Certification Report

Swissbit Cloud SMAERS 1.1.0

- Security Module Application for Electronic Record-keeping Systems (SMAERS) -

Certification pursuant to the European Common Criteria-based Cybersecurity Certification Scheme (EUCC)

Version
1.0

Date
25.09.2026

Certification Body
SRC Zert GmbH & Co. KG
Leipziger Straße 35
65191 Wiesbaden

Certificate ID:
EUCC-3206-2026-0002

Document invariants

Name	Invariant (edit here)	Output value
Current version	1.0	1.0
Date	25.09.2026	25.09.2026
Classification	Public	Public
Type of Product	Security Module Application for Electronic Record-keeping Systems (SMAERS)	Security Module Application for Electronic Record-keeping Systems (SMAERS)
Name of Product	Swissbit Cloud SMAERS 1.1.0	Swissbit Cloud SMAERS 1.1.0
Shortname of Product	Swissbit Cloud SMAERS	Swissbit Cloud SMAERS
Manufacturer	Swissbit AG	Swissbit AG
Protection Profiles	Protection Profile Security Module Application for Electronic Record-keeping Systems (SMAERS), BSI-CC-PP-0105-V2-2020, version 1.0	Protection Profile Security Module Application for Electronic Record-keeping Systems (SMAERS), BSI-CC-PP-0105-V2-2020, version 1.0
Assurance Level	EAL2 (substantial), augmented by ALC_CMS.3 and ALC_LCD.1	EAL2 (substantial), augmented by ALC_CMS.3 and ALC_LCD.1
ITSEF	SRC Security Research & Consulting GmbH	SRC Security Research & Consulting GmbH
Certification Body	SRC Zert GmbH & Co. KG	SRC Zert GmbH & Co. KG
Certificate ID	EUCC-3206-2026-0002	EUCC-3206-2026-0002
Certificate Issuing Date	25.09.2026	25.09.2026
Certificate Expiry Date	24.09.2031	24.09.2031

Table 1: Document Invariants

Change History

Version	Date	Change
0.1	14.07.2026	Update Template (IR (EU) 2025/2462)
0.2	22.09.2026	Content and results based on ITSEF-documents
0.3	24.09.2026	Quality Assurance
1.0	24.09.2026	Final Version

Table 2: Change History

Table of Contents

1. Executive Summary

The Target of Evaluation (TOE) is Swissbit Cloud SMAERS 1.1.0 by Swissbit AG. It 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 CSL-L (EUCC-3206-2026-0001) 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 (see BSI TR-03110-1) by the TOE itself. This CSPL is not part of this TOE.

The evaluation was done by SRC Security Research & Consulting GmbH with no subcontractors. It was completed on 23.09.2026 and the evaluation technical report [ETR] was created by the ITSEF. The evaluation was based on version CC:2022 R1 ([CC:2022]) with assurance level EAL2 (substantial), augmented by ALC_CMS.3 and ALC_LCD.1. The TOE claims strict conformance to the following protection profile:

- Protection Profile Security Module Application for Electronic Record-keeping Systems (SMAERS), BSI-CC-PP-0105-V2-2020, version 1.0

The security policy of the TOE is described in chapter 4 - Security Policy.

Based on the evaluation, the certification body has issued the certificate EUCC-3206-2026-0002 on 25.09.2026, with a validity until 24.09.2031.

Please note: A previous version of the TOE (Swissbit Cloud SMAERS 1.0.5) had been certified under BSI-DSZ-CC-1239-2024, issued on 29 November 2024.

2. Identification of the ICT-Product

The TOE by Swissbit AG is called:

Swissbit Cloud SMAERS 1.1.0

The following table outlines the delivery items and associated delivery methods:

	Delivery item	Description / Additional Information	Type	Delivery method
1	TOE (as software)	The delivered item is a .jar file containing the TOE: smaers-1.1.0.jar For its operation, the TOE needs the following hardware and software requirements fulfilled in its environment:	SW	Since the TOE integrator (which integrates the TOE into the TSE) and the TSE Operator (the entity which will operate the TOE) are

