

Certification Report

BSI-DSZ-CC-1075-2018

for

**IFX_CCI_000Dh, IFX_CCI_0020h, IFX_CCI_0031h,
IFX_CCI_0032h, IFX_CCI_0034h design step T23
with optional HSL v2.62.7626, optional SCL
v2.04.003, UMSLC lib v01.00.0234 with specific IC-
dedicated firmware identifier 80.301.05.1 and user
guidance**

from

Infineon Technologies AG

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111



Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom



Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1075-2018 (*)

**IFX_CCI_000Dh, IFX_CCI_0020h, IFX_CCI_0031h, IFX_CCI_0032h,
IFX_CCI_0034h design step T23 with optional HSL v2.62.7626, optional
SCL v2.04.003, UMSLC lib v01.00.0234 with specific IC-dedicated
firmware identifier 80.301.05.1 and user guidance**

from Infineon Technologies AG

PP Conformance: Security IC Platform Protection Profile with
Augmentation Packages Version 1.0, 13 January
2014, BSI-CC-PP-0084-2014

Functionality: PP conformant plus product specific extensions
Common Criteria Part 2 extended

Assurance: Common Criteria Part 3 conformant
EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5



SOGIS
Recognition Agreement



The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations, by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents as listed in the Certification Report for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) 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 and Notification. For details on the validity see Certification Report part A chapter 4

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) 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 the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 20 September 2018

For the Federal Office for Information Security

Bernd Kowalski
Head of Division

L.S.



Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2 and ALC_FLR
only



Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

Contents

A. Certification.....	6
1. Preliminary Remarks.....	6
2. Specifications of the Certification Procedure.....	6
3. Recognition Agreements.....	7
4. Performance of Evaluation and Certification.....	8
5. Validity of the Certification Result.....	8
6. Publication.....	9
B. Certification Results.....	10
1. Executive Summary.....	11
2. Identification of the TOE.....	12
3. Security Policy.....	14
4. Assumptions and Clarification of Scope.....	15
5. Architectural Information.....	16
6. Documentation.....	16
7. IT Product Testing.....	16
8. Evaluated Configuration.....	16
9. Results of the Evaluation.....	18
10. Obligations and Notes for the Usage of the TOE.....	21
11. Security Target.....	22
12. Definitions.....	22
13. Bibliography.....	23
C. Excerpts from the Criteria.....	25
D. Annexes.....	26

A. Certification

1. Preliminary Remarks

Under the BSIG¹ Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

2. Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- Act on the Federal Office for Information Security¹
- BSI Certification and Approval Ordinance²
- BSI Schedule of Costs³
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1⁴ [1] also published as ISO/IEC 15408.

¹ Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

² Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

³ Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045.
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

3. Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

3.1. European Recognition of CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4. For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at <https://www.sogisportal.eu>.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized under SOGIS-MRA for all assurance components selected.

3.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The current list of signatory nations and approved certification schemes can be seen on the website: <http://www.commoncriteriaportal.org>.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2+ ALC_FLR components.

⁴ Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

4. Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product IFX_CCI_000Dh, IFX_CCI_0020h, IFX_CCI_0031h, IFX_CCI_0032h, IFX_CCI_0034h design step T23 with optional HSL v2.62.7626, optional SCL v2.04.003, UMSLC lib v01.00.0234 with specific IC-dedicated firmware identifier 80.301.05.1 and user guidance has undergone the certification procedure at BSI.

The evaluation of the product IFX_CCI_000Dh, IFX_CCI_0020h, IFX_CCI_0031h, IFX_CCI_0032h, IFX_CCI_0034h design step T23 with optional HSL v2.62.7626, optional SCL v2.04.003, UMSLC lib v01.00.0234 with specific IC-dedicated firmware identifier 80.301.05.1 and user guidance was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 18 September 2018. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)⁵ recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Infineon Technologies AG.

The product was developed by: Infineon Technologies AG.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, as specified in the following report and in the Security Target.

