SDoT SDD
Security Target Lite

Document name:	SDoT_SDDv1.3i_SecurityTargetLite
Document version:	V 1.1
Version date:	06.11.2024
Author:	INFODAS GmbH
Number of pages:	87
DMS Version	0.10

Issued by: INFODAS GmbH
Rhonestraße 2
50765 Cologne, Germany

Table of Contents

List of Figures

List of Tables

Abbreviations

ASE	**A**ssurance Class in the CC Standard referring to the **S**ecurity Target **E**valuation
CA	Certification Authority
CC	Common Criteria for Information Technology Security Evaluation
CCL	Refers to the assurance family "**C**onformance **cl**aims" in the assurance class ASE
CEM	Common Criteria for Information Technology Security Evaluation, Evaluation methodology
CPU	Central Processing Unit
DVD	Digital Versatile Disc
EAL	Evaluation Assurance Level
FAU	SFRs belonging to the **f**unctional class "Security **Au**dit"
FCO	SFRs belonging to the **f**unctional class "**Co**mmunication"
FDP	SFRs belonging to the **f**unctional class "User **D**ata **P**rotection"
FIA	SFRs belonging to the **f**unctional class "**I**dentification and **a**uthentication"
FMT	SFRs belonging to the **f**unctional class "Security **m**anagemen**t**"
FPT	SFRs belonging to the **f**unctional class "**P**rotection of the **T**SF"
FSD	Field Structured Data
FW	Firmware
GUI	Graphical User Interface
HDD	Hard Disk Drive
HMAC	Hash Message Authentication Code
HTTP / S	Hypertext Transfer Protocol / Secure
HW	Hardware
/ICAP	Internet Content Adaptation Protocol

INT	Refers to the assurance family "ST introduction" of the assurance class ASE
IP	Internet Protocol
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
NTP	Network Time Protocol
OBJ	Refers to the assurance family "Security objectives" of the assurance class ASE
OSP	Organisational Security Policy
RAM	Random Access Memory
REQ	Refers to the assurance family "Security requirements" of the assurance class ASE
RNG	Random Number Generator
RTF	Rich Text Format
SAR	Security Assurance Requirement
SDoT	Security Inter-Domain Transition
SFP	Security Function Policy
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SMTP MTA	SMTP Message/Mail Transfer Agent
SPD	Refers to the assurance family "Security problem definition" of the assurance class ASE
SSD	Solid State Drive
ST	Security Target
SW	Software

TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
TSS	Refers to the assurance family "**T**OE **s**ummary **s**pecification" of the assurance class ASE
UDP	User Datagram Protocol
UEFI	Unified Extensible Firmware Interface

General

Revision History:

Version	Date	Application Note	Author
V 1.0	26.08.2024	First Release of lite version based on full ST in accordance with [AIS_35] and supporting document [MC_ST_LITE].	INFODAS GmbH
V 1.1	06.11.2024	Update with changes based on comments from BSI.	INFODAS GmbH

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. Some information in TOE overview
3 and in TOE description contain confidential information which are reduced in the public version of
4 this security target (ST Light). This security target was created considering of BSI.

1.1 ST Reference

5 **Title:** SDoT SDD Security Target Lite

6 **Version:** V 1.1

7 **Date:** 06.11.2024

8 **Author:** INFODAS GmbH

1.2 TOE reference

9 **Product name:** SDoT SDD (SDoT Software Data Diode)

10 **TOE name (long)**: SDoT SDD SW

11 **TOE name (short):** SDoT SDD

12 **TOE version**: 1.3i

13 **Developer name**: INFODAS GmbH

14 **Certification ID:** BSI-DSZ-CC-1193

1.3 TOE overview

15 The TOE version 1.3i refers to the use case for the deployment to the international free market.
16 Hereby, 1.3i describes a mnemonic convention which exact configuration is identified as the
17 following revision: 1.3.1360.33832 P3. This version number is equivalent to 1.3.3.1360.33832. This
18 Security Target defines the security objectives for, and security requirements of the SDoT SDD of
19 INFODAS GmbH. Further, this security target defines the security objectives of the operational
20 environment for the TOE. The following subsections give an overview of the TOE, its usage and major
21 security features, the TOE type, and lists all required non-TOE Hardware, non-TOE
22 Software/Firmware.

1.3.1 TOE definition and operational usage

23 The SDoT SDD belongs to the SDoT Cross Domain Solution product family of INFODAS GmbH. The
24 SDoT SDD serves as boundary protection device between IP Networks with different demands on
25 the level of protection needed. These two IP networks are identified as Source (SRC) and Destination
26 (DST). The SDoT SDD ensures that there is no data leakage from DST to SRC but data from SRC to
27 DST can always pass the TOE.

28 Originally, the terms Source and Destination were identified as LOW and HIGH for protection of
29 sensitive information in the higher classified network HIGH. In a high-level view, however, the terms
30 SRC for identifying the network LOW and DST for describing the network HIGH is used.

The reason for re-defining the terms used is that the use case of a unidirectional system will not be restricted in only one direction. The SDoT SDD can be used for the use case that no sensitive data unintentionally flow out of systems to be protected, as well as for the use case that malicious code unintentionally flows into the system to be protected. An example of the latter could be industrial plants that is able to export system data but are not allowed to inject anything malicious unintentionally.

The SDoT SDD is technologically realized on basis of the SDoT Security Gateway, which was recently certified through the CC-evaluation. The SDoT Security Gateway already can function as a diode. The already proven technology in the SDoT Security Gateway also provides several security mechanisms of the SDoT Diode.

As it is shown in Figure 1, the product SDoT SDD comprises the:

1. SDoT SDD Platform (HW with Crypto Unit, FW, OS),
2. SDoT SDD SW covering the software and compartment allocation of the OS, or in the short form SDoT SDD which is the TOE and
3. SDoT Adminstation.

More information about the non-TOE parts of SDoT SDD will be given in 1.3.4. Therefore, the TOE is an application delivered together with a set of software and hardware components to the customer. The underlying micro kernel operating system with its separation mechanism is part of the TOE environment. Nonetheless, the configuration and type of usage of the separation mechanism of the L4 micro kernel OS is part of the security assessment. All hardware and software which are needed to securely operate the TOE in accordance with the TOE assumptions, and in accordance with the assumptions of the TOE operational environment, are in scope of delivery, see Table 3. The hardware parts and software parts besides the TOE are partially customized for SDoT SDD to ensure that the TOE operates properly as intended with the dedicated delivery parts only.

It is the nature of communication protocols that some protocol responses must be allowed. Simple HTTP responses regarding the status code of HTTP requests from SRC must be sent back by DST interface. These responses are analysed and sanitised by the TOE, so that the response code does not contain any confidential information. SMTP responses to SMTP emails coming from SRC are also analysed and, if required, sanitised.

The protocols TCP and UDP do not transfer any protocol responses from DST to SRC. In case of TCP, the connection of the TCP sender terminates at the SRC network interface of the TOE. The SRC interface of the TOE acknowledges local receipt of data by sending an ACK-package to the TCP sender after an ACK-package was received from DST.

The TOE can synchronise its system time with a target server in DST. From the other side, a system in SRC can directly synchronise its system time with the TOE. That means the system in SRC and the target server in DST can synchronise its time via the TOE without direct connection.

The TOE only accepts connection attempts coming from SRC. Hence, the TOE ensures that only unidirectional data flow from SRC to DST is possible. Any connection attempt from DST is blocked by the TOE. This leads to the main security function of the TOE that any information flow of payload data from DST to SRC is not possible.

1.3.2 Major Security Features of the TOE

In short, the major security function of the TOE is to provide the mechanism that no data flow from DST to SRC is possible. During all kind of data transfer from SRC to DST, no data or information located in DST may flow to SRC.

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

The TOE includes six compartments for different purposes. These are:

- DI_GUI,
- DI_HGH,
- DI_CFG,
- DI_L2H,
- DI_LOW, and
- DI_ADT.

The security mechanisms of the TOE are implemented on the compartments DI_GUI, DI_CFG, and DI_ADT. The TOE collects and checks audit data to identify and provides audit data protection mechanisms. The TOE performs management functions on configuration data in DI_CFG. Authentication of administrators and auditor of the TOE is provided by the DI_GUI which communicates via secure TLS connection to the SDoT Adminstation. Cryptographic Key Generation and Key Storage are provided by a certified Crypto Unit. However, the secure TLS connection itself and the certified Crypto Unit are not scope of the current TOE. The following figure depicts the TOE with its IT environment.

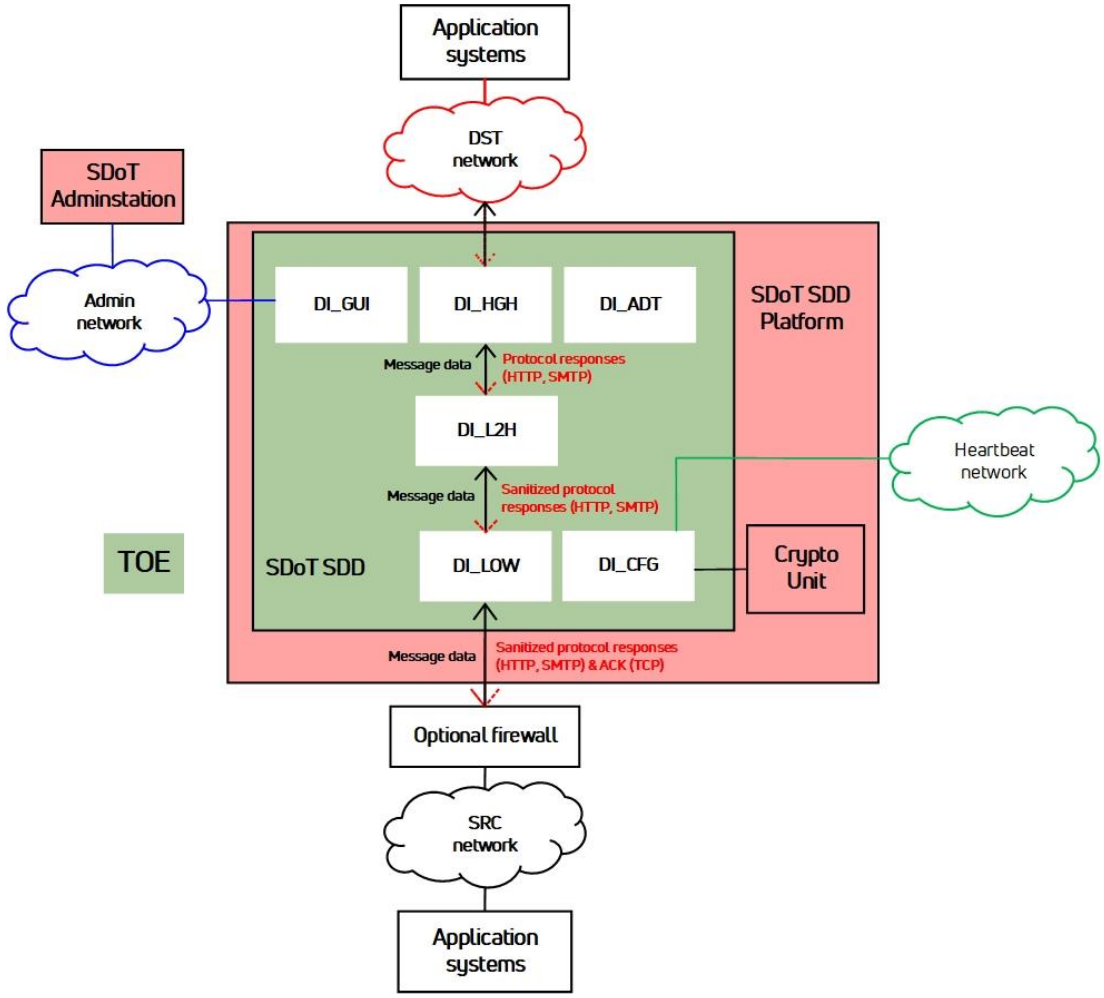

Figure 1: SDoT SDD *located between SRC and DST networks*

97 The information flow from SRC to DST is under control of the compartment DI_L2H which has no
98 direct link to the networks SRC and DST networks.

99 Outside of the TOE the SDoT SDD provides security mechanisms which include the SDoT
100 Adminstation and a dedicated cryptographic unit. These parts outside of the TOE are the operational
101 environment of the TOE. Further, it is recommended that the operator of the TOE considers using a
102 firewall which is located between the SDoT SDD and the network SRC.

103 The SDoT Adminstation allows the administrator or the auditor to fulfil their responsibility and role
104 as such. The SDoT Adminstation is connected to the TOE via the compartment DI_GUI through a
105 dedicated administration network.

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

Compartment	Description
DI_GUI	• Provides the GUIs for administrating and auditing purposes of the TOE. • Performs the signature verification to establish the secure TLS connection to the SDoT Adminstation for administrative

	purposes. TLS is only used to ensure that the correct roles log on to the TOE within the dedicated admin network. Only user roles trusted by the operational environment of the admin network are allowed to have access to the admin network. • Serves as Syslog Relay to distribute the Syslog data. • Serves as a Network Time Protocol Daemon, ensuring synchronization of the TOE system time with the target server in the admin network, or alternatively, provides time for client in the admin network.
DI_CFG	• Responsible for the communication with the Crypto Unit for cryptographic purposes. • Provides functionalities for the administration of the TOE. • Synchronizes internal system time between all of compartments
DI_ADT	• Includes mechanisms for logging security relevant events.
DI_L2H	• Direct forwarding (transfer) of messages from SRC • Analysis and sanitisation of protocol responses (of HTTP requests and SMTP emails originally coming from SRC network) and forwarding sanitised protocol responses back to the SRC network.
DI_HGH	• Includes proxies for SMTP, HTTP, UDP and TCP for communication with the TOE environment within the DST (IP network with higher level of data protection or higher level of confidentiality). • Serves as Syslog Relay to distribute the Syslog data. • Serves as a Network Time Protocol Daemon, ensuring synchronization of the TOE system time with the target server in DST, or alternatively, provides time for client in DST.
DI_LOW	• Includes proxies for SMTP, HTTP, UDP and TCP for communication with the TOE environment within the SRC (IP network with lower level of data protection or lower level of confidentiality). • Serves as a Network Time Protocol Daemon, ensuring synchronization of the TOE system time with the target server in SRC, or alternatively, provides time for client in SRC.

