Certification Report

SECORA™ ID S (SLJ52GxxyyyzS)

Sponsor and developer: ***Infineon Technologies AG***
Am Campeon 5
D-85579 Neubiberg
Germany

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

Report number: **NSCIB-CC-175887-CR**

Report version: **1**

Project number: **175887**

Author(s): **Carolina Lavatelli**

Date: **20 April 2020**

Number of pages: **13**

Number of appendices: **0**

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

Certificate

Standard	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 5 (ISO/IEC 15408)
Certificate number	**CC-20-175887**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer	**Infineon Technologies AG** **Am Campeon 5, D-85579 Neubiberg, Germany**
Product and assurance level	**SECORA™ ID S (SLJ52GxxyyyzS)** Assurance Package: ▪ EAL6 augmented with ALC_FLR.1 Protection Profile Conformance: ▪ Java Card Protection Profile – Open Configuration, registered under the reference ANSSI-CC-PP-2010/03-M01, Version 3.0, May 2012.
Project number	**175887**
Evaluation facility	**Brightsight, located in Delft, the Netherlands** Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5 (ISO/IEC 18045)

Common Criteria Recognition Arrangement for components up to EAL2

SOGIS Mutual Recognition Agreement for components up to EAL4 or 7

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 5 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Validity

Date of 1st issue : **20-04-2020**

Certificate expiry : **20-04-2025**

PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

R. Kruit, LFM Systems
TÜV Rheinland Nederland B.V.
Westervoortsedijk 73, 6827 AV Arnhem
P.O. Box 2220, NL-6802 CE Arnhem
The Netherlands

CONTENTS:

TÜVRheinland®
Precisely Right.

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.

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 S (SLJ52GxxyyyzS). The developer of the SECORATM ID S (SLJ52GxxyyyzS) 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 with Amendment D and Card ID Configuration v1.0 implemented on certified IFX_CCI_000005 *[HW-CERT]*. The TOE provides LDS API for ICAO DOC 9303 and PACE API. The TOE constitutes a secure generic platform that supports multi-application runtime environment and provides facilities for secure loading and interoperability between different applications. The TOE allows post-issuance loading of off-card verified applications and supports static and native modes as well.

The TOE consists of several variants which are reflected in the TOE identifier SLJ52GxxyyyzS:

- the first variable x is for the available interface: ‘C’ (contact), ‘L’ (contactless), ‘D’ (dual)
- the second variable x is for the available RSA cryptography library: ‘T’ (2K), ‘A’ (4K)
- the 3-digit variable yyy is the available user memory in kB
- the variable z is a placeholder for TOE-based products, e.g. ‘A’ (ePassport), ‘B’ (eDriving License), ‘C’ (National eID Open Platform), ‘D’ (National eID with applications).

The TOE has been evaluated by Brightsight located in Delft, The Netherlands. The evaluation was completed on 14 April 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]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies the assumptions made during the evaluation, the intended environment for the SECORATM ID S (SLJ52GxxyyyzS), 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 SECORATM ID S (SLJ52GxxyyyzS) 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 it 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 SECORATM ID S (SLJ52GxxyyyzS) from Infineon Technologies *AG* located in Neubiberg, Germany.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	Integrated Circuit (IC)	IFX_CCI_000005
Embedded Software	Asymmetric Crypto Library (ACL)	2.07.003
	Symmetric Crypto Library (SCL)	2.04.002
	Hardware Support Library (HSL)	03.12.8812
	Java Card OS	1357

IFX_CCI_000005 with ACL, SCL and HSL libraries has been independently certified *[HW-CERT]*.

To ensure the secure usage a set of guidance documents is provided together with the SECORATM ID S (SLJ52GxxyyyzS). Details can be found in section 2.5 of this report.

