Certification Report

IFX_CCI_00003Fh IFX_CCI_000059h IFX_CCI_00005Bh IFX_CCI_00003Ch IFX_CCI_00003Dh IFX_CCI_00005Ah design step G11 and H11 with optional HSL v2.01.6198, optional SCL v2.13.001, optional ACL v3.03.003, optional ACL v3.04.001, optional ACL v3.05.002, optional HCL v1.13.001, optional RCL v1.10.006 and with specific IC-dedicated firmware identifier 80.203.00.3 and Flash Loader v8.06.001

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

Evaluation facility:

TÜV Informationstechnik GmbH
Am TÜV 1
45307 Essen
Germany

Report number:	**NSCIB-CC-2200060-02-CR**
Report version:	**1**
Project number:	NSCIB-**2200060-02**
Author(s):	**Jordi Mujal**
Date:	**30 August 2024**
Number of pages:	**13**
Number of appendices:	**0**

Reproduction of this report is authorised only if the report is reproduced in its entirety.

CONTENTS

Foreword 3

Recognition of the Certificate 4

International recognition 4
European recognition 4

1 Executive Summary 5

2 Certification Results 7

2.1 Identification of Target of Evaluation 7
2.2 Security Policy 7
2.3 Assumptions and Clarification of Scope 7
2.3.1 Assumptions 7
2.3.2 Clarification of scope 8
2.4 Architectural Information 8
2.5 Documentation 8
2.6 IT Product Testing 9
2.6.1 Testing approach and depth 9
2.6.2 Independent penetration testing 10
2.6.3 Test configuration 10
2.6.4 Test results 10
2.7 Reused Evaluation Results 10
2.8 Evaluated Configuration 10
2.9 Evaluation Results 11
2.10 Comments/Recommendations 11

3 Security Target 12

4 Definitions 12

5 Bibliography 13

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TrustCB B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TrustCB B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TrustCB B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TrustCB B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

Recognition of the Certificate

Presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the IFX_CCI_00003Fh IFX_CCI_000059h IFX_CCI_00005Bh IFX_CCI_00003Ch IFX_CCI_00003Dh IFX_CCI_00005Ah design step G11 and H11 with optional HSL v2.01.6198, optional SCL v2.13.001, optional ACL v3.03.003, optional ACL v3.04.001, optional ACL v3.05.002, optional HCL v1.13.001, optional RCL v1.10.006 and with specific IC-dedicated firmware identifier 80.203.00.3 and Flash Loader v8.06.001. The developer of the TOE 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.

There are TOE configurations that are critically dependent on the Embedded Software operational environment (as defined in the [PP]) to provide countermeasures against specific attacks as described in the TOE guidance. As such it is vital that meticulous adherence to the user guidance of both the software and the hardware part of the TOE is maintained.

The TOE was evaluated initially by TÜV Informationstechnik GmbH located in Essen, Germany and was certified on 24 June 2023. The re-evaluation of the TOE has also been conducted by TÜV Informationstechnik GmbH and was completed on 30 August 2024 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:

- Introduction of a new ACL component version

- Major changes in the guidance documentation

- One site is removed from the TOE life cycle

The security evaluation reused 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 TOE, 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 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 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TrustCB B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the

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

NSCIB Certified Products list. Note that the certification results apply only 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 and H11 with optional HSL v2.01.6198, optional SCL v2.13.001, optional ACL v3.03.003, optional ACL v3.04.001, optional ACL v3.05.002, optional HCL v1.13.001, optional RCL v1.10.006 and with specific IC-dedicated firmware identifier 80.203.00.3 and Flash Loader v8.06.001 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 and H11
Firmware	BOS	80.203.00.3
	Flash Loader	V8.06.001
Software	ACL	v3.03.003 or v3.04.001 or V3.05.002
	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 TOE. For details, see section 2.5 “Documentation” of this report.

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 and 4.3 of the *[ST]*.

