TRUST AND VERIFY

Certification Report

DocuSign QSCD for local signing version 1.2.0.7

Sponsor and developer:	***DocuSign*** **Ha'arava Str.1** **Giv'at Shmuel** **Israel**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-2300052-01-CR**
Report version:	**1**
Project number:	NSCIB-**2300052-01**
Author(s):	**Wim Ton**
Date:	**30 January 2024**
Number of pages:	**13**
Number of appendices:	**0**

Reproduction of this report is authorised only if the report is reproduced in its entirety.

CONTENTS

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TrustCB B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TrustCB B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TrustCB B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TrustCB B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

Recognition of the Certificate

Presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the DocuSign QSCD for local signing version 1.2.0.7. The developer of the DocuSign QSCD for local signing version 1.2.0.7 is DocuSign located in Giv'at Shmuel, Israel and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The DocuSign QSCD is a digital signature product intended to be used as a local Qualified Signature/Seal Creation Device (QSigCD or QSealCD) in a secure operational environment.

The DocuSign QSCD Appliance is a network attached Appliance consisting of computer hardware, hardware for tamper resistance, hardened operating system, internal database and the Appliance server software.

The threat environment the TOE is designed for is one of high threat of network compromise, and low threat of physical compromise (for example, a Certification Authority facility with a high degree of physical protection, but an operational requirement to be connected to an untrusted network such as the internet).

The environment is assumed to prevent prolonged unauthorised physical access to the TOE (including theft).

The evaluation of the TOE has been conducted by SGS Brightsight B.V and was completed on 2024-01-30 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the DocuSign QSCD for local signing version 1.2.0.7, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the DocuSign QSCD for local signing version 1.2.0.7 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality. This assurance level is augmented with AVA_VAN.5 (Advanced methodical vulnerability analysis).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TrustCB B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the DocuSign QSCD for local signing version 1.2.0.7 from DocuSign located in Giv'at Shmuel, Israel.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	DocuSign QSCD Appliance	2.0.0.0
Software	DocuSign QSCD for local signing	1.2.0.7

To ensure secure usage a set of guidance documents is provided, together with the DocuSign QSCD for local signing version 1.2.0.7. For details, see section 2.5 "Documentation" of this report.

2.2 Security Policy

The TOE is a digital signature product intended to be used as a local Qualified Signature/Seal Creation Device (QSigCD or QSealCD).

The TOE creates digital signatures, using RSA with a modulus size of 2048, 3072, and 4096 bits.

The TOE securely generates, stores, and destroys keys for signing. Signing keys are assigned by the "SSA admin" to dedicated users, "Signers"

The TOE uses RBAC, with the roles of:

- Appliance Administrator
- Users Administrator
- SSA Admin (signer administrator)
- Signer

The TOE authenticates a signing request before executing it.

The TOE uses TLS to communicate securely with all external systems.

The TOE logs relevant events to an external server.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the *[ST]*.

2.3.2 Clarification of scope

Note that EN 419221-5 Protection Profile [EN419221-5] claims the environment for the TOE protects against loss or theft of the TOE, deters and detects physical tampering, protects against attacks based on emanations of the TOE, and protects against unauthorised software and configuration changes on the TOE and the hardware appliance in which it is contained ("OE.Env Protected operating environment").

The ST follows the PP and also claims OE.Env, thus the environment in which the TOE is used must ensure the above protection.

Any threats violating these objectives for the environment are not considered.