	Delivery item	Description / Additional Information	Type	Delivery method
		• 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		the same as the developer and sponsor of the TOE (Swissbit AG), the signed jar file is stored in the fiscal3-fabric git repository of Swissbit AG and the corresponding commit is tagged with smaers-v1.1.0. This completes the delivery process.
2	Associated guidance documentation	Swissbit Cloud SMAERS – Guidance Documentation, Version: 1.1.0, Date: 2026-06-18, Swissbit AG SHA256: c80531b7badf7e073b3e165914abef9d0dece891f6cd84971bbc26f4ed24b1c4	PDF	The in-house delivery is done by storing the software and guidance documents in the corresponding git repository and tagging it accordingly.
3.	digital signature file	digital signature file in the form smaers-1.1.0.jar.sig	SW	delivery method: see TOE

Table 3: Delivery items

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.

Identification of the TOE by the User

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 AG. This can be done with the command:

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

/smaers_code_signing_public_key.pem smaers-1.1.0.jar
```

3. Contact Information

Developer	Swissbit AG
Holder of the EUCC certificate	Swissbit AG Industriestraße 4 CH-9552 Bronschhofen
Certification Body	SRC Zert GmbH & Co. KG
National Cybersecurity Certification Authority	Bundesamt für Sicherheit in der Informationstechnik (BSI)
ITSEF	SRC Security Research & Consulting GmbH Emil-Nolde-Str. 7 D-53113 Bonn

Table 4: Contact Information

4. Security Policy

The security policy enforced is defined by the selected set of Security Functional Requirements and implemented by the TOE.

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:

TOE Security Functionality	Description
SF.Log	After successful startup and self test, the SMAERS unit of the TOE allows the host / ERS to provide transaction data via commands, which the CTSS interface component forwards to the SMAERS unit of the TOE. Then the SMAERS unit of the TOE creates transaction logs. The transaction logs are partially signed using Hash Last Round on Card and the partial hash (i.e. the internal state of the hash function) and the last block of the hash are sent to the CSP-L, where the hash computation is finalized and the hash being signed by the CSP-L. The corresponding signed logs are exported to the CTSS interface component and stored on the secure storage of the TSE. To do so, each SMAERS

TOE Security Functionality	Description
	unit of the TOE manages one transaction counter and keeps track, which transactions are open. The TOE uses multiple keys for signature creation, each being associated with exactly one SMAERS unit. The dispatcher of the TOE ensures, that each incoming request is associated with the correct SMAERS unit and instantiates the unit in a worker thread. This makes sure, that the correct key is used. Imported data are checked by the SMAERS unit of the TOE. Here the unit assures that ERS clientIDs are configured accordingly and if invoked operations match the internal state of the SMAERS unit of the TOE. The transaction counters are managed by the SMAERS unit of the TOE. They are only changed, when a new transaction is opened and immediatly persisted in the corresponding SMAERS unit and the SMAERS unit of the TOE ensures that it will always be incremented by one when a new transaction is started. The worker thread concept ensures, that each time the correct transaction counter is taken into account, when needed.
SF.Crypto	The TOE implements cryptographic operations to establish a PACE channel with the CSP-L and a random number generator, being required for PACE. This implementation is used by each SMAERS unit on its own independently.