The TOE lifecycle complies with *[ICPP]*. The TOE is delivered to the customer at the end of Phase 5 “Composite Product Integration”. For a detailed description of the TOE lifecycle refer to the *[ST]*, section 1.4.4

2.2 Security Policy

The TOE provides standard Java Card v3.0.5 functionality including cryptographic ciphers (AES 128/192/256, TDES, RSA up to 4K), signature algorithms (ECDSA, RSA PKCS#1, RSA PSS), Key agreement algorithms (ECDH, PACE), Key pair generation (EC, RSA), message digest algorithms (SHA-1, SHA-2).

The TOE provides a hybrid physical RNG compliant with AIS 31 PTG.3, proprietary LDS API compliant with ICAO DOC 9303 and proprietary PACE API for use with low entropy PINs.

The TOE complies with GlobalPlatform Card Specification v2.3.1 with Amendment D and ID Profile v1.0. It supports 4 logical channels, SCP 02 with option 15,55 and SCP 03 with option 00,10, Global CVM with velocity checking, multiple Security Domains, Delegated Management and Authorized Management.

The TOE supports three operation modes: an open configuration for post-issuance loading of off-card verified applications, a static mode which closes the post-issuance loading and a native mode for disabling any identification or tracking information. Bytecode verification must be done off-card with the latest version of Oracle’s Java Card bytecode verifier.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

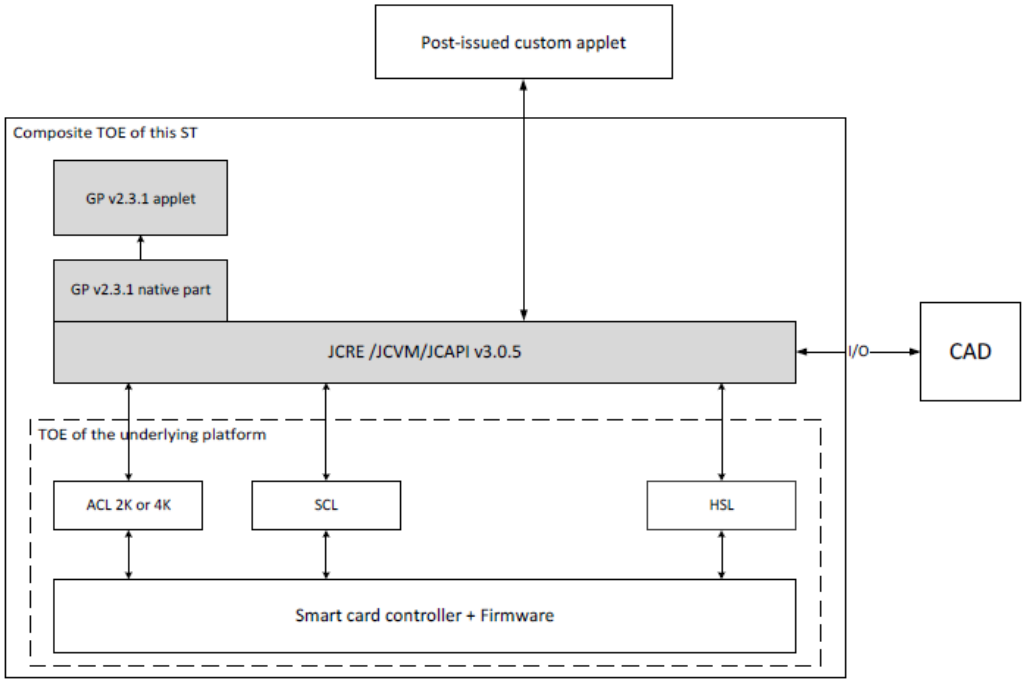
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE environment. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 5.2 of the *[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 and/or by objectives for the TOE environment as specified in the *[JCPP].* Please refer to the *[ST]* section 5.3.1 for a detailed description of the role of the objectives for the environment with regard to the threats' coverage.

2.4 Architectural Information

The TOE is a composite TOE depicted in the following diagram. The underlying platform has been independently certified *[HW-CERT]*.



