CSA
SINGAPORE

Cybersecurity
Certification Centre
CYBER SECURITY AGENCY OF SINGAPORE

Certificate Report

Version 1.0

7 September 2023

CSA_CC_22008

For

SDoT Filter SW
Version 6.2a

From

INFODAS GmbH

This page is left blank intentionally

Foreword

Singapore is a Common Criteria Certificate Authorizing Nation, under the Common Criteria Recognition Arrangement (CCRA). The current list of signatory nations and approved certification schemes can be found at the CCRA portal:

https://www.commoncriteriaportal.org

The Singapore Common Criteria Scheme (SCCS) is established for the info-communications technology (ICT) industry to evaluate and certify their IT products against the requirements of the Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 (ISO/IEC 15408) and Common Methodology for Information Technology Security Evaluation (CEM) Version 3.1 (ISO/IEC 18045) in Singapore.

The SCCS is owned and managed by the Certification Body (CB) under the ambit of Cyber Security Agency of Singapore (CSA).

The SCCS certification signifies that the target of evaluation (TOE) under evaluation has been assessed and found to provide the specified IT security assurance. However, certification does not guarantee absolute security and should always be read with the particular set of threats sought to be addressed and assumptions made in the process of evaluation.

This certification is not an endorsement of the product.

Amendment Record

Version	Date	Changes
1.0	7 September 2023	Released

NOTICE

The Cyber Security Agency of Singapore makes no warranty of any kind with regard to this material and shall not be liable for errors contained herein or for incidental or consequential damages in connection with the use of this material.

Executive Summary

This report is intended to assist the end-user of the product in determining the suitability of the product in their deployed environment.

The Target of Evaluation (TOE) is the SDoT Filter SW, v6.2a. revision 6.2.15566.31149 is a software security filter, which is part of a security gateway, and has undergone the CC certification procedure at the Singapore Common Criteria Scheme (SCCS).

The TOE comprises of the following components:

Identifier	Version
SDoT Filter SW (TOE)	SDoT Filter SW Version 6.2a Revision 6.2.15566.31149

Table 1 - TOE components identifier

The list of guidance documents to use with the product in its certified configuration is as follows.

Name	Version	Method of Delivery
Manual for SDoT Filter	V1.3	All guidance documents are provided digitally via encrypted email attachment in Portable Document Format or via the infodas download portal.
Manual for Administration	V1.5	
Product information – Requirements for Secure Operation	V1.3	

Table 2 - List of guidance documents

The SDoT Security Gateway comprises of the:

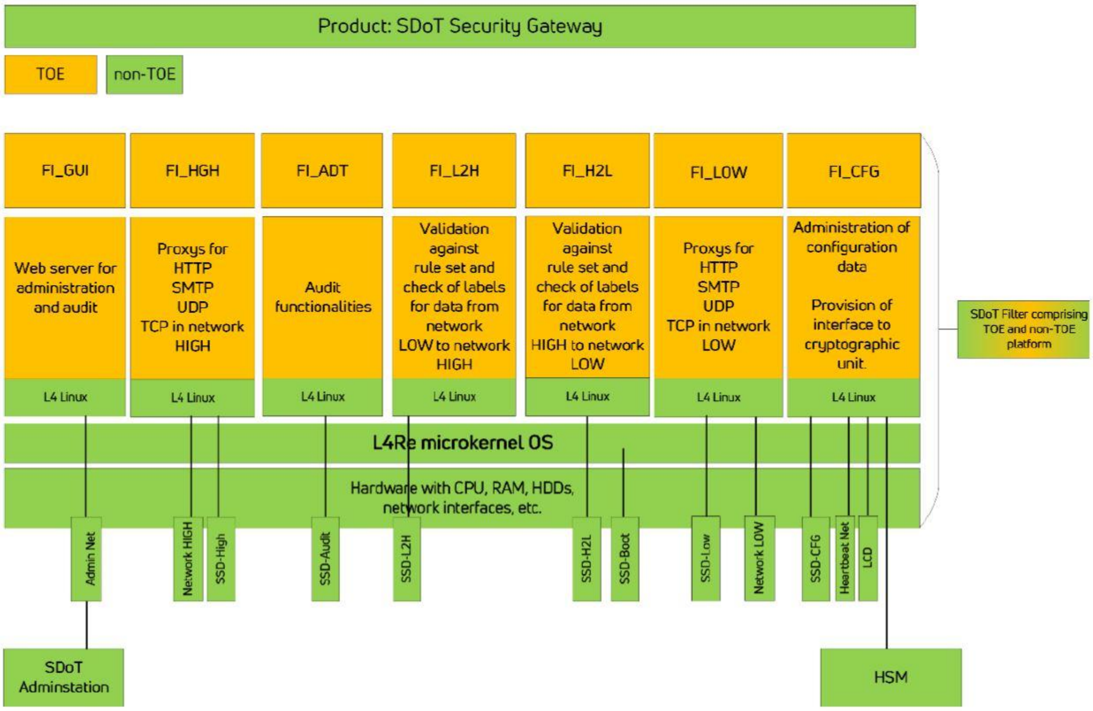
1. SDoT Filter Platform (hardware components including a hardware security module, firmware, and OS)
2. the TOE (i.e. SDoT Filter SW)