SF.Management	The set of roles is fixed for the TOE and cannot be updated during the operation. Also all access rights, i.e. which role is able to execute which function are fixed, so there is no need for a flexible implementation of roles and their rights. Instead the roles and their permissions are hardcoded in the TOE. On startup the SMAERS unit of the TOE performs a set of tests. Prior to and while the tests are running, the CTSS Interface Component has the role unidentified user. Depending on the test results, the user has afterwards the roles CSP and/or CTSS and can then additionally authenticate as administrator. If the test fails, the SMAERS unit of the TOE enters a secure state. To manage which ERS are accepted at startup and which clientIds can be used to start (update and finish) transactions, the SMAERS units of the TOE maintain lists of registered ERS clientIDs and associated SMAERS units. The TOE does not terminate open transactions on its own. It requires the ERS to do so. In case the ERS is not aware which transactions are still open, the SMAERS unit of the TOE offers a function to retrieve a list of open transactions

TOE Security Functionality	Description
	in the corresponding SMAERS unit. This way, the TOE does not have to make assumptions about the transactions or perform business decisions for the ERS.
SF.Audit	The TOE fetches audit records from the CSP-L and stores them. In addition, it creates system log messages and also exports them to the CTSS Interface Compoent, which stores them in the secure storage of Swissbit Cloud-TSE 2 as required.

Table 5: TOE Security Functionality

Specific details concerning the abovementioned security policies can be found in section 8 of the Security Target ([ST]).

Swissbit AG maintains a documented and consistently applied vulnerability management process designed to support compliance with the applicable requirements of the EU Cyber Resilience Act (CRA) throughout the product lifecycle. The process establishes defined roles, responsibilities, escalation paths, and procedures for the identification, intake, assessment, prioritization, remediation, verification, and disclosure of vulnerabilities affecting its products. Identified vulnerabilities are subject to documented risk assessment and remediation activities, including applicable CRA obligations concerning vulnerability handling, reporting, security updates, and communication with affected parties. As part of its coordinated vulnerability disclosure framework, Swissbit AG publishes and maintains a security.txt file in accordance with RFC 9116, providing customers, security researchers, and other stakeholders with an authoritative channel for reporting security vulnerabilities and accessing relevant disclosure information. This process and the associated records provide traceability of vulnerability-handling activities and support the demonstration of conformity with applicable CRA cybersecurity and vulnerability-management requirements.

5. Assumption and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organizational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled and measures to be taken by the IT-environment, the user or the risk manager. The following topics are of relevance:

- OE.ERS – Trustworthy Electronic Record-Keeping System
- OE.SMAERSPlatform – Secure platform storage
- OE.CSP – Cryptographic Service Provider Component
- OE.CSPPlatform – CSP as Secure Platform of the TOE (not applicable for the TOE because the TOE has a client-server architecture)
- OE.Transaction – Verification of Transaction
- OE.SecOEnv – Secure Operational Environment
- OE.SecCommCSP – Secure Communication between TOE and CSP

- OE.SUCP – Signed Update Code Packages
- OE.SecUCP – Secure download and authorized use of Update Code Package

Details can be found in section 4.2 of the Security Target ([ST]).

6. 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 non-TOE platform is expected to provide protection against physical intrusion and tampering.

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 the following security functionality:

