Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1121-V2-2021

for

Swissbit TSE SMAERS Firmware

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-1121-V2-2021 (*)

Swissbit TSE SMAERS Firmware

from	Swissbit AG
PP Conformance:	Security Module Application for Electronic Record-keeping Systems (SMAERS) Version 0.7.5, 6 March 2019, BSI-CC-PP-0105-2019
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 2

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, 12 March 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]
- 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 Swissbit TSE SMAERS Firmware has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1121-2019. Specific results from the evaluation process BSI-DSZ-CC-1121-2019 were re-used.

The evaluation of the product Swissbit TSE SMAERS Firmware was conducted by MTG AG. The evaluation was completed on 11 March 2021. MTG AG is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the 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 12 March 2021 is valid until 11 March 2029. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,

[5] Information Technology Security Evaluation Facility

2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.
4. to conduct a re-assessment after 5 years (i.e. the re-assessment must be finalized before 11.03.2026 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 re-assessment or a re-certification according to the regulations of the BSI-certification-scheme shall be provided.
5. to provide updates for the product in consultation with the Certification Body at BSI if vulnerabilities have been identified that affect the security of the product. This includes vulnerabilities of security functions provided by the underlying CSP, which also might affect the security of the TOE under consideration in this certificate.

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 TSE SMAERS Firmware 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 Swissbit TSE SMAERS Firmware, i.e. the TOE mainly consists of software, but also includes the following hardware components:

- the AES unit in the CPU of the controller of the TSE, and
- the communication capabilities of the controller of the TSE for USB or SD/microSD communication

The TOE exists in three different physical configurations namely, as a:

- micro SD-Card,
- SD-Card or
- USB-Token.

The three physical configurations of the TOE only differ in their physical form factor and the usage of a different flash controller. The difference in the hardware used is required to implement the different external interface standards (USB or SD). Accordingly, their Basis Firmware differs to realize the file system accessible via the communication interfaces. Apart from this, the usage of all TOE configurations is the same as well as the SMAERS Firmware implementing the TOE's business logic. Also, the same certified CSP (see [32]) is used for all TOE configurations.

The table 5 shows the hardware and software version numbers of the evaluated TOE configurations.

The Cryptographic Service Provider (CSP) used is the certified PP [10] certified "TCOS CSP 2.0 Release1/P60D145" (BSI certification id: BSI-DSZ-CC-1118-2020) and is technically identified by its Chip-Information-Data (see [15] Annex " B.2 Get Version Info "):

Product Information	
Hardware manufacturer id (cf. ISO/IEC 7816-6) '	'04' (NXP)
Hardware-ID (major ‖ minor version-number) '	'3007'
Software manufacturer id	'01' (=T-Systems)
Product id	'14" (=TCOS CSP Module)
COS version (version ‖ release number)	'01BE'
Patch version (major ‖ minor version-number)	'0041'

Table 1: Certified version of the TCOS CSP Module

The TOE Software Version number 1.1.0 includes the versions of the Flash Controller's Basis Firmware (depending on the TOE configuration):

TOE configuration:	**Basis Firmware version**
USB	190717_1.06_21
µSD/SD	190614_1.03_15

Table 2: Flash controller Basis Firmware version for TOE Software version 1.1.0

and the version of the Firmware Extension of Swissbit. The versions are those specified in the Security Target [6].

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Security Module Application for Electronic Record-keeping Systems (SMAERS) Version 0.7.5, 6 March 2019, BSI-CC-PP-0105-2019 [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.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6].

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality	Addressed issue
SF.Log	After successful boot and self-test, the TOE allows the host / ERS to provide transaction data via commands, which the TOE uses to create Transaction logs, being signed by the CSP. The corresponding signed logs are returned to the host and stored within the TOE. To do so, the TOE manages a transaction counter and keeps track, which transactions are open, see [12].
SF.Crypto	The TOE implements cryptographic operations to establish a PACE channel with the CSP and a random number generator, being required for PACE. In addition, the TOE encrypts incoming Update Code Packages (UCP) to make them unavailable, if they fail to get verified by the CSP. Thus, the TOE provides cryptographic support for secure communications and protection of information.
SF.Management	The TOE provides administrative services for management of general TOE configuration data, e.g. setting, updating the time of the CSP, management of ERS Serial Numbers, terminating open transactions, updating the TOE Firmware. The TOE uses a role-based access control system implementing the fixed roles “Unidentified User”, “Admin” and “Time Admin”. The authentication mechanism implemented to assign a role is based on PIN and PUK verification during the login command.
SF.Audit	The TOE fetches audit records from the CSP and stores them. In addition, it creates system log messages and also stores them in the flash memory as required. These logs can be exported in the same way as the Transaction logs or a filtered export can be used to export non-transaction logs only.

