Certification Report

ePassport configuration of SECORA™ ID S Infineon Applet - eMRTD V1.2

Sponsor and developer: ***Infineon Technologies AG***
Am Campeon 1-15
85579 Neubiberg
Germany

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

Report number:	**NSCIB-CC-2500014-01-CR**
Report version:	**1**
Project number:	NSCIB-**2500014-01**
Author(s):	**Alireza Rohani**
Date:	**26 August 2025**
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 ePassport configuration of SECORA™ ID S Infineon Applet - eMRTD V1.2. The developer of the ePassport configuration of SECORA™ ID S Infineon Applet - eMRTD V1.2 is Infineon Technologies AG located in Neubiberg, Germany 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 an electronic passport representing a smart card. This smart card/passport provides the following application:

The travel document containing the related user data as well as data needed for authentication with BAC, PACE, EAC or AA protocols (incl. PACE/BAC passwords); this application is intended to be used by governmental organisations as a machine readable travel document (MRTD).

The TOE was previously evaluated by SGS Brightsight B.V. located in Delft, The Netherlands and was certified under the accreditation of TÜV Rheinland Nederland on 27 April 2021 (NSCIB-CC-21-0075541). The current evaluation of the TOE has also been conducted by SGS Brightsight B.V. and was completed on 26 August 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 major changes from previous evaluations are:

- The underlying hardware platform has been updated in terms of applying security hardening to Asymmetric Cryptographic Library (ACL) resulting in a new ACL version.

- AGD documents are updated to reflect the new OS build number

- The ST is updated to reference the new HW and OS certificates.

A full, up-to-date vulnerability analysis has been made, as well as renewed testing.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the ePassport configuration of SECORA™ ID S Infineon Applet - eMRTD V1.2, 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 ePassport configuration of SECORA™ ID S Infineon Applet - eMRTD V1.2 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:

- EAL5 augmented with the components ALC_DVS.2 (Sufficiency of security measures) and AVA_VAN.5 (Advanced methodical vulnerability analysis) in case PACE is used and EAC is not used.
- EAL5 augmented with the components ALC_DVS.2 (Sufficiency of security measures) and AVA_VAN.5 (Advanced methodical vulnerability analysis) in case PACE and EAC are used.
- EAL4 augmented with the components ALC_DVS.2 in case BAC is chosen as authentication method.

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 ePassport configuration of SECORA™ ID S Infineon Applet - eMRTD V1.2 from Infineon Technologies AG located in Neubiberg, Germany.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	Infineon Security Controller IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h H13 including the products from the second production line and optional software packages: Flash Loader, Asymmetric Crypto Library, Symmetric Cryptographic Library, Hardware Support Layer, Hash Crypto Library, Mifare Compatible Software, and CIPURSE™ Crypto Library Identifier: IFX_CCI_000005h is used for the TOE.	HW-Version: H13 FW-Version: 80.100.17.3
IC Dedicated Software	ACL (Asymmetric Crypto Library) ▪ Base library ▪ RSA2048 / RSA4096 ▪ EC ▪ Toolbox	V2.09.002
	HSL (Hardware Support Library)	V03.12.8812
	SCL (Symmetric Crypto Library)	V2.04.002

IC Embedded Software	Embedded OS, SECORA™ID S v1.2 (SLJ52GxxyyyzS)
	x = Available interface (C=contact, L=contactless, D=dual-interface)
	x = RSA cryptography (T=2K RSA, A=4K RSA)
	yyy = Available user memory in KB
	z = Product placement (A=ePassport and eID, B=eDL, H=ePassport and eID with VHBR)
		1518

IC Embedded Software	eMRTD Applet	1.2

To ensure secure usage a set of guidance documents is provided, together with the ePassport configuration of SECORA™ ID S Infineon Applet - eMRTD V1.2. For details, see section 2.5 "Documentation" of this report.