For the meaning of the assurance components and assurance levels please refer to CC itself. Detailed references are listed in part C of this report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-assessment or re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 20 September 2018 is valid until 19 September 2023. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

⁵ Information Technology Security Evaluation Facility

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,
2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

6. Publication

The product IFX_CCI_000Dh, IFX_CCI_0020h, IFX_CCI_0031h, IFX_CCI_0032h, IFX_CCI_0034h design step T23 with optional HSL v2.62.7626, optional SCL v2.04.003, UMSLC lib v01.00.0234 with specific IC-dedicated firmware identifier 80.301.05.1 and user guidance has been included in the BSI list of certified products, which is published regularly (see also Internet: <https://www.bsi.bund.de> and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer⁶ of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

⁶ Infineon Technologies AG

Am Campeon 1-12
85579 Neubiberg

B. Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1. Executive Summary

The Target of Evaluation (TOE) is the Security IC named IFX_CCI_000Dh, IFX_CCI_0020h, IFX_CCI_0031h, IFX_CCI_0032h, IFX_CCI_0034h design step T23 with optional HSL v2.62.7626, optional SCL v2.04.003, UMSLC lib v01.00.0234 with specific IC-dedicated firmware identifier 80.301.05.1 and user guidance.

The Security Target [6] and [9] are the basis for this certification. It is based on the certified Protection Profile Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014 [8].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [9], chapter 6. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality	Addressed issue
SF_DPM	Device Phase Management: The life cycle of the TOE is split up into several phases. Different operation modes help to protect the TOE during each phase of its lifecycle.
SF_PS	Protection against Snooping: The TOE uses various means to protect from snooping.
SF_PMA	Protection against Modifying Attacks: This TOE implements protection against modifying attacks of various TOE parts.
SF_PLA	Protection against Logical Attacks:
SF_CS	Cryptographic Support: The TOE is equipped with a hardware accelerator and an optional symmetric cryptographic library (SCL) to support the standard symmetric cryptographic operations TDES and AES. Additionally, the TOE is equipped with a True Random Number Generator for the generation of random numbers

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] and [9], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [6] and [9], chapter 3.1.2 . Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and [9], chapter 3.1 / 3.2.

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

IFX_CCI_000Dh, IFX_CCI_0020h, IFX_CCI_0031h, IFX_CCI_0032h, IFX_CCI_0034h design step T23 with optional HSL v2.62.7626, optional SCL v2.04.003, UMSLC lib v01.00.0234 with specific IC-dedicated firmware identifier 80.301.05.1 and user guidance.

The following table outlines the TOE deliverables:

Type	Identifier	Release	Form of Delivery
HW	IFX_CCI_000Dh, IFX_CCI_0020h, IFX_CCI_0031h, IFX_CCI_0032h, IFX_CCI_0034h	T23 (produced in Singapore)	plain wafers in an IC case or in bare dies
FW	Flash Loader	v8.07.006	located at the end of User NVM for non-blocked derivatives
FW	BOS	FW identifier: 80.301.05.1	stored in IFX ROM region on IC (BOS Patch Area in IFX region on NVM)
SW	HSL library (optional)	v2.62.7626	Secure download (object code) via ishare. (optional)
SW	UMSLC library	v01.00.0234	Secure download (object code) via ishare.
SW	SCL library (optional)	v2.04.003	Secure download (object code) via ishare. (optional)
DOC	32-bit Security Controller – V02, Hardware Reference Manual [12]	V7.0, 2018-06-13	Secured download (PDF) via ishare.
DOC	32-bit ARM-based Security Controller, SLC 37/40-nm Technology, Programmer's Reference Manual [13]	V4.0, 2018-04-13	Secured download (PDF) via ishare.

Type	Identifier	Release	Form of Delivery
DOC	32-bit Security Controller – V02, Security Guidelines [14]	V1.00-1797, 2018-04-24	Secured download (PDF) via ishare.
DOC	Production and personalization 32-bit ARM-based security controller [15]	V3.4, 2018-05-14	Secured download (PDF) via ishare
DOC	HSL library for SLCx7 in 40nm (optional) [16]	V02.62.7626, 2017-12-13	Secured download of compiled html help (chm) file via ishare (optional)
DOC	UMSLC library for SLCx7 in 40nm, Version 01.00.0234 [17]	V1.1, 2018-05-23	Secured download of compiled html help (chm) file via ishare
DOC	SCL37-uSCP-v3-C40 Symmetric Crypto Library for uSCP-v3 DES /AES [18]	V2.04.003, 2018-03-02	Secured download (PDF) via ishare

Table 2: Deliverables of the TOE

The hardware part of the TOE is identified by its Common Criteria Identifiers (CCI) IFX_CCI_000Dh, IFX_CCI_0020h, IFX_CCI_0031h, IFX_CCI_0032h, IFX_CCI_0034h and the design step T23. The complete chip identification data is accessible via the Generic Chip Identification Mode (GCIM).

