Certification Report

Secure Signature Creation Device with Key generation (SSCD) configuration of SECORA™ ID v2.01 Infineon Applet Collection-eSign V1.0

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-2400176-01-CR**

Report version: **1**

Project number: NSCIB-**2400176-01**

Author(s): **Kjartan Jæger Kvassnes**

Date: **21 July 2025**

Number of pages: **13**

Number of appendices: **0**

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, 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 Secure Signature Creation Device with Key generation (SSCD) configuration of SECORA™ ID v2.01 Infineon Applet Collection-eSign V1.0. The developer of the Secure Signature Creation Device with Key generation (SSCD) configuration of SECORA™ ID v2.01 Infineon Applet Collection-eSign V1.0 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 Dual Interface chip with Java Card Applet “Secure Signature Creation Device with Key generation (SSCD) configuration of SECORA™ ID v2.01 Infineon Applet Collection-eSign V1.0” a combination of hardware and software configured to securely create, use and manage signature creation data (SCD). The SSCD protects the SCD during its whole lifecycle as to be used in a signature creation process solely by its signatory. configured to perform key generation and signature creation operations. The applet also supports authentication mechanisms like PACE, Active Authentication, Chip Authntication and Terminal Authentication.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 21 July 2025 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 Secure Signature Creation Device with Key generation (SSCD) configuration of SECORA™ ID v2.01 Infineon Applet Collection-eSign V1.0, 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 Secure Signature Creation Device with Key generation (SSCD) configuration of SECORA™ ID v2.01 Infineon Applet Collection-eSign V1.0 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 (EAL5+) 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, 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.

The TOE is stated as a Qualified Signature Creation Device for the purposes of electronic identification and trust services as detailed by the [EU-REG]. The evaluation by SGS Brightsight B.V. included an examination of the TOE according to the eIDAS Dutch Conformity Assessment Process Version 6 0.

TrustCB B.V., as the Dutch eIDAS-Designated Body responsible in The Netherlands for the assessment of the conformity of qualified electronic signature and qualified electronic seal creation devices declares that the evaluation meets the conditions for eIDAS certification for listing on the EU eIDAS compiled list of Qualified Signature/Seal Creation Devices.

[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 Secure Signature Creation Device with Key generation (SSCD) configuration of SECORA™ ID v2.01 Infineon Applet Collection-eSign V1.0 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_00005D
Software	Asymmetric Crypto Library (ACL)	03.35.001
	Symmetric Crypto Library (SCL)	02.15.000
	Hardware Support Library (HSL)	03.52.9708
	Hash Crypto Library (HCL) version	01.13.002
	UMSLC version	01.30.0564
	Firmware version	80.309.05.0
	Embedded OS version	CONF1: '01 00 02 FA 15 00 00 13 05' CONF2: '01 00 0C FA 15 00 00 13 05'
	eSign applet	1.3.0.0 (build number coded as '01 03 00 00')

To ensure secure usage a set of guidance documents is provided, together with the Secure Signature Creation Device with Key generation (SSCD) configuration of SECORA™ ID v2.01 Infineon Applet Collection-eSign V1.0. For details, see section 2.5 "Documentation" of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 1.6.6.

2.2 Security Policy

The TOE has the following features (from the underlying platform):

- The standard Java Card features like API, the Java Card Runtime Environment and the Java Card Virtual Machine;
- Proprietary PACE API providing special countermeasures against side channel leakage;
- GP for content management;
- Crypto operations (hash, EC, RSA, TDES and AES);
- Communication via the contactless interface and contact interface.

The TOE has the following features (from the SSCD applet):

- Generation of Asymmetric key pair for ECC and RSA algorithm;
- Computation of Digital Signature using a combination of hash algorithm and digital signature algorithm;
- Encipher and Decipher of Data;
- Active authentication using RSA or ECDSA algorithm;
- Chip authentication using ECDH algorithm;
- Terminal authentication using ECDSA algorithm;

- PACE with ECDH generic mapping, Chip Authentication Mapping and password types MRZ, CAN, PIN and PUK;
- PACE password management feature;
- Secure messaging based on 3DES and AES as per the ICAO specification;
- Support for PIN and its management;
- Optionally supports Match on Card with comparison of stored reference data with data from interface device (not claimed in the certification).

