Certification Report

ePassport configuration of SECORA™ ID S Infineon Applet Collection - eMRTD V1.1

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

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

Report number: **NSCIB-CC-0075541-CR2**

Report version: **1**

Project number: **0075541_2**

Author(s): **Andy Brown**

Date: **27 April 2021**

Number of pages: 15

Number of appendices: **0**

Headoffice:
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 Dutch Chamber of Commerce 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 license 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, in order 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 and SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations.

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting 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. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.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 Collection - eMRTD V1.1. The developer of the ePassport configuration of SECORA™ ID S Infineon Applet Collection - eMRTD V1.1 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 TOE consists of the Infineon ePassport configuration of the SECORA™ ID S platform with an eMRTD application. It is based on the requirements from the ICAO for machine readable travel documents, i.e. *[ICAO-9303-10]*, *[ICAO-9303-11*], *[TR-03110-1]* and *[TR-03110-3]*. This ePassport product provides the travel document application containing the related user data as well as data needed for authentication with BAC, PACE, EAC or AA protocols (including PACE/BAC passwords).

It is a dual-interface product, where the ISO/IEC 14443 Type B *[ISO14443]* interface is present for the ePassport functionality while the ISO/IEC 7816 *[ISO7816]* protocol is supported for the purposes of eID and eDL applications.

The TOE has been originally evaluated by Brightsight B.V. located in Delft, The Netherlands and was certified on 27 May 2020. The re-evaluation also took place by Brightsight B.V. and was completed on 27 April 2021 with the approval of the ETR. The re-certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

This second issue of the Certification Report is a result of a “recertification with major changes”.

The major changes are due to a change in the underlying platform which has been recertified in composition with the hardware. This re-certification has resulted in updates ST, Guidance and ETR for Composition.

The developer has introduced the following changes to the TOE which do not impact its security assurance.

- Product version is changed as result of changes introduced in the certified platform.
- A bug is fixed in the certifying platform allowing PACE support for ECC 521 in the applet
- TOE identification data of the underlying certified platform is updated
- Available user NVM for applet is updated in guidance.
- The STARs for the sites are updated.
- Test results showing that the applet is tested on the re-certified platform are provided.

The security evaluation re-used the evaluation results of previously performed evaluations. A full, up to date vulnerability analysis has been made. For this recertification, no additional testing has been required.

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 Collection - eMRTD V1.1, 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 Collection - eMRTD V1.1 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 provides sufficient evidence that the TOE meets:

- 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).

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

- EAL4 augmented (EAL4+) assurance requirements when authentication method BAC is selected. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 and *[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. It should be noted that the certification results only apply 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 ePassport configuration of SECORA™ ID S Infineon Applet Collection - eMRTD V1.1 from Infineon Technologies *AG* located in Neubiberg, Germany.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
IC 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), which is comprised of: • Base library • RSA2048/4096 • EC • Toolbox	V2.07.003
	HSL (Hardware Support Library)	V03.12.8812
	SCL (Symmetric Crypto Library)	V02.04.002
	MCS	Not Used
	HCL (Hash Crypto Library)	Not Used
IC Embedded Software	Embedded OS, SECORA™ID S v1.1 (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) *Note: For platform configurations used for the TOE as listed in the separate table below*	1442
IC Embedded Software	eMRTD Applet	1.1

Platform configurations used for the TOE.

Platform for TOE	Description
SLJ52GDTyyyAS	eMRTD V1.1 for ePassport and eID
SLJ52GLTyyyAS	eMRTD V1.1 for ePassport and eID
SLJ52GCTyyyAS	eMRTD V1.1 for eID
SLJ52GDTyyyHS	eMRTD V1.1 for ePassport and eID
SLJ52GLTyyyHS	eMRTD V1.1 for ePassport and eID
SLJ52GDTyyyBS	eMRTD V1.1 for eDL
SLJ52GLTyyyBS	eMRTD V1.1 for eDL
SLJ52GCTyyyBS	eMRTD V1.1 for eDL

Note: The available user memory indicated with yyy is customer selectable. The maximum memory size available is yyy=080 indicating 80KB.

To ensure secure usage a set of guidance documents is provided together with the ePassport configuration of SECORA™ ID S Infineon Applet Collection - eMRTD V1.1. Details can be found in section 2.5 of this report.

For a detailed and precise description of the TOE lifecycle refer to the *[ST]*, chapter 2.6.4.

