Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0961-V4-2019

for

Infineon smart card IC (Security Controller) IFX_CCI_000007h, 000009h, 00000Ah, 00000Bh, 000016h, 000017h, 000018h, 000023h, 000024h, design step G13 with optional libraries CCL V02.00.0004, RSA2048/4096 V2.08.007 / V2.07.003 / V2.06.003, EC V2.08.007 / V2.07.003 / V2.06.003, Toolbox V2.08.007 / V2.07.003 / V2.06.003, HSL V03.12.8812 / V03.11.8339 / V02.01.6634 / V01.22.4346, SCL V2.04.002 / V2.02.010 and with specific IC dedicated software

from

Infineon Technologies AG

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

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0961-V4-2019 (*)

Infineon smart card IC (Security Controller) IFX_CCI_000007h, 000009h, 00000Ah, 00000Bh, 000016h, 000017h, 000018h, 000023h, 000024h, design step G13 with optional libraries CCL V02.00.0004, RSA2048/4096 V2.08.007 / V2.07.003 / V2.06.003, EC V2.08.007 / V2.07.003 / V2.06.003, Toolbox V2.08.007 / V2.07.003 / V2.06.003, HSL V03.12.8812 / V03.11.8339 / V02.01.6634 / V01.22.4346, SCL V2.04.002 / V2.02.010 and with specific IC dedicated software

SOGIS
Recognition Agreement

from	Infineon Technologies AG
PP Conformance:	Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 6 augmented by ALC_FLR.1

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, 18 December 2019

For the Federal Office for Information Security

Thomas Gast
Head of Branch

L.S.

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

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

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

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

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

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

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

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

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

2. Specifications of the Certification Procedure

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

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BSI Schedule of Costs[3]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[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 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

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

3. Recognition Agreements

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

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

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

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

The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.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+ ALC_FLR components.

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

4. Performance of Evaluation and Certification

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

The product Infineon smart card IC (Security Controller) IFX_CCI_000007h, 000009h, 00000Ah, 00000Bh, 000016h, 000017h, 000018h, 000023h, 000024h, design step G13 with optional libraries CCL V02.00.0004, RSA2048/4096 V2.08.007 / V2.07.003 / V2.06.003, EC V2.08.007 / V2.07.003 / V2.06.003, Toolbox V2.08.007 / V2.07.003 / V2.06.003, HSL V03.12.8812 / V03.11.8339 / V02.01.6634 / V01.22.4346, SCL V2.04.002 / V2.02.010 and with specific IC dedicated software has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0961-V3-2018. Specific results from the evaluation process BSI-DSZ-CC-0961-V3-2018 were re-used.

The evaluation of the product Infineon smart card IC (Security Controller) IFX_CCI_000007h, 000009h, 00000Ah, 00000Bh, 000016h, 000017h, 000018h, 000023h, 000024h, design step G13 with optional libraries CCL V02.00.0004, RSA2048/4096 V2.08.007 / V2.07.003 / V2.06.003, EC V2.08.007 / V2.07.003 / V2.06.003, Toolbox V2.08.007 / V2.07.003 / V2.06.003, HSL V03.12.8812 / V03.11.8339 / V02.01.6634 / V01.22.4346, SCL V2.04.002 / V2.02.010 and with specific IC dedicated software was conducted by T-Systems International GmbH. The evaluation was completed on 17 December 2019. T-Systems International 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

[5] Information Technology Security Evaluation Facility

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 18 December 2019 is valid until 17 December 2024. Validity can be re-newed by re-certification.

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 smart card IC (Security Controller) IFX_CCI_000007h, 000009h, 00000Ah, 00000Bh, 000016h, 000017h, 000018h, 000023h, 000024h, design step G13 with optional libraries CCL V02.00.0004, RSA2048/4096 V2.08.007 / V2.07.003 / V2.06.003, EC V2.08.007 / V2.07.003 / V2.06.003, Toolbox V2.08.007 / V2.07.003 / V2.06.003, HSL V03.12.8812 / V03.11.8339 / V02.01.6634 / V01.22.4346, SCL V2.04.002 / V2.02.010 and with specific IC dedicated software has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

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

B. Certification Results

The following results represent a summary of

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

1. Executive Summary

The TOE is named Infineon smart card IC (Security Controller) IFX_CCI_000007h, 000009h, 00000Ah, 00000Bh, 000016h, 000017h, 000018h, 000023h, 000024h, design step G13 with optional libraries CCL V02.00.0004, RSA2048/4096 V2.08.007 / V2.07.003 / V2.06.003, EC V2.08.007 / V2.07.003 / V2.06.003, Toolbox V2.08.007 / V2.07.003 / V2.06.003, HSL V03.12.8812 / V03.11.8339 / V02.01.6634 / V01.22.4346, SCL V2.04.002 / V2.02.010 and with specific IC dedicated software and is an integrated circuit (IC) in 65nm technology, providing a platform for an operating system and application software used in smartcards but also in any other device or form factor requiring a high level of resistance against attackers.

