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

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

Qualified Signature and Seal Creation Device (QSCD)
Signer-1 SAM version 1.0.0.1

Applicant:
ComsignTrust Ltd.
Kiryat Atidim BLDG #4
61580 Tel Aviv
Israel

QSCD-Certificate issued on: 2020-10-18
Reference number: A-SIT-VIG-19-077

1. Product Description

The product “Signer-1” is a Qualified Electronic Signature Creation Device (QSCD) to provide users with a remote signing functionality which is operated in the secure operational environment of a qualified Trust Service Provider (TSP). Signer-1 generates qualified electronic signatures as defined in eIDAS with the legal effects of Article 25.

Subcomponents:

The Qualified Remote Electronic Signature Creation Device (“Signer-1”) uses HSM devices as cryptographic modules for the generation and protection of the signature creation data (SCD). Only the HSM device family “Utimaco CryptoServer CP5” can be used for the QSCD. The HSMs are operated according to their issued Common Criteria[1] certification[2] in conjunction with the corresponding security target[3,4].

Furthermore, the QSCD uses a Signature Activation Module (SAM) – a software component placed within the HSM – as single component to communicate with the cryptographic module, in order to authorize and initiate the signature creation process. Those two components, the HSM and the SAM, together form the QSCD, which is intended to be operated by a qualified trust service provider in a secure operational environment as part of a remote electronic signature service. For its services, the

[1] Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 4 (ISO/IEC 15408)
[2] Certificate number: CC-19-222073
[3] Certification ID: NSCIB-CC-19-222073
[4] Document reference: 2018-0014

QSCD also uses other components such as identity providers or applications. However, those components are not part of the QSCD and thus not inside the scope of this certification.

Generation of Signature Creation Data:

Upon an initial registration request of a user by a registration authority, a trusted application can request to the SAM the generation of the corresponding SCD/SVD key pair inside of the HSM protected by this application. Then, the trusted application requests to bind the SCD/SVD key pair to the user. Access to the operations for creating and assigning the SCD is controlled by the SAM, which requires to be delivered by authorized technicians and which is required to be installed prior to delivery by ComsignTrust trusted personnel. An external registration authority (RA) orchestrates the certification of the SCD from a Public Key Infrastructure (PKI), creating the Certificate Signing Request (CSR) for the key pair, requesting to the SAM (via the SCA) its proof-of-possession and finally obtaining the X.509 certificate.

Storage of Signature Creation Data:

The SCD[5]/SVD[6] key pair which is cryptographically associated to each other is generated inside of the HSM. After the SCD/SVD key pair is generated inside of the HSM, the SCD is encrypted using the HSM's hardware key. Afterwards it is returned by the SAM outside of the SAM. The SCD never leaves the HSM unencrypted nor unprotected by the SAM. This way the SCD can only be used by the combination of the SAM and the HSM. All operations of generation, application and destruction of the SCD are implemented with the certified security functions of the HSM.

Signature Activation Protocol:

The SCD is only generated and accessible inside of the HSM after a successful authentication process with the specified Signature Activation Protocol (SAP). The signing interaction with the signatory is performed using a user application via an API the Signer Interaction Component (SIC). The user application is responsible for creating the signed document using the signature values provided by the QSCD.

The SAP ensures the consent on the document to be signed. If the document is not shown by the SAP directly, then a reference to the document is shown during the SAP. Sole control over the SCD is ensured by sending a challenge from the SAM to the signatory via the SIC. The SIC signs the challenge with the key authorization (KA). Moreover, the KA must be appropriately protected by the SIC. The QSCD generates the challenge and associates it with the signatory and the signatory's key pair. The authentication according to SCAL2[7] level according to EN 419 241-1 is performed by an external identity provider (IDP) and confirmed with a signed assertion in conjunction with the SIC by using the KA. Thus, the authentication is in any case performed as 2-factor authentication according to SCAL2.

Signature Creation:

A user can only request a signature creation via trusted applications (through the SSA[8] i.e., Signer-1 Server) and not via direct access in particular to the QSCD. The communication between those external components and the remote QSCD employs the Signature Activation Protocol (SAP). A user requesting the signature of one or more documents (i.e., a set of DTBS/R) interacts with the Signer Interaction Component (SIC). When the user starts a signature request, the DTBS or the set of DTBS are transferred to a Signature Creation Application (SCA) and the SCA initiates the signature process on behalf of the user. The SCA thus creates a hash out of the document or out of the documents. The user is redirected to the SIC which then requests the use of SCD of the user from the SSA. The SSA requests the SAM to restore the SCD and therefore, the SAM generates a cryptographic challenge. After that, the SIC requests the consent from the user who insert the credentials from the IDP. The IDP shall manage the authentication factors for the Signer in a secure manner. The authentication service and the Identity Provider (IDP) component initiate the

[5] SCD – Signature Creation Data

[6] SVD – Signature Validation Data

[7] SCAL2 – Sole Control Assurance Level 2

[8] SSA – Server Signing Application

authorization of the user. The authentication service verifies the authentication factor(s) of the signer user and issues an assertion that the signer user has been authenticated. The QSCD verifies this assertion. The authenticated user can inspect the data to be signed via the SCA, which computes the hash representation (DTBS/R) of the data to be signed by processing the document to be signed.

