Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1205-2023

for

IFX_CCI_00006A, IFX_CCI_00006Bh, IFX_CCI_00006Ch design step S12 with firmware 80.311.04.1, optional NRG SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib 01.30.0695, optional SCL v2.15.000, optional ACL v3.34.000, optional RCL v1.10.007, optional HCL v1.13.002 and userguidance

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-1205-2023 (*)

Smartcard Controller

IFX_CCI_00006A, IFX_CCI_00006Bh, IFX_CCI_00006Ch design step S12 with firmware 80.311.04.1, optional NRG SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib 01.30.0695, optional SCL v2.15.000, optional ACL v3.34.000, optional RCL v1.10.007, optional HCL v1.13.002 and userguidance

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:	27 August 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, 28 August 2023

For the Federal Office for Information Security

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

Matthias Intemann L.S.
Head of Section

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 IFX_CCI_00006A, IFX_CCI_00006Bh, IFX_CCI_00006Ch design step S12 with firmware 80.311.04.1, optional NRG SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib 01.30.0695, optional SCL v2.15.000, optional ACL v3.34.000, optional RCL v1.10.007, optional HCL v1.13.002 and userguidance has undergone the certification procedure at BSI.

The evaluation of the product IFX_CCI_00006A, IFX_CCI_00006Bh, IFX_CCI_00006Ch design step S12 with firmware 80.311.04.1, optional NRG SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib 01.30.0695, optional SCL v2.15.000, optional ACL v3.34.000, optional RCL v1.10.007, optional HCL v1.13.002 and userguidance was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 23 August 2023. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

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

The product was developed by: Infineon Technologies AG.

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

5. Validity of the Certification Result

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

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

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

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

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 28 August 2023 is valid until 27 August 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 IFX_CCI_00006A, IFX_CCI_00006Bh, IFX_CCI_00006Ch design step S12 with firmware 80.311.04.1, optional NRG SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib 01.30.0695, optional SCL v2.15.000, optional ACL v3.34.000, optional RCL v1.10.007, optional HCL v1.13.002 and userguidance 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.

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.

[6] Infineon Technologies AG
Am Campeon 1-15
85579 Neubiberg

1. Executive Summary

The Target of Evaluation (TOE) is the Infineon Security Controller IFX_CCI_00006Ah, IFX_CCI_00006Bh, IFX_CCI_00006Ch design step S12 with firmware 80.311.04.1, optional NRG™ SW v05.03.4097, optional HSL v3.52.9708, UMSLC lib v01.30.0695, optional SCL v2.15.000, optional ACL v3.34.000, optional RCL v1.10.007, optional HCL v1.13.002 and user guidance.

The TOE provides a 32-bit ARMv7-M CPU-architecture. The major components of the core system are the CPU (Central Processing Unit), an MPU (Memory Protection Unit), a Nested Vectored Interrupt Controller (NVIC), and an Instruction Stream Signature (ISS). 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.

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 protection against modifying attacks of memories, alarm lines and sensors.
SF_PLA	Protection against Logical Attacks: The memory model of the TOE provides two distinct, independent levels and the possibility to define up to eight memory regions with different access rights enforced by the Memory Protection Unit (MPU).
SF_CS	Cryptographic Support: The TOE is equipped with several hardware accelerators and software modules to support the standard symmetric and asymmetric cryptographic

TOE Security Functionality	Addressed issue
	operations like RSA, EC, TDES, and AES. Additionally, the TOE is equipped with a Hybrid Random Number Generator and a random crypto library providing different modes of operation: hybrid random number generation, true random number generation, and deterministic random number generation. Furthermore, a hash crypto library provides SHA-1 and SHA-2 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 3.1.2. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and [9], chapter 3.

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

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

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

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

IFX_CCI_00006A, IFX_CCI_00006Bh, IFX_CCI_00006Ch design step S12 with firmware 80.311.04.1, optional NRG SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib 01.30.0695, optional SCL v2.15.000, optional ACL v3.34.000, optional RCL v1.10.007, optional HCL v1.13.002 and userguidance

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1.	HW	IFX_CCI_00006Ah, IFX_CCI_00006Bh, IFX_CCI_00006Ch	S12	Postal transfer in cages as complete modules, wafers, IC cases or packages
2.	FW	Boot Software (BOS)	80.311.04.1	Stored on the delivered hardware
3.	FW	Flash Loader (FL) (optional)	v09.13.0006	Stored on the delivered hardware
4.	FW	Performance Optimized Write Scheme (POWS)	80.311.04.1	Stored on the delivered hardware
5.	FW	Radio Frequency Application Interface (RFAPI)	80.311.04.1	Stored on the delivered hardware
6.	SW	NRG™ SW (optional)	v05.03.4097	Secure download (L251 Library File) via ishare.

