Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1079-V5-2024

for

Infineon Security Controller IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step G12

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-1079-V5-2024 (*)

Smartcard Controller

Infineon Security Controller IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step G12

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, 8 October 2024

For the Federal Office for Information Security

Matthias Intemann L.S.
Head of Section

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

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 Security Controller IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step G12, has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1079-V4-2023. Specific results from the evaluation process BSI-DSZ-CC-1079-V4-2023 were re-used.

The evaluation of the product Infineon Security Controller IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step G12, was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 7 October 2024. 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 8 October 2024 is valid until 12 July 2028. Validity can be re-newed by re-certification.

[5] Information Technology Security Evaluation Facility

The owner of the certificate is obliged:

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 Security Controller IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step G12 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_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch Design Step G12, including optional software libraries and dedicated firmware.

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 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 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.
SF_PS	Protection against Snooping: The TOE is equipped with various countermeasures against snooping. Amongst other countermeasures, the TOE implements complete encryption of the memories in combination with a complex key management, topological measures and dynamic masking of the peripheral bus.
SF_PMA	Protection against Modifying Attacks: This TOE is equipped with various countermeasures against modifying attacks. Amongst other countermeasures, the TOE implements, error detection and correction in the memories, program flow protection and backwards calculation in the SCP.
SF_PLA	Protection against Logical Attacks: The memory access control of the TOE uses a memory management unit (MMU) to control the access to the available physical memory by using virtual memory addresses and to segregate the code and data to a privilege level model. The MMU controls the address permissions of up to seven privileged levels and gives the software the possibility to define different access rights.

TOE Security Functionality	Addressed issue
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. Furthermore, a hash crypto library provides SHA-1 and SHA-2 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 4.1.2 . 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 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 Security Controller IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step G12

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch	G12	Postal transfer in locked cages or metal boxes as plain wafers, bare dies, complete modules, IC cases, with or without antenna mounting, with or without inlay mounting, or in any package
2.	FW	Boot Software (BOS)	80.102.06.0 or 80.102.06.1	Stored on the delivered hardware
3.	FW	Flash Loader (FL) (optional)	80.102.06.0 or 80.102.06.1	Stored on the delivered hardware

No	Type	Identifier	Release	Form of Delivery
4.	FW	NRG ROM part (not part of the TSF)	80.102.06.0 or 80.102.06.1	Stored on the delivered hardware
5.	FW	Radio Frequency Application Interface (RFAPI) (not part of the TSF)	80.102.06.0 or 80.102.06.1	Stored on the delivered hardware
6.	FW	Resource Management System (RMS)	80.102.06.0 or 80.102.06.1	Stored on the delivered hardware
7.	SW	RSA2048 Libraries (optional)	v2.07.003, v2.08.007, or v2.09.002	Secure download (precompiled object code – L251 file) via ishare.
8.	SW	RSA4096 Libraries (optional)	v2.07.003, v2.08.007, or v2.09.002	Secure download (precompiled object code – L251 file) via ishare.
9.	SW	EC Libraries (optional)	v2.07.003, v2.08.007, or v2.09.002	Secure download (precompiled object code – L251 file) via ishare.
10.	SW	Toolbox Libraries (optional, not part of the TSF)	v2.07.003, v2.08.007, or v2.09.002	Secure download (precompiled object code – L251 file) via ishare.
11.	SW	Base Libraries (optional)	v2.07.003, v2.08.007, or v2.09.002	Secure download (precompiled object code – L251 file) via ishare.
12.	SW	Symmetric Cryptographic Libraries (SCL) (optional)	v2.04.002 or v2.13.001	Secure download (precompiled object code – L251 file) via ishare.
13.	SW	Hash Cryptographic Library (HCL) (optional)	v1.12.001	Secure download (precompiled object code – L251 file) via ishare.
14.	SW	CIPURSE™ library (CCL) (optional)	v02.00.0004	Secure download (precompiled object code – L251 file) via ishare.
15.	SW	Hardware Support Libraries (HSL) (optional)	v03.11.8339 or v03.12.8812	Secure download (precompiled object code – L251 file) via ishare.
16.	SW	NRG Software Library (NRGS) (optional, not part of the TSF)	v02.03.3446	Secure download (precompiled object code – L251 file) via ishare.
17	DOC	*16-bit Security Controller Family – V05, Hardware Reference Manual*	5.0 2019-06-14	Secured download (personalized PDF) via ishare or on demand via encrypted email.
18	DOC	*Production and Personalization, 16-bit Security Controller*	3.6 2019-06-24	Secured download (personalized PDF) via ishare or on demand via encrypted email.
19	DOC	*16-bit Security Controller, 65nm-Technology, Programmer's Reference Manual*	9.14 2019-12-03	Secured download (personalized PDF) via ishare or on demand via encrypted email.
20	DOC	*16-bit Security Controller – V05, Security Guidelines*	1.01-2597 2020-08-20	Secured download (personalized PDF) via ishare or on demand via encrypted email.
21	DOC	*16-bit Security Controller – V05, Errata Sheet*	10.0 2021-02-25	Secured download (personalized PDF) via ishare or on demand via encrypted email.