2.2 Security Policy

The TOE has the following features (listed per operating phase):

Personalization phase

- Authentication and secure channel using the certified platform implemented Global Platform *[GP]* functionality using SCP03 *[GP-AMD-D]*.
- Configuration of the TOE.
- Create and populate LDS binary files with the user data.
- Configure SM level for biometric data access.
- Write the document Security Object (SO_D).
- Initialize the keys required for secure communication.
- Load authentication keys in encrypted form.
- Write the initial CVCA Public Key, CVCA certificate and Current Date.
- Set TOE life cycle to Operational Use Phase where ISD functionality is permanently disabled.

Operational 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 per *[ICAO-9303-11]* and EAC as per *[TR-03110-1]*. PACE supports Generic Mapping.
- Averting of inconspicuous tracing of the travel document as per *[TR-03110-1]*.
- Self-protection of the TOE security functionality and the data stored inside as per *[TR-03110-1]*.
- Means to check authenticity of the terminal, Terminal Authentication as per *[TR-03110-1]*
- Means to prove authenticity of the chip by means of Active Authentication or Chip Authentication as per *[TR-03110-1]*.
- Chip authentication followed by terminal authentication used as a precondition to provide access to biometric data known as EAC, as per *[TR-03110-1]*.

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. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 5 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 personalized must perform proper and safe personalization 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.

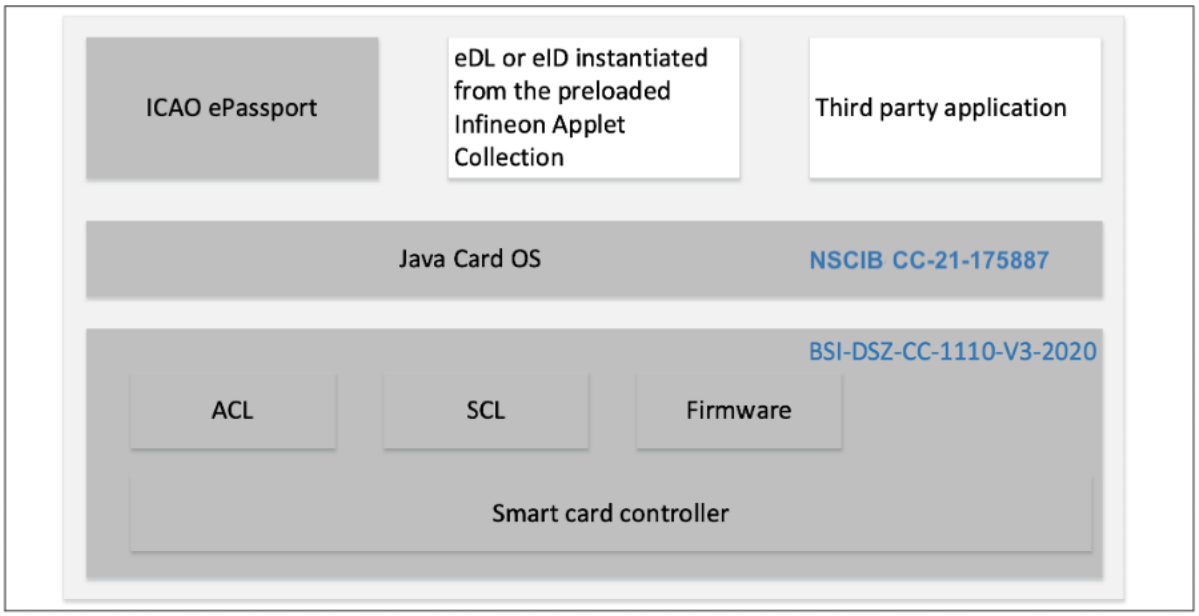
2.4 Architectural Information

The TOE consists of the Infineon ePassport configuration of the SECORA™ ID S platform with an eMRTD application. It is based on the requirements from the ICAO for machine readable travel documents, i.e. *[ICAO-9303-10], [ICAO-9303-11], [TR-03110-1] and [TR-03110-3].* This ePassport product provides the travel document application containing the related user data as well as data needed for authentication with BAC, PACE, EAC or AA protocols (including PACE/BAC passwords).

It is a dual-interface product, where the ISO/IEC 14443 Type B *[ISO14443]* interface is present for the ePassport functionality while the ISO/IEC 7816 *[ISO7816]* protocol is supported for the purposes of eID and eDL applications.

The Security IC is the certified *[CERT-HW]* Infineon smart card controller (BSI-DSZ-CC-1110-V3-2020) conforming *[PP-0084]*. It contains firmware and cryptographic libraries falling under the same certification identifier. The operating system is the certified Infineon SECORA™ ID S v1.1 Java Card OS with certification identifier NSCIB-CC-21-175887 *[CERT-PLAT]*, conforming to *[PP-JC]* which is the Java Card platform of the TOE. The Java Card platform supports Java Card Classic v3.0.5 *[JC-305]*. The ePassport functionality is implemented as a Java Card application on this platform.