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

The TOE (as an application of the overall SDoT Security Gateway solution) provides filtering functionalities to check security labels for the transmission of data between two different classified networks and provides mechanisms to validate structured data objects against a pre-defined rule set.

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

- The TOE validates security labels attached to data and forwards the data after successful validation from the network HIGH to the network LOW or denies the data to be forwarded in case the label is not correct.
- The TOE validates structured data (e.g. XML) against configured rule sets.
- 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 strong binding between data and the corresponding security labels with digital signatures. The digital signatures of external labels are verified by the TOE. For labels created by the TOE, the related digital signature is generated by an HSM (in the operational environment) which does not belong to the TOE.
- The TOE re-builds (sanitisation) and converts (canonicalization) forwarded security labels
- The TOE provides secure auditing mechanisms of logs and secure administration capabilities.
- The TOE provides mechanisms for authentication.



Product: SDoT Security Gateway
TOE
non-TOE
FI_GUI
FI_HGH
FI_ADT
FI_L2H
FI_H2L
FI_LOW
FI_CFG
Web server for administration and audit
Proxys for HTTP SMTP UDP TCP in network HIGH
Audit functionalities
Validation against rule set and check of labels for data from network LOW to network HIGH
Validation against rule set and check of labels for data from network HIGH to network LOW
Proxys for HTTP SMTP UDP TCP in network LOW
Administration of configuration data
Provision of interface to cryptographic unit
L4 Linux
SDoT Filter comprising TOE and non-TOE platform
L4Re microkernel OS
Hardware with CPU, RAM, HDDs, network interfaces, etc.
Admin Net
Network HIGH
SSD-High
SSD-Audit
SSD-L2H
SSD-H2L
SSD-Boot
SSD-Low
Network LOW
SSD-CFG
Heartbeat Net
LCD
SDoT Adminstation
HSM

Figure 1: Logical view of the TOE

The evaluation of the TOE has been carried out by Atsec Information Security GmbH, an approved CC test laboratory, at the assurance level CC EAL 4 augmented with AVA_VAN.5 (Advanced Methodical Vulnerability Analysis) and ALC_FLR.2 (Flaw Reporting Procedures) and completed on 03 July 2023.