Table 1 Main functionalities of each compartment

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

108 • Message flow is only possible from SRC to DST i.e., messages coming from DST are not
109 accepted and blocked by the TOE.

- Analysis and sanitisation of protocol responses (of HTTP requests and SMTP emails originally coming from SRC) and forwarding these sanitised responses to SRC. The response includes only a 3-digit code number with a pre-defined corresponding message and pre-defined header.
- The TOE only accepts connections on configured ports. For each port, only correct communication according to the configured protocol is accepted by the TOE.
- The TOE provides secure auditing mechanisms of logs and secure administration capabilities.
- The TOE provides mechanisms for authentication.
- The TOE can preserve of a secure state in case of appearance of compromising events.
- The TOE regularly checks the integrity of its binary and configuration files.

1.3.3 TOE Type

The TOE (SDoT SDD SW) is the software for the product SDoT Software Data Diode (hardware and software) of INFODAS GmbH.

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

Besides the TOE the SDoT SDD consists of the following parts:

- Underlying platform (hardware and operating system) of the TOE.
- Crypto Unit which provides cryptographic support. This is a server smartcard integrated into the SDoT SDD server hardware.
- SDoT Adminstation including hardware and software parts.
- Smartcard Reader for authentication purposes at the SDoT Adminstation.
- Smartcards for cryptographic support and authentication.

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

Required non-TOE HW/SW/FW components of SDoT SDD	
Underlying Platform of the TOE:	
Hardware	Hardware of server appliance with Crypto Unit, CPU, RAM, HDDs, LC display, and physical interfaces.
Firmware/OS	Installed on the server appliance: UEFI Boot loader, Crypto Unit, L4Re microkernel OS, L4/Linux, BusyBox

SDoT Adminstation (SDoT AAC)	Machine (laptop computer) with CentOS.
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 SDD

1.4 TOE description

135 The following table shows the delivery parts of the SDoT SDD where the TOE belongs to. Following
136 to that, the subsections provide a description of the physical and logical boundaries of the TOE.

Name	Description	Medium
HW, FW, OS, Crypto Unit of SDoT SDD	Comprises all Hardware and FW/OS Parts on which the TOE is running	Hardware with installed Crypto Unit and FW/OS of SDoT SDD
SDoT Adminstation	Laptop Computer for administration of SDoT SDD	Hardware with installed FW/OS for administration purposes
TOE Installation ISO	Software for installation of the TOE on the SDoT SDD	DVD
SDoT Adminstation ISO	Software for installation of the SDoT Adminstation SW	DVD
Guidance Documentation	Manual for SDoT SDD: SDoT SDD-1.3-I-UM-DE/EN-1.6 Manual for administration: SDoT AAC-1.6-I-UM-DE-1.9 Product information sheet: SDoT SDD-1.3-I-PI-DE-0.11	All guidance documents are provided digitally via E-Mail in Portable Document Format
Smartcards	Provides key material for first initialisation and further smartcards for authentication purposes on the SDoT Stations	Smartcard

Table 3 SDoT SDD scope of delivery

1.4.1 TOE Description – Physical Scope

137 The TOE is the main software component of the SDoT SDD. Therefore, there are no physical parts
138 of the SDoT SDD in scope of the TOE. The reader may refer to Table 3 above for information about
139 the physical parts of the SDoT SDD.

1.4.2 TOE Description – Logical Scope

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

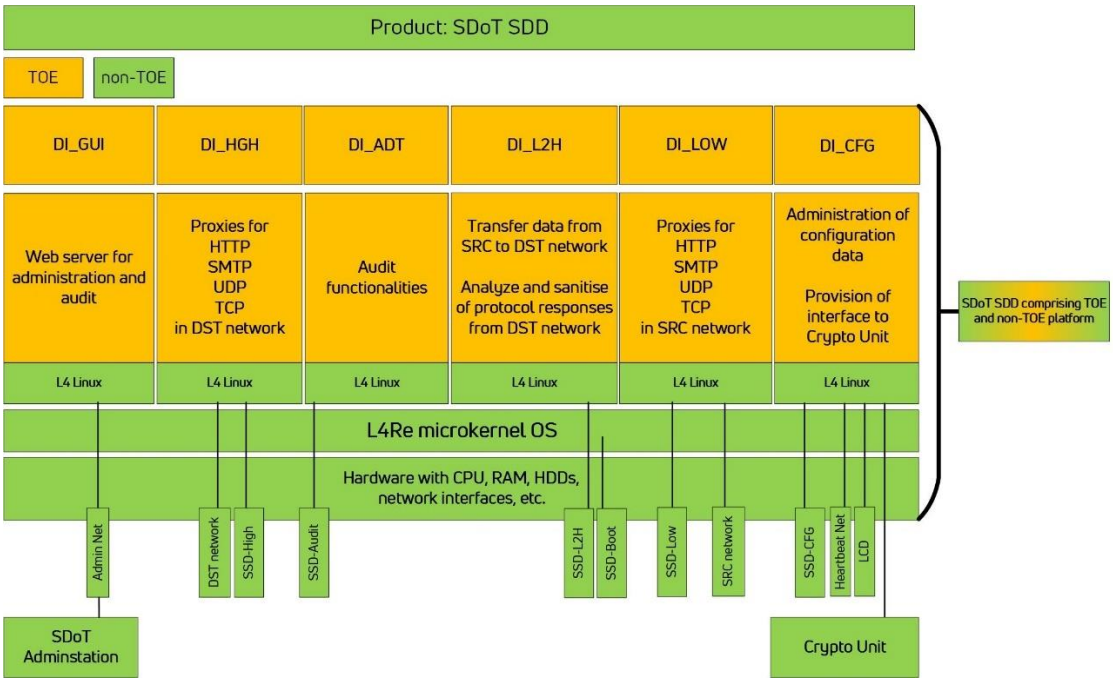

Figure 2: Logical scope of the TOE

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

148 The TOE environment within the SDoT SDD platform includes the SDoT Adminstation and a
149 dedicated Crypto Unit. For a better overview of the SDoT SDD a short description of all components
150 is given in the following.

151 **SDoT Adminstation (non-TOE):**

152 The SDoT Adminstation is based on a CentOS architecture. The functionalities for local
153 administration and local auditing of the SDoT Adminstation are provided by a GUI through a common
154 browser. Configuration parameters and audit data are managed within the administration GUI of the
155 TOE which communicates via TLS with the SDoT Adminstation. The secure TLS connection itself is
156 not in the scope of the TOE.

User SC for authentication called “user smartcard” is used with a dedicated smartcard reader and is included in the scope of delivery.

The SDoT Adminstation is connected to the TOE via a dedicated administration network in the DST domain and can only be used by administrators and auditors.

Crypto Unit (non-TOE):

The Crypto Unit includes the internal server smartcard as signing unit as well as for the secure key storage from company Atos IT Solutions and Services GmbH, see [Atos_ST]. Certified functionalities installed on the Crypto Unit (available to compartment DI_CFG) are:

- Function for generating long term keys for signatures
- Functions for creating signatures
- Random number generation
- Tamper protection and side channel protection of the cryptographic operations of the crypto unit
- Functions for secure storage of checksum values
- Functions for secure storage of keys

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

COMPARTMENT DI_GUI

The web-based administration GUI and audit GUI are displayed by a common web browser installed on the SDoT Adminstation (non-TOE). With administration GUI and audit GUI the configuration data and audit data of the TOE can be managed. Further, DI_GUI conducts signature verification to establish a secure TLS connection with the SDoT Adminstation for administrative tasks. The signature verification mechanism is within the TOE's scope, while the secure TLS connection does not.

The audit keys are generated during installation process of TOE. The generated audit keys are therefore parts of TOE.

Beside these, the DI_GUI acts as Network Time Protocol Daemon to provide or get the TOE system time as well as Syslog Relay to distribute the Syslog data.

COMPARTMENT DI_CFG

This is where the main configuration of the TOE is managed, and monitoring tasks are performed. This is the only compartment with a connection to the Crypto Unit which provides hardware based cryptographic mechanisms used by the TOE. The administration agent is called by the web server of DI_GUI after a TLS connection was initiated from the SDoT Adminstation.

The main administration agent can enable the maintenance mode either by a user who is logged in through the administration GUI on an SDoT Adminstation or the maintenance mode is activated by a security event. In maintenance mode the components of the TOE which are responsible for forwarding messages will not accept any data. Further, the main administration agent communicates with the respective administration agents in each compartment of the TOE. Every administration agent is responsible for the administration of its compartment the agent is belonging to. Similarly, each administration agent monitors the processes of the TOE within the respective compartment, i.e. restarting of stopped or crashed processes are done by the respective agent.

As mentioned above, cryptographic support from the Crypto Unit is forwarded to DI_CFG which is the only compartment with connection to the Crypto Unit.

The TOE supports a functionality called HA-mode (High Availability mode) of the SDoT SDD. Here, a cluster of redundantly designed SDoT SDDs (nodes) are operated, whereby each of these nodes fully implements the TOE. The node that currently accepts and processes the incoming data in operational mode is called the primary node. The other nodes are called secondary nodes.

From an operational point of view, high availability is an important aspect for uninterruptible operation. Communication between primary and secondary nodes take place via a separate network, the so-called heartbeat network. All nodes have a heartbeat network interface. The network interfaces are bound to the DI_CFG of each node. The heartbeat network is physically decoupled from any other networks in SDoT Diode.

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

If the primary node fails or if the connectivity of the primary node with IT systems of the DST network is lost, the system automatically switches to a functioning secondary node. For this purpose, the administration agents in each of the nodes monitor each other by cyclically requesting status information of the other agents via the heartbeat connection. If the primary node fails or is no longer accessible, one of the secondary nodes become the new primary node. The reader may also refer to the Guidance Documents for further description of the HA functionality.

In the context of the SDoT Diode evaluation, it is important to clarify that high availability is not part of the evaluation scope.

COMPARTMENT DI_ADT

This compartment provides functions for logging security relevant events. Only the audit agent within DI_ADT has access to logged audit data of the audit storage. Further, the audit agent monitors the audit storage capacity to avoid any potential overflow of the audit storage. DI_ADT communicates with DI_GUI which establishes the TLS connection for displaying the relevant information on the SDoT Adminstation.

The audit agent is responsible to record security relevant events on the TOE, related to writing entries into the audit trail. The audit agent in DI_ADT is responsible to generate alarms, i.e. e-mails. The SMTP-MTA of the TOE sends then the e-mails to a list of receivers. The list is configurable and integrity protected stored in DI_CFG with checksums stored in the Crypto Unit.

Further, the audit agent covers the following tasks:

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

COMPARTMENT DI_L2H

All messages being sent from SRC to DST are received by DI_L2H. This compartment receives the messages from one of the proxies within the DI_LOW. The process only forwards these messages towards the DST network.

In the opposite direction (from DST to SRC), DI_L2H accepts only HTTP and SMTP responses (ICAP-response protocols from HTTP-Proxy and SMTP-MTA in DI_HGH) initiated through already established connection of the corresponding requests (ICAP-request protocols from HTTP-Proxy and SMTP-MTA in DI_LOW) coming from the SRC network.

Incoming HTTP responses of HTTP requests contain a 3-digit status code. This status code indicates whether the request could be processed correctly by the HTTP server. In this way, it can be recognized on the SRC network whether the data on the DST network could be processed correctly.

DI_L2H sanitises the HTTP response only containing the outgoing status code and the corresponding configured string. Especially the HTTP body will be deleted.

In case of SMTP the receipt of the mail is confirmed by DI_HGH. What happens later with the mail, however, is not reported to the SRC network. This SMTP response contain a 3-digit status code and a corresponding string is sent via ICAP to DI_L2H. This process analyses the response and subsequently sanitises the response.

The protocols TCP and UDP do not transfer any protocol information to the SRC network.

COMPARTMENT DI_HGH

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

- SMTP
- HTTP
- UDP
- TCP

The proxies perform the following tasks which controls all data flow in the DST network.

- accepting messages coming from compartment DI_L2H and forwarding these to the DST network. These messages originally come from the SRC network.
- accepting HTTP responses coming from the DST network over the connection already established for the forwarding of the corresponding requests originally coming from the SRC network.
- except NTP calls to the NTP server at the compartment DI_HGH, denying any new connection attempts from the DST network.

Also, the above-mentioned proxies support the non-TOE functionality for mutually authenticated TLS connection with IT systems of the operational environment of the TOE in the DST network. For synchronising TOE system time DI_HGH also acts as Network Time Protocol Daemon with the target server in DST. Furthermore DI_HGH serves as Syslog Relay to distribute the Syslog data.

COMPARTMENT DI_LOW

DI_LOW provides proxy support for the following types of protocols:

- SMTP
- HTTP
- UDP
- TCP

The proxies perform the following tasks which controls all data flow in the SRC network.

- accepting messages coming from the SRC network and forwarding these messages to DI_L2H.

- accepting sanitised responses (HTTP, SMTP) from compartment DI_L2H and forwarding these to the SRC network.

Also, the above-mentioned proxies support the non-TOE functionality for mutually authenticated TLS connection with IT systems of the operational environment of the TOE within the SRC network. Furthermore, DI_LOW acts as Network Time Protocol server for time synchronisation for systems in SRC.

