Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

A-SIT

1030 Wien, Seidlgasse 22 / 9
Tel.: +43 1 503 19 63-0
Fax: +43 1 503 19 63-66

8010 Graz, Sandgasse 38a
Tel.: +43 316 873-5514
Fax: +43 316 873-5520

http://www.a-sit.at
E-Mail: office@a-sit.at

DVR: 1035461
ZVR: 948166612
UID: ATU60778947

QSCD-CERTIFICATE PURSUANT TO ART. 30 PARA. 3 LIT. B EIDAS[1]

Qualified Signature and Seal Creation Device (QSCD) Ubiqu's qualified remote signature and seal creation device, version 2.8

Applicant:
Ubiqu Access B.V.
Kerstant van de Berglaan 13b
3054 EM Rotterdam
The Netherlands

Reference number: A-SIT-VIG-26-074

QSCD-Certificate valid from:
See Date of Qualified Electronic Signature

1. Product Description

The product is a Qualified Electronic Signature and Seal Creation Device (QSCD) which is operated in the secure operational environment of a qualified Trust Service Provider (TSP) to provide users with a remote signing functionality. When used in combination with qualified certificates ubiqu's QSCD generates qualified electronic signatures or seals as defined in eIDAS with the legal effects of Article 25.

Subcomponents:

The QSCD consists of a certified (Common Criteria EAL4+) HSM and ubiqu specific firmware ("functionality module") loaded onto this HSM. The HSM is operated according to its Common Criteria EAL4+ certification in conjunction with the corresponding security target. The QSCD uses the HSM type "Thales Luna K7 Cryptographic Module"[2].

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC amended by Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024

[2] Vendor: Thales, 20 Colonnade Road, Suite 200, Ottawa, ON K2E 7M6, Canada.
The certified hardware and firmware versions of the used cryptographic modules, for which this QSCD certificate is valid, are given in Section 6.

© A-SIT, Partner für Sicherheitsfragen

Generation of Signature and Seal Creation Data:

An identity provider (IDP)/TSP is responsible for identity vetting and registration of subjects for this purpose the IDP/TSP maintains a signer ID. During the activation procedure the signer ID is bound to the QSCD and the subject's smartphone app using a PUK[3] and an activation nonce that were securely delivered to the subject by the IDP/TSP. During the activation the subject sets a PIN, that will be used as second authentication factor (in addition to the smartphone) for subsequent SCD[4] activations. After this binding is completed the SCD/SVD[5] key pair (generation was done in the HSM before in conjunction with the PUK generation) is activated inside the HSM.

Storage of Signature and Seal Creation Data:

The SCD is stored encrypted outside the HSM using an HSM key. During the SCD activation after a successful two factor authentication the SCD is loaded into the HSM before signature or seal generation. All operations of generation, application and destruction of the SCD are implemented with the certified security functions of the HSM.

Signature and Seal Creation:

A Signature Creation Application (SCA) generates the DTBS/R[6] (i.e. hash of the document to be signed or sealed) on the SCA server and triggers the signature or seal invocation by sending the DTBS/R to the QSCD. The QSCD performs a two-factor authentication using the previously associated smartphone of the signer/seal creator and the PIN. If the authentication is successful, the SCD is loaded into the HSM, and a qualified electronic signature or seal (QES) is generated based on the previously provided DTBS/R. After signature or seal creation the SCD is deactivated inside the HSM, and the result of the signature operation is transferred from the QSCD to the SCA.