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

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 6 augmented by ALC_FLR.1.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [9], chapter 7. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Functionality	Addressed issue
SF_DPM	Device Phase Management
SF_PS	Protection against Snooping
SF_PMA	Protection against Modification Attacks
SF_PLA	Protection against Logical Attacks
SF_CS	Cryptographic Support

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] and [9], chapter 7.4 (Security Requirements Rationale).

The assets to be protected by the TOE are defined in the Security Target [6] and [9], chapter 4.1.2. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and [9], chapters 4.3, 4.1 and 4.2, respectively.

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

Within the Security Target [6] and [9], references to, and aspects of, GBIC (German Banking Industry Committee) are given. Unless Common Criteria relevant refinements are made to CC contents, these GBIC topics are to be regarded as parallel and independent of the CC certification.

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 smart card IC (Security Controller) IFX_CCI_000007h, 000009h, 00000Ah, 00000Bh, 000016h, 000017h, 000018h, 000023h, 000024h, design step G13 with optional libraries CCL V02.00.0004, RSA2048/4096 V2.08.007 / V2.07.003 / V2.06.003, EC V2.08.007 / V2.07.003 / V2.06.003, Toolbox V2.08.007 / V2.07.003 / V2.06.003, HSL V03.12.8812 / V03.11.8339 / V02.01.6634 / V01.22.4346, SCL V2.04.002 / V2.02.010 and with specific IC dedicated software.

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	IFX_CCI_000007h, IFX_CCI_000009h, IFX_CCI_00000Ah, IFX_CCI_00000Bh, IFX_CCI_000016h, IFX_CCI_000017h, IFX_CCI_000018h, IFX_CCI_000023h and IFX_CCI_000024h designstep G13. with dedicated firmware as given in the ST [6] and [9] (note: Firmware includes BOS, Flash Loader (with SCL) and RMS.)	HW-Version: G13 FW-Version 80.101.07.0, 80.101.07.1, 80.101.07.2	Complete modules, with or without inlay mounting, with or without inlay antenna mounting, plain wafers, in any IC case (e.g. TSSOP28, VQFN32, VQFN40, CCS-modules, etc.), in no IC case or package, simply as bare dies or arbitrary type of package. The firmware is stored in reserved areas of ROM and NVM memories.
2	SW	Libraries (to be chosen optionally and individually):		Object code (electronic data in lib format)
		RSA2048,	V2.06.003, V2.07.003, V2.08.007	
		RSA4096,	V2.06.003 , V2.07.003, V2.08.007	

No	Type	Identifier	Release	Form of Delivery
		EC,	V2.06.003, V2.07.003, V2.08.007	
		Toolbox (not in scope of evaluation),	V2.06.003, V2.07.003, V2.08.007	
		HSL,	V01.22.4346 or V02.01.6634 or V03.11.8339	
		SCL,	V2.02.010 or V2.04.002	
		CIPURSE™ CL	V2.0.0004.	
3	Doc	16-bit Security Controller – V02 Errata sheet [13]	Rev. 6.0, Infineon, 2019-06-19	Document in electronic form
4	Doc	16-bit Security Controller – V02 Hardware Reference Manual [12]	Rev. 5, Infineon, 2019-06-13	Document in electronic form
5	Doc	16-Bit Security Controller - V02, Security Guidelines [11]	Rev. 1.01-1958, Infineon, 2018-10-24	Document in electronic form
6	Doc	CIPURSE™ Crypto Library, CCL52_SCP_v4 v2.0.0004, CIPURSE™ V2, Compliant to OSPT™ Alliance CIPURSE™ V2 Cryptographic Protocol, User Interface [19]	Rev. 1.6, 2018-02-02	Document in electronic form
7	Doc	CL52 Asymmetric Crypto Library for Crypto@2304T, RSA/ECC/Toolbox, 16-bit Security Controller, User Interface [14]	Rev. 2.07.003, Infineon, 2019-04-25	Document in electronic form
8	Doc	CL52 Asymmetric Crypto Library for Crypto@2304T, RSA/ECC/Toolbox, 16-bit Security Controller, User Interface (with included Errata Sheet of 10th May 2017) see also [14]	Rev. 2.06.003, Infineon, 2019-04-25	Document in electronic form

