Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1229-2024

for

Infineon Security Controller IFX_CCI_00007Dh, IFX_CCI_00007Eh, IFX_CCI_00007Fh, design step H11 with firmware version 80.506.04.1, optional CryptoSuite version 4.06.002, optional HSL version 04.05.0030, optional UMSLC version 02.01.0040, optional NRG™ version 06.10.0003 and user guidance documents

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-1229-2024 (*)

Smartcard Controller

Infineon Security Controller IFX_CCI_00007Dh, IFX_CCI_00007Eh, IFX_CCI_00007Fh, design step H11 with firmware version 80.506.04.1, optional CryptoSuite version 4.06.002, optional HSL version 04.05.0030, optional UMSLC version 02.01.0040, optional NRG™ version 06.10.0003 and user guidance documents

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 Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 6 augmented by ALC_FLR.1
valid until:	24 January 2029

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 CCSupporting 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, 25 January 2024
For the Federal Office for Information Security

Sandro Amendola L.S.
Director-General

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....6
1. Preliminary Remarks....6
2. Specifications of the Certification Procedure....6
3. Recognition Agreements....7
4. Performance of Evaluation and Certification....8
5. Validity of the Certification Result....8
6. Publication....9
B. Certification Results....10
1. Executive Summary....11
2. Identification of the TOE....12
3. Security Policy....14
4. Assumptions and Clarification of Scope....15
5. Architectural Information....16
6. Documentation....16
7. IT Product Testing....16
8. Evaluated Configuration....17
9. Results of the Evaluation....18
10. Obligations and Notes for the Usage of the TOE....25
11. Security Target....26
12. Regulation specific aspects (eIDAS, QES)....26
13. Definitions....26
14. Bibliography....28
C. Excerpts from the Criteria....30
D. Annexes....31

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_00007Dh, IFX_CCI_00007Eh, IFX_CCI_00007Fh, design step H11 with firmware version 80.506.04.1, optional CryptoSuite version 4.06.002, optional HSL version 04.05.0030, optional UMSLC version 02.01.0040, optional NRG™ version 06.10.0003 and user guidance documents has undergone the certification procedure at BSI.

The evaluation of the product Infineon Security Controller IFX_CCI_00007Dh, IFX_CCI_00007Eh, IFX_CCI_00007Fh, design step H11 with firmware version 80.506.04.1, optional CryptoSuite version 4.06.002, optional HSL version 04.05.0030, optional UMSLC version 02.01.0040, optional NRG™ version 06.10.0003 and user guidance documents was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 23 January 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 25 January 2024 is valid until 24 January 2029. 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_00007Dh, IFX_CCI_00007Eh, IFX_CCI_00007Fh, design step H11 with firmware version 80.506.04.1, optional CryptoSuite version 4.06.002, optional HSL version 04.05.0030, optional UMSLC version 02.01.0040, optional NRG™ version 06.10.0003 and user guidance documents 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
Melli-Beese-Str. 9
86159 Augsburg

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 Security Controller IFX_CCI_00007Dh, IFX_CCI_00007Eh, IFX_CCI_00007Fh, design step H11 with firmware version 80.506.04.1, optional CryptoSuite version 4.06.002, optional HSL version 04.05.0030, optional UMSLC version 02.01.0040, optional NRG™ version 06.10.0003 and user guidance documents.

The TOE provides a secure CPU which is compatible to the 32-bit Arm v8-M architecture. The major components of the processor system are the CPU (Central Processing Unit), a MPU (Memory Protection Unit), a Security Attribution Unit (SAU), a Nested Vectored Interrupt Controller (NVIC), and an Instruction Stream Signature (ISS) coprocessor. The TOE can communicate using contact-less and contact-based interfaces.

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.

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 all selected from Common Criteria Part 2. Thus the TOE is CC Part 2 conformant.

