Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1025-V5-2023

for

Infineon Technologies AG Smartcard IC IFX_CCI_000011h, 00001Bh, 00001Eh,000025h, design step G12 with optional libraries and with specific dedicated software

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-1025-V5-2023 (*)

Smartcard Controller

Infineon Technologies AG Smartcard IC IFX_CCI_000011h, 00001Bh, 00001Eh,000025h, design step G12 with optional libraries and with specific dedicated software

SOGIS
Recognition Agreement

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 6 augmented by ALC_FLR.1
valid until:	12 July 2028

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 5.

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.

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

Bonn, 13 July 2023

For the Federal Office for Information Security

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

Matthias Intemann
Head of Section

L.S.

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

1. Preliminary Remarks

Under the BSIG[1] 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 Security[1]
- BSI Certification and Approval Ordinance[2]
- BMI Regulations on Ex-parte Costs [3]
- Special decrees issued by the Bundesministerium des Innern und für Heimat (Federal Ministry of the Interior and Community)
- 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 3.1[4] [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 BMI Regulations on Ex-parte Costs - Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) - dated 2 September 2019, Bundesgesetzblatt I p. 1365

- 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.sogis.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: https://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 and ALC_FLR components.

[4] Proclamation of the Bundesministerium des Innern und für Heimat 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 Infineon Technologies AG Smartcard IC IFX_CCI_000011h, 00001Bh, 00001Eh,000025h, design step G12 with optional libraries and with specific dedicated software, has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1025-V4-2021. Specific results from the evaluation process BSI-DSZ-CC-1025-V4-2021 were re-used.

The evaluation of the product Infineon Technologies AG Smartcard IC IFX_CCI_000011h, 00001Bh, 00001Eh,000025h, design step G12 with optional libraries and with specific dedicated software, was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 30 June 2023. 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 13 July 2023 is valid until 12 July 2028. 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 Infineon Technologies AG Smartcard IC IFX_CCI_000011h, 00001Bh, 00001Eh,000025h, design step G12 with optional libraries and with specific dedicated software 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 developer[6] 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 1-15
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 Infineon Technologies AG security controller (integrated circuit IC), IFX_CCI_000011h, IFX_CCI_00001Bh, IFX_CCI_00001Eh, IFX_CCI_000025h Design Step G12, with specific IC dedicated firmware and the following optional software: Asymmetric Crypto Library (ACL) RSA 2048/4096 v2.08.006 or v3.03.003 or v3.04.001, EC v2.08.006 or v3.03.003 or v3.04.001, Toolbox v2.08.006 or v3.03.003 or v3.04.001 (Non-TSF), Base library v2.08.006 or v3.03.003 or v3.04.001,Symmetric Crypto Library (SCL) v2.13.001, Hardware Support Library (HSL) v2.01.6198, NRG™ Library (NRG / NRGS) v04.03.3431 (Non-TSF) and CIPURSE™ Cryptographic Library (CCL) v2.00.0005.

TOE is referenced via the firmware identifier 80.201.04.1 or 80.201.04.2.

The TOE provides a proprietary 32-bit RISC CPU designed on the basis of the ARMv7_M architecture. The major components of the core system is the CPU (Central Processing Unit), the MPU (Memory Protection Unit) and MED (Memory Encryption / Decryption Unit).

The TOE consists of the hardware part, the firmware part, the software part as well as the user guidance.

This TOE is intended to be used in smart cards for particularly security relevant applications and for its previous use as developing platform for smart card operating systems. The term smartcard embedded software is used in the following for all operating systems and applications stored and executed on the TOE. The TOE is the platform for the smartcard embedded software.

Depending on the blocking configuration, an IFX_CCI_000011h G12 product can have e.g. different user available memory sizes and can come with or without individual accessible cryptographic coprocessors. All products are identical in regard to module design, layout and footprint.

The Security Target [6] is 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 6 augmented by ALC_FLR.1.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [9], chapter 7. 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 following a defined sequence. Different operation modes with appropriate restrictions help to protect the TOE during each phase of its lifecycle. This also includes the permanent deactivation of the flash loader.