No	Type	Identifier	Release	Form of Delivery
22	DOC	*CL52 Asymmetric Crypto Library for Crypto@2304T, RSA/ECC/Toolbox, 16-bit Security Controller, User Interface, Version 2.07.003* (optional)	2.07.003 2024-08-26	Secured download (personalized PDF) via ishare or on demand via encrypted email.
23	DOC	*ACL52-Crypto2304T-C65 Asymmetric Crypto Library, RSA / ECC / Toolbox, 16-bit Security Controller, User Interface, Version 2.08.007* (optional)	2.08.007 2024-08-26	Secured download (personalized PDF) via ishare or on demand via encrypted email.
24	DOC	*ACL52-Crypto2304T-C65 Asymmetric Crypto Library, RSA / ECC / Toolbox, 16-bit Security Controller, User Interface, Version 2.09.002* (optional)	2.09.002 2024-06-27	Secured download (personalized PDF) via ishare or on demand via encrypted email.
25	DOC	*Hardware Support Library for SLCx2 Version 03.12.8812* (optional)	1.1 2019-07-08	Secured download (personalized PDF) via ishare or on demand via encrypted email.
26	DOC	*Hardware Support Library for SLCx2 Version 03.11.8839* (optional)	1.0 2018-07-12	Secured download (personalized PDF) via ishare or on demand via encrypted email.
27	DOC	*SCL52-SCP-v4-C65 Symmetric Crypto Library for SCP-v4 DES / AES 16-bit Security Controller, User Interface, Version 2.04.002* (optional)	2.04.002 2018-05-22	Secured download (personalized PDF) via ishare or on demand via encrypted email.
28	DOC	*SCL52-SCP-v4-C65 Symmetric Cryptographic Library for SCP-v4 AES/DES/MAC, 16-bit Security Controller, User Interface, Version 2.13.001* (optional)	2.13.001 2020-11-05	Secured download (personalized PDF) via ishare or on demand via encrypted email.
29	DOC	*HCL52-CPU-C65 Hash Crypto Library for CPU SHA 16-bit Security Controller, User interface manual* (optional)	1.12.001 2020-01-04	Secured download (personalized PDF) via ishare or on demand via encrypted email.
30	DOC	*CIPURSE™ Crypto Library, CCLX2xCIP v02.00.0004, CIPURSE™ V2,Compliant to OSPT™ Alliance CIPURSE™ V2 Cryptographic Protocol, User Interface* (optional)	1.6 2018-02-02	Secured download (personalized PDF) via ishare or on demand via encrypted email.
31	DOC	*16-bit Security Controller, Crypto@2304T V3, User Manual* (optional)	2.0 2024-06-21	Secured download (personalized PDF) via ishare or on demand via encrypted email.

