Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1137-2020

for

D-TRUST Web-Dienst TSE-SMAERS, version 1.1.2

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

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1137-2020 (*)

Fiscalization

D-TRUST Web-Dienst TSE-SMAERS
version 1.1.2

from D-Trust GmbH

PP Conformance:	Security Module Application for Electronic-keeping Systems (SMAERS) Version 1.0, 28 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_LCD.1 and ALC_CMS.3

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

Bonn, 30 September 2020

For the Federal Office for Information Security

Sandro Amendola
Head of Division

L.S.

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

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - 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 (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]
- 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 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 under CCRA-2014 for all assurance components selected.

[4] Proclamation of the Bundesministerium des Innern 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 Web-Dienst TSE-SMAERS, version 1.1.2 has undergone the certification procedure at BSI.

The evaluation of the product D-TRUST Web-Dienst TSE-SMAERS, version 1.1.2 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 30 September 2020. 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 30 September 2020 is valid until 30th of June 2021. 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.

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 Web-Dienst TSE-SMAERS, version 1.1.2 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] Bundesdruckerei GmbH
Kommandantenstraße 18
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 Web-Dienst TSE-SMAERS and was evaluated in version 1.1.2. The TOE is a pure software TOE and is provided as a Java 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.

There is one configuration of the TOE which can be executed on Windows, Linux and OS X or any other OS that provides the required support in form of the JVM. The TOE is only intended for use on platforms with CPUs of the x86 or ARMv7 architecture.

The TOE requires one of the following runtime environments:

- AdoptOpenJDK OpenJ9 (jdk8u252-b09_openj9-0.20.0), or
- Azul Zulu Community Java 8 (8u252b14 Zulu: 8.46.0.19).

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Security Module Application for Electronic-keeping Systems (SMAERS) Version 1.0, 28 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_LCD.1 and ALC_CMS.3.

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	Security functionalities and features
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	Handling of transaction operations
TSF.Cryptographic support	Cryptographic support for PACE and RNG
TSF.Secure update	Support for Update Code Package functionality
TSF.System Log	System 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 Web-Dienst TSE-SMAERS, version 1.1.2

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	Software library as JAR file for Windows, Linux and OS X: de.bdr.dtr.tseweb.client.smaers.impl-1.1.2.jar	SHA-256 hash: 3835214C8E1DDE54FA7F6E83DF1C67537D2C02275118FEE00A7A91DDEEA62CD1	Personal delivery, encrypted and signed mail or secure download portal. The deliverable is signed.
2	DOC	Integration-, configuration and operations manual [9]	Version 1.5.3 SHA-256 hash: BCB85D0C1E3365AC63CDDF36B484A4615A2B72F159F37244B0F234B6D9E32B7D	Personal delivery, encrypted and signed mail or secure download portal. The deliverable is signed.
3	DOC	Guidance for the operational environment [10]	Version 2.6 SHA-256 hash: CCE600BE50D1D0C2764E29D59AD2B45F10E71EF5844B3A4C4DEEEAE9255AFB64	Personal delivery, encrypted and signed mail or secure download portal. The deliverable is signed.
4	DOC	Interface definition File name: smaers-api.zip	SHA-256 hash: 872B358843F788D86AAF31BEEAF1C9BD9EFE58A90A6D46E7278AC6ECBCAAF779	Personal delivery, encrypted and signed mail or secure download portal. The deliverable is signed.

Table 2: Deliverables of the TOE

The TOE is internally delivered from the developer Bundesdruckerei to D-Trust either by personal delivery, encrypted and signed mail or via a secure download portal. Similarly, the manuals [9] and [10] and the interface definition are delivered either by personal delivery,

encrypted and signed mail or via a secure download portal. All deliverables are signed by the developer.

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:

- User Data Protection,
- User Identification and Authentication,
- Security Management,
- 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 6.2 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.SecCommCSP,
- OE.SUCP, and
- OE.SecUCP.

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

Additionally there’s a developer document named “D-TRUST-TSE-WEB Schutz durch die Umgebung” [10] available, which further describes requirements concerning the environment.

5. Architectural Information

The TOE consists of the following two subsystems:

SMAERS 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 Light.

TCPackage This subsystem is responsible for the communication to the CSP Light. 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 in the compiled configuration which can be executed on the operating systems Windows, Linux and macOS or any other OS, that provides the required support in form of the JVM, in the runtime environments that are in scope of the certification. Testing was done on a Standard PC running CentOS Linux 8.

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 the interface definition[7],
- good case and bad case tests for each command defined in the interface definition[7] 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.

All test cases were run successfully on this TOE version. The developer’s testing results demonstrate that the TOE operates as expected.

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 the interface definiton[7]. The TSF are stimulated within the test scripts and the behaviour is observed as return value of the TOE.

The tests are performed by test tools which use scripts. Test attributes, preconditions and post processing steps that are coded into the scripts ensure that the script execution is reproducible. The test environment, including also the keys and personalization data used

[7] See table 2 for the provided documentation.

in the test configuration, was provided by the developer and the test scripts were implemented by the evaluator.

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,
- System Log, 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 in the evaluator's test environment with the evaluator's test equipment in a virtual machine prepared and provided by the developer. The samples were provided by the sponsor and by the developer. The test samples were configured and parameterized by the evaluator according to the guidance documentation.