TOE Security Functionality	Addressed issue
SF_PS	Protection against Snooping: The TOE is equipped with various countermeasures against snooping.
SF_PMA	Protection against Modifying Attacks: This TOE is equipped with various countermeasures against modifying attacks.
SF_PLA	Protection against Logical Attacks: The memory model of the TOE provides two distinct, independent levels and the possibility to define up to eight memory regions with different access rights enforced by the Management Protection Unit (MPU).
SF_CS	Cryptographic Support: The TOE is equipped with several hardware accelerators and software modules to support the standard symmetric and asymmetric cryptographic operations like RSA, EC, TDES, and AES. Additionally the TOE is equipped with a Hybrid Random Number Generator providing four different modes of operation: Hybrid random number generation, true random number generation, deterministic random number generation and key stream generation. The TOE is further equipped with an optional CIPURSE™ Library which can be used by the IC embedded software to set up a CIPURSE™ V2 conformant protocol.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] and [9], chapter 8.

The assets to be protected by the TOE are defined in the Security Target [6] and [9], chapter 4. 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 4.

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:

Infineon Technologies AG Smartcard IC IFX_CCI_000011h, 00001Bh, 00001Eh,000025h, design step G12 with optional libraries and with specific dedicated software

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	IFX_CCI_000011h, IFX_CCI_00001Bh, IFX_CCI_00001Eh, IFX_CCI_000025h	G12	Postal transfer in cages as complete modules, wafers, IC cases or packages (see [6],[9] section 2.2.5).
2	SW	BOS	80.201.04.1 or 80.201.04.2	Stored on the delivered hardware.
3	SW	NRG™ base[7]	80.201.04.1 or 80.201.04.2	Stored on the delivered hardware. Not part of the TSF
4	SW	Flash Loader	80.201.04.1 or 80.201.04.2	Optional; depending on order.
5	SW	RSA2048 Library	v2.08.006 or v3.03.003 or v3.04.001	Secure download (L251 Library File; object code) via ishare, Optional; depending on order.
6	SW	RSA4096 Library	v2.08.006 or v3.03.003 or v3.04.001	Secure download (L251 Library File; object code) via ishare, Optional; depending on order.
7	SW	EC Library	v2.08.006 or v3.03.003 or v3.04.001	Secure download (L251 Library File; object code) via ishare, Optional; depending on order.
8	SW	Toolbox Library[7]	v2.08.006 or v3.03.003 or v3.04.001	Optional; depending on order. Not part of the TSF
9	SW	Base Library	v2.08.006 or v3.03.003 or v3.04.001	Optional; depending on presence of RSA, EC, and Toolbox.
10	SW	Symmetric Crypto Library (SCL)	v2.13.001	Optional; depending on order.
11	SW	CIPURSE Library (CCL)	v2.00.0005	Optional; depending on order.
12	SW	Hardware Support Library (HSL)	v2.01.6198	Optional; depending on order.
13	SW	NRG™ Library (NRG / NRGS)[7]	v04.03.3431	Optional; depending on order. Not part of the TSF
14	DOC	32-bit Security controller – V07 Hardware Reference Manual	v6.0, 2019-06-13	Secured download (personalized PDF) via ishare.
15	DOC	ARMv7-M Architecture Reference Manual	2010-02-12	Secured download (personalized PDF) via ishare.
16	DOC	Production and personalization 32-bit ARM-based security controller User´s Manual	v3.5 2021-12-17	Secured download (personalized PDF) via ishare.

[7]Not part of the TSF.

