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) LuxTrust's Qualified Remote Signature and Seal Creation Device, version 1.0

Applicant:
LuxTrust S.A.,
IVY Building, 13-15 Parc d'activités,
L-8308 Capellen, Luxembourg

QSCD-Certificate issued on: 2017-12-14
Reference number: A-SIT-VIG-17-060

1. Product Description

Subcomponents:

LuxTrust's qualified remote signature and seal creation device uses HSM devices (Thales nShield Solo/Solo+ or nShield Connect/Connect+[2]) as cryptographic modules for the generation and protection of the signature resp. seal creation data (SCD). The HSMs are operated according to their Common Criteria EAL4+ certification[3] and provide a secure mechanism for storing private keys outside the HSMs in a database. The Signature Activation Module (SAM) is a software module (part of Cryptomathic Signer, version 4.7[4]) to ensure that users (i.e. signatories or creators of a seal) retain control of their signing keys. The SAM is loaded onto the HSMs as a local application. The QSCD is intended to be operated by the qualified trust service provider LuxTrust in a secure operational environment as part of a remote electronic signature service.

Generation of signature and seal creation data (SCD):

A newly created user (i.e. signatory or creator of a seal) does not hold any privileges or SCD. The user must be at first assigned a privilege which allows her to be allocated a SCD/SVD key pair with specific properties. The SCD/SVD key pair is always generated within the HSM and access to the

[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] Manufacturer: Thales e–Security Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324, USA: nCore firmware version 2.55.1, nShield Connect firmware image version 0.9.9
[3] http://www.ocsi.isticom.it/documenti/certificazioni/thales/rc_thales_nshield_v1.0.pdf
[4] Manufacturer: Cryptomathic A/S, Jaegergardsgade 118, DK-8000 Aarhus C, Denmark

private key is controlled by the SAM. When a key pair has been generated, a certificate request is created and signed by the HSM and subsequently submitted to the certification application of a qualified TSP[5]. The SAM binds the resulting certificate to the SCD.

Storage of signature and seal creation data:

SCD is stored confidentially and integrity protected in an external encrypted key store residing in a database. In this context SCD is protected by an HSM key such that it can only be used within the HSM.

Signature and seal creation:

A Signature Creation Application (SCA) submits the DTBS/R(s)[6] to the QSCD. To activate SCD for signature or seal creation, the user is always authenticated via strong authentication[7] means. This can be performed by either delegating authentication to an external identity provider or by using one of the currently integrated mechanisms such as a static password and a dynamic one-time password (OTP), whereby the OTP validation can either be time-based (SMS, VASCO GO6 token) or context-based (VASCO DIGIPASS Token, aka. VTS – Virtual Transaction Signing). In case of a successful verification of all the authentication parameters, the signature resp. seal is created within the HSM, it is possible to sign or seal several DTBS/Rs within an authenticated session. Upon completion of the sign resp. seal operation the SCD is destroyed inside the HSM.

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 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])

[5] The processes of identification, registration and certificate issuance are outside the scope of this certificate
[6] Data to be Signed/Sealed Representation
[7] i.e. meeting the authentication requirements for SCAL2 as defined in EN 419 241-1
[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.*

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

- components and procedures for the generation of signature resp. seal creation data,
- components and procedures for the storage of signature resp. seal creation data,
- components and procedures for the processing of signature resp. 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 resp. 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 resp. 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 resp. to be sealed during transmission from the signatory resp. 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 resp. creators of a seal are informed that components used for the initiation of the signature resp. sealing process (e.g. OTP device, mobile phone, web browser) must be suitable protected. The users shall keep control of their assigned devices and shall promptly report any circumstance where a 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;

---

[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.*

[18] in accordance with recital 56 of eIDAS

(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 resp. seal creation data may be duplicated for back-up purposes only to the extent strictly necessary to ensure continuity of the service.

5. Algorithms and Corresponding Parameters

For the creation of qualified electronic signatures resp. qualified electronic seals the QSCD uses the cryptographic algorithm

- RSASSA-PSS according to PKCS#1 v2.2 (RFC 8017) with cryptographic key sizes from 2048 bit to 4096 bit.

For the calculation of hash values the algorithms SHA256, SHA384, SHA512 are supported[19].

6. Assurance Level and Strength of Mechanism

For the used HSMs (Thales nShield Solo/Solo+ or nShield Connect/Connect+, firmware version 2.55.1) the certificate No. 1/16 – issued on 2016-03-10 by the Italian Common Criteria certification body OCSI applies. The certificate confirms that the resp. HSM was successfully evaluated against Common Criteria version 3.1., Evaluation Assurance Level EAL4+ augmented with AVA_VAN.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 state of the art.

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-17-060.

Authorized Signature:

A-SIT Secure Information Technology Center – Austria

Vienna, (Date see electronic signature)

SIGNATURE INFORMATION	**Signatory**	Reinhard Posch
	Date/Time-UTC	2017-12-14T17:14:32+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

[19] Hash value calculation is performed outside of the QSCD by the SCA.