Certification Report

SECORA™ ID X v2 Applet Collection with ePasslet Suite v4.0 by cryptovision GmbH, version 1.0 – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE

Sponsor:	***Infineon Technologies AG*** **Am Campeon 1-15** **85579 Neubiberg** **Germany**
Developer:	***cv cryptovision GmbH*** **Munscheidstr. 14** **45886 Gelsenkirchen** **Germany**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-2400168-01-CR**
Report version:	**1**
Project number:	NSCIB-**2400168-01**
Author(s):	**Alireza Rohani**
Date:	**19 May 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 SECORA™ ID X v2 Applet Collection with ePasslet Suite v4.0 by cryptovision GmbH, version 1.0 – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE. The developer of the SECORA™ ID X v2 Applet Collection with ePasslet Suite v4.0 by cryptovision GmbH, version 1.0 – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE is cv cryptovision GmbH located in Gelsenkirchen, Germany and Infineon Technologies AG was 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 a Java Card (SECORA™ ID X v2 Applet Collection with ePasslet Suite v4.0 by cryptovision GmbH, version 1.0) configured to provide a contactless integrated circuit chip containing components for a machine readable travel document (MRTD chip). After instantiation and configuration of the according configuration it can be programmed according to the Logical Data Structure (LDS) and provides the Extended Access Control according to the ICAO document.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 19 May 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 SECORA™ ID X v2 Applet Collection with ePasslet Suite v4.0 by cryptovision GmbH, version 1.0 – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE, 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 SECORA™ ID X v2 Applet Collection with ePasslet Suite v4.0 by cryptovision GmbH, version 1.0 – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL5 augmented (EAL5+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures) and AVA_VAN.5 (Advanced methodical vulnerability analysis).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, 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 SECORA™ ID X v2 Applet Collection with ePasslet Suite v4.0 by cryptovision GmbH, version 1.0 – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE from cv cryptovision GmbH located in Gelsenkirchen, Germany.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	Hardware Platform	IFX_CCI_00005D
Software	Asymmetric Crypto Library (ACL)	03.35.001
	Symmetric Crypto Library (SCL)	02.15.000
	Hardware Support Library (HSL)	03.52.9708
	Hash Crypto Library (HCL) version	01.13.002
	UMSLC	01.30.0564
	Embedded OS	'01 00 07 FA 15 00 00 13 05'
	Applet Collection with ePasslet Suite v4.0 by cryptovision	'0405' (V4.0)

To ensure secure usage a set of guidance documents is provided, together with the SECORA™ ID X v2 Applet Collection with ePasslet Suite v4.0 by cryptovision GmbH, version 1.0 – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE. For details, see section 2.5 "Documentation" of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 1.4.7.

2.2 Security Policy

The TOE is a Java Card (SECORA ID-X Javacard OS Platform) applet configured to provide a contact and contactless integrated chip containing components for machine readable travel document (MRTD chip). After instantiation and configuration it can be programmed to the ICAO documents referenced in the *[ST]* and the set of Security Functional Requirements defined in the *[ST]* and implemented by the TOE.

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 3.2 of the *[ST]*.

2.3.2 Clarification of scope

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

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 consists of:

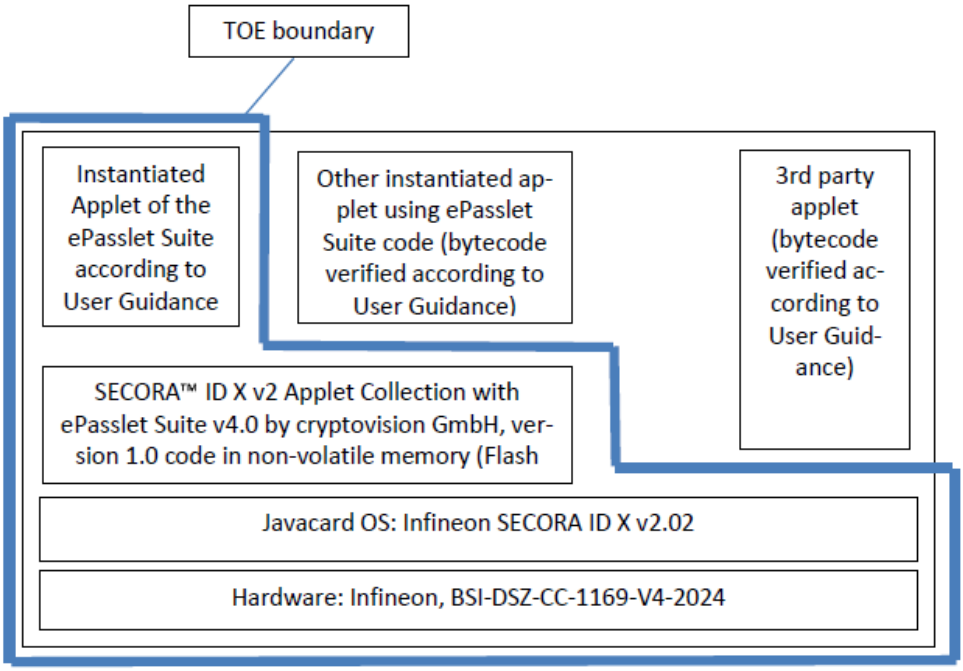

Figure 1 Schematic view on the Target of Evaluation (TOE) and its boundaries. The TOE is based on the Schematic view on the Target of Evaluation (TOE) and its boundaries. The TOE is based on the certified hardware and Javacard OS. Besides the SECORA™ ID X v2 Applet Collection with ePasslet Suite v4.0 by cryptovision GmbH, version 1.0 code in non-volatile memory and the applet instantiated from it which forms the TOE of this security target, it may also contain additional applets which are not part of the TOE.

