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

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) Safelayer's qualified remote electronic signature and seal creation device ("TrustedX eIDAS"), version 4.1.6.0

Applicant:
Safelayer Secure Communications S.A.
World Trade Center (S - 4), Moll de Barcelona s/n
08039 Barcelona
Spain

QSCD-Certificate issued on: 2018-10-29
Reference number: A-SIT-VIG-18-048

1. Product Description

Subcomponents:

Safelayer's qualified remote electronic signature and seal creation device ("TrustedX eIDAS") uses HSM devices as cryptographic modules for the generation and protection of the signature or seal creation data (SCD). The following HSM devices can be used for the QSCD:

- Thales nShield Connect/Connect+/Connect XC

The HSMs are operated according to their FIPS 140-2 level 3 certification in conjunction with the corresponding security policies. Furthermore, the QSCD uses a Server Signing Application (SSA) to communicate with the HSM and to handle the signature and seal creation process. 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. For its services, the QSCD also uses other components such as external identity providers or applications. These, however, are not part of the QSCD and thus not in the scope of this certification.

[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

Generation of signature and seal creation data:

Upon registration of a user, the corresponding private signing key pair is generated inside the HSM. During this process the user also defines a private secret, which is later used to authorize signature or seal creation requests. In detail this secret is used to access a logical token on the HSM, which is associated to the corresponding SCD of the user. A certificate request (CSR) is generated using the created key pair and sent to an external qualified TSP to obtain a X.509 certificate that is bound to the SCD.

Storage of signature and seal creation data:

The SCD is securely stored outside the HSM in a database, which is connected to the TrustedX eIDAS – SSA module. The SCD never leaves the HSM unencrypted; it is always encrypted using the HSM hardware key and therefore only readable by the HSM.

Signature and Seal Creation:

A user can only request a signature or seal creation via trusted external applications (through the SSA) and not through the QSCD directly. The communication between those external components and the remote QSCD employs the Signature Activation Protocol (SAP). An application forwards a signature or seal request to the QSCD, along with the data to be signed or sealed. The identity provider and authentication components of TrustedX eIDAS subsequently authenticate the user by means of a two-factor authentication method. Upon a successful authentication, another component of TrustedX eIDAS calculates the hash representation (DTBS/R[2]) of the data. The data to be signed or sealed along with the DTBS/R and signing key identifier are shown to the user. The user is then able to give a final consent, based on the received information, by providing the secret which has been defined in the registration process. This secret is only shared between the user and the HSM. Finally the QSCD initiates the actual signature or seal generation by letting the HSM encrypt the DTBS/R. For that, the encrypted signing key is loaded from the database into the HSM, and the HSM generates the signature or seal with it. The signed or sealed data is then returned to the requesting application.

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])

[2] DTBS/R – Data To Be Signed Representation

[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.*

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 an ongoing 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.

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 and 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

[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.*

[13] in accordance with recital 56 of eIDAS

- 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 and 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 in FIPS 140-2 level 3 mode.

(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[14].

5. Algorithms and Corresponding Parameters

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

- RSASSA-PKCS1-v1_5 or RSASSA-PSS according to PKCS#1 v2.2 (RFC 8017) with cryptographic key sizes of 2048-bit or 4096-bit
- DSA according to FIPS PUB 186-4 with cryptographic key sizes of 2048-bit or 3072-bit
- ECDSA using the curves P-256, P-384 and P-521 according to FIPS PUB 186-4 with cryptographic key sizes of 256-bit to 512-bit

For the calculation of hash values the algorithms SHA256, SHA384 and SHA512 according to FIPS 180-4 are supported.

6. Assurance Level and Strength of Mechanism

The QSCD supports the following HSM types:

- Thales nShield Connect and Connect +, Firmware: 2.55.1, 2.61.2
- Thales nShield Connect XC, Firmware: 3.4.1, 3.4.2

For the Thales nShield HSMs under firmware 2.55.1, 2.61.2, 3.4.1 and 3.4.2 the following NIST FIPS 140-2 certificates apply:

- FIPS Validation Certificate No. 1742[15] - issued on 2012-06-25 and last updated on 2015-11-16 by the US (National Institute of Standards and Technology) and the Canadian

[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

[15] Cf. https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/1742

(Communications Security Establishment) FIPS 140-2 certification body; for Thales – nShield Solo or nShield Connect, firmware versions 2.50.16, 2.51.10, 2.50.35 and 2.55.1

- FIPS Validation Certificate No. 2148[16] - issued on 2014-05-13 and last updated on 2015-11-24 by the US (National Institute of Standards and Technology) and the Canadian (Communications Security Establishment) FIPS 140-2 certification body; for Thales – nShield Solo+ or nShield Connect+, firmware versions 2.51.10 and 2.55.1
- FIPS Validation Certificate No. 2640[17] - issued on 2016-05-13 by the US (National Institute of Standards and Technology) and the Canadian (Communications Security Establishment) FIPS 140-2 certification body; for Thales – nShield Solo or nShield Connect, firmware version 2.61.2
- FIPS Validation Certificate No. 2644[18] - issued on 2016-05-13 and last updated on 2018-08-17 by the US (National Institute of Standards and Technology) and the Canadian (Communications Security Establishment) FIPS 140-2 certification body; for Thales – nShield Solo+ or nShield Connect+, firmware version 2.61.2
- FIPS Validation Certificate No. 2941[19] - issued on 2017-06-23 and last updated on 2018-08-07 by the US (National Institute of Standards and Technology) and the Canadian (Communications Security Establishment) FIPS 140-2 certification body; for Thales – nShield Solo XC or nShield Connect XC, firmware versions 3.3.21, 3.4.1 and 3.4.2

The certificates confirm that the HSMs were successfully evaluated against FIPS 140-2 level 3.

In addition, the certificate No. 1/16[20] – issued on 2016-03-10 by the Italian Common Criteria certification body OCSI[21] – provides extra assurance for the used HSM Thales nShield Connect/Connect+ with firmware version 2.55.1. The certificate confirms that the respective HSM was successfully evaluated against Common Criteria version 3.1., Evaluation Assurance Level EAL4+ augmented with 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 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-18-048.

Authorized Signature:

A-SIT Secure Information Technology Center – Austria

Vienna, (Date see electronic signature)

SIGNATURE INFORMATION	**Signatory**	Reinhard Posch
	Date/Time-UTC	2018-10-28T15:42:16+01:00
	Verification	Information about the verification of the electronic signature can be found at: https://www.signaturpruefung.gv.at
Note	This document is signed with a qualified electronic signature. According to Art. 25 para. 2 of the Regulation (EU) No 910/2014 of 23. July 2014 ("eIDAS-Regulation") it shall have the equivalent legal effect of a handwritten signature.	

Prof. DI Dr. Reinhard Posch, Director

[16] Cf. https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/2148

[17] Cf. https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/2640

[18] Cf. https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/2644

[19] Cf. https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/2941

[20] Cf. http://www.ocsi.isticom.it/documenti/certificazioni/thales/rc_thales_nshield_v1.0.pdf

[21] OCSI – Organismo di Certificazione della Sicurezza Informatica

[22] AVA_VAN.5 – Advanced methodical vulnerability analysis