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)
SafeNet Luna PCI-E HSM, version 7.0.3.

Applicant:
Gemalto Canada Inc,
20 Colonnade Road, Suite 200
Ottawa, Ontario K2E 7M6
Canada

QSCD-Certificate issued on: 2019-05-17
Reference number: A-SIT-VIG-18-068

1. Product Description

SafeNet Luna PCI-E HSM is a product for both qualified electronic signatures and seals intended to be used as a remote Qualified Electronic Signature resp. Seal Creation Device (QSCD) in the secure operational environment of a qualified trust service provider (QTSP). When used in combination with qualified certificates as well as a suitable Server Signing Application (SSA) and Signature Creation Application (SCA), SafeNet Luna PCI-E HSM generates (1) qualified electronic signatures resp. (2) qualified electronic seals as defined in eIDAS with the legal effects of (1) Article 25 resp. (2) Article 35.

<u>Subcomponents:</u>

The QSCD consists of the SafeNet Luna PCI-E HSM which may either be used as a standalone PCI-E card or as an embedded component in the SafeNet Luna Network HSM.

The HSM is responsible for storing all keys used for the creation of qualified electronic signatures and qualified electronic seals. The HSM hosts all cryptographic operations to establish an end-to-end secure tunnel between the QSCD and a remote SCA, this tunnel is required to use signature or seal creation data.

For the successful deployment of the HSM as a QSCD, the HSM must be integrated with at minimum a 3rd party signature creation application (SCA) and where required a server signing application (SSA). These components (SCA, SSA) are outside 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

Where external identity providers (IdP) are used these are expected to interface to either the SCA or the SSA and as such are not considered further.

Generation of Signature and Seal Creation Data:

The Signature or Seal Creation Data (SCD) is generated and stored within the HSM.

Where long-term signing keys are used, the signatory or creator of a seal must be in control of the partition on the HSM used to store the key ahead of the generation request being issued. This is achieved by the signatory or creator of a seal initializing the login credentials for the target partition ahead of its use.

Where single use signing keys are being used, a single partition may be used to host multiple concurrent sessions used by independent users but all key objects must be ‘session keys’ whereby they are assigned and available to an individual session only and never stored as token based objects on the HSM.

Following generation of SCD, the corresponding public key is extracted from the HSM to support creation of a qualified certificate. Creation of the Certificate Singing Request (CSR) alongside the resulting Qualified Certificate is out of scope of the certification.

Storage of Signature and Seal Creation Data:

Where token based keys are used, SCD is stored with its confidentiality and integrity protected long-term by the HSM. In this context, the SCD is protected by a combination of HSM and end-user keys in a way that

(i) the keys can only be used inside the HSM;

(ii) the keys can only be used following a login to the target partition by the signatory or creator of a seal owning the SCD.

(iii) integrity protection for the keys is provided by the HSM throughout their life.

Where session based keys are used, SCD is only stored by the HSM in volatile memory and is securely overwritten on power-cycle or reset of the HSM or on active close of the associated session.

Signature and Seal Creation:

The HSM enforces a model for session based controls on access and authorization to access and use SCD. Ahead of using SCD, the signatory or creator of a seal must successfully authenticate to the target partition changing the authentication state of the target session to authenticated. Once authenticated, either Data To Be Signed (DTBS) or DTBS/representation (DTBS/r) is sent to the HSM for signing. Once the signature is received, the session is closed.

Where single use key model is deployed, SCD creation and public key extraction alongside signature or seal creation must occur within a single session.

All sessions with active partitions must be performed using the QSCD supplied cryptographic tunnel identified as ‘secure trusted channel’ which provides an additional layer of authentication of the remote client on the one hand and on the other hand confidentiality, integrity and replay protection for traffic during the signature or seal creation request.

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,

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

- 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])

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

[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.*

[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.*

QSCD's system environment[12] 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 must be suitably protected.

(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) 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.

(5) The HSM must be initialised and operated in FIPS 140-2 level 3 mode.

(6) Only those cryptographic algorithms and key sizes listed in section 5 shall be used for the creation of qualified electronic signatures or qualified electronic seals.

(7) External authentication mechanisms, where used with a 3rd party developed SCA or SSA to authenticate the signatory in order to create a qualified signature or seal, shall correspond to an authentication means equivalent to EC Implementing Regulation 2015/1502 for assurance level substantial or higher[13].

(8) Where the HSM is used to replace the cryptographic module in an already approved QSCD for a Remote Server Signing solution including an alternative Signature Activation Module (SAM), requirements to use the client to HSM provided secure tunnel can be relaxed.

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 (IETF RFC 8017) or ANSI X9.31 as per FIPS PUB 186-4 with cryptographic key sizes of 2048-bit, 3072-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 alongside brainpool_p256r1, brainpool_p384r1, brainpool_p512r1 as per RFC 5639 with cryptographic key sizes from 256-bit to 512-bit

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

[12] in accordance with recital 56 of eIDAS

[13] 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

6. Assurance Level and Strength of Mechanism

For the HSMs the following NIST FIPS 140-2 Validation Certificates apply:

- FIPS Validation Certificate No. 3182[14]; for Gemalto – SafeNet Luna K7+ Cryptographic Module, Hardware Versions: 808-000069-001 (when standalone PCI-E card), 808-000070-001 (when integrated as a component of SafeNet Luna Network HSM), Firmware: 7.0.3 with Bootloader version 1.1.2.
- FIPS Validation Certificate No. 3205[15]; for Gemalto – SafeNet Luna K7 Cryptographic Module, Hardware Versions: 808-000048-002 (when standalone PCI-E card), 808-000066-001 and 808-000073-001 (when integrated as component of SafeNet Luna Network HSM), Firmware: 7.0.3 with Bootloader version 1.1.1 or 1.1.2.

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-18-068.

Authorized Signature:

A-SIT Secure Information Technology Center – Austria

Vienna, (Date see electronic signature)

SIGNATURE INFORMATION	**Signatory**	Reinhard Posch
	Date/Time-UTC	2019-05-17T15:26:56+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

[14] Cf. https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3182

[15] Cf. https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3205