Table 3: 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 . 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.

This certification covers the configurations of the TOE as outlined in the Security Target [6] chapter 1.4.1.

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 TSE SMAERS Firmware

The following table outlines the TOE deliverables:

No	Type	Identifier	Release Version	Form of Delivery
1a	HW/ SW	Swissbit TSE SMAERS Firmware USB	Software 1.1.0 Hardware 1.1.0	• TSE containing the TOE is packed on trays. • Trays are packed into standard paper or carton boxes. • Boxes are wrapped with parcels. • Parcels are delivered by logistics partners of Swissbit to customers. • If the parcels will not be delivered by direct delivery, the parcels are additionally wrapped in sealed bags.
1b	HW/ SW	Swissbit TSE SMAERS Firmware SD	Software 1.1.0 Hardware 1.1.0	• TSE containing the TOE is packed on trays. • Trays are packed into standard paper or carton boxes. • Boxes are wrapped with parcels. •Parcels are delivered by logistics partners of Swissbit to customers. • If the parcels will not be delivered by direct delivery, the parcels are additionally wrapped in sealed bags.
1c	HW/ SW	Swissbit TSE SMAERS Firmware microSD	Software 1.1.0 Hardware 1.1.0	•TSE containing the TOE is packed on trays. • Trays are packed into standard paper or carton boxes. • Boxes are wrapped with parcels. • Parcels are delivered by logistics partners of Swissbit to customers. • If the parcels will not be delivered by direct delivery, the parcels are additionally wrapped in sealed bags.
2	DOC	Swissbit TSE SMAERS Firmware – Guidance Manual for ERS-User [25]	Document Version: 1.4.1	Signed email.

No	Type	Identifier	Release Version	Form of Delivery
3	DOC	Swissbit TSE SMAERS Firmware – Integrator‘s Guidance Manual [26]	Document Version: 1.4.1	Signed email.
4	DOC	swissbit TSE - Functional Specification [28]	Document Version: 1.3.0	Signed email.
5	DOC	swissbit TSE – Verpackungsprufanweisung [27]	Document Version: 1.3.1	Signed email.
6	DOC	Swissbit TSE Data Sheets USB [22] SD [23] micro SD [24]	 Version: 1.1.0, Version: 1.1.0 Version: 1.1.0	Signed email.
7	DOC	revocation passwords for certificate revocation	-	Signed email.[7]
8	DOC	optional: host library for TSE communication	-	Download server[7]

Table 4: Deliverables of the TOE

Note that the Swissbit TSE Data Sheet exists for each configuration of the TOE. The documents Swissbit TSE SMAERS Firmware - Guidance Manual, Swissbit TSE - Functional Specification [9], Swissbit TSE - Verpackungsprüfanweisung and Swissbit TSE Data Sheets will be delivered electronically to customer, each time Swissbit TSEs are delivered to a customer. This electronic delivery also contains the revocation passwords. The fingerprint of the root CA can be found in the Security Target [6].

In addition, the host library is an optional component, which is not certified. It eases the communication with the TSE and therefore the TOE by wrapping the TOE’s interface to an API. The library can be obtained from Swissbit

The sourcing process for customers who are ordering a Swissbit device is described in a precise manner. Starting from the contact between customer and Swissbit to order the devices, followed by the description of the packaging and delivery until the identification while opening a batch of TOEs by the customer him self. Also the case for malformed deliverals and the RMA Process in case of a faulty device is covered. For details please refer to the Verpackungsprüfanweisung [27], the integrator guidance documentation [26] section 2.2 and the lifecycle documentation Swissbit TSE - Delivery of TOE (ALC_DEL) [29].

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:

- Protection of transaction data of Electronic Record Keeping Systems
- Role-based access control policy to control administrative access to the TOE
- Usage of a certified cryptographic service provider (CSP) for the signing of Log-Messages

[7] Not in scope of this certification.