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

TOE Security Functionality	Addressed issue
SF_DPM	Device Phase Management: The life cycle of the TOE is split up into several phases. Different operation modes help to protect the TOE during each phase of its lifecycle.
SF_PS	Protection against Snooping: The TOE uses various means to protect from snooping of memories and busses and prevents single stepping.
SF_PMA	Protection against Modifying Attacks: This TOE implements measures to protect the integrity of data and instructions in the CPU and memories, implements sensors to detect fault attacks, and allows blocking access to certain peripherals.
SF_PLA	Protection against Logical Attacks: The TOE implements the Arm v8m Memory Protection Unit regions and Security Attribution Unit with eight regions each.

TOE Security Functionality	Addressed issue
SF_HC	Hardware provided Cryptography: The TOE is equipped with a hardware accelerator for TDES and AES. Additionally, it is equipped with a True Random Number Generator.
SF_CS	CryptoSuite Services: The CryptoSuite library utilizes the symmetric coprocessor and the asymmetric coprocessor of the hardware to implement standard symmetric and asymmetric cryptographic operations RSA, ECC, TDES, and AES. Additionally, the CryptoSuite library provides functions for true random number generation and SHA-1 and SHA-2 hash generation.

Table 1: TOE Security Functionalities

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

The assets to be protected by the TOE are defined in the Security Target [6] and [9], chapter 3.4 . 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 3.

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_00007Dh, IFX_CCI_00007Eh, IFX_CCI_00007Fh, design step H11 with firmware version 80.506.04.1, optional CryptoSuite version 4.06.002, optional HSL version 04.05.0030, optional UMSLC version 02.01.0040, optional NRG™ version 06.10.0003 and user guidance documents

The following table outlines the TOE deliverables:

No.	Type	Item / Identifier	Release / Version	Form of Delivery
1.	HW	IFX_CCI_00007Dh, IFX_CCI_00007Eh, IFX_CCI_00007Fh	H11	Postal transfer in cages as bare dies (sawn wafer) or S-COM8.4-6-2 packages
2.	FW	BOS, Flash Loader, ROM parts of HSL, RFAPI library and NRG™ SW library (not part of the TSF)	80.506.04.1 (Flash Loader version is also separately identified as version 09.30.0001)	Stored on the delivered hardware

No.	Type	Item / Identifier	Release / Version	Form of Delivery
3.	SW	NRG™ SW library (optional) (not part of the TSF)	06.10.0003	Secure download of object file via iShare.
4.	SW	HSL (NVM part) (optional)	04.05.0030	Secure download of object file via iShare.
5.	SW	UMSLC library (optional)	02.01.0040	Secure download of object file via iShare.
6.	SW	CryptoSuite library (optional)	4.06.002	Secure download of object file via iShare.
7.	DOC	TERIGON™ SLC26 (32-bit Security Controller - V19) Hardware Reference Manual	V3.1, 2023-08-08	Personalized PDF via secure iShare server.
8.	DOC	TERIGON™ SLx2 security controller family Programmer's Reference Manual SLx2_DFP	V1.3.0, 2023-10-19	Personalized PDF via secure iShare server.
9.	DOC	SLC26 32-bit Security Controller – V19 Security Guidelines	V1.00-3003, 2023-07-26	Personalized PDF via secure iShare server.
10.	DOC	SLx2 Security Controller Family Production and Personalization Manual Flash Loader V9	V09.30, 2023-08-11	Personalized PDF via secure iShare server.
11.	DOC	Crypto2304T V4, User Manual	v2.0, 2023-07-14	Personalized PDF via secure iShare server.
12.	DOC	TERIGON™ SLC26 (32-bit Security Controller - V19) Errata sheet	V5.0, 2023-12-12	Personalized PDF via secure iShare server.
13.	DOC	CS-SLC26V19 CryptoSuite 32-bit Security Controller User interface manual	v4.06.002, 2023-12-11	Personalized PDF via secure iShare server.

Table 2: Deliverables of the TOE

The delivery documentation describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the user's site including the necessary intermediate delivery procedures.

The delivery documentation describes in a sufficient manner how the various procedures and technical measures provide for the detection of modifications and any discrepancies between the TOE respective parts of it send by the TOE Manufacturer and the version received by the Composite Product Manufacturer.

Therefore, three different delivery procedures must 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 (e.g. ROM / Flash data, initialisation, and pre-personalisation 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).

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

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.

