

Certification Report

BSI-DSZ-CC-1137-V4-2024

for

D-TRUST TSE-SMAERS, Version 1.4.3

from

D-Trust 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



Deutsches
erteilt vom



IT-Sicherheitszertifikat
Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1137-V4-2024 (*)

Fiscalization

D-TRUST TSE-SMAERS

Version 1.4.3

from Bundesdruckerei GmbH

PP Conformance: Common Criteria Protection Profile Security Module
Application for Electronic Record-keeping Systems
(SMAERS) Version 1.0, 15 July 2020, BSI-CC-PP-
0105-V2-2020

Functionality: PP conformant
Common Criteria Part 2 extended

Assurance: Common Criteria Part 3 conformant
EAL 2 augmented by ALC_CMS.3, ALC_LCD.1

valid until: 12 February 2032



SOGIS
Recognition Agreement



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

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.

Bonn, 13 February 2024

For the Federal Office for Information Security

Sandro Amendola
Director-General

L.S.



This page is intentionally left blank.

Contents

| | |
|---|----|
| A. Certification..... | 6 |
| 1. Preliminary Remarks..... | 6 |
| 2. Specifications of the Certification Procedure..... | 6 |
| 3. Recognition Agreements..... | 7 |
| 4. Performance of Evaluation and Certification..... | 8 |
| 5. Validity of the Certification Result..... | 8 |
| 6. Publication..... | 9 |
| B. Certification Results..... | 10 |
| 1. Executive Summary..... | 11 |
| 2. Identification of the TOE..... | 12 |
| 3. Security Policy..... | 13 |
| 4. Assumptions and Clarification of Scope..... | 13 |
| 5. Architectural Information..... | 14 |
| 6. Documentation..... | 14 |
| 7. IT Product Testing..... | 14 |
| 8. Evaluated Configuration..... | 16 |
| 9. Results of the Evaluation..... | 16 |
| 10. Obligations and Notes for the Usage of the TOE..... | 17 |
| 11. Security Target..... | 18 |
| 12. Regulation specific aspects (eIDAS, QES)..... | 18 |
| 13. Definitions..... | 18 |
| 14. Bibliography..... | 20 |
| C. Excerpts from the Criteria..... | 22 |
| D. Annexes..... | 23 |

A. Certification

1. Preliminary Remarks

Under the BSIG¹ 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 Security¹
- BSI Certification and Approval Ordinance²
- BMI Regulations on Ex-parte Costs³
- 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 3.1⁴ [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 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.

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 Proclamation of the Bundesministerium des Innern und für Heimat of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

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 D-TRUST TSE-SMAERS, Version 1.4.3 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1137-V3-2021. Specific results from the evaluation process BSI-DSZ-CC-1137-V3-2021 were re-used.

The evaluation of the product D-TRUST TSE-SMAERS, Version 1.4.3 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 31 January 2024. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)⁵ recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: D-Trust GmbH.

The product was developed by: Bundesdruckerei 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 13 February 2024 is valid until 12 February 2032. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

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,

⁵ Information Technology Security Evaluation Facility

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,
4. to conduct a reassessment before the end of 5 years in order to assess the robustness of the product against new state-of-the-art attack methods. This has to be done on the developer's own initiative and at his own expense. As evidence a report regarding a reassessment or a re-certification according to the regulations of the BSI certification scheme shall be provided.

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 D-TRUST TSE-SMAERS, Version 1.4.3 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 developer⁶ of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

⁶ Bundesdruckerei GmbH
Kommandantenstraße 18+22
10969 Berlin

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 named D-TRUST TSE-SMAERS and was evaluated in version 1.4.3. The TOE is a pure software TOE and is provided in form of a JAR-file as a Java application or JAR-file embedded in an Android application. The TOE provides the functionality of a SMAERS according to the Protection Profile BSI-CC-PP-0105-V2-2020 [8].

D-Trust provides a remote form of the Technical Security System (TSS) in a client / server architecture. The TOE operates as part of the D-Trust TSS client. It communicates with the Remote CSP Service, which is operated by D-Trust.

The TOE as a java application requires the Azul Zulu Community Java 17 runtime environment.

Furthermore, the TOE is only tested on different classes of operating systems which can be found in chapter 7.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Common Criteria Protection Profile Security Module Application for Electronic Record-keeping Systems (SMAERS) Version 1.0, 15 July 2020, BSI-CC-PP-0105-V2-2020 [8].

