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
Protect & Sign Personal Signature, version 4.1

Applicant:
DocuSign France (owning the brand OpenTrust),
175 rue Jean-Jacques Rousseau
92130 Issy-les Moulineaux, France

Confirmation issued on: 2015-12-03
Reference number: A-SIT-1.117

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

Protect & Sign Personal Signature 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 Protect & Sign Personal Signature generates qualified electronic signatures as defined in Directive 1999/93/EC with the legal effects of article 5 para. 1.

Subcomponents:

An HSM device (SafeNet Luna® PCI-e Cryptographic Module[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 component HSS interacts with the HSM through the PKCS#11 protocol. The HSS component is dedicated to the Protect & Sign Core Application and cannot be used by other applications.

The Protect & Sign Core Application interacts with the remote environment (signatory, calling application, SMS gateway provider, certification authority, time stamping authority) through a web interface.

[1] Firmware version: 6.2.1, used as standalone device or as embedded device in Luna® SA
[2] http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1694.pdf

Signature Creation Data:

The SCD/SVD key pair is generated within the HSM. For each signature-transaction a new key pair is generated and a new Certificate Signing Request (CSR) is signed by the HSM and transmitted to a certification authority (the process of issuing qualified certificates is outside the scope of this confirmation). After each signature-transaction the SCD is destroyed by 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 within the HSM after a successful authentication process with the defined Signature Activation Protocol (SAP). Signing interaction with the signatory is performed using a web page presented to the signatory via a web interface. 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 an OTP to the signatory's registered mobile phone. The SSCD generates the OTP and associates it with the signatory and signatory's key pair. The OTP is then sent to the signatory through an SMS Gateway Provider.

Signature Generation:

The signature process is structured as follows:

- A calling application, considered as a trusted source, first identifies and authenticates the signatory as a Registration Authority (RA), generates and shows to the signatory the document to be signed and then transmits the document (or a hash value of the document) as well as signatory's identity and phone number within a signed signature request to the Protect & Sign Core Application. The calling application and the RA procedures are outside the scope of this confirmation.
- The Protect & Sign Core Application creates a unique Token ID dedicated to the transaction and sends this Token ID back to the calling application to be used for the SAP with the signatory.
- The signatory connects to the Token ID (e.g. by redirection through a pre-existing https-session between the calling application and the signatory) using a TLS connection.
- The SAP web page is pushed to the signatory via the TLS connection.
- The Protect & Sign Core Application creates a unique, temporary and random OTP code using a random number generated by the HSM, stores the SHA-2 hash value of the OTP code in a database and transmits the OTP code and signatory's SAP-information (phone number) to the SMS Gateway provider. The SMS Gateway provider transmits the SMS with the OTP to the signatory's phone.
- In the SAP web page the signatory checks the document to be signed or the reference to the document to be signed. If the signatory agrees to sign, the check boxes to approve the legal notices written in the SAP web page must be clicked, and then the signatory fills in the OTP code and clicks the "Sign" button.
- Protect & Sign Core Application verifies the code received in the SAP Web Page against the SHA-2 of the OTP code in the database, a maximum of three attempts is allowed. If the code corresponds to the SHA-2 of the OTP code, the Protect & Sign Core Application requests the generation of the key pair inside the HSM. A CSR for the public key is generated and signed by the HSM.
- The Protect & Sign Core Application sends the CSR and signatory ID information to be set in the certificate to the CA and the CA generates a certificate for the signatory and sends it back to the Protect & Sign Core Application. (The process of issuing qualified certificates is outside the scope of this confirmation). The Protect & Sign Core Application also gets the CRL to verify the status of signatory's certificate.
- When the calling application has sent the entire document to be signed the Protect & Sign Core Application calculates the hash value (SHA-256) of the document. Otherwise the hash value is calculated by the calling application and transmitted to the Protect & Sign Core Application.
- The hash value is signed inside the HSM using the SCD and the signed hash value is returned to the Protect & Sign Core Application.