No	Type	Identifier	Release	Form of Delivery
7.	SW	HSL (optional)	v3.52.9708	Secure download (L251 Library File) via ishare.
8.	SW	UMSLC	v01.30.0695	Stored on the delivered hardware.
9.	SW	SCL (optional)	v2.15.000	Secure download (L251 Library File) via ishare.
10.	SW	ACL (optional)	v3.34.000	Secure download (L251 Library File) via ishare.
11.	SW	RCL (optional)	v1.10.007	Secure download (L251 Library File) via ishare.
12.	SW	HCL (optional)	v1.13.002	Secure download (L251 Library File) via ishare.
13	DOC	SLC39 32-bit Security Controller - V23, Hardware Reference Manual	v2.0 2022-06-15	Personalized PDF via secure iShare server.
14	DOC	SLx1/SLx3 (40 nm) Security Controllers, Programmer's Reference Manual	v5.4 2022-12-21	Personalized PDF via secure iShare server.
15	DOC	SLC39 32-bit Security Controller - V23, Security Guidelines	v1.00-2942 2023-01-05	Personalized PDF via secure iShare server.
16	DOC	SLx3 (40nm) Security Controllers, Production and Personalization Manual	v09.13 2022-02-01	Personalized PDF via secure iShare server.
17	DOC	32-bit Security Controller Crypto2304T V3, User Manual (optional)	v2.1 2022-12-16	Personalized PDF via secure iShare server.
18	DOC	HSL for SLCx7 V23b, Hardware Support Library (optional)	v3.52.9708 2022-06-22	Personalized PDF via secure iShare server.
19	DOC	UMSLC library for SLCx7V23b User Mode Security Life Control	v01.30.0695 2022-07-04	Personalized PDF via secure iShare server.
20	DOC	SCL37-SCP-v440-C40 Symmetric Crypto Library for SCP-v440 AES/DES/MAC (optional)	v2.15.000 2023-03-06	Personalized PDF via secure iShare server.
21	DOC	ACL37-Crypto2304T-C40 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox (optional)	v3.34.000 2022-08-09	Personalized PDF via secure iShare server.
22	DOC	RCL37-X-C40 Random Crypto Library for SCP-v440 & RNG-v3 DRBG/HWRNG 32-bit Security Controller, User interface manual (optional)	v1.10.007 2020-06-16	Personalized PDF via secure iShare server.
23	DOC	HCL37-CPU-C40 Hash Crypto Library for CPU SHA 32-bit Security Controller, User interface manual (optional)	v1.13.002 2020-05-07	Personalized PDF via secure iShare server.

Table 2: Deliverables of the TOE

As the TOE is under control of the user software, the TOE Manufacturer can only guarantee the integrity up to the delivery procedure. It is in the responsibility of the

Composite Product Manufacturer to include mechanisms in the implemented software (developed by the IC Embedded Software Developer) which allows detection of modifications after the delivery.

In detail, regarding identification:

The hexadecimal values listed behind the “IFX_CCI_” are part of the TOE name IFX_CCI_00006Ah, IFX_CCI_00006Bh, IFX_CCI_00006Ch. These identifiers are used by the developer only for this TOE. Different underlying basic hardware configurations are achieved only by the means of blocking; the actual hardware is always present and thus identical but may not be accessible to the user. The design step of the TOE is indicated by byte 11 and 12 of the GCIM. The GCIM is described in [11, 5.6].

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. The optional software consists of the libraries ACL, SCL, HSL, RCL, HCL, and NRG. The UMSLC library is always part of the TOE.

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 [ST, Chapter 9 – 15].

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 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 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. The RCL provides a high-level interface for obtaining random data. This can be deterministic data from an AES CTR_DRBG or non-deterministic data that is provided by the underlying hardware. The RCL 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, 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 6 and 7 of the Security Target [6] and[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, OE.TOE_Auth, and OE.Prevent_Masquerade.