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 2 augmented by ALC_CMS.3, ALC_LCD.1.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.1. 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 |
|---|--|
| TSF.Startup and State | Secure startup |
| TSF.Self Testing and external entities | Self-testing functionality and test of the CSP |
| TSF.Authentication | User authentication |
| TSF.Access Control | Enforcement of access control policy |
| TSF.TOE lifecycle and signature key binding | TOE lifecycle states and signature key binding |
| TSF.Management | Handling of management functionality |
| TSF.Transaction Handling | TSF.Transaction Handling |
| TSF.Cryptographic support | Cryptographic support for PACE and RNG |
| TSF.Secure update | Support for Update Code Package functionality |
| TSF.Logging | Log generation |

Table 1: TOE Security Functionalities

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

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. 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], chapter 3.4, 3.2 and 3.3 respectively.

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:

D-TRUST TSE-SMAERS, Version 1.4.3

The following table outlines the TOE deliverables:

| No | Type | Identifier | Release | Form of Delivery |
|----|------|---|---|--|
| 1 | SW | Software delivered as JAR file: smaers-1.4.3-1856182.jar | SHA-256 hash: 103929c4624482722dafbf81274eec6568e9d2fb68eab61f38329da7db0c9f88 | For the desktop java application: Personal delivery, encrypted and signed mail or secure download portal. The deliverable is signed. In case the TOE is included in an Android application, it is delivered via the Google Play Store. The JAR file is digitally signed by the developer, allowing an integrity check. Further the JAR file included in the Android application is secured by the security mechanisms and delivery via the Google Play Store. |
| 2 | DOC | Integration-, configuration and operations manual [10] | Version 1.9.3 | Personal delivery, encrypted and signed mail or secure download portal. The deliverable is signed. |
| 3 | DOC | Guidance manual for the operational environment in the desktop context [11] | Version 7.2 | Personal delivery, encrypted and signed mail or secure download portal. The deliverable is signed. Delivered in case of desktop deployment |
| 4 | DOC | Guidance manual for the operational environment in the cloud context for Flatcar [12] | Version 1.7 | Personal delivery, encrypted and signed mail or secure download portal. The deliverable is signed. Delivered in case of Flatcar cloud deployment |

| No | Type | Identifier | Release | Form of Delivery |
|----|------|--|---|--|
| 5 | DOC | Guidance manual for the operational environment in the cloud context for Ubuntu [13] | Version 1.6.2 | Personal delivery, encrypted and signed mail or secure download portal. The deliverable is signed. Delivered in case of Ubuntu cloud deployment |
| 6 | DOC | Guidance manual for the operational environment in the Android context [14] | Version 1.7 | Personal delivery, encrypted and signed mail or secure download portal. The deliverable is signed. Delivered in case of Android deployment |
| 7 | DOC | Interface definition [15] File name: smaers-api.zip | SHA-256 hash: 8a39ab390fc9381d6bdd6f 00d60c83d75063ab4fa3d 65e3b115eb79317f072b0 | Personal delivery, encrypted and signed mail or secure download portal. The deliverable is signed. |

Table 2: Deliverables of the TOE

The TOE as a Desktop java application is internally delivered from the developer Bundesdruckerei to D-Trust either by personal delivery, encrypted and signed mail or via upload to a secure shared online storage. Similarly, the Integration-, configuration and operations manual [10], the guidance manuals for the varying operational environments [11], [12], [13] and [14] and the interface definition [15] are delivered either by personal delivery, encrypted and signed mail or via a secure download portal. All deliverables, except the Interface definition, are signed by the developer. The integrity of the Interface definition can be verified by the hash value.

The delivery in the sense of Common Criteria of all above-mentioned deliverables is done from D-Trust to the integrator in the same way as the delivery from Bundesdruckerei to D-Trust.

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:

- Security Management,
- User Identification and Authentication,
- User Data Protection,
- Protection of the TSF,
- Security Audit,
- Code Update Package import, and
- Trusted Channel between TOE and CSP.

Specific details concerning the above mentioned security policies can be found in Chapters 6.1 and 7.1 of the Security Target [6].

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.ERS,
- OE.SMAERSPlatform,
- OE.CSP,
- OE.CSPPlatform,
- OE.Transaction,
- OE.SecOEnv,
- OE.SUCP, and
- OE.SecUCP.

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

5. Architectural Information

The TOE consists of the following two subsystems:

SMAERS Impl This subsystem is responsible for the entire implementation of the SMAERS interface. Therefore, the entire functionality described in the guidance and in the API description is part of this subsystem. This subsystem interacts with the subsystem TCPackage in order to establish a trusted channel with the CSP.