The hardware part of the TOE is identified by IFX_CCI_00007Dh, IFX_CCI_00007Eh, IFX_CCI_00007Fh, design step H11.

Depending on the blocking configuration, a TOE can have different sizes of the available NVM and RAM, available cryptographic coprocessors, and interfaces (see ST [6], [8] chapter 1.4.6 for details). In the field, the IC Embedded Software Developer can identify a product in question using the Generic Chip Identification Mode (GCIM), which is described in [13], chapter 8.4. This information can also be read out using the IFX mailbox area (see [13], chapter 8.9 / 8.10). Thereby, the exact and distinct identification of any product with its exact configuration of this TOE is given.

The bytes 45, 46 and 47 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. 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 bytes 11 and 12 of the GCIM. The GCIM is described in detail in the Programmer’s Reference Manual [13], chapter 8.4 / 8.12.

In addition to the hardware part, the TOE consists of firmware parts and software parts. The firmware part of the TOE is identified also via the GCIM. Bytes 31 to 34 contain the firmware identifier, which uniquely identifies the versions of the BOS, the FL and the ROM part of the HSL, RFAPI and NRG. The optional libraries comprise the HSL (NVM part), UMSLC, NRG™ SW (not part of the TSF), and CryptoSuite. These libraries are identified by their version numbers. The user can identify the versions by calculating the hash value of the provided library files and compare them to the hash values provided in Security Target [6], chapter 8.

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:The security policy of the TOE is to provide basic security functionalities to be used by the smart card operating system and the smart card application, thus providing an overall smart card system security. Therefore, the TOE will implement a symmetric cryptographic block cipher algorithm (Triple-DES and AES) to ensure the confidentiality of plain text data by encryption and to support secure authentication protocols and it will provide a true random number generator.

The CryptoSuite library is used to provide a high-level interface to RSA (Rivest, Shamir, Adleman) cryptography implemented on the hardware component Crypto2304T and includes countermeasures against SPA, DPA and DFA attacks. Even more the CryptoSuite library is used to provide a high-level interface to Elliptic Curve cryptography implemented on the hardware component Crypto2304T and includes countermeasures against SPA, DPA and DFA attacks. It also provides a high-level interface for performing cryptographic hash functions and for obtaining random data and includes countermeasures against SPA, DPA and DFA attacks.

Besides that, the TOE can come with the optional Hardware Support Library (HSL) providing 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 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 6 and 7 of the Security Target (ST).

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance: A.Process-Sec-IC - Protection during Packaging, Finishing and Personalization, A.Resp-Appl - Treatment of User Data.

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 [14] and the Programmer’s Reference Manual [13].

The ST [6] and PP [8] includes multiple objectives for the Composite Product Integrator and Personaliser:

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 [8, 1.2.4], the TOE can be delivered to the composite product manufacturer after phase 3 or after phase 4 depending on the delivery form (as bare dies (sawn wafer) with 150µ Class 2 antenna or as S-COM8.4-6-2/-4 + ID 2/3 antenna modules). However, the actual ICs are identical in all cases. This means that the test mode is deactivated, and the TOE is locked into user mode. Therefore, it is not necessary to distinguish between these forms of delivery. Since IFX 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 Integrator and Personaliser.

The objective OE.TOE_Auth requires the environment to support the authentication and verification mechanism and to know the corresponding authentication reference data. The composite product manufacturer receives sufficient information regarding the authentication mechanism in [15], chapter 4.1. Please note that this mechanism is based on the FL and is thus only available until the FL is permanently deactivated.

The objective OE.Loader_Usage requires the authorised user to support the trusted communication with the TOE’s loader by protecting the confidentiality and integrity of the loaded data and to meet the access conditions defined by the loader. [15] chapter 4

describing the FL's personalization interface 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 FL is described in [15], chapter 4.6. 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 FL 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 3.3.1.

5. Architectural Information

For further information on the TOE architecture, see Security Target [6] and [9], section 1 (especially sections 1.3 and 1.4).

