Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1140-2021

for

SMAERS for a.sign TSE Online Version 1.2.0

from

A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr 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-1140-2021 (*)

Fiscalization

SMAERS for a.sign TSE Online
Version 1.2.0

from	A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr 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, ALC_CMS.3

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, 11 November 2021

For the Federal Office for Information Security

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

Sandro Amendola
Head of Division

L.S.

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]

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

3. Recognition Agreements

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

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

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

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

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

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

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

3.2. International Recognition of CC – Certificates (CCRA)

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

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

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

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

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

4. Performance of Evaluation and Certification

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

The product SMAERS for a.sign TSE Online, Version 1.2.0 has undergone the certification procedure at BSI.

The evaluation of the product SMAERS for a.sign TSE Online, Version 1.2.0 was conducted by SRC. The evaluation was completed on 4 August 2021. SRC is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH.

The product was developed by: A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr 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 11 November 2021 is valid until 10 November 2029. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

[5] Information Technology Security Evaluation Facility

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,
2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.
4. to conduct a reassessment after 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 SMAERS for a.sign TSE Online, Version 1.2.0 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] A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH
Landstraßer Hauptstraße 1b, E02
1030 Wien
Österreich

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 Target of evaluation is the A-Trust SMAERS for a.sign TSE Online provided by A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH.

The Target of Evaluation (TOE) is a Security Module application implemented as software. A-Trust SMAERS for a.sign TSE Online is a software library that implements the client-server architecture running on a platform supporting secure storage of assets after being integrated into a separate CTSS Software of the developer (‘a.sign TSE Online’ TSS).

The TOE relies on an Utimaco CryptoServer CSPLight Version 1.0.0 (BSI-DSZ-CC-1145-2021) as a Cryptographic Service Provider Light (CSPL), located in the A-Trust Datacenter secure environment, for all cryptographic operations except for the TOE sided implementation of the trusted channel which is implemented using the Password Authenticated Connection Establishment (PACE) protocol [19] by the TOE itself. This CSPL is not part of this TOE.

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, ALC_CMS.3.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6. 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.GenLM Generation of Log messages	The TOE generates audit records for the following auditable events: • startup and shutdown • system operation commands as specified in [13] • reaching of the threshold of unsuccessful authentication • failure with preservation of secure state • setting of the version number of the UCP and upgrade of stored data TOE allows manual export of audit trail by the CSP role using the function exportAuditTrail retrieving the audit log messages from CSPL and exports them. Upon successful export the messages are cleared using the function clearAuditTrail.
SF.ImpExp Import of Transaction Data from and Export of Log mes-sage to CTSS interface component	The TOE imports Transaction Data (only if the TOE is in CTSS and CSP role) from the ERS and establishes a trusted channel with the CSPL using the PACE protocol. The TC uses only the signature key. TOE is responsible for the import of audit records. Import and export of data is per-formed

TOE Security Functionality	Addressed issue
	according to [13] and [14].
SF.IAA Identification of external entities and authentication of Administrators	TOE is delivered in an uninitialized state, the administrator has to set a new password. This password is used to authenticate the Administrator when the TOE acts on behalf of Administrator. Authentication reference data is verified using the secure platform mechanism. The administrator is able to reset this Authentication Data Record using unblockUser. The TOE starts in the Unidentified User role. The TOE tests the ERS and CSP Identity. Only if all tests of external entities and self-tests are successful, the TOE enables the CTSS interface and CSP role. A user is only associated with the Administrator role after successful authentication. After 10 unsuccessful attempts, the Administrator role gets blocked until it gets successfully unblocked using a valid PUK.
SF.SecMan Security management	The TOE maintains the following roles which are associated to users: unidentified user, administrator, CTSS interface role and CSP role. The TOE restricts the security management of TSF and TSF data to authenticated Admin-istrators. The TSF prevents management of the Transac-tion Number generation. Security Management functions can only be used after successful authentication of an administrator. Only administrators are allowed to determine and modify the behavior of the function. The last transaction number is incremented by TOE and is stored on the secure platform. No one is allowed to specify alternative initial values for the transaction number. Only administrator is able to delete and reset this Authentication Data Record. The TOE enforces strong passwords and changing the initial password.
SF.TEE Test of external entities	After ERS loads the TOE, it is in the secure state with the Unidentified User role. The TOE tests the ERS and CSP Identity. Only if all tests of external entities and self-tests are successful, the TOE leaves the secure state and enables the CTSS interface and CSP role. At startup and during operation the TOE ensures that the transaction number is strictly monotonically increasing and only registered client_Ids are allowed to use the according signing key and that the version number is only increasing after a successful update Only the role administrator is allowed to use the function password authentication, define a transaction timeout, use the management functions and modify their behaviour in case of failure regarding testing of external entities and select the auditable events and the automatic export of audit trails.
SF.TST Self-test and secure state	A-Trust provides cryptographic checksums of the TOE, user can verify the integrity. Furthermore the client component is signed which can be verified by platforms supporting code

