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 Creation Device (QSCD)
Protect & Sign, version 4.18

Applicant:
DocuSign France,
9-15 Rue Maurice Mallet
92130 Issy-les-Moulineaux
France

QSCD-Certificate issued on: 2017-12-20
Reference number: A-SIT-VIG-17-069

1. Product Description

Protect & Sign is a product for qualified electronic signatures intended to be used as a remote Qualified Electronic Signature Creation Device (QSCD) in the secure operational environment of a qualified trust service provider (TSP). When used in combination with qualified certificates Protect & Sign generates qualified electronic signatures as defined in eIDAS with the legal effects of Article 25.

Subcomponents:

Two particular types of HSM devices are used as cryptographic modules for the generation and the protection of the signature creation data (SCD). The HSMs are operated according to their FIPS 140-2 level 3 certification in conjunction with the corresponding security policies. The QSCD can use the following HSMs:

- Safenet Luna® SA5, Luna® SA6 and Luna® PCI-e K6[2]
- DocuSign HSM Appliance, version 5.0[3]

[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: 6.2.1, 6.2.5, 6.3.1, 6.10.4, 6.10.7, 6.10.9, 6.11.2; Hardware Versions: VBD-05 Version Code 0100, VBD-05 Version Code 0101, VBD-05 Version Code 0103. Manufacturer: Safenet Inc., now integrated into Gemalto N.V. Strozzilaan 382, 1083 HN Amsterdam, Netherlands

[3] Firmware Versions 5.0.0 and 5.0.2; Manufacturer: DocuSign Inc., 221 Main St., Suite 1000, San Francisco, CA 94105, USA

The component HSS (Crypto Server) 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.

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 Creation:

There are two different processes for creating qualified electronic signatures with Protect & Sign:

(1) Electronic signature transactions without the DocuSign TSP interface using the Protect & Sign API
(2) Electronic signature transactions with DocuSign TSP interface

The signature process is structured as follows:

- Process (1): A calling application, considered as a trusted source, first identifies and authenticates the signatory as a Registration Authority (RA)[4], 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 SAP information (phone number) within a signed signature request to the Protect & Sign Core Application.
  Process (2): A calling application creates the document to be signed (transmitted by RA), collects signatory's identity and SAP information from the RA. The signatory can be either in face to face relation with the RA or in remote connection with the calling application portal. The calling application creates a DocuSign Signature Application Signatory Authorization Code and signs it. Then the calling application redirects the signatory to the Protect & Sign Core Application with the DocuSign Signature Application Signatory Authorization Code. The DocuSign Signature Application signs the client request containing signatory information, signatory SAP information and the document to be signed.
- Process (1): 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.
  Process (2): The Protect & Sign Core Application creates a unique Token ID dedicated to the transaction and sends this Token ID back to the signatory to be used for the SAP with the signatory.
- The signatory connects to the SAP web page using the Token ID (e.g. by redirection through a pre-existing https-session between the calling application and the signatory) and the requested page according to the choice of the calling application is pushed to the signatory via the TLS connection.

[4] The calling application and the RA procedures are outside the scope of this QSCD-certificate.

- The Protect & Sign Core Application creates a unique, temporary and random OTP code using a random number generated by the HSM, stores the reference value[5] 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 and all signatory's identity information (name and phone number). 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. If the signatory doesn't want to sign she can click a "Refuse" button.
- Protect & Sign Core Application verifies the code received in the SAP Web Page against the reference value of the OTP code in the database, a maximum of three attempts is allowed. If the code corresponds to the reference value, 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 or OCSP response 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).
- Process (1): Protect & Sign Core Application adds the time stamped token and the CRL or OCSP response to the signed hash value and constructs the signature of the document (without DTM[6]). When the calling application has sent the entire document the Protect & Sign Core Application constructs the signed document. Otherwise the signed document is constructed by the calling application.

  Process (2): Protect & Sign Core Application adds the time stamped token to the signed hash value and constructs the signature of the document (with DTM).
- Process (1): 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.

  Process (2): Protect & Sign Core Application sends back the signature of the document (with DTM) to the DocuSign Signature Application. The DocuSign Signature Application creates the signed document returns the return URL to Protect & Sign Core 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.

