Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1193-2024

for

SDoT Software Data Diode, SDoT SDD 1.3i

from

INFODAS GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1193-2024 (*)

Netzwerk- und Kommunikationsprodukte

SDoT Software Data Diode, SDoT SDD
1.3i

from	INFODAS GmbH
Functionality:	Product specific Security Target Common Criteria Part 2 Extended
Assurance:	Common Criteria Part 3 conformant EAL 5 augmented by ALC_FLR.2, AVA_VAN.5
valid until:	05 December 2029

SOGIS
Recognition Agreement
for components up to
EAL 4

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, 5 December 2024

For the Federal Office for Information Security

Sandro Amendola
Director-General

L.S.

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

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87- D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

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]
- BMI Regulations on Ex-parte Costs [3]
- Special decrees issued by the Bundesministerium des Innern und für Heimat (Federal Ministry of the Interior and Community)
- 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]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408

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 BMI Regulations on Ex-parte Costs - Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) - dated 2 September 2019, Bundesgesetzblatt I p. 1365

- 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 according to the rules of SOGIS-MRA, i.e. up to and including CC part 3 EAL 4 components. The evaluation contained the component AVA_VAN.5 that is not mutually recognised in accordance with the provisions of the SOGIS MRA. For mutual recognition the EAL 4 components of these assurance families are relevant.

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 und für Heimat 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 and 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 Software Data Diode, SDoT SDD, 1.3i has undergone the certification procedure at BSI.

The evaluation of the product SDoT Software Data Diode, SDoT SDD, 1.3i was conducted by atsec information security GmbH. The evaluation was completed on 25 November 2024. 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 5 December 2024 is valid until 04 December 2029. Validity can be renewed 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 Software Data Diode, SDoT SDD, 1.3i 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 TOE (SDoT SDD SW) is the software for the product SDoT Software Data Diode (hardware and software) of INFODAS GmbH. The TOE version is 1.3i.

The SDoT SDD serves as boundary protection device between IP Networks with different demands on the level of protection needed. These two IP networks are identified as Source (SRC) and Destination (DST), and SDoT SDD ensures that there is no data leakage from DST to SRC but data from SRC to DST can always pass the TOE.

The TOE is an application delivered together with a set of software and hardware components, which are considered part of the TOE environment.

The TOE implements the following major security features:

- Limitation of message flow from SRC to DST i.e., messages coming from DST are not accepted and blocked by the TOE;
- Analysis and sanitization of necessary protocol-specific responses;
- Accepting of connections on configured ports, only. For each port, only correct communication according to the configured protocol is allowed;
- Provision of secure auditing mechanisms of logs and secure administration capabilities;
- Provision of authentication mechanisms;
- Preservation of a secure state in case of compromising events being detected;
- Implementation of regular checks for integrity of TOE binary and configuration files.

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 5 augmented by ALC_FLR.2, AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [9], 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
SF_PR: Protocol Response	The TOE provides unidirectional protocol transfer from SRC- to DST network and protocol status responding mechanisms to SRC network which is the main security functionality of the TOE.
SF_CP: Channel Protection	The TOE enforces HTTP response SFP, ICAP header SFP, ICAP response SFP and NTP synchronize SFP on all protocol data units which are sent from DST- to SRC network. The TOE sanitises any protocol responses sent in direction of SRC network. A sanitised response only contains a known status code and a pre-configured corresponding string which shortly describes the status code.

TOE Security Functionality	Addressed issue
SF_DP: Data Protection	The TOE protects TSF data from modification with periodic integrity checks. These are general configuration data, audit parameters, and public certificates. These parameters are integrity protected with a fingerprint value, for cross-checking with known answer stored on the server smartcard. The parameter values are transferred encrypted between the SDoT Adminstation and the TOE via a dedicated admin network over a mutually authenticated TLS connection. However, the secure TLS connection itself is not within the scope of the TOE. The Crypto Unit provides the cryptographic support for signature generation.
SF_AA: Authentication and Authorisation	The TOE includes security functionalities to provide authentication and authorisation mechanisms which addresses the related SFRs. The TOE supports a secure channel initiated by the SDoT Adminstation within a dedicated admin network. Based on Admin TLS connection establishment, the authentication and authorisation can be performed.
SF_AT: Audit Trail	Upon detection of a potential security violation the TOE takes the following actions: a) The TOE sends an e-mail to a configurable list of addresses b) Generates an audit entry into the audit trail c) Indicates the potential security violation on the audit GUI For each auditable event resulting from an action of the authenticated human user, the TOE associates the audit record unambiguously with the user role who performed any auditable action.
SF_SP: Self Protection	The TOE includes several functionalities to provide self-protection mechanisms. The TOE enforces the policy dual control admin SFP on all users attempting to change the general TOE configuration The TOE enforces that two different users of role administrator are required to be able to change (modify, insert, delete) the general TOE configuration. The TOE ensures that no message flow from SRC- to DST network is possible in maintenance mode

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] and [9], chapter 8.