Table 2: Deliverables of the TOE

The hardware part of the TOE is identified by its Common Criteria Identifiers (CCI) IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch and the design step G12. 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:

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 RMS function IFX_ConfigurationRead can be used to retrieve further information. Thereby, the exact and distinct identification of any product with its exact configuration of this TOE is given.

The 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, and the CCI. The interpretation of the chip identification data is described in the Hardware Reference Manual [12] chapter 6.5.

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.

According to the PP [8], chapter 1.2.3 the TOE or parts of it are delivered between the following three parties:

- IC Embedded Software Developer,
- TOE Manufacturer (compromises all roles before TOE delivery),
- Composite Product Manufacturer (compromises all roles after TOE delivery except the end consumer).

Therefore, three different delivery procedures have to be taken into consideration:

1. Delivery of the IC dedicated software components (IC dedicated SW, guidance) from the TOE Manufacturer to the IC Embedded Software Developer.
2. Delivery of the IC Embedded Software (ROM / Flash data, initialisation and prepersonalisation data) from the IC Embedded Software Developer to the TOE Manufacturer.
3. 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),
- KWE Shanghai,
- K&N Großostheim (Distribution Center Europe).

3. Security Policy

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 different random number generators.

The RSA library is used to provide a high-level interface to RSA (Rivest, Shamir, Adleman) cryptography implemented on the hardware component Crypto@2304T and includes countermeasures against SPA, DPA, and DFA attacks. The EC library is used to provide a high-level interface to Elliptic Curve cryptography implemented on the hardware component Crypto@2304T and includes countermeasures against SPA, DPA and DFA attacks. The optional Hash Crypto Library provides a high-level interface for performing cryptographic hash functions and includes countermeasures against SPA, DPA, and DFA attacks.

Furthermore, the TOE also contains the optional CIPURSE Cryptographic Library (CCL), which can be used to implement a CIPURSE V2 conformant protocol in the IC embedded software.

Besides that, the TOE can come with the optional Hardware Support Library (HSL), which provides a simplified interface for NVM management and provides the possibility to write tearing safe into the NVM.

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 Chapter 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: OE.Resp-Appl, OE.Process-Sec-IC, OE.Lim_Block_Loader, OE.Loader_Usage, and OE.TOE_Auth.

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 [6],[9] 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],[9] chapter 2.2.5, 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 [13] chapter 3.2.2.

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. [13], chapter 3 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 [13], chapter 3.5.3. 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.

Details can be found in the Security Target [6] and [9], chapter 5.3.

5. Architectural Information

This ETR abbreviates the TOE as IFX_CCI_00000Fh for the sake of a better readability.

The TOE provides a real 16-bit CPU-architecture and is compatible to the Intel 80251 architecture. The major components of the core system are the two CPUs (Central Processing Units), the MMU (Memory Management Unit), and the MED (Memory Encryption/Decryption Unit). The dual interface controller is able to communicate using either the contact based or the contactless interface.

This TOE is intended to be used in smart cards for particular security relevant applications and as a 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.

Further, more detailed information is readily available in the Security Target [6] and [9].

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,
- Verification Tests,
- Security Evaluation Test,
- Production Tests.

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

The evaluator was able to repeat the tests of the developer by 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 that 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

This certification covers the following configurations of the TOE:

- Smartcard IC IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch G12 (Tainan).

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

As stated and detailed in the ETR [7], developer and evaluator tested the TOE in those configurations/identifiers in which the TOE is delivered and which are described in the Security Target [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 specific for the technology was used:

- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 1, Durchführungder Ortsbesichtigung in der Entwicklungsumgebung des Herstellers, Version 14, 2017-10-11,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 14, Anforderungenan Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nachCC (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 20,Funktionalitätsklassen und Evaluationsmethodologie für

deterministischeZufallszahlengeneratoren, Version 3, 2013-05-15, Herausgeber: Zertifizierungsstelle des BSI im Rahmen des Zertifizierungsschemas,