As the TOE is under control of the user software, the TOE Manufacturer can only guarantee the integrity up to the delivery procedure. It is in the responsibility of the Composite Product Manufacturer to include mechanisms in the implemented software (developed by the IC Embedded Software Developer) which allows detection of modifications after the delivery.

In detail, regarding identification:

The Generic Chip Identification Mode (GCIM) can be activated after power-on with a dedicated signalling sequence and is also accessible by the user software. This GCIM outputs amongst other identifiers for the platform, chip mode, ROM code, chip type, design step, fabrication facility, wafer, die position, firmware, temperature range, and system frequency and the CCI (Common Criteria identifier). The interpretation of the chip identification data is described in [12], section 4.5.2.

Additionally, the customer can identify the present configuration (see [13], section 7.9).

The SCL (optional), UMSLC and HSL library (optional), as separate software parts of the TOE, are identified by their unique version numbers. The user can identify these versions by calculating the hash signatures of the provided library files. The mapping of these hash signatures to the version numbers is provided in [6] and [9], chapters 9–11.

In detail, regarding delivery:

“TOE Delivery” is uniquely used to indicate

- after Phase 3 (or before Phase 4) if the TOE is delivered in form of wafers or sawn wafers (dice) or
- after Phase 4 (or before Phase 5) if the TOE is delivered in form of packaged products.

Therefore three different delivering procedures have to be taken into consideration:

- Delivery of the IC dedicated software components (IC dedicated SW, guidance) from the TOE manufacturer to the IC embedded software developer.
- Delivery of the IC embedded software (ROM / Flash data, initialisation and pre-personalization data, Bundle Business package) from the IC embedded software developer to the TOE manufacturer.
- Delivery of the final TOE from the TOE manufacturer to the composite product manufacturer. After phase 3 the TOE is delivered in form of wafers or sawn wafers, after phase 4 in form of modules (with or without inlay antenna).

The TOE is delivered via the logistics sites:

- DHL Singapore (Distribution Center Asia),
- G&D Neustadt,
- K&N Großostheim (Distribution Center Europe),
- K&N Hayward (Distribution Center USA).

3. Security Policy

The security policy enforced is expressed by the selected set of Security Functional Requirements and consequently implemented by the TOE. It covers the following issues:

The Security Policy of the TOE is to provide basic security functionalities to be used by the smart card operating system and the smart card application, thus providing an overall smart card system security. Therefore, the TOE will implement a symmetric cryptographic block cipher algorithm (Triple-DES and AES) to ensure the confidentiality of plain text data by encryption and to support secure authentication protocols and it will provide a True Random Number Generator (TRNG).

The optional SCL provides TDES and AES cryptography, which is partly implemented on the hardware component μ SCP and includes countermeasures against SPA, DPA and DFA attacks. The SCL is delivered as object code and in this way integrated into the user software,

The optional HSL provides functionality via APIs to the Smartcard Embedded Software, which contains SOLID FLASH™ NVM service routines and functionality for tearing-safe programming of SOLID FLASH™ NVM.

The UMSLC library provides a wrapper around the UMSLC hardware functionality with some software measures to counter fault attacks.

As the TOE is a hardware security platform, the security policy of the TOE is also to provide protection against leakage of information (e.g. to ensure the confidentiality of cryptographic keys during AES and Triple-DES cryptographic functions performed by the TOE), against physical probing, against malfunctions, against physical manipulations and against abuse of functionality. Hence the TOE shall

- maintain the integrity and the confidentiality of data stored in the memory of the TOE and
- maintain the integrity, the correct operation and the confidentiality of security functionalities (security mechanisms and associated functions) provided by the TOE.

Specific details concerning the above mentioned security policies can be found in Chapter 7 and 8 of the Security Target (ST).

