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) Ubiqu's Qualified Remote Signature and Seal Creation Device, version 2.2

Applicant:
Ubiqu Access B.V.
Kerstant van de Berglaan 13b
3054 EM Rotterdam
The Netherlands

QSCD-Certificate issued on: 2020-11-19
Reference number: A-SIT-VIG-19-075

1. Product Description

The product is a Qualified Electronic Signature and Seal Creation Device (QSCD) which is operated in the secure operational environment of a qualified Trust Service Provider (TSP) to provide users with a remote signing functionality. When used in combination with qualified certificates ubiqu's QSCD generates qualified electronic signatures or seals as defined in eIDAS with the legal effects of Article 25.

Subcomponents:

The QSCD consists of a FIPS 140-2 level 3 certified HSM and ubiqu specific firmware ("functionality module") loaded onto this HSM. The HSM is operated according to its FIPS 140-2 level 3 certification in conjunction with the corresponding security policy. The QSCD uses the HSM type "ProtectServer Internal Express 2 (PSI-E2)[2]".

[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] Firmware Versions: 5.01.02 and 5.01.03, Hardware Version: VBD-05, Version Code 0200; FIPS validation certificate #3231; Firmware Versions: 5.03.01 and 5.03.02, Hardware Version: VBD-05, Version Code 0200; FIPS validation certificate #3564; Manufacturer: Gemalto, a Thales Company, 20 Colonnade Road, Suite 200, Ottawa, ON K2E 7M6, Canada

Generation of Signature and Seal Creation Data:

An identity provider (IDP)/TSP is responsible for identity vetting and registration of subjects for this purpose the IDP/TSP maintains a signer ID. During the activation procedure the signer ID is bound to the QSCD and the subject's smartphone app using a PUK[3] and an activation nonce that were securely delivered to the subject by the IDP/TSP. During the activation the subject sets a PIN, that will be used as second authentication factor (in addition to the smartphone) for subsequent SCD[4] activations. After this binding is completed the SCD/SVD[5] key pair (generation was done in the HSM before in conjunction with the PUK generation) is activated inside of the HSM.

Storage of Signature and Seal Creation Data:

The SCD is stored encrypted outside the HSM using an HSM key. During the SCD activation after a successful two factor authentication the SCD is loaded in the HSM before signature or seal generation. All operations of generation, application and destruction of the SCD are implemented with the certified security functions of the HSM.

Signature and Seal Creation:

A Signature Creation Application (SCA) generates the DTBS/R[6] (i.e. hash of the document to be signed) on the SCA server and triggers the signature or seal invocation by sending the DTBS/R to the QSCD. The QSCD performs a two-factor authentication using the previously associated smartphone of the signer/seal creator and the PIN. If the authentication is successful, the SCD is loaded into the HSM and a qualified electronic signature or seal (QES) is generated based on the previously provided DTBS/R. After signature or seal creation the SCD is deactivated inside the HSM and the result of the signature operation is transferred from the QSCD to the SCA.

[3] PUK - Personal Unblocking Key
[4] SCD – Signature/Seal Creation Data
[5] SVD – Signature/Seal Validation Data
[6] DTBS/R – Data To Be Signed/Representation

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 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.

---

[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.*

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[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 (mobile phone, web browser) must be suitably protected. The signatories shall keep control of their assigned 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 HSM must be initialised and operated based on its certification according to FIPS 140-2 level 3.

(5) HSM operations such as backup, storage and restoration of private or secret keys must only be performed by authorized personnel using smartcards and under at least 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.

5. Algorithms and Corresponding Parameters

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

- RSASSA-PKCS#1-v1_5[18] according to PKCS#1 v2.2 (RFC 8017) with a cryptographic key size of 2048[19], 3072 or 4096 bits.

For the calculation of hash values the algorithm SHA-256 according to FIPS 180-4 is supported[20].

[17] in accordance with recital 56 of eIDAS

[18] Annotation: The acceptability deadline for the legacy use of RSASSA-PKCS1-v1_5, is set to at least December 31, 2027 by the SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, p. 28, Version 1.2, January 2020.

[19] Annotation: The acceptability deadline for the legacy use of modulus of size above 1900 bits, but less than 3000 bits, is set to December 31, 2025 by the SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, p. 24, Version 1.2, January 2020.

[20] Annotation: The hash value calculation is performed outside of the QSCD by the SCA.

6. Assurance Level and Strength of Mechanism

For the used HSM ProtectServer Internal Express 2 (PSI-E2) the following FIPS 140-2 validation certificates issued by the US (National Institute of Standards and Technology) and the Canadian (Communications Security Establishment) FIPS 140-2 certification body apply. The certificates confirm that the HSM was successfully evaluated against FIPS 140-2 level 3:

- Certificate #3231 issued on 2018-07-12 and last renewed on 2019-01-31 for ProtectServer Internal Express 2 (PSI-E2); Firmware Versions: 5.01.02 and 5.01.03; Hardware Version: VBD-05, Version Code 0200
- Certificate #3564 issued on 2019-11-15 for ProtectServer Internal Express 2 (PSI-E2); Firmware Versions: 5.03.01 and 5.03.02; Hardware Version: VBD-05, Version Code 0200

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 considering 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-19-075.

Authorized Signature:

A-SIT Secure Information Technology Center – Austria

Vienna, (Date see electronic signature)

SIGNATURE INFORMATION	**Signatory**	Reinhard Posch
	Date/Time-UTC	2020-11-19T15:43:40+01:00
	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