- The HSM destroys the SCD using its certified key-destruction function.
- The Protect & Sign Core Application requests a time stamped token at the Time Stamping Authority (TSA) and the TSA responds with a time stamped token. (The TSA processes are outside the scope of this confirmation).
- When the calling application has sent the entire document the Protect & Sign Core Application constructs the signed document with the signed hash value, the time stamped token and the CRL. Otherwise the signed document is constructed by the calling application.
- When the calling application had sent the entire document the Protect & Sign Core Application sends the signed document back to the signatory, otherwise the signature of the document is sent back to the calling application.
- The Protect & Sign Core Application generates a "Proof File" associated to the signature transaction. This file contains the audit trail provided during the operation of the SAP (client request, document resp. document-reference presented to the signatory in the SAP web page, signed document resp. signature of the document and the time and description of each operation). The Proof File is signed using a dedicated proof-file signature key within the HSM and time stamped using the TSA. The Proof File is stored encrypted (using a dedicated proof-file encryption key within the HSM) in the file storage.

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 for a period of two years from the date of issue.

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],
- integrated into the guidance of the signatory and
- their effect shall be ensured by means of supervision.

[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

(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 (mobile phone, web browser) must be suitable protected.

(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 web servers used for Protect & Sign Core Application and HSS are configured only with authorized certificates to validate the SSL/TLS connections.
- Owners of trusted roles for the administration of SSCD components shall be authenticated using private keys stored on certified tokens.
- Employees holding trusted roles shall meet the personnel requirements defined in ETSI TS 102 042.
- Physical and IT security used to host and operate the SSCD components shall be compliant with ETSI TS 102 042.
- The HSM must be initialised and operated in FIPS 140 level 3 mode.
- In order to guarantee dual control at least two distinct persons shall be used as HSM activation data holders to configure the HSM and the partition inside the HSM used for the SCD as well as for the HSS roles partition master secret (to manage the partition configuration and create the HSS master key) and partition administrator (to manage the HSM partition password that is encrypted with the HSS master key).
- Before a customer is authorized to use the SSCD to deliver qualified signatures, the customer acting as a registration authority shall be checked as compliant with the TSP's Certificate Policy and Certificate Practice Statement (based on ETSI TS 101 456 QCP) and a contract shall be signed by the customer to bind the customer to the Certificate Policy and TSP's signature policy obligation.
- As a registration authority the customer shall authenticate the signatory in order to collect signatory ID and signatory SAP information (phone number) according to ETSI TS 101 456 QCP subscriber registration requirements.
- When the calling application computes the hash of the document to be signed by the signatory, the calling application shall use a secure hash algorithm (SHA-2 minimum).
- The Proof File can be collected by the customer through the Protect & Sign API, and shall be archived by the customer for at least five years according to OpenTrust's Certificate Policy in order to be compliant with ETSI TS 101 456.
- Technical certificates used by the calling application are enrolled by a TSP with a level equivalent to ETSI TS 102 042 LCP.

(3) 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 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 length of 2048 bits.

[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*;'
[9] Defined in Protect & Sign SSCD Compliance, SSCD Environment General Overview

For the calculation of hash values the following algorithm is supported[10]:

- 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 (SafeNet Luna® PCI-e Cryptographic Module, firmware version 6.2.1, used as standalone device or as embedded device in Luna® SA) the FIPS Validation Certificate No. 1694 applies, issued on 2012-03-30 by the US (National Institute of Standards and Technology) and the Canadian (Communications Security Establishment) FIPS 140-2 certification body. The certificate confirms that the HSM was successfully evaluated against FIPS 140-2 level 3.

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-1.117.

Authorized Signature:

	Signatory	Reinhard Posch
	Date/Time-UTC	2015-12-03T17:53:32+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 § 4 art. 1 of the Signature Act.	

[10] Hash value calculation may also be performed outside of the SSCD by the calling application.