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) IvSign, version 1.0

Applicant:
Ivnosys Soluciones S.L.U.
C/ Acceso de Ademuz, 12 – Piso 1º
46980 Paterna, Valencia
Spain

Reference number: A-SIT-VIG-22-035

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

1. Product Description

The hereby certified product “Qualified Signature and Seal Creation Device (QSCD) IvSign” by Ivnosys Soluciones S.L.U. is a Qualified Remote Signature/Seal Creation Device (QSCD). It provides a remote signature or seal creation service, where none of the QSCD’s components are on the client side but deployed in the tamper-protected environment of the Trust Service Provider (TSP). To achieve this remote functionality, the QSCD implements a Trustworthy System Supporting Server Signing (TW4S) in accordance with EN 419 241-1:2018.

Subcomponents:
The QSCD consists of two subcomponents: The Signature Activation Module (SAM) and the Hardware Security Module (HSM). The SAM is a software component connected to the HSM via a trusted channel. Its purpose is to handle the validation of incoming requests and the signing key activation, to this end it implements the Signature Activation Protocol (SAP).

The HSM is a tamper-proof hardware component for the secure execution of cryptographic operations. Currently only the HSM device family “Thales Luna K7 Cryptographic Module”, with

[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

firmware version 7.7.0 is supported. HSMs are operated according to their Common Criteria EAL4+[2] certification in conjunction with the corresponding security target.

Only these two components form the certified area, other components (e.g. Identity Provider) and processes (e.g. certification process) are not part of the assessment and thus not in the scope of this certification.

Generation of Signature and Seal Creation Data:

The Server Signing Application (SSA) initiates the signer and key generation function of the QSCD, which then generates the corresponding SCD/SVD key pair inside the HSM and binds it to the signing identity of the user. For every SCD generation, a random keypass-key is also generated. This keypass is an intermediate key that is used for wrapping the private key before it is persisted into the internal database. The keypass itself is then encrypted by the authorization data of the signer (signerpass) and also saved in the database. This way, the access to the SCD is controlled by the SAM, but only after the initial consent of the signer. The SSA component requests a Certificate Signing Request (CSR) for the key pair to obtain a certificate from a PKI, which is then also bound to the signing identity. The CSR is electronically signed by the CA.

Storage of Signature and Seal Creation Data:

Before the SCD leave the HSM in order to be stored, they are encrypted using a non-exportable encryption key of the HSM, the SKS Master Key (SMK). This encryption is part of the Scalable Key Storage (SKS), a concept of the HSM manufacturer to increase the available key storage, without lowering the security of the stored assets. Within the SKS, keys are not stored in the HSM's internal memory anymore, but encrypted by the HSM's SKM and then saved with their security attributes as key blob to the QSCD's internal database. Therefore, 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, where the HSM also has to be in possession of the correct SKM.

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 to the QSCD. The communication between those external components and the remote QSCD employs the Signature Activation Protocol (SAP). The QSCD's signature or seal creation process is started by the SSA, by calling the function and transmitting the necessary parameters. These include a signer identifier, a signertoken and the Signature Activation Data (SAD) to activate the corresponding signing key in the HSM. The SAD binds the necessary signature and authorization data together. It consists of the hash representation (DTBS/R) of the data to be signed, signerid, signerpass, signertoken as well as information on the signature algorithm. The SAD is encrypted with the public key of the SAM, to ensure their integrity and confidentiality.

The signertoken is the result of an authentication of the signer to level SCAL2 through a trusted third party acting as Identity Provider (IdP). The QSCD only supports delegated authentication and does therefore not directly authenticate a potential signer, but only validates the received assertion of an IdP confirming the successful authentication. The signertoken is therefore the second authentication factor, while the provided signerpass (a password) is the first authentication factor. The signertoken ensures also that the SAD is only used for the particular transaction, since it is bound to the SAD and cannot be used for another transaction.

The SAM verifies the authenticity of the received request and then decrypts the SAD with its private key. Before the actual signature request is sent to the HSM, further checks of the included SAD and the origin of the data need to pass. In the positive case, the SAM loads the corresponding blob and keypass from the database, decrypts the keypass using the signerpass and provides these two items plus the DTBS/R to the HSM. The HSM decrypts the blob using the SMK and receives the SCD by decrypting it with the keypass. It then encrypts the received DTBS/R with the SCD, thus, creating the signature or seal. The seal or signature is then returned to the SSA and further to the calling

[2] EAL – Evaluation Assurance Level

application, usually the Signature Creation Application (SCA), where it is attached to the data to be signed.

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

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.

---

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

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

[5] *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.*

[6] *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.*

[7] *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.*

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

[9] *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.*

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

[11] *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.*

[12] *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.

(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[13] 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 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.

(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, key sizes and hash functions 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 high[14].

[13] in accordance with recital 56 of eIDAS

[14] 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-bits and 3072-bits or
- RSASSA-PSS according to PKCS#1 v2.2 (RFC 8017) with cryptographic key sizes of 2048-bits and 3072-bits

For the calculation of hash values, the hash functions 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:

- Thales Luna K7 Cryptographic Module, firmware version 7.7.0

For the used HSM the security target *Thales - Thales Luna K7 Cryptographic Module, Security Target*, Revision J, published on 2020-09-25, is available. The HSM was evaluated by TÜV Rheinland Nederland B.V. against this security target. The evaluation was performed according to Common Criteria version 3.1, revision 5 with assurance level EAL4, augmented with ALC_FLR.2[15] and AVA_VAN.5[16], and in conformance to the protection profile EN 419 221-5:2018: *Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services*. The certification report NSCIB-CC-195307-CR in conjunction with the certificate CC-20-195307 confirm a successful evaluation of the HSM against its security target. The certificate was published on 2020-10-06 and has a validity of five years, until 2025-10-06.

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-22-035.

Authorized Signature

A-SIT Secure Information Technology Center – Austria

Vienna, (Date see electronic signature)

	Signatory	Arne Tauber
	Date/Time-UTC	2022-07-29T11:55:26+02:00
	Verification	Information about the verification of the electronic signature can be found at: https://www.signaturpruefung.gv.at

Dr. Arne Tauber, Secretary General

[15] ALC_FLR.2 – Flaw reporting procedures
[16] AVA_VAN.5 – Advanced methodical vulnerability analysis