4. Assumptions and Clarification of Scope

The assumptions defined in the Security Target and some aspects of threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled and measures to be taken by the IT environment, the user or the risk manager. The following topics are of relevance:

The ST only includes one security objective for the IC Embedded Software Developer, the objective OE.Resp-Appl.

The objective OE.Resp-Appl states that the IC Embedded Software Developer shall treat user data (especially keys) appropriately. The IC Embedded Software Developer gets sufficient information on how to protect user data adequate in the security guidelines [14].

The ST includes the following security objectives for the operational environment, which are relevant for the Composite Product Manufacturer: OE.Process-Sec-IC, OE.Lim_Block_Loader, OE.Loader_Usage and OE.TOE_Auth.

The objective OE.Process-Sec-IC requires the protection of the TOE, as well as of its manufacturing and test data up to the delivery to the end-consumer. As defined in [6] and [9] section 1.4.5, the TOE can be delivered to the composite product manufacturer after phase 3 or after phase 4. However, the single chips are identical in all cases. This means that the test mode is deactivated and the TOE is locked in the user mode. Therefore it is not necessary to distinguish between these forms of delivery. Since Infineon has no information about the security requirements of the implemented IC embedded software it is not possible to define any concrete security requirements for the environment of the composite product manufacturer.

The objective OE.TOE_Auth requires that the environment has to support the authentication and verification mechanism and has to know the corresponding authentication reference data. The composite product manufacturer receives sufficient information with regard to the authentication mechanism in [15], section 4.2.2.

The objective OE.Loader_Usage requires that the authorised user has to support the trusted communication with the TOE by protecting the confidentiality and integrity of the loaded data and he has to meet the access conditions defined by the flash loader. [15], section 4 provides sufficient information regarding this topic.

The objective OE.Lim_Block_Loader requires the composite product manufacturer to protect the loader against misuse, to limit the capability of the loader and to terminate the loader irreversibly after the intended usage. The permanent deactivation of the flash loader is described in [15] section 4.5.1.3. This objective for the environment originates from the "Package 1: Loader dedicated for usage in secured environment only". However, this TOE also implements "Package 2: Loader dedicated for usage by authorized users only" and thus the flash loader can also be used in an unsecure environment and is able to protect itself against misuse if the authentication and download keys are handled appropriately.

5. Architectural Information

The TOE is a SmartCard (Security IC). Detailed information on the TOE hardware architecture is to be found in [6] and [9] section 1.2, 1.3 and especially 1.4.

6. Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7. IT Product Testing

The developer performed five categories of tests:

- Simulation Tests (Design Verification),
- Qualification Tests / Software Verification,
- Verification Tests,
- Security Evaluation Tests, and
- Production Tests.

The developer tests cover all security functionalities and all security mechanisms as identified in the functional specification.

The evaluators were able to repeat the tests of the developer either using the library of programs, tools and prepared chip samples delivered to the evaluator or at the developer's site. They performed independent tests to supplement, augment and to verify the tests performed by the developer. For the developer tests repeated by the evaluators other test parameters were used and the test equipment was varied. Security features of the TOE realised by specific design and layout measures were checked by the evaluators during layout inspections both in design data and on the final product.

The evaluation has shown that the actual version of the TOE provides the security functionalities as specified by the developer. The test results confirm the correct implementation of the TOE security functionalities.

For penetration testing the evaluators took all security functionalities into consideration. Intensive penetration testing was planned based on the analysis results and performed for the underlying mechanisms of security functionalities. The penetration tests considered both the physical tampering of the TOE and attacks which do not modify the TOE physically. The penetration tests results confirm that the TOE is resistant to attackers with high attack potential in the intended environment for the TOE.

8. Evaluated Configuration

The evaluation and certification covers the following identifiers of the TOE:

- IFX_CCI_000Dh, IFX_CCI_0020h, IFX_CCI_0031h, IFX_CCI_0032h, IFX_CCI_0034h design step T23.

Hardware Configuration:

The hardware of the TOE can be ordered with different SOLID FLASH™ and RAM sizes (up to 800 kBytes SOLID FLASH™ and up to 20 kBytes RAM). The configuration (as listed in [6] and [9] table 3 and 4) can be done during the manufacturing process of the TOE according to the choice of the user.

