Certification Report

SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.0 – Java Card applet configuration providing Secure Signature Creation Device with key import (SSCD)

Sponsor: ***Infineon Technologies AG***
Am Campeon 1 – 15,
85579 Neubiberg
Germany

Developer: ***cv cryptovision GmbH***
Munscheidstr. 14
45886 Gelsenkirchen
Germany

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

Report number:	**NSCIB-CC-0189594-CR**
Report version:	**2**
Project number:	**0189594**
Author(s):	**Jordi Mujal**
Date:	**14 October 2021**
Number of pages:	**13**
Number of appendices:	**0**

Head Office:
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 Netherlands Chamber of Commerce (KVK), 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 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, 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, 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 was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the 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. The current list of signatory nations and approved certification schemes can be found at: http://www.commoncriteriaportal.org.

European recognition

The European SOG-IS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 effective since 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 (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 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 at: http://www.sogisportal.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 1.0 – Java Card applet configuration providing Secure Signature Creation Device with key import (SSCD). The developer of the SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.0 – Java Card applet configuration providing Secure Signature Creation Device with key import (SSCD) 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 consists of an applet and the certified Java Card platform (SECORA ID-X Javacard OS platform) *[PL-CERT]* that can be configured to provide a secure signature creation device (SSCD) with key import for the creation of electronic signatures and electronic seals according to [EN419211-3]. To allow secure access to the signature functionality over the contactless interface, it provides an optional PACE mechanism to build up a secure channel for the signature PIN.

The TOE is delivered during the preparation phase after which the initialisation and personalisation are performed.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 21 June 2021 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 Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.0 – Java Card applet configuration providing Secure Signature Creation Device with key import (SSCD), 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 1.0 – Java Card applet configuration providing Secure Signature Creation Device with key import (SSCD) 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 (EAL4+) 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, 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. 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 releasable 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 1.0 – Java Card applet configuration providing Secure Signature Creation Device with key import (SSCD) 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
Software	Firmware	80.102.06.1
Software	Asymmetric Crypto Library (ACL), including Base, RSA4096, EC, and Toolbox libraries	2.07.003
Software	Symmetric Crypto Library (SCL)	2.04.002
Software	Hardware Support Library (HSL)	03.12.8812
Software	Embedded OS SECORA™ ID X (v1.1)	1482
Software	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 1.0 – Java Card applet configuration providing Secure Signature Creation Device with key import (SSCD). For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle refer to the *[ST]*, chapter 1.4.7.

2.2 Security Policy

The TOE is a Java Card configured to provide a contact and contactless integrated-circuit (IC) chip containing components to securely create, use and manage signature-creation data (SCD) with key import for the creation of electronic signatures and electronic seals according to [EN419211-3]. To allow secure access to the signature functionality over the contactless interface, it provides an optional PACE mechanism to establish a secure channel for the signature PIN.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

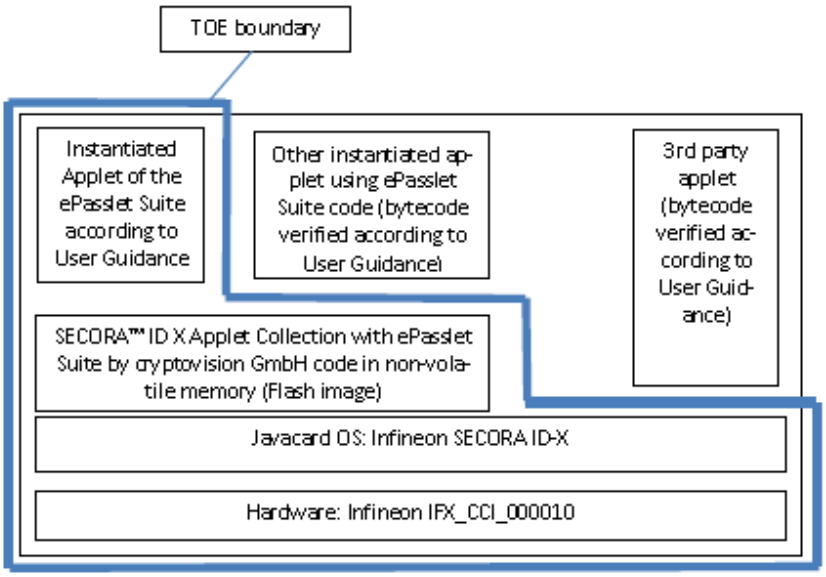
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 3.2 of the *[ST]*.