The TSFI comprises:

- Java Card and proprietary bytecodes
- Java Card, GlobalPlatform and proprietary APIs
- GlobalPlatform and proprietary APDUs
- I/O Protocols
- Boot interface
- Chip surface.

2.5 Documentation

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

Document title	Version	Date
SECORA™ ID S Administrator Guide	1.50	2020-02-24
SECORA™ ID S Data Book	1.30	2020-02-24
SECORA™ ID S Security Guide	1.90	2020-02-24
SECORA™ ID S SLJ52GxAyyyzS System Release Notes	1.80	2020-02-24
SECORA™ ID S SLJ52GxTyyyzS System Release Notes	1.80	2020-02-24
SECORA™ ID S Product API Specification	1.02.1357	2020-02-19

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 comprehensive testing at TSFI, subsystem and module level using static and dynamic techniques. The testing was largely automated using industry standard Java Card and GlobalPlatform test suites. The developer has defined additional tests to ensure appropriate test depth.

The developer tested the TOE in the following configuration:

- Hardware CC identifier: 80 03 00 00 0
- Java Card OS Build Number: 82 02 13 57
- 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 00 and 87 02 00 01

The evaluator repeated the developer's tests on the same TOE configuration. All the test results were either as expected or the developer determined and the evaluator confirmed that there was no security impact.

The evaluator defined additional tests aimed at verifying the presence of the claimed security countermeasures and assessing the sufficiency of the user guidance. Additionally, logical tests were defined to verify the correct behaviour of the TOE in several boundary cases. These tests were performed on the TOE configuration with either Java Card OS 13 57 and/or 12 28. All the test results were as expected and the evaluator concluded that the results for the TOE with Java Card OS 12 28 apply to the final TOE configuration with Java Card OS 13 57.

2.6.2 Independent Penetration Testing

The evaluator independent vulnerability analysis (AVA_VAN.5) consisted in a methodical analysis of the developer's evidence followed by the definition of a penetration test plan:

- When evaluating the ASE, ADV (especially FSP and TDS) and AGD evidence, the evaluator considered whether potential vulnerabilities related to the TOE type or specified behaviour existed
- A thorough review of the TOE implementation representation (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 IC.
- All the potential vulnerabilities were analysed and a judgment was made on their exploitability. The potential vulnerabilities were addressed by penetration testing, by guidance or code update. The list of potential vulnerabilities is included in *[ETRfC]*.
- The evaluator defined and performed 6 (six) penetration tests.

2.6.3 Test Configuration

The evaluator performed independent functional testing on the following TOE configurations :

- Hardware CC identifier: 80 03 00 00 0
- Java Card OS Build Number: 82 02 12 28 and 82 02 13 57
- 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 00 and 87 02 00 01

The evaluator concluded that the independent tests performed on the TOE configuration with Java Card OS 13 32 are fully applicable to version 13 57 which corresponds to the certified TOE.

The evaluator performed independent penetration testing on the following TOE configurations:

- Hardware CC identifier: 80 03 00 00 0
- Java Card OS Build Number: 82 02 12 28 and 82 02 13 57
- 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 00 and 87 02 00 01

The evaluator concluded that the penetration tests performed on the TOE configuration with Java Card OS 12 28 are fully applicable to version 13 57 which corresponds to the certified TOE.

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.

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 applied.

The algorithmic security level exceeds 100 bits for all the evaluated cryptographic functionality 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. The remaining entropy is above 100 bits in all cases provided the user follows the guidance given in SECORA™ ID S Security Guide (SLJ 52GxxyyyzS). Revision 1.90, section 3.

No exploitable vulnerabilities were found with the independent penetration tests.

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

The overall conclusion is that the TOE is protected against attackers possessing a high attack potential, provided the TOE is used as required in the user guidance.