The SIC authenticates the user with the IDP and obtains an assertion from the authentication service.

The IDP authorizes the user access of a concrete signing key to sign the concrete DTBS/R. The fully authenticated user can inspect the hash and DTBS/R and give a final consent to the signature creation. This consent creates an assertion, the Signature Activation Data (SAD), which is only valid for this particular transaction. The SAD binds together three elements: signer user authentication with the signing key and the data to be signed (DTBS/R(s)). The SSA verifies the signature request including the challenge and invokes the SAM component of the QSCD. The SAM verifies the SAD and DTBS/R. If the verification is correct, it loads and activates the signing key in the HSM, which then signs the DTBS/R with this key thus generating the signature. The signature is returned to the SCA and attached to the DTBS/R.

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[9] eIDAS,
- requirements laid down in Annex II eIDAS (para 1 lit. a[10],b[11],c[12],d[13], para 2[14], para 3[15], para 4 lit a[16], b[17])

The compliance of the QSCD is thus confirmed within the following categories:

- components and procedures for the generation of signature creation data,
- components and procedures for the storage of signature creation data,
- components and procedures for the processing of signature creation data

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

[10] *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.*

[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 can practically occur only once.*

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

[13] *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.*

[14] *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.*

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

[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 security of the duplicated datasets must be at the same level as for the original datasets.*

[17] *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.*

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 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 challenge as well as the integrity of the data to be signed during transmission from the signatory to the QSCD are part of the QSCD’s system environment[18] and thus outside the scope of this QSCD-certificate. It must be ensured that the signatories are informed that components used for the initiation of the signature process (user application) must be suitable protected. The signatories shall keep control of their assigned devices and shall promptly report any circumstance where a credential is compromised according to the defined revocation or suspension procedures.

(2) The QSCD must be operated by a qualified trust service provider under the eIDAS regulation.

(3) The qualified trust service provider must operate the QSCD in a protected environment; this environment must provide sufficient measures to protect the QSCD against physical tampering and unauthorized physical or network access. In particular the following procedures shall be adhered to:

- Owners of trusted roles for the administration of QSCD components shall be authenticated using private keys stored on certified tokens (e.g., smartcards).
- 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) External authentication mechanisms, which are used to authenticate a user in order to create a qualified electronic signature, shall correspond to an authentication means equivalent to EC Implementing Regulation 2015/1502 for assurance level substantial or higher[19].

[18] in accordance with recital 56 of eIDAS

[19] 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

(5) Electronic signature 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 and key sizes listed in section five shall be used for the creation of qualified electronic signatures.

5. Algorithms and Corresponding Parameters

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

- RSASSA-PSS according to FIPS PUB 186-4 and RFC 8017 with a cryptographic key size of 2048[20], 3072, 4096 or 8192 bit.

For the calculation of hash values the algorithm SHA256 is supported[21].

6. Assurance Level and Strength of Mechanism

For the used HSM Utimaco CryptoServer CP5 (Version Se12 5.1.0.0, Se52 5.1.0.0, Se500 5.1.0.0, Se1500 5.1.0.0) the issued Common Criteria certificate by TÜV Rheinland Nederland B.V with no. CC-19-222073 applies. The Common Criteria certificate was first issued on 2018-12-19, and renewed on 2019-03-14 and 2020-05-14 with a sunset date on 2023-12-19. The certificate confirms that the hardware security module has been successfully evaluated according to Common Criteria Version 3.1, Evaluation Assurance Level EAL 4+, augmented by AVA_VAN.5[22] and in conformance to the Protection Profile (PP) prEN 419 221-5 *„Cryptographic Module for Trust Services".*

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-19-077.

Authorized Signature:

A-SIT Secure Information Technology Center – Austria

Vienna, (Date see electronic signature)

SIGNATURE INFORMATION	**Signatory**	Reinhard Posch
	Date/Time-UTC	2020-10-18T17:05:46+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

[20] 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.

[21] Annotation: The hash value calculation may also be performed outside of the QSCD by the SCA

[22] AVA_VAN.5 – Advanced methodical vulnerability analysis