[5] PBKDF2 with HMAC-SHA256

[6] Digital Transaction Management

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[7] eIDAS,
- requirements laid down Annex II eIDAS (para 1 lit. a[8],b[9],c[10],d[11], para 2[12], para 3[13], para 4 lit a[14], b[15])

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

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

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

[8] *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*.

[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 practically occur only once.*

[10] *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.*

[11] *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.*

[12] *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.*

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

[14] *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.*

[15] *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.*

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 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 QSCD are part of the QSCD’s system environment[16] and thus outside the scope of this QSCD-certificate. 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. The signatories shall keep control of their assigned devices and shall promptly report any circumstance where a credential is compromised according to the defined revocation or suspension procedures.

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

(3) 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 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 EN 319 401.
- Physical and IT security used to host and operate the SSCD components shall be compliant with ETSI EN 319 401.
- HSMs must be initialised and operated according to their FIPS 140-2 level 3 resp. Common Criteria EAL4+ certification. 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 QSCD 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 EN 319 411-2 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) meeting the requirements defined in eIDAS Article 24 para 1 and the customer shall be audited against ETSI EN 319 411-2 QCP, ETSI EN 319 411-1 and ETSI EN 319 401 for those requirements that apply to an external registration authority.
- 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 (at least SHA-256).
- The proof file shall be archived by the customer or by DocuSign France for at least 7 years and 15 days according DocuSign France’s CP in order to be compliant with ETSI EN 319 411-2.
- Technical certificates used by the calling application are enrolled by a TSP with a level equivalent to ETSI EN 319 411-1 (LCP).

[16] in accordance with recital 56 of eIDAS

5. Algorithms and Corresponding Parameters

For the creation of qualified electronic signatures the QSCD uses the cryptographic algorithm

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

For the calculation of hash values the algorithm SHA256 is supported[17].

6. Assurance Level and Strength of Mechanism

For the used HSMs the following FIPS 140-2 Validation Certificates apply:

- Safenet Luna® SA5, Luna® SA6 and Luna® PCI-e K6: The FIPS Validation Certificates issued 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 HSMs were successfully evaluated against FIPS 140-2 level 3:
  - Certificate #2489 issued on 2015-12-15 and last renewed on 2017-11-20 for Luna® PCI-E Cryptographic Module and Luna® PCI-E Cryptographic Module for Luna® SA; Firmware Versions: 6.10.7, 6.10.9 and 6.11.2,; Hardware Versions: VBD-05-0100, VBD-05-0101 and VBD-05-0103
  - Certificate #2481 issued on 2015-02-12 and last renewed on 2017-06-23 for Luna® PCI-e Cryptographic Module; Firmware Versions 6.2.1 and 6.2.5; Hardware Versions: VBD-05-0100, VBD-05-0101 and VBD-05-0103
  - Certificate #2428 issued on 2015-08-11 and last renewed on 2017-06-23 for Luna® PCI-E Cryptographic Module and Luna® PCI-E Cryptographic Module for Luna® SA; Firmware Versions 6.10.4, 6.10.7 and 6.10.9; Hardware Versions: VBD-05-0100, VBD-05-0101, VBD-05-102 and VBD-05-0103
  - Certificate #1694 issued on 2012-03-30 and last renewed on 2017-06-23 for Luna® PCI-e Cryptographic Module; Firmware Version 6.2.1; Hardware Versions VBD-05-0100, VBD-05-0101 and VBD-05-0103

- DocuSign HSM Appliance: The FIPS Validation Certificate No. 2860 issued on 2017-03-08 and last renewed on 2017-10-03 by the US and the Canadian FIPS 140-2 certification body applies (Firmware Versions: 5.0.0 and 5.0.2; Hardware Version: 5.0). The certificate confirms that the HSM was 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-17-069.

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

Authorized Signature:

A-SIT Secure Information Technology Center – Austria

Vienna, (Date see electronic signature)

SIGNATURE INFORMATION	Signatory	Reinhard Posch
	Date/Time-UTC	2017-12-20T09:57:20+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