No	Type	Identifier	Release	Form of Delivery
17	DOC	SLC37 (65 nm Technology) Programmer´s Reference Manual	V5.3 2022-07-08	Secured download (personalized PDF) via ishare.
18	DOC	32-bit Security Controller – V07 Security Guidelines	v1.01-2761, 2021-07-19	Secured download (personalized PDF) via ishare.
19	DOC	32-bit Security Controller – V07 Errata Sheet	v7.2 2022-01-24	Secured download (personalized PDF) via ishare.
20	DOC	ACL37-Crypto2304T-C65 Asymmetric Crypto Library RSA / ECC / Toolbox 32-bit Security Controller User Interface	v2.08.006 2022-06-20	Secured download (personalized PDF) via ishare,Optional; delivered if RSA, EC, or Toolbox Library is ordered in version v2.08.006.
21	DOC	ACL37-Crypto2304T-C65 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox 32-bit Security Controller User interface manual	v3.03.003 2022-06-20	Secured download (personalized PDF) via ishare,Optional; delivered if RSA, EC, or Toolbox Library is ordered in version v3.03.003.
22	DOC	ACL37-Crypto2304T-C65 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox 32-bit Security Controller User interface manual	v3.04.001 2022-06-20	Secured download (personalized PDF) via ishare,Optional; delivered if RSA, EC, or Toolbox Library is ordered in version v3.04.001.
23	DOC	SLxx7-C65 Hardware Support Library(v2.01.6198)	v1.3 2019-07-05	Secured download (personalized CHM) via ishare.Optional; delivered if HSL is ordered.
24	DOC	SCL37-SCP-v4-C65 Symmetric Crypto Library for SCP-v4 AES/DES/MAC 32-bit Security Controller User interface manual	2021-06-16	Optional; delivered if SCL is ordered.
25	DOC	CIPURSE™ Crypto Library CCL37xCIP v2.00.0005 CIPURSE™ V2 User Interface	V1.4 2018-03-13	Optional; delivered if CCL is ordered.
26	DOC	32-bit Security Controller Crypto@2304T V3 User Manual	V2.1 2022-12-16	Optional; delivered if the Crypto@2304T is available on the TOE.

Table 2: Deliverables of the TOE

The individual TOE hardware is uniquely identified by its identification data. The identification data contains the lot number, the wafer number and the coordinates of the chip on the wafer. Each individual TOE can therefore be traced unambiguously and thus assigned to the entire development and production process.

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 hardware part of the TOE is identified by Common Criteria Identifiers IFX_CCI_000011h, IFX_CCI_00001Bh, IFX_CCI_00001Eh, IFX_CCI_000025h and its

design step G12. Another characteristic of the TOE are the chip identification data, which is accessible via the Generic Chip Identification Mode (GCIM).

In the field, the IC embedded software developer can identify a product in question using the Generic Chip Identification Mode (GCIM) and the user guidance. Furthermore, the IFX-Mailbox area contains further configuration details; this information is provided in [14] 7.10.7. Thereby, the exact and distinct identification of any product with its exact configuration of this TOE is given.

Several bytes of the GCIM include the Common Criteria Certification Identifier. This identifier reflects the name of the TOE and includes the hexadecimal values listed behind the “IFX_CCI_” part of the TOE name. Thus, this TOE is identified by the Common Criteria Certification Identifiers 0x000011, 0x00001B, 0x00001E, and 0x000025. These identifiers are used by the developer only for this TOE and reflect different underlying basic hardware configurations. However, these configurations are achieved only by the means of blocking; the actual hardware is always present and thus identical, but may not be accessible to the user. The design step of the TOE is indicated by byte 11 and 12 of the GCIM. The G12 is coded as 0x060C, where 0x06 stands for G and 0x0C for 12. The GCIM is described in the Hardware Reference Manual [11] section 5.5.

The firmware part of the TOE is identified also via the GCIM: Bytes 31 to 34 contain the firmware identifier 0x 80 20 10 41 or 0x 80 20 10 42. The versions for the individual firmware parts can be received by the mapping giving in the Live Cycle Support Document [24] section 3.1.

The RSA, EC, Toolbox, Base, SCL, HSL, CCL and the NRG™ libraries as separate and optional 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 the Security Target [6],[9] section 10.

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.

The TOE or parts of it are delivered between the following two parties (defined in the Protection Profile [8]).

- IC embedded software developer,
- TOE manufacturer (compromises all roles before TOE delivery),

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).

Respective distribution centers are listed in Appendix B (see end of document).

The individual TOE hardware is uniquely identified by its identification data. Each individual TOE can therefore be traced unambiguously and thus assigned to the entire development and production process.

The hardware part of the TOE is identified by IFX_CCI_000011h, IFX_CCI_00001Bh, IFX_CCI_00001Eh, IFX_CCI_000025h desing step G12.

Another characteristic of the TOE are the chip identification data. These chip identification data is accessible via the Generic Chip Identification Mode (GCIM) (see [11]).

