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) AliasLab CryptoAccelerator, release 3.5.1

Applicant:
AliasLab SpA,
via Cremona 27/6
46100 Mantova
Italy

QSCD-Certificate issued on: 2017-12-20
Reference number: A-SIT-VIG-17-083

1. Product Description

CryptoAccelerator is a product for both electronic signatures and electronic seals that is particularly intended to be used as a remote Qualified Signature resp. Seal Creation Device (QSCD) in the secure operational environment of a qualified trust service provider (TSP). If and only if it is used in combination with qualified certificates, CryptoAccelerator generates (1) qualified electronic signatures resp. (2) qualified electronic seals as defined in eIDAS with the legal effects of (1) Article 25 resp. (2) Article 35.

Subcomponents:

An HSM device (Thales nShield Solo Series or Thales nShield Connect Series[2]) is used as a cryptographic module for the generation and the protection of the signature creation data (SCD). The respective HSM is operated according to its FIPS 140-2 level 3 certification in conjunction with the published security policies resp. according to its Common Criteria EAL4+ certification. The HSMs provide a secure protection mechanism “Security World” for storing private keys outside of 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] Solo, Solo+ and Solo XC resp. Connect, Connect+ and Connect XC; Firmware Versions: 2.50.16 and 2.55.1 as well as 3.3.21 and 3.4.1; Manufacturer: Thales e–Security Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324, USA

The HSM device is accessed exclusively via the CryptoManager module of CryptoAccelerator. For both the enrolment and the certificate management, CryptoAccelerator uses the CryptoProvisioning module and the CryptoProvisioningConnector for connecting to a certificate authority. To ensure that the SCD can be reliably protected by the legitimate signatory against the use of others CryptoAccelerator uses four particular strong authentication techniques. The strong authentication methods are provided by the modules (1) CryptoServices (authentication either with PIN+OTP or only with PIN for seals), (2) CryptoServicesSMS (authentication with native PIN+SMS OTP), (3) SecureCallSign (authentication with PIN+MSISDN+OTP+SecureCall) and (4) BioCryptoService (authentication with PIN+biometric signature).
A Signature Creation Application (SCA) sends the entire document to be signed (resp. to be sealed) or a derived hash value to CryptoAccelerator. There are 2 particular SCA techniques to distinguish: The (1) CryptoClient (installed directly by the signatory) or the (2) CryptoAppliance (installed at a customer's premises). CryptoClient and CryptoAppliance are not part of the QSCD and thus outside of the scope of this QSCD-Certificate.

Generation and Storage of Signature and Seal Creation Data (SCD):

The SCD/SVD key-pair is generated inside of the HSM and the SCD is stored in encrypted form in a database ("Security World"). During the enrolment process the signatory's (resp. the creator's of a seal) secret PIN is defined. To provide strong authentication five different mechanisms are used in addition to this PIN. The type of the authentication mechanism

(1) FDR – certificate with strong authentication based on external OTP with HW or SW token,
(2) FDS – certificate with strong authentication based on SMS OTP,
(3) FSM – certificate with strong authentication based on SecureCall,
(4) FSB – certificate with strong authentication based on biometric signature, and
(5) FRM – certificate used for seals (no strong authentication is used)

as well as related parameters in terms of strong authentication

(1) token serial number in case of hardware OTP token,
(2) mobile phone number in case of SMS OTP or SecureCall,
(6) biometric reference data in case of biometric signature via graphometric authentication

are stored during the enrolment and are particularly bound to the SCD/SVD key-pair resp. the subsequently derived certificate.
All cryptographic operations of generation, encryption and decryption of the SCD are implemented inside of the HSM. The SCD is only accessible inside of the HSM after a successful authentication with the defined strong authentication method and using the signatory's (resp. the creator's of a seal) secret PIN.
After the generation of the SCD a certificate request (PKCS#10) is generated and transmitted to a certificate authority. The process of issuing qualified certificates is outside of the scope of the present QSCD-Certificate.

Strong Authentication Methods:

The SCD can only be decrypted inside of the HSM. Moreover, the decryption of the SCD requires the signatory's secret PIN. In addition to the PIN CryptoAccelerator always uses one out of four different mechanisms to authenticate the signatory (for seal creation no strong authentication method is required in addition to the PIN to authenticate the creator of a seal):

- ***OTP Token:*** A one-time-password (OTP) mechanism using a HW-Token or SW-Token is used. CryptoAccelerator can be configured to address the OTP providers (1) RSA SecureID ACE Server, (2) Vasco Identikey Server, (3) Vasco Vacman Controller, (4) SafeNet-Gemalto Authentication Manager, (5) SafeNet-Gemalto Autentication Service PCE, (6) SecureCallSmart-App[3] and (7) OATH[4] standard based servers[5]. The signatory enters her/his secret PIN and the OTP generated by the Token into the SCA. After that, the SCA submits the data to CryptoAccelerator.