6. Documentation

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

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

7. IT Product Testing

Regarding functional testing:

Different classes of functional tests were performed by the developer to test the TOE:

- Functional verification,
- Qualification tests,
- Verification Tests,
- Security functional Tests,
- Production Tests.

The developer's testing results demonstrate that the TSFs behave as specified. The developer's testing results also demonstrate that the TOE behaves as expected.

In the course of the evaluation of the TOE, the following classes of functional tests were carried out by the ITSEF:

- Module tests,
- Simulation tests,
- Emulation tests,
- Tests in user mode,

- Tests in test mode,
- Hardware tests,
- Optional library tests,
- repetition of developer tests (see above).

With these kinds of tests the entire security functionality of the TOE was tested.

The results of the (functional) developer tests, which have been repeated by the evaluator, matched the results the developer stated.

Overall, the TSF has been tested against the functional specification, the TOE design, and the security architecture description. The tests demonstrate that the TSF performs as specified.

Regarding AVA related tests:

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. No attack scenario with the attack potential high was successful in the TOE's operational environment as defined in the Security Target [6], provided that all measures required by the developer are applied.

The embedded software must implement the security advice given in [12] - [18].

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

- Smartcard IC IFX_CCI_00007Dh, IFX_CCI_00007Eh, IFX_CCI_00007Fh H11 (TSMC fab 15)

This TOE is represented by various configurations called products. The module design, layout, and footprint, of all products are identical. The degree of freedom for configuring the TOE is predefined by the developer.

Furthermore the TOE is comprised of firmware and optional software libraries with revisions stated in section 2. The flash loader (part of FW) was enabled on evaluated derivatives.

An extensive overview over all possible configuration options is given in the Security Target [6] and [9] in sections 1.4.6 and 1.4.7.

The evaluation results, also including results of tests performed by the developer, are valid for all hardware derivates mentioned above. All identifiers represent the equal hardware platform but name differences in configurations or market segments. Configuration differences are achieved by blocking only. The firmware and optional software libraries were examined in those revisions, which are stated in table 2 (above).

The evaluation results are valid for all configurations and blocking options of the hardware stated in section 1.4.6 of the Security Target [6] and [9]. Depending on configuration,

blocking option and on selection of optional software libraries, some of the services might be unavailable to the user. The unavailable services have no security impact on the TOE. The user must ensure a working configuration. The evaluation results apply to all configurations of the Flash Loader as stated in the Security Target [6] and [9].

The evaluation results cannot be extended to further versions/derivates of the TOE and/or other production sites without any extra investigations.

Developer and evaluator tested the TOE in these configurations in which the TOE is delivered and which is described above and in Section 2.

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, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers, Version 14, 2017-10-11, Bundesamt für Sicherheit in der Informationstechnik.
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 14, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 7, 2010-08-03, Bundesamt für Sicherheit in der Informationstechnik.
- 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, Bundesamt für Sicherheit in der Informationstechnik.
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 20, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3, 2013-05-15, Herausgeber: Zertifizierungsstelle des BSI im Rahmen des Zertifizierungsschemas, Bundesamt für Sicherheit in der Informationstechnik.
- A proposal for: Functionality classes for random number generators, W. Killmann, W. Schindler, Version 2.0, 2011-09-18, T-Systems GEI GmbH and Bundesamt für Sicherheit in der Informationstechnik. (same as [KS2011])
- Developer evidence for the evaluation of a deterministic random number generator, Version 0.9, 2013-02-28, Bundesamt für Sicherheit in der Informationstechnik.
- Evaluation Report as part of the Evaluation Technical Report, Part B – ETR-Part Deterministic Random Number Generator, Template-Version 0.10, 2013-02-28, Bundesamt für Sicherheit in der Informationstechnik.

