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

https://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) Monet+ ProID SAM for remote electronic signing and sealing, version 1.0, Update 1

Applicant:
Monet+ a.s.
Za Dvorem 505
763 14 Zlín-Štípa
Czech Republic

Reference number: A-SIT-VIG-21-092

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

1. Product Description

The product "Qualified Signature and Seal Creation Device (QSCD) Monet+ ProID SAM for remote electronic signing and sealing"[2] (abbreviated herein as ProID SAM, subsequently) by Monet+ a.s. is a remote Qualified Signature/Seal Creation Device (QSCD) to provide users (signatories or creators of seals) with a remote signing or sealing functionality. It is intended to be fully operated by a Trust Service Provider (TSP) in a secure operational environment, hence, no components of the QSCD have to be delivered to a user of the service. The QSCD manages the users' Signature or Seal Creation Data (SCD), but ensures the users' sole control over their SCD. When used in combination with qualified certificates, ProID SAM generates qualified electronic signatures and seals as defined in Regulation (EU) No. 910/2014 (eIDAS) with the legal effects defined therein.

Subcomponents:

The QSCD implements a "Trustworthy System Supporting Server Signing" (TW4S) in accordance with EN 419 241-1 and therefore consists of the two components (1) Signature Activation Module (SAM) and (2) Hardware Security Module (HSM).

[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] cf., monetplus.com/remote-sign

The SAM is a software component which is independent of the HSM. It is, however, connected to the HSM and controls the activation of both the SCD and the creation of digital signatures within the HSM. In order to verify incoming signature or seal creation requests, it implements one endpoint of the Signature Activation Protocol (SAP), which delivers the necessary Signature Activation Data (SAD).

The HSM is a tamper-proof hardware component for the secure execution of cryptographic operations. As part of the QSCD, it provides a Cryptographic Module in order to generate and protect the SCD as well as to create the digital signature value for electronic signatures or seals. For the used HSM component, the QSCD currently only supports devices of the Entrust[3] nShield Solo XC product family[4] with firmware v12.60.15[5]. These HSMs are operated according to their Common Criteria EAL4+[6] certification in conjunction with the corresponding security target.

Only these two components, the SAM and HSM, together form the QSCD and therefore the certified area. Other necessary components (e.g., Identity Provider) and processes (e.g., certification process) to provide the signing and sealing services are not part of the assessment and are thus not in the scope of this certification.

Generation of Signature and Seal Creation Data:

For performance reasons the QSCD generates key pairs on stock, without assigning them to a user or activating them. They are generated by the certified HSM in the amount set by thresholds in the configuration file. These pre-generated key pairs are finally assigned during a *key pair generation* operation. The Server Signing Application (SSA) initiates the corresponding function of the QSCD and also forwards an Access Token, as proof of the signer's authorization. It receives this Access Token by a trusted Authorization Server (AS) that the QSCD utilizes for delegated authentication. This authentication through a trusted third-party follows the OAuth concept and requires the AS to conduct an authentication of at least SCAL2[7]. The SAM validates the received request and orders the HSM to assign a pre-generated SCD/SVD[8] key pair to the signing identity.

As a final step, the HSM signs a Certificate Signing Request (CSR) for the SVD, which the QSCD sends to a trusted Public Key Infrastructure (PKI) in order to issue a qualified certificate. The QSCD then also binds this certificate to the signing identity. The process of issuing qualified certificates is outside the scope of this confirmation.

Storage of Signature and Seal Creation Data:

The HSM provides a secure storage mechanism integrated into its "Security World" software for protecting the private keys. Such keys are not stored in the HSM's internal memory anymore, but encrypted by the HSM's hardware key and then saved as key blob along with their security attributes to the QSCD's internal database. The reason for this approach is to increase the available key storage, without lowering the security of the stored assets.

After their generation inside the HSM, the pre-generated key pairs are directly saved to the database, in the form of an encrypted key-blob. Therefore, the SCD neither leaves the HSM unencrypted nor unprotected by the SAM. This way, the SCD can only be used in combination with the SAM and an HSM in possession of the correct hardware key.

[3] nCipher Security Limited (an Entrust company) - One Station Square, Cambridge CB1 2GA, United Kingdom
[4] nShield Solo XC F2 (nC3025E-000 rev 06), nShield Solo XC F3 (nC4035E-000 rev 06), nShield Solo XC for nShield Connect XC (nC4335N-000 rev 06)
[5] The certified hardware and firmware versions of the used cryptographic modules for which this QSCD certificate is valid are given in Section 6.
[6] EAL – Evaluation Assurance Level
[7] SCAL2 – Sole Control Assurance Level 2
[8] SVD – Signature Validation Data

Signature and Seal Creation:

To request the creation of a signature or seal, a signer or the creator of the seal only interacts with a user device and not directly with the QSCD. This user device has a Signer Interaction Component (SIC), which communicates through interfaces with the Server Signing Application (SSA) in the remote environment. The SSA then again handles the communication with the QSCD, more precisely with the SAM. The process of signature or seal creation is implemented in the Signature Activation Protocol (SAP), which ensures the secure transfer of the SAD to the SAM. The QSCD enables the usage of SCD only for the legitimate signer it belongs to. Therefore, the SAM – as endpoint of the SAP – has the final decision on whether to activate the SCD or not. The decision is based on the validation of the received SAD.