The certification body monitored each evaluation to ensure a harmonised procedure and interpretation of the criteria has been applied.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality	
Labelling Mechanism	The TOE provides mechanisms to perform labelling tasks. The TOE enforces data validation on all data which have to be labelled by the TOE. The TOE performs a syntax analysis on incoming structured data. The supported formats are XML, ADEXP, FSD, ASTERIX, FORMDATA, and JSON. All other formats will be rejected by the TOE. The security labels have a strong binding to the corresponding data. Any modification of the data or the related security label will invalidate both data and security label. This will lead to a rejection and the data will not pass the TOE. This feature is achieved with XML signatures. The TOE provides configuration mechanisms to define the parameters regarding the automatic labelling of the message data, in the case where a labelling generation is initiated by the TOE, with cryptographic support of the HSM. The TOE also re-builds (sanitisation) and converts (canonicalization) forwarded security labels.
Filtering Mechanism	The TOE provides filtering mechanisms which is the main security functionality of the TOE. It enforces the flow control policy for all data messages that are sent from the higher classified network to the lower classified network. The filtering policies can verify: • whether the protocol is allowed (SMTP, HTTP, UDP, TCP) and refer to the configured ports • whether an externally provided security label attached to the data has accepted security categories, a known structure, and expected attributes The TOE needs to be set into maintenance mode before configuration changes could be made. When the TOE is set to maintenance mode, no data communication is possible and all data messages are blocked.
Channel Protection	The TOE supports several mechanisms to provide security functionalities related to covert channel protection. It enforces the clean protocol policy on all protocol data units which are sent from network HIGH

	to the lower classified network. Only if the protocol data does not contain confidential information, the TOE will forward the data between the differently classified networks. The TOE controls the bandwidth which can be configured by the operator of the TOE. The TOE will then block all incoming and outgoing connections, if these exceed the configured bandwidth. The TOE can limit the capacity of information flow from the higher classified network to the network LOW.
Data Protection	The TOE enforces check label policy on all data messages with attached external security labels. Security labels are extracted from the data message for all data coming from the higher classified network.
Authentication and Authorisation	The TOE includes security functionalities to provide authentication and authorization mechanisms which addresses the related SFRs. The TOE supports a secure channel initiated by the SDoT Administration within a dedicated network. A separate management port is available, that is distinct from the communication ports. Only users which have the explicit permission to read the audit records of the TOE have access to the audit records. Only the user with the user role “Auditor” can access the GUI for auditing purposes. After successful identification and authentication of the auditor, the GUI grants access to the audit functionalities. The TOE enforces the dual control admin policy for all users trying to modify the general TOE configuration. And only the role of the auditor can read, move or delete audit records from the audit trail of the TOE. The TOE enforces that only two different administrators can make changes to the TOE configuration. One administrator temporarily stores the configuration data regarding any modification of configuration parameters of the TOE. Afterwards, a different administrator must confirm or reject the proposed changes. The changes will only apply, if the second administrator has confirmed the proposed modification of configuration data from the first administrator.
Audit Trail	The TOE creates audit records based on: • changes to the TOE configuration • processing of messages (recording origin, destination, time of transfer, result of the filter

	decision, data for uniquely identifying a message) - rejected messages Upon detection of a potential security violation the TOE takes the following actions: - the TOE sends an e-mail to a configurable list of addresses - generates an audit entry into the audit trail - indicates the potential security violation on the audit GUI For each auditable event resulting from an action of the authenticated human user, the TOE associates the audit record unambiguously with the user role who performed any auditable action. The TOE stores the DN of the certificate of the user role who caused the auditable event.
Self Protection	The TOE includes several functionalities to provide self-protection mechanisms. Part of architecture includes functions like the dual control administration policy and that no data flow is possible in maintenance mode. The TOE provides restrictive default values for parameters of the general TOE configuration, configuration for allowed security labels, rule sets for automatic data inspection, valid classifications, and categories. The TOE preserves a secure state by switching into maintenance mode when the following failures occur: - software failures - hardware failures - out of memory error - audit trail full power outage

Table 3: TOE Security Functionalities

Please refer to the Security Target [1] for more information.

The assets to be protected by the TOE has been defined. Based on these assets, the TOE Security Problem Definition has been defined in terms of Assumptions, Threats and Organisation Policies. These are outlined in Chapter 3 of the Security Target [1]

This Certification covers the configurations of the TOE as outlined in Chapter 5.3 of this report.

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate applies only to the specific version and release of the IT product in its evaluated configuration. This certificate is not an endorsement of the IT product by SCCS, and no warranty of the IT product by SCCS, is either expressed or implied.