- CC Supporting Document Guidance – Collection of Developer Evidence, Version 1.5, April 2012, CCDB-2012-04-005.
- Joint Interpretation Library – Collection of Developer Evidence, Version 1.5, January 2012.
- Application Notes and Interpretation of the Scheme (AIS) – AIS 25, Anwendungen der CC auf integrierte Schaltungen, Version 9, 2017-03-15, Bundesamt für Sicherheit in der Informationstechnik.
- CC Supporting Document Mandatory Technical Document – Security Architecture requirements (ADV_ARC) for smart cards and similar devices, Version 2.1, April 2014, CCDB-2012-04-004.
- CC Supporting Document Guidance – Security Architecture requirements (ADV_ARC) for smart cards and similar devices – Appendix 1, Version 2.0, April 2012.
- CC Supporting Document Mandatory Technical Document – The Application of CC to Integrated Circuits, Version 3.0, Revision 1, March 2009, CCDB-2009-03-002.
- Joint Interpretation Library – Security Architecture requirements (ADV_ARC) for smart cards and similar devices – Appendix 1, Version 2.0, January 2012.
- Joint Interpretation Library – The Application of CC to Integrated Circuits, Version 3.0, February 2009.
- Joint Interpretation Library – Security requirements for post-delivery code loading, Version 1.0, February 2016.
- Validity of conducted tests on Security Smart Card ICs in dependence of test date, Version 1, 2017-03-15, Bundesamt für Sicherheit in der Informationstechnik.
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 26, Evaluationsmethodologie für in Hardware Integrierte Schaltungen, Version 10, 2017-07-03, Bundesamt für Sicherheit in der Informationstechnik.
- Auswahl geeigneter Chips für DPA-Messungen, Version 1.1, 2008-12-07, Bundesamt für Sicherheit in der Informationstechnik.
- Special Attack Methods for Smartcards and Similar Devices, Version 1.4, 2011-06-08, Bundesamt für Sicherheit in der Informationstechnik.
- CC Supporting Document Mandatory Technical Document – Requirements to perform Integrated Circuit Evaluations, Version 1.1, May 2013, CCDB-2013-05-001.
- Joint Interpretation Library – Application of Attack Potential to Smartcards, Version 3.2, 2022-11.
- Joint Interpretation Library – Attack Methods for Smartcards and Similar Devices, Version 2.4, 2020-01, confidential.
- Joint Interpretation Library – Requirements to perform Integrated Circuit Evaluations, Version 1.1, February 2013.
- Application Notes and Interpretation of the Scheme (AIS) – AIS 27, Transition from ITSEC to CC, Version 5, 2010-08-17, Bundesamt für Sicherheit in der Informationstechnik.
- 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.

- Developer evidence for the evaluation of a physical true random generator, Version 0.8, 2013-02-28, Bundesamt für Sicherheit in der Informationstechnik.
- Evaluation Report as part of the Evaluation Technical Report, Part B – ETR-Part True Physical and Hybrid Random Number Generator, Template-Version 0.7, 2013-02-28, Bundesamt für Sicherheit in der Informationstechnik.
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 32, CC-Interpretationen im deutschen Zertifizierungsschema, Version 7, 2011-06-08, Bundesamt für Sicherheit in der Informationstechnik.
- 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, Bundesamt für Sicherheit in der Informationstechnik.
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 35, Öffentliche Fassung eines Security Target (ST-Lite), Version 2, 2007-11-12, Bundesamt für Sicherheit in der Informationstechnik.
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 36, Kompositionsevaluierung, Version 5, 2017-03-15, Bundesamt für Sicherheit in der Informationstechnik.
- CC Supporting Document Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, Version 1.4, December 2015, CCDB-2015-12-001.
- Joint Interpretation Library – Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018.
- CC Supporting Document Guidance – ETR template for composite evaluation of Smart Cards and similar devices, Version 1.1, December 2015, CCDB-2015-12-002.
- Joint Interpretation Library – ETR template for composite evaluation of Smart Cards and similar devices, Version 1.1, August 2015.
- Joint Interpretation Library – Certification of “open” smart card products, Version 1.1 (for trial use), 2013-02-04.
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 37, Terminologie und Vorbereitung von Smartcard-Evaluierungen, Version 3, 2010-05-17, Bundesamt für Sicherheit in der Informationstechnik.
- CC Supporting Document Guidance – Smartcard Evaluation, Version 2.0, February 2010, CCDB-2010-03-001.
- Application Notes and Interpretation of the Scheme (AIS) – AIS 38, Reuse of evaluation results, Version 2, 2007-09-28, Bundesamt für Sicherheit in der Informationstechnik.
- Application Notes and Interpretation of the Scheme (AIS) – AIS 41, Guidelines for PPs and STs, Version 2, 2011-01-31, Bundesamt für Sicherheit in der Informationstechnik.
- Guidance Document – The PP/ST Guide, Version 2, Revision 0, 2010-08, Bundesamt für Sicherheit in der Informationstechnik.
- 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, Bundesamt für Sicherheit in der Informationstechnik.

