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) Intesi PkBox, Version 3.3

Applicant:
Intesi Group S.p.A.
via Torino 48
20123 Milano
Italy

QSCD-Certificate issued on: 2018-07-09
Reference number: A-SIT-VIG-18-051

1. Product Description

PkBox is a product for electronic signatures and seals intended to be used as a Qualified Remote Signature and Seal Creation Device (QSCD) in a secure operational environment. It implements a Trustworthy System Supporting Server Signing (TW4S) in accordance with EN 419241-1:2018. When used in combination with qualified certificates PkBox generates qualified electronic signatures and seals as defined in Regulation (EU) No. 910/2014 (eIDAS) with the legal effects defined within.

Subcomponents:

An HSM device (Thales nShield Solo/Solo+/Solo XC or nShield Connect/Connect+/Connect XC[2]) is used as a cryptographic module for the generation and protection of the signature and seal creation data (SCD). The HSM is operated according to its FIPS 140-2 level 3 certification[3].

The HSM device is accessed only through PkBox COD (“Credential On Database”) which uses a secure mechanism provided by the HSM for storing private keys outside 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

[2] Firmware Versions: 2.50.16, 2.51.10, 2.55.1, 3.3.21 and 3.4.1; Manufacturer: Thales e–Security Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324, USA

[3] https://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1742.pdf
https://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2148.pdf
https://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2941.pdf

The PkBox COD module is also responsible for the validation of the one-time-password (OTP) to ensure that the SCD can be reliably protected by the legitimate signatory against the use of others.

The Signature Creation Application (SCA) sends the entire document to be signed either directly to PkBox COD or uses a PkBox Remote module that is installed in the same IT infrastructure with the SCA. PkBox Remote is then responsible for the hash computation and sends the document hash to PkBox COD. Both PkBox modules guarantee the document integrity during the signature process, verifying the signed hash against the calculated hash value. As an alternative procedure, the SCA sends the document hash to PkBox COD or PkBox Remote and PkBox modules return the signed hash value. In this scenario, the document integrity is verified and guaranteed by the SCA.

The SCA and the PkBox Remote module are not part of the QSCD and thus outside the scope of this confirmation.

Generation and Storage of signature and seal creation data (SCD):

The SCD/SVD key pair is generated within the HSM and the SCD is stored in encrypted form in a database outside the HSM. During the enrolment process the signatory has to define a secret PIN. To provide strong authentication a one-time-password (OTP) mechanism is used in addition to this PIN. PkBox can be configured to address different OTP providers, for example:

- Vasco Vacman controller engine
- Vasco IdentiKey Server
- RSA SecureID Authentication
- RSA SecureID ACE Server
- Radius server together with: Vasco, RSA, SafeNet or McAfee validation server
- Time4ID SMS and Mobile Token OTP Engine
- Time4ID OATH Engine together with Intesi Group virtual tokens and Gemalto OTP devices
- CA Strong Authentication VAS using remote CA Technologies server with a variety of authentication devices
- Asseco Aseba SxS OTP Solution VAS using remote Asseco server with a variety of authentication devices
- Gemalto Authentication Server using remote Gemalto server

PkBox can also be configured to address further OTP providers, not listed here but having the same level of trustworthiness, provided that the conditions in section 4 are fulfilled.

The OTP provider and the OTP identifier are stored together with the encrypted SCD in the database. All cryptographic operations of generation, encryption and decryption of SCD are implemented within the HSM. The application of the SCD within the HSM is only possible after a successful OTP validation and authentication with the signatory's secret PIN.

The remote signature mechanism can also use an alternative two-factor authentication method, in which the authentication of the two factors is split between the SCA and PkBox COD (delegated authentication). In this case the PIN value is not provided by the signatory but it is a derived PIN provided by the SCA to the TOE after a successful user authentication. This method is only available, if the SCA is held by a trustworthy entity, which is audited by the QTSP operating the QSCD.

After SCD generation a certificate request (PKCS#10) is generated and transmitted to a certificate authority. The process of issuing qualified certificates is outside the scope of this confirmation.

Signature and seal creation:

PkBox's signature process is structured as follows:

- The signature credential specified by the signatory is received from the credential database.
- The associated SCD is imported into the HSM.

- The PIN provided by the signatory, resp. the derived PIN provided by the SCA in the case of delegated authentication, is verified inside the HSM.
- The selected credential access policies are verified.
- The validity of the OTP is checked using the vendor defined within the credential access policies.
- In case of a failure in the verification of PIN or OTP values, the signing process is aborted.

In case of a successful verification of all the authentication parameters, the signature is generated within the HSM.