[3] Annotation: The SecureCallSmart-App is based on the HOTP standard
[4] OATH – Open Authentication
[5] Annotation: Vasco and Safenet-Gemalto OTP tokens also support the OATH standard

- ***SMS OTP:*** An OTP code is generated using the HOTP[6] algorithm based on the document to be signed. The OTP is sent via SMS to the signatory's cell phone. The signatory enters her/his secret PIN and the SMS OTP into the SCA. After that, the SCA submits the data to CryptoAccelerator.
- ***SecureCall:*** The signatory has to call a phone number[7] with her/his registered cell phone or – in some cases – the system calls the signatory's registered cell phone. The variable part represents an OTP; it is unique for one transaction and only valid for a limited time-period. CryptoAccelerator verifies both the OTP and the signatory's cell phone number (MSISDN). The signatory enters her/his secret PIN during the phone call.
- ***Biometric Signature:*** This method is based upon capturing the signatory's handwritten signature using a dedicated and specialized hardware (i.e. a signature pad). The module used by CryptoAccelerator is based on the Softpro[8] biometric compare engine[9] and uses both a (1) static (image) as well as (2) dynamic (pressure, acceleration, speed) data to compare the captured signature with a specimen that has been recorded during the enrolment process. The signatory enters her/his secret PIN on the signature pad and subsequently writes her/his signature on the pad with a stylus. PIN and biometric signature data are submitted to CryptoAccelerator. The authentication process can only be performed with pre-registered signature pads[10] in a controlled environment. That means that it requires an operator seat in the premises at a branch or an agency. The operator must identify the signatory and must be present during the signature operation. To prevent the abusive reuse of a captured biometric signature, CryptoAccelerator calculates a hash value of each signature and checks it against a history database.

Signature and Seal Generation:

The signature resp. seal. creation process is structured as follows:

- **Authentication.** CryptoAccelerator authenticates the signatory resp. creator of a seal according to the predefined strong authentication method.
- **Data transmission.** (1) Signatory's resp. creator's of a seal User-ID, (2) Certificate-ID, (3) the hash value of the document to be signed resp. to be sealed and (4) the secret PIN provided by the signatory resp. creator of a seal are transmitted to the HSM.
- **SCD activation.** The associated SCD is loaded from the database into the HSM.
- **SCD decryption.** The PIN provided by the signatory is used to decrypt the SCD inside the HSM.
- **Signature/Seal generation.** In case of a successful verification of all the authentication parameters, the signature resp. seal is generated inside of the HSM. In case of automatic signatures resp. seals a group of documents can be signed resp. sealed with one authentication.

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

[6] HOTP – HMAC-based One-time Password Algorithm
[7] Annotation: The phone number is composed of both a fixed and a variable part where the variable part represents a unique value
[8] Annotation: Softpro is known as Kofax that have been acquired by Lexmark
[9] Annotation: The biometric compare engine is a proprietary solution
[10] Annotation: The signature pad can either be a graphical tablet, Software that is embedded into a notebook or an e-signature pad
[11] *Qualified electronic signature creation devices shall meet the requirements laid down in Annex II.*
[12] *Article 29 shall apply mutatis mutandis to requirements for qualified electronic seal creation devices.*

- requirements laid down Annex II eIDAS (para 1 lit. a[13],b[14],c[15],d[16], para 2[17], para 3[18], para 4 lit a[19], b[20])

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.

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

[13] *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*.

[14] *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.*

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

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

[17] *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.*

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

[19] *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.*

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

of the QSCD's system environment[21] 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 authentication method "Biometric Signature" must be performed with pre-registered signature pads in a controlled environment. A trusted operator must identify the signatory as part of the process and must be present during the signature operation.

(3) The QSCD must be operated by a qualified trust service provider.

(4) 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[22] shall be adhered to:
- The QSCD shall be installed in a secured and controlled access area of the IT department of the organization. No one but the administrator can access the application for admin purposes.
- The administrator must periodically check the application configuration. This check must be performed at least daily or alternatively by a surveillance system with automated checks and alerts.
- The administrator must periodically check that in the secure environment of the QSCD is not installed 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 by a surveillance system with automated checks and alerts.
- All protective measures should be based on a risk management approach, following assessment of the risks in the specific operating environment in which the QSCD is deployed.

(5) The HSM must be initialised and operated in FIPS 140 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 resp. seals the QSCD uses the cryptographic algorithm

- RSASSA-PKCS1-v1_5 according to PKCS#1 v2.2 (RFC 8017) with cryptographic key sizes of 2048 bit or 4096 bit.

For the calculation of hash values the algorithm SHA-256 is supported[23].

[21] in accordance with recital 56 of eIDAS
[22] Defined in CryptoAccelerator Security Target, Security Objectives for the Operational Environment
[23] Hash value calculation may also be performed outside of the QSCD by the SCA.

6. Assurance Level and Strength of Mechanism

For the used HSMs the following Common Criteria resp. FIPS 140-2 Validation Certificates apply:

- Certificate No. 1/16[24] – issued on 2016-03-10 by the Italian Common Criteria certification body OCSI (Organismo di Certificazione della Sicurezza Informatica)

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[25].

- FIPS Validation Certificate No. 1742[26] – 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; for Thales – nCipher nShield Solo or nShield Connect, firmware versions 2.50.16 and 2.55.1
- FIPS Validation Certificate No. 2148[27] – 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; for Thales – nCipher nShield Solo+ or nShield Connect+, firmware versions 2.50.16 and 2.55.1
- FIPS Validation Certificate No. 2941[28] – 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; for Thales – nShield Solo XC or nShield Connect XC, firmware versions 3.3.21 and 3.4.1

The certificates confirm that the HSMs were successfully evaluated against FIPS 140-2 level 3.

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.

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-17-083.

Authorized Signature:

A-SIT Secure Information Technology Center – Austria

Vienna, (Date see electronic signature)

SIGNATURE INFORMATION	**Signatory**	Reinhard Posch
	Date/Time-UTC	2017-12-20T17:01:41+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

[24] Cf. http://www.ocsi.isticom.it/documenti/certificazioni/thales/rc_thales_nshield_v1.0.pdf
[25] AVA_VAN.5 – Advanced methodical vulnerability analysis
[26] Cf. https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/1742
[27] Cf. https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2148
[28] Cf. https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2941