TOE Security Functionality	Addressed issue
	signing. The TOE performs self-tests on startup, shutdown and periodically during operation. If one of the self-tests fails, it enters a secure state. The TOE also enters the secure state if the test of the electronic record-keeping systems fails, or the test of cryptographic service provider fails. User data is stored on the secure platform including a version number, hence illegal modification can be detected. The digital signature of the UCP is verified by the SMAERS platform during the platforms native installation process. After an update and on every startup the TOE verifies that the version number of the user data is not modified and no unauthorized downgrade attempt was made. Security attributes are unambiguously associated with the exported user data, because they are stored in the secure platform including a version number.
SF.SecUCP Secure download and authorized use of Update Code Package	The TOE is updated[7] using Update Code Packages which are signed by an authorized entity. Only Administrator is allowed to import received UCP if the digital signature of the UCP is successfully verified by the platform. Furthermore the version number of the UCP has to be equal or greater than the current version. User data is stored with its associated version number, which is validated after a successful update. In case of an unsuccessful update a log message is generated. The TOE ensures that any previous information content of a resource is made unavailable upon the deallocation of the resource after successful upgrade previous code and data is deleted.
SF.ImpExpUCP Secure Import and Export of User Data	During every export of user data, the version number of user data is included. On every import the TOE verifies that the version number of the user data is not modified and no unauthorized downgrade attempt was made.
SF.SecCommCSP Secure communication between TOE and CSP	The TOE and the CSPL are physically separated components and thus there is a trusted channel between the TOE and the CSPL. The protocol used for the trusted channel is PACE according to [12]. CSPL is authenticated using this PACE channel. Keys for the key agreement are gener-ated. A PACE PIN is used by TOE to establish the trusted channel to CSPL. Transmitted data in the secure channel is authenticated using a MAC. As soon as keys are not needed any more, they are deleted.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1.1. 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 3.2 - 3.4.

[7]The update process itself is an automatic process, that is also realized in part by non-TOE components.

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:

SMAERS for a.sign TSE Online, Version 1.2.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	A-Trust SMAERS for a.sign TSE Online SHA256: 6CD72990D3B1586935D867C6E533845F84F92B4C34C39A2ADEEB8DB05756489E	Version 1.2.0	Delivered as a software module (library).
2	DOC	Operational user guidance - SMAERS for a.sign TSE Online, A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH SHA256: A2D941F56DE711818461B9FE5C08D24ED-BEC1A1049A42C06E2CE34FC17839149	Version: 1.0.3, Date: 26.07.2021	Delivered as a PDF
3	DOC	Functional Specification – SMAERS for a.sign TSE Online, A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH SHA256: BE20682CDFD4D94015FCE6157BFFAD68AF0EA14FCA3CDCF4190F00456E8C4FA7Version: 1.0.2, Date: 26.07.2021,	Version: 1.0.2, Date: 26.07.2021,	Delivered as a PDF

Table 2: Deliverables of the TOE

The TOE is available for download by the TSS developer (A-Trust itself) on the internal GitLab Server. From there the TSS developer can download the package and verify the detached the signature. The signature can only be verified with the public PGP key that is sent directly to the TSS developer by the key owner. The verification of the public key finger print must be performed either over the phone or in person.

The TOE developer also requires the TSS developer to provide the end costumer all relevant information in order to verify that the TSS uses the correct TOE.

The verification procedures are defined by the developer in [10], chapter 8 (“Acceptance Procedures”).

Identification of the TOE by the User (TSS developer)

The TOE is delivered in form of a service and the accompanying documentation

The certified version of TOE is signed by A-Trust before delivery, allowing the developer to ensure that this TOE is a version published by A-Trust using the following steps:

1. download the package and the detached signature from the A-Trust GitLab Server

2. verify the signature using the following command which is shown below as a generic example:

gpg --verify .\smaers-1.0.0.zip.asc

The TOE itself provides the at_get_version command which returns the TOE Version as a string identifier as Version “1.2.0” (Output string of at_get_version: “status:0;data:smaers-service: 1.2.0”).

Since the taxpayer needs to verify the version of the TOE, the functions of TOE (especially at_get_version) need to be made accessible to the taxpayer. Furthermore the TOE needs to be included in the TSE without modifications and installed according to [11].

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 TOE implements a role-based access control policy to control administrative access to the system. In addition, the TOE implements policies pertaining to the following security functional classes:

- Security Management
- User Identification and Authentication
- User data protection
- Protection of the TSF
- Security Audit
- Update Code Package
- Trusted Channel to CSPLight

Specific details concerning the above mentioned security functions can be found in chap. 6 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:

Security Objectives for the operational environment defined in Security Target	Description according to [6]	Reference to Guidance
OE.ERS Trustworthy Electronic Record-Keeping System	The taxpayer shall correctly use an electronic record-keeping system that provides separately, correctly, completely and in real time all transaction data that are legally required for the generation of log messages to the TOE. The electronic record-keeping system shall support testing its presence and identity as an external entity by the TOE. The electronic record-keeping system shall produce receipts including not only the transaction data, but also the points in time whenever a transaction is started, completed or terminated, as well as the transaction number provided by the certified security device.	[10] sec. 2.3.1
OE.SMAERSPlatform Secure platform storage	The platform that executes the TOE has to ensure the integrity of the TOE itself and to provide secure storage which protects the integrity and confidentiality of stored security relevant objects as required. The platform verifies and installs the UCP.	[10] sec. 2.3.2
OE.CSP Cryptographic Service Provider Component	A CSP is remotely accessible via a trusted channel to the TOE (client-server architecture) and certified as compliant to [20] running on hardware that meets Appendix: Operational Requirements for CSPLight. The CSP exports audit records in form of audit logs meeting [13].	This OE may be fulfilled by the Utimaco CryptoServer CSPLight (BSI-DSZ-CC-1145-2021) as a remote CSPL in client-server architecture. The CSPL manu-facturer has to provide evi-dences about the platform hardware certi-fication and the TSS developer running the CSPLight in its

		premises has to provide evidence about being compliant re-garding to the Security Audit requirements as mandated in [8], sec. “Appendix: Operational Requirements for CSPLight”.
OE.CSPPlatform CSP as a Secure Platform of the TOE	In case of the platform architecture, the CSP provides a secure execution environment and security services for the TOE running on top.	This OE is not applicable and can be seen as fulfilled, since the TOE uses a client-server architecture and implements the trusted channel package functionality
OE.Transaction Verification of Transaction	The operational environment shall verify the validity of log message sequences by verification of the corresponding digital signatures, shall verify the transaction numbers as being consecutive without gaps, and shall verify the points in time when the transaction starts as being consecutively increasing with increasing transaction numbers, and consider the log messages. The taxpayer shall ensure that the cryptographic service provider holds digital signature creation data and a corresponding valid certificate. The certificate shall be securely distributed to the tax inspector.	[10] sec. 2.3.3
OE.SecOEnv Secure Operational Environment	The operational environment shall protect the integrity of the communication between the electronic record-keeping system and the TOE. The administrator shall act in a trustworthy way and is assumed to be the manufacturer or integrator. The administrator must be independent of the taxpayer.	[10] sec. 2.3.4

O.SecCommCSP Secure communication between TOE and CSP	The security target shall claim the package trusted channel to protect the integrity of the communication between the TOE and the CSP in the client-server architecture. In case of the platform architecture, the operational environment protects the integrity of the communication between the TOE and the cryptographic service provider.	Since the TOE implements the client-server architecture and this is a part of the TSF. It is listed here for the sake of completeness (since it is an OE in the Base part of the [8]).
OE.SUCP Signed Update Code Packages	The manufacturer issues digitally signed update code packages together with its security attributes.	[10] sec. 2.3.5
OE.SecUCP Secure download and authorized use of Update Code Package	The platform verifies the authenticity of received update code packages and installs only authentic update code packages.	UCP runs automatically, no interaction by user and administrator is required.

Table 3 Security Objectives for the operational environment

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

5. Architectural Information

The TOE is a software binary (32bit) running on Windows 10. It is used as a library for the product “a.sign TSE Online” of the developer A-Trust and must be integrated into the TSS Software by the TSS developer. TOE runs as a service and communicates with TSS using named pipes. The TOE runs as service in its own process. In order to call the TOE functions a TSS has to communicate with the service using an interprocess communication (IPC) protocol. The TOE implements this IPC using a server client architecture using a named pipe.

The TOE is the A-Trust SMAERS for a.sign TSE Online which is a part of the ‘a.sign TSE Online‘ TSS. It implements the client-server architecture running on a platform supporting secure storage of assets and relies on an Utimaco CryptoServer CSPLight Version 1.0.0 as a Cryptographic Service Provider Light (CSPL).

The SFR-enforcing subsystems of the TOE are:

- Initialization and Update (IU)
- State and Role Management (SRM)
- Transaction (TRANS)
- Crypto (CRYPTO)
- Secure Platform (SP)
- Authentication (AUTH)
- Self Test (ST)

- Audit Trail (AT)

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

Test Summary

The developer tested all TOE Security Functions. For all commands and functionality tests, test cases are specified in order to demonstrate its expected behavior. Repetition of developer tests were performed during the independent evaluator tests.

The evaluators have tested the TOE systematically against **basic** attack potential during their penetration testing results.

The achieved test results correspond to the expected test.

TOE Test configuration

Tests are performed on a TOE installed in a virtual machine running on a physical dedicated non-TOE hardware platform owned by the developer. The tested TOE version was 1.2.0.

The configuration respectively the version of the TOE can be retrieved from the test environment via the IPC call `at_get_version()`.The retrieved version number of the TOE was 1.2.0.

Testing approach and coverage

Developer Testing

The developer tests are performed on a TOE installed in a virtual machine running on a physical Platform owned by the developer. Access to this virtual machine is restricted to remote users with previously exchanged credentials.

The test environment is configured by the developer and does not need any actions by the evaluator to run the tests. This means that all necessary configuration is done by the developer.

The developer tests TSFIs by sending the respective command to the external IPC interface of the TOE. The tests consist of 124 distinct test cases and include positive and negative tests in the form of wrong or missing prerequisites and wrong or missing parameters.

All TSFI API test cases were executed successfully and ended up with the expected result.

Independent Testing

The tests are performed remotely on a virtual machine running in a test environment of the developer. The environment includes the TOE virtual machine and all necessary resources to repeat and conduct tests.

All developer tests were repeated by the evaluator and several independent tests were performed using the resources of the test environment. As the developer tests did not cover all of the interfaces of the TOE, the evaluators tested the missing interfaces in the independent test cases.

The overall test result is that no deviations were found between the expected and the actual test results.

Penetration Testing

The penetration testing was carried out in the evaluation lab on the test client which connects remotely to the TOE in the developer's test environment. The overall test result is that no deviations were found between the expected and the actual test results; moreover, no attack scenario with the attack potential "Basic" was actually successful.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

The TOE test configuration is defined by the notation:

- A-Trust SMAERS for a.sign TSE Online, Version 1.2.0, installed on the dedicated Remote VM implementing the SMAERS component in a client-server architecture that relies on the Utimaco CryptoServer CSPLight Version 1.0.0
- The guidance documentation:
  - Operational user guidance – SMAERS for a.sign TSE Online [10]
  - Functional Specification – SMAERS for a.sign TSE Online [15]

Tests are performed on a TOE installed in a virtual machine running on a physical dedicated non-TOE hardware platform owned by the developer. The tested TOE version was 1.2.0.

The configuration respectively the version of the TOE can be retrieved from the test environment via the API call at_get_version(). The retrieved version number of the TOE in the environment was 1.2.0. The version stated in the [6] is 1.2.0.

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.

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, 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, ALC_CMS.3

In the course of the evaluation the assurance refinements in [8], sec. 6.2.1 have been assessed for the TOE.

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

All cryptographic functionalities are described in detail in the Crypto Disclaimer. The strength of the cryptographic algorithms was not rated in the course of this evaluation procedure.

In general, for all applicable entries of cryptographic algorithms listed in the table below, the Security Level provided is greater than 100 bit.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
1	Authentication Trusted Channel Key Generation (ephemeral and session keys) Key Agreement (ECDH)	PACE with brainpoolP256r1	[12], Section 4.4	256	[8]	FCS_CKM.1
2	Integrity Authenticity	AES-256 CMAC	[17] (AES) [18] (CMAC)	256	[8]	FCS_COP.1
3	Cryptographic Primitive	Random Number Generation: hybrid deterministic RNG class DRG.3	[16]	n/a	[8]	FCS_RNG.1

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.

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

- The CTSS shall be installed according to [11]. For this the [11] shall be delivered to the user installing the CTSS as required in [10] chap. 8.1.4 together with the CTSS that integrates the TOE.
- The evaluators have acknowledged the manufacturer's environmental protection concept [11]. The environmental protection concept is a procedural guide with steps for setting up the environmental platform for the TOE. This conceptual guide is not intended to be used as a guidance in the sense of Common Criteria requirements. It addresses the (SMAERS) administrators in the context of the assumption A.Admin and the Security Objectives for the Operational Environment OE.SecOEnv as well as OE.SMAERSPlatform and OE.SecUCP, c.f. [6]. The (SMAERS) administrator role is to be considered trustworthy and trained, so that it can be assumed that they can check, evaluate and execute the steps in the environmental protection concept in order to provide the intended secure runtime environment of the TOE. Thus, the (SMAERS) administrator role mentioned [6] and in [11] is solely responsible to ensure that the platform is set up securely according to the concept depicted in [11]. In addition to the Guidance [10], the manufacturer is obliged to provide the (SMAERS) administrator the environmental protection concept authentically together with the delivery of the TOE and to instruct the (SMAERS) administrator role to comply to it accordingly.

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
CSPL	Cryptographic Service Provider Light
CTSS	Certified Technical Security System
EAL	Evaluation Assurance Level
ERS	Electronic Record-keeping Systems
ETR	Evaluation Technical Report
IPC	Interprocess Communication
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PACE	Password Authenticated Connection Establishment
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SMAERS	Security Module Application for Electronic-keeping Systems
ST	Security Target
TOE	Target of Evaluation
TSE	Technische Sicherheitseinrichtung
TSF	TOE Security Functionality
UCP	Update Code Packages

13.2. Glossary

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

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

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

14. Bibliography

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

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

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

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

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

[6] Security Target BSI-DSZ-CC-1140-2021, SMAERS for a.sign TSE Online, Version: 1.0.3, 26.07.2021, A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH

[7] Evaluation Technical Report - Summary, Version 1.8, 29.07.2021, SRC Security Research & Consulting GmbH, (confidential document)

[8] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 32, Version 7, 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] Configuration list for the TOE, Included in Chapter 3 of Lifecycle Support – SMAERS for a.sign TSE Online, Version 1.0.7, Date: 28.07.2021, A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH (confidential document)

[10] Operational user guidance - SMAERS for a.sign TSE Online, Version: 1.0.3, Date: 26.07.2021, A-Trust Gesellschaft für Sicherheitssysteme im elektroni-schen Datenverkehr GmbH

[11] Umgebungskonzept - SMAERS for a.sign TSE Online 1.0.0, Version: 0.5, Date: March 15 2021, A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH

[12] ICAO, Machine Readable Travel Documents, ICAO Doc9303, Part 11: Security Mechanisms for MRTDSs, seventh edition, 2015

[13] Technical Guideline BSI TR-03151 Secure Element API (SE API), Version 1.0.1, 20. Dezember 2018

[14] Technische Richtlinie BSI TR-03153 Technische Sicherheitseinrich-tung für elektronische Aufzeichnungssysteme, Version 1.0.1, 20. De-zember 2018

[15] Functional Specification – SMAERS for a.sign TSE Online, Version: 1.0.2, Date: 26.07.2021, A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Da-tenverkehr GmbH

[16] Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, AIS20, Version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik

[17] Federal Information Processing Standards Publication 197 (FIPS PUB 197), Advanced Encryption Standard (AES), 2001

[18] NIST Special Publication 800-38B Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication May 2005

[19] BSI, Technical Guideline TR-03110 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

[20] Protection Profile-Module CSPLight Time Stamp Service and Au-dit – Clustering, Version 1.0, registered under BSI-CC-PP-0113-2020, Federal Office for Information Security

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