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 4.67

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

QSCD-Certificate issued on: 2019-12-06
Reference number: A-SIT-VIG-19-070

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) which is operated 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.

Signatory Interaction:
The interaction with the Signatory is provided by 2 distinguished use cases:

The first use case (i.e., TOE SAP) provides the interaction via the Protect and Sign (which is called Signature Activation Protocol (SAP)) application to generate, manage, protect and execute the signing of private keys.

The second use case (i.e., delegated SAP) provides the signatory interaction via the Registration Authority (RA) with its calling application to run its own SAP to generate, manage, protect and execute the signing of private keys.

Subcomponents:

Two particular types of Hardware Security Modules (HSMs) devices are used as cryptographic modules for the generation and the protection of the Signature Creation Data (SCD). The HSMs

[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

are operated according to their issued FIPS 140-2 level 3 certification in conjunction with the corresponding security policies. The QSCD can use the following HSMs:

- Luna®/SafeNet PCI-e K6[2,3] (Version 6.10.7) or newer hardware and software certified version.
- DocuSign HSM Appliance, FIPS 140-2 level 3, version 5.0.2[4] or newer certified version.

The component HSS (Crypto Server) interacts authenticated with the HSM via the PKCS#11 protocol. The HSS component is authenticated and dedicated to the Protect & Sign core application via TLS and it cannot be used by other applications.

The Protect & Sign core application interacts with the remote environment (signatory, calling application[5], SMS gateway provider, Certification Authority – CA, time stamping authority – TSA) through a web interface.

Signature Creation Data:

The SCD[6]/SVD[7] key pair is generated inside of 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 inside of the HSM after a successful authentication process with the defined Signature Activation Protocol (SAP) for both use cases (i.e., TOE SAP and delegated SAP). The 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[8] to the signatory's registered mobile phone. The QSCD generates the OTP and associates it with the signatory and the signatory's key pair. The OTP is then sent to the signatory via the SMS gateway provider.

Signature Creation:

There are two varying processes for creating qualified electronic signatures with Protect & Sign for each use case (i.e., TOE SAP and delegated TOE):

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

(2) Electronic signature transactions with the 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)[9], generates and shows to the

[2] Firmware Versions: 6.10.7, 6.10.9, and 6.11.2; Hardware Versions: VBD-05-0100, VBD-05-0101, VBD-05-0103; FIPS validation certificate #2489; Manufacturer: SafeNet Assured Technologies, LLC., Suite D, 3465 Box Hill Corporate Center Drive, Abingdon, Maryland 21009 (now integrated into Gemalto, a Thales Company)

[3] Firmware Versions: 6.24.6 [1] and 6.24.7 [2]; Hardware Versions: VBD-05-0100 [1, 2], VBD-05-0101 [1, 2], VBD-05-0102 [1, 2] and VBD-05-0103 [1, 2]; FIPS validation certificate #3268; Manufacturer: Gemalto, a Thales Company, 20 Colonade Road, Suite 200, Ottawa, ON K2E 7M6, Canada

[4] Firmware Version 5.0.2; FIPS validation certificate #2860; Manufacturer: DocuSign Inc., 221 Main St., Suite 1000, San Francisco, CA 94105, USA

[5] Annotation: The calling application can either be (1) DocuSign TSP API or (2) P&S Client

[6] SCD – Signature Creation Data

[7] SVD – Signature Validation Data

[8] OTP – One Time Password

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

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 established 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 reference value[10] 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

[10] PBKDF2 with HMAC-SHA256

(without DTM[11]). 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 or document-reference presented to the signatory in the SAP web page, signed document or 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 eIDAS

The QSCD meets the following requirements, provided that the conditions in section 4 are fulfilled:

- requirements laid down in Article 29 para 1[12] eIDAS,
- requirements laid down in 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 creation data,

[11] Digital Transaction Management

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

[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.*

- 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 or 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 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[21] 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 under the eIDAS regulation.

(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 QSCD 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 QSCD components shall be compliant with ETSI EN 319 401.
- HSMs must be initialised and operated according to their FIPS 140-2 level 3 or 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).

[21] in accordance with recital 56 of eIDAS

- 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 with QSCD) 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 with QSCD), 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 (QCP with QSCD).
- The technical certificates used by the calling application are enrolled by a TSP with a level equivalent to ETSI EN 319 411-1 (LCP).
- The TSP shall approve the terms of use (TOU) before they are configured for a customer.
- The HSM used by the TOE to manage the signatory's private key shall be configured to forbid the backup of the signatory's private key if the HSM has such a feature. If such a feature is not supported by the HSM, the TSP shall forbid any backup of the HSM in its internal procedures.

(4) The TSP shall forbid receiving e-mail in production via the SMTP relay used by the TOE for sending messages.

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[22].

6. Assurance Level and Strength of Mechanism

For the used HSMs the following FIPS 140-2 validation certificates apply:

- Luna®/SafeNet 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 HSM was successfully evaluated against FIPS 140-2 level 3:
  - Certificate #2489 issued on[23] 2015-12-15, last renewed on 2018-03-27 and with a sunset date on 2020-12-14 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 #3268 issued on 2018-08-24 and with a sunset date on 2023-08-23 for SafeNet PCIe Hardware Security Module and SafeNet PCIe Hardware Security Module for SafeNet Network HSM; Firmware Versions: 6.24.6 and 6.24.7;

[22] Annotation: The hash value calculation may also be performed outside of the QSCD by the calling application.

[23] Annotation: The first validation date was chosen.

Hardware Versions: VBD-05-0100, VBD-05-0101, VBD-05-0102 and VBD-05-0103

- DocuSign HSM Appliance: The FIPS validation certificate #2860 issued on 2017-03-08 and last renewed on 2018-04-10 by the US and the Canadian FIPS 140-2 certification body applies; Firmware Versions: 5.0.0, 5.0.2, and 5.0.3; 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.

In its intended environment the QSCD resists against attackers with high attack potential.

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-19-070.

Authorized Signature:

A-SIT Secure Information Technology Center – Austria

Vienna, (Date see electronic signature)

SIGNATURE INFORMATION	Signatory	Reinhard Posch
	Date/Time-UTC	2019-12-06T17:16:11+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