- Implementation of cryptographic operations to establish a PACE channel with the CSP

Specific details concerning the above mentioned security policies can be found in Chapter 6 and 7 of the Security Target (ST) [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: Trustworthy electronic record-keeping system
- OE.CSP: Cryptographic service provider component
- OE.Transaction: Verification of Transaction
- OE.SecOEnv: Secure operational environment
- OE.SUCP: Signed Update Code Packages

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

5. Architectural Information

A short description about the TOE subsystem is outlined below:

- Hardware

The parts of the TSE flash controller, which belong to the TOE are the controller's AES Unit and its communication capabilities implementing the USB or (Micro-) SD interface, which allows the communication of the TOE with the Electronic Cash register (ERS). These hardware components constitute the *Hardware* subsystem.

- Basis Firmware

The Basis Firmware subsystem is the host for the Firmware Extension, which consists of the subsystems Transaction Handling, Dispatcher, CryptoServices, CSP Communication,Update and Management. It loads and executes the Firmware Extension, forwards events (for example in the file system) to corresponding callbacks of the Firmware Extension and offers communication with the CSP.

- Dispatcher

The *Dispatcher subsystem* is responsible to manage communication with the subsystem *Basis Firmware* and forwards triggered callbacks to the corresponding subsystems of the Firmware Extension.

- Transaction Handling

The subsystem *Transaction Handling* is responsible to implement the TOE's core functionality: import, storage, and export of transaction data. Besides, it offers functionality for other subsystems to create and store log messages and to fetch the CSP audit data.

- Management

The subsystem *Management* manages all configurations and settings of the TOE, which the Admin / TimeAdmin can manipulate and store. It also includes the authentication of users to roles, being managed by the TOE.

- Update

The *Update* subsystem is responsible to accept, verify and install incoming Update Code Packages.

- Crypto Services

The subsystem *Cryptographic Services* contains all implementations of cryptographic algorithms which the TOE requires. APDUs are built in the subsystem *Crypto Services* for the establishment of the trusted channel to the CSP using PACE. The cryptographic primitives necessary for that purpose are implemented in this subsystem.

- CSP Communication

The subsystem CSP Communication implements the low-level layers of the communication protocol with the CSP.

6. Documentation

The evaluated documentation as outlined in table 5 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

During the ATE related actions, the developer as well as the ITSEF, respectively, conducted tests which intend to satisfy the needs of the EAL 2 assurance families ATE_COV.1, ATE_FUN.1 and ATE_IND.2.

Regarding developer ATE tests:

- The developer performed extensive tests to verify the claimed security functionality in the Security Target [6]. Together with the developer provided mapping of SFRs to commands, this provides a strong evidence that the tests sufficiently cover all the Security Functional Requirements from the ST[6].

Regarding ITSEF ATE tests:

- For independent testing the evaluators specified test cases with the intention to cover all SFRs from the ST. For that purpose, all of the developer’s tests have been chosen as independent. That set of tests has been expanded by testing parts of the device which are only reachable with a none production firmware. The independent testing was performed in the evaluator lab. The overall test result is that no deviations were found between the expected and the actual test results.

Regarding ITSEF AVA tests:

- The approach chosen by the evaluators is appropriate for the assurance component AVA_VAN.2, requiring the resistance of the TOE to an attacker with the *Basic* attack potential. Based on the attack scenarios AS.1 potential scenarios have been chosen, explored and tested. The chosen attack vectors which have been tested are showing that the TOE, when installed and configured and operated as described in the operational guidance documentation, fulfils the security functionality as claimed in the Security Target [6].

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

TOE Identifier and Type	Hardware Version	Software Version
Swissbit TSE SMAERS Firmware USB	1.1.0	1.1.0
Swissbit TSE SMAERS Firmware SD	1.1.0	1.1.0
Swissbit TSE SMAERS Firmware microSD	1.1.0	1.1.0

Table 5: TOE identification

Their differences are solely based on the physical form factor (USB, SD, microSD) and a different controller. This means the hardware, which the TOE is executed on differs, depending on the configuration This is required to implement the different external interface (USB or SD). Accordingly, their Basis Firmware differs, to realize the file system via the different interfaces. Still, the usage of all TOE configurations is the same, as well as the software, implementing the TOE's business logic. Also, the same certified CSP with the certificate BSI-DSZ-CC-1118-2020 is used internally.

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 following guidance specific for the technology was used:

(i) Technical Guideline BSI TR-03151 Secure Element API (SE API), BSI, Version 1.0.1, 20 December 2018 [11]

(ii) Technische Richtlinie BSI TR-03153 Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme, BSI, Version 1.0.1, 20 December 2018 [12]

(iii) Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 5: Anwendungen der Secure Element API, BSI, 01 February 2019 [13]

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 evaluation has confirmed:

- PP Conformance: Security Module Application for Electronic Record-keeping Systems (SMAERS) Version 0.7.5, 6 March 2019, BSI-CC-PP-0105-2019 [8]

- for the Functionality: PP conformant
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 2

For specific evaluation results regarding the development and production environment see annex B in part D of this report.