At TOE start-up the so called GCIM can be chosen by applying special signalling in contactless or contact based communication and the TOE outputs then the generic chip identification data (unless another configuration option is chosen). This data contain the firmware identifier accompanied with the certification identifier, the design step and even more tracking information. In combination with [11] the user can identify the data, interpret it and retrieve the TOE versioning information. This information includes also the required mapping of firmware identifier and certification identifier.

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

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, Triple-DES, RSA and EC 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 Chapters 7 and 8 of the Security Target [6],[9].

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 by the TOE-Environment. The following topics are of relevance: The ST includes the following security objective for the IC embedded software developer: OE.Resp-Appl.

The objective OE.Resp-Appl states that the IC embedded software developer shall treat user data (especially keys) of the composite product appropriately. The IC embedded

software developer gets sufficient information on how to protect user data adequately in the security guidelines [15].

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 the Security Target ([6],[9] section 2.2.5) the TOE can be delivered to the composite product manufacturer after phase 3 or after phase 4 (as complete modules, plain wafers, bare dies, in any IC case, or in any type of package). 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 the Production and personalization Manual [13], section 4.

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. The Production and personalization Manual [13], 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 the Production and personalization Manual [13], section 4. 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.

Details can be found in the Security Target [6] and [9], chapter 5.

5. Architectural Information

Detailed information in the TOE architecture is to be found in [6] and [9] section 2.1.

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 developers' testing effort can be summarised in the following aspects:

TOE test configuration: The tests are performed with the TOE, an emulator and a simulator.

Developer's testing approach:

All TSFs and related security mechanisms, subsystems and modules are tested in order to assure complete coverage of all SFRs.

Different classes of tests are performed to test the TOE in a sufficient manner:

- Simulation tests (design verification)
- Qualification test
- Verification test
- Security Evaluation tests
- Production tests

The evaluator's testing effort can be summarised in the way described in the following:

The evaluator's objective regarding this aspect was to test the functionality of the TOE and to verify the developer's test results by repeating developer's tests contained, respectively referenced and to add independent tests.

In the course of the evaluation of the TOE the following classes of tests were carried out:

- Module tests,
- Simulation tests,
- Emulation tests,
- Tests in user mode,
- Tests in test mode,
- Hardware tests,
- Optional library tests.

With these kinds of tests the entire security functionality of the TOE was (functionally) tested by the ITSEF.

The penetration testing was partially performed using the developer's testing environment, partially using the test environment of the evaluation body.

All configurations of the TOE being intended to be covered by the current evaluation were tested.

The overall test result is that no deviations were found between the expected and the actual test results; moreover, no attack scenario with the attack potential high was actually successful.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

- Smartcard IC IFX_CCI_000011h, IFX_CCI_00001Bh, IFX_CCI_00001Eh, IFX_CCI_000025h G12 (Tainan).

Hardware configuration:

Depending on the blocking configuration, a product can have different user available configuration by order or by BPU (please refer to the Security Target [6],[9] section 1.1, for an identification of the components, which can be blocked via BPU).

The Crypto@2304T coprocessor provides functionalities for asymmetric cryptography. If it is not available, the optional software libraries Toolbox, RSA and EC cannot be used, because they depend on the features of this coprocessor.

If the TOE is delivered with a deactivated SCP, it will not provide the hardware based AES and TDES calculations and the SCL cannot be used.

Deselecting a cryptographic coprocessor 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 the functionality.

Firmware configuration:

There are two firmware packages available for the TOE, referenced via the firmware identifiers 80.201.04.1 or 80.201.04.2.

The firmware package consists of different parts:

- Boot Software (BOS),
- Flash Loader, and
- NRG™ base (not part of the TSF).

An overview of the firmware parts is given by the developer in the Security Target [6],[9] section 2.2.2.

Software libraries:

The TOE can be delivered with optional software libraries, as described in Security Target [6],[9] section 1.1 / 2.2.2.

The optional software libraries listed in Table 2 above can be freely combined according to the demands of the user. If one of the RSA, EC, and Toolbox libraries is selected, a Base Library with the same version number is automatically included, as it is required in order to use the aforementioned libraries. If none of these libraries is selected, the Base Library is not included. Furthermore, the RSA Library can be selected in two variants supporting different key lengths, as indicated in the table above. However, the version of EC, RSA and Toolbox libraries cannot be chosen independently.

