Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1129-2021

for

SDoT Security Gateway
Version 6.2i

from

INFODAS GmbH

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1129-2021 (*)

Netzwerk- und Kommunikationsprodukte

SDoT Security Gateway
Version 6.2i

from	INFODAS GmbH
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.2

SOGIS
Recognition Agreement

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 5.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2 and ALC_FLR
only

Bonn, 27 September 2021

For the Federal Office for Information Security

Sandro Amendola
Head of Division

L.S.

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

2. Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BSI Schedule of Costs [3]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]

[1] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

[2] Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

[3] Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 3 March 2005, Bundesgesetzblatt I, p. 519

- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408.
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

3. Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

3.1. European Recognition of CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4. For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized under SOGIS-MRA for all assurance components selected.

3.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The current list of signatory nations and approved certification schemes can be seen on the website: https://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

[4] Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2+ ALC_FLR components.

4. Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product SDoT Security Gateway, Version 6.2i has undergone the certification procedure at BSI.

The evaluation of the product SDoT Security Gateway, Version 6.2i was conducted by atsec information security GmbH. The evaluation was completed on 21 September 2021. atsec information security GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the applicant is: INFODAS GmbH.

The product was developed by: INFODAS GmbH.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, as specified in the following report and in the Security Target.

For the meaning of the assurance components and assurance levels please refer to CC itself. Detailed references are listed in part C of this report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-assessment or re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 27 September 2021 is valid until 26 September 2026. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

[5] Information Technology Security Evaluation Facility

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,
2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

6. Publication

The product SDoT Security Gateway, Version 6.2i has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] INFODAS GmbH
INFODAS Gesellschaft für Systementwicklung und Informationsverarbeitung mbH
Rhonestraße 2
50765 Köln

B. Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1. Executive Summary

The Target of Evaluation (TOE) is part of the product SDoT Security Gateway which 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 authorized to get hold of confidential information from the higher classified network.

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

The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile.

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by ALC_FLR.2.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [8], chapter 7. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Functionality	Addressed issue
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 the data has accepted security categories, a known structure, and expected attributes While the TOE is managed, it is in maintenance mode. During this mode, no data

TOE Security Functionality	Addressed issue
	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 then 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 the "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 address the related SFRs. The TOE supports a secure channel initiated by the SDoT Adminstation within a dedicated network. Only users who 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. Only the role of the auditor can read, move or delete audit records from the audit trail of the TOE. The TOE enforces that only two different administrators can make changes to the TOE configuration. One administrator temporarily stores the configuration data regarding any modification of configuration parameters of the TOE. Afterwards, a different administrator must confirm or reject the proposed changes. The changes will only apply if the second administrator has confirmed the proposed modification of configuration data by the first administrator.
Audit Trail	The TOE creates audit records. Upon detection of a potential security violation the TOE takes the following actions: ● the TOE sends an e-mail to a configurable list of addressees ● 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

TOE Security Functionality	Addressed issue
	● audit trail full ● power outage

Table 1: TOE Security Functionalities

For more details, please refer to the Security Target [6] and [8], chapter 8.

The assets to be protected by the TOE are defined in the Security Target [6] and [8], chapter 3.2 . Based on these assets, the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and [8], chapter 3.

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

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 is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

SDoT Security Gateway, Version 6.2i

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW ISO	Software for installation of the TOE on the SDoT Security Gateway	6.2.15252. 29203	DVD
2	DOC	Manual for SDoT Filter	1.5	All guidance documents are provided digitally via encrypted email attachment in Portable Document Format or via the infodas download portal.
3	DOC	DOC Manual for SDoT Adminstation	1.0	
4	DOC	Product Information – Requirements for Secure Operation	1.2	

Table 2: Deliverables of the TOE

The SDoT Security Gateway comprises the SDoT Filter Platform (HW with HSM, FW, OS) and the SDoT Filter SW which is the TOE. The SDoT Security Gateway includes an SDoT Adminstation for Administration of the SDoT Filter. Therefore, the TOE is an application delivered together with a set of software and hardware components to the customer. The hardware parts and software parts besides the TOE are partially customized for SDoT Security Gateway to make sure that the TOE operates properly as intended with the dedicated delivery parts only.

The TOE itself is delivered via DVD. The software is signed with the INFODAS key and the related hash is verified during the secure boot process.

The guidance is delivered using an encrypted e-mail or downloaded online over HTTPS. Hashes are also made available to verify the integrity of the obtained guidance documents.