- 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,
- Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 32, CCInterpretationen im deutschen Zertifizierungsschema, Version 7, 2011-06-08,
- 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,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 37, Terminologie und Vorbereitung von Smartcard-Evaluierungen, Version 3, 2010-05-17,
- Application Notes and Interpretation of the Scheme (AIS) – AIS 38, Reuse of evaluation results, Version 2, 2007-09-28,
- Application Notes and Interpretation of the Scheme (AIS) – AIS 41, Guidelines for Pps and STs, Version 2, 2011-01-31,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 46, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren, Version 3, 2013-12-04,
- 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 3.2.1, 2024-02 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.

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 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-1079-V4-2023, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on penetration test updates, the update of the ACL and Crypto@2304T user guidance. As a result, guidance documentation has been updated ([17], [18], [19],[26]).

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, release 2022-01' (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.

Note in particular:

- The RSA encryption is only in the scope of the evaluation up to 2112 bits (RSA decryption up to 4224bits)

No.	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
Cryptographic Primitive				
1	TDES in	[NIST SP800-67_2017], [ISO_18033-3]	|k| = 112	
	ECB mode (SCP, SCL v2.04.002, v2.13.001),	[NIST SP800-38A]		no
	CBC mode (SCP, SCL v2.04.002, v2.13.001),	[NIST SP800-38A]		no
	CTR mode (SCL v2.04.002, v2.13.001) ,	[ISO_9797-1]		no
	CFB mode (SCL v2.04.002, v2.13.001),	[ISO_9797-1]		no
	CBC-MAC (SCP),	[ISO_9797-1]		no
	CBC-MAC-ELB (SCP),	[ISO_9797-1]		no
	PCBC (SCL v2.04.002, v2.13.001)	[Schneier]		no

No.	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
	BLD (blinding) and Recrypt (SCP)	proprietary implementation		no
	CMAC (SCL v2.04.002, v2.13.001)	[NIST SP800-38B]		no
	Retail-MAC (SCL v2.13.001)	[ISO_9797-1]		no
2.	TDES in	[NIST SP800-67_2017],	|k| = 168	
	ECB mode (SCP, SCL v2.04.002, v2.13.001),	[NIST SP800-38A]		no
	CBC mode (SCP, SCL v2.04.002, v2.13.001),	[NIST SP800-38A]		yes
	CTR mode (SCL v2.04.002, v2.13.001),	[NIST SP800-38A]		yes
	CFB mode (SCL v2.04.002, v2.13.001),	[NIST SP800-38A]		yes
	CBC-MAC (SCP),	[ISO_9797-1]		
	CBC-MAC-ELB (SCP),	[ISO_9797-1]		
	PCBC (SCL v2.04.002, v2.13.001)	[Schneier]		yes
	BLD (blinding) and Recrypt (SCP)	proprietary implementation		no
	CMAC (SCL v2.04.002, v2.13.001)	[NIST SP800-38B]		yes

No.	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
3.	AES in,	|k| = 128, 192, 256		-
	ECB mode (SCP, SCL v2.04.002, v2.13.001),	[NIST SP800-38A]		no
	CBC mode (SCP, SCL v2.04.002, v2.13.001),	[NIST SP800-38A]		yes
	CTR mode (SCL v2.04.002, v2.13.001),	[ISO_9797-1]		yes
	CFB mode (SCL v2.04.002, v2.13.001),	[ISO_9797-1]		yes
	CBC-MAC (SCP)	[ISO_9797-1]		no
	CBC-MAC-ELB (SCP)	[ISO_9797-1]		no
	PCBC (SCL v2.04.002, v2.13.001)	[Schneier]		Encryption: Yes Authenticated Encryption: No
	BLD (blinding) and Recrypt (SCP)	proprietary imple-mentation		no
	CMAC (SCL v2.04.002, v2.13.001)	[NIST SP800-38B]		yes