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 6 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	Encryption/ decryption of UCP	AES-CBC	FIPS 197 [17]	256	Yes	-
2	Cipherbased message authentication code for providing the integrity of the Trusted Channel to the CSP	CMAC-AES	FIPS 197 [17], NIST SP 800-38B [19]	256	No	-
3	hash based determi-nistic random number generation for AES key generation and in PACE key establish-ment	HASH-DRBG with SHA2-256	NIST 800-90A Revision 1 [18]	None	N/A	BSI TR-03116 [13]
4	Cryptographic hashing for partial hash of data to be signed by CSP & hash function for the DRBG	SHA2-256 SHA2-384	FIPS 180-4 [20]	None	N/A	BSI TR-03116 [13]
5	PACE for key estab-lishment for Trusted Channel	PACE with brainpool P256r1 and Generic Mapping in PCD role	ICAO, Doc 9303, Part 11 [21]	256	N/A	BSI TR-03110-3 [31]

Table 6: TOE cryptographic functionality

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 5 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.

As the TOE relies on security functionality provided by the underlying CSP, it must be operated in conjunction with the CSP of the evaluated configuration. For details concerning the CSP and its certification refer to the certification procedure BSI-DSZ-CC-1118-2020.

In regard of the further operational environment, it is to be noted that the certification and evaluation were conducted under the condition, that the objective for the operational environment “OE.SecOEnv: Secure operational environment” (Security Target [6]) is upheld. In detail, the objective states:

> *OE.SecOEnv: Secure operational environment :*
>
> *The operational environment shall protect the electronic record-keeping system and the certified technical security system including the TOE against manipulation, perturbation and misuse. It protects the integrity of the communication between the electronic record-keeping system and 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.

Also note that the UCP (Update Code Package) mechanism itself is certified according to this certificate’s evaluation assurance level and the respective Security Target’s Security Functional Requirements. However, installation and usage of other TOE configuration items than specified in the Security Target [6] (and thus evaluated during the course of this certification) will, void the certification status. Recertifications are required in order to maintain a valid certification status in cases where such TOE changes are to be applied. As a consequence, only certified updates of the TOE should be used via a respective UCP deployment procedure. If non-certified Update Code Packages are available, TOE user discretion is advised on whether the sponsor should 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.

Regarding Public Key Infrastructure (PKI) it is to be noted, that neither the Protection Profile [8] nor the Security Target [6] address (security-assurance- or security-functional) requirements concerning a PKI. Therefore, no PKI aspects were CC evaluated by the ITSEF in the course of the underlying CC evaluation. Hence the CC certification scope does not cover the Public Key Infrastructure. However, the developer Swissbit AG provided a (confidential) PKI concept document [14], outlining relevant PKI structures, definitions and processes. The document was considered by a dedicated BSI Section and deemed suitable.

The TOE includes guidance documentation (see table 5) which contains obligations and guidelines for the user and/or developer of the product layer on top on how to securely use this certified TOE and which measures have to be taken in order to fulfil the overall security requirements of the Security Target of the TOE.

If the TOE is subject to an evaluation in a composite product or system, it must be examined if the required measures have been correctly and effectively implemented by the product layer on top.

At the point in time when evaluation and certification results are reused, there might be an updated documentation available. Therefore, the certified products list on the BSI website has to be checked for latest information on reassessments, recertifications or maintenance result available for the product.

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

- Usage of the CSP which is listed under the certificate BSI-DSZ-CC-1118-2020.

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 standards
AIS	Application Notes and Interpretations of the Scheme
APDU	Application Protocol Data Unit
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
CSP	Crypto Service Provider
EAL	Evaluation Assurance Level
ERS	Electronic Record-keeping System
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility

PACE	Password Authenticated Connection Establishment
PKI	Public key infrastructure
PP	Protection Profile
RMA	Return Merchandize Authorization
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TDS	TOE Design
TOE	Target of Evaluation
TR	Technische Richtlinie
TSE	Technische Sicherheitseinrichtung
TSF	TOE Security Functionality
UCP	Update code package

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-1121-V2-2021, Version 1.9.7, 26.November.2020, Swissbit TES SMAERS Firmware – Common Criteria Security Target, Swissbit

[7] Evaluation Technical Report, Version 2.4, 11 March 2021, ETR Part Summary, MTG AG Prüfstelle für IT-Sicherheit, (confidential document)