Based on the library selection the TOE can be delivered with or without the functionality of the RSA, EC, SCL, HSL, CCL, NRG™, and Toolbox libraries. This is considered in the developer documentation and corresponding notes are added where required.

If the user decides not to use the RSA, EC, SCL, HSL, CCL, NRG™, and Toolbox libraries it is not delivered to the user and the accompanying additional specific security functionality as listed in Table 10 is not provided by the TOE. Deselecting the libraries excludes the code implementing functionality, which the user decided not to use. 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 the functionality.

Overall:

In accordance with these configuration possibilities, developer and evaluator tested the TOE in these configurations.

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 specific for the technology was used:

- *AIS 1, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers, Version 14, 2017-10-11, Bundesamt für Sicherheit in der Informationstechnik.*
- *AIS 14, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 7, 2010-08-03, Bundesamt für Sicherheit in der Informationstechnik.*
- *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, Bundesamt für Sicherheit in der Informationstechnik.*
- *AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren*
- *AIS 23, Zusammentragen von Nachweisen der Entwickler, Version 4, 2017-03-15, Bundesamt für Sicherheit in der Informationstechnik.*
- *AIS 25, Version 9, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document*
- *AIS 26, Version 10, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document*
- *AIS 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren*
- *AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema*
- *AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)*
- *AIS 35, Version 2, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies*
- *AIS 36, Version 5, Kompositionsevaluierung including JIL Document and CC Supporting Document*
- *AIS 37, Terminologie und Vorbereitung von Smartcard-Evaluierungen, Version 3, 2010-05-17, Bundesamt für Sicherheit in der Informationstechnik.*
- *AIS 38, Version 2, Reuse of evaluation results*

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 3.2, 2022-11,
- CC Supporting Document, Mandatory Technical Document, Composite product evaluation for Smart Cards and similar devices, Version 1.4, 2015-12, CCDB-2015-12-001,
- CC Supporting Document Guidance, Smartcard Evaluation, Version 2.0, February 2010, CCDB-2010-03-001 and
- CC Supporting Document, Guidance, ETR template for composite evaluation of Smart Cards and similar devices, Version 1.1, 2015-12, CCDB-2015-12-002

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.

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

- All components of the EAL 6 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_FLR.1 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-1025-V4-2021, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the update of the user guidance, on the firmware, software and the vulnerability testing. As a result, guidance documentation has been updated ([16],[23],[17],[18],[19],[13],[14]),

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 6 augmented by ALC_FLR.1

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.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
1	Key Agreement	ECDH (ACL v2.08.006, v3.03.003 and v3.04.001)	[X963], [IEEE_P1363], [ISO_11770-3]	Key sizes corresponding to the used elliptic curves NIST: P-{192, 224, 256, 384, 521}, K-{163, 233, 283, 409}, B-{233, 283, 409} [FIPS186-4]; brainpool: P{160, 192, 224, 256, 320, 384, 512}t1, P{160, 192, 224, 256, 320, 384, 512}r1 [RFC5639]	Key sizes 160, 163, 192: No Key sizes >= 250: Yes
2	Cryptographic Primitive	TDES in modes ECB,CBC, CTR, CFB, (SCP, SCL v2.13.001) CBC-MAC, CBC-MAC-ELB (SCP) PCBC (SCL v2.13.001) CMAC (SCL v2.13.001)	[N867] [N838] [ISO_9797-1] [Schneier] [N838]	|k| = 168 |k| = 112 (for legacy use only, see [N867]),	168: Yes ECB:No CBC,CTR,CFB 168 Yes No Encryption (168): Yes Authenticated Encryption (168): No 112 No 112:No