The logical architecture, originating from the Security Target *[ST]* can be depicted as in Figure 1. The grey coloured components are depicting the TOE components. The white coloured components, i.e. eDL (electronic driver's license) and eID (electronic identification) applications can be instantiated from the existing ePassport functionality however no claims are made as part of *[ST]*. Furthermore, any Third-party applications are not in scope of the evaluation.



Logical architecture of the TOE.

2.5 Documentation

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

Identifier	Version
Infineon Applet Collection eMRTD Administration Guide SLJ52GxxyyyzS V1.1	1.0, 2020-12-08
Infineon Applet Collection eMRTD Databook SLJ52GxxyyyzS V1.1	1.0, 2020-12-08

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

Code coverage analysis was 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 were analysed. For each tool, the developer investigated and documented inherent limitations that could 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. During the re-evaluation the developer provided updated test results showing that the e-MRTD was tested on the re-certified platform.

During the baseline evaluation the evaluator repeated a selection of developer tests that cover various aspects of the TOE, as well as areas where the code coverage approach has limitations. Additionally, the witnessing session was used to sample and check the actual test results. During the re-evaluation

the developer tests were not repeated, because the test results provided by the developer show that identical tests were performed as for the base evaluation.

Evaluator-defined tests were chosen to supplement the developer's extensive testing. Six evaluator-defined tests were performed. During the re-evaluation these tests have not been repeated. The evaluator analysis shows that the changes that were introduced did not require repeating these tests and the tests performed during the base evaluation also provided sufficient assurance for the re-evaluation.

2.6.2 Independent Penetration Testing

The methodical analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ADV and AGD, potential vulnerabilities for all eMRTD authentication methods were identified from generating questions to the type of TOE and the specified behaviour. From the ASE class, no potential vulnerabilities were identified.
- For ADV_IMP a thorough implementation representation review was performed on the TOE considering all eMRTD authentication methods. During this attack oriented analysis, the protection against the attack scenarios was analysed using the knowledge gained from all previous evaluation classes. This resulted in the identification of additional potential vulnerabilities. This analysis was supported by the attack list in *[JIL-AM]* and application of attack potential in *[JIL-AAPS]*.
- All potential vulnerabilities were analysed using the knowledge gained from all evaluation classes and the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. For most of the potential vulnerabilities a penetration test was defined. Several potential vulnerabilities were found to be not exploitable due to an impractical attack path.

Potential vulnerabilities were grouped per similarity and addressed by penetration testing aiming at the weakest case. A total of six tests were performed, one perturbation and five software attacks, which were applicable for all eMRTD authentication methods provided by the TOE. A total of two weeks test effort was used. Many of the attack categories were already addressed by the certified platform.

During the re-evaluation the vulnerability analysis was refreshed, although these tests have not been repeated. The evaluator analysis showed that the changes introduced did not require the tests to be repeated and the tests performed during the baseline evaluation provided sufficient assurance also for the re-evaluation.

2.6.3 Test Configuration

The penetration tests were performed on an actual TOE sample in its evaluated configuration of the baseline evaluation. Some tests were performed in a pre-personalized state while most were performed in personalized state. Samples were provided in ID-1 form factor with a memory size of 80KB.

2.6.4 Testing 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).

2.7 Re-used evaluation results

This is a re-certification. Documentary evaluation results of the earlier version of the TOE have been re-used, but vulnerability analysis has been renewed. For this recertification, no additional evaluator testing was required.

There has been extensive re-use of the ALC aspects for the sites involved in the development and production of the TOE, by use of 5 Site Technical Audit Re-use 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 S Infineon Applet Collection - eMRTD V1.1.

2.9 Results of the Evaluation

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 Collection - eMRTD V1.1, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 5 augmented ALC_DVS.2 and AVA_VAN.5** for **PACE authentication** (with or without EAC selected) and **EAL** 4 **augmented ALC_DVS.2 for BAC authentication**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims 'strict' conformance to:

- [PP-0055], if a BIS chooses BAC as authentication method
- [PP-0068], if a BIS chooses PACE as authentication method
- [PP-0056], if a EIS choses PACE as authentication method and additionally uses Extended Access Control, which consists of two parts (i) the Chip Authentication Protocol Version 1 (v.1) and (ii) the Terminal Authentication Protocol Version 1 (v.1) as defined in *[TR-03110-1].*

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 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 with respect to 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 need to 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. In order for the evolution of attack methods and techniques to be covered, he 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 Security Target, ePassport configuration of SECORA™ ID S Applet Collection - eMRTD V1.1, v1.3, 12 April 2021 *[ST]* is included here by reference.

