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) certSIGN's qualified remote electronic signature and seal creation device ("Paperless"), version 1.0

Applicant:
CERTSIGN S.A.,
Şos. Olteniţei Nr. 107A, bl. C1,
041303 Bucureşti - Sector 4,
Romania

QSCD-Certificate issued on: 2019-05-21
Reference number: A-SIT-VIG-18-067

1. Product Description

CertSIGN's qualified remote electronic signature and seal creation device ("Paperless") is a product for qualified electronic signatures and seals intended to be used as a remote Qualified Electronic Signature Creation Device (QSCD) in the secure operational environment of a qualified trust service provider (TSP).

Subcomponents:

Paperless 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. The Remote Signing Service component acts as Signature Activation Module (SAM) and allows users to retain exclusive control of their signing keys. It uses an SMS Gateway component to authenticate the signature or seal creation process. The Signing Service Application (SSA) is responsible for accepting signing requests by the SAM and forwarding them to the HSM. The last component is the CryptoService, which is responsible for handling requests for key generation and certificate signing.

[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

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. The QSCD also uses further components (e.g. certification authority, client application, etc.) to provide its services. These, however, are not part of the QSCD and thus not in the scope of this certification

Generation of Signature and Seal Creation Data:

On the first use of the QSCD by a user (signatory or creator of a seal), the corresponding SCD/SVD key pair is generated inside the HSM. Users only interact with the QSCD through trusted client applications (i.e. server applications), which use mutual authentication to consume the QSCD's services through a SOAP interface. This implementation is referred to by certSIGN as system-to-system. Access to the private key is controlled by the SAM. After SCD generation a certificate request (PKCS#10), signed by the HSM, is sent to a trusted Certificate Authority (CA). The returned certificate is bound to the SCD and stored within the SSA's application keystore. The process of issuing qualified certificates is outside the scope of this confirmation.

Storage of Signature and Seal Creation Data:

The SCD is securely stored within the HSM throughout its lifecycle in encrypted form. As soon as the SCD is out of use (e.g. user unregisters from the service) it is securely destroyed using the HSM's security functions.

Signature and Seal Creation:

Creating a signature or seal is only possible to users that are already registered to the service, i.e. already possess a private signing key inside the HSM. A user can then initiate a signature or seal creation process through an external client application (i.e. trusted server application), by passing on the data to be signed or sealed and the personal identification credentials. The client application calculates the hash of the data to be signed or sealed (DTBS/R) and forwards the request to the Remote Signing Service (SAM). After checking the received request and credentials the SAM starts the authentication by requiring the user's Signature Interaction Component (SIC) to authenticate itself using a client certificate. This PIN secured client certificate was issued by the certSIGN CA for the specific user in the course of enrolment. As second authentication factor the SAM utilizes the SMS Gateway to send the user a SMS message containing an OTP. The user sends the OTP over a secure channel through the client application to the SAM, in order to prove the possession of the mobile device and authorize the signature or seal creation process. After the SAM validates the received OTP, it forwards the request to the SSA, which uses the HSM to create the signature or seal. The signed or sealed data is then returned to the requesting client application, which includes the signature or seal into the DTBS.

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

[2] *Qualified electronic signature creation devices shall meet the requirements laid down in Annex II.*
[3] *Article 29 shall apply mutatis mutandis to requirements for qualified electronic seal creation devices.*
[4] *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*.

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[12] 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 (OTP device, mobile phone, web browser) must be

---

[5] *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.*

[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 cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology.*

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

[8] *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.*

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

[10] *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.*

[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 number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service.*

[12] in accordance with recital 56 of eIDAS

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 (QTSP).

(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 in FIPS 140-2 level 3 mode.

5. Algorithms and Corresponding Parameters

For the creation of qualified electronic signatures or qualified electronic seals the QSCD uses the cryptographic algorithm:

- RSASSA-PKCS1-v1_5 according to PKCS#1 v2.2 (IETF RFC 8017) with a cryptographic key size of 2048-bit.

For the calculation of hash values the algorithm SHA-256 according to FIPS 180-4 is supported.

6. Assurance Level and Strength of Mechanism

The QSCD 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, 3.4.2

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

- FIPS Validation Certificate No. 1742[13] - issued on 2012-06-25 and last updated on 2015-11-16 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 2.50.16, 2.51.10, 2.50.35 and 2.55.1
- FIPS Validation Certificate No. 2148[14] - issued on 2014-05-13 and last updated on 2015-11-24 by the US (National Institute of Standards and Technology) and the Canadian

[13] Cf. https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/1742
[14] Cf. https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/2148

(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[15] - 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[16] - 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[17] - 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[18] – issued on 2016-03-10 by the Italian Common Criteria certification body OCSI[19] – 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[20].

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-18-067.

Authorized Signature:

A-SIT Secure Information Technology Center – Austria

Vienna, (Date see electronic signature)

SIGNATURE INFORMATION	**Signatory**	Reinhard Posch
	Date/Time-UTC	2019-05-21T23:50:03+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

[15] Cf. https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/2640
[16] Cf. https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/2644
[17] Cf. https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/2941
[18] Cf. http://www.ocsi.isticom.it/documenti/certificazioni/thales/rc_thales_nshield_v1.0.pdf
[19] OCSI – Organismo di Certificazione della Sicurezza Informatica
[20] AVA_VAN.5 – Advanced methodical vulnerability analysis