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

A-SIT

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

Inffeldgasse 16a, 8010 Graz
Tel.: +43 316 873-5514
Fax: +43 316 873-5520

https://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) Entrust Signature Activation Module, version 1.0.4

Applicant:
Entrust EU S.L.
Paseo del Club Deportivo 1, Bloque 3, Bajo
28223 Pozuelo de Alarcón (Madrid)
Spain

Reference number: A-SIT-VIG-23-092

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

1. Product Description

The product “Entrust Signature Activation Module, version 1.0.4” by Entrust EU S.L. is a Qualified Remote Signature/Seal Creation Device (QSCD) to provide users with a remote signing or sealing functionality.

Subcomponents:

The Qualified Remote Electronic Signature and Seal Creation Device (“Entrust Signature Activation Module”) uses HSM (Hardware Security Module) devices[2] as cryptographic modules for the generation and protection of the signature or seal creation data (SCD). Only the HSM device family “Entrust[3] nShield Solo XC” can be used for the QSCD. HSMs are operated according to their Common Criteria EAL4+ certification in conjunction with the corresponding security target.

Furthermore, the QSCD uses a Signature Activation Module (SAM) as a single component to communicate with the HSM, in order to authorize and initiate the signature or seal creation process.

[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

[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] nCipher Security Limited (an Entrust company) - One Station Square, Cambridge CB1 2GA, United Kingdom

These two components, the HSM and the SAM, together form the QSCD, which is intended to be operated by a qualified trust service provider in a secure operational environment as part of a remote electronic signature and seal service. For its services, the QSCD also uses other components such as identity providers or applications. These, however, are not part of the QSCD and thus not in the scope of this certification

Generation of Signature and Seal Creation Data:

Upon an initial registration request of a user by a registration authority, a trusted application can request to the SAM the generation of the corresponding SCD[4]/SVD[5] key pair inside the HSM. Then, the trusted application requests binding the SCD/SVD key pair to the user and optionally also requires the user to provide a private secret (i.e., user credential), which is used for authorizing both signature or seal creation requests and the access to the SCD. Access to the operations for creating and assigning the SCD is controlled by the SAM, which requires to be started by an authenticated operator in a protected environment. An external registration provider component orchestrates the certification of the SCD from a Public Key Infrastructure (PKI), creating the Certificate Signing Request (CSR) for the key pair, requesting to the SAM (via the trusted application) its proof-of-possession and finally obtaining the X.509 certificate.

Storage of Signature and Seal Creation Data:

The HSM provides a secure protection mechanism integrated into its "Security World" software for protecting the private keys in a secure way, which is used from the SAM component in the same trusted environment that runs the "Security World" software. After the SCD/SVD key pair is generated within the HSM, the SCD is encrypted using the HSM's hardware key and it is protected by a certified key which is managed by the SAM. After that, it is returned by the SAM outside the SAM. The SCD never leaves the HSM unencrypted nor unprotected by the SAM. This way the SCD can only be used by the combination of the SAM and the HSM.

Signature and Seal Creation:

A user can only request both a signature or seal creation via trusted applications (through the SSA) and not via direct access, in particular to the QSCD. The communication between those external components and the remote QSCD employs the Signature Activation Protocol (SAP). A user requesting the signature of one or more documents (i.e., a set of Data to be Signed (DTBS)) interacts with the Signer Interaction Component (SIC), which can be any device that supports the secured TLS[6] connection (e.g., web browser, mobile app, desktop app). To start the signature or seal creation request, typically the Signature Creation Application (SCA) requires the user to log in. This can be done by the SCA, also through third parties, or directly by the Identity Provider and Authorization Server (IdP/AS) component. The latter option provides a single sign-on experience. The IdP/AS component initiates the authorization of the user. A two-factor authorization that reaches SCAL2[7] level is required for this step; it may be split into two steps, where the second factor is postponed until the authorization of the concrete signing key and hash representation or request the optional user credential, which is managed by the HSM/SAM. The authenticated user provides the DTBS or set of DTBS to the SCA, which displays it back to the user to review, before computing the hash representation (Data to be Signed / Representation (DTBS/R)) and proceeding to sign it. The SCA sends the DTBS/R to the SSA to invoke the signature or seal operation. IdP/AS authorizes the user access of a concrete signing key to sign the concrete DTBS/R. The fully authenticated user can inspect the signing key identifier and DTBS/R and give a final consent to the signature or seal creation. This consent creates an assertion, the Signature Activation Data (SAD), which is only valid for this particular transaction. The SSA verifies the signature request including the token and invokes the SAM component of the QSCD. The SAM verifies the SAD and DTBS/R. If the verification is correct, it loads and activates the signing key in the HSM, which then encrypts the DTBS/R with this key thus generating the signature or seal. The signature or seal is returned to the SCA and attached to the DTBS.

