Certification Report

Swissbit Cloud CSP-L 1.1.0

- Cryptographic Service Provider Light (CSPLight) -

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-3206-2026-0001

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	Cryptographic Service Provider Light (CSPLight)	Cryptographic Service Provider Light (CSPLight)
Name of Product	Swissbit Cloud CSP-L 1.1.0	Swissbit Cloud CSP-L 1.1.0
Shortname of Product	Swissbit Cloud CSPL	Swissbit Cloud CSPL
Manufacturer	Swissbit AG	Swissbit AG
Protection Profiles	• Base-PP: Protection Profile Cryptographic Service Provider Light (CSPLight) Version 1.0, BSI-CC-PP-0111-2019 • PP-Module: CSPLight Time Stamp Service and Audit (PPM-TS-Au), Version 1.0, BSI-CC-PP-0112-2020 • PP-Module: CSPLight Clustering (PPM-Cl), Version 1.0, BSI-CC-PP-0113-2020	• Base-PP: Protection Profile Cryptographic Service Provider Light (CSPLight) Version 1.0, BSI-CC-PP-0111-2019 • PP-Module: CSPLight Time Stamp Service and Audit (PPM-TS-Au), Version 1.0, BSI-CC-PP-0112-2020 • PP-Module: CSPLight Clustering (PPM-Cl), Version 1.0, BSI-CC-PP-0113-2020
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-3206-2026-0001	EUCC-3206-2026-0001

Name	Invariant (edit here)	Output value
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	17.09.2026	Content and results based on ITSEF-documents
0.3	24.09.2026	Incorporation of update of ITSEF documents
0.4	24.09.2026	Quality Assurance
1.0	25.09.2026	Final Version

Table 2: Change History

Table of Contents

1. Executive Summary

The TOE is Swissbit Cloud CSP-L 1.1.0 by Swissbit AG running on FIPS 140-3 Level 4 certified version of the Private Machines Enforcer R2 compute blades as the execution platform, which is not part of the 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 profiles:

- Base-PP: Protection Profile Cryptographic Service Provider Light (CSPLight) Version 1.0, BSI-CC-PP-0111-2019
- PP-Module: CSPLight Time Stamp Service and Audit (PPM-TS-Au), Version 1.0, BSI-CC-PP-0112-2020
- PP-Module: CSPLight Clustering (PPM-Cl), Version 1.0, BSI-CC-PP-0113-2020

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-3206-2026-0001 on 25.09.2026, with a validity until 24.09.2031.

Please note: A previous version of the TOE (Swissbit Cloud CSPL 1.0.7) had been certified under BSI-DSZ-CC-1238-2025, issued on 27 March 2025.

2. Identification of the ICT-Product

The Target of Evaluation (TOE) is called:

Swissbit Cloud CSP-L 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)	For its operation, the TOE needs the following hardware and software requirements fulfilled in its environment. 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: Manufacturer: PMI Product: E-RX2 hardware version: R2-XD1736NT Firmware Version: 2.5.3 Ubuntu server, version 24.04	SW	The signed jar file is stored in the *fiscal3-fabric git repository* of Swissbit AG and the corresponding commit is tagged with cspl-v1.1.0 (1.1.0 is the version of the Swissbit Cloud CSP-L of the current Common Criteria certification process).
2	Associated guidance documentation	Swissbit Cloud CSP-L - Guidance Documentation, Version 1.10.1, 24.06.2026, Swissbit AG SHA256: 02c148691d47f335753f022982c73c20f7a0fac65f284f9d5c64475189df776c	PDF	The guidance documents and the TOE are delivered to the customer via a personal delivery, encrypted and signed email or a secure download portal.

Table 3 Delivery items

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 documents 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-1.1.0.jar

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

The TOE is Swissbit Cloud CSPL, TOE Version: 1.1.0 according to [ST].

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
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
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.
User identification and authentication	The TOE implements user identification and authentication, all subsystems implementing TSFI must perform this before giving access to the specific TOE services.
Access control	The TOE enforces a strict role based access control. The roles associated with the authenticated user and user's current status define 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.

TOE Security Functionality	Description
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 5: TOE Security Functionality

Specific details concerning the above mentioned security policies can be found in sec. 7 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.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 [ST], section 4.2.