2. Compliance with the Requirements of eIDAS

The QSCD meets the following requirements, provided that the conditions in section 4 are fulfilled:

- requirements laid down in Article 29 para 1[7] eIDAS,
- requirements laid down in Article 39 para 1[8] eIDAS,

[3] PUK - Personal Unblocking Key
[4] SCD – Signature/Seal Creation Data
[5] SVD – Signature/Seal Validation Data
[6] DTBS/R – Data To Be Signed/Representation
[7] *Qualified electronic signature creation devices shall meet the requirements laid down in Annex II.*
[8] *Article 29 shall apply mutatis mutandis to requirements for qualified electronic seal creation devices.*

- requirements laid down in Annex II eIDAS (para 1 lit. a[9],b[10],c[11],d[12], para 2[13], para 3[14], para 4 lit a[15], b[16])

The compliance of the QSCD is thus confirmed within the following categories:

- components and procedures for the generation of signature or seal creation data,
- components and procedures for the storage of signature or seal creation data,
- components and procedures for the processing of signature or seal creation data

3. Validity Period of the QSCD-Certificate

This QSCD-Certificate is valid up to 5 years or up to a preceding revocation by A-SIT.

On assignment A-SIT will conduct a continuous surveillance concerning the security of the technical components and processes used as well as the suitability of the cryptographic algorithms and parameters. The issuance of this QSCD-Certificate includes surveillance for a period of two years. In order to maintain a valid certification, the applicant has to conduct a vulnerability assessment every two years and remedy any identified vulnerabilities in a timely manner. The QSCD-Certificate will be revoked if the technical components and processes or the cryptographic algorithms and parameters used no longer reflect the state of the art, if vulnerability assessments are not conducted every two years, if identified vulnerabilities are not remedied in a timely manner or if there is no further surveillance assigned.

4. Operating Conditions

The validity of this QSCD-Certificate is subject to the conditions stated below. The measures taken shall be

- ascertained by the trust service provider's security and certification policy,
- integrated into the guidance of the signatory or creator of a seal and

[9] *Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that the confidentiality of the electronic signature creation data used for electronic signature creation is reasonably assured*.

[10] *Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that the electronic signature creation data used for electronic signature creation can practically occur only once.*

[11] *Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that the electronic signature creation data used for electronic signature creation cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology.*

[12] *Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others.*

[13] *Qualified electronic signature creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing.*

[14] *Generating or managing electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider.*

[15] *Without prejudice to point (d) of point 1, qualified trust service providers managing electronic signature creation data on behalf of the signatory may duplicate the electronic signature creation data only for back-up purposes provided the following requirements are met: the security of the duplicated datasets must be at the same level as for the original datasets.*

[16] *Without prejudice to point (d) of point 1, qualified trust service providers managing electronic signature creation data on behalf of the signatory may duplicate the electronic signature creation data only for back-up purposes provided the following requirements are met: the number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service.*

- their effect shall be ensured by means of supervision (in accordance with Article 20 eIDAS).

(1) The unambiguous assignment and the safe completion of the user session, the confidentiality and integrity of the authorization codes as well as the integrity of the data to be signed or to be sealed during transmission from the signatory or creator of a seal to the QSCD are part of the QSCD's system environment[17] and thus outside the scope of this QSCD-certificate. It must be ensured that the signatories or creators of a seal are informed that components used for the initiation of the signature or sealing process (OTP device, mobile phone, web browser) must be suitably protected. The signatories shall keep control of their assigned OTP devices and shall promptly report any circumstance where the credential is compromised according to the defined revocation or suspension procedures.

(2) The QSCD must be operated by a qualified trust service provider.

(3) The qualified trust service provider must operate the QSCD in a protected environment, in particular it must be ensured that
- physical access to the QSCD is limited to authorized privileged users
- the QSCD or any of its externally stored assets are protected against loss or theft
- the QSCD is regularly inspected to deter and detect tampering (including attempts to access side-channels, or to access connections between physically separate parts of the QSCD, or parts of the hardware appliance)
- the QSCD is protected against the possibility of attacks based on emanations (e.g. electromagnetic emanations) according to risks assessed for the operating environment
- the QSCD is protected against unauthorized software and configuration changes
- all instances of the QSCD holding the same assets (e.g. where a key is present as a backup in more than one instance of the QSCD) are protected to an equivalent level

(4) The HSM must be initialised and operated based on its Common Criteria EAL4+ certification.