No	Type	Identifier	Release	Form of Delivery
	Doc	ACL52-Crypto2304T-C65 Asymmetric Crypto Library RSA / ECC / Toolbox	Rev. 2.08.007, Infineon, 2019-04-25	Document in electronic form
9	Doc	Crypto@2304T V3 User manual [15]	Rev. 1.4.1, Infineon, 2014-11-10	Document in electronic form
10	Doc	Hardware Support Library for SLCx2 (HSL) as active document [18]	1st version: Rev. 01.22.4346, 2016, Infineon and 2nd version: Rev. 02.01.6634, 2017, Infineon and 3rd version: Rev. 03.11.8339, 2018-07-12 and Rev. 03.12.8812, 2018-11-23	Document in electronic form
11	Doc	Production and Personalization, 16-bit Security Controller in 65 nm [17]	Rev. 3.6, Infineon, 2019-06-24	Document in electronic form
12	Doc	16-bit Security Controller 65-nm Technology, Programmer's Reference Manual [16]	Rev. 9.12, Infineon, 2019-07-14	Document in electronic form
14	Doc	SCL52 Symmetric Cryptogaphic Library for DES / AES, 16-bit Security Controller, User Interface (2.02.010) [20]	Version 2.02.010, Infineon, 2016-12-09	Document in electronic form
		SCL52 Symmetric Cryptogaphic Library for DES / AES, 16-bit Security Controller, User Interface (2.04.002) [20]	Version 2.04.002, Infineon, 2018-01-15	

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.

Furthermore, 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.

Three different delivery procedures have to be taken into consideration:

- Delivery of the IC dedicated software components (IC dedicated SW, guidance) from the TOE Manufacturer to the IC Embedded Software Developer.
- Delivery of the IC Embedded Software (ROM / Flash data, initialisation and pre-personalisation data) from the IC Embedded Software Developer to the TOE Manufacturer.
- Delivery of the final TOE from the TOE Manufacturer to the Composite Product Manufacturer. After phase 3 the TOE is delivered in form of wafers or sawn wafers, after phase 4 in form of modules (with or without inlay antenna).

Respective distribution centers are listed in Appendix B (see below).

The individual TOE hardware is uniquely identified by its identification data. The identification data contains the CCI (Common Criteria identifier), 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_000007h, IFX_CCI_000009h, IFX_CCI_00000Ah, IFX_CCI_00000Bh, IFX_CCI_000016h, IFX_CCI_000017h, IFX_CCI_000018h, IFX_CCI_000023h and IFX_CCI_000024h design step G13.

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

At TOE start-up the so called GCIM can be chosen by applying special signalling in contactless or contact based communication and the TOE outputs then the generic chip identification data. This data contain the firmware identifier accompanied with the certification identifier, the design step and even more tracking information. In combination with [12] (section 6.5) the user can identify the data, interpret it and retrieve the TOE versioning information. This information includes also the required mapping of firmware identifier and certification identifier.

The optional software libraries can be identified by calculating a hash value (e.g. SHA-256) over the delivered lib-files (.lib) and comparing the calculated vales to the values stated in Security Target [6] and [9], section 11.

Please also note, that 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.

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE.

It provides basic security functionalities to be used by a smart card operating system and a smart card application, thus providing an overall smart card system security. Therefore, the TOE implements a symmetric cryptographic block cipher algorithm (Triple-DES and AES) to ensure the confidentiality of plain text data by encryption and to support implementations of secure authentication protocols.

It furthermore provides a True Random Number Generator (TRNG), Hybrid Random Generator (HRNG), and Deterministic Random Number Generator (DRNG).

The RSA Library is used to provide a high level interface to RSA (Rivest, Shamir, Adleman) cryptography implemented on the core and on the hardware asymmetric coprocessor 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 core and on hardware asymmetric coprocessor and includes countermeasures against SPA, DPA and DFA attacks.

As the TOE is a hardware security platform, the security policy of the TOE is also to provide protection against leakage of information (e.g. to ensure the confidentiality of cryptographic keys during AES, 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.

The TOE as well implements user manageable memory access control policy. The security policy of memory access control policy has been formally modelled. The formal model covers further security policies.

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.