2.2 Security Policy

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

- Verifying authenticity and integrity as well as securing confidentiality of user data in the communication channel between the TOE and the connected terminal supporting the protocols BAC, SAC(PACE).
- Averting of inconspicuous tracing of the travel document
- Self-protection of the TOE security functionality and the data stored inside.

- Means to check authenticity of the terminal.
- Means to prove authenticity of the chip by means of Active Authentication or Chip Authentication
- Chip authentication followed by terminal authentication used as a precondition to provide access to biometric data known as EAC.

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 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.

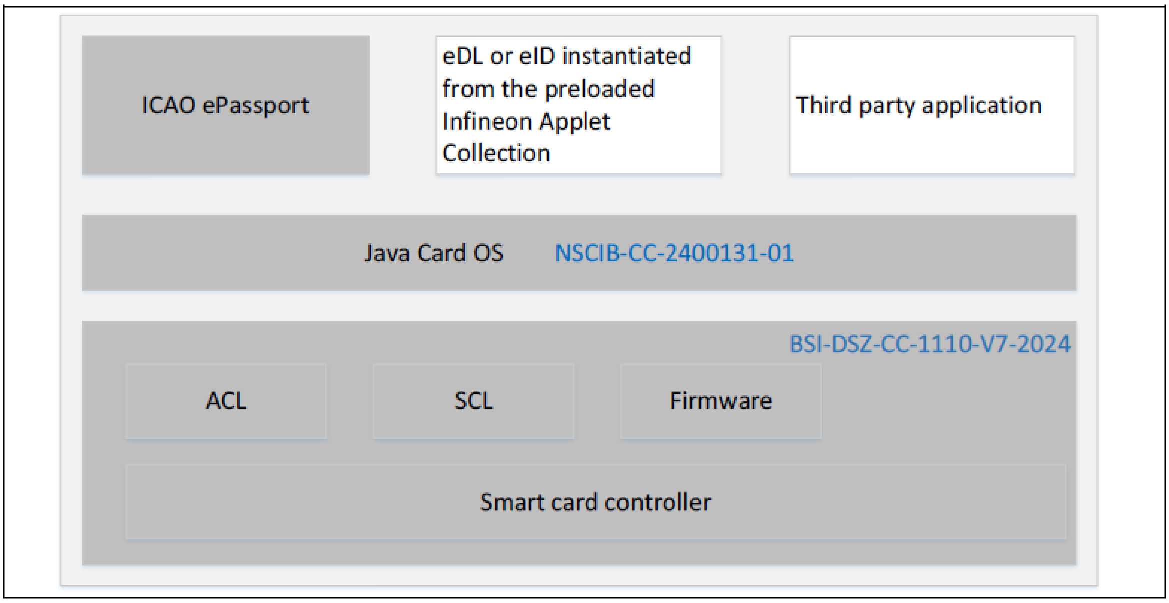
Note that the ICAO MRTD infrastructure critically depends on the objectives for the environment to be met. These are not weaknesses of this particular TOE, but aspects of the ICAO MRTD infrastructure as a whole.

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 following diagram shows the TOE architecture as depicted in the *[ST]*:



2.5 Documentation

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

Identifier	Version
Infineon Applet Collection eMRTD V1.2 Administration Guide	1.2, date: 2025-05-06
Infineon Applet Collection eMRTD V1.2 Databook	1.5, date: 2025-06-19

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 has performed extensive testing on FSP, subsystem, module and module interface level. The tests are performed by the developer through execution of the test scripts using an automated system. Test tools and scripts are extensively used to verify that the tests return expected values.

Code coverage analysis is used by the developer to verify overall test completeness. Test benches for the

various TOE parts are executed using code coverage measurement and analysis tools to determine the code coverage (i.e. lines, branches and/or instructions, depending on tool) of each test bench. Cases with incomplete coverage are analysed. For each tool, the developer has investigated and documented inherent limitations that can lead to coverage being reported as less than 100%. In such cases the developer provided a "gap" analysis with rationales.

The evaluator evaluated ATE based on code coverage analysis. The evaluator also used an acceptable alternative approach (as described in the application notes, Section 14.2.2 in [CEM]) and used analysis of the implementation representation (i.e. inspection of source code) to validate the rationales provided by the developer.