Table of Contents

1 Certification

1.1 Procedure

The certification body conducts the certification procedure according to the following criteria:

- Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 [2] [3] [4];
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 5 [5]; and
- SCCS scheme publications [6] [7] [8]

1.2 Recognition Agreements

The international arrangement on the mutual recognition of certificates based on the Common Criteria Recognition Arrangement had been ratified on 2 July 2014. The arrangement covers certificates with claims of compliance against collaborative protection profiles (cPPs) or evaluation assurance levels (EALs) 1 through 2 and ALC_FLR. Hence, the certification for this TOE is partially covered by the CCRA.

The Common Criteria Recognition Arrangement mark printed on the certificate indicates that this certification is recognised under the terms of this agreement by all signatory nations listed on the CC web portal (https://www.commoncriteriaportal.org).

2 Validity of the Certification Result

This Certification Report only applies to the version of the TOE as indicated. The Certificate is valid till **6 September 2028**[1].

In cases of changes to the certified version of the TOE, the validity may be extended to new versions and releases provided the TOE sponsor applies for Assurance Continuity (i.e. re-certification or maintenance) of the revised TOE, in accordance with the requirements of the Singapore Common Criteria Scheme (SCCS).

The owner of the Certificate is obliged:

- When advertising the Certificate or the fact of the product's certification, to refer to and provide the Certification Report, the Security Target and user guidance documentation herein to any customer of the product for the application and usage of the certified product;
- To inform the SCCS immediately about vulnerabilities of the product that have been identified by the developer or any third party; and
- To inform the SCCS immediately in the case that relevant security changes in the evaluated life cycle has occurred or the confidentiality of documentation and information related to the TOE or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is no longer valid.

[1] Certificate validity could be extended by means of assurance continuity. Certificate could also be revoked under the conditions specified in SCCS Publication 3 [8]. Potential users should check the SCCS website (https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/singapore-common-criteria-scheme/product-list) for the up-to-date status regarding the certificate's validity.

3 Identification

The Target of Evaluation (TOE) is: SDoT Filter SW v6.2a Revision 6.2.15566.31149

The following table identifies the TOE deliverables.

Identifier	Version
SDot Filter SW	V6.2a Revision 6.2.15566.31149

Table 4 - TOE Deliverables

The guide for receipt and acceptance of the above-mentioned TOE are described in the set of guidance documents.

Name	Version	Method of Delivery
Manual for SDoT Filter	V1.3	All guidance documents are provided digitally via encrypted email attachment in Portable Document Format or via the infodas download portal.

Table 5 - Guidance Document (part of TOE deliverables)

Additional identification information relevant to this Certification procedure as follows:

TOE	SDoT Filter SW
Security Target	SDoT Filter SW Security Target Version 1.1
Developer	INFODAS GmbH
Sponsor	INFODAS GmbH
Evaluation Facility	Atsec Information Security GmbH
Completion Date of Evaluation	3 July 2023
Certification Body	Cyber Security Agency of Singapore (CSA)
Certificate ID	CSA_CC_22008
Certificate Validity	5 years from date of issuance

Table 6: Additional Identification Information

4 Security Policy

The TOE's Security Policy is expressed by the set of Security Functional Requirements listed and implemented by the TOE.

The TOE implements policies pertaining to the following security functional classes:

- Cryptographic Support
- Identification and Authentication
- User Data Protection
- Trusted Path/Channels
- Protection of the TSF
- Security Management
- Security Audit

Specific details concerning the above mentioned security policy can be found in Chapter 7 of the Security Target [1].

5 Assumptions and Scope of Evaluation

5.1 Assumptions

The assumptions defined in the Security Target [1] and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE environment and are listed in the tables below:

Environmental Assumptions	Description
OE.DIFF_NET	The TOE shall be connected to two networks with different classifications. The two networks are classified as HIGH and LOW.
OE.TRUSTW_ONLY	If besides the TOE, there are other connections between the two networks HIGH and LOW, these are established using trustworthy components only and do not violate the security policy of the TOE.
OE.HIGH_PROTECTION	The TOE and all physical parts outside the TOE which are scope of the delivery of the SDoT Security Gateway shall be connected within the higher classified network HIGH only.
OE.ACCESS	All access to the TOE and its physical operational environment is restricted to authorised persons only. These include the auditor, administrators and human users.

