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) certSIGN's qualified remote electronic signature and seal creation device ("Paperless"), version 1.0, update 2

Applicant:
CertSIGN S.A.,
Şos. Olteniţei Nr. 107A, bl. C1,
041303 Bucureşti - Sector 4, Romania

Reference number: A-SIT-VIG-26-076

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

1. Product Description

CertSIGN's qualified remote electronic signature and seal creation device ("Paperless") is a product for qualified electronic signatures and seals intended to be used as a remote Qualified Electronic Signature Creation Device (QSCD) in the secure operational environment of a qualified trust service provider (TSP).

Subcomponents:

Paperless uses HSM devices as cryptographic modules for the generation and protection of the signature or seal creation data (SCD). The HSMs are operated according to their respective certification in conjunction with the corresponding security policies or security targets[2]. The Remote Signing Service component acts as Signature Activation Module (SAM) and allows users to retain exclusive control of their signing keys. It uses either an SMS Gateway component or a TOTP[3] Authentication Service to authorize the signature or seal creation process. The Signing Service Application (SSA) is responsible for accepting signing requests by the SAM and forwarding them to

[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] The certified hardware and firmware versions of the used cryptographic modules, for which this QSCD certificate is valid, are given in Section 6.

[3] TOTP – Time-Based One-Time Password

© A-SIT, Partner für Sicherheitsfragen

the HSM. The last component is the CryptoService, which is responsible for handling requests for key generation and certificate signing.

The QSCD is intended to be operated by a qualified trust service provider in a secure operational environment as part of a remote electronic signature service. The QSCD also uses further components (e.g. certification authority, client application, etc.) to provide its services. These, however, are not part of the QSCD and thus not in the scope of this certification.

Generation of Signature and Seal Creation Data:

On the first use of the QSCD by a user (signatory or creator of a seal), the corresponding SCD/SVD key pair is generated inside the HSM. Users only interact with the QSCD through trusted client applications (i.e. server applications), which use mutual authentication to consume the QSCD's services through a SOAP interface. This implementation is referred to by certSIGN as system-to-system. Access to the private key is controlled by the SAM. After SCD generation a certificate request (PKCS#10), signed by the HSM, is sent to a trusted Certificate Authority (CA). The returned certificate is bound to the SCD and stored within the SSA's application keystore. The process of issuing qualified certificates is outside the scope of this confirmation.

Storage of Signature and Seal Creation Data:

The SCD is securely stored within the HSM throughout its lifecycle in encrypted form. As soon as the SCD is out of use (e.g. user unregisters from the service) it is securely destroyed using the HSM's security functions.

Signature and Seal Creation:

Creating a signature or seal is only possible to users that are already registered to the service, i.e. already possess a private signing key inside the HSM. A user can then initiate a signature or seal creation process through an external client application (i.e. trusted server application), by passing on the data to be signed or sealed and the personal identification credentials. The client application calculates the hash of the data to be signed or sealed (DTBS/R) and forwards the request to the Remote Signing Service (SAM). After checking the received request and credentials the SAM starts the authentication by requiring the user's Signature Interaction Component (SIC) to authenticate itself using a client certificate. This PIN secured client certificate was issued by the certSIGN CA for the specific user in the course of enrolment. As a secondary authentication factor, the SAM supports one of two paths.

(1) The SAM utilizes the SMS Gateway to send the user an SMS message containing an OTP[4]. The user sends the OTP over a secure channel through the client application to the SAM, in order to prove the possession of the mobile device and authorize the signature or seal creation process. After the SAM validates the received OTP, it forwards the request to the SSA, which uses the HSM to create the signature or seal.
(2) The SAM uses a transaction-bound time-based OTP (TBTOTP) as the second authentication factor. The signer generates a TOTP using their enrolled authenticator application and computes a transaction-bound TOTP code using the associated signing session identifier. This code is then submitted as the SAD second-factor element. The TOTP Authentication Service then retrieves the stored encrypted TOTP seed and performs the same calculation to receive the correct TBTOTP code and compares it with the code provided by the signer, before returning the verification result to the SAM. After verification, the SAM forwards the request to the SSA, which uses the HSM to create the signature or seal.

The signed or sealed data is then returned to the requesting client application, which includes the signature or seal into the DTBS.

[4] OTP – One-Time Password

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[5] eIDAS,
- requirements laid down in Article 39 para 1[6] eIDAS,
- requirements laid down in Annex II eIDAS (para 1 lit. a[7],b[8],c[9],d[10], para 2[11], para 3[12], para 4 lit a[13], b[14])

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.

---

[5] *Qualified electronic signature creation devices shall meet the requirements laid down in Annex II.*

[6] *Article 29 shall apply mutatis mutandis to requirements for qualified electronic seal creation devices.*

[7] *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*.

[8] *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.*

[9] *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.*

[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 be reliably protected by the legitimate signatory against use by others.*

[11] *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.*

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

[13] *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.*

[14] *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.*

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
- 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[15] 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 (QTSP).

