Certification Report

DocuSign QSCD for local signing version 1.1.5.5

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-0647974-CR**

Report version: **1**

Project number: **0647974**

Author(s): **Denise Cater**

Date: **25 January 2023**

Number of pages: **11**

Number of appendices: **0**

Head Office:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Netherlands Chamber of Commerce (KVK), under number 27288788.

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

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, TÜV Rheinland Nederland 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 TÜV Rheinland Nederland 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 TÜV Rheinland Nederland 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, TÜV Rheinland Nederland 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.

Recognition of the Certificate

The 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 1.1.5.5. The developer of the DocuSign QSCD for local signing version 1.1.5.5 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 TOE is a digital signature product intended to be used as a Qualified Signature Creation Device (QSCD) in a secure operational environment, to be used in Use Case 1: Local signing as defined in *[EN 419221-5]*. Any reference to QSCD in this report should be understood to refer to both qualified signature and seal creation devices.

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 TOE is the whole DocuSign QSCD Appliance.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 25 January 2023 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 1.1.5.5, 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 1.1.5.5 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 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).

TÜV Rheinland Nederland 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 1.1.5.5 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	2.0.0.0
Software	DocuSign QSCD	1.1.5.5

To ensure secure usage a set of guidance documents is provided, together with the DocuSign QSCD for local signing version 1.1.5.5. For details, see section 2.5 "Documentation" of this report.

2.2 Security Policy

The TOE provides the following security features:

- The TOE is designed for is one of high threat of network compromise, and low threat of physical compromise. The environment is assumed to prevent prolonged unauthorised physical access to the TOE (including theft).
- The TOE provides physical protection mechanisms to deter undetected compromise of its security functions by low attack potential individuals that do have physical access to the TOE.
- The TOE is responsible for protecting the keys against logical attacks that would result in disclosure, compromise and unauthorised modification, and for ensuring that the TOE services are only used in an authorized way.
- Client applications request cryptographic functions from the TOE, typically using a key managed by the TOE, once the appropriate authorization has been provided. **Note**: Only after the signer is authorized to use his/her signature key, the signature key is allowed for signing. Besides signatures keys all other keys are support keys.

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

The logical architecture, originating from *[ST]* is depicted as follows:

