Certification Report

ePassport configuration of SECORA™ ID v2.01 Infineon Applet Collection - eMRTD V2.0

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-2400086-01-CR**

Report version: **1**

Project number: NSCIB-**2400086-01**

Author(s): **Alireza Rohani and Jordi Mujal**

Date: **10 April 2025**

Number of pages: **12**

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 ePassport configuration of SECORA™ ID v2.01 Infineon Applet Collection - eMRTD V2.0. The developer of the ePassport configuration of SECORA™ ID v2.01 Infineon Applet Collection - eMRTD V2.0 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.

TOE is a composition of Java Card platform with eMRTD application. The eMRTD application stores the related user data as well as data needed for authentication with BAC, PACE, EAC or AA protocols; this application is intended to be used by governmental organisations as a machine readable travel document (MRTD). All the Java Card OS secure functionalities from [JCS-CERT] are available to the user during personalization phase.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 10 April 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 ePassport configuration of SECORA™ ID v2.01 Infineon Applet Collection - eMRTD V2.0, 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 ePassport configuration of SECORA™ ID v2.01 Infineon Applet Collection - eMRTD V2.0 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 when authentication method BAC is selected. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures)
- EAL5 augmented (EAL5+) assurance requirements when authentication method PACE, with or without EAC, is selected. 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, CEM:2022 [CEM] for conformance to the Common Criteria for Information Technology Security Evaluation, CC:2022 [CC].

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 v2.01 Infineon Applet Collection - eMRTD V2.0 from Infineon Technologies AG located in Neubiberg, Germany.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	IFX_CCI_00005D	S11
Firmware	BOS & POWS & RFAPI (ROM)	80.309.05.0
	Flash-loader	09.13.0004
IC Software	ACL	03.35.001
	SCL	02.15.000
	HSL	03.52.9708
	HCL	01.13.002
	UMSLC	01.30.0564
Embedded OS software	JCVM 3.1, JCRE 3.1, JCAPI 3.1 and GP 2.3.1 framework with CIC and FC Config, proprietary API	CONF1: '01 00 02 FA 15 00 00 13 05' CONF2: '01 00 0C FA 15 00 00 13 05'
Applet	Applet Collection - eMRTD V2.0	1.1.0.0

To ensure secure usage a set of guidance documents is provided, together with the ePassport configuration of SECORA™ ID v2.01 Infineon Applet Collection - eMRTD V2.0. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 1.6.4.

2.2 Security Policy

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

- All the Java Card OS secure functionalities from [JCS-CERT] are available to the user during personalization phase.
- 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) as and EAC
- 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, Terminal Authentication.
- 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.

- Any product using BAC will be conformant to [PP_55] only. Any product using PACE but not using EAC will be conformant to [PP_68] only. Any product using PACE and EAC will be conformant to [PP_56] only.

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.