(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) During Entrust HSM initialisation a quorum of at least two has to be defined for the HSM's Administrator Card Set (ACS) and the generated smart cards have to be controlled by different persons to ensure the principle of dual control.

(5) During Thales HSM initialisation the principle of dual control must be ensured and at least one person must have the role "HSM Security Officer". For further administrative tasks during the operation the principle of dual control must be ensured.

(6) 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.

(7) The HSMs must be initialised and operated according to their respective certification.

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

(9) 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 or seal creation.

5. Algorithms and Corresponding Parameters

[15] in accordance with recital 56 of eIDAS

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

- RSASSA-PKCS1-v1_5 according to PKCS#1 v2.2 (IETF RFC 8017) with a cryptographic key size of 3072 or 4096 bits or
- ECDSA using the curves P-256 and P-521 of the NIST-family according to FIPS 186-5 with a cryptographic key size of 256-bit and 521-bit.

For the calculation of hash values the hash functions SHA-256 and SHA-512 according to FIPS 180-4 are supported.

6. Assurance Level and Strength of Mechanism

The QSCD supports the following HSM types:

- Entrust nShield 5s, Firmware: 13.2.4
- Entrust nShield 5s, Firmware: 13.4.5
- Entrust nShield 5s, Firmware: 13.5.1
- Thales Luna Network HSM 7, Firmware: 7.7.0
- Thales Luna Network HSM 7, Firmware: 7.7.1
- Thales Luna Network HSM 7, Firmware: 7.7.2
- Thales Luna Network HSM 7, Firmware: 7.8.5

NIST FIPS 140-3: For the Entrust HSMs with firmware versions 13.2.4 or 13.4.5, the following FIPS 140-3 level 3 certifications apply:

- FIPS validation certificate No. 4745[16]
  Issued on 2024-07-31 and last updated on 2025-04-01 by the US (National Institute of Standards and Technology) and the Canadian (Canadian Centre for Cyber Security) FIPS 140 Series certification body for *nShield 5s F3* and *nShield 5s for nShield 5c and for nShield HSMi* with firmware version 13.2.4 (recovery-version 13.2.4; uboot-versions 1.1.0 and 1.4.1) and hardware versions PCA10005-01 revision 03 and 04.
- FIPS validation certificate No. 5329[17]
  Issued on 2026-06-15 and last updated on 2026-06-29 by the US (National Institute of Standards and Technology) and the Canadian (Canadian Centre for Cyber Security) FIPS 140 Series certification body for *nShield 5s F3* and n*Shield 5s for nShield 5c and for nShield HSMi* with firmware version 13.4.5 (recovery-version 13.2.4; uboot-versions 1.1.0 and 1.4.1) and hardware versions PCA10005-01 revision 03 and 04.

The certificate confirms that the respective HSM was successfully evaluated against FIPS 140-3 level 3.

Common Criteria EAL4+: For the Entrust HSMs with firmware version 13.5.1 and the Thales HSMs with firmware versions 7.7.0, 7.7.1, 7.7.2 or 7.8.5 the following Common Criteria certificates apply:

- Common Criteria certificate NSCIB-CC-2200057-01[18]
  Issued on 2024-04-11 by TrustCB B.V. for the HSM types Entrust *nShield5s* and *nShield5c*, with firmware version 13.5.1 (Bootloader 1.4.1; recovery image 13.5.0) and hardware version PCA10005-01 revision 03.
- Common Criteria certificate NSCIB-CC-2400054-01[19]
  Issued on 2025-09-05 by TrustCB B.V. for the HSM type Thales Luna K7 Cryptographic Module with firmware versions 7.7.0, 7.7.1, 7.7.2 or 7.8.5 (Bootloader: 1.1.1, 1.1.2, 1.1.4 or

[16] https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4745
[17] https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/5329
[18] https://www.commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/NSCIB-CC-2200057-01-Cert.pdf
[19] https://www.commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/NSCIB-CC-2400054-01-Cert.pdf

1.1.5) and hardware versions 808-000048-002, 808-000048-003, 808-000073-001, 808-000073-002, 808-000066-001, 808-000069-001 or 808-000070-001.

The certificates confirm that the respective HSM was successfully evaluated against Common Criteria version 3.1 revision 5, EAL4+[20] (augmented with 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 taking into account the 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-26-076.

Authorized Signature:

A-SIT Secure Information Technology Center – Austria

Vienna, (Date see electronic signature)

SIGNATURE INFORMATION	**Signatory**	Herbert Leitold
	Date/Time-UTC	2026-09-02T23:26:26+02:00
	Verification	Information about the verification of the electronic signature can be found at: https://www.signaturpruefung.gv.at

Herbert Leitold, Director

[20] EAL – Evaluation Assurance Level
[21] Life-Cycle Support – Flaw reporting procedures
[22] Vulnerability Assessment – Advanced methodical vulnerability analysis