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
		RMAC (SCL v2.13.001)	[ISO_9797-1]		
3	Cryptographic Primitive	AES in modes ECB, CTR,CBC, CFB, (SCL v2.13.001) CBC-MAC, CBC-MAC-ELB, (SCP) PCBC CMAC (SCL v2.13.001)	[FIPS197] [N838] [ISO_9797-1] [Schneier] [N838]	|k| = 128, 192, 256	ECB: No CTR, CBC, CFB: Yes No Encryption: Yes Authenticated Encryption: No 128: No
4	Cryptographic Primitive	RSA encryption / decryption / signature generation / verification (only modular exponentiation part) (ACL v2.08.006 and v3.03.003 and v3.04.001)	[PKCS-1], [IEEE_P1363]	Modulus length = 1976 – 4224 RSA encryption is only in the scope of the evaluation up to 2112 bits	Yes
5	Cryptographic Primitive	ECDSA signature generation (ACL v2.08.006 and v3.03.003 and v3.04.001)	[X962], [IEEE_P1363], [ISO_14888-3	Key sizes corresponding to the used elliptic curves NIST: P-{192, 224, 256, 384, 521}, K-{163, 233, 283, 409}, B-{233, 283, 409} [FIPS186-4]; brainpool: P{160, 192, 224, 256, 320, 384, 512}t1, P{160, 192, 224, 256, 320, 384, 512}r1 [RFC5639]	Key size 160,163,192: No Key sizes >=250: Yes
6	Cryptographic Primitive	ECDSA signature verification	[X962], [IEEE_P1363], [ISO_14888-3]	Key sizes corresponding to the used elliptic	Key size 160,163,192: No

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
		(ACL v2.08.006 and v3.03.003 and v3.04.001)		curves NIST: P-{192, 224, 256, 384, 521}, K-{163, 233, 283, 409}, B-{233, 283, 409} [FIPS186-4]; brainpool: P{160, 192, 224, 256, 320, 384, 512}t1, P{160, 192, 224, 256, 320, 384, 512}r1 [RFC563]	Key sizes >=250: Yes
7	Random Number Generation	Physical True RNG PTG.2	[AIS31]	N/A	N/A
8	Random Number Generation	Hybrid Random Number Generator PTG.3		N/A	N/A
9	Random Number Generation	Deterministic Random Number Generation DRG.3		N/A	N/A
10	Random Number Generation	Key Stream Generation DRG.2		N/A	N/A
11	Session key agreement	AES	[CIPURSE_Crypto, 5.3 "Session Key Derivation and Authentication Algorithm"]	|k| = 128	Yes
12	Authentication	AES	[CIPURSE_Crypto, 5.3 "Session Key Derivation and Authentication Algorithm"] and [CIPURSE_Crypto, 6.3 "Integrity Protection"]	|k| = 128	Yes
13	Secure Messaging for Integrity	MAC based on AES	[CIPURSE_Crypto, 6.3 "Integrity Protection"]	|k| = 128	No
14	Secure Messaging for Confidentiality	AES	[CIPURSE_Crypto, 6.3 "Confidential Communication"]	|k| = 128	Yes

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
15	Key generation	RSA key Generation using CryptoGeneratePrime (ACL v2.08.006 and v3.03.003)	Proprietary The generated Keys meet [PKCS1, 3.1 / 3.2] [IEEE_P1363, 8.1.3.1]	|K| = 1976 – 4096 (note: TOE supports larger and smaller key sizes, which are generally out of scope of evaluation in BSI scheme)	Yes (only for ACL v.2.08.006 and v3.03.003)
16	Key generation	RSA key Generation using CryptoGeneratePrimeMask (ACL v2.08.006)	Proprietary The generated Keys meet [PKCS1, 3.1 / 3.2.] [IEEE_P1363, 8.1.3.1]	|K| = 1976 – 4096	No statement
17	Key generation	RSA key Generation using CryptoRsaKeyGenMask_PQ (ACL v3.33.003 and v3.04.001)	The generated keys meet [PKCS #1, 3.1 / 3.2] and [IEEE_P1363, 8.1.3.1]	|K| = 1976 – 4096	yes
18	Key generation	EC using ECC_ECDSAKeyGen (ACL v2.08.006)	[X962, A 4.3] [ISO_14888-3, 6.4.2] [IEEE_P1363, A.16.9]	|k| = 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512, 521 bits	Key sizes < 250: no Key sizes >= 250 : yes
19	Key generation	EC using ECC_ECDSAKeyGenMask (ACL v2.08.006 and v3.03.003 and v3.04.001)	[X962, A 4.3] [ISO_14888-3, 6.4.2] [IEEE_P1363, A.16.9]	|k| = 160, 163, 192, 224, 233, 256, 283, 320, 384, 409, 512, 521 bits	Key sizes < 250: no Key sizes >= 250 : yes

Table 3: TOE cryptographic functionality

For the Cryptographic Functionality

- CryptoGeneratePrimeMask() which might be used in conjunction with RSA Key Generation in ACL v2.08.006,

no statement on the respective cryptographic strength can be given.

