Certification Report

SOMA-ck022 Travel Document, Version 1.0

Sponsor and developer:	***TOPPAN Security S.r.l.*** **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-2400045-01-CR**
Report version:	**1**
Project number:	**NSCIB-2400045-01**
Author(s):	**Andy Brown**
Date:	**13 June 2025**
Number of pages:	**14**
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.

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-ck022 Travel Document, Version 1.0. The developer of the SOMA-ck022 Travel Document, Version 1.0 is TOPPAN Security S.r.l. located in Arzano, 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 TOE is an electronic document representing a contactless smart card implementing ICAO Doc 9303 8th ed. 2021 – LDS1 and BSI TR-03110

The TOE is composed by:

- the circuitry of Infineon IFX_CCI_000039h chip with its firmware and user guidance;
- the IC Dedicated Software and Crypto Library;
- the smart card operating system Soma-ck022;
- the LDS1 eMRTD Application compliant with ICAO Doc 9303;
- the associated guidance documentation.

The authentication methods supported by the TOE in its operational state are:

- Basic Access Control (BAC), according to ICAO Doc 9303 8th edition Part 11
- Password Authenticated Connection Establishment (PACE), according to ICAO Doc 9303 8th edition Part 11
- Extended Access Control (EAC) v1, which includes Chip Authentication according to ICAO Doc 9303 8th ed. Part 11 and Terminal Authentication according to BSI TR-03110
- Active Authentication, according to ICAO Doc 9303 8th ed. 2021 Part 11

The TOE is configurable in BAC, EAC with BAC, PACE, BAC and PACE, EAC with BAC or PACE, EAC with PACE, with or without conditionally Active Authentication.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft. The evaluation was completed on 13 June 2025 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-ck022 Travel Document, Version 1.0, 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-ck022 Travel Document, Version 1.0 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

- EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality when authentication method BAC (with or without AA) is selected. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures)
- EAL5 augmented (EAL5+) assurance requirements for the evaluated security functionality when authentication method PACE (with or without AA) is selected. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures) and AVA_VAN.5 (Advanced methodical vulnerability analysis).
- EAL5 augmented (EAL5+) assurance requirements for the evaluated security functionality when authentication method PACE and EAC (with or without AA) is selected. This assurance

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

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.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the SOMA-ck022 Travel Document, Version 1.0 from TOPPAN Security S.r.l. located in Arzano, Italy.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	Infineon IFX_CCI_000039h	T11 (design step)
Firmware	BOS	80.306.16.0
	POWS	80.306.16.1
	RFAPI (ROM)	80.312.02.0
Dedicated Software	HSL	3.52.9708
	UMSLC	01.30.0564
	SCL	2.15.000
	ACL	3.35.001
	RCL	1.10.007
	HCL	1.13.002
Software	SOMA-ck022 Travel Document	1.0

To ensure secure usage a set of guidance documents is provided, together with the SOMA-ck022 Travel Document, Version 1.0. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 1.5.

2.2 Security Policy

The following TOE security features are the most significant for its operational use:

- During Initialization, the Initialization Agent must prove his/her identity by means of an authentication mechanism based on AES with 256-bit key.
- During Pre-personalization, the Pre-personalization Agent must prove his/her identity by means of an authentication mechanism based on SCP03 with AES with 128, 192, 256-bit keys.
- During Personalization, the Personalization Agent must prove his/her identity by means of an authentication mechanism based on SCP03 with AES with 128, 192, 256-bit keys.
- During Operational State, the following authentication mechanisms are supported:
    - Basic Access Control (BAC), according to ICAO Doc 9303 8th edition Part 11
    - Password Authenticated Connection Establishment (PACE), according to ICAO Doc 9303 8th edition Part 11
    - Extended Access Control (EAC) v1, which includes Chip Authentication according to ICAO Doc 9303 8th ed. Part 11, and Terminal Authentication according to BSI TR-03110
    - Active Authentication, according to ICAO Doc 9303 8th ed. 2021 Part 11.
- After a successful authentication, the communication between the e-Document and the terminal is protected by the Secure Messaging mechanism defined in section 6 of the ISO 7816-4 specification.

- The integrity of the data stored under the LDS can be checked by means of the Passive Authentication mechanism.