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 [13]

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

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 1.4.5, the TOE can be delivered to the composite product manufacturer after phase 3 or after phase 4. However, the single chips are identical in all cases. This means that the test mode is deactivated and the TOE is locked in the user mode. Therefore, it is not necessary to distinguish between these forms of delivery. Since Infineon has no information about the security requirements of the implemented IC embedded software, it is not possible to define any concrete security requirements for the environment of the composite product manufacturer.

The objective OE.TOE_Auth requires that the environment has to support the authentication and verification mechanism and has to know the corresponding authentication reference data. The composite product manufacturer receives sufficient information with regard to the authentication mechanism in [14], chapter 2.1.5. Please note that this objective is only valid in case the Flash Loader is ordered with mutual authentication (i.e., option External Authentication is unavailable).

The objective OE.Prevent_Masquerade is valid in case the Flash Loader is ordered with External Authentication (EA) instead of mutual authentication. In this case, customers need to take care that no masquerading attacks can be performed. The objective replaces OE.Prevent_Masquerade. A description of the External Authentication is given in [14] chapter 2.1.5 and the ST highlights the risks of masquerading attacks when using this order option of the flash loader:

The objective OE.Prevent_Masquerade requires measures by customers to ensure the authenticity of the TOE.

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. [14] chapter 4 provides sufficient information regarding this topic.

The objective OE.Lim_Block_Loader requires the composite product manufacturer to protect the loader against misuse, to limit the capability of the loader and to terminate the loader irreversibly after the intended usage. The permanent deactivation of the flash loader is described in [14] chapter 2.1.2.2]. 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 4.2.

5. Architectural Information

The TOE hardware consists basically of a core, a memory system, and peripherals. There are two separate bus entities: a memory bus and a peripheral bus for high-speed communication with the peripherals. In more detail, the TOE hardware can be further divided into Major core components: CPU, MPU, NVIC,ISS, Memory system components: ROM, Cache, RAM, NVM, ICS, Memory bus and peripherals such as SPAU, SCP, RNG,CRC module.

Further, more detailed information is readily available in the Security Target [6] and [9] Chapter 1.4. .

6. Documentation

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

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

7. IT Product Testing

The tests performed by the developer were divided into the following categories:

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

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

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

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

For penetration testing, the evaluators took all security functionalities into consideration. Intensive penetration testing was planned based on the analysis results and performed for the underlying mechanisms of security functionalities. The penetration tests considered both the physical tampering of the TOE and attacks, which do not modify the TOE physically. The penetration test 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_00006Ah, IFX_CCI_00006Bh, IFX_CCI_00006Ch S12 (Global Foundries Fab 7)

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).

- 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 derCC 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

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.

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 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

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

No.	Purpose	Cryptographic Mechanism	Stdandard of Implementation	Key Size in Bits	Comments	Security Level above 100 Bits
Symmetric Co-Processor (SCP)						
1	Cryptographic primitive	TDES	[NIST SP800-67], [ISO18033-3]	112, 168	-	Yes (for |k|=168 bit)
2	Cryptographic primitive	AES	[FIPS197], [ISO18033-3]	128, 192, 256	-	Yes
3	Confidentiality	TDES #1 in ECB mode for encryption and decryption	[NIST SP800-38A]	112, 168	-	No
4	Confidentiality	TDES #1 in CBC mode for encryption and decryption	[NIST SP800-38A]	112, 168	-	Yes (for |k|=168 bit)
5	Confidentiality	#2 in ECB mode for encryption and decryption	[NIST SP800-38A]	128, 192, 256	-	No
6	Confidentiality	#2 in CBC mode for encryption and decryption	[NIST SP800-38A]	128, 192, 256	-	Yes
Symmetric Cryptographic Libraries						
7	Cryptographic primitive	TDES	[NIST SP800-67]	112, 168	-	Yes (for |k|=168 bit)
8	Cryptographic primitive	AES	[FIPS197]	128, 192,	-	Yes