Furthermore, regarding the additional notes “Note to DRG.2.2” and “Note to DRG.2.3” in [6] and [9] (section 7.1.1.5) for FCS_RNG.1/KSG, no statement is given in this Certification Report.

The Flash Loader's cryptographic strength was also 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 [25].

Reference of Legislatives and Standards quoted above:

[N867] NIST SP800-67 Revision 1, Recommendation for Triple Data Encryption Algorithm (TDEA) Block Cipher, 2012-01, National Institute of Standards and Technology (NIST)

[N838] NIST SP800-38A, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, 2001, National Institute of Standards and Technology (NIST)

[ISO_9797-1] Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher, 2011-03, ISO/IEC

[Schneier] Applied Cryptography, Second Edition, B. Schneier, John Wiley & Sons, 1996

[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)

[PKCS1] PKCS #1 v2.2: RSA Cryptography Standard, 2012-10, RSA Laboratories

[IEEE_P1363] IEEE P1363. Standard specifications for public key cryptography. IEEE, 2000

[X962] American National Standard for Financial Services, ANS X9.62–2005, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), 2005-11, American National Standard Institute

[ISO_14888-3] Information technology - Security techniques – Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms, 2006-11, ISO/IEC

[AIS31] Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 31, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3, 2013-05-15

[X963] American National Standard for Financial Services, ANS X9.63–2011, Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve Cryptography, 2011-12, American National Standard Institute

[ISO_11770-3] Information technology - Security techniques - Key management - Part 3: Mechanisms using asymmetric techniques, 2008-07, ISO/IEC

[FIPS186-4] Federal Information Processing Standards Publication FIPS PUB 186-4, Digital Signature Standard (DSS), July 2013, U.S. department of Commerce / National Institute of Standards and Technology (NIST)

[RFC5639] RFC 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, 2010-03

[Achterbahn] ACHTERBAHN-128/80, 2006-06-30, Infineon Technologies AG

[CIPURSE_Crypto] The CIPURSE™V2 Specification Cryptographic Protocol, Revision 1.0, 2012-09-28, Infineon Technologies AG

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.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process, too.

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 [Auswahl im Einzelfall: IC Dedicated Support Software and/or 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].

At the point in time when evaluation and certification results are reused there might be an update of the document "ETR for composite evaluation" available. Therefore, the certified products list on the BSI website has to be checked for latest information on reassessments, recertifications or maintenance result available for the product.

The TOE is delivered to the composite product manufacturer and to the security IC embedded software developer. The actual end-consumer obtains the TOE from the composite product issuer together with the application, which runs on the TOE.

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 [15],[11],[14],[23],[16],[21],[17], [18],[19],[22] 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 [13] have to be considered.

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. Regulation specific aspects (eIDAS, QES)

None.

13. Definitions

13.1. 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

13.2. 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.

14. 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
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017, https://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 TOE[8] 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/zertifizierungsreporte

[6] Security Target BSI-DSZ-CC-1025-V5-2023, Version 1.6, 2022-12-17, Confidential Security Target IFX_CCI_000011h IFX_CCI_00001Bh IFX_CCI_00001Eh IFX_CCI_000025h G12, Infineon Technologies AG (confidential document)

[7] Evaluation Technical Report, Version 3, 2023-05-11, EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY), TÜV Informationstechnik GmbH, (confidential document)

[8] specifically see Chapter 9.1.