No.	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
4.	RSA encryption / decryption / signature generation / verification (only modular exponentiation part) (ACL v2.07.003, v2.08.007, and v2.09.002)	[PKCS-1], [IEEE_P1363]	Modulus length = 1976 – 4224 RSA encryption is only in the scope of the evaluation up to 2112 bits (RSA decryption up to 4224bits). Please note that the RSA library supports key lengths from 65 to 4224 bits; however, key lengths below 1976 bits are not included in the certificate.	yes
5.	ECDSA signature generation (ACL v2.07.003, v2.08.007, and v2.09.002)	[ANS X9.62], [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 sizes 160, 163, 192: no Key sizes >= 224 : yes
6.	ECDSA signature verification (ACL v2.07.003, v2.08.007, and v2.09.002)	[ANS X9.62], [IEEE_P1363], [ISO_14888-3]		Key sizes 160, 163, 192: no Key sizes >= 224 : yes
7.	Physical True RNG PTG.2	[AIS31]	N/A	n/a
8.	Hybrid Random Number Generator PTG.3	[AIS31]	N/A	n/a
9.	Deterministic Random Number Generation DRG.3	[AIS31]	N/A	n/a
10.	Key Stream Generation DRG.2	[AIS31]	N/A	n/a

No.	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
Key agreement				
11.	ECDH (ACL v2.07.003, v2.08.007, and v2.09.002)	[ANS X9.63], [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 sizes 160, 163, 192: no Key sizes >= 224 : yes
12.	CIPURSE™ Session Key Agreement (using AES) (CCL v02.00.0004)	[CIPURSE-1, 5.3], [FIPS197], [NIST SP800-38A]	|k| = 128	Yes

No.	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
Key generation				
13.	RSA key generation using CryptoGeneratePrime (ACL v2.09.002)	Proprietary The generated keys meet [PKCS #1, 3.1 / 3.2] and [IEEE_P1363, 8.1.3.1].	1976 – 4096 (note: TOE supports larger and smaller key sizes, which are generally out of scope of evaluation in BSI scheme)	yes
14.	EC key generation using ECC_ECDSAKeyGen (ACL v2.07.003, v2.08.007 and v2.09.002)	[ANS X9.62, A 4.3] [ISO_14888-3, 6.4.2] [IEEE_P1363, A.16.9]	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 >= 224 : yes
15.	EC key generation using ECC_ECDSAKeyGenMask (ACL v2.07.003, v2.08.007, and v2.09.002)	[ANS X9.62, A 4.3] [ISO_14888-3, 6.4.2] [IEEE_P1363, A.16.9]	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 >= 224 : yes
Authentication				
16.	CIPURSE™ Authentication (using AES) (CCL v02.00.0004)	[CIPURSE-1, 5.3 / 6.3], [FIPS197], [NIST SP800-38A]	|k| = 128	yes
Confidential communication				
17.	CIPURSE™ Secure Messaging for Confidentiality (using AES) (CCL v02.00.0004)	[CIPURSE-1, 6.4], [FIPS197], [NIST SP800-38A]	|k| = 128	yes

No.	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
Integrity protected communication				
18.	CIPURSE™ Secure Messaging for Integrity (using AES) (CCL v02.00.0004)	[CIPURSE-1, 6.3], [CIPURSE-2, P.2], [FIPS197], [NIST SP800-38A]	|k| = 128	no
Digest computation				
19.	SHA-1 (HCL v1.12.001)	[FIPS180-4]	N/A	n/a (keyless operation)
20.	SHA-2 (HCL v1.12.001)	[FIPS180-4]	N/A	n/a (keyless operation)

Table 3: TOE cryptographic functionality

The Flash Loader's 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 [27].

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 BlockCipher 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.

[ANS X9.62] 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), November 16, 2005, American National Standards Institute.

[ANS X9.63] American National Standard for Financial Services X9.63-2011, Public Key Cryptography for the Financial Services Industry: Key Agreement and key transport using Elliptic Curve Cryptography, 2011-12-21, American National Standards Institute.

