Federal Office
for Information Security

# Certification Report

## BSI-DSZ-CC-1238-2025

for

## Swissbit Cloud CSPL, Version 1.0.7

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-1238-2025** (*)

Cryptographic Service Provider Light (CSPL)

**Swissbit Cloud CSPL**, Version 1.0.7

| | |
|---|---|
| from | Swissbit AG |
| PP Conformance: | Common Criteria Protection Profile BSI-CC-PP-0111-2019, Version 1.0, 12 November 2019<br>Common Criteria Protection Profile Configuration with PP-Modules BSI-CC-PP-0112-2020 and BSI-CC-PP-0113-2020 each in Version 1.0 from 26 February 2020 |
| Functionality: | PP conformant<br>Common Criteria Part 2 extended |
| Assurance: | Common Criteria Part 3 conformant<br>EAL 2 augmented by ALC_CMS.3 and ALC_LCD.1 |
| valid until: | 26 March 2030 |

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
recognition for components
up to EAL 2 and ALC_FLR
only

Bonn, 27 March 2025

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 CSPL, Version 1.0.7 has undergone the certification procedure at BSI.

The evaluation of the product Swissbit Cloud CSPL, Version 1.0.7 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 13 March 2025. 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 27 March 2025 is valid until 26 March 2030. 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 CSPL, Version 1.0.7 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 the product Swissbit Cloud CSPL, Version 1.0.7, provided by Swissbit AG running on FIPS 140-3 Level 4 certified version of the Private Machines Enforcer R2 compute blades as the execution platform. The hardware is not part of the TOE.

The TOE is a Cryptographic Service Provider Light (CSPL or CSP-L) claiming the following Common Criteria Protection Profile configuration:

- Cryptographic Service Provider Light, Version 1.0, registered under BSI-CC-PP-0111-2019, 12 November 2019, Federal Office for Information Security.

In combination with the following PP-Modules:

- Protection Profile-Module CSPLight Time Stamp Service and Audit, registered under BSI-CC-PP-0112-2020, 26 February 2020, Federal Office for Information Security.
- Protection Profile-Module CSPLight Time Stamp Service and Audit – Clustering, Version 1.0, registered under BSI-CC-PP-0113-2020, 26 February 2020, Federal Office for Information Security.

The Security Target [6] is the basis for this certification. It is based on the above mentioned certified Common Criteria Protection Profiles [8].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 2 augmented by ALC_CMS.3 and ALC_LCD.1.

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 |
|---|---|
| Key management | The key management functionality covers several management functionalities with regards to cryptographic keys, including an access control security functional policy on the corresponding cryptographic keys. This policy governs all functions of the TOE that use (or result in) a key, including but not limited to key creation, key derivation, key deletion, key property modification, key import and key export. |
| Cryptographic operations for encryption & decryption | The TOE supports symmetric data encryption and decryption using AES in CBC mode with cryptographic key lengths of 128 and 256 bits. |
| Hybrid encryption for user data | The TOE provides hybrid data encryption/decryption and MAC calculation/verification of user data. |
| Data integrity mechanisms | The TOE provides data integrity protection by symmetric and asymmetric cryptography. |
| Authentication & attestation of the TOE, trusted channel | The TOE provides a cryptographically protected trusted communication channel between the TOE and external entities as well as the authentication of external entities. |
| Access control | The TOE enforces a strict role based access control. The roles associated with the authenticated user and user’s current status define |

| TOE Security Functionality | Addressed issue |
|---|---|
| | the authorization and allowed use of services and objects. |
| Security management | The TOE provides administrative services such as management of security functions, roles and attributes. |
| Protection of the TSF | The TOE performs tests of the configuration of the TOE, availability of the time source, access control system, availability of entropy and cryptographic subroutines. |
| Secure Update | The TOE supports downloading, integrity and authenticity verification and decryption of Update Code Packages (UCP) and is provided to the Administrator only. |
| Time stamping | The TOE provides a time stamp service. All time-related services take place using access to the TOE's internal system clock which is synchronized using a secure local trusted Network Time Protocol (NTP) Server. |
| Security Audit | The TOE generates audit records on selected user activities and security events of the TOE. Audit records are exported by the TOE in signed and time stamped form. |
| Clustering | The TOE supports clustering of a single master node and one slave node to improve the availability of the TOE. |

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 which are outlined in the Security Target [6], chapters 3.4, 3.2 and 3.3 respectively.