2.6.2 Independent penetration testing

The methodical analysis is performed during the baseline evaluation and it is 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. This analysis has been performed according to the attack methods in [JIL-AAPS]. An important source for assurance in this step is the technical report [JCS-ETRFC] 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 1 week. During that test campaign, 50% was on Perturbation Attacks, 50% was on software attacks, 0% was on Physical Attacks, %0 on Overcoming Sensors and Filters, 0% on Retrieving Keys with DFA, 0% on Side Channel Attacks, 0% on Exploitation of Test Features, 0% on Attacks on RNG and 0% on Application isolation.

2.6.3 Test configuration

The configuration of the sample used for independent evaluator testing and penetration testing was the same as described in the *[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.

2.7 Reused Evaluation Results

This is a re-certification. Documentary evaluation results of the earlier version of the TOE have been reused, but vulnerability analysis and penetration testing has been renewed.

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 ePassport configuration of SECORA™ ID S Infineon Applet - eMRTD V1.2.

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 ePassport configuration of SECORA™ ID S Infineon Applet - eMRTD V1.2, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of:

- EAL5 augmented with the components ALC_DVS.2 (Sufficiency of security measures) and AVA_VAN.5 (Advanced methodical vulnerability analysis) in case PACE is used and EAC is not used.
- EAL5 augmented with the components ALC_DVS.2 (Sufficiency of security measures) and AVA_VAN.5 (Advanced methodical vulnerability analysis) in case PACE and EAC are used.
- EAL4 augmented with the components ALC_DVS.2 in case BAC is chosen as authentication method.

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.

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 Security Target, ePassport configuration of SECORA™ ID S Infineon Applet Collection - eMRTD V1.2, rev 2.0, 2025-07-31 *[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:

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

[HW-CERT] BSI-DSZ-CC-1110-V7-2024 for Infineon Security Controller IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 000022h in the design step H13 from Infineon Technologies AG, v1.0, 30 September 2024

[HW-ST] Public Security Target IFX_CCI_000003h IFX_CCI_000005h IFX_CCI_000008h IFX_CCI_00000Ch IFX_CCI_000013h IFX_CCI_000014h IFX_CCI_000015h IFX_CCI_00001Ch IFX_CCI_00001Dh IFX_CCI_000021h IFX_CCI_000022h H13, Including optional Software Libraries Flash Loader – 4x ACL – 4x HSL – 3x SCL – HCL - NRG – CCL, rev. 5.1, 2024-09-11

[PLAT_CERT] Certificate, NSCIB-CC-2400131-01, SECORA™ ID S v1.2 (SLJ52GxxyyyzS), EAL6 augmented with ALC_FLR.1, 30 May 2025

[PLAT-ETRfC] Evaluation Technical Report for Composition "SECORA™ ID S v1.2 (SLJ52GxxyyyzS)" – EAL6+, [25-RPT-625], v3.0, 30 May 2025

[PLAT-ST] SECORA™ ID S v1.2 (SLJ52GxxyyyzS) Security Target, Rev. 2.8, 2025-04-16

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

[ETR] Evaluation Technical Report ePassport configuration of SECORA™ ID S Infineon Applet Collection - eMRTD V1.2 – EAL4+ for BAC, EAL5+ for EAC-PACE and EAL5+ for PACE, 25-RPT-1009, v2.0, 20 August 2025.

[EAR] Evaluator Assessment of Changes Report (EAR) ePassport configuration of SECORA™ ID S Infineon Applet Collection - eMRTDV1.2 – EAL4+ for BAC, EAL5+ for EAC-PACE and EAL5+ for PACE – Partial ETR, 25-RPT-870, v3.0, 20 August 2025

[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-MA-01

[ST] Security Target, ePassport configuration of SECORA™ ID S Infineon Applet Collection - eMRTD V1.2, rev 2.0, 2025-07-31

(This is the end of this report.)