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[4] eIDAS,
- requirements laid down in Article 39 para 1[5] eIDAS,
- requirements laid down Annex II eIDAS (para 1 lit. a[6],b[7],c[8],d[9], para 2[10], para 3[11], para 4 lit a[12], b[13])

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

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

3. Validity Period of the QSCD-Certificate

This QSCD-Certificate is valid up to revocation by A-SIT.

---

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

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

[6] *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*.

[7] *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.*

[8] *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.*

[9] *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.*

[10] *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.*

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

[12] *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.*

[13] *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 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 resp. 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 resp. 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 resp. to be sealed during transmission from the signatory resp. creator of a seal to the QSCD are part of the QSCD's system environment[14] and thus outside the scope of this QSCD-certificate. It must be ensured that the signatories resp. creators of a seal are informed that components used for the initiation of the signature resp sealing process (OTP device, mobile phone, web browser) must be suitable 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 (QTSP).

(3) In case of delegated authentication the QTSP deploying PkBox COD shall ensure that the party deploying the SCA to which the authentication is delegated uses authentication means and mechanisms that meet the requirements specified in EC Implementing Regulation 2015/1502 for assurance level substantial or higher[15]. The SCA shall not cache the derived PIN obtained by PkBox COD for a signature operation for longer than necessary to complete the resp. transaction.

(4) 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 shall be installed in a secured and controlled access area of the IT department of the organization, no one but the appliance administrator shall be able to physically access the appliance or its surroundings
- 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 appliance administrator must periodically check the appliance's case for any evidence of physical tampering, the check must be performed at least daily, alternatively a remote continuous monitoring and surveillance system (RCMSS)[16] can be set up; in case of any evidence of physical tampering the HSM shall be disconnected and reinitialized

[14] in accordance with recital 56 of eIDAS

[15] 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

[16] Defined in PkBox RCMSS Based Procedure version 1.0. In this case a physical check on-premise is required only when a security alert has been triggered by the monitoring and surveillance system.

- 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; the appliance administrator must periodically check that the secure environment of the QSCD is not compromised with any hardware or software that can violate the security of the QSCD; this includes network sniffers and devices that may be used for timing attacks. This check must be performed at least daily or alternatively – if the RCMSS is available – when a security alert is received
- 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

(5) The HSMs must be initialised and operated in FIPS 140-2 level 3 mode.

(6) 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.

(7) Electronic signature resp. 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 and seals the QSCD uses the following algorithms:

- RSASSA-PKCS1-v1_5 or RSASSA-PSS[17] and modulus lengths of 2048 or 4096 bits.
- ECDSA with the following curves defined in NIST FIPS PUB 186-4: P-256, P-384, P-521, K-283, B-283, K-409, B-409, K-571, B-571.

For the calculation of hash values the following algorithms are supported[18]:

- SHA-256, SHA-384 and SHA-512 according to FIPS 180-4

6. Assurance Level and Strength of Mechanism

For the used HSMs (Thales nShield Solo/Solo+/Solo XC or nShield Connect/Connect+/Connect XC, firmware versions 2.50.16, 2.51.10, 2.55.1, 3.3.21 and 3.4.1) the following certifications apply:

- FIPS Validation Certificate No. 1742 – issued on 2012-06-25 and last updated on 2015-11-16 by the US (National Institute of Standards and Technology) and the Canadian (Communications Security Establishment) FIPS 140-2 certification body
- FIPS Validation Certificate No. 2148 – issued on 2014-05-13 and last updated on 2015-11-24 by the US (National Institute of Standards and Technology) and the Canadian (Communications Security Establishment) FIPS 140-2 certification body
- FIPS Validation Certificate No. 2941 – issued on 2017-06-23 and last updated on 2017-11-07 by the US (National Institute of Standards and Technology) and the Canadian (Communications Security Establishment) FIPS 140-2 certification body

The certificates confirm that the resp. HSM was successfully evaluated against FIPS 140-2 level 3.

For the used HSMs (Thales nShield Solo/Solo+ or nShield Connect/Connect+, firmware version 2.55.1) the certificate No. 1/16 – issued on 2016-03-10 by the Italian Common Criteria certification body OCSI applies. The certificate confirms that the resp. HSM was successfully evaluated against Common Criteria version 3.1., Evaluation Assurance Level EAL4+ augmented with AVA_VAN.5[19].

[17] According to PKCS#1 v.2.2 (IETF RFC 8017)

[18] Hash value calculation may also be performed outside of the QSCD (either by the SCA or – in the case of PKBox Remote configuration – by the PKBox Remote Module)

[19] Vulnerability Assessment – Advanced methodical vulnerability analysis

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-18-051.

Authorized Signature:

A-SIT Secure Information Technology Center – Austria

Vienna, (Date see electronic signature)

SIGNATURE INFORMATION	**Signatory**	Reinhard Posch
	Date/Time-UTC	2018-07-09T16:47:05+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