Certification Report

SOMA-c016 Machine Readable Electronic Document eIDAS QSCD Application, version 4

Sponsor and developer: ***HID Global S.p.A.***
Viale Remo De Feo 1
80022 Arzano (NA)
Italy

Evaluation facility: ***SGS Brightsight B.V.***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-CC-2200047-01-CR**

Report version: **2**

Project number: NSCIB-**2200047-01**

Author(s): **Kjartan Jæger Kvassnes**

Date: **18 April 2024**

Number of pages: **13**

Number of appendices: **0**

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 SOMA-c016 Machine Readable Electronic Document eIDAS QSCD Application, version 4. The developer of the SOMA-c016 Machine Readable Electronic Document eIDAS QSCD Application, version 4 is HID Global S.p.A. located in Naples, Italy 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 Target Of Evaluation (TOE) is the integrated circuit chip NXP N7121 with IC Dedicated Software and Crypto Library, the operating system SOMA-c016 and with an eIDAS Qualified Signature Creation Device (QSCD) application providing signature features and encrypted data decipherment feature. The signature features are compliant with the eIDAS Regulation (EU) No 910/2014 and the according Commission Implementing Decision (EU) 2016/650, repealing the European Parliament Directive 1999/93/EC. The eIDAS QSCD application can optionally be configured as a PKCS #15 application.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 10 November 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 SOMA-c016 Machine Readable Electronic Document eIDAS QSCD Application, version 4, 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 SOMA-c016 Machine Readable Electronic Document eIDAS QSCD Application, version 4 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 EAL5 augmented (EAL5+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures) and 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.

The TOE is stated as a Qualified Signature Creation Device and Qualified Seal Creation Device for the purposes of electronic identification and trust services as detailed by the [EU-REG]. The evaluation by SGS Brightsight included an examination of the TOE according to the eIDAS Dutch Conformity Assessment Process Version 6 0.

TrustCB B.V., as the Dutch eIDAS-Designated Body responsible in The Netherlands for the assessment of the conformity of qualified electronic signature and/or qualified electronic seal creation devices declares that the evaluation meets the conditions for eIDAS certification for listing on the EU eIDAS compiled list of Qualified Signature/Seal Creation Devices.

This document was re-issued as version 2 on 18 April 2024 to add the eIDAS assessment details.

[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 SOMA-c016 Machine Readable Electronic Document eIDAS QSCD Application, version 4 from HID Global S.p.A. located in Naples, Italy.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	NXP secure Smart Card controller N7121 with IC Dedicated Software and Crypto Library registered under BSI-DSZ-CC-1136-V3-2022	Release B1
Software	IC Dedicated Test Software (included in the scope of the HW certification BSI-DSZ-CC-1136-V3-2022)	Release 9.2.3
	IC Dedicated Software and Crypto Library (included in the scope of the HW certification BSI-DSZ-CC-1136-V3-2022)	Release 9.2.3 including: • Flashloader OS Release 1.2.5 • Communication Library Release 6.0.0 • CRC Library 1.1.8 • Memory Library 1.2.3 • Flash Loader Library 3.6.0 • System Mode OS Release 13.2.3 • Crypto Library Release 0.7.6
	Native OS SOMA-c016, including eIDAS QSCD Application	Version 4

To ensure secure usage a set of guidance documents is provided, together with the SOMA-c016 Machine Readable Electronic Document eIDAS QSCD Application, version 4. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 2.3.

2.2 Security Policy

The TOE is a combination of hardware and software configured to securely create, use, and manage Signature Creation Data (SCD). The QSCD protects the SCD during its whole life cycle as to be used in a signature creation process solely by its Signatory.

The TOE comprises all IT security functionality necessary to ensure the secrecy of the SCD and the security of the electronic signature and deciphered data.

The TOE provides the following functions:

- generate Signature Creation Data (SCD) and the corresponding Signature Verification Data (SVD),
- export the SVD for certification to the CGA over a trusted channel,
- prove the identity as QSCD to external entities,
- optionally, receive and store certificate info,
- switch the QSCD from a non-operational state to an operational state, and
- if in an operational state, to create digital signatures for data with the following steps:
    - select an SCD if multiple are present in the QSCD,

- authenticate the Signatory and determine its intent to sign,
- receive data to be signed or a unique representation thereof (DTBS/R) from the SCA over a trusted channel,
- apply an appropriate cryptographic signature creation function to the DTBS/R using the selected SCD.