The TOE version is printed on the screen before confirming the installation, and can also later be reviewed under the "About SDoT" menu item in the Administration GUI as follows: SDoT-Version: 6.2.15252.29203 P1 Kurt[7]

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues: audit access control, admin access control, policy admin access control, dual control admin, dual control policy admin, data validation, check label, data to low, pre-filtering, supported protocol and clean protocol. Details can be found in chapter 5 of the Security Target [6] and [8].

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target 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. The following topics are of relevance:

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.

[7] Note that "P1 Kurt" is the internal name and patch level. It is not part of the TOE version.

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 is 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.

Details can be found in the Security Target [6] and [8], chapter 4.2.

5. Architectural Information

The system platform required by the TOE provides multiple environments for the implementation of compartments with strong separation mechanisms. Each compartment represents an isolated security domain with its own underlying L4Linux. The microkernel architecture provides control mechanisms to restrict the communication between the compartments. Each compartment houses an agent process which implements specific tasks. The short description of all components is given below:

- COMPARTMENT FI_GUI: provides access to the Administration GUI and Audit GUI
- COMPARTMENT FI_CFG: manages main configuration and performs monitoring tasks
- COMPARTMENT FI_ADT: this compartment provides functions for logging security relevant events.
- COMPARTMENT FI_H2L: all data which are sent from the higher classified network HIGH to the lower classified network LOW are processed by the so called “H2L SchemaValidator”
- COMPARTMENT FI_L2H: forwards data from network LOW to network HIGH
- COMPARTMENT FI_HGH: provides proxies for the supported components
- COMPARTMENT FI_LOW: performs the tasks analogous to the COMPARTMENT FI_HGH

For some cryptographic functions, an HSM in the TOE environment (resides inside the appliance hardware) is used.

Internally, the processes communicate with different protocols. The audit agent receives requests via the audit protocol while the admin agents receive commands using the MGMT protocol. Business data received from the LOW or HIGH network is wrapped in ICAP packets. With that, meta data is added to it that can be uniformly interpreted by the processes within different compartments.

The compartments contain several processes. The distribution of the processes over the compartment follows the rule that processes of the same trust level are part of the same compartment. Based on that, the proxies for example reside in their own compartments (FI_HGH and FI_LOW). The proxies themselves do not implement security functions, but they are be separated from other processes that do so.

For more information see the ST [6] and [8], section 1.4.2.

6. Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7. IT Product Testing

7.1. Developer Testing

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.

Test Approach

The developer performed all tests against the user-visible interfaces of the TOE. In some cases, data is analysed or manipulated outside the TOE:

- verify the contents of the audit hard disk after detaching it from the TOE
- manipulate the contents of the audit hard disk after detaching it from the TOE
- manipulating the system hard disk through booting into another system

In one case, the developer relies on his own code reviews to be sure that certain properties apply to the audit data (AES-GCM encryption of the audit data).

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:

Component	Version
SDot Security Gateway, SDoT Filter (TOE)	6.2.15252.29203
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

Table 3: Test Configuration

Results

All developer tests showed the expected results.

7.2. Evaluator Testing

The testing applied to two versions of the product. The first testing was performed on a previous revision (revision 6.2.14883.27405). After findings during the penetration testing, the TOE was slightly updated. As the updated TOE (revision 6.2.15252.29203) does not completely invalidate the previous test run where functionality was not affected by the update, the tests against the previous revision are mentioned here as well.

The evaluator rerun about 50% of the the developer tests on the previous revision and 20% on the final TOE version.

He further devised nine additional independent tests that he ran on the previous TOE revision. From these nine tests he reran three on the final TOE version. These were tests of functions that were affected by the TOE changes. The results of the remaining independent tests were considered to be still applicable to the final TOE version.

All tests that were performed on the final TOE version are marked with "P1" in the evaluator testplan.

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, he did a review of the code to verify that the AES-encryption is applied for audit events.

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.

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 (see table 3).

Test results

All tests were successfully executed without relevant deviation.

7.3. Evaluator Penetration Testing

The evaluator performed 14 penetration tests. Some existing open-source tools were used. In addition, the evaluator created a custom program that systematically generates new security labels based on a valid label.

Test approach

The evaluator used the MITRE CVE portal and general Google searches for finding publicly documented vulnerabilities against the TOE or its involved components.

Test depth

All 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.

Configuration

The initial run of the penetration tests identified some issues which required a TOE update (P1). After provision of the update, the majority of the penetration tests were rerun. The P1 update is the TOE version 6.2.15252.29203 as defined in the ST. Further configuration requirements as defined in the guidance for the secure use of the TOE were applied where relevant for the testing.

Test results

All tests were successfully executed without relevant deviation.

