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

A-1030 Wien, Seidlgasse 22 / 9
Tel.: (+43 1) 503 19 63–0
Fax: (+43 1) 503 19 63–66

A-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

Confirmation pursuant to § 18 para. 5 SigG

Secure Signature Creation Device
PkBox, Version 3.1.0

Applicant:
Intesi Group SpA
Via Torino 48
I-20123 Milano, Italy

Confirmation issued on: 2016-05-17
Reference number: A-SIT-VI-16-038

Preliminary Remarks

Zentrum für sichere Informationstechnologie - Austria (A-SIT) is declared by the Federal Chancellor's Ordinance BGBl II 31/2000 as a confirmation body pursuant to § 19 of the Austrian Signature Act (Signaturgesetz - SigG), BGBl I 190/1999 as amended by BGBl I 75/2010.

A-SIT is notified as a designated body under the European Signature Directive (1999/93/EC) article 3 para. 4.

A-SIT is thus made responsible for confirming the compliance of secure signature creation devices with the security requirements laid down in the Austrian Signature Act as transposition of the Annex III requirements of Directive 1999/93/EC into Austrian legislation.

1. Product Description

PkBox is a product for electronic signatures intended to be used as a Secure Signature Creation Device (SSCD) in a secure operational environment. It implements a Trustworthy System Supporting Server Signing (TW4S) in accordance with CEN/TS 419241:2014. When used in combination with qualified certificates PkBox generates qualified electronic signatures as defined in Directive 1999/93/EC with the legal effects of article 5 para. 1.

Subcomponents:

An HSM device (Thales nShield Solo/Solo+ or nShield Connect/Connect+[1]) is used as a cryptographic module for the generation and protection of the signature creation data (SCD). The HSM is operated according to its FIPS 140-2 level 3 certification[2].

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. 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.

[1] Firmware Versions: 2.50.16-3, 2.51.10-3 and 2.55.1-3; Manufacturer: Thales e–Security Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324, USA

[2] http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1742.pdf
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2148.pdf

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 SSCD and thus outside the scope of this confirmation.

<u>Signature Creation Data:</u>

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:

- 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

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.

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.

<u>Signature Generation:</u>

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 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 SigG[3] and SigV[4]

The Signature Creation Device meets the following requirements, provided that the conditions in section 4 are fulfilled:

- requirements laid down in § 18 para. 1 and para. 2 SigG, therefore fulfilling the requirements laid down in Annex III of Directive 1999/93/EC
- requirements laid down in § 3 para. 1 and para. 2 SigV[5]
- requirements laid down in § 6 para. 3 SigV[6]

The compliance of the Signature Creation Device is thus confirmed within the following categories:

- components and methods for generating the signature creation data
- components and methods for storing the signature creation data
- components and methods for applying the signature creation data

3. Validity Period of the Confirmation

This confirmation 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 confirmation includes surveillance for a period of two years. The confirmation 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 confirmation is subject to the conditions stated below. The measures taken shall be

- ascertained by the CSP's security and certification policy in accordance with § 12 SigV[7] or an equivalent applicable rule at European or national level,
- 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 authorization codes as well as the integrity of the data to be signed during transmission from the signatory to the SSCD are part of the SSCD's system environment (§ 4 SigV[8]) and thus outside the scope of this confirmation. It must be ensured that the signatories are informed that components used for the initiation of the signature process (OTP device, 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.

[3] Austrian Signature Law: „Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG", BGBl I Nr. 190/1999 as amended by BGBl. I Nr. 75/2010

[4] Austrian Signature Ordinance: „Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung 2008 – SigV 2008", BGBl. II Nr. 3/2008 as amended by BGBl. II Nr. 401/2010

[5] Requirements regarding the examination of technical components and procedures for qualified signatures (see section 6 of this confirmation) and regarding suitable algorithms and parameters (see section 5 of this confirmation)

[6] The Secure Signature Creation Device must be operated in a secure operational environment (see section 4 para. 2 of this confirmation)

[7] § 12 SigV defines the minimum content of the CSP's security- and certification policy

[8] in accordance with recital (15) of Directive 1999/93/EC: '*Annex III covers requirements for secure signature-creation devices to ensure the functionality of advanced electronic signatures; it does not cover the entire system environment in which such devices operate*;'

(2) The SSCD must be operated in a secure operational environment; this environment must provide sufficient measures to protect the SSCD against physical tampering and unauthorized physical or network access. In particular the following procedures[9] shall be adhered to:

- The SSCD 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 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)[10] can be set up. In case of any evidence of physical tampering the HSM shall be disconnected and reinitialized.
- The appliance administrator must periodically check that the secure environment of the SSCD is not compromised with any hardware or software that can violate the security of the SSCD. 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.
- The HSM must be initialised in FIPS 140 level 3 mode.
- 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.

Compliance of the measures taken by the operator of the SSCD shall be subject to a periodic review.

5. Algorithms and Corresponding Parameters

For the creation of qualified electronic signatures the SSCD uses the following algorithms:

- RSA (corresponds to SigV Annex, table 4, index number 1.01) with padding EMSA-PKCS1-v1_5 (corresponds to SigV Annex, table 3, index number 3.01)

  RSA is used with modulus lengths of 2048 or 4096 bits.

- ECDSA (corresponds to SigV Annex, table 4, index numbers 1.03[11] and 1.04[12])

  ECDSA is used 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[13]:

- SHA-256, SHA-384 and SHA-512 (corresponds to SigV Annex, table 2, index numbers 2.04, 2.05 and 2.06)

Thus the requirements of § 3 para. 2 SigV are met.

6. Assurance Level and Strength of Mechanism

For the used HSMs (Thales - nCipher nShield Solo/Solo+ or nShield Connect/Connect+, firmware versions 2.50.16-3, 2.51.10-3 and 2.55.1-3) the 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 – resp. the FIPS Validation Certificate No. 2148 – issued on 2014-05-

[9] Defined in PkBox Security Target version 1.6, Security Objectives for the Operational Environment resp. PkBox Operational User Guidance version 1.4

[10] 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.

[11] DSA with elliptic curves based on a prime field GF(p)

[12] DSA with elliptic curves based on a binary field GF(2^m)

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

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 – apply. The certificates confirm that the resp. HSM was successfully evaluated against FIPS 140-2 level 3. For the used HSMs (Thales - nCipher nShield Solo/Solo+ or nShield Connect/Connect+, firmware version 2.55.1-3) 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[14].

Since there is no certification against a suitable protection profile published as reference number for generally recognised standards in the Official Journal of the European Communities in accordance with article 3, paragraph 5 of Directive 1999/93/EC A-SIT verified the fulfilment of organizational and technical security requirements according to § 6 para. 3 SigV.

The results of the performed assessment which is the basis for this confirmation are documented in the confirmation report under the reference A-SIT-VI-16-038.

Authorized Signature:

SIGNATURINFORMATIONEN	**Unterzeichner**	Reinhard Posch
	Datum/Zeit-UTC	2016-05-17T14:02:23+02:00
	Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at
Hinweis	Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument ist gemäß EU Verordnung Nr. 910/2014 (eIDAS) einem handschriftlich unterzeichneten Dokument grundsätzlich rechtlich gleichgestellt.	

[14] Vulnerability Assessment – Advanced methodical vulnerability analysis