2. SFRs addressed by SF\_AA

706 FAU\_SAR.2 Restricted audit review, FDP\_ACC.1/AuditAccess Subset access control,  
707 FDP\_ACC.1/Admin Subset access control, FDP\_ACC.1/PolicyAdmin Subset access control,  
708 FDP\_ACC.1/AdminAccess Subset access control, FDP\_ACC.1/PolicyAdminAccess Subset access  
709 control, FDP\_ACF.1/AuditAccess Security attribute based access control, FDP\_ACF.1/AdminAccess  
710 Security attribute based access control, FDP\_ACF.1/PolicyAdminAccess Security attribute based  
711 access control, FDP\_ACF.1/Admin Security attribute based access control,  
712 FDP\_ACF.1/PolicyAdmin Security attribute based access control, FDP\_IFF.1/DataToLow Simple  
713 security attributes, FIA\_UAU.2 User authentication before any action, FIA\_UID.2 Timing of  
714 identification, FMT\_MSA.1, Management of security attributes, FMT\_MTD.1/Admin Management of  
715 TSF data, FMT\_MTD.1/AuditAccess Management of TSF data, FMT\_MTD.1/AuditDelete  
716 Management of TSF data, FMT\_MTD.1/PolicyAdmin Management of TSF data, FMT\_SMF.1  
717 Specification of Management Functions, FTP\_TRP.1 Trusted path , FMT\_SMR.2 Restriction on  
718 security roles, FTP\_TRP.1Trusted Path FCS\_CKM.1/ECDSA, , FCS\_COP.1/AES,  
719 FCS\_COP.1/ECDSA, FCS\_COP.1/RSA and FCS\_COP.1/SHA2.

### 8.1.6 SF\_AT: Audit Trail

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

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

- 723 a. The TOE sends an e-mail to a configurable list of addressees
- 724 b. Generates an audit entry into the audit trail
- 725 c. Indicates the potential security violation on the audit GUI

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

#### 8.1.6.1 Auditable Events

730 In the following, the main auditable events are listed.

- 731 • Not available in ST-Lite version

#### 8.1.6.2 SFRs addressed by SF\_AT

732 FAU\_ARP.1 Security audit automatic response, FAU\_GEN.1 Audit data generation, FAU\_GEN.2 User  
733 identity association, FAU\_SAA.1 Potential violation analysis, FAU\_SAR.1 Audit review, FAU\_SAR.2

734 Restricted audit review, FAU\_STG.2 Guarantees of audit data availability, FAU\_STG.3 Action in case  
 735 of possible audit data loss, FAU\_STG.4 Prevention of audit data loss, FDP\_ACC.1/AuditAccess  
 736 Subset access control, FDP\_IFF.1/DataToLow Simple security attributes, FDP\_IFF.3 Limited illicit  
 737 information flows, FIA\_UAU.2 User authentication before any action, FIA\_UID.2 Timing of  
 738 identification, FMT\_MSA.1 Management of security attributes, FMT\_MSA.3 Static attribute  
 739 initialisation, FMT\_MTD.1/AuditAccess, Management of TSF data, FMT\_MTD.1/AuditDelete,  
 740 Management of TSF data, FMT\_SMF.1 Specification of Management Functions, FMT\_SMR.2  
 741 Restriction on security roles, FPT\_STM.1 Reliable time stamps, FCS\_COP.1/HMAC,  
 742 FCS\_COP.1/SHA2 and FCS\_COP.1/AES.

### 8.1.7 SF\_SP: Self Protection

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

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

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

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

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

- 761 • software failure
- 762 • hardware failure
- 763 • power outage
- 764 • out of memory error
- 765 • audit trail full

#### 8.1.7.1 SFRs addressed by SF\_SP

766 FDP\_ACC.1/Admin Subset access control, FDP\_ACF.1/Admin Security attribute based access  
 767 control, FDP\_IFF.1/DataToLow Simple security attributes, FMT\_MSA.3 Static attribute initialisation,  
 768 FMT\_MTD.1/Admin Management of TSF data, FPT\_INC.1 TSF integrity, FMT\_MTD.3 Secure TSF  
 769 data, and FMT\_SMF.1 Specification of Management Functions.

## 8.2 TOE Summary Specification Rationale

770 The following table provides an overview of the demonstration in 8.1 regarding the coverage of the  
771 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, SF_AA
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

### 772 Criteria and methodology interpretation

773 [CC\_Part1] Common Criteria for Information Technology Security Evaluation, Part 1:  
774 Introduction and general model, Version 3.1, Revision 5, April 2017, CCMB-  
775 2017-04-002

776 [CC\_Part2] Common Criteria for Information Technology Security Evaluation, Part 2:  
777 Security functional components, Version 3.1, Revision 5, April 2017,  
778 CCMB-2017-04-002

779 [CC\_Part3] Common Criteria for Information Technology Security Evaluation, Part 3:  
780 Security assurance components, Version 3.1, Revision 5, April 2017,  
781 CCMB-2017-04-003

782 [CEM] Common Criteria for Information Technology Security Evaluation,  
783 Evaluation methodology, Version 3.1, Revision 5, April 2017, CCMB-2017-  
784 04-00

785 [AIS\_41] Application Notes and Interpretation of the Scheme (AIS), AIS 41, Version  
786 2, 31.01.11, Certification body of the BSI in the context of the certification  
787 scheme

788 [AIS\_35] Application Notes and Interpretation of the Scheme (AIS), AIS 35, Version  
789 2, 12.11.11, Öffentliche Fassung eines Security Target (ST-lite)

790 [MC\_ST\_LITE] Common Criteria Recognition Arrangement, Management Committee,  
791 Policies and Procedures, ST sanitising for publication, Version 1.0, April  
792 2006, CCDB-2006-04-004

### 793 Technical references

794 [Crypt\_Filter] SDoT Filter, Cryptographic Mechanisms, V0.5, 06.08.2019, INFODAS  
795 GmbH

796 [Kon\_Label] SDoT Produktfamilie International - Konzeptpapier zum Labelling, V0.3,  
797 10.09.2019, INFODAS GmbH

798 [Kon\_Filter] SDoT Security Gateway International, Konzeptpapier Filtermechanismen,  
799 V0.3, 16.08.2019, INFODAS GmbH

800 [ADaTP\_4774] „Confidentiality Metadata Label Syntax“, Edition A Version 1, Dec 2017,  
801 NATO STANDARDIZATION Organization

802 [ADaTP\_4778] „Metadata Binding Mechanism“, Edition A Version 1, Oct 2018, NATO  
803 STANDARDIZATION Organization

804 [RFC3986] IETF RFC 3986, “Uniform Resource Identifier (URI): Generic Syntax”, at  
805 <http://tools.ietf.org/html/rfc3986>

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

807 [XML\_SYN] World Wide Web Consortium standard 'XML Signature Syntax and  
808 Processing Version 1.1', W3C Recommendation 11 April 2013, at  
809 <http://www.w3.org/TR/xmlsig-core1/>



810 [XML\_SPEC] Extensible Markup Language (XML) 1.0 (Fifth Edition) W3C  
811 Recommendation, 26 November 2008, <http://www.w3.org/TR/xml/>.