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.

2.4 Architectural Information

The TOE consists of:



- The circuitry of the chip (the integrated circuit, IC) including the contact-based interface with hardware for the contactless interface including contacts for the antenna, providing basic cryptographic functionalities.
- The platform with the Java Card operation system SECORA ID-X (SLJ52GxAyyyzX; please refer to the platform security target *[PL-ST]* for details of this designation),
- The guidance documentation of SECORA ID-X (SLJ52GxAyyyzX) according to *[PL-ST]*, section 1.4.1.4.
- SECORA™ ID X Applet Collection with ePasslet Suite v.3.5 by cryptovision GmbH, version 1.0 – Java Card applet configuration providing a secure signature creation device (SSCD) with key import.
- The associated guidance documentation: Administrator and User Guidance in PDF format.

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 the *[ST]* 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 Applet Collection v1.0 with cryptovision ePasslet Suite v3.5 – Java Card applet configuration providing a Secure Signature Creation Device application with on-chip key generation / key import Preparation Guidance (AGD_PRE)	1.0.6
SECORA™ ID X Applet Collection v1.0 with cryptovision ePasslet Suite v3.5 –, Java Card applet configuration, providing a Secure Signature Creation Device, application with on-chip key generation / key import,	1.0.5

Operational Guidance (AGD_OPE)	
SECORA™ ID X Applet Collection v1.0 with cryptovision ePasslet Suite v3.5 – Java Card Applet Suite providing Electronic ID Documents applications, Guidance Manual	1.0.9
SECORA™ ID X v1.1 Administration Guide	1.50
SECORA™ ID X v1.1 Security Guide	1.40
SECORA™ ID X v1.1 Databook	1.40
SECORA™ ID X v1.1 SLJ52GxxyyyzX System Release Notes	1.20
SECORA™ ID X v1.1 Product API Specification	1.00.1482

2.6 IT Product Testing

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

2.6.1 Testing approach and depth

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

The underlying hardware, crypto-library and Javacard test results are extendable to composite evaluations, as 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 has provided samples and a test environment. The evaluators have 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 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-AAPS]* and *[JIL-AM]*. An important source for assurance in this step is the ETR for composition of the underlying platform *[PL-CERT]*.
- 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% of the total time was spent on Perturbation attacks and 50% on logical tests.

2.6.3 Test configuration

It has been tested in pre-personalisation, personalisation and operational life-cycle states with applet instance configurations specified in the Security Target [ST].

Functional testing was carried out by witnessing of the developer testing and by repeating some tests by the Laboratory. A combination of standard commercial tools and proprietary developer 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 Re-Used Evaluation Results

There is no re-use of evaluation results in this certification.

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 1.0 – Java Card applet configuration providing Secure Signature Creation Device with key import (SSCD). The guidance documents describe how to verify the TOE and configure it.

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 SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.0 – Java Card applet configuration providing Secure Signature Creation Device with key import (SSCD), to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 5 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 Profile *[EN419211-3]*.

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 1.0–Java Card applet configuration providing Secure Signature Creation Device with key import (SSCD)-Security Target, Version 1.6, 11 June 2021 *[ST]* is included here by reference.

Please note that for the need of 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:

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
SCD	Signature Verification Device
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
[ETR]	ETR EAL5+ SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.0, 20-RPT-675, version 7.0, 18 June 2021.
[PL-CERT]	Certification Report SECORA™ ID X v1.1 (SLJ52GxAyyyzX), Report Number: NSCIB-CC-0031318-CR2, TÜV Rhein-land Nederland B.V., 16 April 2021.
[PL-ST]	SECORA™ ID X v1.1 (SLJ52GxAyyyzX), Rev1.3, 22 March 2021.
[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
[EN419211-3]	EN 419 211-3:2013, Protection profiles for secure signature creation device - Part 3: Device with key import, V1.0.2, registered under the reference BSI-CC-PP-0075-2012-MA-01
[ST]	SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.0– Java Card applet configuration providing Secure Signature Creation Device with key import (SSCD)- Security Target, Version 1.6, 11 June 2021
[ST-lite]	SECORA™ ID X Applet Collection with ePasslet Suite v3.5 by cryptovision GmbH, version 1.0– Java Card applet configuration providing Secure Signature Creation Device with key import (SSCD)- Security Target Lite, Version 1.6, 11 June 2021
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)