- Functionality to store and retrieve data from the storage of the host platform

The subsystem CSP Handler provides the following security functionality:

- Management of the communication of the SMAERS-Units with the CSP-L

The subsystem Crypto provides the following security functionality:

- Implementation of the cryptographic functionality of the TOE (PACE, hashing
- of authentication data, integrity checks, hash with LastRoundOnCard)

The subsystem network provides the following security functionality:

- Management of the network connection of the SMAERS with the external CSP-L

The following figure shows the overall architecture with the TOE within.

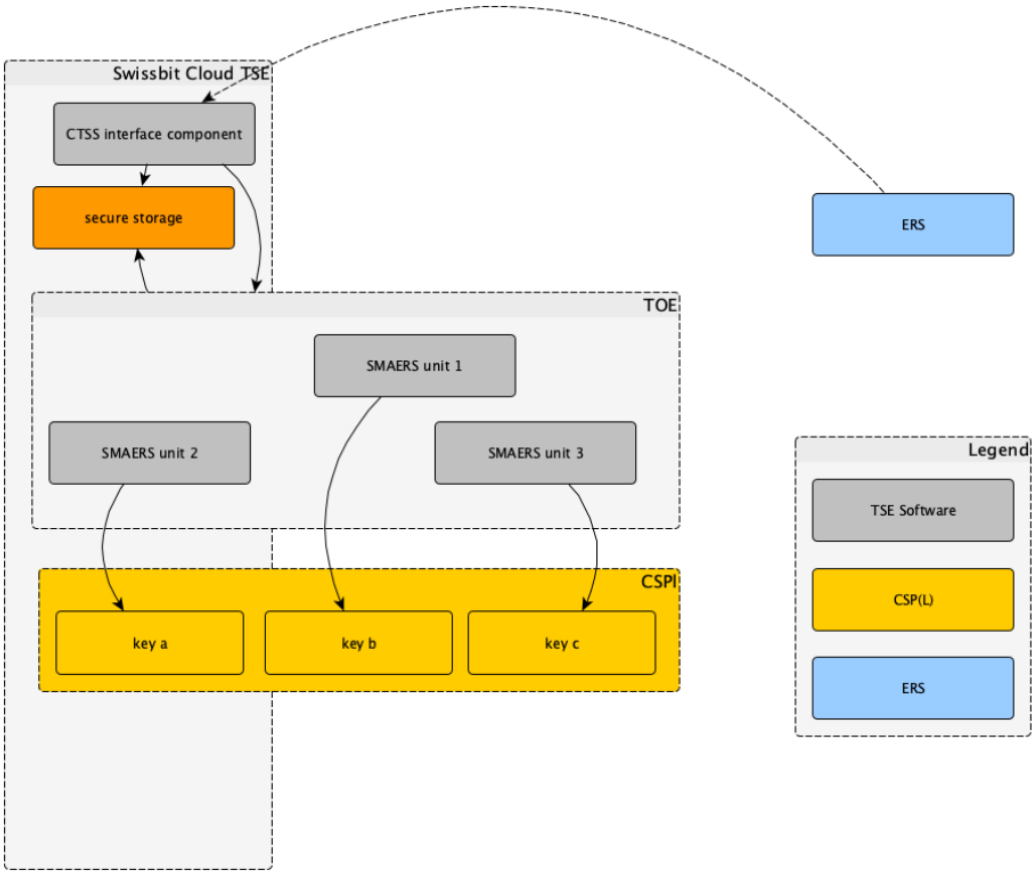

Figure 1: Overview of the TSE, the TOE, its SMAERS units and CSP-L relations

7. Supplementary Cybersecurity Information

The evaluated documentation is provided with the product to the customer and contains the required information for secure usage of the TOE in accordance with the Security Target ([ST]).

The developer supplies the following website for supplementary cybersecurity and contact information:

- https://www.swissbit.com/.well-known/security.txt

8. ICT-Product evaluation summary and configuration

The following assurance components were used:

CC Aspect	Result
CC Class ASE	PASS
ASE_INT.1	PASS
ASE_CCL.1	PASS
ASE_SPD.1	PASS
ASE_OBJ.2	PASS
ASE_ECD.1	PASS
ASE_REQ.2	PASS
ASE_TSS.1	PASS
CC Class ALC	PASS
ALC_CMC.2	PASS
ALC_CMS.3	PASS
ALC_DEL.1	PASS
ALC_LCD.1	PASS
CC Class ADV	PASS
ADV_FSP.2	PASS
ADV_TDS.1	PASS
ADV_ARC.1	PASS
CC Class AGD	PASS
AGD_OPE.1	PASS
AGD_PRE.1	PASS
CC Class ATE	PASS
ATE_COV.1	PASS
ATE_FUN.1	PASS
ATE_IND.2	PASS
CC Class AVA	PASS
AVA_VAN.2	PASS

Table 6: Assurance Components and Results

In addition to the state-of-the-art documents published by ENISA the following further security evaluation criteria were used:

- Supporting Document for Common Criteria Protection Profile SMAERS, Version 1.0, 16.05.2023 (with overall verdict PASS)

The following protection profile is used:

- Protection Profile Security Module Application for Electronic Record-keeping Systems (SMAERS), BSI-CC-PP-0105-V2-2020, version 1.0

Testing and vulnerability analysis were done both by the developer and the evaluator.

The TOE test configuration is defined by the notation:

- Swissbit Cloud SMAERS 1.1.0
- The documents:
  - Swissbit Cloud SMAERS - Guidance Documentation [AGD]
  - Swissbit Cloud-TSE 2 – Secure Platform Concept (Umgebungsschutzkonzept) [USK]

The exact version number of the TOE has been gathered by checking 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. The version number of the TOE was verified as 1.1.0.

The TOE is running in Docker on the underlying operating system Ubuntu 24.04.

Tests of the Developer

TOE test configuration: 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 is set up to the CSP-L specifications and connected to the test system. The tested TOE version is 1.1.0.

Testing approach: The developer tests cover all interfaces. The tests performed can be categorized into three groups: automatic tests, manual tests (only one) and code review tests. The test environment is configured by the developer and does not need any actions by the evaluator to run the tests except the starting commands. This means that all necessary configuration files and flags are set.

Testing Results: All test cases were executed successfully and ended up with the expected result. If necessary the developer gives additional annotations.

Independent Evaluator Tests

Test Configuration: The TOE test configuration is defined by the notation: Swissbit Cloud SMAERS 1.1.0

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 1.1.0 is set up to the CSP-L specifications and connected to the test system.

The TOE version as stated in [ST] is 1.1.0. The evaluator verified that the TOE version is compliant with the documentation according to the guidance in [AGD].