OE.TRUSTW_STAFF	The operational environment shall make sure that all privileged users of the TOE are trusted by the organisation operating the TOE.
OE.AUDIT_ENFORCE	The operational environment shall ensure that the audit data is regularly checked by an authorised and well-trained auditor in accordance with the security policy defined by the organisation operating the TOE.
OE.ROLE_SEPARATION	The operational environment shall ensure that the roles of the administrator and the auditor are owned by different persons.
OE.HSM	The operational environment shall ensure that the TOE is operated with IT systems which are capable of properly assigning labels to the corresponding data. Only appropriate data are signed with labels. The labelling mechanism is sufficiently cryptographically supported by hardware related security mechanisms. Since generation of cryptographic keys are not in scope of the TOE the operational environment shall ensure that state- of-the-art cryptographic mechanisms are used. The HSM and Smartcards which are in scope of delivery of the SDoT Security Gateway ensure that adequate cryptographic operations are used. Further, the output from the Random Bit Generator of the HSM shall be used directly without further post-processing by software. If TLS is used for communication to external systems the operational environment shall ensure that the digital signature for TLS used by the web server and communication proxies is generated by the HSM. Further, it shall be ensured that keys used for audit data protection is generated by the HSM.
OE.PKI	The operator of the TOE shall use a trustworthy PKI for digital signing certificates (CSRs) and generating and administrating CAs and CRLs.
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.

OE.USER_IDENT	The operational environment shall identify and authenticate all privileged users within the higher classified network HIGH before any actions can be performed.
OE.L4_PLATFORM	The operational environment regarding the operating system on which the TOE is running shall be an L4Re microkernel OS where each logically separated part of the TOE runs in a dedicated compartment. Within each compartment an own L4Linux, which is a para-virtualised Linux kernel within the provided hypervisor of L4Re, shall be used without privileges, and execute the processes of the TOE. The process separation properties of the L4Linux Kernel are shall be properly used.
OE.DEDICATED_ADMIN_NET	The TOE shall be connected to the SDoT Adminstation only through a dedicated network for administration purposes. The dedicated admin network shall be an isolated network within the higher classified domain HIGH.
OE.HIGH_AVAILABILITY	The operational environment shall ensure that if the operator of the TOE decides to use the optional functionality, namely the HA variant of the SDoT Filter, the operator will provide a physically separated network. The physically separated network shall be the only connection via the Heartbeat interface of the SDoT Filter designed to operate a cluster of redundant SDoT Filters.
OE.BOOT	The TOE shall use the secure start-up and initialisation mechanisms provided by the UEFI based secure boot process of the SDoT Filter platform. Further, the administrators shall follow the Guidance Documents to not modify the pre-configured BIOS-settings.

Table 7: Environmental Assumptions

Details can be found in section 4.2 of the Security Target [1].

5.2 Clarification of Scope

The TOE is limited to the software component of the SDoT Security Gateway.

The scope of evaluation is limited to the claims made in the Security Target [1].

Users are reminded to set up the TOE as per guidance documents to correctly deploy and use the TOE in the evaluated configuration.

5.3 Evaluated Configuration

The evaluated configuration comprises the following:

- the TOE itself with the version 6.2a and with the exact revision number being 6.2.15566.31149

5.4 Non-Evaluated Functionalities

Note that the following is non-TOE functionality of the product SDoT Security Gateway:

- The SMTP, HTTP, UDP, and TCP proxies support the functionality for mutually authenticated TLS connection with IT systems of the operational environment of the TOE within the network HIGH.
- The SMTP, HTTP, UDP, and TCP proxies support the functionality for mutually authenticated TLS connection with IT systems of the operational environment of the TOE within the network LOW.