Firmware Packages:

The firmware of the TOE comprises the BOS (FW identifier provided in table 2) and the Flash Loader (version provided in Table 2). The latter can be configured in three different ways as outlined in the following:

- Option 1: The user or/and a subcontractor downloads the software into the SOLID FLASH™ memory. Infineon Technologies does not receive any user software.

Result: Flash Loader can be activated or reactivated by the user or subcontractor to download software into the SOLID FLASH™ memory.

- Option 2: The user provides software to download into the SOLID FLASH™ memory to Infineon Technologies AG. The software is loaded into the SOLID FLASH™ memory during chip production.

Result: No Flash Loader present.

- Option 3: The user provides software to download into the SOLID FLASH™ memory to Infineon Technologies AG. The software is loaded into the NVM memory during chip production.

Result: Flash Loader is blocked by Infineon but can be activated or reactivated by the user or subcontractor to download software into the SOLID FLASH™ memory. The user is required to provide a reactivation procedure as part of the software to Infineon Technologies AG.

An overview about the different Flash Loader options is also given in [6] and [9], section 1.4.8.

Optional Software Libraries:

The TOE can be delivered with up to three software libraries, as described in [6] and [9] section 1.4.1.2. All libraries are delivered as object code and in this way integrated into the user software.

The optional software libraries listed in Table 2 can be combined according to the demands of the user. Based on the library selection the TOE can be delivered with or without the functionality of the HSL and/or SCL library. This is considered in the developer documentation and corresponding notes are added where required.

If the user decides not to use the HSL and/or SCL library, it is not delivered to the user and the accompanying additional specific security functionality as listed in Table 2 is not provided by the TOE. Upon deselection of a library the code implementing the functionality is excluded and thus this functionality is not available to the user.

Excluding the code of the deselected functionality has no impact on any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use this functionality.

Evaluation scope:

The ITSEF tested the TOE in those configurations, in which the TOE is delivered, and which are stated above (and in the ST [6] and [9]).

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used for those components up to EAL 5 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance (mostly) specific for the technology was used:

- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 1, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers, Version 14, 2017-10-11,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 14, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 7, 2010-08-03,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 19, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 9, 2014-11-03,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 23, Zusammentragen von Nachweisen der Entwickler, Version 4, 2017-03-15,
- Application Notes and Interpretation of the Scheme (AIS) – AIS 25, Anwendungen der CC auf integrierte Schaltungen, Version 9, 2017-03-15,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 26, Evaluationsmethodologie für in Hardware integrierte Schaltungen, Version 10, 2017-07-03,
- Special Attack Methods for Smartcards and Similar Devices, Version 1.4, 2011-06-08,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 31, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3, 2013-05-15,
- Application Notes and Interpretation of the Scheme (AIS) – AIS 34, Evaluation Methodology for CC Assurance Classes for EAL5+ (CC v2.3 & v3.1) and EAL6 (CC v3.1), Version 3, 2009-09-03,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 35, Öffentliche Fassung eines Security Target (ST-lite), Version 2, 2007-11-12,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 36, Kompositionsevaluierung, Version 5, 2017-03-15,
- Application Notes and Interpretation of the Scheme (AIS) – AIS 38, Reuse of evaluation results, Version 2, 2007-09-28,

- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 47, Regelungen zu Site Certification, Version 1.1, 2013-12-04

are considered.

Additionally the CC Supporting Mandatory Technical Documents

- Joint Interpretation Library – The Application of CC to Integrated Circuits, Version 3.0, February 2009,
- Joint Interpretation Library – Application of Attack Potential to Smartcards, Version 2.9, 2013-01 and
- Joint Interpretation Library – ETR template for composite evaluation of Smart Cards and similar devices, Version 1.1, August 2015

are considered.

For RNG assessment the scheme interpretations AIS 20/31 was used (see [4]).

To support composite evaluations according to AIS 36 the document ETR for composite evaluation [10] was provided and approved. This document provides details of this platform evaluation that have to be considered in the course of a composite evaluation on top of it.