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

# 2. Identification of the TOE

The Target of Evaluation (TOE) is called:

**Swissbit Cloud CSPL,** Version 1.0.7

The following table outlines the TOE deliverables:

| Type | Identifier | Description/ Additional Information | Release | Form of Delivery |
|---|---|---|---|---|
| SW | TOE (as software) | For its operation, the TOE needs the following hardware and software requirements fulfilled in its environment.<br><br>The Enforcer R2 by Private Machines as the execution platform which has been certified according to FIPS 140-2 level 4 with following characteristics has to be used:<br><br>Manufacturer: PMI<br>Product: E-RX2<br>Hardware version: R2-XD1736NT<br>Firmware Version: 2.1.2<br>Libucl Version: 2.7.1<br>Libdrbg Version: 2.0.0<br><br>Ubuntu server version: 24.04 | 1.0.7 | The signed jar file is stored in the fiscal3- fabric git repository of Swissbit AG and the corresponding commit is tagged with cspl-v1.0.7 (1.0.7 is the version of the Swissbit Cloud CSP-L of the current Common Criteria certification process). |
| DOC | Associated guidance documentation , [10] | Swissbit Cloud CSP-L - Guidance Documentation, Version 1.1.5, 06.11.2024, Swissbit AG<br><br>SHA256:<br>e9705ebece421ed28895b0fd60fd489869522815a9369f2ff28be045256a97d0 | 1.1.5 | The guidance document and the TOE are delivered to the customer via a personal delivery, encrypted and signed email or a secure download portal. |

Table 2: Deliverables of the TOE

The CSP-L (as a software) is delivered from the developer (and sponsor of the certification) (Swissbit AG) to the operator of the CSP-L (again Swissbit AG). This is done by storing the software and guidance document in the corresponding git repository and tagging it accordingly.

### Identification of the TOE by the User

Before the actual installation, it shall be ensured that the provided *.jar file that implements the Swissbit Cloud CSP-L is authentic. This can be achieved by either checking the hash value of the *.jar file and compare it to the known value. This known value has to be received from the developer of the Swissbit Cloud CSP-L via a secured channel (e.g. a signed email). Alternatively, the signature of the *.jar file can be verified using the following command:

jarsigner -verify -verbose -keystore truststore cspl-1.0.7.jar

The required truststore file has to be received from the developer of the Swissbit Cloud CSPL via a secured channel (e.g. a signed email).

# 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:

- Key management
- Data encryption
- Hybrid encryption with MAC for user data
- Data integrity mechanisms
- Time Stamp
- Authentication and attestation of the TOE, trusted channel
- User identification and authentication
- Access control
- Security Management
- Security Audit
- Protection of the TSF
- Import and verification of Update Code Package
- Clustering

Specific details concerning the above mentioned security policies can be found in chapter 7 of the Security Target [6].

# 4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- OE.CommInf: Communication infrastructure
- OE.AppComp: Support of the Application component
- OE.SecManag: Security management
- OE.SecComm: Protection of communication channel
- OE.SUCP: Signed Update Code Packages
- OE.SecPlatform: Secure Hardware Platform
- OE.Audit: Review and availability of audit records
- OE.TimeSource: External time source
- OE.ClusterCtrl: Control of the cluster
- OE.TSFdataTrans: Transfer of TSF data within the CSPLight cluster

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

# 5. Architectural Information

The TOE is a software-only TOE running on dedicated non-TOE hardware (Private Machines Enforcer R2) as well as dedicated non-TOE software (Ubuntu Linux), which together build the platform. The TOE is operated on the hardware platform “Enforcer R2” which is certified according to FIPS 140-2 Level 4. The non-TOE Enforcer R2 platform is expected to provide protection against physical intrusion and tampering. Additionally, the TOE protects itself from tampering by untrusted entities due to its SFR-enforcing subsystems. The non-TOE software is Ubuntu Linux distribution with a minimal functionality.