- Review-Protokoll zum (Krypto-)AVA-KickOff, Template-Version/Date: 2019-08-23, Bundesamt für Sicherheit in der Informationstechnik.
- Minimal Requirements for Evaluating Side-Channel Attack Resistance of Elliptic Curve Implementations, Version 1.0.4, 2011-07-01, BSI.
- Methodology for cryptographic rating of memory encryption schemes used in smartcards and similar devices, Version 1.0, 2013-10-31, BSI.
- Minimum Requirements for Evaluating Side-Channel Attack Resistance of RSA, DSA and Diffie-Hellman Key Exchange Implementations, Version 1.0, 2013-01-14, BSI.
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 47, Regelungen zu Site Certification, Version 1.1, 2013-12-04, Bundesamt für Sicherheit in der Informationstechnik.
- Guidance for Site Certification, Version 1.1, 2013-12-04, Bundesamt für Sicherheit in der Informationstechnik.
- Joint Interpretation Library – Minimum Site Security Requirements, Version 3.0, 02/2020.

(see [4] for respective AIS references).

For RNG assessment the scheme interpretations AIS 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.

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
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 120 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 120 Bits*' of the following table with '*no*' achieves a security level of lower than 120 Bits (in general context) only.

#	Purpose	Cryptographic mechanism	Implementation standard	Key size in Bit	Security Level above 120 Bits?
Symmetric Co-Processor (SCP)					
1	Cryptographic primitive	TDES	[NIST SP800-67], [ISO18033-3]	112, 168	-
2	Cryptographic primitive	AES	[FIPS197], [ISO18033-3]	128, 192, 256	-
3	Confidentiality	#1 in ECB mode for encryption and decryption	[NIST SP800-38A]	112, 168	No
4	Confidentiality	#2 in ECB mode for encryption and decryption	[NIST SP800-38A]	128, 192, 256	No
Crypto Suite: Symmetric Functionality					
5	Cryptographic primitive	TDES	[NIST SP800-67]	112, 168	-
6	Cryptographic primitive	AES	[FIPS197]	128, 192, 256	-
7	Confidentiality	#5 in ECB mode for encryption and decryption	[NIST SP800-38A]	112, 168	No
8	Confidentiality	#5 in CBC mode for encryption and decryption	[NIST SP800-38A]	112, 168	No
9	Confidentiality	#6 in ECB mode for encryption and decryption	[NIST SP800-38A]	128, 192, 256	No
10	Confidentiality	#6 in CBC mode for encryption and decryption	[NIST SP800-38A]	128, 192, 256	Yes
11	Integrity	#5 in Retail MAC mode for MAC generation	[ISO_9797-1]	112	No
12	Integrity	#6 in CMAC mode for MAC	[NIST SP800-38B]	128, 192, 256	Yes