Subset size chosen: The evaluators repeated all developer tests, including TSFI and unit tests.

Selection criteria for the interfaces and interfaces tested: The developer tests cover all TSFIs. Since the evaluators repeated the complete list of developer tests, all given interfaces are covered by the testing.

Independent evaluator tests performed: Additionally the following independent evaluator tests were performed:

Test-ID	Description
T.Limits	The TOE correctly handles out of bounds exceptions.
T.Random	Statistical tests of provided hardware based random numbers via the AIS31 statistical test suite.
T.User	The TOE correctly checks user roles.
T.Fuzzing	Fuzzing of HTTP requests and responses send to and retrieved from/to the CSP-L resulting in a misbehaviour of the TOE observable at the CTSS interface of the TOE.

Table 7: Independent Evaluator Tests

The evaluators determined that all tests were executed successfully.

Penetration tests performed

The penetration testing was carried out in the evaluation lab on the test client which connects remotely to the TOE in the developers test environment. All configurations of the TOE being intended to be covered by the current evaluation were tested, i.e. Swissbit Cloud SMAERS 1.1.0.

The overall test result is that no deviations were found between the expected and the actual test results; moreover, no attack scenario with the attack potential Basic was actually successful.

Penetration testing approach: The approach chosen by the evaluator is commensurate with the assurance component chosen (AVA_VAN.2) treating the resistance of the TOE to an attack with the Basic attack potential. I.e. amongst other that the evaluator used sources of information publicly available to identify potential vulnerabilities in the TOE. The evaluator analysed which potential vulnerabilities are not applicable to the TOE in its operational environment. For the potential vulnerabilities being applicable to the TOE in its operational environment and, hence, which were candidates for testing applicable to the TOE in its operational environment, the evaluator devised the attack scenarios where these potential vulnerabilities could be exploited. For each such attack scenario he firstly performed a theoretical analysis on the related attack potential. Where the attack potential was Basic or near to Basic, the evaluator conducted penetration tests for such attack scenarios. He analysed then the results of these tests with the aim to determine, whether at least one of the attack scenarios with the attack potential **Basic** was actually successful.

For this the resulting approach is to try to inject arbitrary data into the TOE by a fuzzing attack on the HTTP interface. Since the TOE accepts only communication via this protected service (which implements all SFR-enforcing TSFIs, namely one), this means to overcome the protection of the TOE's access and service protection.

TOE test configurations: The tests are performed remotely on a virtual machine running in a test environment of the developer. The environment includes the TOE virtual machine and all necessary resources to repeat and conduct tests. The developer uses the identical environment for all tests. Since the developer uses the same test environment, including the TOE, for his tests it is warranted that the configuration used for the evaluator tests is the same.

Attack scenarios having been tested: The attack scenario that has been tested is AS.1 "Fuzzing of HTTP responses retrieved from the CSP-L resulting in a misbehaviour of the TOE observable at the CTSS interface of the TOE".

SFRs penetration tested: The following SFR was covered by the penetration tests:

- FTP_ITC.1/TC

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 [ST] provided that all measures required by the developer are applied.

