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

A-SIT

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) "Certilia eSign", version 1.0

Applicant:
AKD d.o.o.
Savska cesta 31
HR-10000 Zagreb,
Croatia

Reference number: A-SIT-VIG-24-049

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

1. Product Description

The herein certified product *AKD's qualified remote electronic signature and seal creation device "Certilia eSign"*, version 1.0 developed and operated by AKD d.o.o., is a Qualified Remote Signature/Seal Creation Device (QSCD). It offers users a remote functionality for electronic signature and electronic seal creation, where none of its components are in the users unprotected environment but deployed in the tamper-protected environment of the qualified Trust Service Provider (QTSP) AKD d.o.o., while still ensuring the users sole control over their signing keys. To achieve this remote functionality, the QSCD implements a Trustworthy System Supporting Server Signing (TW4S) in accordance with CEN EN 419 241-1.

Subcomponents:
The QSCD consists of two separate components: The Signature Activation Module (SAM) and a Hardware Security Module (HSM).

The SAM is a software component that conforms to the CEN EN 419 241-1 standard and manages the signing key activation within the HSM. It is the only components to communicate directly with the HSM in order to validate an incoming request and initiate the signature or seal creation process

[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

within the HSM. To this end it implements the Signature Activation Protocol (SAP), thereby ensuring the sole control principle for the respective signing keys.

The HSM is a tamper-proof hardware component for the secure execution of cryptographic operations, especially the generation, usage and protection of the Signature and Seal Creation Data (SCD). It serves as a Cryptographic Module (CM) as defined in CEN EN 419 241-2 and also conforms to the protection profile CEN EN 419 221-5. Only the HSM device family "Entrust nShield Solo XC"[2] is used for the QSCD[3]. HSMs are operated according to their Common Criteria EAL4+[4] certification in conjunction with the corresponding security target.

These two components, the SAM and the HSM, together form the QSCD, which is intended to be operated by the qualified trust service provider AKD d.o.o. in a secure operational environment as part of a remote electronic signature and seal creation service. To fully provide its services, the QSCD relies on additional components, such as a Server Signing Application (SSA), Identity Provider (IdP) or Certificate Authorities (CA). These, however, are not part of the QSCD and are thus not in the scope of this certification.

Generation of Signature and Seal Creation Data:

SCD is generated by the HSM using the configured key algorithms and parameters and only as a result of a valid incoming key pair request during the signer enrolment process. The request consists of Signature Activation Data (SAD), which combines the required information, such as a derived password key for SCD activation. This request is forwarded to the QSCD, if it came from an already identified and authenticated user (requires SCAL2[5]). In the course of this process a certificate for the generated signing keys is also issued by the connected CA. Pre-generation of SCD, where the generated keys are pre-computed, stacked and later assigned in the course of an incoming request, is not supported.

Storage of Signature and Seal Creation Data:

The HSM provides a secure protection mechanism integrated into its "Security World" software for protecting the SCD. Once the SCD/SVD[6] key pair is generated in the course of signer enrolment, the SCD is encrypted using the HSM's non-exportable hardware key and stored in the SSA database, along with additional related signer data. The password provided during key pair generation is also assigned to the SCD and is required for any SCD usage. The SCD never leaves the HSM in unencrypted form and can only be processed by an HSM in possession of the corresponding hardware key. Access to the SCD is controlled by the SAM, thus SCD can only be used by the combination of SAM and HSM.

Signature and Seal Creation:

After the successful enrolment and key generation, a signer can invoke a signature or seal operation using the Signer Interaction Component (SIC), by providing a document to the Signature Creation Application (SCA). The SIC can be a local device or third-party IT system, which logs the user in directly or through an external IdP. The SCA in turn calculates the hash representation (DTBS/R) of the document and presents the prepared document to the signer for review. The signer reviews the document and selects the certificate of a corresponding signing key and also provides the user password that was set during enrolment. At this point, the user has to be authenticated at assurance level SCAL 2, therefore, an IdP – either external or as part of the TSP – authenticates the signer to the required level and issues a signed confirmation of the successful authentication.

[2] nCipher Security Limited (an Entrust company) - One Station Square, Cambridge CB1 2GA, United Kingdom
[3] The certified hardware and firmware versions of the used cryptographic modules, for which this QSCD certificate is valid, are given in Section 6.
[4] EAL – Evaluation Assurance Level
[5] SCAL2 – Sole Control Assurance Level 2
[6] SVD – Signature Validation Data

The necessary signer data is transferred in the SAD using the SAP. Incoming requests are first handled by the SSA, which validates that the required authentication level has been reached as well as that the included signer data corresponds to the stored data from enrolment and then forwards the request to the SAM. The SAM is responsible for the validation of the SAD and invokes the activation of the signing keys as well as the signature or seal creation process in the HSM, if the provided SAD is valid (e.g. user password). The HSM finally signs the provided DTBS/R using the corresponding SCD to create the signature value. The generated signature value is then sent back to the SCA to create the final signed or sealed document.

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[7] eIDAS,
- requirements laid down in Article 39 para 1[8] eIDAS,
- requirements laid down in Annex II eIDAS (para 1 lit. a[9],b[10],c[11],d[12], para 2[13], para 3[14], para 4 lit a[15], b[16])

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.

---

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

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

[9] *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*.

[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 practically occur only once.*

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

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

[13] *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.*

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

[15] *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.*

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

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. 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[17] 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 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 the qualified trust service provider AKD d.o.o.

(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 according to their Common Criteria EAL4+ certification.

(7) 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.

[17] in accordance with recital 56 of eIDAS

(8) External authentication mechanisms, which are used to authenticate a user in order to create a qualified electronic signature or seal, shall correspond to an authentication means equivalent to EC Implementing Regulation 2015/1502 for assurance level substantial or high[18].

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

5. Algorithms and Corresponding Parameters

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

- ECDSA using the curves P-384 and P-521 of the NIST-family according to FIPS 186-4 with a cryptographic key size of 384-bit and 512-bit

For the calculation of hash values the hash functions SHA-384 and SHA-512 according to FIPS 180-4 are supported.

6. Assurance Level and Strength of Mechanism

For cryptographic operations and key management, the QSCD currently utilizes the following HSM type and firmware:

- Entrust nShield Solo XC product family[19], firmware: v12.60.15

The *Certification Report nShield Solo XC Hardware Security Module v12.60.15* in conjunction with the *Assurance Continuity Maintenance Report nShield Solo XC Hardware Security Module v12.60.15* by TÜV Rheinland confirm a successful evaluation of the HSM against its security target *Entrust - nShield Solo XC HSM Security Target*. The evaluation was performed according to Common Criteria version 3.1, revision 5 with assurance level EAL4 augmented with ALC_FLR.2 and AVA_VAN.5 and in conformance to the protection profile CEN EN 419 221-5.

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 current 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-24-049.

[18] 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

[19] nShield Solo XC F2, nShield Solo XC F3, nShield Solo XC for nShield Connect XC

Authorized Signature:

A-SIT Secure Information Technology Center – Austria

Vienna, (Date see electronic signature)

Signatory	Herbert Leitold
Date/Time-UTC	2025-02-19T12:41:22+01:00
Verification	Information about the verification of the electronic signature can be found at: https://www.signaturpruefung.gv.at

Herbert Leitold, Director