Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1239-2024

for

Swissbit Cloud SMAERS Version 1.0.5

from

Swissbit AG

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-1239-2024 (*)

Fiscalization

Swissbit Cloud SMAERS
Version 1.0.5

from Swissbit AG

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_LCD.1 and 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 and CC Supporting Documents as listed in the Certification Report 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, 29 November 2024

For the Federal Office for Information Security

Sandro Amendola
Director-General

L.S.

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

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 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 und für Heimat (Federal Ministry of the Interior and Community)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408

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

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

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

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

3. Recognition Agreements

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

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

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

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

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

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

This certificate is recognized 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 Swissbit Cloud SMAERS, Version 1.0.5 has undergone the certification procedure at BSI.

The evaluation of the product Swissbit Cloud SMAERS, Version 1.0.5 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 20 November 2024. SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Swissbit AG.

The product was developed by: Swissbit AG.

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 29 November 2024 is valid until 28 November2032. 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 Swissbit Cloud SMAERS, Version 1.0.5 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] Swissbit AG
Industriestraße 4
9552 Bronschhofen
Schweiz

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 Swissbit Cloud SMAERS, Version 1.0.5 by Swissbit AG which is a Security Module application for Electronic Record-keeping Systems implemented as software. The TOE implements the client-server architecture running on a platform supporting secure storage of assets.

The TOE relies on the Swissbit Cloud CSP-L (BSI-DSZ-CC-1238) as a Cryptographic Service Provider Light (CSPL) 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 by the TOE itself. This CSP-L is not part of this TOE.

The TOE claims conformance to the Common Criteria Protection Profile Security Module Application for Electronic Recordkeeping Systems (SMAERS) [8].

The TOE provides the following functions:

- Generation and export of time-stamped and signed log messages, audit logs and system logs
- Secure Channel between SMAERS and CSPL
- Provision of Security Management of the TSF for administrators
- Support of receiving and integrity verification of Update Code Packages (UCPs)
- Self-test functionality

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_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. 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	Reference
SF.Log	Security Target [6], chapter 8.1
SF.Crypto	Security Target [6], chapter 8.2
SF.Management	Security Target [6], chapter 8.3
SF.Audit	Security Target [6], chapter 8.4

Table 1: TOE Security Functionalities

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 3.2 to 3.4.

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:

Swissbit Cloud SMAERS, Version 1.0.5

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	The delivered item is a .jar file containing the TOE.	Smaers-1.0.5.jar	Since the TOE integrator and the TSE Operator are the same as the developer and sponsor of the TOE (Swissbit AG), the signed jar file is stored in the git repository of Swissbit and the corresponding commit is tagged with smaers-v1.0.5. This completes the delivery process.
2	DOC	Swissbit Cloud SMAERS – Guidance Documentation, Version: 1.0.5, Date: 2024-11-13, Swissbit AG [10]	SHA256: caa7c2bbc8ab24857a59bf24a9c5acd7bbc05de733e215bef02717914e089e4f	The in-house delivery is done by storing the software and guidance documents in the corresponding git repository and tagging it accordingly.
3	DOC	digital signature file	smaers-1.0.5.jar.sig	Delivery method as above.

Table 2: Deliverables of the TOE

For its operation, the TOE needs the following hardware and software requirements fulfilled in its environment:

- Cryptographic Service Provider Light (CSPLight or CSPL) with CC EAL2 certification. The CSPL used with the TOE is the Swissbit Cloud CSP-L.
- The TOE is to be integrated into the Swissbit Cloud-TSE 2 of Swissbit AG which runs on a Google cloud server.
- Mass storage device for persisting signed transaction logs.
- Secure mass storage device for persisting internally stored data.

Swissbit AG describes a single delivery procedure for the TOE as the delivery of a pure software TOE.

The TOE integrator (which integrates the TOE into the TSE) and the TSE Operator (the entity which will operate the TOE) are the same as the developer and sponsor of the TOE (Swissbit AG). Therefore, no external delivery process of the TOE to a customer takes place. The in-house delivery is done by storing the software and guidance documentation in the corresponding git repository and tagging it accordingly.