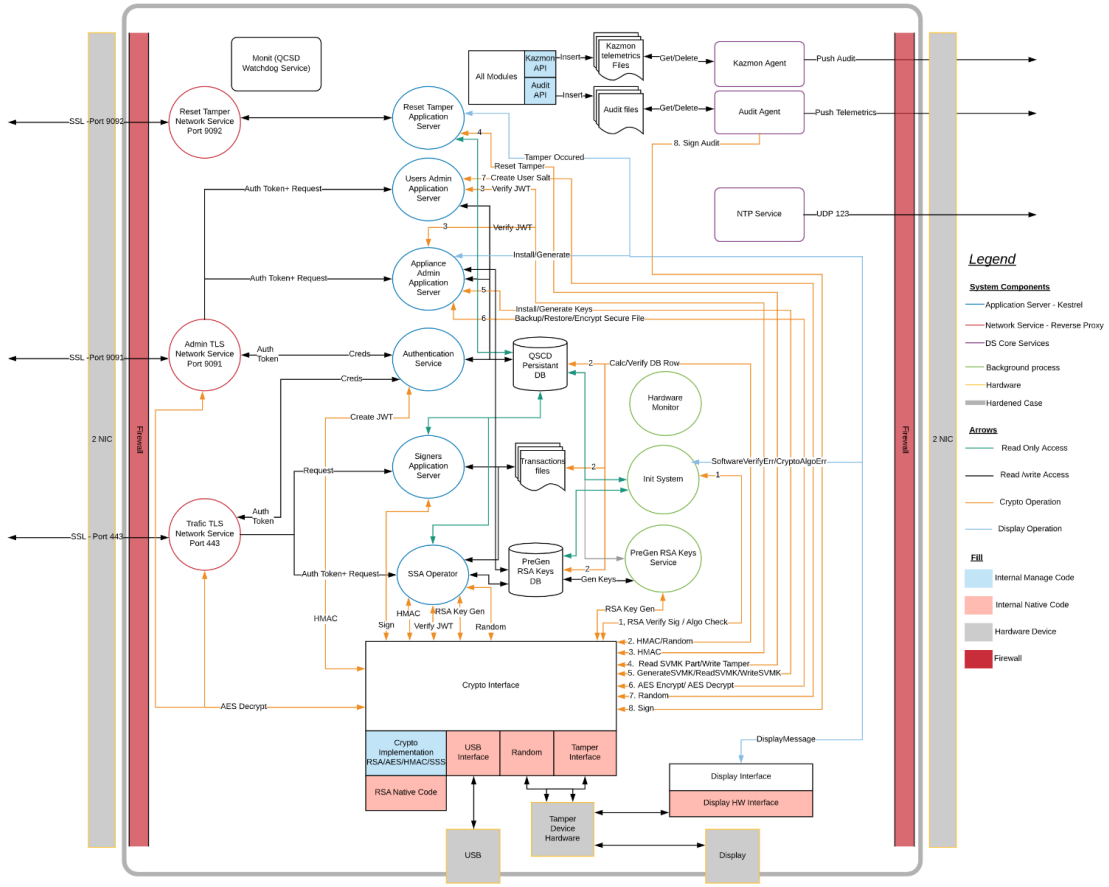

Figure 1. Logical architecture of the TOE

2.5 Documentation

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

Identifier	Version
QSCD Appliance Preparative Procedures Administrator Guide	Version 1.1.5.5
DocuSign QSCD Appliance Administrator Guide	Version 1.1.5.5
DocuSign QSCD Appliance Developer Guide (delivered as compressed archive “REST API List 1.1.5.5.rar”)	Version 1.1.5.5

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 (both automatic and manual test cases), as well as execution of a small number of test cases designed by the evaluator.

2.6.2 Independent penetration testing

The vulnerability analysis consists of two phases. In the first phase, a flaw hypothesis is created by collecting possible vulnerabilities. For the collection of possible vulnerabilities a methodical approach is taken, which consists of:

- A collection of possible vulnerabilities in Design Assessment
- Using applicable attack lists, including consideration of *[JIL-AMHD]*
- Public vulnerability search

Each possible vulnerability was then investigated and if there is no clear and direct argumentation why this possible vulnerability is not applicable, it is transformed in the second phase into a potential vulnerability. Each potential vulnerability is investigated in more detail and either a penetration test is created to further explore the issue or the rationale for closure was reported.

The total test effort expended by the evaluators was 10 days. Due to the restrictions on physical attacks imposed by *[EN 419221-5]* the penetration test campaign was focused on logical tests.

2.6.3 Test configuration

All developer automated tests were executed on the TOE version as reported in section 2.1 above, namely:

- SW: 1.1.5.5
- HW: 2.0.0.0

Some developer manual testing was performed on an earlier version of the TOE SW. The assurance gained from testing on an earlier version has been assessed to be valid for the final TOE version, because the changes introduced did not impact the tested functionality.

The evaluator testing was performed using the TOE version as reported in section 2.1 above, namely:

- SW: 1.1.5.5
- HW: 2.0.0.0

Some of the tests were performed in the TOE configuration “Local Server Signing”, as specified in *[ST]*. The remainder of the tests were performed with the TOE in the associated configuration “Remote signing”. The differences in the configuration of the TOE did not affect the tested functionality and it was concluded that the testing was equally applicable to the TOE configured as specified in *[ST]*.

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 (as certified with the certificate identifier CC-21-0388535), but vulnerability analysis and penetration testing has been renewed.

There has been reuse of the ALC aspects for the sites involved in the development of the TOE certified with the certificate identifier CC-21-0388535, although the site audit results were refreshed through a remote audit.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number DocuSign QSCD for local signing version 1.1.5.5.

2.9 Evaluation Results

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

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 1.1.5.5, 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 Profiles *[EN 419221-5]*.

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 4.1.6, 05 December 2022 *[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:

DTBS/R	Data To Be Signed / Representation to be signed
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
QSCD	Qualified Signature/Seal Creation Device
SAD	Signature Activation Data
SAP	Signature Activation Protocol
SVD	Signature Verification Data
TOE	Target of Evaluation

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
[EN419221-5]	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 1.1.5.5" – EAL4+, 22-RPT-1252, v3.0, 24 January 2023
[EU-REG]	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
[JIL-AAPHD]	Application of Attack Potential to Hardware Devices with Security Boxes, Version 3.0, July 2020
[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 2.5, 28 March 2019
[ST]	DocuSign QSCD for local signing Security Target, Version 4.1.6, 05 December 2022

(This is the end of this report.)