Certification Report

IFX_CCI_00003Fh, IFX_CCI_000059h, IFX_CCI_00005Bh, IFX_CCI_00003Ch, IFX_CCI_00003Dh, IFX_CCI_00005Ah, design step G11 with optional HSL v2.01.6198, optional SCL v2.13.001, optional ACL v3.03.003, optional HCL v1.13.001, optional RCL v1.10.006 and with specific IC-dedicated firmware identifier 80.203.00.3

Sponsor and developer: ***Infineon Technologies AG***
Am Campeon 1-12
85579 Neubiberg
Germany

Evaluation facility: ***TÜV Informationstechnik GmbH***
Langemarckstr. 2
45141 Essen
Germany

Report number:	**NSCIB-CC-0173264-CR2**
Report version:	**1**
Project number:	**0173264_2**
Author(s):	**Jordi Mujal**
Date:	**22 April 2021**
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

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 IFX_CCI_00003Fh, IFX_CCI_000059h, IFX_CCI_00005Bh, IFX_CCI_00003Ch, IFX_CCI_00003Dh, IFX_CCI_00005Ah, design step G11 with optional HSL v2.01.6198, optional SCL v2.13.001, optional ACL v3.03.003, optional HCL v1.13.001, optional RCL v1.10.006 and with specific IC-dedicated firmware identifier 80.203.00.3. The developer of the IFX_CCI_00003Fh, IFX_CCI_000059h, IFX_CCI_00005Bh, IFX_CCI_00003Ch, IFX_CCI_00003Dh, IFX_CCI_00005Ah, design step G11 with optional HSL v2.01.6198, optional SCL v2.13.001, optional ACL v3.03.003, optional HCL v1.13.001, optional RCL v1.10.006 and with specific IC-dedicated firmware identifier 80.203.00.3 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 consists of smart card IC (Security Controller), firmware and user guidance. This TOE is intended to be used in smart cards for security-relevant applications and as developing platform for smart card operating systems. The TOE major security features include HW cryptographic support for TDES, AES, and RNG, memory protection unit supporting different memory access levels, authentication of the smartcard IC, support for loading of flash content in secured locations and in loading by authorized users only. In addition, optional software libraries with HW NVM support and cryptographic support for TDES, AES, RSA, ECC, SHA, Hash and MAC calculation and RNG is also included.

The TOE has been originally evaluated by TÜV Informationstechnik GmbH. located in Essen, Germany and was certified on 31 January 2021. The re-evaluation also took place by TÜV Informationstechnik GmbH. and was completed on 22 April 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:

- TOE is now equipped with a set of optional libraries (SCL, ACL, HCL, HSL, and RCL).
- Additional variant IFX_CCI_00003Dh has a different configuration of the HRNG.

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 new 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 TOE (IFX_CCI_00003Fh, IFX_CCI_000059h, IFX_CCI_00005Bh, IFX_CCI_00003Ch, IFX_CCI_00003Dh, IFX_CCI_00005Ah, design step G11 with optional HSL v2.01.6198, optional SCL v2.13.001, optional ACL v3.03.003, optional HCL v1.13.001, optional RCL v1.10.006 and with specific IC-dedicated firmware identifier 80.203.00.3), 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 TOE (IFX_CCI_00003Fh IFX_CCI_000059h, IFX_CCI_00005Bh, IFX_CCI_00003Ch, IFX_CCI_00003Dh, IFX_CCI_00005Ah, design step G11 with optional HSL v2.01.6198, optional SCL v2.13.001, optional ACL v3.03.003, optional HCL v1.13.001, optional RCL v1.10.006 and with specific IC-dedicated firmware identifier 80.203.00.3) 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).

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

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).