2.7 Re-used evaluation results

There has been an extensive re-use of the ALC requirements based on *[STAR]* reports for the sites involved in the TOE embedded software:

Site
Infineon Technologies AG Alter Postweg 101, 86159 Augsburg, Germany
Infineon Technologies India Pvt. Ltd. Mahatma Gandhi (M.G) Road No. 11, Bangalore-560001, India
Infineon Technologies AG Am Campeon 1-12, 85579 Neubiberg, Germany
Infineon Technologies AG Development Center Bucharest Nr. 6 Dimitrie Pompei Blvd., Novopark, Building B+C, 020337 Bucharest, Romania
Infineon Technologies Austria AG, Development Center Graz Babenberger-str. 10, 8020 Graz, Austria
Infineon Technologies Austria AG Siemensstraße 2, 9500 Villach, Austria

The 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 SECORATM ID S (SLJ52GxxyyyzS).

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[2] which references the 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 a 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 SECORATM ID S (SLJ52GxxyyyzS), 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 the Security Target *[ST]*.

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

2.10 Comments/Recommendations

The 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 software and hardware parts of the TOE. There are no particular obligations or recommendations for the user apart from following the 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 implemented 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 Security Target 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", sufficiently large cryptographic key sizes shall be used (references can be found in national and international documents and standards).

[2] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

3 Security Target

The SECORATM ID S (SLJ52GxxyyyzS) Security Target, Rev 1.7, 2020-02-24 *[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:

AES	Advanced Encryption Standard
CVM	Cardholder Verification Method
DES	Data Encryption Standard
ECDH	Elliptic Curve Diffie-Hellman algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
ETR	Evaluation Technical Report
IC	Integrated Circuit
JIL	Joint Interpretation Library
NSCIB	Netherlands scheme for certification in the area of IT security
OS	Operating System
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
TDES	Triple DES

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.
[JCPP]	Java Card Protection Profile – Open Configuration, v3.0, May 2012, ANSSI-CC-PP-2010/03-M01.
[ICPP]	Security IC Platform Protection Profile, v1.0, BSI-PP-0084-2014.
[ETR]	Evaluation Technical Report "SECORA™ ID S (SLJ52GxxyyyzS)" – EAL6+, 19-RPT-629, Version 8.0, 8 April 2020.
[ETRfC]	ETR for Composite Evaluation "SECORA™ ID S (SLJ52GxxyyyzS)" – EAL6+, 19-RPT-630, Version 5.0, 6 March 2020.
[HW-CERT]	BSI-DSZ-CC-1110-V2-2019 for Infineon Security Controller IFX_CCI_000003h,000005h, 000008h, 00000Ch, 000013h, 000014h,000015h, 00001Ch, 00001Dh, 000021h, 000022hH13 including the products from the second production line and optional software packages: Flash Loader, Asymmetric Crypto Library, Symmetric Cryptographic Library, Hardware Support Layer, Hash Crypto Library, Mifare Compatible Software, and CIPURSE™ Crypto Library, 2019-06-18
[HW-ETRfC]	EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION (ETR COMP) BSI-DSZ-CC-1110-V2, Version 2, 2019-06-14.
[HW-ST]	Confidential Security Target IFX_CCI_000003h IFX_CCI_000005h IFX_CCI_000008h IFX_CCI_00000Ch IFX_CCI_000013h IFX_CCI_000014h IFX_CCI_000015h IFX_CCI_00001Ch IFX_CCI_00001Dh IFX_CCI_000021h IFX_CCI_000022h H13 including the products from the second production line, Rev. 2.8, 2019-04-30.
[STAR]	BSI-DSZ-CC-0891-V4 comprising: STAR Augsburg, v1.0, 2019-07-25 STAR Bangalore, v1.0, 2019-07-25 STAR Bucharest, v1.0, 2019-07-25 STAR Graz, v1.0, 2019-07-25 STAR Munich, v1.0, 2019-07-22 STAR Villach, v1.0, 2019-07-25
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, March 2019.
[ST]	SECORA™ ID S (SLJ52GxxyyyzS) Security Target, Rev 1.7, 2020-02-24.

(This is the end of this report).