- the circuitry of the chip (the integrated circuit, IC) including the contact-based interface with hard-ware for the contactless interface including contacts for the antenna, providing basic cryptographic functionalities,
- the platform with the Java Card operation system SECORA ID X v2.02 (please refer to the platform security target *[PL-ST]* for details),
- the guidance documentation of SECORA ID X v2.02 according to *[PL-ST]*,
- SECORA™ ID X v2 Applet Collection with ePasslet Suite v4.0 by cryptovision GmbH, version 1.0 – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Applica-tion", Extended Access Control with PACE,
- the associated guidance documentation: Administrator and User Guidance in PDF format.

The whole applet code resides in the Flash memory; the applets providing these different configurations are instantiated into Flash memory. Multiple configurations (and hence support for different applications) can be present at the same time by instantiating multiple applets with their distinct configurations. Such additional functionality is independent of the functionality of the TOE as

described in this security target and the guidance manuals. This is ensured by the isolation properties of the Java Card platform.

2.5 Documentation

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

Identifier	Version
Secora ID X v2 Applet Collection v1.0 with cryptovision ePasslet Suite v4 – Java Card Applet Suite providing Electronic ID Documents applications. Guidance Manual	Version 1.3, 2025-03-28.
Secora ID X v2 Applet Collection v1.0 with cryptovision ePasslet Suite v4 – Java Card applet configuration providing an ICAO MRTD application with Extended Access Control (EACv1) or with Basic Access Control (BAC) and Supplemental Access Control (SAC) - Preparation Guidance (AGD_PRE)	Version 1.7, 2025-05-06.
Secora ID X v2 Applet Collection v1.0 with cryptovision ePasslet Suite v4 – Java Card applet configuration providing an ICAO MRTD application with Extended Access Control (EACv1) or with Basic Access Control (BAC) and Supplemental Access Control (SAC) - Operational Guidance (AGD_OPE)	Version 1.6, 2025-05-06.
SECORA ID v2.02, Security Guide	1.3, 2024-11-14
SECORA ID v2.02, Administration Guide	1.2, 2024-09-13
SECORA ID v2.02, Extended Datasheet	1.1, 2024-07-30
SECORA™ ID (SLJ38Gxymmmap) Product API Specification	1.00.1193, 2024-03-05
SECORA™ ID v2 Sandbox Application Programmer's Reference Manual	1.0, 2024-04-23
SECORA_ID_v2_Erratasheet	1.1, 2024-12-13
SECORA ID v2.02, Security Guide	1.3, 2024-11-14

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

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

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

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

2.6.2 Independent penetration testing

The methodical analysis performed was conducted along the following steps: When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considers whether potential vulnerabilities can already be identified due to the TOE type and/or specified behavior 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 analyzed using the knowledge gained from all previous evaluation classes. This results in the identification of (additional) potential vulnerabilities. For this analysis will be performed according to the attack methods in *[JIL-AP]* and *[JIL-AM]*. An important source for assurance in this step is the technical report *[PL-ETRfC]* of the underlying platform.

The total test effort expended by the evaluators was two weeks for testing and reporting. During that test campaign, 0% was on Perturbation Attacks, 100% 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 TOE was tested in the following configurations:

- TOE configured in initialization stage
- TOE personalized as MRTD

Functional testing was carried out by witnessing of the developer testing and by repeating some tests by the laboratory. A combination of the standard commercial and proprietary developers tools were used. Penetration testing was performed by using the lab's equipment.

2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

2.7 Reused Evaluation Results

There is no reuse of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number SECORA™ ID X v2 Applet Collection with ePasslet Suite v4.0 by cryptovision GmbH, version 1.0 – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE. The guidance documents describe how to verify the TOE and configure it.

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 SECORA™ ID X v2 Applet Collection with ePasslet Suite v4.0 by cryptovision GmbH, version 1.0 – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application", Extended

Access Control with PACE, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL5 augmented with ALC_DVS.2 and AVA_VAN.5**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims 'strict' conformance to the Protection Profiles *[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.

3 Security Target

The SECORA™ ID X V2 Applet Collection with ePasslet Suite v4.0 by cryptovision GmbH, version 1.0 - Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE, v1.0, 2025-05-06 *[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:

BAC	Basic Access Control
EAC	Extended Access Control
eMRTD	electronic MRTD
ICAO	International Civil Aviation Organisation
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 1 to 5, CC:2022 Revision 1, November 2022
[CEM]	Common Methodology for Information Technology Security Evaluation, CEM:2022 Revision 1, November 2022
[ETR]	Evaluation Technical Report “SECORA™ ID X v2 Applet Collection with ePasslet Suite v4.0 by cryptovision GmbH, version 1.0”, 25-RPT-136, version 3.0, date: 12 May 2025
[PL-CERT]	Certificate, NSCIB-CC-2400063-01, SECORA™ ID v2.02 (SLJ38Gxymm2ap), EAL6 augmented with ALC_FLR.1, 20-12-2024
[PL-ETRfC]	ETR for Composition SECORA™ ID v2.02 (SLJ38Gxymm2ap), 24-RPT-1336 version 2.0, 2024-12-19
[PL-ST]	SECORA™ ID v2.02 (SLJ38Gxymm2ap) Security Target, Rev 1.1, 2024-12-19
[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_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]	SECORA™ ID X V2 Applet Collection with ePasslet Suite v4.0 by cryptovision GmbH, version 1.0 - Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application”, Extended Access Control with PACE, v1.0, 2025-05-06
[ST-lite]	SECORA™ ID X V2 Applet Collection with ePasslet Suite v4.0 by cryptovision GmbH, version 1.0 – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application”, Extended Access Control with PACE, Security Target Lite, v 1.0, 2025-05-06
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)