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 IFX_CCI_00003Fh, IFX_CCI_000059h, IFX_CCI_00005Bh, IFX_CCI_00003Ch, IFX_CCI_00003Dh, IFX_CCI_00005Ah, design step G11 with optional HSL v2.01.6198, optional SCL v2.13.001, optional ACL v3.03.003, optional HCL v1.13.001, optional RCL v1.10.006 and with specific IC-dedicated firmware identifier 80.203.00.3 from Infineon Technologies AG located in Neubiberg, Germany.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	IFX_CCI_00003Fh, IFX_CCI_000059h, IFX_CCI_00005Bh, IFX_CCI_00003Ch, IFX_CCI_00003Dh, IFX_CCI_00005Ah	G11
Firmware	BOS	80.203.00.3
	Flash Loader	V8.06.001
Software	ACL	v3.03.003
	SCL	v2.13.001
	HCL	v1.13.001
	RCL	v1.10.006
	HSL	v2.01.6198

To ensure secure usage a set of guidance documents is provided together with the IFX_CCI_00003Fh, IFX_CCI_000059h, IFX_CCI_00005Bh, IFX_CCI_00003Ch, IFX_CCI_00003Dh, IFX_CCI_00005Ah, design step G11 with optional HSL v2.01.6198, optional SCL v2.13.001, optional ACL v3.03.003, optional HCL v1.13.001, optional RCL v1.10.006 and with specific IC-dedicated firmware identifier 80.203.00.3. Details can be found in section 2.5 of this report.

For a detailed and precise description of the TOE lifecycle refer to the *[ST]*, chapter 1.4.5.

2.2 Security Policy

This TOE is intended to be used in smart cards for security-relevant applications and as developing platform for smart card operating systems. The TOE major security features include cryptographic support for TDES, AES, and RNG, memory protection unit supporting different memory access levels, authentication of the smartcard IC, support for loading of flash content in secured locations and in loading by authorized users only. In addition, optional software libraries with HW NVM support and cryptographic support for TDES AES, RSA, ECC, SHA, Hash and MAC calculation and RNG is also included.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

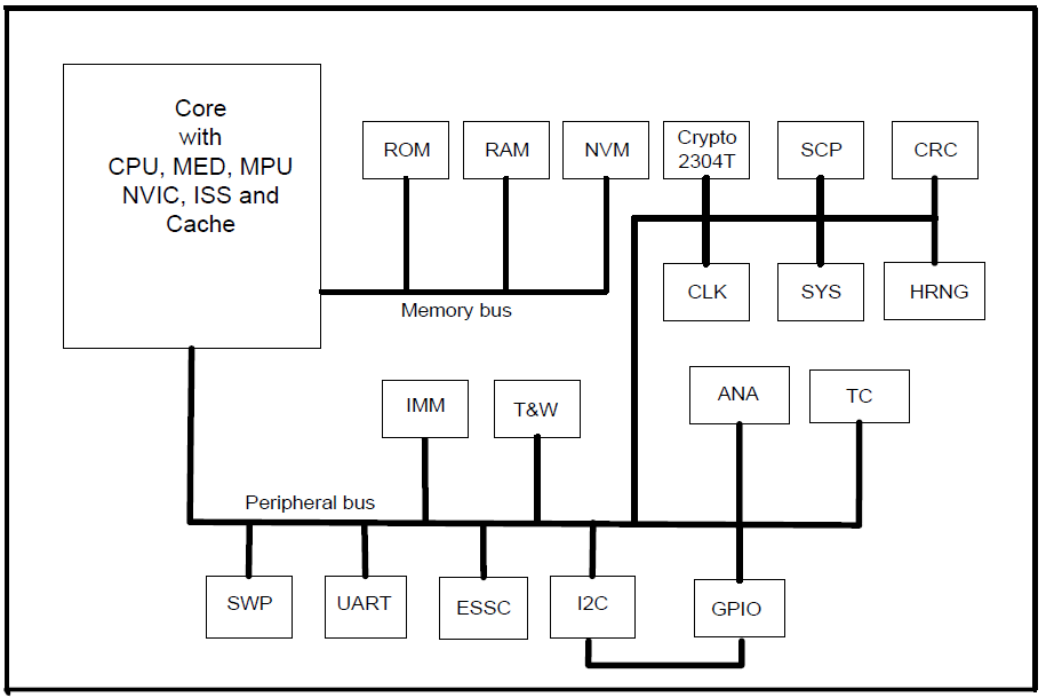
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 4.2 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information

The TOE consists of the hardware and software described in section 2.1.