2 Conformance claims (ASE_CCL.1)

2.1 CC conformance claim

285 This Security Target claims conformance to

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

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

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

295 in the following way

296 • Part 2 extended

297 • Part 3 conformant

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

2.2 PP Claim

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

2.3 Package Claim

302 The assurance packages claimed by the TOE is EAL5 augmented by ALC_FLR.2 and AVA_VAN.5 to
303 the Evaluation Assurance Level EAL5+.

2.4 Conformance Rationale

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

3 Security Problem Definition (ASE_SPD.1)

3.1 Introduction

306 This chapter introduces the relevant assets which are protected by the TOE and/or its operational
307 environment. Following to that, the subjects and external entities interacting with the TOE are
308 described. Table 8 in section 3.5 outlines the assumptions which describe the security attributes of
309 the TOE operational environment to achieve the intended level of security. Possible threats which
310 must be effectively averted by the TOE, its operational environment, or a combination of both are
311 listed in 3.4, Table 7. The relevant organisational security policies (OSPs) are described in 3.6, Table
312 9.

3.2 Assets

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

3.2.1 Primary Assets

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

#	Assets	Description	Protective Objective
1.	DATA_IN_PROT	All confidential data within the network environment to be protected. If the use case defines that the network environment of SRC should be protected against malicious transmission into the network SRC and against unwanted intrusion of any type of data, then the confidential data in SRC must be considered as main asset. If the use case defines that the network environment of DST should be protected against unintentional transmission of confidential information from DST, then the confidential data in DST must be considered as main asset.	C

Table 4 Primary assets

3.2.2 Secondary Assets

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

#	Assets	Description	Protective Objective

1.	TOE_CFG	The integrity of the configuration data of the TOE shall be protected.	I
2.	TOE_SW	The integrity of program files of the TOE shall be protected.	I
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, integrity and authenticity of cryptographic key data shall be protected.	C, I, A

Table 5 Secondary assets

3.3 Subjects and external entities

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

#	Subjects and External Entities	Description
1.	Human Attacker	This threat agent could be in both DST- and in SRC network with the intention to leak protected data from DST to SRC.
2.	Non-educated human user	This threat agent resides within dedicated admin network. 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 SDD.
4.	Users with the role Administrator or Auditor	Authorised persons with access to administrating and auditing functionalities of the TOE.

Table 6 Subjects

3.4 Threats

320 Any user of the TOE may act as threat agent. This section describes the threats which must be
321 countered by the TOE independently, by its operational environment, or in combination of the two.

#	Threats	Description
1.	T.REVEAL_PA	**Adverse action:** Where DST is the network to be protected against unwanted transmission out of DST, the threat agent tries to transfer confidential information from DST to a user (human or IT-system) in SRC network. In the case where

		SRC is the network to be protected, the threat agent tries to inject malicious data or program files in SRC. Nonetheless which use case is relevant, in both cases the goal of the threat agent is to perform data flow from DST back to SRC. **Threat agent:** Human Attacker, IT environment **Asset:** DATA_IN_PROT
2.	T.REVEAL_SA_TO_UNAUTH	**Adverse action:** The threat agent tries to export or deliver secondary assets, namely, the TOE configuration data, TOE program files, audit trail, or cryptographic key data from TOE to unauthorized user(s) or other IT-system(s) outside of the TOE or outside of the SDoT SDD. **Threat agent:** Human Attacker, IT environment **Asset:** TOE_CFG, TOE_SW, AUDIT_DATA, KEY_DATA
3.	T.MALICIOUS_CODE	**Adverse action:** A human attacker bypasses the security functionality of the TOE by importing malicious code into the TOE so that data can pass against the unidirectional data flow in the TOE. **Threat agent:** Human Attacker, IT environment **Asset:** TOE_CFG, TOE_SW
4.	T.AUTH	**Adverse action:** An attacker tries to get unauthorised access to the TOE by bypassing the TOEs authentication mechanisms. The attacker may pretend to be an authorised user of the TOE. **Threat agent:** Human attacker **Asset:** DATA_IN_PROT, TOE_CFG, TOE_SW, KEY_DATA, AUDIT_DATA
5.	T.MISCONFIG	**Adverse action:** A non-educated administrator or auditor may configure the TOE in an un-intended way. The same holds for careless administrators. **Threat agent:** Administrators and Auditor of the TOE. **Asset:** DATA_IN_PROT, TOE_CFG
6.	T.AUDIT_CONTROL	**Adverse action:** A human attacker or an IT system, modifies the audit records of the TOE, so that security incidents or illegal actions can remain undetected. **Threat agent:** Human attacker, IT environment **Asset:** AUDIT_DATA

7.	T.AUDIT_COLLAPSE	**Adverse action:** A human attacker or an IT system in the network area to be protected manipulates the audit trail of the TOE, to produce an audit overflow or produce a huge amount of audit data, to make an analysis of audit logs become increasingly unfeasible. **Threat agent:** Human attacker, IT environment **Asset:** DATA_IN_PROT, AUDIT_DATA
8.	T.AUDIT_ACCESS	**Adverse action:** A human attacker or an IT system from outside the dedicated admin network tries to gain access to confidential information from the data records of the audit trail via a connected network. **Threat agent:** Human attacker, IT environment **Asset:** DATA_IN_PROT, AUDIT_DATA

Table 7 Threats

3.5 Assumptions

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

#	Assumptions	Description
1.	A.TRUSTW_ONLY	It is assumed that if other components besides the TOE connect the SRC- and DST network, these do not violate the security policy of the TOE.
2.	A.DIFF_NET	It is assumed that the TOE is connected to two different and separated networks, which are connected to each other only according to A.TRUSTW_ONLY.
3.	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.
4.	A.TRUSTW_STAFF	It is assumed that the administrators and the auditors of the TOE, as well as the privileged users of the underlying platform, and operational environment are well trained and follow all policies.
5.	A.CRYPTO_UNIT	It is assumed that state-of-the-art cryptographic mechanisms are used. The Crypto Unit which is in scope of delivery of the TOE SDoT SDD ensure that evaluated cryptographic operations are used. Further, the Random Bit Generator of the Crypto Unit is used to securely obtain random numbers. Further, keys used for audit data protection are generated by the Crypto Unit.
6.	A.CRYPTO_UNIT_USER	It is assumed that the private key of privileged users of the TOE is stored on the users' personal smart card.
7.	A.PKI	It is assumed that a trustworthy PKI is available to the TOE.
8.	A.NTP_SERVER	It is assumed that the operator of the TOE uses a reliable NTP server for generating trustworthy time stamps.
9.	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.
10	A.DEDICATED_ADMIN_NET	It is assumed that the physical admin network interface is connected only to a dedicated network for administration purposes. Further, it is assumed that the network is protected and the access to this network is restricted to authorised users only.
11	A.HIGH_AVAILABILITY	It is assumed that the physical HA network interface is only connected to a dedicated, secure HA network and that access to this interface is restricted to authorised users. The physically separated network is the only connection via the SDoT SDD's heartbeat interface, which is designed to operate a cluster of redundant SDoT SDDs. In addition, it is assumed that the HA network is implemented in a protected operational environment. The security of the HA network can be achieved by restricting access to its components to authorised users only and/or by using suitable network encryption (e.g. a suitable Layer 2 or 3 VPN).
12	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 SDD 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

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

#	OSPs	Description
1.	OSP.ADMINS	The organisation operating the TOE shall ensure that at least two different persons have the role of administrator. Only configuration changes, which are mutually approved by two administrators of the TOE, shall be accepted.
2.	OSP.AUDIT	Regarding TOE audit at least one auditor is needed. Due to the role separation, the auditor shall not be the administrator at the same time. The auditor is obligated to check the audit logs in regular time intervals. The time intervals must be defined in a meaningful manner by the organisation operating the TOE.

Table 9 OSPs

4 Security Objectives (ASE_OBJ.2)

328 This chapter describes the security objectives for the TOE and the security objectives for the
329 operational environment of the TOE.

4.1 Security Objectives for the TOE

330 The TOE must comply with the following security objectives

#	Objective for the TOE	Description
1.	OT.SANITISED	The TOE shall allow a message flow only from SRC to DST, i.e., any attempts to transfer messages from DST to SRC shall always be blocked by the TOE. Only HTTP- and SMTP responses of HTTP- and SMTP requests from DST, which are defined by the TOE-external DST systems, can pass the TOE to SRC after successful sanitisation of the protocol response.
2.	OT.COMM	The TOE shall allow only pre-defined communication channels from SRC- to DST network, which have following fixed configuration parameters: entry port, protocol, and destination, namely, host or -IP address.
3.	OT.USER_AUTHENTICATION	The TOE shall authenticate all privileged users of the TOE before any actions on the TOE can be performed.
4.	OT.ROLE_SEPARATION	The TOE shall be able to separate the role of the administrators and auditor of the TOE.
5.	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.
6.	OT.AUDIT_LOG	The TOE shall log all security relevant events which enables the auditor to track all the security relevant events. Each audit log entry shall include details about the event. In case of a critical security relevant event, the TOE shall additionally send an alarm email to a configurable list of privileged users to report this event.
7.	OT.AUDIT_PROTECT	The TOE shall provide mechanism to ensure confidentiality and integrity of the audit trail. Further, the TOE shall provide mechanisms to protect audit records against event loss or saturation of the storage device. These mechanisms can consist of sending an alarm email to a configurable list of privileged users and changing mode of the TOE from operational- to maintenance.
8.	OT.SECURE_STATE	After the initialisation process the TOE shall be constantly in a secure state. Additionally, the TOE shall always be able to

		protect check its integrity and configuration. If it is, for any reason, not possible to operate in the secure sate, the TOE shall block all network traffic trying to pass the TOE by means of changing the mode from “Operational” to “Maintenance”. Further the TOE shall send an alarm message to configured privileged users.

Table 10 Security Objectives for the TOE

4.2 Security Objectives for the Operational Environment

331 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 between two different and separated networks. The two networks can be identified as DST and SRC.
2.	OE.TRUSTW_ONLY	If besides the TOE, there are other connections between the two, DST- and SRC network, these are established using trustworthy components only and do not violate the security policy of the TOE.
3.	OE.ACCESS	All access to the TOE and its physical operational environment is restricted to authorised persons only. These include the auditor and administrators.
4.	OE.TRUSTW_STAFF	The operational environment shall ensure that all privileged users of the TOE are trusted by the organisation operating the TOE.
5.	OE.CRYPTO_UNIT	The operational environment shall ensure that the TOE is operated with IT systems which are capable of properly administrating and auditing of the TOE is sufficiently cryptographically supported by hardware related security mechanisms. Since generation of cryptographic keys are not in scope of the TOE, the operational environment shall ensure that state-of-the-art cryptographic mechanisms are used. The Crypto Unit and Smartcards which are in scope of delivery of the SDoT SDD ensure that adequate cryptographic operations are used. 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 Crypto Unit. Further, it shall be ensured that keys used for audit data protection is generated by the Crypto Unit.
6.	OE.CRYPTO_UNIT_USER	The organization operating the TOE shall ensure that the private key of privileged users of the TOE is stored on the users' personal smart card.

7.	OE.PKI	The operator of the TOE shall use a trustworthy PKI for digital signing certificates and generating and administrating CAs.
8.	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.
9.	OE.L4_PLATTFORM	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.
10	OE.DEDICATED_ADMIN_NET	The TOE shall be connected to a dedicated network for administration purposes via a specified physical administration interface. The dedicated administration network shall be an isolated network. The connection via the administration network shall be secure and in a protected operating environment.
11	OE.HIGH_AVAILABILITY	In case of usage of High Availability variant of SDoT SDD, the TOE shall be connected to a physically separated network consisting of redundant SDoT SDDs cluster via the specified HA interface only. The connection shall be secure, and the heartbeat network shall be in a protected operating environment.
12	OE.BOOT	The TOE shall use the secure start-up and initialisation mechanisms provided by the UEFI based secure boot process of the SDoT SDD platform.

Table 11 Security Objectives for the Operational Environment

4.3 Rationale between SPD and security objectives

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

	Objectives for the TOE	OT.SANITISED	OT.COMM	OT.USER_AUTHENTICATION	OT.ROLE_SEPARATION	OT.FOUR_EYES	OT.AUDIT_LOG	OT.AUDIT_PROTECT	OT.SECURE_STATE
Threats									
T.REVEAL_PA		x	x	x		x	x		x
T.REVEAL_SA_TO_UNAUTH								x	x
T.MALICIOUS_CODE									x
T.AUTH									
T.MISCONFIG			x		x	x	x	x	
T.AUDIT_CONTROL					x			x	
T.AUDIT_COLLAPSE								x	
T.AUDIT_ACCESS					x				
OSPs									
OSP.ADMINS					x	x			
OSP.AUDIT					x				

Table 12 Security Objective for the TOE coverage

	Objectives for the op. environment	OE.DIFF_NET	OE.TRUSTW_ONLY	OE.ACCESS	OE.TRUSTW_STAFF	OE.CRYPTO_UNIT	OE.CRYPTO_UNIT_USER	OE.PKI	OE.L4_PLATTFORM	OE.NTP_SERVER	OE.DEDICATED_ADMIN_NET	OE.HIGH_AVAILABILITY	OE.BOOT
Threats													
T.REVEAL_PA		x	x		x						x		
T.REVEAL_SA_TO_UNAUTH			x	x	x						x		
T.MALICIOUS_CODE													x
T.AUTH											x		
T.MISCONFIG				x							x		
T.AUDIT_CONTROL				x							x		
T.AUDIT_COLLAPSE													
T.AUDIT_ACCESS				x							x		
OSPs													
OSP.ADMINS				x	x								
OSP.AUDIT				x	x								
Assumptions													
A.DIFF_NET		x											
A.TRUSTW_ONLY		x	x										
A.ACCESS				x									
A.TRUSTW_STAFF					x								
A.CRYPTO_UNIT						x							
A.CRYPTO_UNIT_USER							x						
A.PKI								x					

	Objectives for the op. environment	OE.DIFF_NET	OE.TRUSTW_ONLY	OE.ACCESS	OE.TRUSTW_STAFF	OE.CRYPTO_UNIT	OE.CRYPTO_UNIT_USER	OE.PKI	OE.L4_PLATTFORM	OE.NTP_SERVER	OE.DEDICATED_ADMIN_NET	OE.HIGH_AVAILABILITY	OE.BOOT
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

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

4.4 Rationale Threats

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

4.4.1 T.REVEAL_PA

Potential data flow from the DST network to a user (human or IT-System) within the SRC network is countered by a combination of several objectives for the TOE and objectives for the operational environment of the TOE.

