TrustCB B.V.

Certification Report

SECORA™ ID v2.01 (SLJ38Gxymm1ap)

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-2400062-01-CR**

Report version: **1**

Project number: NSCIB-**2400062-01**

Author(s): **Jordi Mujal, Alireza Rohani**

Date: **20 December 2024**

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 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 8
2.6 IT Product Testing 8
2.6.1 Testing approach and depth 9
2.6.2 Independent penetration testing 9
2.6.3 Test configuration 9
2.6.4 Test results 9
2.7 Reused Evaluation Results 10
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 v2.01 (SLJ38Gxymm1ap). The developer of the SECORA™ ID v2.01 (SLJ38Gxymm1ap) 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 based on the following specifications:

- Java Card Specification (Classic Edition) version 3.1
- GlobalPlatform Card Specification v.2.3.1
- GlobalPlatform Amendment D (Version 1.1.1)
- GlobalPlatform Amendment E (Version 1.0)
- GlobalPlatform Financial Configuration v1.0.2
- GlobalPlatform Common Implementation Configuration v2.1

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 SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 20 December 2024 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 v2.01 (SLJ38Gxymm1ap), 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 v2.01 (SLJ38Gxymm1ap) 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 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]* (Parts I, II and III).

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 v2.01 (SLJ38Gxymm1ap) from Infineon Technologies AG located in Neubiberg, Germany.

The TOE is comprised of the following main components (The TOE consists of two configurations):

Delivery item type	Identifier	Version
Hardware	IFX_CCI_00005D	S11
Firmware	BOS & POWS & RFAPI (ROM)	80.309.05.0
	Flash-loader	09.13.0004
IC Software	ACL	03.35.001
	SCL	02.15.000
	HSL	03.52.9708
	HCL	01.13.002
	UMSLC	01.30.0564
Embedded OS software	JCVM 3.1, JCRE 3.1, JCAPI 3.1 and GP 2.3.1 framework with CIC and FC Config, proprietary API	CONF1: '01 00 02 FA 15 00 00 13 05'
		CONF2: '01 00 0C FA 15 00 00 13 05'

To ensure secure usage a set of guidance documents is provided, together with the SECORA™ ID v2.01 (SLJ38Gxymm1ap). For details, see section 2.5 "Documentation" of this report.

2.2 *Security Policy*

The Java Card OS supports an open platform mode. In this mode loading, installation and deletion of several applet packages are permitted post issuance. This is default mode.

The Java Card OS supports the following cryptographic algorithms:

- AES 128/192/256 Cipher Scheme for secure messaging (ENC), message authentication (MAC) and authentication procedures
- TDES Cipher Scheme for secure messaging (ENC), message authentication (MAC) and authentication procedures
- RSA encryption and decryption up to 4k
- ECDSA with SHA-1/SHA-2
- RSA PKCS#1 with SHA-1/SHA-2
- RSA PSS with SHA256

Key agreement algorithms

- ECDH with KDF and with XY
- PACE with generic mapping and chip authentication mapping

Key pair generation

- EC
- RSA with modulus/exponent and CRT

Message digest algorithms

- SHA-1 (SHA-1 as a security algorithm is only used as part of a session key derivation)
- SHA-2 family: SHA224, SHA256, SHA384, SHA512
- HMAC family: SHA256, SHA384, SHA512

Random number generation algorithms

- Hybrid physical RNG according to AIS31 PTG.2, PTG.3 and DRG.4

Java Card OS proprietary features:

- Java Card static mode
- Java Card native mode
- LDS-API
- PACE API
- SandBox
- In-Field-Update (IFU) Loader

GlobalPlatform features:

- GlobalPlatform GP FC and CIC profile
- Secure channel
- Logical channel
- Optional APIs
- Global object
- TOE identification
- Administration options

For the details of features, see section 1.3.2 of the *[ST]*.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