The SFR-enforcing subsystems of the TOE are:

- Frontend subsystem:
  - Management of the three external interfaces of the TOE
  - Responsible for the start-up of the CSPL and thereby for the correct initialization of all other subsystems
  - Performs extraction of the message contained in the request,
  - User identity checks, MAC verification, Decryption
  - Forwarding to the respective handler, the handler performs formal validity checks, checks on the authentication level based on the claimed user and execution of actions belonging to the respective handler,
  - Starts a timer which performs a self-test once every time the timer runs out
  - Handles five different authentication ways
- Crypto subsystem:
  - Implements all cryptographic functionality needed by the TOE. It is also responsible for secure key storage and export based on access control attributes.
  - The crypto subsystem is also responsible to seed the DRNG of Bouncy Castle at startup and during every self-test.
- Audit subsystem: Generates audit log messages and to write an application log. The audit log is signed and stored on the persistent memory of the hardware platform.
- Storage subsystem: Writes to and reads data from the persistent storage of the system. The persisted storage is used to store configuration files.
- Timekeeping subsystem: Handles the system time via chrony daemon and via a dedicated command. The chrony daemon synchronizes the clock of the local machine against an authenticated time server at PTB. The time can be adjusted manually, if the chrony daemon stops working.

# 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 Swissbit Cloud CSPL is a pure software implementation and it is dedicated to provide cryptographic services for the protection of the confidentiality and the integrity of user data, and for entity authentication. The TOE has to be initialized/personalized in terms of a clustering behaviour (each master is assigned exactly one slave).

The current test environment comprises the following components:

- The TOE as JAR file
- The CSP-L Repository, which includes the test scripts
- Instantiation of a TOE-master and a TOE-slave on an Enforcer R2 (by Private Machines)
- A Test-PC with an SSH connection to a controller instance which has an SSH connection to the TOE-master and TOE-slave

### Tests of the Developer

Testing approach

The developer tests cover all interfaces. The tests performed can be categorized into three groups: unit, manual tests and source code review tests. Some unit tests are implemented as parameterized test which are executed in multiple iterations for a number of parameter combinations.

Testing Results

All developer test results are either ‘pass’ or ‘skipped’. Skipped tests are either code review tests or parameterized test cases which are executed in multiple iterations for a number of parameter combinations.

### Independent Evaluator Tests

Subset size chosen:

The evaluators repeated all developer tests, including TSFI, unit and manual tests.

Evaluator tests performed:

The developer tests cover all TSFIs. Since the evaluators repeated the complete list of developer tests, all given interfaces are covered by the testing. In addition some independent evaluator tests were performed.

All tests were executed successfully.

**Penetration tests performed**

Penetration testing approach:

For the general communication with the TOE for external entities connecting from the internet the interface IF.REST is used. The approach is to try to inject arbitrary data into the TOE by a fuzzing attack on the interface IF.REST. Since the TOE accepts only communication via the PACE protocol, this means to overcame the protection of the PACE protocol.

Some SFRs were covered by the penetration tests. The remaining SFRs were analysed, but not penetration tested due to non-exploitability of the related attack scenarios in the TOE's operational environment also including an attacker with a Basic attack potential.

Verdict for the sub-activity:

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 as defined in the Security Target [6] provided that all measures required by the developer are applied.

# 8. Evaluated Configuration

This certification covers the following configuration of the TOE:

The TOE test configuration is defined by the notation:

- Swissbit Cloud CSP-L, version 1.0.7
- The document Swissbit Cloud CSP-L 1.0.7, Guidance Documentation [10]

The evaluators verified in the documentation and the test environment, that the correct version is used for testing by analysing the test result of a "PerformSelftestRequest" as part of the test case "checkSelftestFormat". The test case checks for a correct TOE identification which is "Swissbit Cloud CSP-L, Version 1.0.7".