#	Purpose	Cryptographic mechanism	Implementation standard	Key size in Bit	Security Level above 120 Bits?
		generation			
Crypto Suite: Asymmetric Functionality					
13	Key agreement	Finite field Diffie-Hellman	[PKCS#3, 7.2]	1024-2048	No
14	Confidentiality	RSA Encryption	[PKCS #1, 5.1.1]	1024 – 4224	Yes >= 2800 bit
15	Confidentiality	RSA Decryption	[PKCS #1, 5.1.2, 2a]	1024 – 2112	No
16	Confidentiality	RSA Decryption with CRT	[PKCS #1, 5.1.2, 2b]	1024 – 4224	Yes >= 2800 bit
17	Authenticity	RSA Signature generation	[PKCS #1, 5.2.1, 2a]	1024 – 2112	No
18	Authenticity	RSA Signature generation with CRT	[PKCS #1, 5.2.1, 2b]	1024 – 4224	Yes >= 2800 bit
19	Authenticity	RSA Signature verification	[PKCS #1, 5.2.2]	1024 – 4224	Yes >= 2800 bit
20	N/A	Supported elliptic curves: • All curves in [FIPS186-4], • All curves in [RFC5639].	[FIPS186-4] [RFC5639]	-	-
21	Authenticity	ECDSA signature generation on curves listed in #20[7]	[FIPS186-4, 6.4]	160-521	Key sizes 160, 163, 192, 224 : No Key sizes >= 250: Yes
22	Authenticity	ECDSA signature verification on curves listed in #20[7]	[FIPS186-4, 6.4]	160-521	Key sizes 160, 163, 192, 224 : No Key sizes >= 250: Yes
23	Key agreement	Elliptic Curve Diffie-Hellman (ECDH) key agreement on curves listed in #20	[NIST SP800-56A, 5.7.1.2]	160-521	Key sizes 160, 163, 192, 224 : No Key sizes >= 250: Yes
24	Key generation	Elliptic Curve key generation on	[FIPS186-4, B.4.1]	160-521	Key sizes 160, 163, 192,

[7]Note that the hash calculation of ECDSA is not implemented by the library and lies in the responsibility of the user

#	Purpose	Cryptographic mechanism	Implementation standard	Key size in Bit	Security Level above 120 Bits?
		curves listed in #20			224 : No Key sizes >= 250: Yes
Crypto Suite: Hash Functionality					
25	Hash	SHA-1	[FIPS180-4]	N/A	N/A
26	Hash	SHA-2	[FIPS180-4]	N/A	N/A
Hardware RNG					
27	RNG	Physical RNG	Corresponds to PTG.2 in [KS2011]	N/A	N/A
Crypto Suite: Hash Functionality					
28	RNG	Physical RNG	Corresponds to PTG.2 in [KS2011]	N/A	N/A
29	RNG	Physical RNG with cryptographic post-processing	Corresponds to PTG.3 in [KS2011]	N/A	N/A
Flash Loader					
30	Cryptographic primitive	AES	[FIPS197]	128	Not rated
31	Authenticated encryption	#30 in CCM mode	[NIST SP 800-38C]	128	Not rated
32	Key derivation	KDF in counter mode with AES CMAC as PRF[8]	[NIST SP 800-108, 5.1], [NIST SP 800-38B, 6.2]	128	Not rated

Table 3: TOE cryptographic functionality

[NIST SP800-67] NIST Special Publication 800-67 – Revision 2, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, 2017-11, National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce.

[PKCS#1] *PKCS #1: RSA Cryptography Standard*, Version 2.2, October 27, 2012, RSA Laboratories.

[PKCS#3] PKCS #3: Diffie-Hellman Key-Agreement Standard, Version 1.4, November 1, 1993, RSA Laboratories.

[FIPS 197] FIPS 197, Federal Information Processing Standards Publication, Advanced Encryption Standard (AES), Published 2001-11-26, Updated 2023-05-09, National Institute of Standards and Technology (NIST).

[FIPS 180-4] FIPS PUB 180-4 Federal Information Processing Standards Publication Secure Hash Standard (SHS), August 2015, Information Technology Laboratory National Institute of Standards and Technology.

[FIPS 186-4] 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).

[8]This algorithm is only used by the Flash Loader and not provided as service for the Embedded Software.

[SP 800-38A] NIST SP800-38A, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, 2001, National Institute of Standards and Technology (NIST).

[SP 800-67] NIST Special Publication 800-67 – Revision 2, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, 2017-11, National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce.

[SP 800-38A] NIST SP800-38A, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, 2001, National Institute of Standards and Technology (NIST).

[SP 800-56A] NIST SP800-56A, Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography, Revision 3, 2018-04, National Institute of Standards and Technology (NIST).

[SP 800-38C] NIST SP800-38C, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, 2004-05 with updates as of 2007-07-20, National Institute of Standards and Technology (NIST).