The following attack scenarios have been tested, including but not restricted to: Statistical tests of random numbers, attacks on network protocol parameters and authentication mechanisms.

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:

There is one configuration of the TOE for Windows, Linux and OS X or other operating systems which provide the necessary JVM. The D-TRUST Web-Dienst 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 table 2 and the operational environment needs to be secured according to the guidance for the operational environment [10].

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 resp. Protection Profile 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_LCD.1 and ALC_CMS.3 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Security Module Application for Electronic-keeping Systems (SMAERS) Version 1.0, 28 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_LCD.1 and ALC_CMS.3

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 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 100 Bits*' of the following table with '*no*' achieves a security level of lower than 100 Bits (in general context) only.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Standard of Application
1	Authenticity (of exported Log Messages)	SHA384withPLAIN-ECDSA	[FIPS_186-4] B.4 and D.1.2.4, [BSI-TR-03111]	384 bit, curve secp384r1	Yes	[TR-03153] [TR-03116-5]

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Standard of Application
2	Communication with CSP	PACE with AES CMAC CBC mode with PKCS5 padding	[BSI-TR-03110-2], [NIST800-90A], [NIST800-38B], [NIST800-38A], [PKCS5]	256 bit, curve brainpoolP256r1	Yes	[TR-03153] [TR-03116-5]

Table 3: TOE cryptographic functionality

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).

References for the Table above:

[FIPS_186-4] Federal Information Processing Standards Publication FIPS PUB 186-4, Digital Signature Standard (DSS), July 2013, U.S. department of Commerce / National Institute of Standards and Technology (NIST).

[BSI-TR-03110-2] BSI - Technical Guideline, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 2: Protocols for electronic IDentification, Authentication and trust Services (eIDAS), Version 2.21, 2016-12-21, Bundesamt für Sicherheit in der Informationstechnik.

[BSI-TR-03111] BSI - Technical Guideline, Elliptic Curve Cryptography, Version 2.10, 2018-06-01, Bundesamt für Sicherheit in der Informationstechnik.

[TR-03116-5] BSI - Technische Richtlinie, Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 5: Anwendungen der Secure Element API, 2020-01-27

[BSI-TR-03153] BSI - Technische Richtlinie, Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme, Version 1.0.1, 2018-12-20, Bundesamt für Sicherheit in der Informationstechnik.

[NIST800-90A] The NIST SP 800-90A Deterministic Random Bit Generator Validation System (DRBGVS), 2015-10-29, National Institute of Standards and Technology (NIST).

[NIST800-38B] NIST SP800-38B, Recommendation for Block Cipher Modes of Operation, The CMAC Mode for Authentication, 2005-05, National Institute of Standards and Technology (NIST).

[NIST800-38A] The NIST SP 800-90A Deterministic Random Bit Generator Validation System (DRBGVS), 2015-10-29, National Institute of Standards and Technology (NIST).

[PKCS5] PKCS #5: Password-Based Cryptography Specification Version 2.0, September 2000, https://tools.ietf.org/html/rfc2898.

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 integrator manual [9] and the supplementary guidance for the operational environment [10] 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).
- Other requirements in document [10] MUST be followed by the integrator.

Please note that the variants I and II described in [10] in chapter 8.1 only address the Microsoft Windows 10 operating system. The other operating systems listed in the ST [6] are covered by variant III and are based on an industry-specific standard that does not yet exist. In this case, the user of the certificate (the integrator) must agree his individual solution with the BSI until an agreed sector specific standard exists.

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

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
CRE	Client Remote Entity
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FW	Firmware
HW	Hardware
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
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSE	Technische Sicherheitseinrichtung
TSF	TOE Security Functionality
TSS	here in the fiscal context: Technical Security System / in general CC Context: TOE Security Summary

13.1. 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-1137-2020, Version 1.7.0, 2020-09-29, D-TRUST Web-Dienst TSE-SMAERS Security, D-TRUST GmbH

[7] Evaluation Technical Report, Version 3, 2020-09-29, TÜV Informationstechnik GmbH, (confidential document)

[8] specifically

- AIS 19, Version 9, 2014-11-03, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC
- AIS 20, Version 3, 2013-05-15, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 32, Version 7, 2011-06-08, CC-Interpretationen im deutschen Zertifizierungsschema

[8] Security Module Application for Electronic-keeping Systems (SMAERS) Version 1.0, 28 July 2020, BSI-CC-PP-0105-V2-2020

[9] D-TRUST Web-Dienst TSE-SMAERS – API, Dokumentation und Integratorhandbuch, Version 1.5.3, 2020-08-28, D-TRUST GmbH

[10] D-TRUST-TSE-WEB Schutz durch die Umgebung, Version 2.6, 2020-09-29, Bundesdruckerei GmbH

[11] Configuration list consists of:

D-TRUST Web-Dienst TSE-SMAERS – Referenzliste, Version 1.0.9, 2020-09-29, D-TRUST GmbH

List of all files of the git repository of TSE-SMAERS, files-smaers.txt, SHA-256 hash: F18F2FC3CB794F9453BB6A241651C6799B9313E11A4F075FB93FAB1D190FA629 (confidential document)

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 detailled 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