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

[ISO_11770-3] International Standard ISO/IEC 11770-3: 2008, Technical Corrigendum 1, Information technology - Security techniques – Key management Part 3: Mechanisms using asymmetric techniques, 2009-09-15.

[CIPURSE-1] CIPURSE™ V2 Cryptographic Protocol issued by OSPT™ Alliance,2012-09-28

[CIPURSE-2] CIPURSE™ V2 Cryptographic Protocol issued by OSPT™ Alliance, 2014-09-18 (with errata and precision list)

[ISO_18033-3] ISO/IEC 18033-3: Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers, 2005.

[ISO_9797-1] Information technology – Security techniques – Message Authentication Codes (MACs), Part 1: Mechanisms using a block cipher, 2011-03-01, ISO/IEC.

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

[PKCS-1] PKCS #1: RSA Cryptography Standard, Version 2.2, 2012-10-27, RSA Cryptographic Standard, RSA Laboratories.

[ISO_14888-3] International Standard ISO/IEC 14888-3: 2006, Technical Corrigendum 2: Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms, 2009-02-15.

[ANS X9.62] 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), November 16, 2005, American National Standards Institute.

[ANS X9.63] American National Standard for Financial Services X9.63-2011, Public Key Cryptography for the Financial Services Industry: Key Agreement and key transport using Elliptic Curve Cryptography, 2011-12-21, American National Standards Institute.

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 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.

Furthermore:

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 that 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], [12], [14], [26], [16], [22],[23], [18], [19], [17], [24], [20], [21], and [25] have to be considered.

The composite product manufacturer receives all necessary recommendations and hints todevelop his software in form of the delivered documentation.

All security hints described in [13] have to be considered.

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

- The security IC embedded software developer can deliver his software either to Infineon to let them implement it in the TOE (in the Flash memory) or to the composite product manufacturer to let him download the software in the Flash memory.
- The delivery procedure from the security IC embedded software developer to the composite product manufacturer is not part of this evaluation and a secure delivery isrequired.

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

3DES / TDES	Triple DES
ACL	Asymmetric Cryptographic Library
AES	Advanced Encryption Standard
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
CMAC	Cipher-bases Message Authentication Code
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
DES	Data Encryption Standard
DRNG	Deterministic RNG
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HSL	Hardware Support Library
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
MED	Memory Encryption/Decryption Unit
MMU	Memory Management Unit
NVM	Non Volatile Memory
PP	Protection Profile
PRNG	Pseudo Random Number Generator
PTRNG	Physical True Random Number Generator
RMS	Resource Management System
RNG	Random Number Generator
ROM	Read-Only Memory
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[7] 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-1079-V5-2024, Version 2.5, 2024-09-12, Confidential Security Target Common Criteria v3.1 – EAL6 augmented / EAL6+ IFX_CCI_00000Fh IFX_CCI_000010h IFX_CCI_000026h IFX_CCI_000027h IFX_CCI_000028h IFX_CCI_000029h IFX_CCI_00002Ah IFX_CCI_00002Bh IFX_CCI_00002Ch G12, Infineon Technologies AG (confidential document)

[7] Evaluation Technical Report, Version 2, 2023-09-20, EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY), TÜV Informationstechnik (confidential document)

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

[7] See section 9.1 for detailed list of used AIS

[9] Security Target Lite BSI-DSZ-CC-1079-V5-2024, Version 2.5, 2024-09-12, Public Security Target Common Criteria v3.1 – EAL6 augmented / EAL6+ IFX_CCI_00000Fh IFX_CCI_000010h IFX_CCI_000026h IFX_CCI_000027h IFX_CCI_000028h IFX_CCI_000029h IFX_CCI_00002Ah IFX_CCI_00002Bh IFX_CCI_00002Ch G12, Infineon Technologies AG (sanitised public document)