OT.SANITISED addresses T.REVEAL_PA with the corresponding unidirectional data transfer from SRC- to DST network and sanitising mechanism which sanitises HTTP and SMTP protocol responses sent from DST- to SRC network.

OT.COMM ensures that only communication channels with fixed configured parameter can be used for data transfer from SRC- to DST network. Therefore, this objective prevents any other arbitrary communication channel for data transfer from SRC- to DST network or vice versa.

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

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

OT.AUDIT_LOG enables the auditor to track all changes to the TOE configuration, and identify the corresponding auditors. This objective for the TOE addresses T.REVEAL_PA by motivating the user to not make any light-minded change to the TOE configuration and avoid any misconfiguration of the TOE.

OT.SECURE_STATE counters T.REVEAL_PA in the case where after TOE initialisation a secure state cannot be achieved. Here, the TOE will block all traffic and no confidential information can be passed from DST- to SRC network.

OE.DIFF_NET, OE.TRUSTW_STAFF and OE.TRUSTW_ONLY support OT.SANITISED by ensuring that all data to be sent between DST- and SRC network have to pass the sanitising mechanism since, there are only trustworthy connection between DST- and SRC network. Further, the organisation operating the TOE ensures that only trustworthy personnel have privileged user roles.

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

4.4.2 T.REVEAL_SA_TO_UNAUTH

OT.SECURE_STATE and OT.AUDIT_PROTECT ensure that the TOE is able to protect own- software, configuration data and integrity, as well as the audit trail against threat, which tries to expose, export or deliver them to unauthorised user or IT-system outside of the TOE. This is supported by OE.TRUSTW_STAFF, OE.TRUSTW_ONLY, and OE.ACCESS to ensure that there are only trustworthy connection between DST- and SRC network and trustworthy personnel accessing the TOE. OE.DEDICATED_ADMIN_NET supports to counter the threat by providing a dedicated and trusted administration network.

4.4.3 T.MALICIOUS_CODE

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

372 Further, OE.BOOT helps to mitigate the risk of T.MALICIOUS_CODE in the presence of secure boot
373 mechanisms which only allows authentic software to be executed. Additionally, OE.BOOT requires the
374 administrators to keep the securely pre-configures settings of the used BIOS.

4.4.4 T.AUTH

375 OE.DEDICATED_ADMIN_NET counters the threat by providing a dedicated administration network.

4.4.5 T.MISCONFIG

376 OT.FOUR_EYES addresses T.MISCONFIG by avoiding that an administrator could unintentionally
377 misconfigure the TOE by means of enforcing the dual control mechanism.

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

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

382 OE.DEDICATED_ADMIN_NET supports to counter the threat by providing a dedicated and trusted
383 administration network.

384 OT.COMM ensures that only allowed protocols are used to avoid any bypass of sanitization mechanisms
385 of the TOE if a threat agent tries to perform any misconfiguration. Fixed and pre-defined communication
386 configuration parameters such as entry port, protocol, and destination, namely, host or -IP address counter
387 the threat so, that it is not possible to choose any other arbitrary parameter.

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

392 OT.AUDIT_PROTECT ensures that logged configurations are cryptographically protected against
393 manipulation.

4.4.6 T.AUDIT_CONTROL

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

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

397 OE.ACCESS supports to counter the threat by ensuring that only auditors and administrators have physical
398 access to the TOE.

399 OE.DEDICATED_ADMIN_NET supports to counter the threat by providing a dedicated and trusted
400 administration network.

4.4.7 T.AUDIT_COLLAPSE

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

4.4.8 T.AUDIT_ACCESS

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

406 OE.DEDICATED_ADMIN_NET supports to counter the threat by providing a dedicated and trusted
407 administration network and OE.ACCESS ensures that only authorised persons have physical access to the
408 TOE and its operational environment.

4.5 Rationale OSPs

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

4.5.1 OSP.ADMINS

410 This policy addresses the objective OT.ROLE_SEPARATION about the ability of the TOE to distinguish the
411 administrator role from the auditor, which is assigned to at least two specific persons which are not auditors
412 at the same time. Moreover, the objective OT.FOUR_EYES is also addressed to fulfil dual control process
413 by TOE configuration changes by administrators.

414 The objective OE.TRUSTW_STAFF ensures that the TOE environment is responsible that all privileged
415 users of the TOE are trusted by the organisation operating the TOE.

416 OE.ACCESS ensures that access to the TOE and its physical operational environment is restricted to
417 authorised persons only. These include the auditor and administrators.

4.5.2 OSP.AUDIT

418 This policy addresses the objective OT.ROLE_SEPARATION about the ability of the TOE to distinguish the
419 auditor role from the administrator, which is assigned to specific persons which are not administrators at
420 the same time.

421 The objective OE.TRUSTW_STAFF ensures that the TOE environment is responsible that all privileged
422 users of the TOE are trusted by the organisation operating the TOE.

423 OE.ACCESS ensures that access to the TOE and its physical operational environment is restricted to
424 authorised persons only. These include the auditor and administrators.

4.6 Rationale Assumptions

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

4.6.1 A.DIFF_NET

427 The security objective for the operational environment of the TOE OE.DIFF_NET corresponds to the
428 assumption A.DIFF_NET by requiring the TOE to be connected between two different and separated
429 networks.

4.6.2 A.TRUSTW_ONLY

430 OE.TRUSTW_ONLY requires that the TOE is the only connection between the DST- and the SRC network.
431 OE.DIFF_NET supports OE.TRUSTW_ONLY because it requires that the TOE is connected to two different
432 and separated networks.

4.6.3 A.ACCESS

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

4.6.4 A.TRUSTW_STAFF

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

4.6.5 A.CRYPTO_UNIT

437 OE.CRYPTO_UNIT addresses A.CRYPTO_UNIT which ensures that all needed cryptographic support is
438 derived from the cryptographic units which are delivered together with the TOE.

4.6.6 A.CRYPTO_UNIT_USER

439 A.CRYPTO_UNIT_USER is directly addressed by OE.CRYPTO_UNIT_USER.

4.6.7 A.PKI

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

4.6.8 A.NTP_SERVER

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

4.6.9 A.L4_PLATFORM

444 The assumption A.L4_PLATFORM is covered by the objective OE.L4_PLATTFORM which requires the TOE
445 to run on a L4Re microkernel OS which provides dedicated logical separation mechanisms for each
446 compartment.

4.6.10 A.DEDICATED_ADMIN_NET

447 The assumption A.DEDICATED_ADMIN_NET is covered by the objective OE.DEDICATED_ADMIN_NET
448 which requires that the TOE is connected to the SDoT Adminstation only through a dedicated network for
449 administration purposes in a protected operating environment. Further, the objective requires that the
450 dedicated admin network is a physically isolated network.

4.6.11 A.HIGH_AVAILABILITY

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

4.6.12 A.BOOT

454 The assumption A.BOOT is directly addressed by OE.BOOT which requires that the TOE uses the secure
455 start-up and boot mechanisms provided by the underlying platform. Further, the administrators of the TOE
456 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	• User	See FDP_ACF.1.1/AuditAccess FCS_COP.1/ECDSA/AdminTLS
Object	• AUDIT_DATA	
Security Attributes	• users X509 signature	
Operation	• Read/Delete audit records	See FDP_ACF.1.2/AuditAccess
Condition/Rule	• Certificate is signed by the configured AuditCA • Title field in Distinguished Name contains "auditor".	

Table 14 audit access control SFP

admin access control SFP		
Type	**Name**	**Remark**
Subject	• User	See FDP_ACF.1.1/AdminAccess FCS_COP.1/ECDSA/AdminTLS
Object	• TOE_CFG	
Security Attributes	• users X509 signature	
Operation	• all possible operation of the subject.	See FDP_ACF.1.2/AdminAccess
Condition/Rule	• Certificate is signed by the configured AdminCA • Title field in Distinguished Name contains "sifi-admin".	

Table 15 admin access control SFP

data from SRC SFP		
Type	**Name**	**Remark**
Subject	• Systems in SRC sending data • Systems in DST receiving data • DATA_IN_SRC	See FDP_IFF.1.1/DataFromSRC
Information	• Content of data	
Security Attribute	• The domain from which the data is coming	
Operation	• permit an information flow between a controlled subjects and controlled information via a controlled operation	See FDP_IFF.1.2/DataFromSRC
Condition/Rule	• Data is received via a supported protocol at a configured port for the protocol.	

	• The destination address corresponds to the allowed destination addresses for the incoming port.	

Table 16 data from SRC SFP

HTTP response SFP		
Type	**Name**	**Remark**
Subject	• HTTP-PROXY_HIGH, • HTTP-PROXY_LOW, • DATA_IN_DST	See FDP_IFF.1.1/HTTP
Information	• HTTP_response	
Security Attributes	• The domain from which the HTTP_response is coming • Transfer Protocol • Mode of operation	
Operation	permit an information flow between a controlled subjects and controlled information via a controlled operation	See FDP_IFF.1.2/HTTP
Condition/Rule	• Source of HTTP_response is DST • HTTP_response is transferred via HTTP(S) • Mode of operation is "Operational" • HTTP_response must be an answer to a request from network SRC.	See FDP_IFF.1.2/HTTP
	HTTP sanitisation rule: • The http body is sanitised such that it only contains the status line, • The status line is sanitised based on the received status code (a three-number digit): a) The status code is matched against a configured list of allowed status codes b) The status message is replaced by a fixed text from the configured list. • Header Elements a) Content-Length: 0 b) Date	See FDP_IFF.1.3/HTTP

Table 17 HTTP response SFP

ICAP header SFP		
Type	**Name**	**Remark**
Subject	• SMTP-MTA_HIGH • SMTP-MTA_LOW • TCP-RELAY_HIGH • TCP-RELAY_LOW • UDP-RELAY_HIGH • UDP-RELAY_LOW • DATA_IN_DST	FDP_IFF.1.1/ICAP
Information	• ICAP_response	
Security Attributes	• Mode of operation • Protocol state	
Condition/Rule	• Mode of operation is "operational" • Message is a response to a ICAP request	FDP_IFF.1.2/ICAP
Operation	• permit an information flow between a controlled subjects and controlled information via a controlled operation	FDP_IFF.1.2/ICAP
	• Remove all headers	FDP_IFF.1.3/ICAP

Table 18 ICAP header SFP

ICAP response SFP		
Type	**Name**	**Remark**
Subject	• SMTP-MTA_HIGH • SMTP-MTA_LOW • TCP-RELAY_HIGH • TCP-RELAY_LOW • UDP-RELAY_HIGH • UDP-RELAY_LOW • DATA_IN_DST	FDP_IFF.1.1/ICAP
Information	• ICAP-response	
Security Attributes	• Mode of operation • Protocol state	
Condition/Rule	• Mode of operation is "operational" • Message is a response to a ICAP request	FDP_IFF.1.2/ICAP

ICAP response SFP		
Operation	• permit an information flow between a controlled subjects and controlled information via a controlled operation	FDP_IFF.1.2/ICAP
	• Parse the Response-Line into "Response code" (three digits) and "Response string" • Check that the "Response code" is between "100" and "999" (inclusive) Replace with default if fails • Check the "Response string" against hard coded list. Replace with default (based on the "Response code" (full or first digit)) if fails • Remove any other content of the ICAP response	FDP_IFF.1.3/ICAP

Table 19 ICAP response SFP

NTP synchronize SFP		
Type	**Name**	**Remark**
Subject	• NTP services in DST or in SRC • NTP service and hosts in Admin Net • NTP clients in DST or in SRC	See FDP_IFF.1.1/NTP
Information	• TOE system time	
Security Attributes	• Origin of time reference	
Operation	• permit an information flow between a controlled subjects and controlled information via a controlled operation	See FDP_IFF.1.2/NTP
Condition/Rule	**NTP synchronize rule:** The time can be synchronized between SRC and DST using the TOE by one of the following ways: • The system time of the TOE is optionally synchronized via: a) the NTP Server in subsystem DI_HGH to a NTP Service in network DST. b) the NTP Server in subsystem DI_GUI to a	See FDP_IFF.1.3/NTP

	NTP Service in Admin Net. c) the NTP Server in subsystem DI_LOW to a NTP Service in Network SRC • The system time of the TOE is optionally provided via: a) the NTP Server in subsystem DI_HGH to hosts in network DST b) the NTP Server in subsystem DI_GUI to hosts in Admin Net c) the NTP Server in subsystem DI_LOW to hosts in network SRC.	

Table 20 NTP synchronize SFP

dual control admin SFP		
Type	**Name**	**Remark**
Subject	• 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 FMT_MTD.1/AdminModify
Condition/Rule	• user_role = administrator	

Table 21 dual control admin SFP

6 Extended components definition (ASE_ECD.1)

6.1 Class FPT: Protection of the TSF

6.1.1 TSF integrity checks (FPT_INC)

457 **Family Behaviour**

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

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

465 **Component Levelling**

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

469 **Management FPT_INC.1**

470 a) management of the conditions under which TSF self-testing occurs, such as during initial
471 start-up, regular interval, or under specified conditions.

472 b) management of the time interval if appropriate.

473 **Audit: FPT_INC.1**

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

476 a) Basic: Execution of the TSF self-tests and the results of the tests.