8. Evaluated Configuration

This certification covers the configuration of the TOE with the version 6.2i and with the exact revision number being 6.2.15252.29203. More information can be found in the SecurityTarget [6] and [8], section 1.3.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used for those components up to EAL 5.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_FLR.2 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: None
- for the Functionality: Product specific Security Target
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by ALC_FLR.2

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But cryptographic functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

The table in annex C of part D of this report gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its rating from cryptographic point of view. Any Cryptographic Functionality that is marked in column '*Security Level above 100 Bits*' of the following table with '*no*' achieves a security level of lower than 100 Bits (in general context) only.

The strength of the these cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2).

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 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 not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process, too.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

11. Security Target

For the purpose of publishing, the Security Target [8] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

12. Regulation specific aspects (eIDAS, QES)

None

13. Definitions

13.1. Acronyms

ADEXP	**ATS** Data Exchange Presentation
ASCII	American Standard Code for Information Interchange

AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CA	Certification Authority
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DN	Distinguished Name
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FSD	Field Structured Data
GUI	Graphical User Interface
H2L	High-to-Low
HDD	Hard Disk Drive
HMAC	Hash Message Authentication Code
HSM	Hardware Security Module
HTTP/S	Hypertext Transfer Protocol / Secure
ICAP	Internet Content Adaptation Protocol
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
JSON	Java Script Object Notification
L2H	Low-to-high
L4	Implementation of microkernel L4
L4Linux	Modified kernel of Linux running on top of L4
L4Re	L4 Runtime environment
Net SPIF	Network Security Policy Information File
NTP	Network Time Protocol
PP	Protection Profile
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
SPIF	Security Policy Information File
SSD	Solid State Drive
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
UDP	User Datagram Protocol
UEFI	Unified Extensible Firmware Interface
XML	Extensible Markup Language
XSD	XML Schema Definition

13.2. Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

Extension - The addition to an ST or PP of functional requirements not contained in CC part 2 and/or assurance requirements not contained in CC part 3.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Package - named set of either security functional or security assurance requirements

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

14. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017, https://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[8] https://www.bsi.bund.de/AIS

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website, https://www.bsi.bund.de/zertifizierungsreporte

[6] Security Target BSI-DSZ-CC-1129-2021, Version 2, 06.07.2021, SDoT Security Gateway Security Target, INFODAS GmbH (confidential document)

[7] Evaluation Technical Report, Version 4, 20.09.2021, Final Evaluation Technical Report, atsec (confidential document)

[8] Security Target BSI-DSZ-CC-1129-2021, Version 2, 08.07.2021, SDoT Security Gateway Security Target Lite, INFODAS GmbH (sanitised public document)

[9] Configuration list for the TOE, 19.07.2021, Main Configuration List (confidential document)

[10] SDoT Security Gateway - Produktinformation - Anforderungen an den sicheren Betrieb Product,Version SDoT SGW-62-I-PI-DE-1.2, July 2021

[8] specifically

- AIS 1, Version 14, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 14, Version 7, Anforderungen an Aufbau und Inhalt von Einzelprüfberichten für Evaluationen nach CC
- AIS 19, Version 9, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 23, Version 4, Zusammentragen von Nachweisen der Entwickler (Collection of Developer Evidence)
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 35, Version 2, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies

C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria can be followed:

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12
- On the detailed definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17
- The table in CC part 3 , Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published at https://www.commoncriteriaportal.org/cc/

D. Annexes

List of annexes of this certification report

Annex A:	Security Target provided within a separate document.
Annex B:	Overview and rating of cryptographic functionalities implemented in the TOE

Annex B of Certification Report BSI-DSZ-CC-1129-2021

Overview and rating of cryptographic functionalities implemented in the TOE

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
1		X.509 certificates	[RFC5246] (TLS1.2) [RFC5758]	n/a	n/a	Certificates are generated externally and imported into the TOE by a competent administrator.
2	Authentication (Server)	ECDSA signature verification and generation using SHA-2	[ANSIX9.62] [FIPS186-4] , B.4 [FIPS180-4] (SHA)	secp256r1 secp384r1 brainpoolP256r1 brainpoolP384r1 brainpoolP512r1	yes	Signature generation: done by HSM Signature verification: done by TOE Hashing: done by TOE
3	Authentication (Client)	ECDSA signature verification and generation using SHA-2	[ANSIX9.62] [FIPS186-4] , B.4 [FIPS180-4] (SHA)	secp256r1 secp384r1 brainpoolP256r1 brainpoolP384r1 brainpoolP512r1	yes	
4	Key establishment: Key agreement Ephemeral	TLS_ECDHE	[IEEE1363] (ECKAS_DH1)	secp384r1 brainpoolP384r1 brainpoolP512r1	yes	
5	Key derivation	PRF: HMAC with SHA-256, SHA-384 (default: prf_sha256 for TLSv1.2, also prf_sha384 possible)	[RFC2104] (HMAC) [FIPS180-4] (SHA) [RFC5246] (TLSv1.2)	variable	yes	
6	Authenticated Encryption	AES in GCM mode (AES_128_GCM, AES_256_GCM)	[FIPS197] (AES) [SP800-38D] (GCM) [RFC5288] (AES GCM within TLS)	Key Length: 128, 256	yes	
7	Trusted channel	FTP_TRP.1 [8] , Sec. 7.1.2	cf. all lines above	see above	yes	