The assets to be protected by the TOE are defined in the Security Target [6] and [9], 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 [9], 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 Software Data Diode, SDoT SDD, 1.3i

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	Installation ISO for installation of the TOE on the SDot SDD	1.3i	DVD
2	DOC	Manual for SDoT SDD: SDoT SDD-1.3-I-UM-DE/EN-1.6	1.3i	Provided digitally via E-Mail in Portable Document Format
3	DOC	Product information sheet: SDoT SDD-1.3-I-PI-DE-0.11	1.3i	

Table 2: Deliverables of the TOE

The TOE is delivered to the customer on an installation DVD (see item #1 in table 2 above), which contains a minimal buildroot system, the signed UEFI-Bootlader and the signed TOE and L4-microkernel components. The DVD is burnt using respective signed ISO9660-images available for various target system architectures. As all components are signed with a GPG key and cannot be modified once burnt to DVD, the integrity of the TOE is guaranteed during delivery. Confidentiality is of no concern, so no additional measures are implemented.

Guidance documentation is provided as password-protected PDF to the customer via encrypted email or via the Infodas Download portal, where the files can be placed encrypted for the respective customer for download using TLS version 1.2 or 1.3. In addition to the integrity protection provided by TLS during download, the password protection of the PDF files ensures that the files cannot be edited.

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: The security policy enforced is defined by the selected set of Security Functional Requirements and implemented by the TOE. The TOE implements two role-based access control policy to control access to the system for administrators and auditors, respectively. Regarding the modification of the TOE configuration, the TOE implements a dual-control policy requiring two separate administrators to activate such a configuration modification.

Data may only pass the TOE from the configured SRC network to the configured DST network as covered by a respective security policy. Due to standard communication protocols used, respective protocol-specific responses must be returned to the configured SRC network. The TOE implements response sanitation policies that ensure that no sensitive information is contained in those responses.

In order to enable time synchronization between the servers in the configured DST network and the servers in the configured SRC network, the TOE implements an NTP synchronization policy allowing for such synchronization without those servers needing to directly interact with each other.

Specific details concerning the above-mentioned security policies can be found in chapter 5 of the Security Target [6]. and [9]

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, OE.TRUSTW_ONLY, OE.ACCESS, OE.TRUSTW_STAFF, OE.CRYPTO_UNIT, OE.CRYPTO_UNIT_USER, OE.PKI, OE.NTP_SERVER, OE.L4_PLATTFORM, OE.DEDICATED_ADMIN_NET, OE.HIGH_AVAILABILITY, OE.BOOT

Details can be found in the Security Target [6] and [9], chapter 4.2.

5. Architectural Information

The Target of Evaluation is the software application SDoT SDD SW at version 1.3i, which is integral part of the INFODAS product SDoT SDD. The TOE is software only and is accompanied by guidance documentation.

The TOE can be installed on dedicated hardware and firmware provided by INFODAS for that purpose and as part of the overall SDoT SDD product- The hardware, firmware and the operating system are not part of the TOE but together form the underlying platform for TOE operation.

The TOE and its configuration is managed by a separate, administrative component, i.e. the SDoT Adminstation, consisting of hardware and software components and also being part of the operational environment of the TOE.

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. DeveloperTesting

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 harddisk after detaching it from the TOE
- manipulate the contents of the audit harddisk after detaching it from the TOE

Test Configuration

The evaluated configuration was performed according to the ST. and the guide that details the CC-related requirements. The only exception is, no other SDoT SDD was installed in the ITSEF lab and therefore high availability (HA) testing is not possible.

Component	Version
SDoT SDD (TOE)	1.3.1360.33832 P3 (which is equivalent to 1.3.3.1360.33832)

Component	Version
SDoT Adminstation	1.6 P4
Test client HIGH/LOW	Rockylinux 9.2
Smartcard	Smartcard with CardOS 5.3 QES and Middleware v5.4 from ATOS

Table 3: Test Configuration

Results

All developer tests showed the expected results.

7.2. Evaluator Testing

Test Approach

As for the developer tests, the evaluator used the user-visible external interfaces of the TOE for the tests.

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

- Input sanitization of GUI (FMT_MTD.3)
- Secure values test for MTD.3 (FMT_MTD.3)
- Allowed HTTP methods (FDP_IFC.2/HTTP, FDP_IFF.1/HTTP)
- Multiple NTP server (FDP_IFF.1/NTP)
- TLS support on Admin interface (no longer in scope after [ST]. update)
- HTTP parsing (FDP_IFC.2/HTTP, FDP_IFF.1/HTTP)
- TLS support on HA interface (no longer scope after [ST]. update)
- Mail from DST to SRC (FDP_IFC.2)
- TOE binary hash calculation (FPT_INC.1)

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

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.