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

7 Statement of security requirements (ASE_REQ.2)

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

7.1 Security functional requirements

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

#	User Data Protection (FDP)	
1.	FDP_ACC.2/AuditAccess	Complete access control
2.	FDP_ACC.2/AdminAccess	Complete access control
3.	FDP_ACF.1/AuditAccess	Security attribute based access control
4.	FDP_ACF.1/AdminAccess	Security attribute based access control
5.	FDP_ETC.1/AuditKeys	Export of user data without security attributes
6.	FDP_IFC.2/DataFromSRC	Subset information flow control
7.	FDP_IFC.2/HTTP	Complete information flow control
8.	FDP_IFC.2/ICAP	Complete information flow control
9.	FDP_IFC.2/NTP	Complete information flow control
10.	FDP_IFF.1/DataFromSRC	Simple security attributes
11.	FDP_IFF.1/HTTP	Simple security attributes
12.	FDP_IFF.1/ICAP	Simple security attributes
13.	FDP_IFF.1/NTP	Simple security attributes
14.	FDP_ITC.1/Keys/AdminTLS	Import of user data without security attributes
	Identification and authentication (FIA)	
15.	FIA_UAU.2	User authentication before any action
16.	FIA_UID.2	User identification before any action
	Cryptographic support (FCS)	
17.	FCS_CKM.1/AES/Audit	Cryptographic key generation
18.	FCS_CKM.1/HMAC/Audit	Cryptographic key generation
19.	FCS_CKM.2/AES/Audit	Cryptographic key distribution
20.	FCS_CKM.2/HMAC/Audit	Cryptographic key distribution
21.	FCS_CKM.4	Cryptographic key destruction
22.	FCS_COP.1/ECDSA/AdminTLS	Cryptographic operation
23.	FCS_COP.1/AES/Audit	Cryptographic operation
24.	FCS_COP.1/HMAC/Audit	Cryptographic operation
25.	FCS_COP.1/SHA2/Audit	Cryptographic operation
26.	FCS_COP.1/SHA2/Integrity	Cryptographic operation
	Security management (FMT)	
27.	FMT_MSA.1/AdminCA	Management of security attributes
28.	FMT_MSA.1/OpMode	Management of security attributes
29.	FMT_MSA.3	Static attribute initialisation
30.	FMT_MTD.1/AdminAccess	Management of TSF data
31.	FMT_MTD.1/AdminModify	Management of TSF data
32.	FMT_MTD.1/AuditAccess	Management of TSF data
33.	FMT_MTD.1/AuditDelete	Management of TSF data
34.	FMT_MTD.3	Secure TSF data

35.	FMT_SMF.1	Specification of management functions
36.	FMT_SMR.2	Restrictions on security roles
	Protection of the TSF (FPT)	
37.	FPT_STM.1	Reliable time stamps
38.	FPT_INC.1	TSF integrity
39.	FPT_RCV.1	Manual recovery
	Security audit (FAU)	
40.	FAU_ARP.1	Security audit automatic response
41.	FAU_GEN.1	Audit data generation
42.	FAU_GEN.2	User identity association
43.	FAU_SAA.1	Security audit analysis
44.	FAU_SAR.1	Security audit review
45.	FAU_SAR.2	Restricted audit review
46.	FAU_STG.2	Guarantees of audit data availability
47.	FAU_STG.4	Prevention of audit data loss

Table 22 SFRs of the TOE

480 The following styles of marking operations are applied:

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

482 • Selections are marked in *italic underlined.*

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

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

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

7.1.1 User Data Protection (FDP)

FDP_ACC	**Access control policy**
FDP_ACC.2/AuditAccess	Complete access control
Hierarchical to:	FDP_ACC.1 Subset access control
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.2.1/AuditAccess	The TSF shall enforce the **audit access control SFP** on **users, AUDIT_DATA** and all operations among subjects and objects covered by the SFP.
FDP_ACC.2.2/AuditAccess	The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.
FDP_ACC.2/AdminAccess	Complete access control
Hierarchical to:	FDP_ACC.1 Subset access control
Dependencies:	FDP_ACF.1 Security attribute based access control

FDP_ACC.2.1/AdminAccess	The TSF shall enforce the **admin access control SFP** on **users, TOE_CFG**, and all operations among subjects and objects covered by the SFP.
FDP_ACC.2.2/AdminAccess	The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.
FDP_ACF	**Access control functions**
FDP_ACF.1/AuditAccess	Security attribute based access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/AuditAccess	The TSF shall enforce the **audit access control SFP** to objects based on the following: 1. **Subject: user** 2. **Object: AUDIT_DATA** 3. **Security Attributes: users X509 signature.**
FDP_ACF.1.2/AuditAccess	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **operation: Read/Delete audit records** **condition:** 1. **Certificate is signed by the configured AuditCA** 2. **Title field in Distinguished Name contains "auditor".**
FDP_ACF.1.3/AuditAccess	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none.**
FDP_ACF.1.4/AuditAccess	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **none.**
FDP_ACF.1/AdminAccess	Security attribute based access control
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/AdminAccess	The TSF shall enforce the **admin access control SFP** to objects based on the following: 1. **Subject: user** 2. **Object: TOE_CFG**

	3. **Security Attributes: users X509 signature.**
FDP_ACF.1.2/AdminAccess	The TSF shall enforce the following rules to determine if an operation among controlled subject and controlled objects is allowed: **operation:** 1. **all possible operation of the subject.** **condition:** 1. **Certificate is signed by the configured AdminCA** 2. **Title field in Distinguished Name contains "sifi-admin".**
FDP_ACF.1.3/AdminAccess	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none.**
FDP_ACF.1.4/AdminAccess	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **none.**
FDP_ETC	**Export from the TOE**
FDP_ETC.1/AuditKeys	Export of user data without security attributes
Hierarchical to:	No other components
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_ETC.1.1/AuditKeys	The TSF shall enforce the **audit access control SFP** when exporting ~~user data, controlled under the SFP(s)~~ ***the keys used to protect the confidentiality and integrity of the Audit Trail***, outside of the TOE.
~~FDP_ETC.1.2/AuditKeys~~	~~The TSF shall export the user data without the user data's associated security attributes~~

Application Note: FDP_ETC.1.2/AuditKeys is crossed out because there are no user data's associated security attributes to be considered.

FDP_IFC	**Information flow control policy**
FDP_IFC.2/DataFromSRC	Complete information flow control
Hierarchical to:	FDP_IFC.1 Subset information flow control
Dependencies:	FDP_IFF.1 Simple security attributes
FDP_IFC.2.1/DataFromSRC	The TSF shall enforce the **data from SRC SFP** on **Systems in SRC sending data, Systems in DST receiving data, DATA_IN_SRC, Content of data** and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2/DataFromSRC	The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.
FDP_IFC.2/HTTP	Complete information flow control
Hierarchical to:	FDP_IFC.1 Subset information flow control
Dependencies:	FDP_IFF.1 Simple security attributes
FDP_IFC.2.1/HTTP	The TSF shall enforce the **HTTP response SFP** on **HTTP-PROXY_HIGH, HTTP-PROXY_LOW, DATA_IN_DST, HTTP_response** and all operations that cause that information to flow to and from subjects covered by the SFP.
FDP_IFC.2.2/HTTP	The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.
FDP_IFC.2/ICAP	Complete information flow control
Hierarchical to:	FDP_IFC.1 Subset information flow control
Dependencies:	FDP_IFF.1 Simple security attributes
FDP_IFC.2.1/ICAP	The TSF shall enforce **the ICAP header SFP and ICAP response SFP** on **SMTP-MTA_HIGH, SMTP-MTA_LOW, TCP-RELAY_HIGH, TCP-RELAY_LOW, UDP-RELAY_HIGH, UDP-RELAY_LOW, DATA_IN_DST, ICAP_response** and all operations that cause that information to flow to and from subjects covered by the SFP.
FDP_IFC.2.2/ICAP	The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.
FDP_IFC.2/NTP	Complete information flow control
Hierarchical to:	FDP_IFC.1 Subset information flow control
Dependencies:	FDP_IFF.1 Simple security attributes
FDP_IFC.2.1/NTP	The TSF shall enforce the **NTP synchronize SFP** on **NTP services in DST or in SRC, NTP service and hosts in Admin Net, NTP clients in DST or in SRC, TOE system time** and all operations that cause that information to flow to and from subjects covered by the SFP.
FDP_IFC.2.2/NTP	The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

FDP_IFF	Information flow control functions
FDP_IFF.1/DataFromSRC	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/DataFromSRC	The TSF shall enforce the **data from SRC SFP** based on the following types of subjects and information security attributes: **Subjects:** 1. **Systems in SRC sending data** 2. **Systems in DST receiving data** 3. **DATA_IN_SRC** **Information:** 1. **Content of data** **Security Attribute:** 1. **The domain from which the data is coming**
FDP_IFF.1.2/DataFromSRC	The TSF shall permit an information flow between a controlled subjects and controlled information via a controlled operation if the following rules hold: 1. **Data is received via a supported protocol at a configured port for the protocol.** 2. **The destination address corresponds to the allowed destination addresses for the incoming port.**
FDP_IFF.1.3/DataFromSRC	The TSF shall enforce the **none**.
FDP_IFF.1.4/DataFromSRC	The TSF shall explicitly authorise an information flow based on the following rules**: none**
FDP_IFF.1.5/DataFromSRC	The TSF shall explicitly deny an information flow based on the following rules: **none**

Application Note: The supported protocols are SMTP, HTTP, TCP and UDP

FDP_IFF.1/HTTP	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/HTTP	The TSF shall enforce the **HTTP response SFP** based on the following types of subjects and information security attributes: **Subjects:** 1. **HTTP-PROXY_HIGH,** 2. **HTTP-PROXY_LOW,** 3. **DATA_IN_DST** **Information:** 1. **HTTP_response** **Security Attributes:** 1. **The domain from which the HTTP_response is coming** 2. **Transfer Protocol** 3. **Mode of operation**
FDP_IFF.1.2/HTTP	The TSF shall permit an information flow between a controlled subjects and controlled information via a controlled operation if the following rules hold: 1. **Source of HTTP_response is DST** 2. **HTTP_response is transferred via HTTP(S)** 3. **Mode of operation is "Operational"** 4. **HTTP_response must be an answer to a request from network SRC.**
FDP_IFF.1.3/HTTP	The TSF shall enforce the **HTTP sanitisation rule:** 1. **The http body is sanitised such that it only contains the status line,** 2. **The status line is sanitised based on the received status code (a three-number digit):** a. **The status code is matched against a configured list of allowed status codes** b. **The status message is replaced by a fixed text from the configured list.** 3. **Header Elements** a. **Content-Length: 0** b. **Date**
FDP_IFF.1.4/HTTP	The TSF shall explicitly authorise an information flow based on the following rules**: none**
FDP_IFF.1.5/HTTP	The TSF shall explicitly deny an information flow based on the following rules: **none**
FDP_IFF.1/ICAP	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/ICAP	The TSF shall enforce the **ICAP header SFP and the ICAP response SFP** based on the following types of subjects and information security attributes: **Subjects:** 1. SMTP-MTA_HIGH 2. SMTP-MTA_LOW 3. TCP-RELAY_HIGH 4. TCP-RELAY_LOW 5. UDP-RELAY_HIGH 6. UDP-RELAY_LOW 7. DATA_IN_DST **Information:** 1. ICAP_response **Security Attributes:** 1. Mode of operation 2. Protocol state
FDP_IFF.1.2/ICAP	The TSF shall permit an information flow between a controlled subjects and controlled information via a controlled operation if the following rules hold: 1. Mode of operation is "Operational". 2. Message is a response to an ICAP request
FDP_IFF.1.3/ICAP	The TSF shall enforce the **ICAP header SFP:** 1. Remove all headers **and the ICAP response SFP:** 1. Parse the Response-Line into "Response code" (three digits) and "Response string" 2. Check that the "Response code" is between "100" and "999" (inclusive) Replace with default if fails 3. Check the "Response string" against hard coded list. Replace with default (based on the "Response code" (full or first digit)) if fails 4. Remove any other content of the ICAP response
FDP_IFF.1.4/ICAP	The TSF shall explicitly authorise an information flow based on the following rules: **none**
FDP_IFF.1.5/ICAP	The TSF shall explicitly deny an information flow based on the following rules: **none**
FDP_IFF.1/NTP	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/NTP	The TSF shall enforce the **NTP synchronize SFP** based on the following types of subjects and information security attributes: **Subjects:** 1. **NTP services in DST or in SRC** 2. **NTP service and hosts in Admin Net** 3. **NTP clients in DST or in SRC** **Information:** 1. **TOE system time** **Security Attributes:** 1. **Origin of time reference**
FDP_IFF.1.2/NTP	The TSF shall permit an information flow between a controlled subjects and controlled information via a controlled operation if the following rules hold: **none**
FDP_IFF.1.3/NTP	The TSF shall enforce the **NTP synchronize rule:** **The time can be synchronized between SRC and DST using the TOE by one of the following ways:** 1. **The system time of the TOE is optionally synchronized via:** a. **the NTP Server in subsystem DI_HGH to a NTP Service in network DST.** b. **the NTP Server in subsystem DI_GUI to a NTP Service in Admin Net.** c. **the NTP Server in subsystem DI_LOW to a NTP Service in Network SRC** 2. **The system time of the TOE is optionally provided via:** a. **the NTP Server in subsystem DI_HGH to hosts in network DST** b. **the NTP Server in subsystem DI_GUI to hosts in Admin Net** c. **the NTP Server in subsystem DI_LOW to hosts in network SRC.**
FDP_IFF.1.4/NTP	The TSF shall explicitly authorise an information flow based on the following rules: **none**
FDP_IFF.1.5/NTP	The TSF shall explicitly deny an information flow based on the following rules: **none**
FDP_ITC	**Import from outside of the TOE**
FDP_ITC.1/Keys/AdminTLS	Import of user data without security attributes

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation
FDP_ITC.1.1/Keys/AdminTLS	The TSF shall enforce the **admin access control SFP** when importing ~~user data, controlled under the SFP~~ ***ECDSA Keys for AdminTLS in accordance with PKCS#12***, from outside of the TOE.
~~FDP_ITC.1.2/Keys/AdminTLS~~	~~The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.~~
FDP_ITC.1.3/Keys/AdminTLS	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: 1. **The Key must be defined on one of the following curves: secp384r1, brainpoolP384r1, and brainpoolP512r1**

Application Note: FDP_ITC.1.2/Keys/AdminTLS crossed out because there are no security attributes associated with user data

7.1.2 Identification and authentication (FIA)

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

Application Note: TSF mediated actions can only be accessed via the AuditGUI or the AdminGUI. The AuditGUI and the AdminGUI can only be accessed via TLS with mutual authentication. The user role is determined by its title field within the Distinguished Name of the user's certificate.