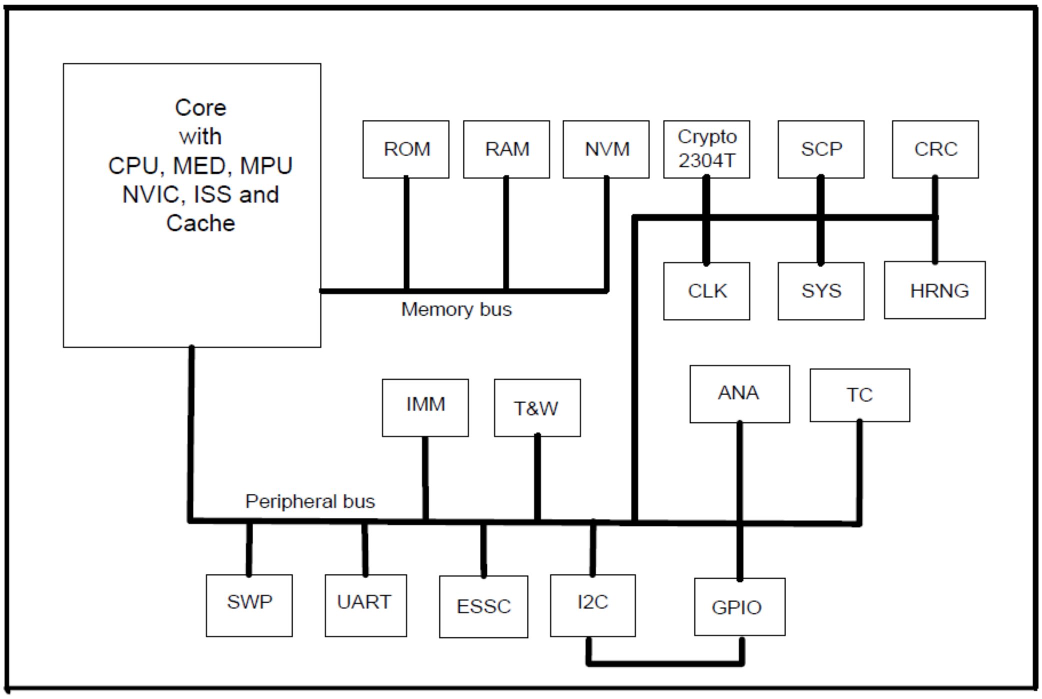
2.3.2 Clarification of scope

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

Note that there are TOE configurations that are critically dependent on the Embedded Software operational environment (as defined in the [PP]) to provide countermeasures against specific attacks as described in the TOE guidance and [ETRfc]. It is important to remark that in this specific context, the evaluation considered the specific guidance on countermeasures relying on the Embedded Software operational environment. Alternative implementations of this guidance, or other mitigations not relying on the Embedded Software operational environment were not in the scope of this evaluation.

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	V4.0 dated 2021-06-29
32-bit Security Controller – V21 Hardware Reference Manual	V4.0 dated 2021-06-29
ARMv7-M Architecture Reference Manual	DDI 0403D

	ID021310 dated 2010-02-12
Production and personalization 32-bit ARM-based security controller User´s Manual	V3.5 dated 2021-12-17
SLC37 (65 nm Technology) Programmer's Reference Manual	V5.3 dated 2022-07-08
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	V5.1 dated 2023-08-04
32-bit Security Controller – V21 Errata Sheet	V5.1 dated 2023-08-04
32-bit Security Controller Crypto@2304T V3 User Manual	V3 dated 2024-06-21
ACL37-Crypto2304T-C65 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox User interface manual	v3.03.003 dated 2024-08-16
ACL37-Crypto2304T-C65 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox User interface manual	3.04.001 dated 2024-08-16
ACL37-Crypto2304T-C65 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox User interface manual	3.05.002 dated 2024-06-03
SCL37-SCP-v4-C65 Symmetric Crypto Library for SCP-v4 AES/DES/MAC User interface manual	v2.13.001 dated 2024-07-25
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 the baseline evaluations 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 the baseline evaluations and this 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 this re-evaluation, additional test effort expended by the evaluators was 6 weeks, of which 30% on Perturbation Attacks, 70% on side channel.