Regarding the operational environment of the TOE the security objectives OE.Resp-Appl (Treatment of User Data of the Composite TOE), and OE.Process-Sec-IC (Protection during composite product manufacturing), OE.Lim_Block_Loader (Limitation of capability and blocking the Loader), OE.TOE_Auth (External entities authenticating of the TOE) and OE.Loader_Usage (Secure communication and usage of the Loader) are relevant for the user in context of secure installation of the TOE and the secure preparation of the operational environment. All objectives are properly covered by user guidance.

5. Architectural Information

The TOE is an integrated circuit (IC) providing a platform for an operating system and application software used in smartcards but also in any other device or form factor requiring a high level of resistance against attackers. A top level block diagram and a list of subsystems can be found within the TOE description of the Security Target [6] and [9], chapter 2.1.

The TOE provides a real 16-bit CPU-architecture and is compatible to the Intel 80251 architecture.

The major components of the core system are the two CPUs (Central Processing Units), the MMU (Memory Management Unit) and MED (Memory Encryption/Decryption Unit). The two CPUs control each other in order to detect faults and serve by this for data integrity. The TOE implements a linear addressable memory space for each privilege level and a simple scalable Memory Management concept. The flexible memory concept consists of ROM- and Flash-memory as part of the non volatile memory (NVM). There is no user available on-chip ROM module. The user software and data are now located in a dedicated and protected part of the NVM.

The two cryptographic co-processors serve the need of modern cryptography: The symmetric co-processor (SCP) combines both AES and Triple-DES with dual-key or triple-key hardware acceleration. The Asymmetric Crypto Co-processor is used for RSA and Elliptic Curve (EC) cryptography.

The software part of the TOE consists of the cryptographic CIPURSE™, EC-, RSA- and symmetric cryptography libraries and the supporting Toolbox libraries.

The Flash Loader is a firmware located in the ROM and enables the download of the user software or parts of it to the NVM. After completion of the download and before delivery the final user the Flash Loader shall be locked by the user.

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 can be divided into following categories:

- technology development tests as the earliest tests to check the technology against the specification and to get the technology parameters used in simulations of the circuitry (this testing is not strictly related to Security Functions),
- tests which are performed in a simulation environment for analogue and for digital simulations,
- regression tests which are performed for the IC Dedicated Test Software (optional software libraries) and for the IC Dedicated Support Software (BOS) on emulator versions of the TOE or within the simulation of chip in special hardware, or on final hardware and firmware,
- qualification tests to release the TOE to production:
  - used to determine the behaviour of the chip with respect to different operating conditions and varied process parameters (often also referred to as characterisation tests)
  - special verification tests for Security Functions which were done with samples of the TOE (referred also as developers security evaluation) and which include also layout tests by automatic means and optical control, in order to verify statements concerning the layout;

- functional production tests, which are done for every chip to check its correct functionality as a last step of the production process (phase 3 or phase 4 depending on the TOE delivery form).

The developer tests cover all Security Functions and all security mechanisms as identified in the functional specification, and in the high and low level designs.

The evaluators were able to repeat the tests of the developer either using the library of programs, tools and prepared chip samples delivered to the evaluator or at the developer's sites. They performed independent tests to supplement, augment and to verify the tests performed by the developer by sampling or by complete repetition of regression tests especially for the software. Besides repeating exactly the developer's tests, test parameters and test equipment are varied and additional analysis was done. 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 developer has tested the TOE. In cases that different configurations were tested, the evaluators assessed the validity of test results for the TOE.

The evaluators supplied evidence that the actual version of the TOE provides the Security Functions as specified by the developer. The test results confirm the correct implementation of the TOE Security Functions.

For penetration testing the evaluators took all Security Functions into consideration. Intensive penetration testing was planed based on the analysis results and performed for the underlying mechanisms of Security Functions using bespoke equipment and expert know how. The penetration tests considered both the physical tampering of the TOE and attacks which do not modify the TOE physically (i.e. DPA/SPA testing).

The evaluators have tested the TOE. In cases that different configurations were tested, the evaluators assessed the validity of test results for the TOE.

8. Evaluated Configuration

The evaluated derivate of the TOE is IFX_CCI_000007h (with options/other identifiers, see below), G13 with firmware and optional software libraries (CCL, RSA2048 2k and 4k, EC, Toolbox, HSL, SCL) with revisions stated in section 2. The flash loader (part of FW) was enabled on evaluated derivative.

The BPU feature was not used. All hardware modules and all interfaces incl. options were activated and the ranges of available memories was not limited (i.e. maximum size was available). The system frequency was set at its maximum value. The derivative was manufactured in wafer fab Tainan, Taiwan.

An extensive overview over all possible configuration options is given in the Security Target [6] and [9] in table 4.