5.5 Non-TOE Components

- (as part of the TOE operating environment, and therefore outside the scope of evaluation) the underlying platform which is a server appliance with UEFI Boot loader, HSM FW, L4Re microkernel OS, L4/Linux, and BusyBox,
- (as part of the TOE operating environment, and therefore outside the scope of evaluation) a HSM for cryptographic support in terms of labelling mechanisms, random numbers and secure storage
- (as part of the TOE operating environment, and therefore outside the scope of evaluation) a SDoT Adminstation laptop computer of the manufacturer GETAC with CentOS
- (as part of the TOE operating environment, and therefore outside the scope of evaluation) attached to the SDoT Adminstation a smartcard reader of the manufacturer Reiner SCT of type CyberJack Secoder or CyberJack RFID for authentication purposes at the SDoT Adminstation, and
- (as part of the TOE operating environment, and therefore outside the scope of evaluation) smartcards with certificate for initialisation purposes and empty user smartcards which must be initialised for authentication purposes.

6 Architecture Design Information

As described in the Security Target *[1]*, the high-level logical architecture of the TOE can be depicted as follows:

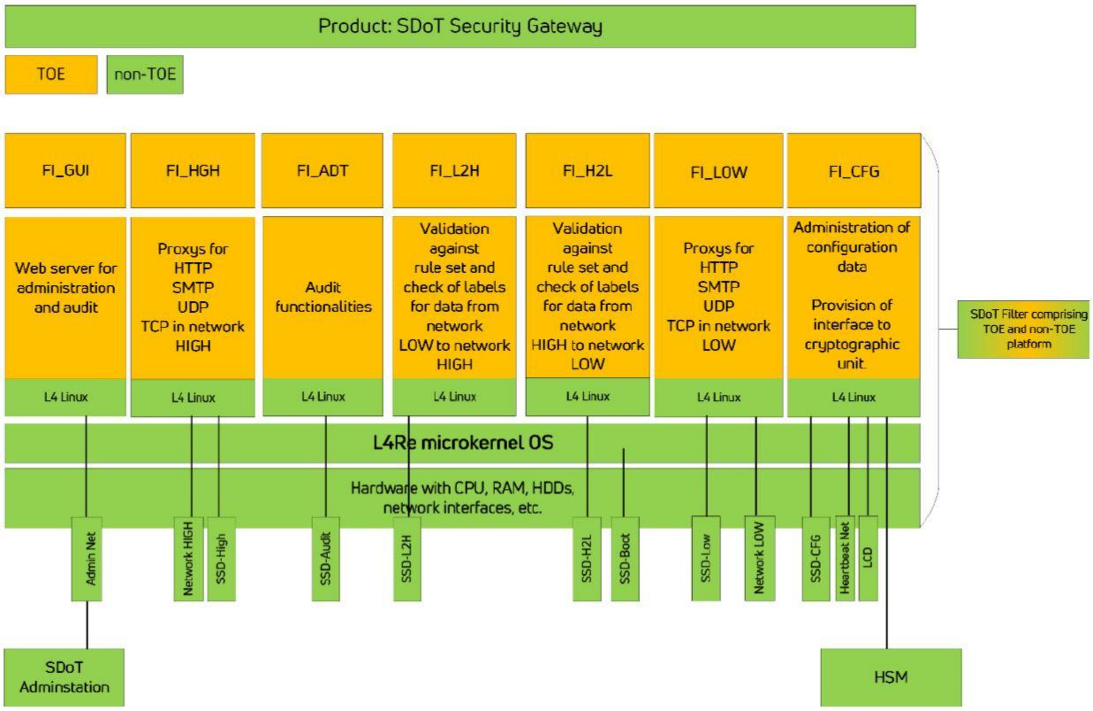

Product: SDoT Security Gateway
TOE
non-TOE
FI_GUI
FI_HGH
FI_ADT
FI_L2H
FI_H2L
FI_LOW
FI_CFG
Web server for administration and audit
Proxys for HTTP SMTP UDP TCP in network HIGH
Audit functionalities
Validation against rule set and check of labels for data from network LOW to network HIGH
Validation against rule set and check of labels for data from network HIGH to network LOW
Proxys for HTTP SMTP UDP TCP in network LOW
Administration of configuration data
Provision of interface to cryptographic unit
L4 Linux
SDoT Filter comprising TOE and non-TOE platform
L4Re microkernel OS
Hardware with CPU, RAM, HDDs, network interfaces, etc.
Admin Net
Network HIGH
SSD-High
SSD-Audit
SSD-L2H
SSD-H2L
SSD-Boot
SSD-Low
Network LOW
SSD-CFG
Heartbeat Net
LCD
SDoT Adminstation
HSM