7.1.3 Cryptographic support (FCS)

FCS_CKM	Cryptographic key management

FCS_CKM.1/AES/Audit	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/AES/Audit	The TSF shall generate cryptographic keys ***for Advanced Encryption Standard*** in accordance with a specified cryptographic key generation algorithm **direct generation from a PTG.2** and specified cryptographic key sizes **256 bits** that meet the following: **NIST SP 800-133 Rev. 2**

Application Note: This SFR is partially fulfilled by the TOE environment (the installer and crypto unit).

FCS_CKM.1/HMAC/Audit	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/HMAC/Audit	The TSF shall generate cryptographic keys ***for HMAC-SHA-384*** in accordance with a specified cryptographic key generation algorithm **direct generation from a PTG.2** and specified cryptographic key sizes **384 bits** that meet the following: **NIST SP 800-133 Rev. 2.**

Application Note: This SFR is partially fulfilled by the TOE environment (the installer and crypto unit).

FCS_CKM.2/AES/Audit	Cryptographic key distribution
Hierarchical to:	No other components
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_CKM.2.1/AES/Audit	The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **Inter-Compartment Key Copy via MNGT Interface** that meets the following: **MNGT Protocol**.

Application Note: The MNGT Interface is specified in the FSP part of the ADV Doxy-documentation.

FCS_CKM.2/HMAC/Audit	Cryptographic key distribution
Hierarchical to:	No other components
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
FCS_CKM.2.1/HMAC/Audit	The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **Inter-Compartment Key Copy via MNGT Interface** that meets the following: **MNGT Protocol**.

Application Note: The MNGT Interface is specified in the FSP part of the ADV Doxy-documentation.

FCS_CKM.4	Cryptographic key destruction
Hierarchical to:	No other components
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **overwriting the key with zeros** that meets the following: **none**.

Application Note: This SFR refers to the keys in ephemeral memory and not to the keys stored for long-term storage on the smart card.

FCS_COP.1/ECDSA/AdminTLS	Cryptographic operation
Hierarchical to:	No other components
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1/ECDSA/AdminTLS	The TSF shall perform **digital signature verification** in accordance with a specified cryptographic algorithm **ECDSA** and cryptographic key sizes **384 Bit and 512 Bit** that meet the following: **signature verification as specified in ANSI X9.62 with keys based on the ECC domain parameters secp384r1, brainpoolP384r1, and brainpoolP512r1 with sha2 according to curve size as sub function**.

Application Note: Although the establishment of the secure TLS connection itself is not within the scope of the TOE, for evaluation purposes, information about cryptographic procedures is considered. As already mentioned in the introductory part in Table 1: In this SFR TLS is only used to ensure that the correct roles log on to the TOE within the dedicated admin network.

The TLS supports the following:

TLS-Version	*1.3, 1.2*
Cipher Suites 1.3	*TLS_AES_256_GCM_SHA384* *TLS_AES_128_GCM_SHA256*
Cipher Suites 1.2	*TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384* *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256*
Signature Algorithms	*ecdsa_brainpoolP512r1tls13_sha512* *ecdsa_brainpoolP384r1tls13_sha384* *ecdsa_secp384r1_sha384*
Supported Groups	*brainpoolP512r1* *brainpoolP384r1* *secp384r1*
Permitted signature algorithms of the client certificate	*ECDSA_with_SHA512* *ECDSA_with_SHA384* *ECDSA_with_SHA256*
Certificate Verification	*Mutually Mandatory*

FCS_COP.1/AES/Audit	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/Audit	The TSF shall perform **encryption and decryption** in accordance with a specified cryptographic algorithm **AES in GCM mode** and cryptographic key sizes **256 Bit** that meet the following: **FIPS 197 and SP800-38D.**

FCS_COP.1/HMAC/Audit	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/Audit	The TSF shall perform **hash-based message authentication code** in accordance with a specified cryptographic algorithm **HMAC-SHA2** and cryptographic key sizes **384 Bit** that meet the following**: RFC 2104**.
FCS_COP.1/SHA2/Audit	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/Audit	The TSF shall perform ***Hash value calculation*** in accordance with a specified cryptographic algorithm **SHA-384** and cryptographic key size **none** that meet the following**: FIPS 180-4**.

Application Note: The cryptographic algorithm specified here is SHA-384.

FCS_COP.1/SHA2/Integrity	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/Integrity	The TSF shall perform ***Hash value calculation*** in accordance with a specified cryptographic algorithm **SHA-384** and cryptographic key size **none** that meet the following**: FIPS 180-4**.

Application Note: The cryptographic algorithm specified here is SHA-384.

7.1.4 Security management (FMT)

FMT_MSA	Management of security attributes

FMT_MSA.1/AdminCA	Management of security attributes
Hierarchical to:	No other components
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1Specification of Management Functions
FMT_MSA.1.1/AdminCA	The TSF shall enforce the **admin access control SFP** to restrict the ability to **change accepted values of** the security attributes **AdminCA** to **Administrators**.
FMT_MSA.1/OpMode	Management of security attributes
Hierarchical to:	No other components
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1Specification of Management Functions
FMT_MSA.1.1/OpMode	The TSF shall enforce the **admin access control SFP** to restrict the ability to *modify* the security attributes **mode of operation** to **Administrators**.
FMT_MSA.3	Static attribute initialisation
Hierarchical to:	No other components
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1	The TSF shall enforce the **admin access control SFP, audit access control SFP, data from SRC SFP, dual control admin SFP, HTTP response SFP, ICAP header SFP, ICAP response SFP, and NTP synchronize SFP** to provide **fixed** default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow ~~the~~ **no one** to specify alternative initial values to override the default values when an object or information is created.

Application Note: Security Attributes, as mentioned in FDP_IFF and FDP_ACF, are not configurable.

FMT_MTD	**Management of TSF data**
FMT_MTD.1/AdminAccess	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/AdminAccess	The TSF shall restrict the ability to **access** the **TOE_CFG** to **administrators of the TOE.**
FMT_MTD.1/AdminModify	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/AdminModify	The TSF shall restrict the ability to *modify* the **TOE_CFG** to **two different administrators under dual control.**
FMT_MTD.1/AuditAccess	Management of TSF data
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1/AuditAccess	The TSF shall restrict the ability to **access** the **audit trail** to **auditors.**
FMT_MTD.1/AuditDelete	Management of TSF data
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1/AuditDelete	The TSF shall restrict the ability to **delete or move** the **audit data** to **auditors.**
FMT_MTD.3	Secure TSF data
Hierarchical to:	No other components.
Dependencies:	FMT_MTD.1 Management of TSF data
FMT_MTD.3.1	The TSF shall ensure that only secure values are accepted for **the TOE_CFG.**
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: **General management of TOE_CFG** **Management of security notifications:** - **Define receiver of notifications regarding security events** - **Define rules for monitoring audited events regarding security violations.** **Operation mode management:** - **Change the mode of the TOE from "Operational" to "Maintenance"** - **Change the mode of the TOE from "Maintenance" to "Operational"** **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.

FMT_SMR	**Security management roles**
FMT_SMR.2	Restriction on security roles
Hierarchical to:	FMT_SMR.1 Security roles
Dependencies:	FIA_UID.2 Timing of identification
FMT_SMR.2.1	The TSF shall maintain the roles: **administrator and auditor.**
FMT_SMR.2.2	The TSF shall be able to associate users with roles.
FMT_SMR.2.3	The TSF shall ensure that the conditions **Administrator and auditor roles are strictly separated,** are satisfied.

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

7.1.5 Protection of the TSF (FPT)

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

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

FPT_INC	TSF integrity checks
FPT_INC.1	TSF integrity
Hierarchical to:	No other components
Dependencies:	No dependencies
FPT_INC.1.1	The TSF shall run a suite of integrity checks *during initial start-up, periodically during normal operation* to demonstrate the integrity of **general configuration data and stored TSF executable code.**
FPT_INC.1.2	The TSF shall provide authorised users with the capability to verify the integrity of **general configuration data.**
FPT_INC.1.3	The TSF shall provide authorised users with the capability to verify the integrity of **stored TSF executable code.**
FPT_RCV	**Trusted recovery**
FPT_RCV.1	Manual recovery
Hierarchical to:	No other components.
Dependencies:	AGD_OPE.1 Operational user guidance
FPT_RCV.1.1	After**, refer to list in Application Note,** the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

Application Note: The maintenance mode can also be activated by an administrator under dual control. The following lists the events for entering the maintenance mode by the TOE

- *SmartCard as CryptoUnit is non-responsive*

- *Not all compartments could be reached*
- *Webserver certificate on SmartCard invalid*
- *Error from audit check*
- *Audit not available*
- *Configuration integrity fail*
- *Time has been manipulated*
- *TPM-Error*
- *System not initializied*
- *CryptoUnit not ready*
- *Problems while initializing at least one process, when changing in operational mode*
- *Integrity check failed*
- *Full storage*

7.1.6 Security audit (FAU)

FAU_ARP	**Security audit automatic response**
FAU_ARP.1	Security alarms
Hierarchical to:	No other components
Dependencies:	FAU_SAA.1 Potential violation analysis
FAU_ARP.1.1	The TSF shall take **the following actions:** - **send an e-mail to a configurable list of recipients** - **report into the audit-trail** - **place an indicator of any potential security violation on the Audit GUI** upon detection of a potential security violation.
FAU_GEN	**Security audit data generation**
FAU_GEN.1	Audit data generation
Hierarchical to:	No other components
Dependencies:	FPT_STM.1 Reliable time stamps
FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for *not Specified* level of audit; and c) **See Table 23.**
,FAU_GEN.1.2	The TSF shall record within each audit record at least the following information:

	a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the ~~PP/~~ST, **the information in Table 23**

Application Note:

For all the auditable events for the TOE, see 8.1.5.1 The following table gives an overview of auditable events and information available in the audit trail.

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

Table 23 auditable events

FAU_GEN.2	User identity association
Hierarchical to:	No other components
Dependencies	FAU_GEN.1 Audit data generation FIA_UID.2 Timing of identification
FAU_GEN.2.1	For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.
FAU_SAA	**Security audit analysis**
FAU_SAA.1	Potential violation analysis
Hierarchical to:	No other components
Dependencies	FAU_GEN.1 Audit data generation

FAU_SAA.1.1	The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.
FAU_SAA.1.2	The TSF shall enforce the following rules for monitoring audited events: a) Accumulation or combination of **auditable events:** **- Underflow of audit storage capacity** **- Upcoming expiration of certificates** **- Errors during self-tests.** known to indicate a potential security violation; b) **none**

Application Note: The TSF examines not only the validity of GUI certificates but also any other key materials, which are imported and stored in the key storage. If any of the certificates expires or will expire soon, there is a corresponding entry in the audit and alarm email for privileged users.

FAU_SAR	**Security audit review**
FAU_SAR.1	Audit review
Hierarchical to:	No other components
Dependencies:	FAU_GEN.1 Audit data generation
FAU_SAR.1.1	The TSF shall provide **auditors** with the capability to read **all audit information** from the audit records.
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
FAU_SAR.2	Restricted audit review
Hierarchical to:	No other components
Dependencies:	FAU_SAR.1 Audit review
FAU_SAR.2.1	The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read access.
FAU_STG	**Security audit event storage**
FAU_STG.2	Guarantees of audit data availability
Hierarchical to:	FAU_STG.1 Protected audit trail storage
Dependencies:	FAU_GEN.1 Audit data generation

FAU_STG.2.1	The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG.2.2	The TSF shall be able to *prevent* unauthorised modifications to the stored audit records in the audit trail.

Application Note:

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

FAU_STG.2.3	The TSF shall ensure that **all** stored audit records will be maintained when the following conditions occur: *audit storage exhaustion, failure, attack*
FAU_STG.4	Prevention of audit data loss
Hierarchical to:	FAU_STG.3 Action in case of possible audit data loss
Dependencies:	FAU_STG.1 Protected audit trail storage
FAU_STG.4.1	The TSF shall *prevent audited events, except those taken by the authorised user with special rights* and 1. **inform a configurable list of recipients (E-Mail Addresses of administrators and auditors) by an alarm message and** 2. **inform the auditor by an audit record and an alarm counter on the audit GUI, if the audit trail exceeds 80% of the total capacity of the audit trail storage device;** 3. **preserve a secure state (maintenance mode), if the audit trail exceeds 95% of the total capacity of the audit trail storage device and inform the administrators and the auditors by an audit record in which no data can be forwarded from SRC- to DST network;** 4. **prevent the change of the TOE configuration and send an alarm email to the administrators,** if ***99% of the total capacity of*** the audit trail ***storage device*** is full.