6. Architectural Information

The TOE is a software TOE running on dedicated non-TOE hardware (Private Machines Enforcer R2) as well as dedicated non-TOE software (Ubuntu Linux), building the non-TOE platform. The TOE is operated on a hardware platform, namely “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 an Ubuntu Linux distribution with a minimal functionality.

The SFR-enforcing subsystems of the TOE are:

- Frontend subsystem
- Crypto subsystem
- Audit subsystem
- Storage subsystem
- Timekeeping subsystem

The frontend subsystem provides the following security functionality:

- Management of the three external interfaces of the TOE and is therefore the first point of contact for incoming request.
- Is 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

The crypto subsystem provides the following functionality to the server subsystem:

- Implements all cryptographic functionality needed by the TOE. It is also responsible for secure key storage and export based on access control attributes.
- Has been built around the open source library Bouncy Castle. The following functions are provided:
  - general cryptographic functions
  - key related functions
  - channel related functions
- The crypto subsystem is also responsible to seed the DRNG of Bouncy Castle at start-up and during every self-test.

The audit subsystem provides the following functionality to the server 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.

The storage subsystem provides the following functionality to the server subsystem:

- Writes to and reads data from the persistent storage of the system. The persisted storage is used to store configuration files.

The timekeeping subsystem provides the following functionality to the server 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.

The following picture shows the overall design of the TOE.