No.	Purpose	Cryptographic Mechanism	Stdandard of Implementation	Key Size in Bits	Comments	Security Level above 100 Bits
				256		
9	Confidentiality	#7 in ECB mode for encryption and decryption	[NIST SP800-38A]	112, 168	-	No
10	Confidentiality	#7 in CBC mode for encryption and decryption	[NIST SP800-38A]	112, 168		Yes (for |k|=168 bit)
11	Confidentiality	#7 in CTR mode for encryption and decryption	[NIST SP800-38A]	112, 168		Yes (for |k|=168 bit)
12	Confidentiality	#7 in CFB mode for encryption and decryption	[NIST SP800-38A]	112, 168	-	Yes (for |k|=168 bit)
13	Integrity protection	#7 in CMAC mode for MAC generation and verification	[NIST SP800-38B]	112, 168	-	Yes (for |k|=168 bit)
14	Integrity protection	#7 in Retail MAC (Algorithm 3) for MAC generation and verification	[ISO9797-1]	112	-	No
15	Confidentiality	#8 in ECB mode for encryption and decryption	[NIST SP800-38A]	128, 192, 256	-	No
16	Confidentiality	#8 in CBC mode for encryption and decryption	[NIST SP800-38A]	128, 192, 256	-	Yes
17	Confidentiality	#8 in CTR mode for encryption and decryption	[NIST SP800-38A]	128, 192, 256	-	Yes
18	Confidentiality	#8 in CFB mode for encryption and decryption	[NIST SP800-38A]	128, 192, 256	-	Yes
19	Integrity protection	#8 in CMAC mode for MAC generation and verification	[NIST SP800-38B]	128, 192, 256	-	Yes
Asymmetric Cryptographic Library (ACL) v3.34.000						
20	Confidentiality	RSA Encryption	[PKCS #1, 5.1.1] [IEEE_P1363, 8.2.2]	512 – 4224	-	2048 bit Sec.Lev. > 100bit
21	Confidentiality	RSA Decryption	[PKCS #1, 5.1.2] [IEEE_P1363,	512 – 2112	-	2048 bit Sec.Lev.

No.	Purpose	Cryptographic Mechanism	Stdandard of Implementation	Key Size in Bits	Comments	Security Level above 100 Bits
			8.2.1 (I) / 8.2.3]			> 100bit
22	Confidentiality	RSA Decryption with CRT	[PKCS #1, 5.1.2] [IEEE_P1363, 8.2.1 (II) / 8.2.3]	512 – 4224	-	2048 bit Sec.Lev. > 100bit
23	Authenticity	RSA Signature generation	[PKCS #1, 5.2.1] [IEEE_P1363, 8.2.1 (I) / 8.2.4]	512 – 2112	-	2048 bit Sec.Lev. > 100bit
24	Authenticity	RSA Signature generation with CRT	[PKCS #1, 5.2.1] [IEEE_P1363, 8.2.1 (II) / 8.2.4]	512 – 4224	-	2048 bit Sec.Lev. > 100bit
25	Authenticity	RSA Signature verification	[PKCS #1, 5.2.2] [IEEE_P1363, 8.2.5]	512 – 4224	-	n/a
26	Key generation	RSA key generation returning CRT key components dp, dq and qinv (prime generation not included)	[PKCS #1, 3.1 / 3.2] [IEEE_P1363, 8.1.3. 1]	512 – 4224	Method CRT	<2048bit No >=2048bit Yes
27	Key generation	RSA key generation returning key representation n and d (prime generation not included)	[PKCS #1, 3.1 / 3.2] [IEEE_P1363, 8.1.3. 1]	512 – 2112	Method n_d	n/a
28	Key generation	RSA key generation returning key representation p, q and d (prime generation included)	[IEEE_P1363, 8.1.3. 1]	512 – 2047	Method p_q_d; Prime generation method follows [FIPS186-4, B.3.3] with random primes instead of “primes with condition”	No
29	Key generation	RSA key generation returning key representation p, q and d (prime generation included)	[IEEE_P1363, 8.1.3. 1] [FIPS186-4, B.3.3]	2048 – 2112	Method p_q_d	Yes
30	Key agreement	RSA Diffie-Hellman (DH) key agreement	[FIPS186-4, 5.5] [PKCS #1, 5.2.1 / 5.1.2] [IEEE_P1363, 8.2.4 / 8.2.3]	512 - 4224	Method RSA_DH	<2048bit No >=2048bit Yes
31	Cryptographic primitive	Prime number generation	-	length of prime: 512 –	Method PRIME_GEN; Proprietary prime number	Not rated

