

Certification Report

SECORA™ ID X v1.2 (SLJ52GxAyyyzX)

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

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

Report number: **NSCIB-CC-2400127-01-CR**

Report version: **1**

Project number: **NSCIB-2400127-01**

Author(s): **Jordi Mujal**

Date: **12 February 2026**

Number of pages: **12**

Number of appendices: **0**

Reproduction of this report is authorised only if the report is reproduced in its entirety.

CONTENTS

Foreword	3
Recognition of the Certificate	4
International recognition	4
European recognition	4
1 Executive Summary	5
2 Certification Results	7
2.1 Identification of Target of Evaluation	7
2.2 Security Policy	7
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	8
2.6 IT Product Testing	8
2.6.1 Testing approach and depth	8
2.6.2 Independent penetration testing	9
2.6.3 Test configuration	9
2.6.4 Test results	9
2.7 Reused Evaluation Results	9
2.8 Evaluated Configuration	10
2.9 Evaluation Results	10
2.10 Comments/Recommendations	10
3 Security Target	11
4 Definitions	11
5 Bibliography	12

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.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

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 v1.2 (SLJ52GxAyyyzX). The developer of the SECORA™ ID X v1.2 (SLJ52GxAyyyzX) 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 is a Java Card Platform compliant with Java Card Specification (Classic Edition) version 3.0.5 and GlobalPlatform Specification v.2.3.1 and the GlobalPlatform Card ID Configuration v1.0. The TOE allows post-issuance downloading of applications that have been previously verified by an off-card verifier. It constitutes a secure generic platform that supports multi-application runtime environment and provides facilities for secure loading and interoperability between different applications.

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 30 August 2022 ([CC-22-0031318](#)). The current evaluation of the TOE has also been conducted by SGS Brightsight B.V. and was completed on 12 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:

- Guidance documents update
- HW platform recertification
- OS updates
- ST updated to CC:2022 with multi assurance claim

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 v1.2 (SLJ52GxAyyyzX), 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 v1.2 (SLJ52GxAyyyzX) 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 following multi assurance package:

Global conformance EAL5 augmented (EAL5+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_TAT.3, ALC_FLR.1, ATE_COV.3, ATE_FUN.2 and AVA_VAN.5. Also, Composite product package.

The access control policy sub-TSF meets EAL6 augmented with ALC_FLR.1.

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

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



NSCIB Certified Products list. Note that the certification results apply only 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 SECORA™ ID X v1.2 (SLJ52GxAyyyzX) from Infineon Technologies AG located in Neubiberg, 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	1521

To ensure secure usage a set of guidance documents is provided, together with the SECORA™ ID X v1.2 (SLJ52GxAyyyzX). 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 1.4.4.

2.2 Security Policy

The TOE is a Java Card Platform compliant with Java Card Specification (Classic Edition) version 3.0.5 and GlobalPlatform Specification v.2.3.1 and the GlobalPlatform Card ID Configuration v1.0. The TOE allows post-issuance downloading of applications that have been previously verified by an off-card verifier. It constitutes a secure generic platform that supports multi-application runtime environment and provides facilities for secure loading and interoperability between different applications.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

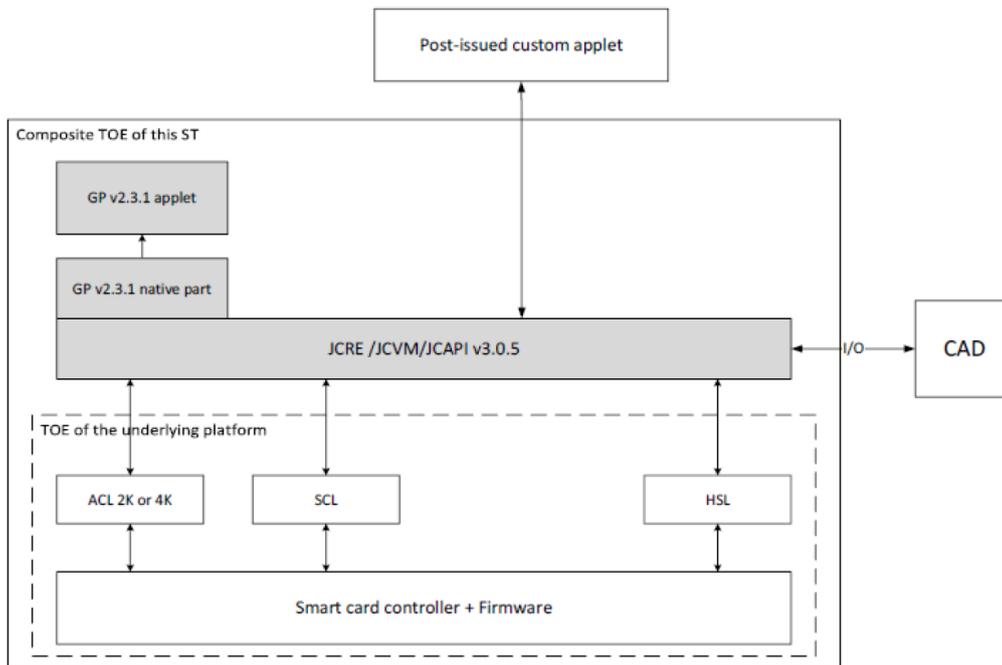
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 5.2 of the [ST].

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 logical architecture, originating from the Security Target of the TOE can be depicted as follows:



The TOE has the features that are described in Section 1.3.2 of [ST]. In the following, the JCRC/JVM/JCAPI v3.0.5 is referred to as JC OS.