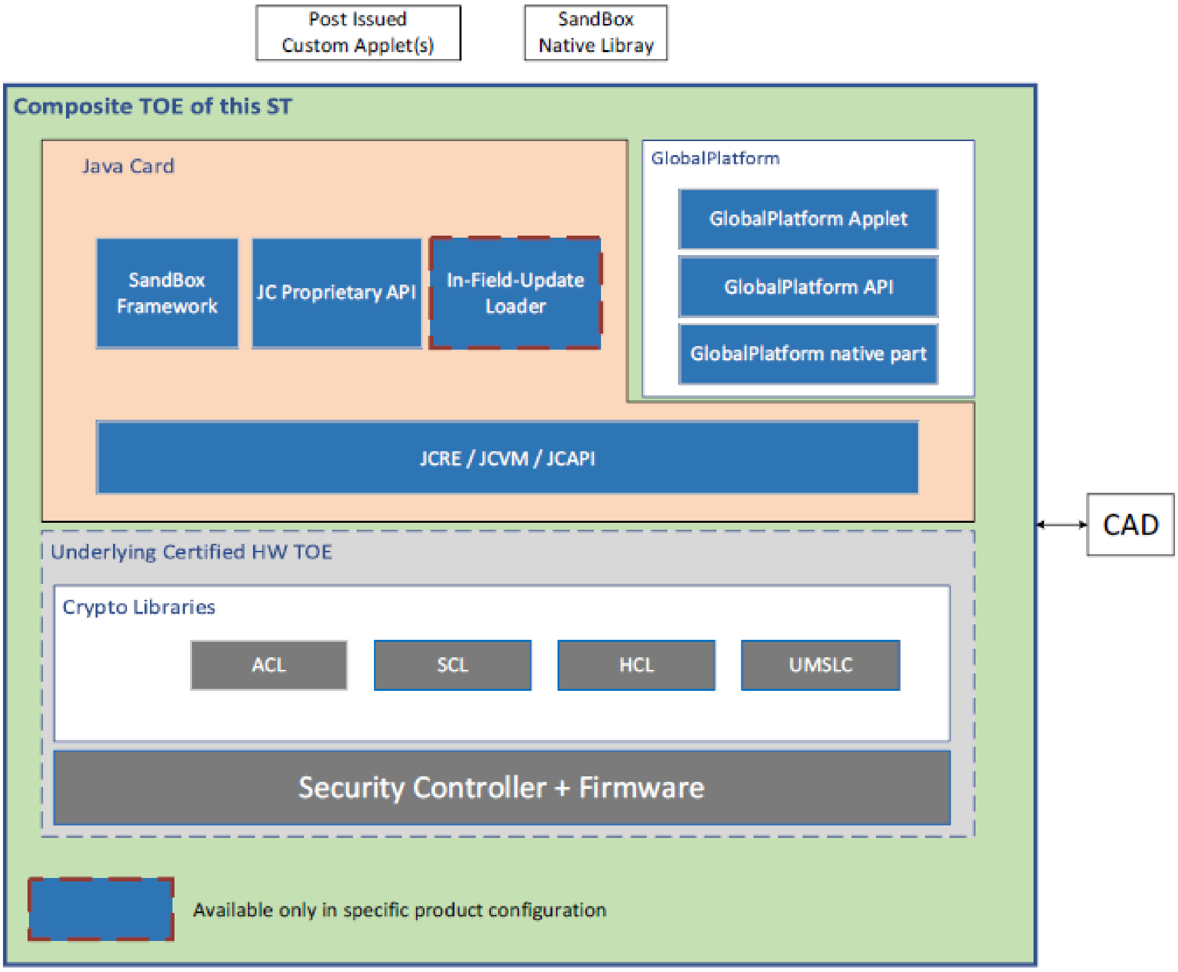
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.4 of the *[ST]*.

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 hardware and the software described in section 2.1



2.5 Documentation

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

Identifier	Version
SECORA™ ID v2.01 (SLJ38Gxymm1ap) Administration Guide	Revision 1.4/2024-12-13
SECORA™ ID v2.01 (SLJ38Gxymm1ap) Extended datasheet	Revision 1.2/2024-07-30
SECORA™ ID v2.01 (SLJ38Gxymm1ap) Security Guide	Revision 1.5/2024-12-02
SECORA™ ID v2 (SLJ38Gxymmmap) Product API Specification	Rev 1.00.1193/2024-03-05
SECORA™ ID v2 (SLJ38Gxymmmap) Sandbox Application Programmer's Reference Manual	Rev 1.0/2024-04-23
SECORA™ ID v2 (SLJ38Gxymmmap) Errata sheet	Rev 1.1/2024-12-13

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 is performed during the baseline evaluation and it is 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-AAPS]*. 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.