Figure 2: Logical Architecture of the TOE (From [ST])

7 Documentation

The evaluated documentation as listed in Table 5 - Guidance Document (part of TOE deliverables) is being provided with the product to the customer. These documentations contain the required information for secure usage of the TOE in accordance with the Security Target.

Name	Version	Method of Delivery
Manual for SDoT Filter	V1.3	All guidance documents are provided digitally via encrypted email attachment in Portable Document Format or via the infodas download portal.

8 IT Product Testing

8.1 Developer Testing (ATE_FUN)

8.1.1 Test Approach and Depth

The developer tests were all specified in the test plan and grouped in several test areas:

- Authentication
- Data protection and cryptographic support
- Labelling
- Filtering
- Covert Channels
- Logging
- TOE Self Protection
- Admin commands
- Audit commands

The test plan contains a total of 113 tests, including test variations with different parameters.

8.1.2 Test Configuration

The TOE used for testing is configured according to the TOE guidance document [9] [10] [11].

8.1.3 Test Results

The test results provided by the developer covered all operational functions as described in the Security Target [1].

All test results from all tested environment showed that the expected test results are identical to the actual test results.

8.2 Evaluator Testing (ATE_IND)

8.2.1 Test Approach and Depth

As for the developer tests, the evaluator used the user-visible external interfaces of the TOE for most tests. In one case, did a review of the code to verify the AES-encryption is applied for audit events.

The following is a list of tested TOE functions (i.e. the affected SFRs) covered by the independent evaluator tests:

- identification and authentication of administrators (FIA_UID.2, FIA_UAU.2)
- dual access control of administrators (FDP_ACC.1)
- filter configurations based on ambiguous or missing port assignments, and detail tests for specific HTTP methods (FDP_IFC.1/DataToLow)
- label checking and its related e-mail that is associated with the label (FDP_IFC.1/Validation)
- NTP server configuration (FPT_STM.1)
- Failed authentication audit records (FAU_GEN.1)
- configuration of secure values (FMT_MTD.3)

The tests were mainly defined to exercise TSFI specifications, but also to verify claims made in the architecture/design documentation.

After the TOE was updated, the evaluator rerun parts of the developer sample (20 tests) and two of the additional evaluator tests.

8.2.2 Test Configuration

The evaluated configuration was performed according to the ST and the guide that details the CC-related requirements.

The TOE and environment configuration was equivalent to the developer test setup:

Component	Version
SDoT Filter SW (TOE)	Version 6.2a Revision 6.2.15566.31149
SDoT Adminstation	Version 1.5 (based on CentOS 6.9)
Test client HIGH/LOW	CentOS 8.2
Smartcard	Smartcard with CardOS 5.4 QES and Middleware v5.4 from ATOS

8.2.3 Test Results

All tests were successfully executed without relevant deviations.

8.3 Penetration Testing (AVA_VAN)

8.3.1 Test Approach and Depth

The evaluator used the MITRE CVE portal, general Google searches, and Google Scholar for finding publicly documented vulnerabilities against the TOE or its involved components. In addition he examined the ST, guidance, design, and testing information which lead to different types of tests:

- rather simple tool runs like testssl or nmap
- tests using the normal TOE functions and interfaces manually
- tests using the normal TOE application-level network interface involving a large number of input that has been adapted based on valid examples
- fuzzing on the layer of the used parser libraries where parts of the fuzzing framework is compiled into these TOE components
- source code reviews for usage of insecure functions