2.5 Documentation

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

Identifier	Version
SECORA™ ID X v1.2 Administration Guide	1.70
SECORA™ ID X v1.2 Data Book	1.90
SECORA™ ID X v1.2 Security Guide	2.10
SECORA™ ID X v1.2 SLJ52GxAyyyZ System Release Notes	1.80
SECORA™ ID X v1.2 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 performed extensive testing on functional specification, subsystem and SFR-enforcing module level. All parameter choices were addressed at least once. All boundary cases identified were tested explicitly, and additionally the near-boundary conditions were covered probabilistically. The testing was largely automated using industry standard and proprietary test suites. Test scripts were used extensively to verify that the functions return the expected values.

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

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

2.6.2 Independent penetration testing

The methodical analysis 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.
- A thorough implementation representation review (ADV_IMP) was performed. The analysis was driven by the attack methods defined in [JIL-AP]. An important source for assurance in this step is the technical report [HW-ETRFC] of the underlying platform.
- All potential vulnerabilities are analysed and a judgment was made on their exploitability. The potential vulnerabilities are addressed by penetration testing, a guidance update or code update.

The total test effort expended by the evaluators was 7 weeks. During that test campaign, 14.3% of the total time was spent on Perturbation attacks, 71.4% on side-channel testing, and 14.3% on logical tests.

2.6.3 Test configuration

The configuration of the sample used for independent evaluator testing and penetration testing was the same as described in the [ST].

Penetration testing was also performed on an earlier revision of the TOE. The assurance gained from testing on an earlier revision has been assessed to be valid for the final TOE version, because the changes introduced were minimal and did not have an impact on the TSF.

2.6.4 Test results

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

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

No exploitable vulnerabilities were found with the independent penetration tests.

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

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

The strength of the implementation of the cryptographic functionality has been assessed in the evaluation, as part of the AVA_VAN activities.

For composite evaluations, please consult the [ETRFC] for details.

2.7 Reused Evaluation Results

There is no reuse of evaluation results in this certification.

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

The EUCC certificate EUCC-3087-2025-12-0001 of the underlying platform, issued by the SOGIS CB BSI, has been re-used, using the same standards, methodology, and interpretations.

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 SECORA™ ID X v1.2 (SLJ52GxAyyyzX).

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the [ETR], which references an ASE Intermediate Report and other evaluator documents. To support composite evaluations according to [COMP] a derived document [ETRFC] was provided and approved. This document provides details of the TOE evaluation that must be considered when this TOE is used as platform in a composite evaluation.

The verdict of each claimed assurance requirement is “Pass”.

Based on the above evaluation results the evaluation lab concluded the SECORA™ ID X v1.2 (SLJ52GxAyyyzX), to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of:

EAL 5 augmented with ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_TAT.3, ALC_FLR.1, ATE_COV.3, ATE_FUN.2 and AVA_VAN.5 for Global conformance.

EAL6 augmented with ALC_FLR.1 for the access control policy sub-TSF.

The Security Target claims ‘demonstrable’ conformance to the Protection Profile [JCPP].

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 “Documentation” contains necessary information about the usage of the TOE. Certain aspects of the TOE’s security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: None.

Not all key sizes specified in the [ST] have sufficient cryptographic strength to satisfy the AVA_VAN.5 “high attack potential”. To be protected against attackers with a “high attack potential”, appropriate cryptographic algorithms with sufficiently large cryptographic key sizes shall be used (references can be found in national and international documents and standards).

3 Security Target

The SECORA™ ID X v1.2 (SLJ52GxAyyyzX) Security Target, Rev 3.0, 08 January 2026 [ST] is included here by reference.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

AES	Advanced Encryption Standard
APDU	Application Protocol Data Unit
CRT	Chinese Remainder Theorem
EC	Elliptic Curve
ECDH	Elliptic Curve Diffie-Hellman algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
GPAPI	Global Platform Application Programming Interface
IO	Input/Output
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JCAPI	Java Card Application Programming Interface
JCVM	Java Card Virtual Machine
JIL	Joint Interpretation Library
KDF	Key Derivation Function
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PACE	Password-Authenticated Connection Establishment
PKCS	Public Key Cryptography Standards
PP	Protection Profile
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
TDES	Triple Data Encryption Standard
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

- [CC] Common Criteria for Information Technology Security Evaluation, Parts 1 to 5, CC:2022 Revision 1, November 2022
- [CEM] Common Methodology for Information Technology Security Evaluation, CEM:2022 Revision 1, November 2022
- [COMP] Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.6, April 2024
- [ETR] Evaluation Technical Report “SECORA™ ID X v1.2 (SLJ52GxAyyyzX)” – EAL5+/6+, 25-RPT-209, version 7.0, 12 February 2026
- [ETRFc] Evaluation Technical Report for Composition “SECORA™ ID X v1.2 (SLJ52GxAyyyzX)” – EAL5+/6+, 25-RPT-569, version 7.0, 10 February 2026
- [HW-CERT] EUCC-3087-2025-12-0001, Administration ID BSI-DSZ-CC-1079-V6-2025 Smartcard Controller 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, 19 December 2025
- [HW-ETRFc] EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION (ETR COMP) Common Criteria CC 2022 (Multi-Assurance with global assurance level EAL5 augmented with ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_FLR.3, ALC_TAT.3, ATE_FUN.2, ATE_COV.3, AVA_VAN.5 and sub-TSF assurance level EAL6 augmented with ALC_FLR.3) for the Product BSI-DSZ-CC-1079-V6, 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 from Infineon Technologies AG Version 4, 2025-12-18,
- [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, version 3.7, 28 November 2025
- [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
- [JCPP] Javacard Protection Profile Open Configuration, v3.0.5, December 2017, registered under the reference BSI-CC-PP-0099-2017.
- [ST] SECORA™ ID X v1.2 (SLJ52GxAyyyzX) Security Target, Rev 3.0, 08 January 2026

(This is the end of this report.)