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) Cryptomathic Signer, version 4.8

Applicant:
Cryptomathic A/S,
Jægergårdsgade 118,
8000 Aarhus C
Denmark

QSCD-Certificate issued on: 2018-07-03
Reference number: A-SIT-VIG-18-043

1. Product Description

Subcomponents:

The TOE is a qualified remote signature and seal creation device, which uses HSM devices (Thales nShield Connect/Connect+/Connect XC[2]) as cryptographic modules for the generation and protection of the signature resp. seal creation data (SCD). The HSMs are operated based on their certification either according to Common Criteria EAL4+[3] or in strict FIPS 140-2 level 3 mode in conjunction with the published security policies. The HSMs provide a secure protection mechanism "Security World" for storing private keys outside of the HSM in a database. The Signature Activation Module (SAM) is a software module to ensure that users (i.e. signatories or creators of a seal) retain control of their signing keys. It is loaded onto the HSMs as a local application. The whole QSCD is operated in a secure environment.

Generation of signature and seal creation data (SCD):

After registration through an identity provider a new user is created in the SAM. Only after receiving a privilege (i.e. ability to get a key under a certain policy), a SCD/SVD key pair is generated for the user within the HSM. Access to the private key is controlled by the SAM. After

[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, 2.61.2, 3.4.1, nShield Connect firmware image version 0.9.9 & 12.40.2
[3] Cf. http://www.ocsi.isticom.it/documenti/certificazioni/thales/rc_thales_nshield_v1.0.pdf

the key pair generation a certificate request, signed by the HSM, is sent to a trusted Certificate Authority (CA). The SAM binds the returned certificate to the SCD.

Storage of signature and seal creation data:

All signature and seal creation data is stored in a key store within a database, in which it is integrity protected and encrypted with the HSM hardware key. Hence the SCD can only be used within the HSM.

Signature and seal creation:

In order to use the created SCD, a signature or seal operation has to be started through an application (e.g. browser) on the client-side. The applications' underlying API (Signer User API) – acting as Signer Interaction Component (SIC) – is responsible for the communication with the Server Signing Application (SSA) on the server-side. After a signer user supplies a document to be signed or sealed, the SIC calculates its hash (DTBS/R). The DTBS/R together with the signer authentication and signing key identifier form the Signature Activation Data (SAD). The SAD is securely transmitted to the SSA using the Signature Activation Protocol (SAP). Relevant data to create a signature or seal is then forwarded from the SSA to the SAM. The SAM verifies the received SAD and creates signatures resp. seals by using an HSM for cryptographic operations.

Identification and Authentication:

A signer user must first be registered by a Registration Authority (RA). To access the application and the subsequent signing and seal creation service, the user also needs to login using the credentials defined in the registration process. Some or all authentication factors are verified by an external identity provider (IdP) that will issue a SAML Assertion. If all the credentials are verified by the IdP these must correspond to an authentication means equivalent to EC Implementing Regulation 2015/1502 for assurance level substantial or higher[4]. If only some of the credentials are verified by the IdP and these are not enough to correspond to an authentication means equivalent to EC Implementing Regulation 2015/1502 for assurance level substantial or higher, an additional factor is required to trigger the seal or signing operation. This factor may be one of the following supported token-types:

- OATH-TOTP
- OATH-HOTP
- SMS
- OATH-OCRA

The SAML assertion is send to the SAM, which verifies the assertion.

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 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])

[4] 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] *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.*

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[15] 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

---

[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.*

[15] in accordance with recital 56 of eIDAS

used for the initiation of the signature resp sealing process (OTP device, mobile phone, web browser) must be suitable 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 resp. 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.

5. Algorithms and Corresponding Parameters

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

- RSASSA-PKCS1-v1.5 or RSASSA-PSS according to PKCS#1 v2.2 (RFC 8017) and cryptographic key sizes of 2048-bit to 4096-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

Cryptomathic Signer supports the following HSM types:
- Thales nShield Connect , Firmware: 2.55.1, 2.61.2
- Thales nShield Connect +, Firmware: 2.55.1, 2.61.2
- Thales nShield Connect XC, Firmware: 3.4.1

For the used HSMs under firmware 2.55.1, the certificate No. 1/16[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[17].

[16] Cf. http://www.ocsi.isticom.it/documenti/certificazioni/thales/rc_thales_nshield_v1.0.pdf
[17] AVA_VAN.5 – Advanced methodical vulnerability analysis

For the HSMs under firmware 2.61.2 resp. 3.4.1 the following NIST FIPS 140-2 certificates apply:

- FIPS Validation Certificate No. 2640[18] - 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[19] - 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. 2941[20] - issued on 2017-06-23 and last updated on 2017-11-07 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 and 3.4.1

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

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-18-043.

Authorized Signature:

A-SIT Secure Information Technology Center – Austria

Vienna, (Date see electronic signature)

SIGNATURE INFORMATION	**Signatory**	Reinhard Posch
	Date/Time-UTC	2018-07-03T15:51:59+02:00
	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

[18] Cf. https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/2640
[19] Cf. https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/2644
[20] Cf. https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/2941