[SP 800-108] NIST Special Publication 800-108, Recommendation for Key Derivation Using Pseudorandom Functions (Revised), 2009-10, National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce.

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 requirements described in [14],[16],[17],[18],[12],[15], and [13] shall be fulfilled.
- All recommendations and other security hints described in [14],[16],[17],[18],[12],[15], and [13] should be followed. These recommendations are not mandatory; however, it is advised to consider them.

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

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

In addition, the following hints resulting from the ALC evaluation aspect must be considered:

- The security IC embedded software developer can deliver their software either to Infineon to let them implement it in the TOE (in the NVM) or to the composite product manufacturer to let them download the software into the NVM.
- Except for ECC, the TOE does not implement key generation (FCS_CKM.1) or key insertion (FDP_ITC.1/2) as required by the FCS_COP.1 iterations (dependency) used in the PP for symmetric cryptography. The IC Embedded Software has to provide this functionality instead.
- 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 is required.

11. Security Target

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

12. 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
FL	Flash Loader
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
NVM	None Volatile Memory
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[9] 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-1229-2024, Version 1.0.3, 2024-01-15, IFX_CCI_00007Dh, IFX_CCI_00007Eh, IFX_CCI_00007Fh H11 with optional CryptoSuite Security Target, Infineon Technologies AG. (confidential document)

[7] Evaluation Technical Report, Version 3, 2024-01-18, EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY), TÜV Informationstechnik GmbH, (confidential document)

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

[9] Security Target Lite BSI-DSZ-CC-1229-2024, Version 1.0.3, 2024-01-15, IFX_CCI_00007Dh, IFX_CCI_00007Eh, IFX_CCI_00007Fh H11 with optional CryptoSuite Security Target Lite, Infineon Technologies AG. (sanitised public document)

[10] Evaluation Technical Report for composite evaluation according to AIS 36 for the Product BSI-DSZ-CC-1229-2024, Version 3, 2024-01-18, EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION (ETR COMP), TÜV Informationstechnik GmbH, (confidential document)

[11] Configuration list for the TOE, Version 0.2, 2023-11-28, M5376 H11 ALC, Infineon Technologies AG (confidential document)

[12] Hardware Reference Manual,TERIGON SLC26 (32-bit Security Controller - V19) Hardware Reference Manual, Version 3.1 ,2023-08-08, Infineon Technologies AG

[9] specifically

- See chapter 9.1

[13] Programmer’s Reference Manual, TERIGON SLx2 security controller family Programmer’s Reference Manual SLx2_DFP, Version 1.3.0, 2023-10-19, Infineon Technologies AG

[14] Security Guidelines, SLC26 32-bit Security Controller – V19 Security Guidelines, Version 1.00-3003, 2023-07-26, Infineon Technologies AG

[15] Production and Personalization Manual Flash Loader , SLx2 Security Controller Family Production and Personalization Manual Flash Loader V9, Version 09.30, 2023-08-11, Infineon Technologies AG

[16] User Manual Crypto Coprocessor, Crypto2304T V4, User Manual, Version 2.0, 2023-07-14, Infineon Technologies AG

[17] Errata Sheet, TERIGON SLC26 (32-bit Security Controller - V19) Errata sheet, Version 5.0, 2023-12-12, Infineon Technologies AG

[18] User interface manual, CS-SLC26V19 CryptoSuite 32-bit Security Controller User interface manual, Version 4.06.002, 2023-12-11, Infineon Technologies AG

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 of Certification Report BSI-DSZ-CC-1229-2024

Evaluation results regarding development and production environment

The IT product Infineon Security Controller IFX_CCI_00007Dh, IFX_CCI_00007Eh, IFX_CCI_00007Fh, design step H11 with firmware version 80.506.04.1, optional CryptoSuite version 4.06.002, optional HSL version 04.05.0030, optional UMSLC version 02.01.0040, optional NRG™ version 06.10.0003 and user guidance documents (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 and 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 25 January 2024, 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)

are fulfilled for the development and production sites of the TOE listed below:

Distribution Center name	Address
DHL Singapore	DHL Supply Chain Singapore Pte 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 – Building 8A 63762 Großostheim Germany

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