The Swissbit Cloud SMAERS is provided as a pure software TOE. The integrator shall check its authenticity as follows:

To accept the TOE check that the version number in the jar file name matches the version in the tag and verify the jar file's signature with the code signing public key of Swissbit. This can be done with the command:

```
openssl dgst -sha256 -signature smaers-VERSION.jar.sig -verify
/smaers
/smaers_code_signing_public_key.pem smaers-VERSION.jar
```

Note that `version` has to be replaced accordingly with the current TOE version, i.e. 1.0.5. If these checks succeed, the TOE binary can be accepted and integrated as final TOE version.

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. The TOE implements policies pertaining to the security functional classes as described in chapter 6.1 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 topics listed in chapter 4.2 of the ST [6] are of relevance.

5. Architectural Information

The TOE is a software TOE running as part of a TSE on dedicated non-TOE hardware (Google Cloud server) as well as dedicated non-TOE software (Docker, Ubuntu 24.04), building the non-TOE platform. It consists of multiple SMAERS units which operate independently from each other. The platform is expected to provide protection against physical intrusion and tampering, the protection mechanisms by the environment and non-TOE hardware platform are described in [12].

The SFR-enforcing subsystems of the TOE are:

- CommandHandler,
- Storage,
- CSP Handler,
- Crypto,

- network.

The subsystem CommandHandler provides the following security functionality:

- Execution of the TOE's selftest, authentication and management operations,
- Provision and retrieval of log message information,
- Permission checks, identification and authentication state of external entities,
- Tracking of the TOE internal state.

The subsystem Storage provides functionality to store and retrieve data from the storage of the host platform. The subsystem CSP Handler provides management of the communication of the SMAERS-Units with the CSP-L. The subsystem Crypto provides an implementation of the cryptographic functionality of the TOE (PACE, hashing of authentication data, integrity checks, hash with LastRoundOnCard). The subsystem network provides management of the network connection of the SMAERS with the external CSP-L.

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

TOE Test configuration

The TOE test configuration is defined as Swissbit Cloud SMAERS, Version 1.0.5.

The tests are performed on a test system running the Ubuntu 24.04 operating system with Docker installed. The tests are run in a Docker image of the test suite. A fully operational Swissbit Cloud CSP-L instance version 1.0.7 is set up to the CSP-L specifications and connected to the test system.

The TOE version as stated in the ST [6] is 1.0.5. The evaluator verified that the TOE version is compliant with the documentation according to the guidance in [10].

Developer Testing

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 222 distinct test cases and include positive and negative tests in the form of wrong or missing prerequisites and wrong or missing parameters.

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

Independent Testing

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 evaluators examined publicly available information to find hints for potential vulnerabilities in the TOE. This includes gathering information about the TOE type and common attacks against it as well as collect CVEs of the libraries used in the TOE and the environment. Then the evaluators conducted a focused search of ST, guidance and all other developer deliverables for the various evaluation aspects, to find potential vulnerabilities.

Furthermore, penetration testing was carried out in the evaluation lab on a test system set up by the evaluators after the specifications of the developer. For this the approach was to try to inject arbitrary data into the TOE by a fuzzing attack on the HTTP interface.

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 Basic was actually successful in the TOE's operational environment provided that all measures required by the developer are applied.

8. Evaluated Configuration

This certification covers the following version of the TOE: Swissbit Cloud SMAERS, Version 1.0.5. It is defined by the items in table 2 of this report and by descriptions in the security target [6]. The components of the TOE are defined by the TOE configuration list [9].

The TOE is part of a TSE and requires a platform to be executed. Swissbit as TSE operator sets up the platform, which is hosted in a cloud by a cloud service provider. In addition, the TOE requires a CSP-L, which has to be hosted according to the requirements of the CSP-L. The CSP-L shall export audit records in form of system logs. The TOE has to be integrated into Swissbit Cloud-TSE 2 to build a complete TSE. To operate the TOE according to the certification, the operator has to fullfil all requirements of the guidance documents, including especially the Umgebungschutzkonzept [12] of the Swissbit Cloud-TSE 2.

The TOE as part of its TSE protects accounts and records of one or more ERS. The TOE contains multiple SMAERS units, each of which has its own private signature key and certificate. Each SMAERS unit uses one signature key exclusively. So there is a 1:1 relation between SMAERS units and signature keys. Each of the signatures keys is stored in one CSP-L, so the SMAERS unit does not directly use it, but utilizes the CSP-L to perform the corresponding cryptographic operation.