- if in an operational state, to decipher encrypted data with the following steps:
  - select an SCD if multiple are present in the QSCD,
  - authenticate the Signatory and determine its intent to decipher,
  - receive data to be deciphered (DTBD) from the DDA over a trusted channel,
  - apply an appropriate cryptographic decipher function to the DTBD using the selected SCD. (cf. ST eIDAS QSCD section 1.5.1)

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

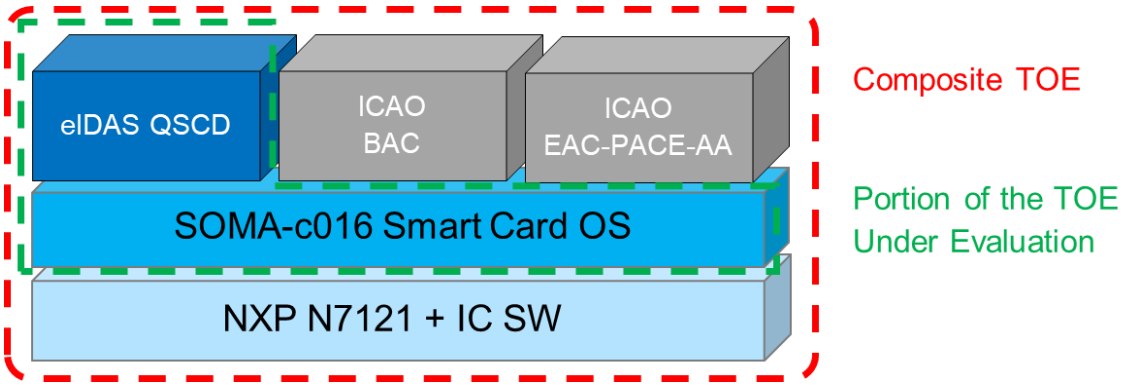
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 5.2 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information

The logical architecture, originating from the Security Target *[ST]* of the TOE can be depicted as follows (the red box depicts shows the Composite TOE while the green box shows the portion of the TOE under evaluation):



The TOE is composed of:

- the circuitry of the dual-interface e-Document's chip NXP N7121
- the IC Dedicated Software with the parts IC Dedicated Test Software, IC Dedicated Support Software, and Crypto Library
- the smart card operating system SOMA-c016
- the eIDAS QSCD application
- the associated guidance documentation

2.5 Documentation

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

Identifier	Version
SOMA-c016 Machine Readable Electronic Document Initialization Guidance, TCAE180013, Dated 01 December 2022	2.0
SOMA-c016 Machine Readable Electronic Document Pre-Personalization Guidance eIDAS QSCD application, TCAE180015, Dated 04 April 2023	2.1
SOMA-c016 Machine Readable Electronic Document Personalization Guidance eIDAS QSCD application, TCAE180017, Dated 04 April 2023	2.1
SOMA-c016 Machine Readable Electronic Document Operational User Guidance ICAO application, TCAE 180019, Dated 04 April 2023	2.1

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

The developer performed extensive testing on functional specification, subsystem and module level. All parameter choices were addressed at least once. All boundary cases identified were tested explicitly, and additionally the near-boundary conditions were covered probabilistically. The testing was largely automated using industry standard and proprietary test suites. Test scripts were used extensively to verify that the functions return the expected values.

The underlying hardware and crypto-library test results are extendable to composite evaluations, because the underlying platform is operated according to its guidance and the composite evaluation requirements are met.

For the testing performed by the evaluators, the developer provided samples and a test environment. The evaluators reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator.