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

[9] Security Target BSI-DSZ-CC-1025-V5-2023, Version 1.6, 2022-12-17, Public Security Target IFX_CCI_000011h IFX_CCI_00001Bh IFX_CCI_00001Eh IFX_CCI_000025h G12, Infineon Technologies AG (sanitised public document)

[10] ETR for composite evaluation according to AIS 36 for the Product IFX_CCI_000011h IFX_CCI_00001Bh IFX_CCI_00001Eh IFX_CCI_000025h G12, Version 1, 2023-05-11, Evaluation Technical for Composite Evaluation (ETR COMP) for the IFX_CCI_000011h, IFX_CCI_00001Bh, IFX_CCI_00001Eh, IFX_CCI_000025h G12, version 3, 2023-05-11, TÜV Informationstechnik GmbH (confidential document)

[11] 32-bit Security controller – V07 Hardware Reference Manual, v6.0, 2019- 06-13, Infineon Technologies AG

[12] ARMv7-M Architecture Reference Manual, 2010-02-12, ARM

[13] Production and personalization 32-bit ARM-based security controller User´s Manual, v3.5, 2021-12-17, Infineon Technologies AG

[14] Programmer's Reference Manual, Version 5.3, 2022-07-08, SLC37 (65-nm) Security Controller Programmer´s Reference Manual, Infineon Technologies AG

[15] 32-bit Security Controller – V07 Security Guidelines, v1.01-2761, 2021-07-19, Infineon Technologies AG

[16] 32-bit Security Controller – V07 Errata Sheet, v7.2, 2022-01-24, Infineon Technologies AG

[17] ACL37-Crypto2304T-C65 Asymmetric Crypto Library RSA / ECC / Toolbox 32-bit Security Controller User Interface, 2022-06-20, v2.08.006, Infineon Technologies AG

[18] ACL37-Crypto2304T-C65 Asymmetric Crypto Library RSA/ECC/Toolbox 32-bit Security Controller User interface manual, 2022-06-20, v3.03.003, Infineon Technologies AG

[19] ACL37-Crypto2304T-C65 Asymmetric Crypto Library RSA/ECC/Toolbox 32-bit Security Controller User interface manual, 2022-06-20, v3.04.001, Infineon Technologies AG

[20] SLxx7-C65 Hardware Support Library (v2.01.6198), v1.3, 2019-07-05, SLxx7-C65 Hardware Support Library Low Level Documentation,SLxx7–C65 Hardware Support Library (v2.01.6198), Infineon Technologies AG

[21] SCL37-SCP-v4-C65 Symmetric Crypto Library for SCP-v4 AES/DES/MAC 32-bit Security Controller User interface manual, 2021-06-16, SCL37-SCP-v4-C65 Symmetric Crypto Library for SCP-v4 AES/DES/MAC 32-bit Security Controller User interface manual (v2.13.001),Infineon Technologies AG

[22] CIPURSE™ Crypto Library CCL37xCIP v2.00.0005 CIPURSE™ V2 User Interface, 1.4, 2018-03-13, CIPURSE™ Crypto Library CCL37xCIP v2.00.0005 CIPURSE™ V2 User Interface (v2.00.005),Infineon Technologies AG

[23] 32-bit Security Controller Crypto@2304T V3 User Manual, 2.1, 2022-12-16, Infineon Technologies AG

[24] Life Cycle Support IFX_CCI_11h including optional Software Libraries and Flash Loader according Package 1 and Package 2, v0.8, 2022-09-21,Infineon Technologies AG

[25] SINGLE EVALUATION REPORT ADDENDUM to ETR-Part ASE Cryptographic Standards Compliance Verification, v1 , 2022-09-28, TÜV Informationstechnik

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 https://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-1025-V5-2023

Evaluation results regarding development and production environment

The IT product Infineon Technologies AG Smartcard IC IFX_CCI_000011h, 00001Bh, 00001Eh,000025h, design step G12 with optional libraries and with specific dedicated software (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 13 July 2023, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.5, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.3)

Besides the production and development sites, the relevant TOE distribution centers are as follows:

Site ID	Company name and address
DHL Singapore	DHL Supply Chain Singapore Pte Ltd., Advanced Regional Center Tampines LogisPark 1 Greenwich Drive Singapore 533865
KWE Shanghai	KWE Kintetsu World Express (China) Co., Ltd. Shanghai Pudong Airport Pilot Free Trade Zone No. 530 Zheng Ding Road Shanghai, P.R. China
K&N Großostheim	Kühne & Nagel Stockstädter Strasse 10 63762 Großostheim Germany
Infineon Morgan Hill	Infineon Technologies North America Corp. 18275 Serene Drive Morgan Hill, CA 95037 USA

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