After a signer selects one or more documents to be signed or sealed, the Signature Creation Application (SCA) calculates the hash representation (DTBS/R)[9]. SAD is only valid for a particular transaction, authorizing the signing of a specific DTBS/R or a set of them with a specific signing key (SCD). For ProID SAM the authorization is done indirectly by a trusted Authorization Server (AS). The AS is a component defined in the OAuth framework (RFC[10] 6749) and is responsible for the authentication of signers and their authorization of the particular operation. The authentication procedures are required to reach an assurance level of SCAL2 according to EN 419 241-1 for qualified signatures. After verifying the signer's authentication factors, the AS issues an Access Token, which is in the form of a JSON[11] Web Token (JWT) with the SAD as payload. It is further signed by the AS using JSON Web Signature (JWS), for the SAM to verify its authenticity.

The SIC receives the Access Token – including the SAD – back from the AS and sends it to the SAM as a signature creation request. The SAM verifies the token's signature and expiration date as well as the SAD within. If they are valid, it authorizes the signature or seal creation by activating the corresponding SCD and loading the key blob from the database into the HSM.

In order to receive the plain SCD and be able to use it, the HSM decrypts the key-blob with its hardware key. The HSM then creates the digital signature value by encrypting the DTBS/R with the SCD and returns it back to the SCA. After each signature or seal creation operation, the SCD is removed again from the HSM. The SCA then creates the signed document using the digital signature value it received from the QSCD.

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[12] eIDAS,
- requirements laid down in Article 39 para 1[13] eIDAS,

[9] DTBS/R – Data to be signed / representation
[10] RFC – Request for Comments
[11] JSON – JavaScript Object Notation
[12] *Qualified electronic signature creation devices shall meet the requirements laid down in Annex II.*
[13] *Article 29 shall apply mutatis mutandis to requirements for qualified electronic seal creation devices.*

- requirements laid down in Annex II eIDAS (para 1 lit. a[14],b[15],c[16],d[17], para 2[18], para 3[19], para 4 lit a[20], b[21])

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 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. 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

---

14 *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.*

15 *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.*

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

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

18 *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.*

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

20 *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.*

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

QSCD's system environment[22] 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 (one-time password (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 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) The HSMs must be initialised and operated according to their Common Criteria EAL4+ certification.

(5) During HSM initialisation a quorum of at least two has to be defined for the HSM's Administrator Card Set (ACS) and the generated smartcards have to be controlled by different persons to ensure the principle of dual control.

(6) 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.

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

(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 higher[23].

(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 or seal creation.

5. Algorithms and Corresponding Parameters

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

- RSASSA[24]-PSS[25] according to PKCS#1 v2.2 (IETF RFC 8017) with cryptographic key sizes of 3072-bit or 4096-bit

[22] in accordance with recital 56 of eIDAS
[23] 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
[24] RSASSA – Rivest Shamir Adleman Server Signing Application
[25] PSS – Probabilistic Signature Scheme

- ECDSA[26] using the curves P-256, P-384 and P-521 of the NIST family according to FIPS PUB 186-4 with cryptographic key sizes of 256-bit to 512-bit.

For the calculation of hash values the following algorithms are supported[27]:

- RSASSA-PSS: SHA[28]-256, SHA-384, and SHA-512 according to FIPS PUB 180-4 and ISO/IEC 10118-3
- ECDSA: SHA-256, SHA-384, and SHA-512 according to FIPS PUB 180-4 and ISO/IEC 10118-3 and SHA3-256, SHA3-384, and SHA3-512 according to FIPS PUB 202

6. Assurance Level and Strength of Mechanism

The QSCD utilizes an HSM as cryptographic module according to EN 419 241-1. Only the following type and firmware are supported:

- Entrust nShield Solo XC product family[29], firmware v12.60.15

For this type family and firmware, 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[30] augmented with AVA_VAN.5[31] and ALC_FLR.2[32] and in conformance to the protection profile 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-21-092.

Authorized Signature

A-SIT Secure Information Technology Center – Austria

Vienna, (Date see electronic signature)

SIGNATURE INFORMATION	**Signatory**	Herbert Leitold
	Date/Time-UTC	2023-01-27T14:53:28+01:00
	Verification	Information about the verification of the electronic signature can be found at: https://www.signaturpruefung.gv.at

Herbert Leitold, Director

[26] ECDSA – Elliptic Curve Digital Signature Algorithm
[27] Hash value calculation may also be performed outside of the QSCD.
[28] SHA – Secure Hash Algorithm
[29] nShield Solo XC F2, nShield Solo XC F3, nShield Solo XC for nShield Connect XC
[30] EAL – Evaluation Assurance Level
[31] AVA_VAN.5 – Advanced methodical vulnerability analysis
[32] ALC_FLR.2 – Flaw reporting procedures