Certification Report

SECORA™ ID S v1.1 (SLJ52GxxyyyzS)

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

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

Report number:	**NSCIB-CC-175887-CR2**
Report version:	**1**
Project number:	**175887**_2
Author(s):	**Denise Cater**
Date:	**05 March 2021**
Number of pages:	**14**
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

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, 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 v1.1 (SLJ52GxxyyyzS). The developer of the SECORA™ ID S v1.1 (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 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 consists of several variants which are reflected in the TOE name. The letters x, y, and z are placeholders for the following values:

- The first variable x is for the available interface (can be ‘C’, ‘L’, or ‘D’ for the contact based, contactless or dual Interface)
- The second variable x is for the available RSA cryptography library (‘T’ stands for 2K RSA , ‘A’ for 4K RSA)
- The 3 digit variable yyy is the available user memory in kB
- The variable z is a place holder for products that will be based on the TOE (e.g. ‘A’ for ePassport with HBR, 'B’ for eDriving License with HBR, ‘C’ for National eID open platform configuration with HBR, ‘D’ for National eID with applications and HBR or ‘V’ for open platform configuration with VHBR, etc.)

The TOE has been originally evaluated by Brightsight B.V. located in Delft, The Netherlands and was certified on 20 April 2020. The re-evaluation also took place by Brightsight B.V. and was completed on 05 March 2021 with the approval of the ETR. The re-certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

This second issue of the Certification Report is a result of a “recertification with major changes”.

The major changes are related to the update of the platform and discrete Java Card OS updates. In addition, there were updates to the Security target and user guidance.

The security evaluation re-used the evaluation results of previously performed evaluations. A full, up to date vulnerability analysis has been made, as well as renewed testing.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the SECORA™ ID S v1.1 (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 SECORA™ ID S v1.1 (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 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 and *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 5 *[CC]* (Parts I, II and III).

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

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.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the SECORA™ ID S v1.1 (SLJ52GxxyyyzS) 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_000005
Software	Asymmetric Crypto Library (ACL)	2.07.003
	Symmetric Crypto Library (SCL)	2.04.002
	Hardware Support Library (HSL)	03.12.8812
	Embedded OS	1442

The TOE can be in one of the following configurations (different binary images):

- RSA 2K
- RSA 4K

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

To ensure secure usage a set of guidance documents is provided together with the SECORA™ ID S v1.1 (SLJ52GxxyyyzS). Details can be found in section 2.5 of this report.

The TOE is delivered at the end of Phase 5 “Composite Product Integration. For a detailed and precise description of the TOE lifecycle refer to the *[ST]*, chapter 1.4.4.

2.2 Security Policy

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
- Signature algorithms
  - ECDSA with SHA-1/SHA-2
  - RSA PKCS#1 with SHA-2
  - RSA PSS with SHA256
- Key agreement algorithms
  - ECDH with KDF and with XY
  - PACE with generic mapping
- Key pair generation
  - EC
  - RSA with modulus/exponent and CRT
- Key Sizes
  - AES 128/192/256
  - TDES 128/192
  - RSA modulus sizes from 512 to 4096 bits

  - EC curves according to NIST and Brainpool
    - NIST standard curves from FIPS 186-3: P224, P256, P384, P521
    - Brainpool curves from RFC 5639: BrainpoolP224, BrainpoolP256r1, BrainpoolP320r1, BrainpoolP384r1,BrainpoolP512r1, BrainpoolP256t1,BrainpoolP320t1,BrainpoolP384t1, BrainpoolP512t1

- Message digest algorithms
  - SHA-1 (Note: SHA-1 as a security algorithm is only used as part of a session key derivation)
  - SHA-2 family: SHA224, SHA256, SHA384, SHA512
- Random number generation algorithms
  - Hybrid physical RNG according to [AIS 31] PTG.3