The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 5 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_DVS.2 and AVA_VAN.5 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014 [8]
- for the Functionality: PP conformant plus product specific extensions
Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5

For specific evaluation results regarding the development and production environment see annex B in part D of this report.

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But cryptographic functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some

further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (<https://www.bsi.bund.de>).

The following table gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its rating from cryptographic point of view. Any Cryptographic Functionality that is marked in column 'Security Level above 100 Bits' of the following table with 'no' achieves a security level of lower than 100 Bits (in general context) only:

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
Cryptographic Primitive	TDES in modes	[NIST SP 800-67]	All modes: k = 112, 168	CBC, CFB, CTR, CMAC: 168: Yes, 112: No
	ECB, CBC, CFB and CTR	[NIST SP 800-38A]		
	CMAC	[NIST SP 800-38B]		
	AES in modes	[FIPS197]	All modes: k = 128, 192, 256	CBC, CFB, CTR, CMAC: 128, 192, 256: Yes
	ECB, CBC, CFB and CTR	[NIST SP 800-38A]		
	CMAC	[NIST SP 800-38B]		
Physical True RNG PTG.2	[AIS31] (proprietary)	N/A	N/A	

Table 3: TOE cryptographic functionality

The Flash Loader's and the ICS' (internal ciphering system, see [6] and [9]) cryptographic strength was not assessed by BSI. However, the evaluation according to the TOE's Evaluation Assurance Level did not reveal any implementation weaknesses.

Please note, that this holds true also for those algorithms, where no cryptographic 100-Bit-Level assessment was given. Consequently, the targeted Evaluation Assurance Level has been achieved for those functionalities as well.

Detailed results on conformance have been compiled into the report [19].

Reference of Legislatives and Standards quoted above:

[NIST SP800-67] NIST Special Publication 800-67 – Revision 2, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, November 2017, National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce.

[NIST SP800-38A] NIST SP800-38A, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, 2001, National Institute of Standards and Technology (NIST).

- [NIST SP 800-38B]** NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication, 2005-05, National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce.
- [FIPS197]** Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTION STANDARD (AES), November 2001, U.S. department of Commerce / National Institute of Standards and Technology (NIST).
- [AIS31]** Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 31, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3, 2013-05-15, Bundesamt für Sicherheit in der Informationstechnik.

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs 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 of the TOE is required and thus requested from the sponsor of the certificate.

Some security measures are partly implemented in this certified TOE, but require additional configuration or control or measures to be implemented by a product layer on top, e.g. the Embedded Software using the TOE. For this reason the TOE includes guidance documentation (see table 2) which contains obligations and guidelines for the developer of the product layer on top on how to securely use this certified TOE and which measures have to be implemented in order to fulfil the security requirements of the Security Target of the TOE. In the course of the evaluation of the composite product or system it must be examined if the required measures have been correctly and effectively implemented by the product layer on top. Additionally, the evaluation of the composite product or system must also consider the evaluation results as outlined in the document ETR for composite evaluation [10].

The Security IC Embedded Software Developer receives all necessary recommendations and hints to develop his software in form of the delivered documentation.

- All security hints described in the delivered documents [12]-[14] and [16]-[18] (also listed in Table 2) have to be considered.

The Composite Product Manufacturer receives all necessary recommendations and hints to develop his software in form of the delivered documentation.

- All security hints described in [15] have to be considered.

In addition the following hints resulting from the evaluation of the ALC evaluation aspect has to be considered:

- The IC Embedded Software Developer can deliver his software either to Infineon to let them implement it in the TOE (in Flash memory) or to the Composite Product Manufacturer to let him download the software in the Flash memory.

- The delivery procedure from the IC Embedded Software Developer to the Composite Product Manufacturer is not part of this evaluation and a secure delivery is required.