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 4.2.4 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

Note that the ICAO MRTD infrastructure critically depends on the objectives for the environment to be met. These are not weaknesses of this particular TOE, but aspects of the ICAO MRTD infrastructure as a whole.

The environment in which the TOE is personalised must perform proper and safe personalisation according to the guidance and referred ICAO guidelines.

The environment in which the TOE is used must ensure that the inspection system protects the confidentiality and integrity of the data send and read from the TOE.

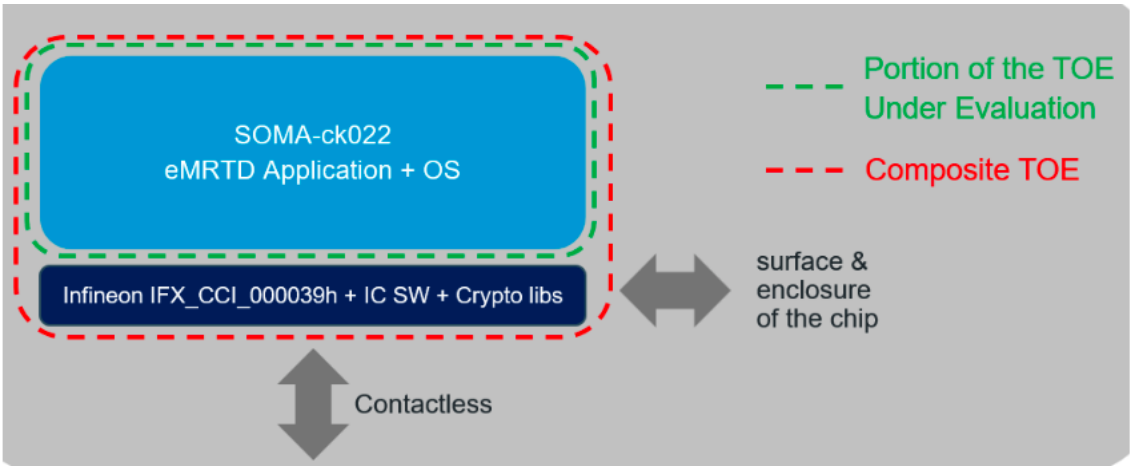
2.4 Architectural Information

The TOE is an electronic document representing a contactless smart card implementing ICAO Doc 9303 8th ed. 2021 – LDS1 and BSI TR-03110.

The TOE is composed by:

- The circuitry of Infineon IFX_CCI_000039h chip with its firmware and user guidance
- The IC Dedicated Software and Crypto Library
- The smart card operating system SOMA-ck022
- The LDS1 eMRTD Application compliant with ICAO Doc 9303
- The associated guidance documentation

The logical architecture of the TOE can be depicted as follows:



2.5 Documentation

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

Identifier	Version
SOMA-ck022 Travel Document Initialization Guidance	v1.1
SOMA-ck022 Travel Document PERSONALIZATION GUIDANCE	v1.1
SOMA-ck022 Travel Document PRE-PERSONALIZATION GUIDANCE	v1.1
SOMA-ck022 Travel Document OPERATIONAL USER GUIDANCE	v1.1

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 SFR-enforcing 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 considered whether potential vulnerabilities could 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 was performed on the TOE. During this attack-oriented analysis, the protection of the TOE was analysed using the knowledge gained from all previous evaluation classes. This resulted in the identification of (additional) potential vulnerabilities. This analysis was performed according to the attack methods in [JIL-AM]. An important source for assurance in this step were the ETR for Composition documents of the underlying platform.
- All potential vulnerabilities were 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 were not exploitable. The potential vulnerabilities were 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, 25% of the total time was spent on Perturbation attacks, 25% on side-channel testing, and 50% on logical tests.

2.6.3 Test configuration

The TOE was tested in the following configuration:

- SOMA-ck022_1.0 (ASCII codes 53h 4Fh 4Dh 41h 2Dh 63h 6Bh 30h 32h 32h 5Fh 31h 2Eh 30h)

All configurations are covered with this configuration. The evaluators provided a justification for this.

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.

The algorithmic security level exceeds 100 bits for all evaluated cryptographic functionality as required for high attack potential (AVA_VAN.5).