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

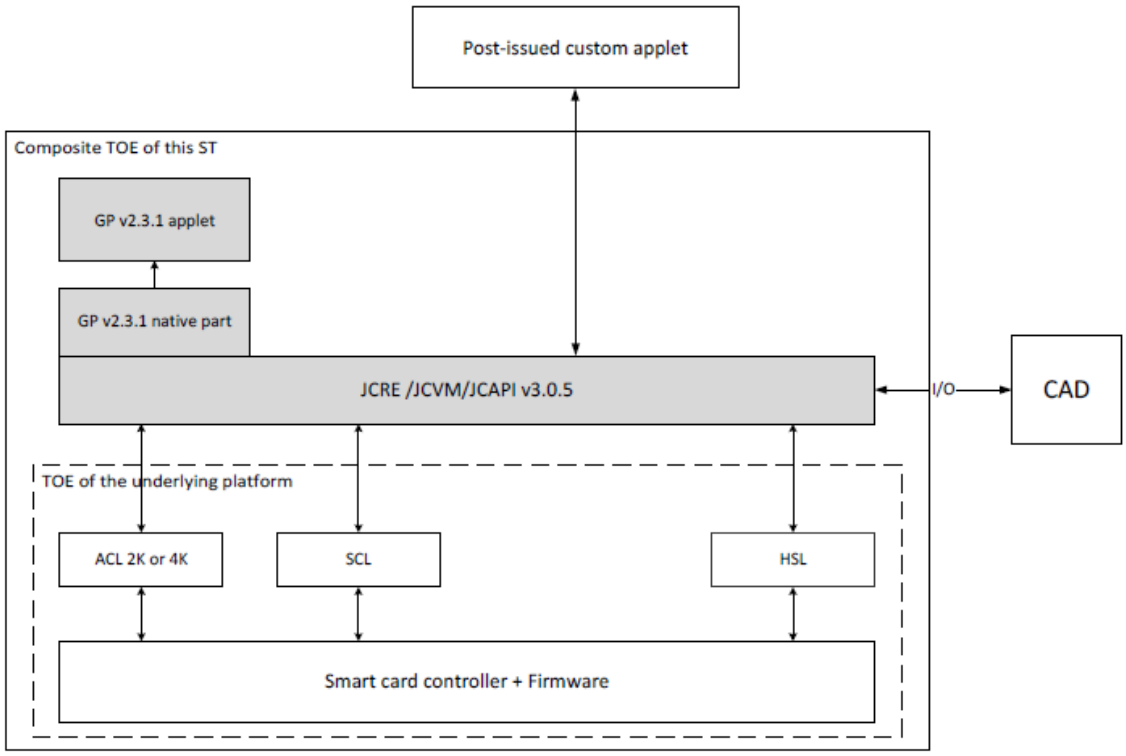
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 4.4 of the *[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 and/or by objectives for the TOE environment as specified in *[JCPP]*. Please refer to *[ST]* section 5.2 for a detailed description of the role of the objectives for the environment with regard to the coverage of the threats.

2.4 Architectural Information

The logical architecture of the TOE can be depicted as follows, the underlying platform of which has been independently certified *[HW-CERT]*:



The TSFIs can be categorized as follows:

- Bytecodes, comprised of JCVM and Proprietary
- API, comprised of JCAPI, Proprietary extensions and GPAPI
- APDU, comprised of GP and Proprietary APDU
- IO Protocols
- Boot interface
- Chip surface

2.5 Documentation

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

Identifier	Version
SECORA™ ID S v1.1 Administration Guide	1.70, 2021-01-27
SECORA™ ID S v1.1 Data Book	1.70, 2021-01-27
SECORA™ ID S v1.1 Security Guide	2.20, 2021-01-27
SECORA™ ID S v1.1 SLJ52GxAyyyzS System Release Notes	2.20, 2021-01-27
SECORA™ ID S v1.1 SLJ52GxTyyyzS System Release Notes	2.20, 2021-01-27
SECORA™ ID S v1.1 Product API Specification	1.02.1442, 2020-11-18

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 TSFI, subsystem and module level using static and dynamic techniques. The testing was largely automated using industry standard and proprietary test suites to verify the Java Card and GlobalPlatform component behaviour. In addition to the test suites, the developer defines additional tests to cover various corner cases and improve the test depth.

The developer tested the TOE in the following configuration during the baseline evaluation:

- HW identifier: 80 03 00 00 05
- EMVCo identifier: 81 06 00 13 00 27 00 00
- JC 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 developer tested the TOE in the following configuration during this re-evaluation:

- HW identifier: 80 03 00 00 05
- EMVCo identifier: 81 06 00 13 00 27 00 00
- JC OS Build Number: 82 02 14 42.
- 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

A total of 14 new test cases added for the re-evaluation of the TOE (version 1442). They are mainly automatic tests and one simple manual test. All additional developer tests resulted in a PASS verdict.

During the baseline evaluation the evaluator repeated the developer's tests on the same TOE configuration. The set of repeated developer tests was chosen based on getting a good representation over different test categories, i.e., it covers System Tests, Component Tests, as well as Black, Grey, and White-box Tests. Additionally, it was chosen to be able to cover different configurations, i.e., RSA 2K vs RSA 4K. These were executed during the baseline evaluation. All test results were either as expected or the developer determined, and the evaluator confirmed, that there was no security impact.