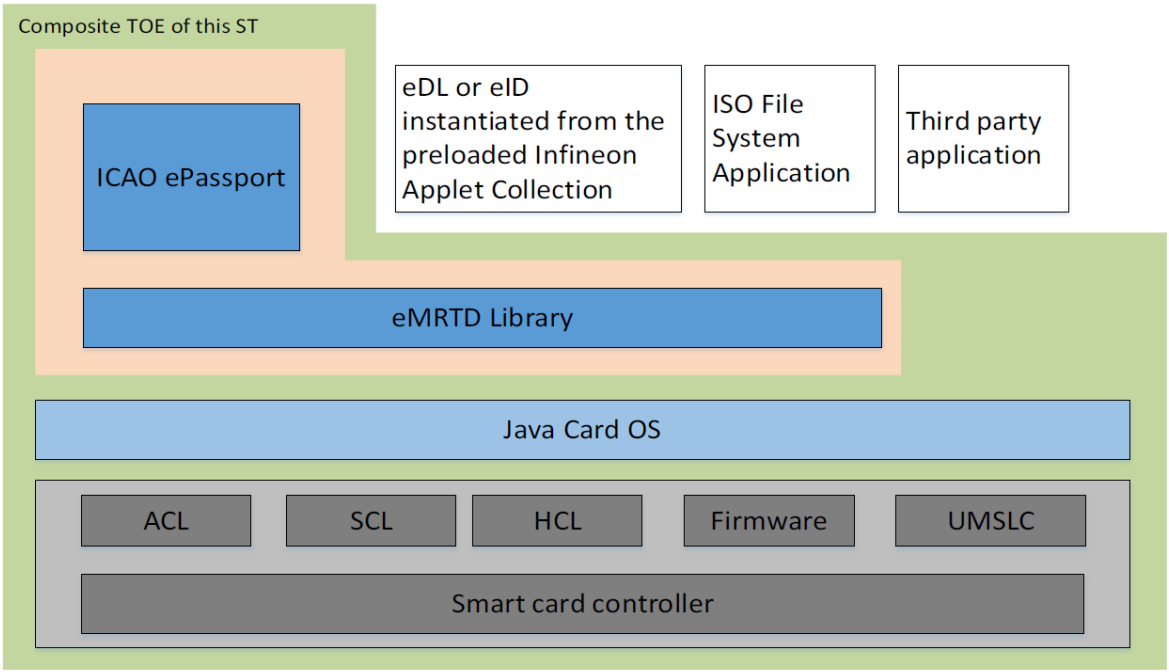
Note that the ICAO MRTD infrastructure critically depends on the objectives for the environment to be met. These are not weaknesses of this particular TOE, but aspects of the ICAO MRTD infrastructure as a whole.

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
ePassport configuration of SECORA™ ID v2.01 Infineon Applet Collection - eMRTD V2.0 Administration Guide	Rev 1.1
ePassport configuration of SECORA™ ID v2.01 Infineon Applet Collection - eMRTD V2.0 Extended datasheet	Rev 1.3
Additional guidance for Java Card platform with open mode: Underlying OS platform guidances as listed in section 1.4.1.4 of *[JCS_ST]*.	-

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 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 2 weeks. 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.

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.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength for satisfying the AVA_VAN.5 "high attack potential". The TOE supports a wider range of key sizes (see *[ST]*), including those with sufficient algorithmic security level to exceed 100 bits 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.

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of multiple site certificates and Site Technical Audit Reports.

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 ePassport configuration of SECORA™ ID v2.01 Infineon Applet Collection - eMRTD V2.0.

2.9 Evaluation Results

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

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 v2.01 Infineon Applet Collection - eMRTD V2.0, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of:

EAL 4 augmented ALC_DVS.2 for BAC authentication and

EAL 5 augmented with ALC_DVS.2 and AVA_VAN.5 for **PACE authentication** (with or without EAC 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.

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 ePassport configuration of SECORA™ ID v2.01 Infineon Applet Collection - eMRTD V2.0, Rev 1.0, 21 March 2025 *[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:

AA	Active Authentication
BAC	Basic Access Control
EAC	Extended 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 1 to 5, CC:2022 Revision 1, November 2022
[CEM]	Common Methodology for Information Technology Security Evaluation, CEM:2022 Revision 1, November 2022
[COMP]	Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, for CC:2022 Version 1.6, April 2024
[ETR]	Evaluation Technical Report “ePassport configuration of SECORA™ ID v2.01 Infineon Applet Collection - eMRTD V2.0” – EAL4+ for BAC, EAL5+ for EAC-PACE and EAL5+ for PACE, version 2.0, 21 March 2025
[JCS-CERT]	Certification Report SECORA™ ID v2.01 (SLJ38Gxymm1ap), NSCIB-CC-2400062-01-CR , version 1, 20 December 2024
[JCS-ETRfC]	Evaluation Technical Report for Composition “SECORA™ ID v2.01 (SLJ38Gxymm1ap)" – EAL6+, 24-RPT-696, version 2.0, 19 December 2024
[JCS-ST]	SECORA™ ID v2.01 (SLJ38Gxymm1ap), Rev 1.1, 19 December 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]	ePassport configuration of SECORA™ ID v2.01 Infineon Applet Collection - eMRTD V2.0, Rev 1.0, 21 March 2025

(This is the end of this report.)