The TOE is running on a special hardware platform, the Enforcer R2 (by Private Machines) (hardware version: R2-XD1736NT, firmware version: 2.1.2 with libucl version: 2.7.1 and libdrbg version: 2.0.0). The installation of a productive system on a different hardware (or a different version of the hardware) is not allowed. In addition the developer states, that the user has to setup the Enforcer R2 by installing a Ubuntu server.

The evaluator confirmed the following versions by querying the enforcer blade version:

- Manufacturer: PMI
- Product: E-RX2
- Firmware version: 2.1.2
- Libucl version: 2.7.1
- Libdrbg version: 2.0.0

The hardware carries a certification according to FIPS 140-3 level 4.

A Ubuntu server (non-TOE) with version 24.04 is used.

# 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.

For RNG assessment the scheme interpretations AIS 20/31 was used (see [4]).

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

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

The evaluation has confirmed:

- PP Conformance to the following PP configuration:
  Protection Profile Cryptographic Service Provider Light (CSPL) Version 1.0, 12 November 2019, BSI-CC-PP-0111-2019,
  Common Criteria Protection Profile Configuration Cryptographic Service Provider Light – Time Stamp Service and Audit (PPC-CSPLight-TS-Au) Version 1.0, 26 February 2020, BSI-CC-PP-0112-2020,
  Common Criteria Protection Profile Configuration Cryptographic Service Provider Light - Time Stamp Service and Audit – Clustering (PPC-CSPLight-TS-Au-Cl), Version 1.0, 26 February 2020, BSI-CC-PP-0113-2020[8]
- for the Functionality: PP conformant
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 2 augmented by ALC_CMS.3 and ALC_LCD.1

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

## 9.2. Results of cryptographic assessment

The following table gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines the standard of application where its specific appropriateness is stated.

| No. | Purpose | Cryptographic Mechanism | Standard of Implementation | Key Size in Bits | Standard of Application | Comments |
|---|---|---|---|---|---|---|
| 1 | Establishing trusted channel | PACE | TR-03110 [11] | 256 | CSPL PP [8] | ST, [6], chap. 6.1 |

| No. | Purpose | Cryptographic Mechanism | Standard of Implementation | Key Size in Bits | Standard of Application | Comments |
|---|---|---|---|---|---|---|
| 2 | Establishing trusted channel | Terminal Authentication | TR-03110 [11] | 256 (ECDSA) | CSPL PP [8] | ST, [6], chap. 6.1 |
| 3 | Establishing trusted channel | Chip Authentication | TR-03110 [11] | 256 (ECDSA) | CSPL PP [8] | ST, [6], chap. 6.1 |
| 4 | Trusted channel | AES CBC/CMAC | TR-03110 [11] | 128, 256 | CSPL PP [8] | ST, [6], chap. 6.1 |
| 5 | Serving pseudo random numbers | Serving Random Numbers | Iterated hash RNG as in Example 39 of SP-800-38E [12] | ≥ 125 bits of entropy | CSPL PP [8] | ST, [6], chap. 6.1 |
| 6 | Serving random numbers | Serving Random Numbers | By (non-TOE) HW-platform | ≥ 125 bits of entropy | CSPL PP [8] | ST, [6], chap. 6.1 |
| 7 | Signing user data | (ECDSA with SHA-256) or (RSA-4096 with SHA-256) | FIPS186-4 [13] or (ISO/IEC 14888-2 [14] and PKCS #1 [15]) | 256 | CSPL PP [8] | ST, [6], chap. 6.1 |
| 8 | Verifying user data | (ECDSA with SHA-256) or (RSA-4096 with SHA-256) | FIPS186-4 [13] or (ISO- IEC_14888-2 [14] and PKCS #1 [15]) | 256 | CSPL PP [8] | ST, [6], chap. 6.1 |
| 9 | Attestation | ECDSA with SHA-256 | FIPS186-4 [13] | 256 | CSPL PP [8] | ST, [6], chap. 6.1 |
| 10 | Clustering of keys | keywrap and unwrap | NIST-SP800- 38F [16] | 128, 256 | PP-Configuration CSPLight- TS-Au-Cl [8] | ST, [6], chap. 6.3 |

Table 3: TOE cryptographic functionality

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

According to the Common Criteria Protection Profile Configurations [8] the algorithms are suitable for the corresponding purpose. An explicit validity period is not given.