No.	Purpose	Cryptographic Mechanism	Stdandard of Implementation	Key Size in Bits	Comments	Security Level above 100 Bits
				2112 Bits	generation method, which follows [PrimeGen]	
32	Cryptographic primitive	Generation of probable primes, Miller Rabin test	[FIPS186-4, B.3.3 / C.3.1]	length of prime: 512 – 2064 Bits	Method 2PRIME_GEN [N186-4] B.3.3: (only for prime Bitlength >= 1024; in case prime Bitlength < 1024 identical algorithm is used, but considered proprietary) [N186-4] C.3.1	Not rated for Bitlength of prime <1024bit
33	Cryptographic primitive	Primality test	-	length of prime: 512 – 2112 Bits	Method PRIME_CHECK; Proprietary primality test	not rated
34	Cryptographic primitive	Primality test	[FIPS186-4, C.3.1 / C.3.2]	length of prime: 512 – 2064 Bits	Method PRIME_CHECK_MASK	n/a
35	N/A	Supported elliptic curves: • All curves in [FIPS186-4], • All curves in [RFC5639].	[FIPS186-4] [RFC5639]	N/A	-	n/a
36	Cryptographic primitive	EC point addition on curves listed in #35	N/A	160 – 521	-	n/a
37	Authenticity	ECDSA signature generation on curves listed in #35[7]	[ANS X9.62, 7.3] [IEEE_P1363, 7.2.7]	160 – 521	-	Yes (for |k|≥224 bit)
38	Authenticity	ECDSA signature verification on curves	[ANS X9.62, 7.4.1]	160 –	-	Yes (for |

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

No.	Purpose	Cryptographic Mechanism	Stdandard of Implementation	Key Size in Bits	Comments	Security Level above 100 Bits
		listed in #35	[IEEE_P1363, 7.2.8]	521		k|≥224 bit)
39	Key agreement	Elliptic Curve Diffie-Hellman (ECDH) key agreement on curves listed in #35	[ANS X9.63, 5.4.1] [ISO_11770-3, D.6] [IEEE_P1363, 7.2.1]	160 – 521		Yes (for | k|≥224 bit)
40	Key generation	Elliptic Curve key generation on curves listed in #35	[ANS X9.62, A.4.3] [IEEE_P1363, A.16.9]	160 – 521	-	Yes (for | k|≥224 bit)
41	PACE integrated mapping	Point encoding for the ECDH-integrated mapping on curves listed in #35	[ICAO_11, B.2]	160 – 521	-	N/A
Flash Loader						
42	Confidentiality	#2 in CCM mode for encryption and decryption	[NIST SP800-38C]	128	-	Yes
43	Authenticity	#2 in CCM mode for MAC verification	[NIST SP800-38C]	128	-	Yes
44	Authentication	Mutual authentication protocol based on #43	[AGD_PPUM, 2.1.5]	128	-	Yes
45	Authentication	External authentication protocol based on #5	[AGD_PPUM, 2.1.5]	128	-	No
Random Number generation (Hardware)						
46	RNG	Physical RNG	PTG.2 in [AIS31]	N/A	-	n/a
47	RNG	Hybrid RNG	Corresponds to PTG.3 in [AIS31]	N/A	-	n/a
48	RNG	Deterministic RNG	Corresponds to DRG.3 in [AIS20]	N/A	-	n/a
49	RNG	Deterministic RNG	Corresponds to DRG.4 in [AIS31]	N/A	-	n/a
Random Crypto Library (RCL) v1.10.007						
50	RNG	Physical RNG	PTG.2 in [AIS31]	N/A	The RCL acts as interface to the PTG.2 hardware RNG	n/a
51	RNG	Deterministic RNG	Corresponds to DRG.3 in [AIS20]	128, 256	CTR_DRBG	n/a

