TÜV Rheinland Nederland B.V.

TÜVRheinland®
Precisely Right.

Certification Report

SECORA™ ID X (SLJ52GxAyyyzX)

Sponsor and developer: ***Infineon Technologies AG***
81726 Munich
Germany

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

Report number: **NSCIB-CC-0031318-CR**

Report version: **1.1**

Project number: **0031318**

Author(s): **Wouter Slegers**

Date: **20 July 2020**

Number of pages: **12**

Number of appendices: **0**

Reproduction of this report is authorized provided the report is reproduced in its entirety.

Headoffice:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Dutch Chamber of Commerce under number 27288788

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS:

Foreword 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 6
2.4 Architectural Information 6
2.5 Documentation 7
2.6 IT Product Testing 7
2.7 Re-used evaluation results 9
2.8 Evaluated Configuration 9
2.9 Results of the Evaluation 9
2.10 Comments/Recommendations 9

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, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a license is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

Recognition of the certificate

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations.

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the SECORA™ ID X (SLJ52GxAyyyzX). The developer of the SECORA™ ID X (SLJ52GxAyyyzX) is Infineon Technologies AG located in Munich, 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 has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 9 July 2020 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]*.

A minor update to the ETR and this Certification Report addressing a minor but impactful typo in the versions of the guidance addressed. The *[ST]* continues to list the correct versions.

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 (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 (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 provides sufficient evidence that the TOE meets the EAL6 augmented (EAL6+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.1 (Basic Flaw Remediation).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 5 *[CC]*.

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. It should be noted that the certification results only apply to the specific version of the product as evaluated.

[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 (SLJ52GxAyyyzX) from Infineon Technologies AG located in Munich, Germany.

The TOE is comprised of the following main components:

	Name	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	2.07.003
	Symmetric Crypto Library (SCL)	2.04.002
	Hardware Support Library (HSL)	03.12.8812
	Embedded OS	1358

No other optional IC dedicated software library is used in the embedded software.

To ensure secure usage a set of guidance documents is provided together with the SECORA™ ID X (SLJ52GxAyyyzX). Details can be found in section 2.5 of this report.

For a detailed and precise description of the TOE lifecycle refer to the *[ST]*, chapter 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. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in 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:

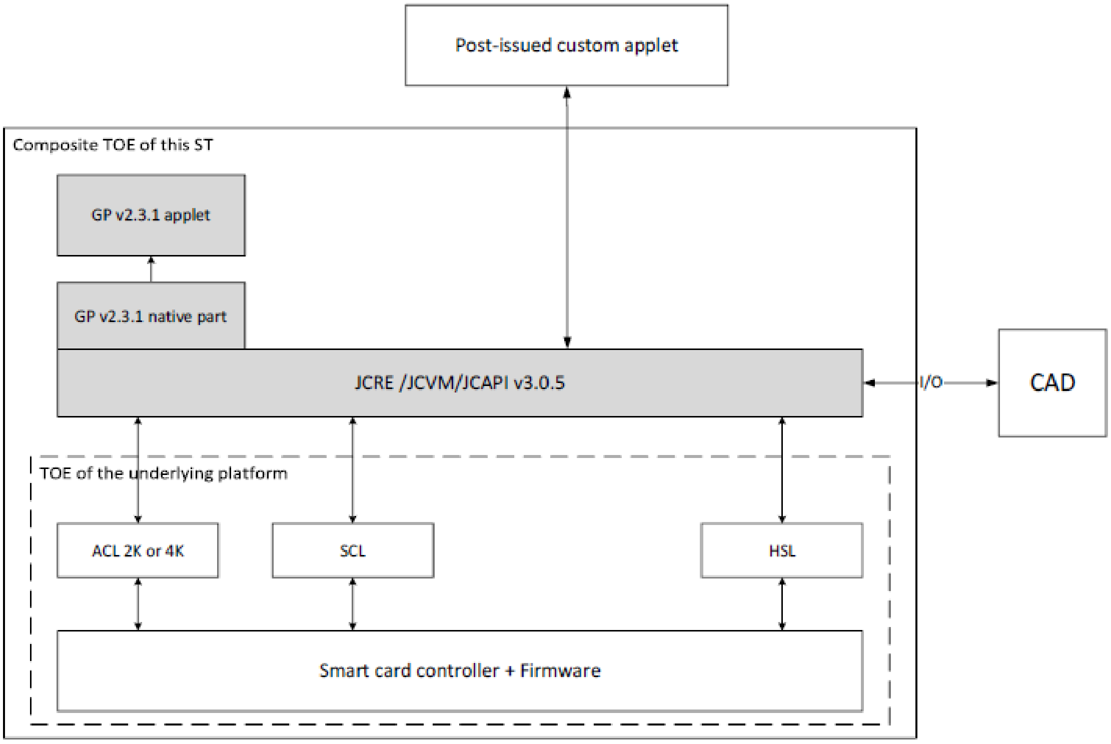

Figure 1 Logical architecture of the TOE.

The TOE has the features that are described in Section 1.3.2 of *[ST]*. In the following, the JCRE/JCVM/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:

Reference	Name	Version	Date
[AG]	SECORA™ ID X Administration Guide	1.40	2020-03-09
[DB]	SECORA™ ID X Databook	1.30	2020-06-08
[SG]	SECORA™ ID X Security Guide	1.30	2020-03-09
[SRN]	SECORA™ ID X SLJ52GxxyyyzX System Release Notes	1.10	2020-06-08
[API]	SECORA™ ID X Product API Specification	1.00.1358	2020-03-09

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 SFR-enforcing 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 and crypto-library 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. This analysis has been performed according to the attack methods 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 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 3 perturbation attacks, 1 side-channel attack, 2 logical attack penetration tests were performed, for a total of 12 weeks.

2.6.3 Test Configuration

The TOE was to tested in the following configuration:

- HW identifier: 80 03 00 00 10
- EMVCo identifier: 81 06 00 22 00 1C 00 00
- JC OS Build Number: 82 02 13 58
- HCL version: 83 04 00 00 00 00
- ACL version: 84 05 20 70 03 34 20
- SCL version: 85 04 20 40 02 20
- HSL version: 86 04 03 12 88 12
- RSA: 87 02 00 01

This is the same configuration as stated in the ST.

2.6.4 Testing Results

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

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

No exploitable vulnerabilities were found with the independent penetration tests.

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

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. No exploitable vulnerabilities were found with the independent penetration tests.

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

2.7 Re-used evaluation results

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

There has been extensive re-use of the ALC aspects for the sites involved in the software component of the TOE. There has been extensive re-use of the ALC aspects for the sites involved in the development and production of the TOE, by use of 6 Site Technical Audit Re-use report approaches.

Sites involved in the development and production of the hardware platform were re-used by composition.

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 (SLJ52GxAyyyzX).

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]* which references a ASE Intermediate Report and other evaluator documents. To support composite evaluations according to *[CCDB-2007-09-01]* a derived document *[ETRfC]* was provided and approved. This document provides details of the TOE evaluation that have to 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 (SLJ52GxAyyyzX), to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 6** augmented with ALC_FLR.1. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims 'demonstrable' conformance to the Protection Profile *[PP]*.

2.10 Comments/Recommendations

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

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

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

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

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength for satisfying the AVA_VAN.5 "high attack potential". In order 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 (SLJ52GxAyyyzX) Security Target, Rev 1.1, dated 2020-06-09 *[ST]* is included here by reference.

4 Definitions

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

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 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] Evaluation Technical Report SECORA™ ID X (SLJ52GxAyyyzX), 20-RPT-305, Version 4.0.

[ETRfC] ETR for Composition Evaluation SECORA™ ID X (SLJ52GxAyyyzX), 20-RPT-306, Version 3.0.

[HW-CERT] BSI-DSZ-CC-1079-V2-2020 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 and including optional software libraries and dedicated firmware, 2020-06-16.

[HW-ETRfC] EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION (ETR COMP) BSI-DSZ-CC-1079-V2, Version 2, 2020-05-15.

[HW-ST] Public Security Target Common Criteria v3.1 – EAL6 augmented / EAL 6+ 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, Revision 0.8, 2020-04-03.

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.

[PP] Java Card Protection Profile Open Configuration 3.0.5.

[ST] SECORA™ ID X (SLJ52GxAyyyzX) Security Target, Rev 1.1, dated 2020-06-09.

(This is the end of this report).