Test results

All tests were successfully executed without relevant deviations.

7.3. Penetration Testing

Test Approach

The evaluator used the MITRE CVE portal and general Google searches to find publicly documented vulnerabilities against the TOE or its involved components. In addition the evaluator 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
- source code reviews for usage of insecure functions

Tests have been performed for the following potential vulnerable scenarios:

- Data leakage through back channels
- Data exfiltration from DST to SRC (NTP)
- Undocumented network interfaces/services
- Potential software weaknesses in C/C++ implementation
- HTTP vulnerabilities within HTTP request or responses
- SMTP header parsing
- Information gathering through system/service fingerprinting
- TLS vulnerabilities
- Improper data handling during startup
- Proper enforcement of connection limits
- Certificate validation

Test results

All tests run successfully against the current TOE. The tests showed at most minor deviations from the expected results. The evaluator did not find any exploitable vulnerability through testing.

8. Evaluated Configuration

This certification covers the following configurations of the TOE: The Target of Evaluation is the software application SDoT SDD SW at version 1.3i, which is integral part of the INFODAS product SDoT SDD. The TOE is software only and is accompanied by guidance documentation. The items listed in table 2 above represent the TOE.

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 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the technology was used:

(i) Joint Interpretation Library: Collection of Developer Evidence, version 1.5 as of January 2012.

(ii) *AIS* see [4].

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

- All components of the EAL 5 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_FLR.2, AVA_VAN.5 augmented for this TOE evaluation.

The evaluation has confirmed:

- for the Functionality: Product specific Security Target
  Common Criteria Part 2 Extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 5 augmented by ALC_FLR.2, AVA_VAN.5

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 120 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 following table 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 120 Bits*' of the following table with '*no*' achieves a security level of lower than 120 Bits (in general context) only. Note that the column “Security Level” refers to the pure cryptographic (mathematical) strength only, and does not take into account whatever exploitable weaknesses induced by side-channel leakage, physical attacks, or implementation flaws of any kind.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits	Comments
1	Role Identification	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	Role Identification	ECDSA signature verification using SHA-2	ANSI X9.62 [FIPS180-4] (SHA)	secp384r1 brainpoolP384r1 brainpoolP512r1	yes	Signature verification: TOE Hashing: TOE
3	Audit data encryption	AES in GCM mode	[FIPS197], [SP800-38D]	Key length: 256	yes	The smart card provides the AES key used by the TOE.
4	HMAC	HMAC-SHA-384	HMAC-SHA-384	Key length: 384	yes	Private key is

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits	Comments
	computation for audit records					stored on the smart card.
5	HMAC computation for audit records	SHA-2 SHA-384	[FIPS180-4]	N/A	yes	
6	Hash computation for integrity check	SHA-2 SHA-384	[FIPS180-4]	N/A	yes	

Table 4: TOE cryptographic functionality

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 [9] 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. Definitions

12.1. Acronyms

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
DVD	Digital Versatile Disc
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FSD	Field Structured Data
FW	Firmware
GUI	Graphical User Interface
HMAC	Hash Message Authentication Code
HTTP / S	Hypertext Transfer Protocol / Secure
HW	Hardware
ICAP	Internet Content Adaptation Protocol
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
L2H	Low-to-high
L4	Implementation of microkernel L4
NTP	Network Time Protocol
PP	Protection Profile
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
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality

UDP User Datagram Protocol

UEFI Unified Extensible Firmware Interface

12.2. 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.

13. 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[7] 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] SDoT SDD Security Target BSI-DSZ-CC-1193-2024, Version 2.2 14.10.2024, Infodas GmbH (confidential document)

[7] Final Evaluation Technical Report, Version 2, 21.11.2024, atsec information security GmbH, (confidential document)

[8] Configuration List SDoT Software Data Diode 1.3.3i, Version 0.4, 2024-08-07, Infodas GmbH (confidential document)

[9] SDoT SDD Security Target Lite, BSI-DSZ-CC-1193-2024, Version 1.1, 06.11.2024, INFODAS GmbH (sanitised public document)

[10] Manual for SDoT SDD (SDoT Software Data Diode - Handbuch), Version SDoT SDD-1.3-I-UM-DE/EN-1.6, July 2024, Infodas GmbH

[11] Product information sheet (SDoT Software Data Diode - Produktinformation), Version SDoT SDD-1.3-I-PI-DE-0.11,Oktober 2024, Infodas GmbH

[12] Joint Interpretation Library: Collection of Developer Evidence, version 1.5 as of January 2012.

[7] specifically

- AIS 1, Version 14, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 23, Version 4, Zusammentragen von Nachweisen der Entwickler (Collection of Developer Evidence)
- AIS31, Version 3.0, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- 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.