The total test effort expended by the evaluators was 12 weeks. During that test campaign, 41% of the total time was spent on Perturbation attacks, 50% on side-channel testing, and 9% on application isolation and software attacks.

2.6.3 Test configuration

The penetration tests were performed on both OS builds, i.e., CONF1 and CONF2. Due to the similarities (and only minor differences) between these configurations, the results equally apply to all the two OS Builds.

The testing was performed on earlier OS versions. Due to the minor differences between these configurations, the results equally apply to final OS version of the TOE.

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.

The algorithmic security level exceeds 100 bits for all evaluated cryptographic functionality as required for high attack potential (AVA_VAN.5).

2.7 Reused Evaluation Results

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of 6 site certificates and Site Technical Audit Reports.

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 v2.01 (SLJ38Gxymm1ap). There are two configurations of the TOE, each one has a unique identification.

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 v2.01 (SLJ38Gxymm1ap), to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL6 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 "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 v2.01 (SLJ38Gxymm1ap), Rev 1.1, 19 December 2024 *[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
DES	Data Encryption Standard
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
EMFI	Electro-Magnetic Fault Injection
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
LAN	Local Area Network
LM	Light Manipulation
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PACE	Password Authenticated Connection Establishment
PKI	Public Key Infrastructure
PUK	PIN Unblocking Key
QSCD	Qualified Signature/Seal Creation Device
RNG	Random Number Generator
RMI	Remote Method Invocation
SCA	Side channel analysis
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm

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

[COMP] Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018

[ETR] Evaluation Technical Report "SECORA™ ID v2.01 (SLJ38Gxymm1ap) and SECORA™ ID v2.02" (SLJ38Gxymm2ap) – EAL6+, 24-RPT-695, version 5.0, 19 December 2024

[ETRfC] Evaluation Technical Report for Composition "SECORA™ ID v2.01 (SLJ38Gxymm1ap)" – EAL6+, 24-RPT-696, version 2.0, 19 December 2024

[HW-CERT] BSI-DSZ-CC-1169-V4-2024 for IFX_CCI_00003Bh, 000043h, 00005Dh, 00005Eh, 00005Fh, 000060h, 000061h, 000062h, 000063h, 000064h, design step S11 with firmware 80.309.05.0, optional NRG™ SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib v01.30.0564, optional SCL v2.15.000, optional ACL v3.33.003 and v3.34.000 and v3.35.001, optional RCL v1.10.007, optional HCL v1.13.002 and user guidance from Infineon Technologies AG, Bonn, 13 September 2024

[HW-ETRfC] ETR for composite evaluation according to AIS 36 for the Product BSI-DSZ-CC-1169-V3-2024, Version 3, 2024-02-15, EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION (ETR COMP), TÜV Informationstechnik GmbH

ETR for composite evaluation ADDENDUM according to AIS 36 for the Product BSI-DSZ-CC-1169-V4-2024, Version 2, 2024-09-02, EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION ADDENDUM (ETR COMP Add), TÜV Informationstechnik GmbH

[HW-ST] Security Target Lite, IFX_CCI_00003Bh, IFX_CCI_000043h, IFX_CCI_00005Dh, IFX_CCI_00005Eh, IFX_CCI_00005Fh, IFX_CCI_000060h, IFX_CCI_000061h, IFX_CCI_000062h, IFX_CCI_000063h, IFX_CCI_000064h S11 Security Target, Version 5.9, 2024-08-20, Infineon Technologies AG

[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] Common Criteria Java Card System – Open Configuration Protection Profile, v3.1, April 2020

[ST] SECORA™ ID v2.01 (SLJ38Gxymm1ap), Rev 1.1, 19 December 2024

(This is the end of this report.)