9. Results of the Evaluation

Based on the evaluation, the following assurance level was attained:

- EAL2 (substantial), augmented by ALC_CMS.3 and ALC_LCD.1

10. Comments and recommendations

The documents as outlined in Table 3: Delivery items provide essential instructions for operating the TOE, and all security guidelines within them must be followed. Furthermore, the operational environment must satisfy all assumptions, threats, and organizational security policies (OSPs) specified in the Security Target [ST] that the TOE does not address directly.

Product users must integrate certification results into their system risk management process. To address evolving attack methods, users should establish a clear timeframe for when a TOE re-assessment is required and request it from the certificate sponsor.

11. Signature of the personnel responsible for the certification decision

The final certification decision was taken by Mr. Christoph Sesterhenn in the capacity of head of certification body.

Christoph Sesterhenn
25.09.2026 14:09 Uhr
.....
Christoph Sesterhenn

Annex A: Additional information

There is no additional information necessary.

Annex B: References, glossary and bibliography

B.1: Security Target

The following security target was evaluated: Swissbit Cloud SMAERS – Common Criteria Security Target, version 1.1.3, 14 September 2026 ([ST])

The evaluated security target will be published on the website of the European Union Agency for Cybersecurity, ENISA. The published security target is not sanitized.

B.2: Mark or Label associated to the Scheme

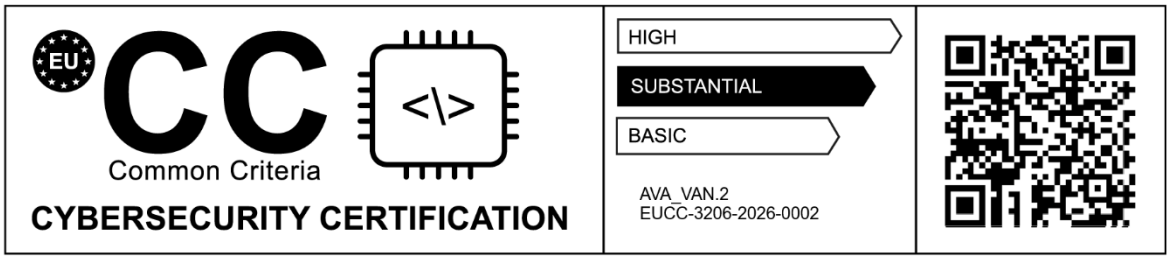

Figure 2: EUCC label

B.3: Bibliography

[CSA] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

[CSA IA] Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)

[CSA IA Normen] Commission Implementing Regulation (EU) 2024/3144 of 18 December 2024 amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation

[ENISA EUCC CB] ENISA, EUCC Scheme, State of the Art Document, Accreditation of CBs for the EUCC Scheme, Version 1.6b, November 2024

[CC:2022] Common Criteria for Information Technology Security Evaluation, CC:2022, Revision 1, November 2022
Part 1: Introduction and general model
Part 2: Security functional components
Part 3: Security assurance components
Part 4: Framework for the specification of evaluation methods and activities
Part 5: Pre-defined packages of security requirements
https://www.commoncriteriapportal.org

[CEM:2022] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, CEM:2022, Revision 1, November 2022
https://www.commoncriteriapportal.org

[CCErrata:2022] Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), version 1.2, 15.10.2025

[EUCC-SotA] EUCC State-of-the-Art documents: https://certification.enisa.europa.eu/publications/eucc-state-art-documents_en

[ETR] Evaluation Report – Evaluation Technical Report (ETR) – Summary, version 1.0, 23 September 2026

[PPs] Protection Profile Security Module Application for Electronic Record-keeping Systems (SMAERS), BSI-CC-PP-0105-V2-2020, version 1.0

[SOG-IS] SOG-IS Crypto Working Group; SOG-IS Crypto Evaluation Scheme; Agreed Cryptographic Mechanisms; Version 1.3 February 2023

[ST] Swissbit Cloud SMAERS – Common Criteria Security Target, version 1.1.3, 14 September 2026

[AGD] Swissbit Cloud SMAERS – Guidance Documentation, version: 1.1.0, 18 June 2026

[USK] Swissbit Cloud-TSE 2 – Secure Platform Concept (Umgebungsschutzkonzept, USK). version 1.1.0, 18 June 2026

B.4: List of Figures

B.5: List of Tables

B.6: Glossary

BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Common Criteria
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
EUCC	European Common Criteria-based cybersecurity certification scheme
ITSEF	Information Technology Security Evaluation Facility
NCCA	National Cybersecurity Certification Authority
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation