# Certification Report

# SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.1 – Java Card applet configuration providing Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use with BAC option

| | |
|---|---|
| Sponsor: | ***Infineon Technologies AG***<br>**Am Campeon 1-15**<br>**85579 Neubiberg**<br>**Germany** |
| Developer: | ***cv cryptovision GmbH***<br>**Munscheidstr. 14**<br>**45886 Gelsenkirchen**<br>**Germany** |
| Evaluation facility: | ***SGS Brightsight B.V.***<br>**Brassersplein 2**<br>**2612 CT Delft**<br>**The Netherlands** |
| Report number: | **NSCIB-CC-2500015-01-CR** |
| Report version: | **1** |
| Project number: | NSCIB-**2500015-01** |
| Author(s): | **Alireza Rohani** |
| Date: | **16 February 2026** |
| Number of pages: | **12** |
| Number of appendices: | **0** |

# CONTENTS

**Foreword** **3**

**Recognition of the Certificate** **4**

International recognition 4
European recognition 4

**1 Executive Summary** **5**

**2 Certification Results** **6**

2.1 Identification of Target of Evaluation 6
2.2 Security Policy 6
2.3 Assumptions and Clarification of Scope 7
2.3.1 Assumptions 7
2.3.2 Clarification of scope 7
2.4 Architectural Information 7
2.5 Documentation 7
2.6 IT Product Testing 7
2.6.1 Testing approach and depth 7
2.6.2 Independent penetration testing 8
2.6.3 Test configuration 8
2.6.4 Test results 8
2.7 Reused Evaluation Results 9
2.8 Evaluated Configuration 9
2.9 Evaluation Results 9
2.10 Comments/Recommendations 9

**3 Security Target** **10**

**4 Definitions** **10**

**5 Bibliography** **11**

# 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 Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.1 – Java Card applet configuration providing Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use with BAC option. The developer of the SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.1 – Java Card applet configuration providing Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use with BAC option 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 Applet Collection with ePasslet Suite v.3.5 by cryptovision GmbH, version 1.1) 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 Basic Access Control according to the ICAO document.

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 13 July 2021 (NSCIB-CC-21-0189569). The current evaluation of the TOE has also been conducted by SGS Brightsight B.V. and was completed on 16 February 2026 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 update of underlying java card OS and hardware platform.

The certification took into account that the security evaluation reused the evaluation results of previously performed evaluations. 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 SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.1 – Java Card applet configuration providing Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use with BAC option, 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 Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.1 – Java Card applet configuration providing Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use with BAC option 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 EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures). The composite evaluation package (COMP) is also claimed in the TOE.

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 Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.1 – Java Card applet configuration providing Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use with BAC option 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_000010 |
| Firmware | Firmware | 80.102.06.1 |
| Software | Asymmetric Crypto Library (ACL), including Base, RSA4096, EC, and Toolbox libraries | 2.09.002 |
| | Symmetric Crypto Library (SCL) | 2.04.002 |
| | Hardware Support Library (HSL) | 03.12.8812 |
| | Embedded OS SECORA™ ID X (v1.1) | 1521 |
| | Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH | internal version 3.5.1 |

To ensure secure usage a set of guidance documents is provided, together with the SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.1 – Java Card applet configuration providing Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use with BAC option. For details, see section 2.5 “Documentation” of this report.

## 2.2 Security Policy

The TOE in the **BAC configuration** encompasses the following features:

- TSF_Access manages the access to objects (files, directories, data and secrets) stored in the applet’s file system. It also controls write access of initialization, pre-personalization and personalization data.
- TSF_Admin manages the storage of manufacturing data, pre-personalization data and personalization data.
- TSF_Secret ensures secure management of secrets such as cryptographic keys. This covers secure key storage, access to keys as well as secure key deletion. These mechanisms are mainly provided by TSF_OS.
- TSF_Crypto performs high level cryptographic operations. The implementation is mainly based on the Security Functionalities provided by TSF_OS. The supported crypto mechanisms are:
  - Triple-DES for encryption/decryption and MAC calculation.
  - SHA-1 for key derivation
- TSF_SecureMessaging realizes a secure communication channel with MACs and encryption based on Triple-DES (112 bit key length).
- TSF_Auth_Sym performs an authentication mechanism based on TDES used for BAC and based on AES for symmetric authentication with pre-shared keys for personalization.
- TSF_Integrity protects the integrity of internal applet data like the Access control lists.

- TSF_OS contains all security functionalities provided by the certified platform (IC, crypto library, Javacard operation system). Besides some minor additions, the cryptographic operations are provided by this platform.

## 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

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 an applet and the certified Java Card platform (SECORA™ ID X (SLJ52GxAyyyzX)) that can be configured to be used as an eMRTD with BAC and EAC.

## 2.5 Documentation

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

| Identifier | Version |
|---|---|
| Secora ID X Applet Collection v1.1 with cryptovision ePasslet Suite v3.5 – Java Card Applet Suite providing Electronic ID Documents applications. Guidance Manual. | Document Version 1.2.4, 2025-11-10. |
| Secora ID X Applet Collection v1.1 with cryptovision ePasslet Suite v3.5 – 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). | Document Version 1.4.1, 2026-01-28. |
| Secora ID X Applet Collection v1.1 with cryptovision ePasslet Suite v3.5 – 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). | Document Version 1.3.1, 2026-01-28. |

## 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.

During the first recertification the developer tests were performed on an actual TOE sample in its evaluated configuration. The repeated (witnessed) tests are performed on samples with an older OS build (1519), but the results are valid for this current version of the TOE.

### 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 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. 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 [plat-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

In total 0 physical attacks, 0 tests covering overcoming sensors and filters, 1 perturbation attacks, 0 attacks retrieving keys with FA, 0 side-channel attacks, 0 attacks exploiting test features, 0 attacks on the RNG, 0 attacks applying ill-formed applets, 1 software attack and 0 attacks on application isolation were performed, for a total of 2 weeks. During the recertification, only logical tests were performed, defined as part of ATE & AVA.

### 2.6.3 Test configuration

The TOE was tested in the following configurations:

TOE configured in initialization stage (configuration 1)

TOE personalized as MRTD (BAC and EAC) (configuration 2)

TOE personalized as SSCD (configuration 3)

During the first recertification, the ATE_IND tests (both the witnessed tests, and the independent evaluator tests) have been executed on a TOE version that is not the final one (OS build 1519, instead of 1521). This is considered acceptable, as build 1519 contains the majority of code changes with security and functional impact (code changes meant to address requirements of the updated HW crypto library). The only difference between build 1519 of the OS and 1521 is the change of a SCL parameter value in the OS code, meant to address the following HW security guidance update:

*Improved SCP configuration to increase DFA protection.*

This has no negative security impact towards the TOE, as it consists of a security improvement for DFA protection. Furthermore, the Applet TOE follows all the guidance of the OS platform, which in turn follows the guidance of the IC platform.

### 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 development and production of the TOE, by use of several site certificate and Site Technical Audit Reports.

No sites have been visited as part of this evaluation.

The EUCC certificate [HW-CERT] of the underlying HW, issued by the SOGIS CB BSI, has been re-used, using the same standards, methodology, and interpretations.

## 2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.1 – Java Card applet configuration providing Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use with BAC option.

## 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 Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.1 – Java Card applet configuration providing Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use with BAC option, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL4 augmented with ALC_DVS.2**. The composite evaluation package (COMP) is also claimed in the TOE. 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]*.

## 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 Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.1 – Java Card applet configuration providing Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use with BAC option – Security Target, v2.12, 2026-01-28 *[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 |
| 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 |
| [Plat-CERT] | Certificate SECORA™ ID X v1.2 (SLJ52GxAyyyzX), NSCIB-CC-2400127-01, 12 February 2026 |
| [Plat-ETRfC] | Evaluation Technical Report for Composition “SECORA™ ID X v1.2 (SLJ52GxAyyyzX)” – EAL5+/6+, 25-RPT-569, v7.0 |
| [Plat-ST] | SECORA™ ID X v1.2 (SLJ52GxAyyyzX), Revision 3.0, 2026-01-08 |
| [COMP] | Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.6, April 2024 |
| [ETR] | Evaluation Technical Report “SECORA™ ID X v1.2 Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH” – EAL4+/EAL5+, 25-RPT-1204, version 2.0, 30 January 2026 |
| [HW-CERT] | Certification Report EUCC-3087-2025-12-0001, Administration ID BSI-DSZ-CC-1079-V6-2025 for Infineon Security Controller IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step G12 from Infineon Technologies AG |
| [HW-ST] | Public Security Target IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch; G12 Including optional Software Libraries Flash Loader – 3x ACL – 2xHSL – 2xSCL – HCL - CCL – NRG; Author: Infineon Technologies AG, Revision: 3.7 |
| [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 |
| [ST] | SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.1 – Java Card applet configuration providing Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use with BAC option – Security Target, v2.12, 2026-01-28 |
| [ST-lite] | SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.1 - Java Card applet configuration providing Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use with BAC option, v2.12, 2026-01-29 |
| [ST-SAN] | ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006 |

(This is the end of this report.)