TCPackage This subsystem is responsible for the communication to the CSP. It provides communication functionality to the subsystem SMAERS.

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

The TOE was tested on several operating systems and different hardware platforms, by the developer and also independently by the evaluator. The tested platforms were chosen to cover all classes of the evaluated configuration as specified in chapter 8. For all tests the TOE is configured and parameterized according to the guidance documents.

7.1. Developer testing

The tests are performed as Unit tests in the development tool. The developer considered the following aspects when designing his test approach:

- Tests to cover all actions and interfaces defined in [15],
- good case and bad case tests for each command defined in the document [15] and executable on the TOE, and

- tests of the cryptographic functionality by test vectors and functional negative tests of the PACE and trusted channel implementation.

In addition, there are so-called integration tests. These tests are implemented and performed by the developer to test the correct interaction of the SMAERS TOE with the CSP of the same developer. The test scenarios are based on use cases for the SMAERS.

7.2. Evaluator Tests

The evaluator tested all TSF using a series of test cases where each test case tests a specific aspect of the expected behaviour.

The TSF are mainly tested by running test scripts within the test environment at the TOE interface using the commands defined in [SMAERS-API]. In addition, the interface of the TOE to the CSP is tested by tests aiming at the PACE protocol and the secure messaging established after PACE. The TSF are stimulated within the test scripts and the behaviour is observed as return value of the TOE.

The selected tests cover tests of the TSFI related to

- Startup and State,
- Self-Testing and testing of external entities,
- Authentication,
- Access Control,
- TOE life cycle and signature by key binding,
- Management,
- Transaction handling,
- Cryptographic support,
- Secure update,
- Logging, and
- Preparative procedures, performed by the evaluator according to the guidance.

The test results have not shown any deviations between the expected test results and the actual test results.

7.3. Penetration Testing

The penetration testing was performed at the site of the evaluation body TÜVIT. The following attack scenarios have been tested, including but not restricted to: Statistical tests of random numbers, changing the predefined sequence of invocation of components, invalid input data (test on buffer overflows), attacks on authentication / access control, direct protocol attacks on authentication mechanisms / replay attacks on authentication mechanisms, padding oracle attack, PIN and PUK timing attack.

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential of Basic was actually successful in the TOE's operational environment as defined in the security target provided that all measures required by the developer are applied.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

The TOE has been developed as a Java application and requires a runtime environment as specified in the ST [6], Chapter 1.3.4. The TOE can be executed on any operating system that provides the specified runtime environment or integrated into an application running on an Android with outlined API level.

The TOE is intended for use on platforms based on the CPU architectures x64 and ARMv8 and the following classes of Operating Systems:

- Windows on x64: Windows POSReady 7, Windows 8.1, Windows 10, Windows 11, Windows 10 IoT Enterprise, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019
- Linux on x64: Red Hat Enterprise Linux, CentOS, Suse Enterprise Linux, Ubuntu, Debian, Rocky Linux, Flatcar
- Ubuntu LTS 20.04 or 22.04 on ARMv8
- macOS v13 Ventura on x64
- Android with an API level between 30 and 34 on ARMv8

All platforms and operating systems must be in a supported state (especially security updates) and must have been released before the certification date.

The D-TRUST TSE-SMAERS is part of the D-Trust TSS Client and requires the availability of the D-Trust TSS Client component that provides the functions for SE-API and a network connection to a certified CSP as part of the D-Trust back end.

The TOE needs to be installed according to the guidelines given in [10] and the operational environment needs to be secured according to one of the guidance manuals for the operational environment [11], [12], [13] or [14].

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.

The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

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

- All components of the EAL 2 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_CMS.3 and ALC_LCD.1 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-1137-V3-2021, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on a combination of

versions for desktop and Android, additional environments and their simplification and the removal of one API function.

The evaluation has confirmed:

- PP Conformance: Common Criteria Protection Profile Security Module Application for Electronic Record-keeping Systems (SMAERS) Version 1.0, 15 July 2020, BSI-CC-PP-0105-V2-2020 [8]
- for the Functionality: PP conformant
Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
EAL 2 augmented by ALC_CMS.3, ALC_LCD.1

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 "Cryptographic primitives" presented in chapter 1.4.2 of the Security Target gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its rating from cryptographic point of view. In this table, each Cryptographic Functionality achieves a security level of at least 100 Bits (in general context).

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.