[4] SCD – Signature Creation Data
[5] SVD – Signature Verification Data
[6] TLS – Transport Layer Security
[7] SCAL2 – Sole Control Assurance Level 2

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[8] eIDAS,
- requirements laid down in Article 39 para 1[9] eIDAS,
- requirements laid down in Annex II eIDAS (para 1 lit. a[10],b[11],c[12],d[13], para 2[14], para 3[15], para 4 lit a[16], b[17])

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 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. 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 or if there is no further surveillance assigned.

---

[8] *Qualified electronic signature creation devices shall meet the requirements laid down in Annex II.*
[9] *Article 29 shall apply mutatis mutandis to requirements for qualified electronic seal creation devices.*
[10] *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.*
[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 can practically occur only once.*
[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 cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology.*
[13] *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.*
[14] *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.*
[15] *Generating or managing electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider.*
[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 security of the duplicated datasets must be at the same level as for the original datasets.*
[17] *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[18] 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 (one-time password (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) During 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) 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.

(6) The HSMs must be initialised and operated according to their Common Criteria EAL4+ certification.

(7) 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.

(8) External authentication mechanisms, which are used to authenticate a user in order to create a qualified electronic signature or seal, shall correspond to an authentication means equivalent to EC Implementing Regulation 2015/1502 for assurance level substantial or higher[19].

(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 creation.

[18] in accordance with recital 56 of eIDAS

[19] COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market; as defined in ANNEX Clauses 2.1, 2.2.1 and 2.3.1

5. Algorithms and Corresponding Parameters

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 (RFC 8017) with cryptographic key sizes of 2048-bit or 4096-bit
- ECDSA[20] using the curves P-256, P-384 and P-521 of the NIST family according to FIPS 186-4 with cryptographic key sizes of 256-bit to 512-bit

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

6. Assurance Level and Strength of Mechanism

The QSCD supports the following HSM type and firmware:

- Entrust nShield Solo XC product family[21], Firmware: v12.50.7 and v12.60.15

Entrust nShield Solo XC HSM v12.50.7: The *Certification Report nShield Solo XC Hardware Security Module v12.50.7* by TÜV Rheinland confirms a successful evaluation of the HSM against its security target *nCipher - nShield Solo XC HSM Security Target*. The evaluation was performed according to Common Criteria version 3.1, revision 5 with assurance level EAL4[22] augmented with ALC_FLR.2[23] and AVA_VAN.5[24] and in conformance to the protection profile CEN EN 419 221-5.

Entrust nShield Solo XC HSM v12.60.15: The *Certification Report nShield Solo XC Hardware Security Module v12.60.15* in conjunction with the *Assurance Continuity Maintenance Report nShield Solo XC Hardware Security Module v12.60.15* by TÜV Rheinland confirm a successful evaluation of the HSM against its security target *Entrust - nShield Solo XC HSM Security Target*. The evaluation was performed according to Common Criteria version 3.1, revision 5 with assurance level EAL4 augmented with ALC_FLR.2 and AVA_VAN.5 and in conformance to the protection profile CEN EN 419 221-5.

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 current state of the art.

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

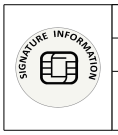
The results of the performed assessment, which is the basis for this QSCD-Certificate, are documented in the QSCD-Certification report under the reference A-SIT-VIG-23-092.

[20] ECDSA – Elliptic Curve Digital Signatuer Algorithm
[21] nShield Solo XC F2, nShield Solo XC F3, nShield Solo XC for nShield Connect XC
[22] EAL – Evaluation Assurance Level
[23] ALC_FLR.2 – Flaw reporting procedures
[24] AVA_VAN.5 – Advanced methodical vulnerability analysis

Authorized Signature

A-SIT Secure Information Technology Center – Austria

Vienna, (Date see electronic signature)



Signatory	Herbert Leitold
Date/Time-UTC	2023-12-19T13:22:51+01:00
Verification	Information about the verification of the electronic signature can be found at: https://www.signaturpruefung.gv.at

Herbert Leitold, Director