The strength of the implementation of the cryptographic functionality has been assessed in the evaluation, as part of the AVA_VAN activities.

2.7 Reused Evaluation Results

There is no reuse of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number SOMA-ck022 Travel Document, Version 1.0.

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 Site Technical Audit Report(s) for the site(s) *[STAR]* [2].

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the SOMA-ck022 Travel Document, Version 1.0, to be **CC Part 2 extended, CC Part 3 conformant** and to meet the requirements of:

EAL4 augmented with ALC_DVS.2 and for BAC authentication (with or without AA selected) and

EAL5 augmented with ALC_DVS.2 and AVA_VAN.5 for PACE (with or without AA selected) and

EAL5 augmented with ALC_DVS.2 and AVA_VAN.5 for PACE and EAC (with or without AA selected)

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_0055], [PP_0056] and [PP_0068].

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.

---

[2] The Site Technical Audit Report contains information necessary to an evaluation lab and certification body for the reuse of the site audit report in a TOE evaluation.

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 SOMA-ck022 Travel Document Security Target, TS-IT_25016, Version 1.2, 12 June 2025 *[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:

IT	Information Technology
AA	Active Authentication
BAC	Basic Access Control
EAC	Extended Access Control
eMRTD	electronic MRTD
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PACE	Password Authenticated Connection Establishment
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
[ETR]	Evaluation Technical Report “SOMA-ck022 Travel Document v1.0” – EAL4/5+, 24-RPT-319, Version 5.0, 12 June 2025
[PLT-CERT]	Certification Report BSI-DSZ-CC-1107-V5-2024 for IFX_CCI_00002Dh, 000039h, 00003Ah, 000044h, 000045h, 000046h, 000047h, 000048h, 000049h, 00004Ah, 00004Bh, 00004Ch, 00004Dh, 00004Eh design step T11 with firmware 80.306.16.0, 80.306.16.1 or 80.312.02.0, optional NRGTM SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib v01.30.0564, optional SCL v2.15.000 or v2.11.003, optional ACL v3.35.001, v3.34.000, v3.33.003 or v3.02.000, optional RCL v1.10.007, optional HCL v1.13.002 and user guidance from Infineon Technologies AG, 04 September 2024
[PLT-ETRfC]	Evaluation Technical Report for Composite Evaluation (ETR COMP), Version 3, 15 February 2024
[PLT-ETRfC-ADD]	Evaluation Technical Report for Composite Evaluation Addendum (ETR COMP_ADD), Version 2, 02 September 2024
[HW-ST]	IFX_CCI_00002Dh, IFX_CCI_000039h, IFX_CCI_00003Ah, IFX_CCI_000045h, IFX_CCI_000046h, IFX_CCI_000047h, IFX_CCI_000049h, IFX_CCI_00004Ah, IFX_CCI_00004Bh, IFX_CCI_00004Dh, IFX_CCI_00004Eh T11 Security Target Lite, Version 6.5, 20 August 2024
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.2.1, February 2024
[JIL-AMS]	Attack Methods for Smartcards and Similar Devices, Version 2.5, May 2022 (sensitive with controlled distribution)
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[PP_0055]	Protection Profile Machine Readable Travel Document with “ICAO Application”, Basic Access Control (MRTD-PP), Version 1.10, 25 March 2009, registered under the reference BSI-CC-PP-0055-2009
[PP_0056]	Protection Profile Machine Readable Travel Document with “ICAO Application”, Extended Access Control with PACE (EAC PP), Version 1.3.2, 05 December 2012, registered under the reference BSI-CC-PP-0056-V2-2012
[PP_0068]	Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE, Version 1.0.1, 22 July 2014, registered under the reference BSI-CC-PP-0068-V2-2011-MA-01
[ST]	SOMA-ck022 Travel Document Security Target, TS-IT_25016, Version 1.2, 12 June 2025

[ST-lite]	SOMA-ck022 Travel Document Security Target Lite, TS-IT_25027, Version 1.1, 12 June 2025
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006
[STAR]	Site Technical Audit Report SOMA-ck022 Travel Document, Version 2.0, 24-RPT-1365, 05 May 2025

(This is the end of this report.)