2.6.2 Independent penetration testing

The methodical analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considers whether potential vulnerabilities can already be identified due to the TOE type and/or specified behaviour in such an early stage of the evaluation.
- For ADV_IMP a thorough implementation representation review is performed on the TOE. During this attack, oriented analysis the protection of the TOE is analysed using the knowledge gained from all previous evaluation classes. This results in the identification of (additional) potential vulnerabilities. For this analysis will be performed according to the attack methods in [JIL-AM]. An important source for assurance in this step is the technical report [ETRfC-HW] of the underlying platform.
- All potential vulnerabilities are analysed using the knowledge gained from all evaluation classes and information from the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. The potential vulnerabilities are addressed by penetration testing, a guidance update or in other ways that are deemed appropriate.

The total test effort expended by the evaluators was 6 weeks. During that test campaign, 30% of the total time was spent on Perturbation attacks, 70% on side-channel testing.

2.6.3 Test configuration

The developer tested the TOE in the following configuration:

- TOE Identification Data:

SOMA-c016_4 (ASCII codes 53h 4Fh 4Dh 41h 2Dh 63h 30h 31h 36h 5Fh 34h)

- Product Identification Data:

  SOMA-c016_4_0 (ASCII codes 53h 4Fh 4Dh 41h 2Dh 63h 30h 31h 36h 5Fh 34h 5Fh 30h)

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

There has been extensive reuse of the ALC aspects for the sites involved in the software component of the TOE. Sites involved in the development and production of the hardware platform were reused by composition.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number SOMA-c016 Machine Readable Electronic Document eIDAS QSCD Application, version 4.

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 SOMA-c016 Machine Readable Electronic Document eIDAS QSCD Application, version 4, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 5 augmented with ALC_DVS.2 and 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 *[EN419211-2], [EN 419211-4]* and *[EN419211-5]*.

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>.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength to satisfy the AVA_VAN.5 “high attack potential”. To be protected against attackers with a "high attack potential", appropriate cryptographic algorithms with sufficiently large cryptographic key sizes shall be used (references can be found in national and international documents and standards).

3 Security Target

The SOMA-c016 Machine Readable Electronic Document Security Target eIDAS QSCD Application, TCAE180021, Version 2.4, 06 April 2023 *[ST]* is included here by reference.

Please note that, to satisfy the need for publication, a public version *[ST-lite]* has been created and verified according to *[ST-SAN]*.

4 Definitions

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

[DCAP]	Dutch Conformity Assessment Process
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
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

[COMP] Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018

[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

[eIDAS-REP] Assessment Reporting Sheet eIDAS dated 12 of January 2024 with ID 23-RPT-1341, version 1.0

[ETR] Evaluation Technical Report “SOMA-c016 Machine Readable Electronic Document eIDAS QSCD Application, version 4” – EAL5+", 23-RPT-339, Version 3.0, 20 October 2023

[HW-CERT] NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4), 7 September 2022 registered under the reference BSI-DSZ-CC-1136-V3-2022

[HW-ETRfC] TÜV Informationstechnik Gmbh, Evaluation Technical Report for Composite Evaluation of NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) B1, 2022-08-25, v2.0

[HW-ST] NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4), Security Target Lite Rev. 2.6 – 13 June 2022

[JIL-AAPS] JIL Application of Attack Potential to Smartcards, Version 3.2, November 2022

[JIL-AM] Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution)

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022

[EN419211-2] EN 419 211-2:2013, Protection profiles for secure signature creation device - Part 2: Device with key generation, V2.0.1, registered under the reference BSI-CC-PP-0059-2009-MA-02

[EN 419211-4] EN 419 211-4 Protection Profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted channel to certificate generation application, version 1.0.1, 2013, BSI-CC-PP-0071-2012-MA-01

[EN419211-5] EN 419 211-5:2013, Protection profiles for secure signature creation device - Part 5: Extension for device with key generation and trusted communication with signature creation application, V1.0.1, registered under the reference BSI-CC-PP-0072-2012-MA-01

[ST]	SOMA-c016 Machine Readable Electronic Document Security Target eIDAS QSCD Application, TCAE180021, Version 2.4, 06 April 2023
[ST-lite]	SOMA-c016 Machine Readable Electronic Document Security Target eIDAS QSCD Application, TCLE180024, Version 2.0, Dated 19 June 2023
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)