No.	Purpose	Cryptographic Mechanism	Stdandard of Implementation	Key Size in Bits	Comments	Security Level above 100 Bits
			[NIST SP800-90A]			
52	RNG	Deterministic RNG	Corresponds to DRG.4 in [AIS31] [NIST SP800-90A]	128, 256	CTR_DRBG	n/a
Hash Crypto Library (HCL) v1.13.002						
53	Hash calculation	SHA-1	[FIPS180-4]	N/A	-	No
54	Hash calculation	SHA-224	[FIPS180-4]	N/A	-	n/a (keyless operation)
55	Hash calculation	SHA-256	[FIPS180-4]	N/A	-	n/a (keyless operation)
56	Hash calculation	SHA-384	[FIPS180-4]	N/A	-	n/a (keyless operation)
57	Hash calculation	SHA-512	[FIPS180-4]	N/A	-	n/a (keyless operation)
58	Hash calculation	SHA-512/224	[FIPS180-4]	N/A	-	n/a (keyless operation)
59	Hash calculation	SHA-512/256	[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.

Where no cryptographic 100-Bit-Level assessment was given at all (i.e where ”N/A” was stated), nevertheless the targeted CC Evaluation Assurance Level has been achieved for those functionalities as well.

In course of the evaluation process, a source code analysis was performed to compare the TOE implementation of the cryptographic functionality with the preconditions and steps defined in the referenced standards. The results of this analysis, including the deviations found by the evaluator and the conformance verification results were summarized in the [22] report. For the deviations, which are stated to be conformant to the referenced specifications, the evaluator confirms that the implementation is conformant with the referenced standard in the boundary conditions and operational environment of the TOE

and in sense of equivalent process as specified by Federal Information Processing Standards Publications, cf. [FIPS186-4]:

> *Equivalent process: Two processes are equivalent if, when the same values are input to each process (either as input parameters or as values made available during the process or both), the same output is produced.*

Reference of Legislatives and Standards quoted above:

[AIS20] Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 20, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3, 2013-05-15, Bundesamt für Sicherheit in der Informationstechnik

[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, December 21, 2011, American National Standards Institute

[AGD_PPUM] see reference [14] in bibliography (section 14)

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

[FIPS197] Federal Information Processing Standards Publication 197, Announcing the ADVANCED ENCRYPTION STANDARD (AES), 2001-11-26, National Institute of Standards and Technology (NIST)

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

[ISO_9797-1] Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher, 1999-12, ISO/IEC

[ISO_11770-3] ISO 11770-3: Information technology - Security techniques – Key management Part 3: Mechanisms using asymmetric techniques, ISO/IEC 11770-3:2008

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

[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 SP800-38B] NIST SP800-38B, Recommendation for Block Cipher Modes of Operation, The CMAC Mode for Authentication, 2005-05, National Institute of Standards and Technology (NIST)

[NIST SP800-38C] 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)

[NIST SP800-67] NIST Special Publication 800-67 – Revision 2, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher – Revised November 2017, 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

[RFC5639] RFC 5639 - Elliptic Curve Cryptography (ECC) Brainpool Standard Curves *and Curve Generation, IETF Trust and the persons identified as the document authors, March 2010 (http://www.ietf.org/rfc/rfc5639.txt)*

[PrimeGen] Details about Prime Number Generation, Infineon CCS Statement, Version 0.2, 2017-12-13

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.

In addition, the following aspects need to be fulfilled when using the TOE:

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 in [11],[12],[13],[14],[15],[16],[17], [18],[19],[20], [21] have to be considered.

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

• All security hints described in [14] 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 is required.

• The firmware flash loader requires either mutual authentication to establish a secure channel or a one-way authentication of the user without establishing a secure channel even though the communication is encrypted and integrity protected. This latter configuration does not satisfy the Loader Package 2.

• The TOE can come with a pre-loaded image called Performance Flash Loader, which is a non-TOE component. Using the PFL results in a non-certified product.

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
BPU	Bill per use
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
CPU	Central Processing Unit
cPP	Collaborative Protection Profile
CRC	cyclic redundancy check
DES	Data Encryption Standard
DRNG	Deterministic RNG
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ISS	Instruction Stream Signature Checking
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
MPU	Memory Protection Unit
NVIC	Nested Vectored Interrupt Controller
NVM	SOLID FLASH™ Memory
PFL	Performance Flash Loader
PP	Protection Profile
RAM	Read-Only Memory
RNG	Random Number Generator
ROM	Read only Memory
SAR	Security Assurance Requirement
SCP	Symmetric Cryptographic Processor
SFP	Security Function Policy
SFR	Security Functional Requirement
SPAU	System Peripheral Access Unit
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