2.3 Assumptions and Clarification of Scope

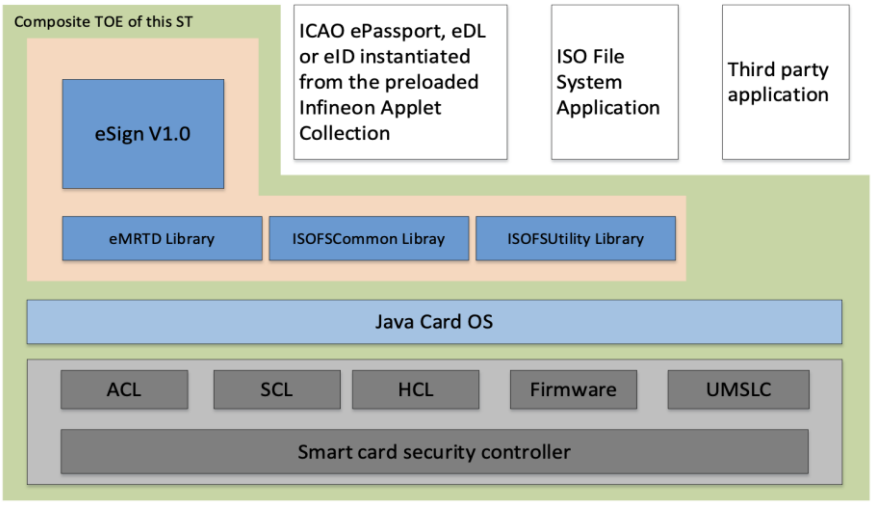
2.3.1 Assumptions

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 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 two lower layers in the picture represent the smart card controller referenced by IFX_CCI_00005D together with the Firmware, Asymmetric Cryptographic Library (ACL) and a Symmetric Crypto Library (SCL). Note that these components are certified by the same CC certificate BSI-DSZ-CC-1169-V4-2024. The hardware platform provides effective protection mechanisms against fault attacks. The platform contains hardware co-processors, which support cryptographic standards such as TDES, AES, RSA and EC. The hardware co-processor SCP has integrated measures against successful SCA.

The white colour indicates optional components which are not in the scope of the security claims of this ST, in CC terminology these are non interfering with the TSF of the TOE. The eSign V1.0 applet optionally supports the Match on Card (MoC) operations. This does not interfere with the any of the claimed security features. That means, both PIN and Biometric assets maintains its own control parameters. The personalizer could configure the required verification operation either with PIN or Biometric or both. However, the Biometric operation is not part of the certification claim in the eSign v1.0 Applet.

2.5 Documentation

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

Identifier	Version
SLJ38Gxymm1ap Infineon Applet Collection - eSign V1.0 Administration Guide, dated 05 June 2025	Rev.1.2
SLJ38Gxymm1ap Infineon Applet Collection - eSign V1.0 Extended datasheet, dated 14 June 2025	Rev.1.1

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 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-AM]. An important source for assurance in this step is the technical report [ETR_COMP] 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 1 week. During that test campaign, 50% of the total time was spent on Perturbation attacks, and 50% on logical tests.

2.6.3 Test configuration

The TOE was tested in the following configurations:

- Applet version 1.2.0.0 with Key Import and PACE-PIN/User-PIN authentication method on OS CONF1.

- Since the functionality the code that the vulnerability was found and testing was performed on is similar in other configurations of TOE (Key Gen, OS CONF 2), it is concluded that the results obtained from the test applies for other TOE configurations as well.
- TOE was updated with applet version 1.3.0.0. Delta code review was performed to check the updated functionality. No impact was detected on the Vulnerability analysis and therefore the performed test on TOE with applet version 1.2.0.0 is valid for the final TOE version.

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 Reused Evaluation Results

There has been extensive reuse of the ALC aspects for the sites involved in the software component of the TOE. Sites involved in the development and production of the hardware platform were reused 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 Secure Signature Creation Device with Key generation (SSCD) configuration of SECORA™ ID v2.01 Infineon Applet Collection-eSign V1.0.

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 Secure Signature Creation Device with Key generation (SSCD) configuration of SECORA™ ID v2.01 Infineon Applet Collection-eSign V1.0, 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 *[EN419211-2]*.

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 Secure Signature Creation Device with Key generation (SSCD) configuration of SECORA™ ID v2.01 Infineon Applet Collection-eSign V1.0 Rev_0.9, 2025-06-05 *[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:

DCAP	eIDAS Dutch Conformity Assessment Process
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
[COMP]	Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.6, April 2024
[eIDAS-REP]	Assessment Reporting Sheet eIDAS, 25-RPT-787, version 2.0, dated 21 July 2025
[EN419211-2]	EN 419 211-2:2013, Protection profiles for secure signature creation device - Part 2: Device with key generation, V2.0.1, registered under the reference BSI-CC-PP-0059-2009-MA-02
[ETR]	Evaluation Technical Report “Secure Signature Creation Device with Key Generation (SSCD) configuration of SECORA™ ID v2.01 Infineon Applet Collection – eSign, v1.0” – EAL5+, 25-RPT-546, Version 2.0, Dated 23 June 2025
[EU-REG]	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
[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, 13 September 2024
[HW-ST]	Security Target BSI-DSZ-CC-1169-V3-2024, 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 (confidential document)
[PLAT-CERT]	Certificate NSCIB-CC-2400062-01, SECORA™ ID v2.01 (SLJ38Gxymm1ap), issued 20 December 2024
[PLAT-ST]	SECORA™ ID v2.01 (SLJ38Gxymm1ap) Security Target, Rev 1.1, 19 December 2024
[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)

[JIL_QSCD] Security Evaluation and Certification of Qualified, Electronic Signature/Seal Creation Devices, JIL Interpretations for Security Certification according to eIDAS Regulation 910/2014, Version 1.0, July 2022

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022

[ST] Secure Signature Creation Device with Key generation (SSCD) configuration of SECORA™ ID v2.01 Infineon Applet Collection-eSign V1.0 Rev_0.9, 2025-06-05

(This is the end of this report.)