[8] Security Module Application for Electronic Record-keeping Systems (SMAERS) Version 0.7.5, 6 March 2019, BSI-CC-PP-0105-2019

[9] Functional Specification Swissbit TSE SMAERS Firmware, Swissbit AG, Version 1.3.0, 24 June 2020

[10] Common Criteria Protection Profile, Cryptographic Service Provider (CSP), BSI ,Version 0.9.8, 19 February 2019

[11] Technical Guideline BSI TR-03151 Secure Element API (SE API), BSI, Version 1.0.1, 20 December 2018

[12] Technische Richtlinie BSI TR-03153 Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme, BSI, Version 1.0.1, 20 December 2018

[8] specifically

- AIS14, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 7, 03.08.2010, Bundesamt für Sicherheit in der Informationstechnik
- AIS19, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 9,
- AIS 20, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, 15.05.2013, Version 3, Bundesamt für Sicherheit in der Informationstechnik
- AIS 32, CC-Interpretationen im deutschen Zertifizierungsschema, Version 0.7, 08.06.2011, Bundesamt für Sicherheit in der Informationstechnik
- AIS 46, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren, Version 3, 04.12.2013, Bundesamt für Sicherheit in der Informationstechnik

[13] Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 5: Anwendungen der Secure Element API, BSI, 01 February 2019

[14] Swissbit TSE - PKI Concept, Swissbit AG, Version 1.6.3, 26 November 2019

[15] TCOS CSP Module - User's Guidance Manual, T-Systems International GmbH, Version 1.0.4, 24 March 2020, State: Certified Version, Confidential

[16] Swissbit TSE - PKI Concept, Swissbit AG, Version 1.6.3, 26 November 2019

[17] ADVANCED ENCRYPTION STANDARD (AES) (FIPS PUB 197), 26 November 2001

[18] Recommendation for Random Number Generation Using Deterministic Random Bit Generators, NIST 800-90A Revision 1, 12 August 2015 https://nvlpubs.nist.gov/nistpubs/legacy/SP/nistspecialpublication800-90a.pdf

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

[20] Secure Hash Standard (SHS), FIPS PUB 180-4, October 2015

[21] Machine Readable Travel Documents , ICAO, Doc 9303,Part 11: Security Mechanisms for MRTDSs, Seventh Edition, 2015

[22] Swissbit Product Data Sheet – Swissbit USB TSE, Swissbit AG, Revision: 1.1.0, 12 June, 2020

[23] Swissbit Product Data Sheet – Swissbit SD TSE, Swissbit AG, Revision: 1.1.0, 12 June 2020

[24] Swissbit Product Data Sheet – Swissbit microSD TSE, Swissbit AG, Revision: 1.1.0, 12 June 2020

[25] Swissbit TSE SMAERS Firmware – Guidance Manual, Swissbit AG, Version 1.4.0, 03 November 2020

[26] Swissbit TSE SMAERS Firmware – Integrator’s Guidance Manual, Swissbit AG, Version 1.4.1, 03 November 2020

[27] Swissbit TSE SMAERS Firmware – Verpackungsprüfanweisung, Swissbit AG, Version 1.3.1, 26 November 2020

[28] Functional Specification Swissbit TSE SMAERS Firmware, Swissbit AG, Version 1.3.0, 24 June 2020

[29] Swissbit TSE - Delivery of TOE (ALC_DEL), Swissbit AG, Version 1.4.1, 25 June 2020

[30] Swissbit TSE SMAERS Firmware – TOE Design, Swissbit AG, Version 1.4.1, 24 June 2020

[31] Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 3: Common Specifications, BSI, Version 2.21, 21. December 2016

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.

Annex B: Evaluation results regarding development and production environment

Annex B of Certification Report BSI-DSZ-CC-1121-V2-2021

Evaluation results regarding development and production environment

The IT product Swissbit TSE SMAERS Firmware (Target of Evaluation, TOE) 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.

As a result of the TOE certification, dated 12 March 2021, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.2, ALC_CMS.2, ALC_DEL.1) are fulfilled for the development and production sites of the TOE listed below:

Function	Address
TOE development	Swissbit München Leuchtenbergring 3 81667 München
Production and Delivery	Cleantek Business Park Berlin Wolfener Straße 36 12681 Berlin

Table 7: Sites of the TOE

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]. The evaluators verified, that the threats, security objectives and requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6]) are fulfilled by the procedures of these sites.

Note: End of report