Table 4: TOE cryptographic functions used for TLS protocol

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
1	Authentication	x.509 certificates		n/a	n/a	Certificates are generated externally and imported into the TOE by a competent administrator.
2		RSA signature generation and verification RSASSA-PKCS1-v1_5 using SHA-256, SHA-384, and SHA-512	[FIPS186-4] , B.3 [FIPS180-4] (SHA) [RFC3447]	Modulus length: 2048 to 8192	yes	Signature generation: done by HSM Signature verification: done by TOE Hashing: done by TOE
3		ECDSA signature generation and verification using SHA-2	[ANSIX9.62] [FIPS186-4] , B.4 [FIPS180-4] (SHA)	secp256r1 secp384r1 brainpoolP256r1 brainpoolP384r1 brainpoolP512r1	yes	Signature generation: done by HSM Signature verification: done by TOE Hashing: done by TOE
4	Integrity	SHA-2 SHA-256, SHA-384, SHA-512	[RFC6234] (cf. [FIPS180-4])	n/a	yes	

Table 5: TOE cryptographic functions used for security labelling

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
1	Audit data encryption	AES in GCM mode	[FIPS197] (AES) [SP800-38D] (GCM)	Key length: 256	yes	The HSM provides the AES key used by the TOE.
2	HMAC computa-tion for the audit records	HMAC-SHA-384	[RFC2104]	Key length: 384	yes	Private key stored on the HSM.
3		SHA-2 SHA-384	[RFC6234] (cf. [FIPS180-4])	n/a	yes	

Table 6: TOE cryptographic functions used for the audit data protection

References to cryptographic algorithms

[ANSI X9.62] Public Key Cryptography for the Financial Services Industry: the Elliptic Curve Digital Signature Algorithm (ECDSA), Version American National Standard X9.62-2005, Date 2005-11-16, https://standards.globalspec.com/std/1955141/ANSI%20X9.62

[FIPS180-4] Secure Hash Standard (SHS), 2015-08-04, https://csrc.nist.gov/publications/detail/fips/180/4/final

[FIPS186-4] Digital Signature Standard (DSS), 2013-07-19, https://csrc.nist.gov/publications/detail/fips/186/4/final

[FIPS197] Advanced Encryption Standard (AES), 2001-11-26, https://csrc.nist.gov/publications/detail/fips/197/final

[IEEE Std 1363-2000] IEEE Standard Specifications for Public-Key Cryptography, Version IEEE Std 1363-2000, 2000-08-29, https://standards.ieee.org/standard/1363-2000.html

[RFC2104] HMAC: Keyed-Hashing for Message Authentication, H. Krawczyk, M. Bellare, R. Canetti, 1997-02-01, Location http://www.ietf.org/rfc/rfc2104.txt

[RFC3447] Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, Jonsson, B. Kaliski, 2003-02-01, http://www.ietf.org/rfc/rfc3447.txt

[RFC5246] The Transport Layer Security (TLS) Protocol Version 1.2, T. Dierks, E. Rescorla, 2008-08-01, http://www.ietf.org/rfc/rfc5246.txt

[RFC5288] AES Galois Counter Mode (GCM) Cipher Suites for TLS, J. Salowey, A. Choudhury, D. McGrew, 2008-08-01, http://www.ietf.org/rfc/rfc5288.txt

[RFC5758] Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA, Q. Dang, S. Santesson, K. Moriarty, D. Brown, T. Polk, 2010-01-01, http://www.ietf.org/rfc/rfc5758.txt

[RFC6234] US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF), D. Eastlake 3rd, T. Hansen, 2011-05-01, http://www.ietf.org/rfc/rfc6234.txt

[SP800-38D] Recommendation for Block Cipher Modes of Operation: Galois/ Counter

Mode (GCM) and GMAC, 2007-11-28, https://csrc.nist.gov/publications/detail/sp/800-38d/final

Note: End of report