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

AA	Active Authentication
BAC	Basic Access Control
CA	Chip Authentication
CVCA	Country Verifying Certificate Authority
EAC	Extended Access Control
eDL	Electronic Driver's Licence
eID	Electronic Identification
eMRTD	Electronic Machine Readable Travel Document
IC	Integrated Circuit
ICAO	International Civil Aviation Organization
ISD	Issuer Security Domain
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
LDS	Logical Data Structure
NSCIB	Netherlands Scheme for Certification in the area of IT security
PACE	Password Authentication Connection Establishment
PP	Protection Profile
SAC	Supplemental Access Control
SM	Secure Messaging
SO_D	Security Object
TA	Terminal Authentication
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.

[CERT-HW] Certificate BSI-DSZ-CC-1110-V3-2020, 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 and including optional software packages and dedicated firmware in several versions, 13 May 2020.

[CERT-PLAT] Certificate, CC-21-175887, SECORA™ ID S v1.1 (SLJ52GxxyyyzS), EAL6 augmented with ALC_FLR.1, 05 March 2021.

[ETR-COMP] ETR for Composite Evaluation SECORA™ ID S v1.1, 19-RPT-630, Version 7.0, 02 March 2021.

[ETR] Evaluation Technical Report Infineon “ePassport configuration of SECORA™ ID S Infineon Applet Collection - eMRTD V1.1” EAL4+ for BAC, EAL5+ for EAC-PACE and EAL5+ for PACE, 20-RPT-050, version 6.0, 16 April 2021.

[GP-AMD-D] Global Platform Card Technology, Secure Channel Protocol 03, Card Specification v2.2 – Amendment D, Version 1.0, April 2009, GlobalPlatform, Inc.

[GP] Global Platform Card Specification, v2.3.1, March 2018, GlobalPlatform, Inc.

[ICAO-9303-10] ICAO Doc 9303, Machine Readable Travel Documents, Seventh Edition, 2015, Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC), ICAO

[ICAO-9303-11] ICAO Doc 9303, Machine Readable Travel Documents, Seventh Edition, 2015, Part 11: Security Mechanisms for MRTDs.

[ISO14443] ISO/IEC 14443 Proximity Cards - Part 3: Initialization and anti-collision - ISO/IEC 14443- 3:2011.

ISO/IEC 14443 Proximity Cards - Part 4: Transmission protocol - ISO/IEC 14443-2:2008.

[ISO7816] ISO/IEC 7816-4: Part 4: Identification cards - Integrated circuit cards - Organization, security and commands for interchange, ISO, November 2006.

[JC-305] Java Card Platform, Classic Edition 3.0.5 JCRE, JCAPI and JCVM specifications.

[JIL-AAPS] JIL Application of Attack Potential to Smartcards, Version 3.1, June 2020.

[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 2.5, 28 March 2019.

[PP-0055] Protection Profile Machine Readable Travel Document with “ICAO Application”, Basic Access Control, registered under the reference BSI-CC-PP-0055, version 1.1, 25 March 2009.

[PP-0056] Protection Profile Machine Readable Travel Document with ICAO Application, Extended Access Control with PACE (EAC PP), registered under the reference BSI-CC-PP-0056-V2-2012, Version 1.3.2, 05 December 2012.

[PP-0068] Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE, registered under the reference BSI-CC-PP-0068-V2-MA-01, Version 1.0.1, 22 July 2014.

[PP-0084] Security IC Platform Protection Profile with Augmentation Packages Version 1.0, registered under the reference BSI-CC-PP-0084-2014, 13 January 2014.

[PP-JC] Java Card Protection Profile – Open Configuration, Oracle, registered under the reference ANSSI-CCPP-2010/03-M01, v3.0, May 2012.

[ST-PLAT] SECORA™ ID S v1.1 (SLJ52GxxyyyzS) Security Target, Rev. 1.9, 27 January 2021.

[ST] Security Target, ePassport configuration of SECORA™ ID S Applet Collection - eMRTD V1.1, v1.3, 12 April 2021.

[TR-03110-1] Technical Guideline TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 1 - eMRTD with BAC/PACEv2 and EACv1, Version 2.20, 26 February 2015.

[TR-03110-3] Technical Guideline TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 3: Common Specifications, Version 2.21, 21 December 2016.

(This is the end of this report).