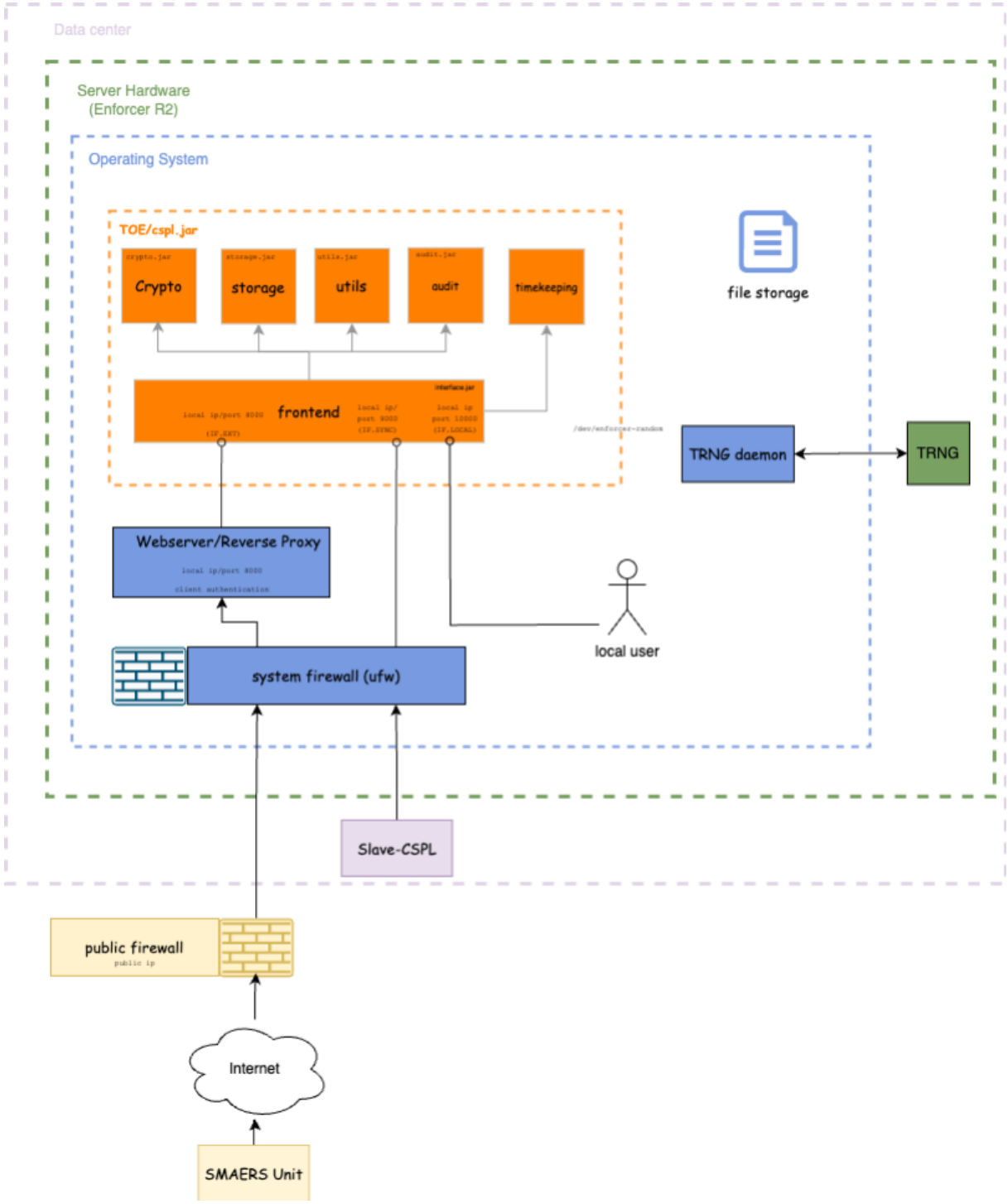

Figure 1: TOE Design

7. Supplementary Cybersecurity Information

The evaluated documentation as outlined in Table 3 Delivery items 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

CC Aspect	Result
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 component

The state-of-the-art documents of relevance to the TOE published by ENISA [EUCC SotA] were used.

The following protection profiles were used:

- Base-PP: Protection Profile Cryptographic Service Provider Light (CSPLight) Version 1.0, BSI-CC-PP-0111-2019
- PP-Module: CSPLight Time Stamp Service and Audit (PPM-TS-Au), Version 1.0, BSI-CC-PP-0112-2020
- PP-Module: CSPLight Clustering (PPM-Cl), Version 1.0, BSI-CC-PP-0113-2020

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

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 1.1.0”.

The TOE is running on a special hardware platform, the Enforcer R2 (by Private Machines) (hardware version: R2-XD1736NT, firmware version: 2.5.3). 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 an Ubuntu server.

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

Manufacturer: PMI
Product: E-RX2
Firmware Version: 2.5.3
The hardware carries a certification according to FIPS 140-3 level 4.

An Ubuntu server with version 24.04 is used.

Tests of the Developer

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 one or more slaves).

The current test environment comprises the following components:

- The TOE as JAR file [CSPL_JAR]
- The CSP-L Repository [CSPL_Repo], 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

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, the following independent evaluator tests were performed:

Test Case	Description
1	Request execution with an invalid role
2	Login with an incorrect password
3	Data decryption with an invalid key
4	TOE state after disconnected TRNG service
5	Repetition of the lifecycle manual test case
6	Fuzzing of the HTTP-Endpoint.

Table 7: Independent evaluator tests

Testing Results: The evaluators determined that 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 [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 14:08 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 CSP-L - Common Criteria Security Target, Version 1.10.3, 2026-09-14 ([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

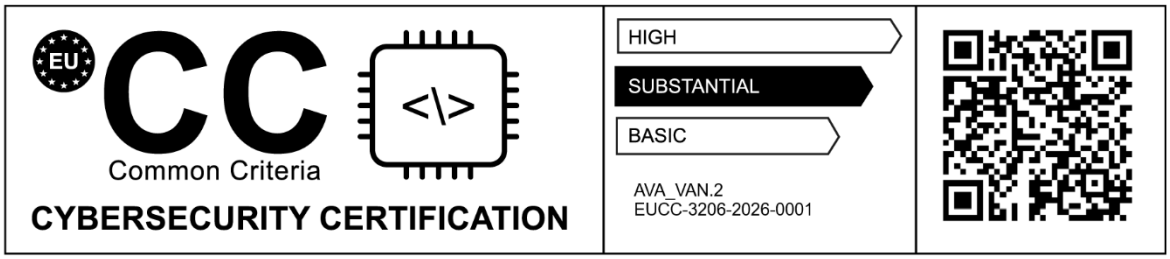

Figure 2: EUCC label

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 Cryptographic Service Provider Light (CSPLight) Version 1.0, BSI-CC-PP-0111-2019

CSPLight Time Stamp Service and Audit (PPM-TS-Au), Version 1.0, BSI-CC-PP-0112-2020

CSPLight Clustering (PPM-Cl), Version 1.0, BSI-CC-PP-0113-2020

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

[ST] Swissbit Cloud CSPL - Common Criteria Security Target, Version 1.10.3, 14.09.2026, Swissbit AG

[AGD] Swissbit Cloud CSP-L - Guidance Documentation, Version 1.10.1, 24.06.2026, Swissbit AG

[TDS] Swissbit Cloud CSP-L - TOE Design (TDS), Version 1.10.0, 09.06.2026, Swissbit AG

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