As part of a cloud TSE, the TOE shall be configured so that it will only accept connections from ERS in the same cloud environment.

The TOE integrator (which integrates the TOE into the TSE) and the TSE Operator (the entity which will operate the TOE) are the same as the developer and sponsor of the TOE (Swissbit AG). Therefore no external delivery process of the TOE to a customer takes place.

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 Supporting Document for Common Criteria Protection Profile SMAERS, Version 1.0, 16.05.2023 [11] 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_LCD.1 and ALC_CMS.3 augmented for this TOE evaluation.

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_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.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments
1	Authentica-tion/ Authenticity	ECDSA Digital Signature generation with SHA	[FIPS 186-4]	P-256	FMT_MSA.4

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments
2	Key Agreement (for PACE)	EC-DH	[FIPS 186-4]	P-256	FCS_CKM.1
3	Integrity	CMAC with AES	[NIST-SP800-38B]	256	FCS_COP.1
4	Trusted Channel	PACE	[TR-03110-2] (PACE)	see above for 'Key Agreement'	FCS_CKM.1
5	Crypto-graphic Primitive	RNG	DRG.3 according to [AIS20], NTG.1 according to [AIS20]	≥ 125 bits of entropy	FCS_RNG.1 Seed length 32 byte entropy + 16 byte nonce + 256 bits personalization

Table 3: TOE cryptographic functionality

Reference details for table 3:

***[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).*

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

***[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 f ür Sicherheit in der Informationstechnik.*

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

For all applicable entries of cryptographic algorithms listed in the table above, the Security Level provided is greater than 100 bit.

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

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

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

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

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

The environmental protection concept [12] is a guide to set up the environmental platform for the TOE. It addresses the SMAERS administrator role in the context of the assumption A.Admin and the Security Objectives for the Operational Environment. The SMAERS administrator role is therefore responsible to ensure that the platform is set up securely according to the environmental protection concept [12].

The CTSS shall be installed according to the environmental protection concept [12]. Therefore, the document shall be delivered to the SMAERS administrator installing the CTSS as required in the guidance [10] together with the CTSS that integrates the TOE.

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

AES Advanced Encryption Standard

AIS Application Notes and Interpretations of the Scheme

BSI Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany

BSIG BSI-Gesetz / Act on the Federal Office for Information Security

CA Certification Authority

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation

CEM Common Methodology for Information Technology Security Evaluation

cPP Collaborative Protection Profile

CSP Cryptographic Service Provider

CSPL Cryptographic Service Provider Light

CTSS Certified Technical Security System

EAL Evaluation Assurance Level

ERS Electronic Record-keeping Systems

ETR Evaluation Technical Report

HTTP	Hypertext Transfer Protocol
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
TLS	Transport Layer Security
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 TOE[7] https://www.bsi.bund.de/AIS

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

[6] Swissbit Cloud SMAERS - Common Criteria Security Target BSI-DSZ-CC-1239-2024, Version 1.0.11, 2024-11-13, Swissbit AG

[7] Evaluation Technical Report BSI-DSZ-CC-1239-2024, Swissbit Cloud SMAERS 1.0.5, Version 0.9, Date: 15.11.2024, SRC Security Research & Consulting 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, Bundesamt für Sicherheit in der Informationstechnik

[9] Configuration list for the TOE, source code configuration list of the Swissbit Cloud SMAERS, TOE Version 1.0.5, Document date 13.11.2024, file name: smaers-v1.0.5-konfiguration-sliste.txt, Swissbit AG, (confidential document)

[10] Swissbit Cloud SMAERS – Guidance Documentation, Version: 1.0.5, Date: 2024-11-13, Swissbit AG, file name: swissbit-Cloud-SMAERS-AGD-1.0.5.pdf, Swissbit AG, (confidential document)

[11] Supporting Document for Common Criteria Protection Profile SMAERS, Version 1.0, 2023-05-16, Bundesamt für Sicherheit in der Informationstechnik

[12] Swissbit Cloud-TSE 2 - Secure Platform Concept (Umgebungsschutzkonzept, USK), Version 1.0.2, 09.07.2024, file name: swissbit-TSE-USK-1.0.2.pdf, Swissbit AG, (confidential document)

[7] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

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