No additional witnessing or repetition of developer testing was necessary during this re-evaluation since the same test set-ups were used as for the baseline evaluation and the developer evidence contains full test log information.

During the baseline evaluation the evaluator defined independent functional tests aimed at verifying the presence of implemented security countermeasures, as well as assessing the sufficiency of the provided user guidance documents. Additionally, several logical tests are defined to verify the correct behaviour of the TOE in a variety of boundary cases. These tests were performed during the baseline evaluation and all test results were as expected.

As the developer has added sufficient additional test cases for RC5 (OS version 1357) and RC7 (OS version 1442) to cover the associated changes to the implementation, the evaluator has not added any additional independent tests during this re-evaluation. The evaluator also analysed the changes to the TOE during this re-evaluation and determined the results of the previous testing were unaffected by the changes. Therefore, no independent functional testing was necessary as part of this re-evaluation.

2.6.2 Independent Penetration Testing

The methodical analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considers whether potential vulnerabilities can already be identified due to the TOE type and/or specified behaviour.
- A thorough implementation representation review (ADV_IMP) was performed. The analysis was driven by the attack methods defined in *[JIL-AP]*. An important source for assurance in this step is the technical report *[HW-ETRfC]* of the underlying platform.
- All potential vulnerabilities are analysed and a judgment was made on their exploitability. The potential vulnerabilities are addressed by penetration testing, a guidance update or code update.

During this re-evaluation, the vulnerability analysis and assurance from penetration testing were refreshed. The methodical analysis is repeated on the basis of a delta code review, resulting in the identification of an additional penetration test. As the penetration testing campaign for the baseline evaluation was performed more than one year ago, the evaluator also performed penetration testing to demonstrate the ongoing validity of the test results from the baseline penetration test campaign. The total test effort expended by the evaluators in this re-evaluation was 2.5 weeks, of which 89% on SCA, and 11% on logical tests.

2.6.3 Test Configuration

During the baseline evaluation the evaluator performed independent penetration testing on the following TOE configurations:

- HW identifier: 80 03 00 00 05
- EMVCo identifier: 81 06 00 13 00 27 00 00
- JC 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 test performed on the TOE configuration with Java Card 12 28 were also fully applicable to version 13 57, the TOE being certified in the baseline evaluation.

The evaluator tested the TOE in the following configuration during this re-evaluation:

- HW identifier: 80 03 00 00 05
- EMVCo identifier: 81 06 00 13 00 27 00 00
- JC OS Build Number: 82 02 14 42.
- 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 (for functional test cases) and 87 02 00 01 (for penetration test cases)

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 taken into account.

The algorithmic security level exceeds 100 bits for all 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 provided in SECORA™ ID S v1.1 Security Guide, version 2.20, Section 3.2.4.

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

This is a re-certification. Documentary evaluation results of the earlier version of the TOE have been re-used, but vulnerability analysis and penetration testing has been renewed.

There has been extensive re-use 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 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 S v1.1 (SLJ52GxxyyyzS).

2.9 Results of the Evaluation

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 *[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 S v1.1 (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 Security Target *[ST]*.

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

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.

3 Security Target

The SECORA™ ID S v1.1 (SLJ52GxxyyyzS) Security Target, Rev. 1.9, 2021-01-27 *[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:

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 S v1.1, 19-RPT-629, Version 10.0, 02 March 2021.
[ETRfC]	ETR for Composite Evaluation SECORA™ ID S v1.1, 19-RPT-630, Version 7.0, 02 March 2021.
[HW-CERT]	BSI-DSZ-CC-1110-V3-2020 2020forInfineon Security Controller IFX_CCI_000003h,000005h, 000008h, 00000Ch, 000013h, 000014h,000015h, 00001Ch, 00001Dh, 000021h, 000022h in the design step H13 and including optional software libraries and dedicated firmware in several versions from Infineon Technologies AG, v1.0, 13 May 2020.
[HW-ETRfC]	Evaluation Technical Report for Composite Evaluation (ETR COMP) BSI-DSZ-CC-1110-V3, Version 1, 2020-04-23.
[HW-ST]	Common Criteria Public Security Target EAL6 augmented/EAL6+ 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 optional Software Libraries Flash Loader – 3x ACL – 4x HSL – 2x SCL – NRG – CCL Version 1.8, 2020-04-22.
[JCPP]	Java Card Protection Profile – Open Configuration, v3.0, May 2012, registered under the reference ANSSI-CC-PP-2010/03-M01.
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.1, June 2020.
[JIL-AM]	Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution).
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.
[ST]	SECORA™ ID S v1.1 (SLJ52GxxyyyzS) Security Target, Rev. 1.9, 2021-01-27.

(This is the end of this report).