11. Security Target

For the purpose of publishing, the Security Target [9] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

12. Definitions

12.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

12.2. Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

Extension - The addition to an ST or PP of functional requirements not contained in CC part 2 and/or assurance requirements not contained in CC part 3.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Package - named set of either security functional or security assurance requirements

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

13. Bibliography

- [1] Common Criteria for Information Technology Security Evaluation, Version 3.1, Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
<http://www.commoncriteriaportal.org>
- [2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017,
<http://www.commoncriteriaportal.org>
- [3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen), <https://www.bsi.bund.de/zertifizierung>
- [4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE⁷
<https://www.bsi.bund.de/AIS>
- [5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website, <https://www.bsi.bund.de/zertifizierungsberichte>
- [6] Security Target for BSI-DSZ-CC-1075-2018, "IFX_CCI_000Dh, IFX_CCI_0020h, IFX_CCI_0031h, IFX_CCI_0032h, IFX_CCI_0034h T23 Security Target", Version 3.6, 2018-09-17, Infineon Technologies AG (confidential document)
- [7] Evaluation Technical Report, Version 5, 2018-09-19, "EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY)", TÜV Informationstechnik GmbH, (confidential document)

⁷ See section 9.1 for detailed list of used AIS

- [8] Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014
- [9] Security Target for BSI-DSZ-CC-1075-2018, “IFX_CCI_000Dh, IFX_CCI_0020h, IFX_CCI_0031h, IFX_CCI_0032h, IFX_CCI_0034h T23 Security Target Lite”, Version 3.6, 2018-09-17, Infineon Technologies AG (sanitised public document)
- [10] ETR for composite evaluation according to AIS 36 for BSI-DSZ-CC-1075-2018, Version 5, 2018-09-19, “EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION (ETR COMP)”, TÜV Informationstechnik GmbH (confidential document)
- [11] Configuration list for the TOE, “Configuration Management Scope”, Version 1.0, 2018-06-06, Infineon Technologies AG (confidential document)
- [12] “32-bit Security Controller – V02, Hardware Reference Manual”, v7.0, 2018-06-13, Infineon Technologies AG
- [13] “32-bit ARM-based Security Controller, SLC 37/40-nm Technology, Programmer’s Reference Manual”, v4.0, 2018-04-13, Infineon Technologies AG
- [14] “32-bit Security Controller – V02, Security Guidelines”, v1.00-1797, 2018-04-24, Infineon Technologies AG
- [15] “Production and personalization 32-bit ARM-based security controller”, v3.4, 2018-05-14, Infineon Technologies AG
- [16] “HSL library for SLCx7 in 40nm (optional)”, V02.62.7626, 2017-12-13, Infineon Technologies AG
- [17] “UMSLC library for SLCx7 in 40nm, Version 01.00.0234”, V1.1, 2018-05-23, Infineon Technologies AG
- [18] “SCL37-uSCP-v3-C40 Symmetric Crypto Library for uSCP-v3 DES /AES”, V2.04.003, 2018-03-02, Infineon Technologies AG
- [19] “Cryptographic Standards Compliance Verification”, Version 4, 2018-09-13, TÜV Informationstechnik GmbH (confidential document)

C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria can be followed:

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12
- On the detailed definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17
- The table in CC part 3 , Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published at <http://www.commoncriteriaportal.org/cc/>

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development
and production environment

Annex B of Certification Report BSI-DSZ-CC-1075-2018

Evaluation results regarding development and production environment



The IT product IFX_CCI_000Dh, IFX_CCI_0020h, IFX_CCI_0031h, IFX_CCI_0032h, IFX_CCI_0034h design step T23 with optional HSL v2.62.7626, optional SCL v2.04.003, UMSLC lib v01.00.0234 with specific IC-dedicated firmware identifier 80.301.05.1 and user guidance (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations, by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 20 September 2018, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.2)

are fulfilled for the development and production sites of the TOE.

The relevant delivery sites are as follows:

Site ID	Company name and address
DHL Singapore	DHL Exel Supply Chain Richland Business Centre 11 Bedok North Ave 4, Level 3, Singapore 489949
G&D Neustadt	Giesecke & Devrient Secure Data Management GmbH Austraße 101b 96465 Neustadt bei Coburg Germany
K&N Großostheim	Infineon Technology AG Distribution Center Europe (DCE) Kühne & Nagel Stockstädter Strasse 10 – Building 8A 63762 Großostheim Germany
K&N Hayward	Kuehne & Nagel 30805 Santana Street Hayward, CA 94544 USA

Table 4: TOE Delivery / Distribution Sites

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]. The evaluators verified, that the threats, security objectives and requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6] and [9]) are fulfilled by the procedures of these sites.

Note: End of report