2.4 Architectural Information

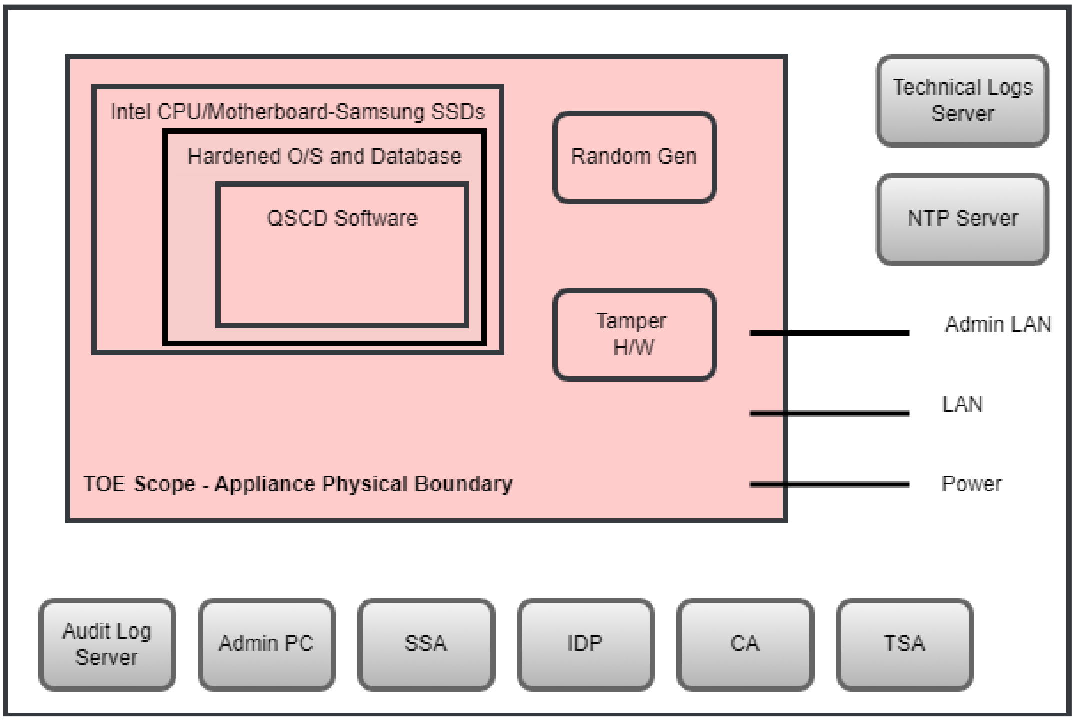

Figure 1 TOE boundary

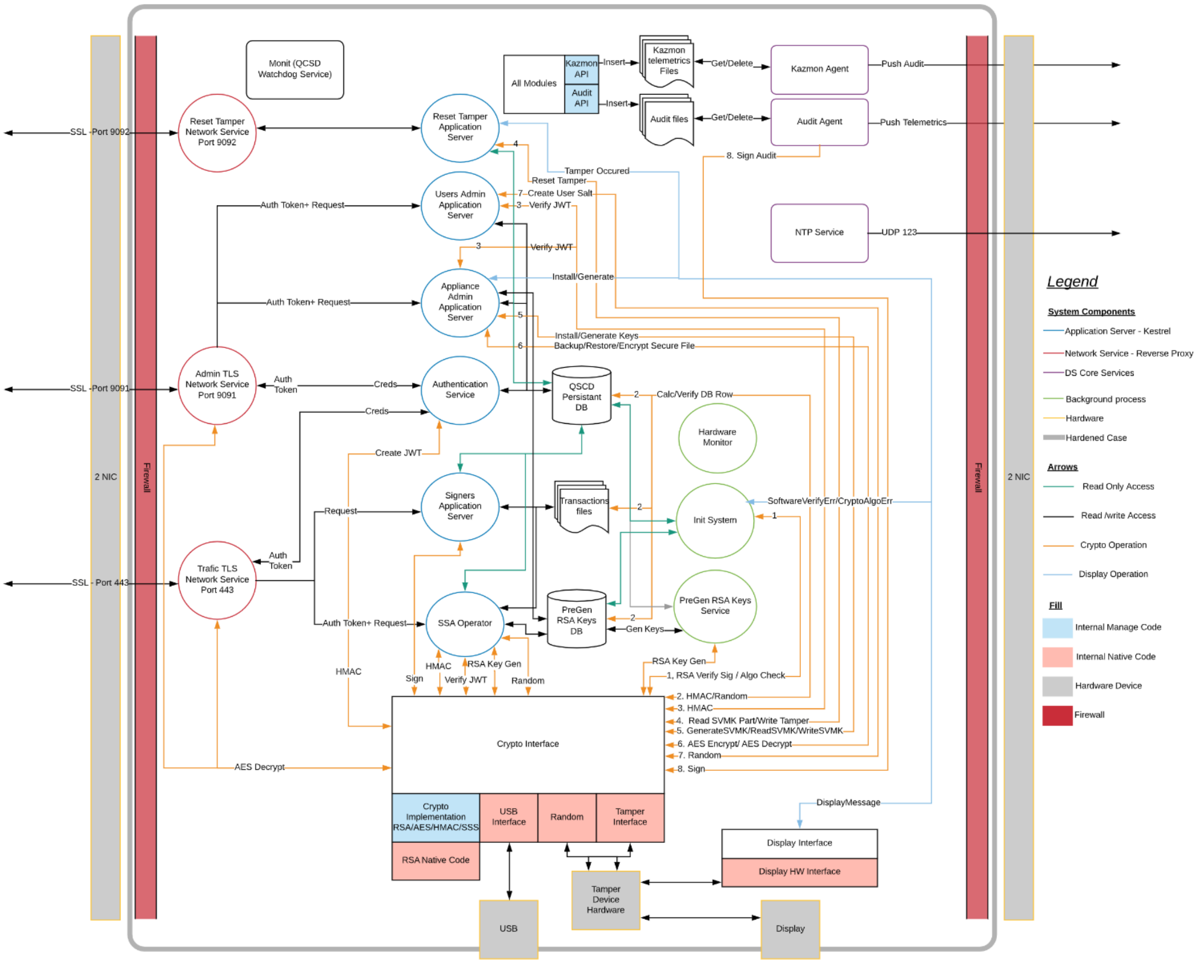

Figure 2 Logical architecture of the TOE.

The TOE is a network attached appliance consisting of computer hardware, hardware for tamper resistance and random number generation, a hardened operating system, an internal database, and the appliance server software.

2.5 *Documentation*

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
DocuSign QSCD Appliance Administrator Guide Version	1.2.0.7
DocuSign QSCD Appliance Developer Guide Version	1.2.0.7
QSCD Appliance Preparative Procedures Administrator Guide Version	1.2.0.7

2.6 *IT Product Testing*

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer’s testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

Automatic test cases performed by the developer include both positive and negative tests that are performed for all the TSFIs. Both negative tests and positive tests include the validation step of verifying the test purpose. In particular, the test approach for negative tests contains the following:

- Test the command with the incorrect parameters
- Test the command by sending it to the incorrect URI
- Test the command with an incorrect/expired token
- Test the TOE via sending multiple commands at the same time

Manual test cases cover the TOE physical interfaces and interfaces that have not been tested via the automatic tests.

The evaluators witnessed a selection of the developer tests, as well as execution of a small number of test cases designed by the evaluator

5 automated developer tests for the parts of the TOE that where changed since the last evaluation and that are relevant for security, are repeated by the evaluator.

The evaluator created additional test cases to confirm the version of the TOE and for the new features of the TOE:

- JWT in addition to the existing SAML format for authentication and signing.
- Increased the possible number of key-shares for the master key.
- Updates to the network interfaces
- The TOE restarts after the temperature returns to the allowable range.

2.6.2 Independent penetration testing

The penetration testing concentrated on the new JWT interface.

The total test effort expended by the evaluators was 2 weeks. During that test campaign, all of the total time was spent on software attacks. 50% was spent on existing penetration tests, 50% on new penetration tests.

2.6.3 Test configuration

The tests are executed on the TOE in a normal operational state:

- The TOE is not tampered.
- The TOE is the production version.
- The TOE is in operational mode.