In addition, the following aspects need to be fulfilled when using the TOE:

The secure usage of the TOE largely depends on the assumption OE.SMAERSPlatform. Therefore, the integration-, configuration and operations manual [10] and the supplementary guidances for the operational environment ([11], [12], [13] and [14]) are of particular importance. Central aspects in this context are:

- The configuration of the computer at the taxpayer (host computer) including hardware, firmware (UEFI), operating system and applications/services on which SMAERS and the FCC are installed MUST result in a secure execution environment on which the FCC, TSS Client and SMAERS can run.
- The taxpayer must not be the administrator of the host system of the SMAERS component. Personnel of the integrator or a subcontractor of the integrator MUST perform administration of the host computer (platform).
- All requirements in the documents [11], [12], [13] and [14] MUST be followed by the integrator.

Please note that the ST [6] lists in chapter 1.3.4. classes of operating systems on which the TOE was tested. This list may also include versions of operating systems which are no longer supported. The evaluated configuration requires that all platforms and operating systems must be in a supported state (especially security updates) and must have been released before the certification date.

11. Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12. Regulation specific aspects (eIDAS, QES)

None

13. Definitions

13.1. 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 |
| CCRA | Common Criteria Recognition Arrangement |
| CC | Common Criteria for IT Security Evaluation |
| CEM | Common Methodology for Information Technology Security Evaluation |
| cPP | Collaborative Protection Profile |
| CSP | Cryptographic Service Provider |
| EAL | Evaluation Assurance Level |
| ETR | Evaluation Technical Report |
| IT | Information Technology |

| | |
|---------------|---|
| ITSEF | Information Technology Security Evaluation Facility |
| JVM | Java Virtual Machine |
| PP | Protection Profile |
| SAR | Security Assurance Requirement |
| SE-API | Secure Element API (BSI TR-03151) |
| SFP | Security Function Policy |
| SFR | Security Functional Requirement |
| SMAERS | Security Module Application for Electronic Record-keeping Systems |
| ST | Security Target |
| SW | Software |
| TOE | Target of Evaluation |
| TSE | Technische Sicherheitseinrichtung |
| TSF | TOE Security Functionality |

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 TOE⁷
<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/zertifizierungsberichte>
- [6] Security Target BSI-DSZ-CC-1137-V4-2024, Version 2.3.8, 23 January 2024, D-TRUST TSE-SMAERS Security Target, D-Trust GmbH
- [7] Evaluation Technical Report, Version 2, 30 January 2024, TÜV Informationstechnik GmbH, (confidential document)
- [8] Common Criteria Protection Profile Security Module Application for Electronic Record-keeping Systems (SMAERS) Version 1.0, 15 July 2020, BSI-CC-PP-0105-V2-2020
- [9] Configuration list for the TOE, consists of (confidential documents): D-TRUST TSE-SMAERS - Referenzliste, Version 2.2.7, 30 January 2023, D-Trust GmbH
List of all files of the git repository of TSE-SMAERS, SHA-256 hash: 101e0b1fd2518e4216c01f1aad2fbeat50b869c3111b6220e3e7d33a3b81d9fb (files-smaers.txt)
- [10] D-TRUST TSE-SMAERS – API Dokumentation und Integratorhandbuch, Version 1.9.3, 23 January 2024
- [11] D-TRUST-TSE-WEB LEITLINIE ZUM SCHUTZ DER D-TRUST SMAERS DURCH DIE UMGEBUNG, Version 7.2, 28 August 2022, Bundesdruckerei GmbH
- [12] D-TRUST-TSE-WEB LEITLINIE ZUM SCHUTZ DER D-TRUST TSE-SMAERS DURCH DIE UMGEBUNG – CLOUD (for Flatcar), Version 1.7, 29 July 2022, Bundesdruckerei GmbH
- [13] D-TRUST-TSE-WEB LEITLINIE ZUM SCHUTZ DER D-TRUST TSE-SMAERS DURCH DIE UMGEBUNG – CLOUD (for Ubuntu), Version 1.6.2, 04 September 2023, Bundesdruckerei GmbH

⁷specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 38, Version 2, Reuse of evaluation results

- [14] D-TRUST-TSE-WEB LEITLINIE ZUM SCHUTZ DER D-TRUST SMAERS DURCH DIE UMGEBUNG - DF FISKAL CLOUD CONNECT, Version 1.7, 25 July 2022, Bundesdruckerei GmbH
- [15] Interface definition, SMAERS API Schnittstellenspezifikation, SHA-256 hash: 8a39ab390fc9381d6bdd6f00d60c83d75063ab4fa3d65e3b115eb79317f072b0, D-Trust GmbH

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.

Note: End of report