7.2 Dependency Rationale

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

#	SFR	Dependencies	Support of the Dependencies
1.	FDP_ACC.2	FDP_ACF.1 Security attribute based access control	Fulfilled by FDP_ACF.1

#	SFR	Dependencies	Support of the Dependencies
2.	FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	Fulfilled by FDP_ACC.2 which is hierarchical Fulfilled by FMT_MSA.3
3.	FDP_ETC.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	Fulfilled by FDP_ACC.2 which is hierarchical Fulfilled by FDP_IFC.2 which is hierarchical
4.	FDP_IFC.2	FDP_IFF.1 Simple security attributes	Fulfilled by FDP_IFF.1
5.	FDP_IFF.1	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	Fulfilled by FDP_IFC.2 which is hierarchical Fulfilled by FMT_MSA.3
6.	FDP_ITC.1	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation	Fulfilled by FDP_ACC.2 which is hierarchical Fulfilled by FDP_IFC. 2 which is hierarchical Fulfilled by FMT_MSA.3
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.1FCS_CKM.1FCS_CKM.1FCS_CKM.1	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	Fulfilled by FCS_COP.1 and FCS_CKM.4
10.	FCS_CKM.2	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Fulfilled by FDP_ITC.1 and FCS_CKM.4

#	SFR	Dependencies	Support of the Dependencies
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 FDP_ITC.1 and FCS_CKM.1FCS_CKM.1
12.	FCS_COP.1	[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 Crypto Unit in the operational environment.
13.	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.2 which is hierarchical Fulfilled by FMT_SMR.2 which is hierarchical to FMT_SMR.1 Fulfilled by FMT_SMF.1
14.	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
15.	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
16.	FMT_MTD.3	FMT_MTD.1 Management of TSF data	Fulfilled by FMT_MTD.1
17.	FMT_SMF.1	No dependencies	n.a.
18.	FMT_SMR.2	FIA_UID.2 Timing of identification	Fulfilled by FIA_UID.2

#	SFR	Dependencies	Support of the Dependencies
19.	FPT_STM.1	No dependencies	n.a.
20.	FPT_INC.1	No dependencies	n.a.
21.	FPT_RCV.1	AGD_OPE.1 Operational user guidance	n.a.
22.	FAU_ARP.1	FAU_SAA.1 Potential violation analysis	Fulfilled by FAU_SAA.1
23.	FAU_GEN.1	FPT_STM.1 Reliable time stamps	Fulfilled by FPT_STM.1
24.	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
25.	FAU_SAA.1	FAU_GEN.1 Audit data generation	Fulfilled by FAU_GEN.1
26.	FAU_SAR.1	FAU_GEN.1 Audit data generation	Fulfilled by FAU_GEN.1
27.	FAU_SAR.2	FAU_SAR.1 Audit review	Fulfilled by FAU_SAR.1
28.	FAU_STG.2	FAU_GEN.1 Audit data generation	Fulfilled by FAU_GEN.1
29.	FAU_STG.4	FAU_STG.1 Protected audit trail storage	Fulfilled by FAU_STG.2 which is hierarchical to FAU_STG.1

Table 24 Dependencies between the Security Functional Requirements (SFRs) for the TOE

7.3 Security assurance requirements rationale

490 The assurance level for evaluation of the TOE, its life cycle and operating environment are chosen as the
491 pre-defined assurance level EAL5 augmented with the following assurance components in accordance
492 with [CC_Part3]:

493 • ALC_FLR.2 Flaw reporting procedures.

494 • AVA_VAN.5 Advanced methodical vulnerability analysis

495 This corresponds to a total assurance level EAL5+. EAL5 is the highest level at which it is likely to be
496 economically to retrofit the existing product line of INFODAS GmbH.

497 The Level EAL5 augmented with ALC_FLR.2 was chosen to permit INFODAS GmbH as a developer to gain
498 maximum assurance from positive security engineering based on good commercial development practices

499 which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. The
500 selection of the component ACL_FLR.2 provides additional assurance of the TOE that potential security
501 flaws can be tracked and corrected by the developer.

502 Using AVA_VAN.5 component as augmentation for the level EAL5 allows to confirm that the TOE's security
503 measures provide the uppermost level of protection against the high attack potential.

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

Assurance class	Assurance Family	Assurance Component
Development	ADV_ARC	ADV_ARC.1 Security architecture description
	ADV_FSP	ADF_FSP.5 Complete semi-formal functional specification with additional error information
	ADV_IMP	ADV_IMP.1 Implementation representation of the TSF
	ADV_INT	ADV_INT.2 Well-structured internals
	ADV_TDS	ADV_TDS.4 Semiformal modular design
Guidance documents	AGD_OPE	AGD_OPE.1 Operational user guidance
	AGD_PRE	AGD_PRE.1 Preparative procedures
Life-cycle support	ALC_CMC	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS	ALC_CMS.5 Development tools 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.2 Compliance with implementation standards
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.3 Testing: modular design
	ATE_FUN	ATE_FUN.1 Functional testing
	ATE_IND	ATE_IND.2 Independent testing – sample
Vulnerability assessment	**AVA_VAN**	**AVA_VAN.5 Advanced methodical vulnerability analysis**

Table 25 Security Assurance Requirements (SARs)

7.4 Security Functional Requirements Rationale

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

#	SFRs	OT.SANITISED	OT.COMM	OT.USER_AUTHENTICATION	OT.ROLE_SEPARATION	OT.FOUR_EYES	OT.AUDIT_LOG	OT.AUDIT_PROTECT	OT.SECURE_STATE
1.	FDP_ACC.2/AuditAccess			x	x			x	
2.	FDP_ACC.2/AdminAccess			x	x				
3.	FDP_ACF.1/AuditAccess			x	x			x	
4.	FDP_ACF.1/AdminAccess			x	x				
5.	FDP_ETC.1/AuditKeys			x	x				
6.	FDP_IFC.2/DataFromSRC		x						x
7.	FDP_IFC.2/HTTP	x							
8.	FDP_IFC.2/ICAP	x							
9.	FDP_IFC.2/NTP	x							
10.	FDP_IFF.1/DataFromSRC		x						x
11.	FDP_IFF.1/HTTP	x							
12.	FDP_IFF.1/ICAP	x							
13.	FDP_IFF.1/NTP	x							
14.	FDP_ITC.1/Keys/AdminTLS			x					x
15.	FIA_UAU.2			x					
16.	FIA_UID.2			x					
17.	FCS_CKM.1/AES/Audit							x	
18.	FCS_CKM.1/HMAC/Audit							x	
19.	FCS_CKM.2/AES/Audit							x	
20.	FCS_CKM.2/HMAC/Audit							x	
21.	FCS_CKM.4			x					
22.	FCS_COP.1/ECDSA/AdminTLS			x					
23.	FCS_COP.1/AES/Audit							x	
24.	FCS_COP.1/HMAC/Audit							x	
25.	FCS_COP.1/SHA2/Audit							x	
26.	FCS_COP.1/SHA2/Integrity								x
27.	FMT_MSA.1/AdminCA			x	x				x
28.	FMT_MSA.1/OpMode			x	x				x
29.	FMT_MSA.3								x
30.	FMT_MTD.1/AdminAccess				x	x			
31.	FMT_MTD.1/AdminModify				x	x			
32.	FMT_MTD.1/AuditAccess				x				
33.	FMT_MTD.1/AuditDelete				x			x	
34.	FMT_MTD.3								x
35.	FMT_SMF.1				x		x		x
36.	FMT_SMR.2				x				

#	SFRs	OT.SANITISED	OT.COMM	OT.USER_AUTHENTICATION	OT.ROLE_SEPARATION	OT.FOUR_EYES	OT.AUDIT_LOG	OT.AUDIT_PROTECT	OT.SECURE_STATE
37.	FPT_STM.1						x		
38.	FPT_INC.1								x
39.	FPT_RCV.1								x
40.	FAU_ARP.1								x
41.	FAU_GEN.1						x		
42.	FAU_GEN.2						x		
43.	FAU_SAA.1								x
44.	FAU_SAR.1							x	
45.	FAU_SAR.2				x			x	
46.	FAU_STG.2							x	
47.	FAU_STG.4							x	

Table 26 Coverage of the Security Objectives for the TOE by SFRs

7.4.1 OT.SANITISED

508 OT.SANITISED is fulfilled by FDP_IFC.2/HTTP, FDP_IFC.2/ICAP, FDP_IFC.2/NTP, FDP_IFF.1/HTTP,
509 FDP_IFF.1/ICAP, FDP_IFF.1/NTP . These SFRs make sure that only data which comply to HTTP
510 response SFP, ICAP header SFP, ICAP response SFP, and NTP synchronize SFP are allowed to be
511 sent from DST- to SRC network.
512

7.4.2 OT.COMM

513 The SRFs, FDP_IFC.2/DataFromSRC and FDP_IFF.1/DataFromSRC address the security objective
514 OT.COMM about information flow through secure and defined communication channels from SRC-
515 to DST network.

7.4.3 OT.USER_AUTHENTICATION

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

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

520 FDP_ACC.2/AuditAccess and FDP_ACF.1/AuditAccess enforce the audit access control SFP in order
521 to identification and authentication of auditors to access, read, delete the audit trail.

522 FDP_ACC.2/AdminAccess and FDP_ACF.1/AdminAccess enforce the admin access control SFP in
523 order to identification and authentication of auditors to access and read the General TOE
524 configuration.

525 FDP_ETC.1/AuditKeys enforces the audit access control SFP for identification and authentication of
526 auditors to export the audit keys via AuditGUI using TLS connection.

527 Secure import of the cryptographic keys from outside of the TOE is ensured via
528 FDP_ITC.1/Keys/AdminTLS.

529 The destruction of the keys at ephemeral memory, when they are no longer needed, is fulfilled via
530 FCS_CKM.4.

531 FCS_COP.1/ECDSA/AdminTLS makes it possible to perform signature verification to authenticate
532 the user via the secure TLS connection.
533 FMT_MSA.1/AdminCA and FMT_MSA.1/OpMode ensure that only Administrators permitted to
534 access and change the security attributes in the TOE.

535

7.4.4 OT.ROLE_SEPARATION

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

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

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

544 FDP_ETC.1/AuditKeys enforces the audit access control SFP in order to identification and
545 authorisation of auditors to export the audit keys via Audit-GUI.

546 FMT_MTD.1/AdminAccess, FMT_MTD.1/AdminModify, FMT_MSA.1/AdminCA,
547 FMT_MSA.1/OpMode, FDP_ACC.2/AdminAccess, FDP_ACF.1/AdminAccess achieve the security
548 objective by assuring that only the role of the respective administrator is able to read or
549 delete/modify general TOE configuration data as well as TOE's security attributes.

550

7.4.5 OT.FOUR_EYES

551 FMT_MTD.1/AdminAccess ensure that only the administrator can have the access to the TOE
552 configuration and FMT_MTD.1/AdminModify ensures that the administrator can make the
553 corresponding change only under dual control through second administrator.

554

7.4.6 OT.AUDIT_LOG

555 This security objective aims that the TOE logs all changes to configuration data where the auditor
556 can track all changes and identify the user. FAU_GEN.1 is achieving this objective by requiring the
557 TOE to provide audit records for all changes made on the TOE configuration with time data and user
558 data. FAU_GEN.2 ensures that each individual user who made any change is tracked. FPT_STM.1
559 ensures that the TOE obtains reliable time stamps which added to the audit record. FMT_SMF.1
560 assures the configuration capability of the addressees of the warning notification.

561

7.4.7 OT.AUDIT_PROTECT

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

567 FCS_COP.1/HMAC/Audit, FCS_COP.1/AES/Audit, FCS_COP.1/SHA2/Audit,
568 FCS_CKM.1/AES/Audit, FCS_CKM.1/HMAC/Audit, FCS_CKM.2/AES/Audit,
569 FCS_CKM.2/HMAC/Audit addresses the cryptographic algorithms used to protect the integrity and
570 confidentiality of the audit records.

571 FAU_SAR.1 requires that the TOE provides mechanisms that auditors can read the audit records and
572 FAU_SAR.2 ensures that only users who have been granted access have read access to the records.

573 FAU_STG.4 reduces the risk of losing audit records by providing alerting mechanisms to be able to
574 detect exhaustions of the storage.

575

7.4.8 OT.SECURE_STATE

576 OT.SECURE_STATE has the objective that after initialisation process the TOE is constantly in a
577 secure state FAU_ARP.1, enables the TOE to detect potential insecure states, and if so, enter the
578 maintenance mode.

579 FDP_IFC.2/DataFromSRC and FDP_IFF.1/DataFromSRC support the TOE to enforce the data from
580 SRC SFP to perform correctly under operational mode, which prevents bypassing the secure data
581 transfer path.

582 FCS_COP.1/SHA2/Integrity addresses the cryptographic algorithms used to check the integrity of
583 the TOE's general configuration data.

584 FAU_SAA.1 corresponds to the TOE monitoring and detection ability of critical security events
585 concerning audit storage capacity and upcoming certificate expiration as well as errors during self-
586 tests.

587 FPT_INC.1 addresses performing self-test of the TOE during initial start-up and periodically whilst
588 operational mode. This functionality enables the TOE to check up the integrity of the general
589 configuration. If any failure is detected, the TOE changes its mode from operational to maintenance.
590 Regarding to manual recovery, FPT_RCV.1 ensures that the TOE can return to a secure state again.

591 FDP_ITC.1/Keys/AdminTLS enforces the admin access control SFP to protect the TOE when the
592 keys (as part of secondary assets) are imported from the outside of the TOE. Beside that these keys
593 shall fulfil pre-defined elliptic curves requirements.

594 FMT_MSA.1/AdminCA also enforces the admin access control SFP to restrict ability for change of
595 accepted values of AdminCA to administrators.

596 FMT_MSA.1/OpMode enforces the admin access control SFP to restrict the ability to modify
597 security attributes mode of operation, as part of general configuration of the TOE, to administrator
598 to protect secure operation.

599 FMT_MSA.3 ensures that through enforcing all defined security function policies for the TOE to
600 provide fixed default values for security attributes for the TOE.

601 To protect the TOE Security Functionality FMT_MTD.3 ensures that only secure values for the TOE
602 configuration and the TOE software are accepted.

603 FMT_SMF.1 ensures the management ability of general configuration, audit functions, security
604 notifications, as well as mode of operation of the TOE.