(5) Only those cryptographic algorithms and key sizes listed in section 5 shall be used for the creation of qualified electronic signatures or qualified electronic seals.

(6) HSM operations such as backup, storage and restoration of private or secret keys must only be performed by authorized personnel using smartcards and under at least dual control.

(7) Electronic signature or seal creation data may be duplicated for back-up purposes only to the extent strictly necessary to ensure continuity of the service.

(8) It must be ensured that components of signers, which have vulnerabilities or are otherwise not suitable for authentication, cannot be used to authorize a signature creation.

5. Algorithms and Corresponding Parameters

For the creation of qualified electronic signatures or qualified electronic seals the QSCD uses the cryptographic algorithms[18]:

- RSASSA-PKCS#1-v1_5[19] or RSASSA-PSS according to PKCS#1 v2.2 (RFC 8017) with a cryptographic key size of 3072 or 4096 bits.
- ECDSA using the curves P-256, P-384 and P-521 according to FIPS 186-5 with cryptographic key sizes from 256-bit to 512-bit.

[17] in accordance with recital 56 of eIDAS

[18] Annotation: The applicable version of the Agreed Cryptographic Mechanisms issued by the European Cybersecurity Certification Group Sub-group on Cryptography applies and is subject to surveillance.

[19] Annotation: The acceptability deadline for the legacy use of RSASSA-PKCS1-v1_5 is set to at least December 31, 2031 by "European Cybersecurity Certification Group Sub-group on Cryptography, Agreed Cryptographic Mechanisms", Version 2.0, April 2025

For the calculation of hash values the algorithms SHA-256, SHA-384 and SHA-512 according to FIPS 180-4 are supported[20].

6. Assurance Level and Strength of Mechanism

The QSCD supports the following HSM type:

- Thales Luna K7 Cryptographic Module; Firmware 7.8.5

For the used HSM Thales Luna K7 Cryptographic Module the following Common Criteria certificate issued by TrustCB B.V. under “The Netherlands scheme for Certification in the Area of IT Security (NSCIB)” applies:

- Certificate number NSCIB-CC-2400054-01 for Thales Luna K7 Cryptographic Module issued by TrustCB B.V. on 05-09-2025.
  The certification report by TrustCB B.V. (report number: NSCIB-CC-2400054-CR) confirms a successful evaluation of the HSM (Hardware versions: 808-000048-002, 808-000048-003, 808-000073-001, 808-000073-002, 808-000066-001, 808-000069-001, 808-000070-001; Firmware versions: 7.7.0, 7.7.1, 7.7.2 or 7.8.5; Bootloader versions 1.1.1, 1.1.2, 1.1.4 or 1.1.5) against its Security Target. The Security Target claims ’strict’ conformance to the Protection Profile EN 419 221-5. The evaluation was performed according to Common Criteria version 3.1 Release 5 with assurance level EAL4+ augmented by ALC_FLR.2[21] and AVA_VAN.5[22].

Since there are no standards for the security assessment published by the European Commission by means of implementing acts, the QSCD certification was performed under eIDAS article 30 para. 3 lit. b and the confirmation body applied equivalent security levels considering the current state of the art.

In its intended environment the QSCD resists against attackers with high attack potential.

The results of the performed assessment which is the basis for this QSCD-Certificate are documented in the QSCD-Certification report under the reference A-SIT-VIG-26-074.

Authorized Signature:

A-SIT Secure Information Technology Center – Austria

Vienna, (Date see electronic signature)

	Signatory	Herbert Leitold
	Date/Time-UTC	2026-11-02T20:28:23+01:00
	Verification	Information about the verification of the electronic signature can be found at: https://www.signaturpruefung.gv.at

Herbert Leitold, Director

[20] Annotation: The hash value calculation is performed outside of the QSCD by the SCA.
[21] ALC_FLR.2 – Flaw reporting procedures
[22] AVA_VAN.5 – Advanced methodical vulnerability analysis