Several instances of the TOE (in the configuration as specified in 2.1) were used in parallel to speed up the test program.

The tests were performed at the developer’s premises and the evaluator witnessed the tests remotely.

2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer’s tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

2.7 Reused Evaluation Results

Documentary evaluation results of the earlier version of the TOE have been reused, but vulnerability analysis and penetration testing has been renewed.

Test designs of the earlier version of the TOE have been reused, but additional test cases to confirm the version of the TOE and for the new features of the TOE have been added.

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by reuse of the audit report *[SITE-AUDIT]* of the previous evaluation.

No sites have been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number DocuSign QSCD for local signing version 1.2.0.7.The user can see the hardware- and software version of the TOE on the LCD display on the front of the TOE hardware and in the response to the connect request.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents, and the Site Audit Report *[SITE-AUDIT]*.

The verdict of each claimed assurance requirement is “**Pass**”.

Based on the above evaluation results the evaluation lab concluded the DocuSign QSCD for local signing version 1.2.0.7, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with AVA_VAN.5**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims strict conformance to the Protection Profile *[PP]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 “Documentation” contains necessary information about the usage of the TOE. Certain aspects of the TOE’s security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: **none**

3 Security Target

The DocuSign QSCD for local signing Security Target, Version 4.3.8, 5 October 2023 *[ST]* is included here by reference.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

ACL	Access Control List
AES	Advanced Encryption Standard
BAC	Basic Access Control
CA	Certification Authority
CBC	Cipher Block Chaining (a block cipher mode of operation)
DTBS	Data To Be Signed
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
EMA	Electromagnetic Analysis
eMRTD	electronic MRTD
GCM	Galois Counter Mode
IDP	Identity Provider
IPS	Intrusion Prevention Systems I
JIL	Joint Interpretation Library
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
JWT	Java Web Token
LCD	Liquid Crystal Display
MAC	Message Authentication Code
MRTD	Machine Readable Travel Document
NSCIB	Netherlands Scheme for Certification in the area of IT Security
NTP	Network Time Protocol
PACE	Password Authenticated Connection Establishment
PKI	Public Key Infrastructure
PP	Protection Profile
PUK	PIN Unblocking Key
QSCD	Qualified Signature/Seal Creation Device
RBAC	Role Based Access Control

RNG	Random Number Generator
RMI	Remote Method Invocation
RSA	Rivest-Shamir-Adleman Algorithm
SAD	Signature Activation Data
SAM	Signature Activation Mode.
SCA	Signature Creation Application
SCD	Signature Creation Device
SCP	Secure Channel Protocol
SHA	Secure Hash Algorithm
SM	Secure Messaging
SPA/DPA	Simple/Differential Power Analysis
SSA	Server Signing Application
SSD	Solid State Disk
SVD	Signature Verification Device
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TRNG	True Random Number Generator
VLAN	Virtual LAN

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[PP]	EN 419 221-5:2018, Protection Profiles for TSP Cryptographic Modules – Part 5 Cryptographic Module for Trust Services, v1.0, registered under the reference ANSSI-CC-PP-2016/05-M01, 18 May 2020
[ETR]	Evaluation Technical Report “DocuSign QSCD for local signing version 1.2.0.7" – EAL4+, 23-RPT-1200, Version 5.1, 30 January 2024
[JIL-AAPHD]	Application of Attack Potential to Hardware Devices with Security Boxes, Version 3.0, July 2020
[SITE-AUDIT]	Site Audit Checklist / Report DocuSign Israël, 22-RPT-881, Version 4.0, 23 January 2023
[JIL-AMHD]	Attack Methods for Hardware Devices with Security Boxes, Version 3.0, February 2020 (sensitive with controlled distribution)
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[ST]	DocuSign QSCD for local signing Security Target, Version 4.3.8, 5 October 2023

(This is the end of this report.)