605 The focus of the SDoT SDD is on the aspect of confidentiality, i.e. it prevents sensitive information
606 from flowing from the network DST to the network SRC. From an operational perspective,
607 availability is also a very important aspect for uninterrupted operation. However, high availability is
608 not a primary security function. Despite this, it must be ensured that when configuration changes
609 are made on the primary node of the high availability variant, the configuration data on the
610 secondary nodes is synchronized with integrity, since manipulation could negatively affect the
611 security functionality of a node.

8 TOE Summary Specification (ASE_TSS.1)

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

8.1 TOE Security Functions

8.1.1 SF_PR: Protocol Response

613 The TOE provides unidirectional protocol transfer from SRC- to DST network and protocol status
614 responding mechanisms to SRC network which is the main security functionality of the TOE. The
615 following subsections will describe the main security properties of SF_PR.

8.1.1.1 SF_PR.1

616 The TOE enforces the HTTP- and ICAP response SFPs as well as ICAP header SFP for messages
617 which is sent between two different and separated networks. The TOE allows only a unidirectional
618 message flow from SRC- to DST network. No message flow from DST- to SRC network is possible.
619 Except for time synchronisation purposes (NTP), there shall not exist any other open port at the
620 interface between the TOE compartment, DI_HGH and DST network.

8.1.1.2 SF_PR.2

621 The TOE enforces the data from SRC SFP for all protocol data units coming from SRC network. In
622 accordance with FDP_IFF.1/DataFromSRC the only supported communication protocols are the
623 following: SMTP, HTTP, UDP, and TCP. Also, within the TOE only the following configured set of
624 communication protocols is supported: SMTP, HTTP, UDP and TCP.

8.1.1.3 SF_PR.3

625 The TOE being in maintenance mode does not let pass any message. The component of the TOE
626 which is responsible for forwarding the messages and sanitising the responses do not accept
627 messages and responses in maintenance mode. The components that are responsible for
628 administration and logging respectively auditing are not influenced in their functionality by this state
629 change.

8.1.1.4 SF_PR.4

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

632 8.1.1.5 SFRs addressed by SF_PR

633 The security function SF_PR addresses the requirements of the following SFRs:
634 FDP_IFC.2/DataFromSRC, FDP_IFC.2/HTTP, FDP_IFC.2/ICAP, FDP_IFC.2/NTP Subset information
635 flow control; FDP_IFF.1/DataFromSRC, FDP_IFF.1/HTTP, FDP_IFF.1/ICAP, FDP_IFF.1/NTP
636 Simple security attributes; and FMT_SMF.1 Specification of Management Functions and.

8.1.2 SF_CP: Channel Protection

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

8.1.2.1 SF_CP

639 The TOE enforces HTTP response SFP, ICAP header SFP, ICAP response SFP and NTP synchronize
640 SFP on all protocol data units which are sent from DST- to SRC network. The TOE sanitises any
641 protocol responses sent in direction of SRC network. A sanitised response only contains a known
642 status code and a pre-configured corresponding string which shortly describes the status code.

8.1.2.2 SFRs addressed by SF_CP

643 The security function SF_CP addresses the requirements of the following SFRs: FDP_IFF.1/HTTP,
644 FDP_IFF.1/ICAP, FDP_IFF.1/NTP Simple security attributes.

8.1.3 SF_DP: Data Protection

645 The TOE protects TSF data from modification with periodic integrity checks. These are general
646 configuration data, audit parameters, and public certificates. These parameters are integrity
647 protected with a fingerprint value, for cross-checking with known answer stored on the server
648 smartcard. The parameter values are transferred encrypted between the SDoT Adminstation and
649 the TOE via a dedicated admin network over a mutually authenticated TLS connection. However, the
650 secure TLS connection itself is not within the scope of the TOE. The Crypto Unit provides the
651 cryptographic support for signature generation.

652 Further, the TOE imports only the message data which are sent through the communication
653 protocols SMTP, HTTP, UDP and TCP.

8.1.3.1 SFRs addressed by SF_DP

654 The security function SF_DP addresses the requirements of the following SFRs: FDP_IFC.2/HTTP,
655 FDP_IFC.2/ICAP Subset information flow control FDP_IFF.1/HTTP, FDP_IFF.1/ICAP Simple
656 security attributes.

8.1.4 SF_AA: Authentication and Authorisation

657 The TOE includes security functionalities to provide authentication and authorisation mechanisms
658 which addresses the related SFRs. The TOE supports a secure channel initiated by the SDoT
659 Adminstation within a dedicated admin network. Based on Admin TLS connection establishment, the
660 authentication and authorisation can be performed.

661 SFRs addressed by SF_AA

662 FAU_SAR.2 Restricted audit review, FDP_ACC.2/AuditAccess Subset access control,
663 FDP_ACC.2/AdminAccess Subset access control, FDP_ACF.1/AuditAccess Security attribute based
664 access control, FDP_ACF.1/AdminAccess Security attribute based access control,
665 FDP_ETC.1/AuditKeys Export of user data without security attributes, FIA_UAU.2 User
666 authentication before any action, FIA_UID.2 Timing of identification, FMT_MSA.1/AdminCA,
667 FMT_MSA.1/OpMode Management of security attributes, FMT_MTD.1/AdminAccess,
668 FMT_MTD.1/AdminModify, Management of TSF data, FMT_MTD.1/AuditAccess Management of

669 TSF data, FDP_IFF.1/HTTP, FDP_IFF.1/ICAP, FDP_ITC.1/Keys/AdminTLS Import of user data
670 without security attributes, FDP_IFF.1/NTP Simple security attributes, FMT_MTD.1/AuditDelete
671 Management of TSF data, FMT_SMF.1 Specification of Management Functions, FMT_SMR.2
672 Restriction on security roles, FCS_CKM.4 Cryptographic key destruction,
673 FCS_COP.1/ECDSA/AdminTLS Cryptographic operation.

8.1.5 SF_AT: Audit Trail

674 The TOE includes security functionalities to meet the requirements addressed in the related SFRs
675 as listed in 8.1.5.2.

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

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

678 b. Generates an audit entry into the audit trail

679 c. Indicates the potential security violation on the audit GUI

680 For each auditable event resulting from an action of the authenticated human user, the TOE
681 associates the audit record unambiguously with the user role who performed any auditable action.

682 All audited records are provided by the TOE in a manner suitable for the auditor to interpret the
683 information. Audit information are displayed in a human readable presentation on the audit GUI. Only
684 the user with the role of the auditor has read access to the audit records.

685 8.1.5.1 Auditable Events

686 • Not available in ST-Lite version

8.1.5.2 SFRs addressed by SF_AT

687 FDP_ACF.1/AuditAccess Security attribute based access control, FDP_ETC.1/AuditKeys Export of
688 user data without security attributes, FAU_ARP.1 Security alarms, FAU_GEN.1 Audit data
689 generation, FAU_GEN.2 User identity association, FAU_SAA.1 Potential violation analysis,
690 FAU_SAR.1 Audit review, FAU_SAR.2 Restricted audit review, FAU_STG.2 Guarantees of audit data
691 availability, FAU_STG.4 Prevention of audit data loss, FDP_ACC.2/AuditAccess Subset access
692 control, FMT_MSA.3 Static attribute initialisation, FMT_MTD.1/AuditAccess, Management of TSF
693 data, FMT_MTD.1/AuditDelete, Management of TSF data, FMT_SMF.1 Specification of
694 Management Functions, FMT_SMR.2 Restriction on security roles, FPT_STM.1 Reliable time
695 stamps, FCS_COP.1/AES/Audit, FCS_COP.1/HMAC/Audit, and FCS_COP.1/SHA2/Audit
696 Cryptographic operation, FCS_CKM.1/AES/Audit, FCS_CKM.1/HMAC/Audit, Cryptographic key
697 generation, and FCS_CKM.2/AES/Audit, FCS_CKM.2/HMAC/Audit.

8.1.6 SF_SP: Self Protection

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

702 The TOE ensures that no message flow from SRC- to DST network is possible in maintenance mode.

703 The factory settings of all processes, i.e. after installation or after reset to default values, must be
704 strictly defined. If a process cannot start because of problems with the actual configuration data, i.e.
705 there are missing or erroneous values, the process will start with the factory settings.

706 The TOE provides a function to manage the mode of operation, for instance to put the TOE into
707 maintenance mode and back to operational mode.

708 The TOE provides authorised users with the capability to verify the integrity of general configuration
709 data and public certificates. The TOE provides authorised users the capability to verify the integrity
710 of stored TSF executable code. Further, the TOE cicely triggers integrity checks which are
711 automatically performed and during each restart of the TOE the integrity checks are performed.
712 Cryptographic references are securely stored in the Crypto Unit within the operational environment
713 of the TOE, which is included in the scope of delivery.

8.1.6.1 SFRs addressed by SF_SP

714 FDP_IFF.1/HTTP, FDP_IFF.1/ICAP, , FDP_IFF.1/NTP Simple security attributes, FMT_MSA.3 Static
715 attribute initialisation, FMT_MTD.1/AdminModify Management of TSF data, FPT_INC.1 TSF
716 integrity, FCS_COP.1/SHA2/Integrity Cryptographic operation, FPT_RCV.1 Manual recovery,
717 FMT_MTD.3 Secure TSF data, and FMT_SMF.1 Specification of Management Functions.

8.2 TOE Summary Specification Rationale

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

#	SFRs	TSFs
1.	FDP_ACC.2/AuditAccess	SF_AA, SF_AT
2.	FDP_ACC.2/AdminAccess	SF_AA,
3.	FDP_ACF.1/AuditAccess	SF_AA, SF_AT
4.	FDP_ACF.1/AdminAccess	SF_AA
5.	FDP_ETC.1/AuditKeys	SF_AA, SF_AT
6.	FDP_IFC.2/DataFromSRC	SF_PR
7.	FDP_IFC.2/HTTP	SF_DP, SF_PR
8.	FDP_IFC.2/ICAP	SF_DP, SF_PR
9.	FDP_IFC.2/NTP	SF_PR
10.	FDP_IFF.1/DataFromSRC	SF_PR
11.	FDP_IFF.1/HTTP	SF_AA, SF_SP, SF_DP, SF_CP, SF_PR
12.	FDP_IFF.1/ICAP	SF_AA, SF_SP, SF_DP, SF_CP, SF_PR
13.	FDP_IFF.1/NTP	SF_AA, SF_SP, SF_CP, SF_PR
14.	FDP_ITC.1/Keys/AdminTLS	SF_AA
15.	FIA_UAU.2	SF_AA
16.	FIA_UID.2	SF_AA
17.	FCS_CKM.1/AES/Audit	SF_AT
18.	FCS_CKM.1/HMAC/Audit	SF_AT
19.	FCS_CKM.2/AES/Audit	SF_AT
20.	FCS_CKM.2/HMAC/Audit	SF_AT
21.	FCS_CKM.4	SF_AA
22.	FCS_COP.1/ECDSA/AdminTLS	SF_AA
23.	FCS_COP.1/AES/Audit	SF_AT
24.	FCS_COP.1/HMAC/Audit	SF_AT
25.	FCS_COP.1/SHA2/Audit	SF_AT
26.	FCS_COP.1/SHA2/Integrity	SF_SP
27.	FMT_MSA.1/AdminCA	SF_AA
28.	FMT_MSA.1/OpMode	SF_AA
29.	FMT_MSA.3	SF_AT, SF_SP
30.	FMT_MTD.1/AdminAccess	SF_AA
31.	FMT_MTD.1/AdminModify	SF_AA, SF_SP
32.	FMT_MTD.1/AuditAccess	SF_AA, SF_AT
33.	FMT_MTD.1/AuditDelete	SF_AA, SF_AT
34.	FMT_MTD.3	SF_SP
35.	FMT_SMF.1	SF_AA, SF_AT, SF_SP, SF_PR
36.	FMT_SMR.2	SF_AA, SF_AT
37.	FPT_STM.1	SF_AT
38.	FPT_INC.1	SF_SP
39.	FPT_RCV.1	SF_SP
40.	FAU_ARP.1	SF_AT

41.	FAU_GEN.1	SF_AT
42.	FAU_GEN.2	SF_AT
43.	FAU_SAA.1	SF_AT
44.	FAU_SAR.1	SF_AT
45.	FAU_SAR.2	SF_AA, SF_AT
46.	FAU_STG.2	SF_AT
47.	FAU_STG.4	SF_AT

Table 27 TSS Rationale Overview

9 Bibliography

720 **Criteria and methodology interpretation**

721 [CC_Part1] Common Criteria for Information Technology Security Evaluation, Part 1:
722 Introduction and general model, Version 3.1, Revision 5, April 2017, CCMB-
723 2017-04-002

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

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

730 [CEM] Common Criteria for Information Technology Security Evaluation,
731 Evaluation methodology, Version 3.1, Revision 5, April 2017, CCMB-2017-
732 04-004

733 [AIS_41] Application Notes and Interpretation of the Scheme (AIS), AIS 41, Version
734 2, 31.01.11, Certification body of the BSI in the context of the certification
735 scheme

736 [AIS_35] Application Notes and Interpretation of the Scheme (AIS), AIS 35, Version
737 2, 12.11.11, Öffentliche Fassung eines Security Target (ST-lite)

738 [MC_ST_LITE] Common Criteria Recognition Arrangement, Management Committee,
739 Policies and Procedures, ST sanitising for publication, Version 1.0, April
740 2006, CCDB-2006-04-004

741 **Technical references**

742 [Atos_ST] Security Target „CardOS V5.3 QES“, Atos IT Solutions and Services GmbH,
743 Version 1.0, Revision 1.61, 07/2014

744 [Atos_CC] Certification Report for the Target „CardOS V5.3 QES V1.0“ from Atos IT
745 Solutions and Services GmbH, Cert-ID: BSI-DSZ-CC-0921-2014,
746 Maintainance Report BSI-DSZ-CC-0921-2014-MA-0