# 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 or she 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.

# 11. Security Target

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

# 12. Regulation specific aspects (eIDAS, QES)

None

# 13. Definitions

## 13.1. Acronyms

| | |
|---|---|
| **AIS** | Application Notes and Interpretations of the Scheme |
| **BSI** | Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany |
| **BSIG** | BSI-Gesetz / Act on the Federal Office for Information Security |
| **CCRA** | Common Criteria Recognition Arrangement |
| **CC** | Common Criteria for IT Security Evaluation |
| **CEM** | Common Methodology for Information Technology Security Evaluation |
| **cPP** | Collaborative Protection Profile |
| **CSP** | Cryptographic Service Provider |
| **CSPL** | Cryptographic Service Provider Light |
| **EAL** | Evaluation Assurance Level |
| **ETR** | Evaluation Technical Report |
| **FIPS** | Federal Information Processing Standards |
| **IT** | Information Technology |
| **ITSEF** | Information Technology Security Evaluation Facility |
| **JAR** | Java Archive |
| **JVM** | Java Virtual Machine |
| **NIST** | National Institute of Standards and Technology |
| **NTP** | Network Time Protocol |

| | |
|---|---|
| **PACE** | Password Authenticated Connection Establishment |
| **PP** | Protection Profile |
| **RNG** | Random Number Generator |
| **SAR** | Security Assurance Requirement |
| **SFP** | Security Function Policy |
| **SFR** | Security Functional Requirement |
| **SMAERS** | Security Module Application for Electronic Record-keeping Systems |
| **ST** | Security Target |
| **TOE** | Target of Evaluation |
| **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] Security Target BSI-DSZ-CC-1238-2025, Swissbit Cloud CSP-L - Common Criteria Security Target, Version 1.2.6, 06.11.2024, Swissbit AG

[7] Evaluation Technical Report, Evaluation Report - Evaluation Technical Report (ETR) - Summary -, Version 0.6, 15.11.2024, SRC Security Research & Consulting GmbH, (confidential document)

[8] Protection Profile Cryptographic Service Provider Light (CSPL) Version 1.0, 12 November 2019, BSI-CC-PP-0111-2019, Common Criteria Protection Profile Configuration Cryptographic Service Provider Light – Time Stamp Service and Audit (PPC-CSPLight-TS-Au) Version 1.0, 26 February 2020, BSI-CC-PP-0112-2020, Common Criteria Protection Profile Configuration Cryptographic Service Provider Light - Time Stamp Service and Audit – Clustering (PPC-CSPLight-TS-Au-Cl), Version 1.0, 26 February 2020, BSI-CC-PP-0113-2020

[9] Configuration List including the implementation representation, File name: Swissbit-CSPL-SourceCodeList-v0.9.0.csv, Version 0.9.0, SHA256-value: 3696775b4517d1e08eee55c306b6b92e5d75b06698315166b68953e927b079fc

[10] Swissbit Cloud CSP-L - Guidance Documentation, Version 1.1.5, 06.11.2024, Swissbit AG

[7] specifically

- AIS14, Version 7, Anforderungen an Aufbau und Inhalt von Einzelprüfberichten für Evaluationen nach CC
- AIS19, Version 9, Gliederung des ETR
- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 38, Version 2, Reuse of evaluation results
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren

[11] 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, BSI

[12] [SP800-38E], Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices, January 2010

[13] [FIPS186-4], Digital Signature Standard (DSS), 2013, NIST

[14] [ISO/IEC 14888-2], Information technology – Security techniques, Digital signatures with appendix – Part 2: Integer factorization based mechanisms, 2008

[15] [PKCS #1 v2.2], RSA Cryptographic Standard, 27.10.2012, RSA Laboratories

[16] [SP800-38F], Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, 2012, NIST

# 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