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
AliasLab CryptoAccelerator, release 3.4.9

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

Confirmation issued on: 2016-06-24
Reference number: A-SIT-VI-16-048

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

CryptoAccelerator 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 CryptoAccelerator 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] and provides a secure mechanism “Security World” for storing private keys outside the HSM in a database.

The HSM device is accessed only through the CryptoManager module of CryptoAccelerator. For enrolment and 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 strong authentication methods that are provided by the modules

[1] Firmware Versions: 2.50.16-3 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

CryptoServices (authentication with PIN+OTP), CryptoServicesSMS (authentication with PIN+SMS OTP), SecureCallSign (authentication with PIN+SecureCall) and BioCryptoService (authentication with PIN+biometric signature).

A Signature Creation Application (SCA) sends the entire document to be signed or a hash value to CryptoAccelerator. CryptoClient (installed directly by the signatory) or CryptoAppliance (installed at a customer's premises) can be used as SCAs. CryptoClient and CryptoAppliance are not part of the SSCD and thus outside the scope of this confirmation.

Signature Creation Data:

The SCD/SVD key pair is generated within the HSM and the SCD is stored in encrypted form in a database ("Security World"). During the enrolment process the signatory's secret PIN is defined. To provide strong authentication four different mechanisms are used in addition to this PIN. The type of the authentication mechanism (FDR – certificate with strong authentication based on external OTP with HW token, FDS – certificate with strong authentication based on SMS OTP, FSM – certificate with strong authentication based on SecureCall or FSB - certificate with strong authentication based on biometric signature) as well as strong authentication related parameters (token serial number in case of hardware OTP token, mobile phone number in case of SMS OTP or SecureCall, biometric reference data in case of biometric signature) are stored during enrolment and bound to the SCD/SVD key pair resp. the subsequently generated certificate.

All cryptographic operations of generation, encryption and decryption of SCD are implemented within the HSM. The SCD is only accessible within the HSM after a successful authentication with the defined strong authentication method and using 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.

Strong Authentication Methods:

The SCD can only be encrypted within the HSM using the signatory's secret PIN. In addition to the PIN CryptoAccelerator always uses one out of four different mechanisms to authenticate the signatory:

- *OTP Token:* A one-time-password (OTP) mechanism using a HW-Token is used. CryptoAccelerator can be configured to address the OTP providers RSA SecureID ACE Server, Vasco Identikey Server, Vasco Vacman Controller, SafeNet-Gemalto Authentication Manager, SafeNet-Gemalto Autentication Service PCE and OATH standard based servers[3]. The signatory enters her/his secret PIN and the OTP generated by the Token into the SCA which submits the data to CryptoAccelerator.
- *SMS OTP:* An OTP code is generated using the HOTP algorithm based on the document to be signed. The OTP is sent via SMS to the signatory's mobile phone. The signatory enters her/his secret PIN and the SMS OTP into the SCA which submits the data to CryptoAccelerator.
- *SecureCall:* The signatory has to call a phone number (composed of a fixed and a variable part) with her/his registered mobile phone. The variable part represents an OTP; it is unique for one transaction and only valid for a limited time-period. CryptoAccelerator verifies the OTP and signatory's mobile 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 (signature pad). The module used by CryptoAccelerator is based on the SoftPro/Kofax biometric compare engine and uses static (image) as well as dynamic (pressure, acceleration, speed) comparison of the captured signature with a specimen that has been recorded during enrolment. The signatory enters her/his secret PIN on the signature pad and subsequently writes her/his signature on the pad. PIN and biometric signature data are submitted to CryptoAccelerator. The authentication process can only be performed with pre-

[3] Note: Vasco and Safenet-Gemalto OTP tokens also support the OATH standard

registered signature pads in a controlled environment, such as an operator seat in a branch or agency. The operator must identify the signatory and must be present during signature operation. To prevent the reuse of a captured biometric signature CryptoAccelerator calculates a hash of each signature and checks it against a history database.

Signature Generation:

The signature process is structured as follows:

- CryptoAccelerator authenticates the signatory according to the predefined strong authentication method.
- Signatory's User-ID, Certificate-ID, the hash value of the document to be signed and the secret PIN provided by the signatory are submitted to the HSM.
- The associated SCD is loaded from the database into the HSM.
- The PIN provided by the signatory is used to decrypt the SCD inside the HSM.
- In case of a successful verification of all the authentication parameters, the signature is generated within the HSM. In case of automatic signatures a group of documents can be signed with one authentication.

2. Compliance with the Requirements of SigG[4] and SigV[5]

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[6]
- requirements laid down in § 6 para. 3 SigV[7]

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

[5] 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

[6] 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)

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

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[8],
- 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[9]) 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, 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 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[10] 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 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 SSCD is not installed 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 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 SSCD is deployed.

(4) The HSM must be initialised and operated in FIPS 140 level 3 mode.

(5) 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.

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

[8] § 12 SigV defines the minimum content of the CSP's security- and certification policy

[9] 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*;'

[10] Defined in CryptoAccelerator Security Target, Security Objectives for the Operational Environment

5. Algorithms and Corresponding Parameters

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

- 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.

For the calculation of hash values the following algorithm is supported[11]:

- SHA-256 (corresponds to SigV Annex, table 2, index number 2.04)

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

6. Assurance Level and Strength of Mechanism

For the used HSM (Thales - nCipher nShield Solo/Solo+ or nShield Connect/Connect+, firmware versions 2.50.16-3 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 2014-05-13 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 HSM with 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[12].

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-16-048.

Authorized Signature:

SIGNATURE INFORMATION	**Signatory**	Reinhard Posch
	Date/Time-UTC	2016-06-24T10:41:20+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 § 4 art. 1 of the Signature Act.	

[11] Hash value calculation may also be performed outside of the SSCD by the SCA.
[12] Vulnerability Assessment – Advanced methodical vulnerability analysis