[10] ETR for composite evaluation according to AIS 36 for the Product BSI-DSZ-CC-1079-V4-2022, Version 3, 2023-06-26, Evaluation Technical for Composite Evaluation (ETR COMP) for the IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch G12, (confidential document), TÜV Informationstechnik GmbH

and

Addendum to ETR for composite Version 2, 2024-09-20, TÜV Informationstechnik GmbH (confidential document)

[11] Configuration list for the TOE, 0.9, 2024-07-03, “Life Cycle Support Configuration Management for Common Criteria with Evaluation Assurance Level EAL6 augmented (EAL6+) IFX_CCI_00000Fh with options Including optional Software Libraries Flash Loader – 3x ACL – 2xHSL –2x SCL HCL - – CCL – NRG”, Infineon Technologies AG (confidential document)

[12] 16-bit Security Controller Family – V05, Hardware Reference Manual, Version 5.0, 2019-06-14, Infineon Technologies AG

[13] Production and Personalization, 16-bit Security Controller, Version 3.6, 2019-06-24, Infineon Technologies AG

[14] 16-bit Security Controller, 65nm-Technology, Programmer’s Reference Manual,Version 9.14, 2019-12-03, Infineon Technologies AG

[15] 16-bit Security Controller – V05, Security Guidelines, Version 1.01-2597, 2020-08-20, Infineon Technologies AG

[16] 16-bit Security Controller – V05, Errata Sheet, Version 10.0, 2021-02-25, Infineon Technologies AG

[17] ACL52 Asymmetric Crypto Library for Crypto@2304T, RSA/ECC/Toolbox, 16-bit Security Controller, User Interface, Version 2.07.003, 2024-08-26, Infineon Technologies AG

[18] ACL52-Crypto2304T-C65 Asymmetric Crypto Library, RSA / ECC / Toolbox, 16-bit Security Controller, User Interface, Version 2.08.007, 2024-08-26, Infineon Technologies AG

[19] ACL52-Crypto2304T-C65 Asymmetric Crypto Library, RSA / ECC / Toolbox, 16-bit Security Controller, User Interface, Version 2.09.002, 2024-06-27, Infineon Technologies AG

[20] Hardware Support Library for SLCx2 Version 03.12.8812, 2019-07-08, Version 1.1, Infineon Technologies AG

[21] Hardware Support Library for SLCx2 Version 03.11.8339, Version 1.0,2018-07-12, Version 1.0, Infineon Technologies AG

[22] SCL52-SCP-v4-C65 Symmetric Crypto Library for SCP-v4 DES / AES 16-bit Security Controller, User Interface, Version 2.04.002, 2018-05-22, InfineonTechnologies AG

[23] SCL52-SCP-v4-C65 Symmetric Cryptographic Library for SCP-v4 AES/DES/MAC, 16-bit Security Controller, User Interface, Version 2.13.001, 2020-11-05, Infineon Technologies AG

[24] HCL52-CPU-C65 Hash Crypto Library for CPU SHA 16-bit Security Controller, User interface manual, Version 1.12.001, 2020-01-14, Infineon Technologies AG

[25] CIPURSE™ Crypto Library, CCLX2xCIP v02.00.0004, CIPURSE™ V2,Compliant to OSPT™ Alliance CIPURSE™ V2 Cryptographic Protocol, User Interface, Version 1.6, 2018-02-02, Infineon Technologies AG

[26] 16-bit Security Controller, Crypto@2304T V3, User Manual, Version 2, 2024-06-21, Infineon Technologies AG

[27] Cryptographic Standards Compliance Verification, Version 1, 2024-09-12, 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 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-1079-V5-2024

Evaluation results regarding development and production environment

The IT product Infineon Security Controller IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step G12 (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 8 October 2024, 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 listed below:

Site ID	Company name and address
DHL Singapore	DHL Supply Chain Singapore Pte Ltd., Advanced Regional Center Tampines LogisPark 1 Greenwich Drive Singapore 533865
K&N Großostheim	Kühne & Nagel Stockstädter Strasse 10 63762 Großostheim Germany
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

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.