Logically the TOE provides cryptographic support for TDES, AES, and RNG, memory protection unit supporting different memory access levels, authentication of the smartcard IC, support for loading of flash content in secured locations and in loading by authorized users only. In addition, optional software libraries with HW NVM support and cryptographic support for TDES AES, RSA, ECC, SHA, Hash and MAC calculation and RNG is also included.

2.5 Documentation

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

Identifier	Version
32-bit Security Controller – V20 Hardware Reference Manual	V2.3 dated 2020-10-15
32-bit Security Controller – V21 Hardware Reference Manual	V2.3 dated 2020-10-15
ARMv7-M Architecture Reference Manual	DDI 0403D ID021310 dated 2010-02-12
Production and personalization 32-bit ARM-based security controller User´s Manual	V3.4 dated 2018-05-14
32-bit Security Controller SLC37 (65 nm Technology) Programmer's Reference Manual	V4.6 dated 2020-10-13
32-bit Security Controller – V20 Security Guidelines	1.00-2621 dated 2020-09-09

32-bit Security Controller–V21 Security Guidelines	1.00-2622 dated 2020-09-09
32-bit Security Controller – V20 Errata Sheet	V3.0 dated 2020-10-13
32-bit Security Controller – V21 Errata Sheet	V3.0 dated 2020-11-02
32-bit Security Controller Crypto@2304T V3 User Manual	V2.0 dated 2019-04-24
ACL37-Crypto2304T-C65 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox User interface manual	v3.03.003 dated 2021-04-13
SCL37-SCP-v4-C65 Symmetric Crypto Library for SCP-v4 AES/DES/MAC User interface manual	v2.13.001 dated 2021-03-18
HCL37-CPU-C65 Hash Crypto Library for CPU SHA User interface manual	v1.13.001 dated 2020-03-11
RCL37-X-C65 Random Crypto Library for SCP-v4 & HRNG-v2 DRBG/HWRNG User interface manual	v1.10.006 dated 2020-06-16
SLxx7-C65 Hardware Support Library	v2.01.6198 dated 2019-07-05

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

For both the baseline evaluation and this re-evaluation, the developer performed extensive testing on functional specification, subsystem and module level. All parameter choices have been addressed at least once. All boundary cases identified have been tested explicitly, and additionally the near-boundary conditions have been covered probabilistically. The testing was largely automated using industry standard and proprietary test suites. Test scripts were extensively used to verify that the functions return the expected values.

For the testing performed by the evaluators in both the baseline and re-evaluation, 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 independent vulnerability analysis has been performed according to *[CC]*, *[JIL-AAPS]*, *[JIL-AM]* and *[CCDB-SC-EVAL]*. The ratings have been calculated according to 'Application of attack potential to smartcards' *[JIL-AAPS]* document.

During this re-evaluation, the vulnerability analysis was refreshed and extended to the new TOE components.

For the baseline evaluation, the total test effort expended by the evaluators was 14 weeks. During that test campaign 57% of the total time was spend on Perturbation attacks, 36% on side channel testing and 7% on logical tests. Additional test effort expended by the evaluators in this re-evaluation was 15 weeks, of which 25% on Perturbation Attacks, 69% on side channel, and 6% on logical tests.

2.6.3 Test Configuration

Testing was performed on the TOE as specified in this Certification Report. The tests are performed with the chips IFX_CCI_00003Fh uniquely identified by the chip identification data. The configuration

of the TOE used for testing had all optional components available. Test results are applicable equally for all variants of the TOE as described.

2.6.4 Testing Results

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

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

No exploitable vulnerabilities were found with the independent penetration tests.

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

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. These activities revealed that for some cryptographic functionality the security level could be reduced from an algorithmic security level above 100 bits to a practical remaining security level lower than 100 bits. As the remaining security level still exceeds 80 bits, this is considered sufficient. So 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. Vulnerability analysis has been renewed and penetration tests have been re-used.

There has been extensive re-use of the ALC aspects for the sites involved in the development and production of the TOE, by use of 5 site certificates and 24 Site Technical Audit Re-use report approaches.