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 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.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength for satisfying the AVA_VAN.5 "high attack potential". The TOE supports a wider range of key sizes (see *[ST]*), including those with sufficient algorithmic security level to exceed 100 bits 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.

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

2.7 Reused Evaluation Results

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

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

No sites have been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number IFX_CCI_00003Fh IFX_CCI_000059h IFX_CCI_00005Bh IFX_CCI_00003Ch IFX_CCI_00003Dh IFX_CCI_00005Ah design step G11 and H11 with optional HSL v2.01.6198, optional SCL v2.13.001, optional ACL v3.03.003, optional ACL v3.04.001, optional ACL v3.05.002, optional HCL v1.13.001, optional RCL v1.10.006 and with specific IC-dedicated firmware identifier 80.203.00.3 and Flash Loader v8.06.001.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents. To support composite evaluations according to *[COMP]* a derived document *[ETRfC]* was provided and approved. This document provides details of the TOE evaluation that must be considered when this TOE is used as platform in a composite evaluation.

The verdict of each claimed assurance requirement is “**Pass**”.

Based on the above evaluation results the evaluation lab concluded the TOE, 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 ’strict’ conformance to the Protection Profile *[PP]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 “Documentation” contains necessary information about the usage of the TOE. There are TOE configurations that are critically dependent on the Embedded Software operational environment (as defined in the [PP]) to provide countermeasures against specific attacks as described in the TOE guidance. As such it is vital that meticulous adherence to the user guidance of both the software and the hardware part of the TOE is maintained.

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, which are out of scope as there are no security claims relating to these.

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 Confidential Security Target IFX_CCI_00003Fh IFX_CCI_000059h IFX_CCI_00005Bh IFX_CCI_00003Ch IFX_CCI_00003Dh IFX_CCI_00005Ah G11 and H11 including optional software libraries: Flash Loader according Package1 and Package2, HCL, RCL, HSL, ACL and SCL, Revision 2.6, 16 August 2024 *[ST]* is included here by reference.

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

4 Definitions

This list of acronyms and definitions 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

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

[ETR] EVALUATION TECHNICAL REPORT (ETR SUMMARY), IFX_CCI_00003Fh IFX_CCI_000059h IFX_CCI_00005Bh IFX_CCI_00003Ch IFX_CCI_00003Dh IFX_CCI_00005Ah G11 and H11, 8122852298 / NSCIB-2200060-02, version 3, 22 August 2024

[ETRfC] EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION (ETR COMP), IFX_CCI_00003Fh IFX_CCI_000059h IFX_CCI_00005Bh IFX_CCI_00003Ch IFX_CCI_00003Dh IFX_CCI_00005Ah G11 and H11, 8122852298 / NSCIB-2200060-02, version 3, 22 August 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)

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

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

[ST] Confidential Security Target IFX_CCI_00003Fh IFX_CCI_000059h IFX_CCI_00005Bh IFX_CCI_00003Ch IFX_CCI_00003Dh IFX_CCI_00005Ah G11 and H11 including optional software libraries: Flash Loader according Package1 and Package2, HCL, RCL, HSL, ACL and SCL, Revision 2.6, 16 August 2024

[ST-lite] Public Security Target IFX_CCI_00003Fh IFX_CCI_000059h IFX_CCI_00005Bh IFX_CCI_00003Ch IFX_CCI_00003Dh IFX_CCI_00005Ah G11 and H11 including optional software libraries: Flash Loader according Package1 and Package2, HCL, RCL, HSL, ACL and SCL, Revision 2.6, 16 August 2024

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

(This is the end of this report.)