Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

1030 Wien, Seidlgasse 22 / 9
Tel.: +43 1 503 19 63-0
Fax: +43 1 503 19 63-66

8010 Graz, Inffeldgasse 16a
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 Fix pack 8, Update 1

Applicant:
Cryptomathic A/S
Aaboulevarden 22, 2.
8000 Aarhus C
Denmark

Reference number: A-SIT-VIG-25-033

QSCD-Certificate valid from:
See Date of Qualified Electronic Signature

1. Product Description

The hereby certified product "Cryptomathic Signer, version 4.8 Fix pack 8, Update 1" (also denoted as Cryptomathic Signer or Target of Evaluation - TOE) is a Qualified Remote Signature and Seal Creation Device (QSCD). When used in conjunction with qualified certificates as well as a suitable Server Signing Application (SSA) and a Signer Interaction Component (SIC) either (1) qualified electronic signatures or (2) qualified electronic seals as defined in eIDAS[Fehler! Textmarke nicht definiert.] with the legal effects of (1) Article 25 or (2) Article 35 are created.

<u>Subcomponents:</u>

The TOE uses a Hardware Security Module (HSM) device[2] (nShield Connect XC) as a cryptographic module for the generation and for the protection of the signature or seal creation data (SCD). The HSM is operated based on its NIST FIPS 140-2 certification with the exception of a transfer of the existing security world. The used HSM provides a secure protection mechanism which is denoted as "Security World" for storing private keys outside of the HSM in a database.

[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 amended by Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024

[2] The certified hardware and firmware versions of the used cryptographic modules, for which this QSCD certificate is valid, are given in Section 6.

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 tamper-protected HSM as a local application.

Both (HSM and SAM) together form the QSCD and are operated in the protected environment of a Qualified Trust Service Provider (QTSP).

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., the ability to get a key under a certain applicable policy), a SCD/SVD key pair is generated for the user inside of the HSM. Access to the private key is controlled by the SAM. After 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 are stored in a key store inside of a database, in which it is integrity protected and encrypted with the HSM hardware key. Hence the SCD can only be used inside of the HSM after successful authentication.

Signature and seal creation:

In order to use the created SCD, a signature or seal operation has to be initialized through an application (e.g., using a web-browser) on the client-side. The applications' underlying API[3] (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)[4,5]. 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 or seals by using an HSM for cryptographic operations.

Identification and Authentication:

A signatory or a creator of a seal must first be registered by a Registration Authority (RA). To access the application and the subsequent signing and seal creation service, the signatory or the creator of a seal 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[6] 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[7]. 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 of authentication is required to trigger the seal or signing operation. This factor may be one of the following supported token-types:

- OATH[8]-TOTP[9]
- OATH-HOTP[10]

[3] API – Application Programming Interface

[4] DTBS – Data To Be Signed

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

[6] SAML – Security Assertion Markup Language

[7] 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

[8] OATH – Open AuTHentication

[9] TOTP – Time-based one-time Password

[10] HOTP – HMAC-based one-time Password (HMAC – Hash-based Message Authentication Code)

- SMS[11]
- OATH-OCRA[12]

The SAML assertion is sent 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[13] eIDAS,
- requirements laid down in Article 39 para 1[14] eIDAS,
- requirements laid down in Annex II eIDAS (para 1 lit. a[15],b[16],c[17],d[18], para 2[19], para 3[20], para 4 lit a[21], b[22])

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 5 years or up to a preceding revocation by A-SIT.

On assignment A-SIT will conduct a continuous 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.

[11] SMS – Short Message Service

[12] OCRA – OATH Challenge-Response Algorithm

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

[14] *Article 29 shall apply mutatis mutandis to requirements for qualified electronic seal creation devices.*

[15] *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*.

[16] *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.*

[17] *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.*

[18] *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.*

[19] *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.*

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

[21] *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.*

[22] *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.*

In order to maintain a valid certification, the applicant has to conduct a vulnerability assessment every two years and remedy any identified vulnerabilities in a timely manner. 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, if vulnerability assessments are not conducted every two years, if identified vulnerabilities are not remedied in a timely manner 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 (in accordance with Article 20 eIDAS).

(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[23] 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[24] 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
- 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) Only those cryptographic algorithms, key sizes and hash functions listed in section five shall be used for the creation of qualified electronic signatures or qualified electronic seals.

(7) The HSM must be operated based on its certification according to FIPS 140-2 with the exception of a transfer of the existing security world.

(8) If all authentication factors that are used to authenticate a user in order to create a qualified electronic signature or seal are verified by an external identity provider (IdP), these authentication

[23] in accordance with recital 56 of eIDAS

[24] OTP – One-time Password

mechanisms shall correspond to an authentication means equivalent to EC Implementing Regulation 2015/1502 for assurance level substantial or higher[25].

(9) It must be ensured that components of signatories (or creators of a seal), which have vulnerabilities or are otherwise not suitable for authentication, cannot be used to authorize a signature creation.

(10) The qualified trust service provider operating the QSCD must ensure that RSA keys with a key size lower than 3000-bit cannot be used for the creation of qualified electronic signatures or qualified electronic seals after 31.12.2025.

(11) Qualified trust service providers issuing qualified certificates based on keys generated by the QSCD must ensure that qualified certificates based on RSA keys with a key size lower than 3000-bit are not valid beyond 31.12.2025.

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 or RSASSA-PSS according to PKCS#1 v2.2 (RFC 8017) and cryptographic key size of 2048-bit until 31.12.2025 at the latest.
- RSASSA-PKCS1-v1.5 or RSASSA-PSS according to PKCS#1 v2.2 (RFC 8017) and cryptographic key sizes of 3072-bit or 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

For the used nShield HSM the following NIST FIPS 140-2 validation certificate issued by the US (National Institute of Standards and Technology) and the Canadian (Communications Security Establishment) FIPS 140-2 certification body applies. The certificate confirms that the HSM was successfully evaluated against FIPS 140-2 level 2:

- FIPS Validation Certificate No. 4334[26] - issued on 2022-10-16 and last updated on 2024-06-18; for Entrust – nShield Solo XC F3 for nShield Connect XC and for nShield HSMi,
  Firmware versions: 12.72.1, 12.72.3
  Hardware versions: nC4035E-000 and nC4335N-000, Build Standard A

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-25-033.

[25] 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

[26] cf., https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4334

Authorized Signature:

A-SIT Secure Information Technology Center – Austria

Vienna, (Date see electronic signature)

SIGNATURE INFORMATION	**Signatory**	Herbert Leitold
	Date/Time-UTC	2025-03-05T21:55:56+01:00
	Verification	Information about the verification of the electronic signature can be found at: https://www.signaturpruefung.gv.at

Herbert Leitold, Director