13.2. Glossary

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

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

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

14. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

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

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[8] https://www.bsi.bund.de/AIS

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website, https://www.bsi.bund.de/zertifizierungsreporte

[6] Security Target BSI-DSZ-CC-1205-2023, Version 5.3, 2023-06-28, IFX_CCI_00006Ah,IFX_CCI_00006Bh, IFX_CCI_00006Ch S12 Security Target, Infineon Technologies AG (confidential document)

[7] Evaluation Technical Report, Version 3, 2023-08-11, EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY, TÜV Informationstechnik GmbH, (confidential document)

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

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

[9] Security Target Lite BSI-DSZ-CC-1205-2023, Version 5.3, 2023-06-28, IFX_CCI_00006Ah, IFX_CCI_00006Bh,IFX_CCI_00006Ch S12 Security Target Lite, Infineon Technologies AG (sanitised public document)

[10] ETR for composite evaluation according to AIS 36 for the Product IFX_CCI_00006Ah, IFX_CCI_00006Bh,IFX_CCI_00006Ch S12, Version 3, 2023-08-11, EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION (ETR COMP), TÜV Informationstechnik GmbH (confidential document)

[11] Guidance documentation for the TOE, Version 2, 2022-06-15, SLC39 32-bit Security Controller - V23, Hardware Reference Manual Infineon Technologies AG

[12] Guidance documentation for the TOE, Version 5.4, 2022-12-21, SLx1/SLx3 (40 nm) Security Controllers, Programmer's Reference Manual, Infineon Technologies AG

[13] Guidance documentation for the TOE, Version 1.00-2942, 2023-01-05, SLC39 32-bit Security Controller - V23, Security Guidelines, Infineon Technologies AG

[14] Guidance documentation for the TOE, Version 09.13, 2023-02-01, SLx3 (40nm) Security Controllers, Production and Personalization Manual, Infineon Technologies AG

[15] Guidance documentation for the TOE, Version 2.1, 2022-12-16, 32-bit Security Controller Crypto2304T V3 User Manual, Infineon Technologies AG

[16] Guidance documentation for the TOE, Version v3.52.9708, 2022-06-22, HSL for SLCx7 V23b, Hardware Support Library, Infineon Technologies AG

[17] Guidance documentation for the TOE, Version 01.30.0695, 2022-07-04, UMSLC library for SLCx7V23b User Mode Security Life Control, Infineon Technologies AG

[18] Guidance documentation for the TOE, Version 2.15.000, 2023-03-06, SCL37-SCP-v440-C40 Symmetric Crypto Library for SCP-v440 AES/DES/MAC, Infineon Technologies AG

[19] Guidance documentation for the TOE, Version 3.34.000, 2022-08-09, ACL37-Crypto2304T-C40 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox, Infineon Technologies AG

[20] Guidance documentation for the TOE, Version 1.10.007, 2020-06-16, RCL37-X-C40 Random Crypto Library for SCP-v440 & RNG-v3 DRBG/HWRNG 32-bit Security Controller, User interface manual, Infineon Technologies AG

[21] Guidance documentation for the TOE, Version 1.13.002, 2020-05-07, HCL37-CPU-C40 Hash Crypto Library for CPU SHA 32-bit Security Controller, User interface manual, Infineon Technologies AG

[22] Cryptographic Standards Compliance Verification, Version 2, 2022-13-09, TÜVInformationstechnik GmbH (confidential document)

[23] "Site Technical Audit Report (STAR) Infineon Technologies Sdn. Bhd., Melaka, Malaysia", Version 4, 2023-06-27, 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-1205-2023

Evaluation results regarding development and production environment

The IT product IFX_CCI_00006A, IFX_CCI_00006Bh, IFX_CCI_00006Ch design step S12 with firmware 80.311.04.1, optional NRG SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib 01.30.0695, optional SCL v2.15.000, optional ACL v3.34.000, optional RCL v1.10.007, optional HCL v1.13.002 and userguidance (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 28 August 2023, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.5, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_FLR.1, ALC_LCD.1, ALC_TAT.3).

The Site Technical Audit Reports (STAR) ([23]) is thus part of this certification procedure.

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

Distribution Center name	Company name and address
DHL Singapore	DHL Supply Chain Singapore Ptd Tampinese 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.

Note: End of report