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 IFX_CCI_00003Fh, IFX_CCI_000059h, IFX_CCI_00005Bh, IFX_CCI_00003Ch, IFX_CCI_00003Dh, IFX_CCI_00005Ah, design step G11 with optional HSL v2.01.6198, optional SCL v2.13.001, optional ACL v3.03.003, optional HCL v1.13.001, optional RCL v1.10.006 and with specific IC-dedicated firmware identifier 80.203.00.3.

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, and Site Technical Audit Report(s) for the site(s) *[STAR]*[2]. 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 IFX_CCI_00003Fh, IFX_CCI_000059h, IFX_CCI_00005Bh, IFX_CCI_00003Ch, IFX_CCI_00003Dh, IFX_CCI_00005Ah, design step G11 with optional HSL v2.01.6198, optional SCL v2.13.001, optional ACL v3.03.003, optional HCL v1.13.001, optional RCL v1.10.006 and with specific IC-dedicated firmware identifier 80.203.00.3, to be **CC Part 2 extended**, **CC Part 3 conformant**, and to meet the requirements of **EAL**

[2] The Site Technical Audit Report contains information necessary to an evaluation lab and certification body for the reuse of the site audit report in a TOE evaluation.

6 augmented with ALC_FLR.1. This implies that the product satisfies the security requirements specified in Security Target [ST].

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

2.10 Comments/Recommendations

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

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

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

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

3 Security Target

The Confidential Security Target IFX_CCI_00003Fh IFX_CCI_000059h IFX_CCI_00005Bh IFX_CCI_00003Ch IFX_CCI_00003Dh IFX_CCI_00005Ah G11 including optional software libraries: Flash Loader according Package1 and Package2, HCL, RCL, ACL and SCL,v1.5, 14 April 2021 *[ST]* is included here by reference.

Please note that for the need of publication a public version *[ST-lite]* has been created and verified according to *[ST-SAN]*.

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
IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT security
RNG	Random Number Generator
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 Summary (ETR Summary), IFX_CCI_00003Fh IFX_CCI_000059h IFX_CCI_00005Bh IFX_CCI_00003Ch IFX_CCI_00003Dh, IFX_CCI_00005Ah design step G11 with optional HSL v2.01.6198, optional SCL v2.13.001, optional ACL v3.03.003, optional HCL v1.13.001, optional RCL v1.10.006 and with specific IC-dedicated firmware identifier 80.203.00.3 and user guidance, 0173264-CR2_ETR_210422_v5, version 5, dated 22 April 2021.

[ETRfC] ETR for Composite Evaluation (ETR COMP), IFX_CCI_00003Fh IFX_CCI_000059h IFX_CCI_00005Bh IFX_CCI_00003Ch IFX_CCI_00003Dh, IFX_CCI_00005Ah design step G11 with optional HSL v2.01.6198, optional SCL v2.13.001, optional ACL v3.03.003, optional HCL v1.13.001, optional RCL v1.10.006 and with specific IC-dedicated firmware identifier 80.203.00.3 and user guidance ,0173264-CR2_ETRfC_210422_v5, version 5, dated 22 April 2021.

[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.

[PP] Security IC Platform Protection Profile with Augmentation Packages, registered under the reference BSI-CC-PP-0084-2014, Version 1.0, dated 2014-01-13.

[ST] Confidential Security Target IFX_CCI_00003Fh IFX_CCI_000059h IFX_CCI_00005Bh IFX_CCI_00003Ch IFX_CCI_00003Dh IFX_CCI_00005Ah G11 including optional software libraries: Flash Loader according Package1 and Package2, HCL, RCL, ACL and SCL,v1.5, 14 April 2021.

[ST-lite] Public Security Target IFX_CCI_00003Fh IFX_CCI_000059h IFX_CCI_00005Bh IFX_CCI_00003Ch IFX_CCI_00003Dh IFX_CCI_00005Ah G11 including optional software libraries: Flash Loader according Package1 and Package2, HCL, RCL, HSL, ACL and SCL, v1.5, 14 April 2021.

[ST-SAN] ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.

(This is the end of this report).