Tests have been performed for the following potential vulnerable scenarios:

- OpenSSL vulnerabilities
- Certificate validation
- Susceptible to fuzzing attacks

- Data exfiltration from HIGH to LOW – SMTP
- Data exfiltration from HIGH to LOW - SMTP extended
- Insecure state after HSM reset during operation
- Corrupted external labels
- Undocumented network interfaces/services
- Improper data handling during startup
- Certificates with weak hash sums
- Unsupported XSLT transformations in label
- Unallowed processing instructions in label
- Access to the MGMT interface from HIGH
- Improper handling of mixed labels and data
- Potential software weaknesses in C/C++ implementation
- Data leakage through back channels
- Flooding attacks
- Information gathering through system/service fingerprinting
- ICAP wrapping attack

Most tests used the external interfaces of the TOE, covering a wide range of security functions. Specifically in the area of certificates and label validation, the test approach was more focused to also exercise detailed TOE behavior.

In two cases, a different approach was chosen: a source code review was done for detecting problematic use of insecure C functions, and fuzzing was done against internal interfaces of recompiled parser components.

9 Results of the Evaluation

The Evaluation Technical Report (ETR) was provided by the CCTL in accordance with the CC, CEM and requirements of the SCCS. As a result of the evaluation, the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 4 augmented by ALC_FLR.2 and AVA_VAN.5 assurance package

This implies that the TOE satisfies the security requirements specified in the Security Target [1].

10 Obligations and recommendations for the usage of the TOE

The documents as outlined in Table 2 - List of guidance documents contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition, all aspects of Assumptions, Threats and OSPs as outlined in the Security Target [1] that are not covered by the TOE shall be fulfilled by the operational environment of the TOE.

Potential user of the product shall consider the results of the certification within his/her system risk management process. As attack methods and techniques evolve over time, he/she should define the period of time whereby a re-assessment of the TOE is required and convey such request to the sponsor of the certificate.

Potential users shall note that it is by design that Labels is accorded with higher priority over the Filter rules. Data to be sent from HIGH to LOW with a valid label will be allowed, regardless of the SDoT Filter rules configuration. It is recommended not to use the external Labelling Server, to prevent any unintended data leakages.

Users are reminded to set up the TOE as per guidance documents to correctly deploy and use the TOE in the evaluated configuration.

No additional recommendation was provided by the evaluators.

11 Acronyms

CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CCTL	Common Criteria Test Laboratory
CSA	Cyber Security Agency of Singapore
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
PP	Protection Profile
SAR	Security Assurance Requirement
SCCS	Singapore Common Criteria Scheme
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

12 Bibliography

[1] Infodas GmbH, “SDoT Security Gateway - SDoT Filter SW Security Target v1.1,” 21 August 2023.

[2] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model [Document Number CCMB-2017-04-001]. Version 3.1 Revision 5,” 2017.

[3] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components [Document Number CCMB-2017-04-002], Version 3.1 Revision 5,” 2017.

[4] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components [Document Number CCMB-2018-04-003] Version 3.1 Revision 5,” 2017.

[5] Common Criteria Maintenance Board (CCMB), “Common Methodology for Information Technology Security Evaluation - Evaluation Methodology [Document Number CCMB-2017-04-004], Version 3.1 Revision 5,” 2017.

[6] Cyber Security Agency of Singapore (CSA), “SCCS Publication 1 - Overview of SCCS, Version 5.0,” 2018.

[7] Cyber Security Agency of Singapore (CSA), “SCCS Publication 2 - Requirements for CCTL, Version 5.0,” 2018.

[8] Cyber Security Agency of Singapore (CSA), “SCCS Publication 3 - Evaluation and Certification, Version 5.0,” 2018.

[9] Infodas GmbH, “SDoT Filter Manual v1.3,” January 2023.

[10] Infodas GmbH, “SDoT Adminstation Manual v1.0,” August 2021.

[11] Infodas GmbH, “SDoT Security Gateway Product Information - Requirements for Secure Operations,” February 2022.

---End of Report --