The evaluation results, also including results of tests performed by the developer, are valid for all hardware derivates of the configuration IFX_CCI_000007h, G13 (including all further identifiers 000009h, 00000Ah, 00000Bh, 000016h, 000017h, 000018h, 000023h, 000024h in design step G13). 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 (RSA2048 2k and 4k, EC, Toolbox, HSL, SCL 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 table 4 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, e.g. the RAM size shall be selected to fulfill the minimum requirement of RSA library, if it was also selected as an option. The evaluation results apply to all configurations of Flash Loader, BPU and PIN-Letter as stated in table 3 of 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.

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:

- AIS1, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers, Version 13, BSI, 2008-08-14,
- AIS14, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 7, BSI, 2010-08-03,
- AIS19, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria) und ITSEC, Version 9, BSI, 2014-11-03,
- AIS20, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3.0, BSI, 2013-05-15,
- AIS20-Part Functionality Classes and Evaluation Methodology for Deterministic Random Number Generators, Part of AIS20, Version 3.0, BSI, 2013-05-15,
- AIS20-Part Deterministic Random Number Generator, Part of AIS20, Version 0.10, BSI, 2013-02-28,
- AIS25, Anwendung der CC auf Integrierte Schaltungen, Version 8, BSI, 2013-02-13,
- AIS25-Part The Application of CC to Integrated Circuits, Part of AIS25, JIL, version 3.0, 02-2009,
- AIS25-JIL JIL-HW-ADV_ARCSecurity Architecture requirements (ADV_ARC) for smart cards and similar devices, Version 2.0, JIL, 01-2012,
- AIS26, Evaluationsmethodologie für in Hardware integrierte Schaltungen, Version 9, BSI, 2013-03-21,
- AIS26-Part Application of Attack Potential to Smartcards, Version 2.9, JIL, 01-2013,

- AIS26-Part Attack Methods for Smartcards and Similar Devices, Version 2.2, JIL, 01-2013,
- AIS31, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3.0, BSI, 2013-05-15,
- AIS31-Part A proposal for: Functionality classes and evaluation methodology for true (physical) random number generators, Part of AIS31, Version 3.1, BSI, 2001-09-25,
- AIS31-Part A proposal for: Functionality classes for random number generators, Part of AIS31, Version 2.00, BSI, 2011-09-18,
- AIS31-Part True Physical and Hybrid Random Number Generator, Part of AIS31, Version 0.7, BSI, 2013-02-28,
- AIS39 Guideline for the Development and Evaluation of formal security policy models in the scope of ITSEC and Common Criteria, Part of AIS39, Version 2.0, BSI, 2007-12-04,
- AIS46, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren, Version 3, BSI, 2013-12-04,
- AIS46-Part Minimum Requirements for Evaluating Side-Channel Attack Resistance of Elliptic Curve Implementations, Part of AIS46, Version 1.0.4, BSI, 2011-07-01,
- AIS46-Part Methodology for cryptographic rating of memory encryption schemes used in smartcards and similar devices, Part of AIS46, Version 1.0, BSI, 2013-10-31,
- AIS46-Part Minimum Requirements for Evaluating Side-Channel Attack Resistance of RSA, DSA and Diffie-Hellman Key Exchange Implementations, Part of AIS46, Version 1.0, BSI, 2013-01-14.

For the non-technology specific aspects, the following guidances apply:

- AIS32, CC-Interpretationen im deutschen Zertifizierungsschema, Version 6, BSI, 2011-06-08,
- AIS34, Evaluation Methodology for CC Assurance Classes for EAL5+, Version 3, BSI, 2009-09-06,
- AIS35, Öffentliche Fassung eines Security Target (ST-lite), Version 2, BSI, 2007-11-12,
- AIS35-Part ST sanitising for publication, Part of AIS35, CCDB-2006-04-004, Version 1.0, 2006-04,
- AIS36, Kompositionsevaluierung, Version 4, BSI, 2013-05-15,
- AIS36-Part Composite product evaluation for Smart Cards and similar devices, Part of AIS36, Version 1.2, JIL, 01-2012,
- AIS36-Part template for composite evaluation of Smart Cards and similar devices, Part of AIS36, Version 1.0, Revision 1, CCDB-2007-09-002, 09-2007,
- AIS38, Wiederverwendung von Evaluationsergebnissen, Version 2, BSI, 2007-09-28,
- AIS39, Formal Method, Version 3.0, BSI, 2008-10-24,

(see [4] for respective AIS references).

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

The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE. Please note that those parts, which are to be read in the GBIC

context, are solely relevant in the GBIC context and not in the CC context (hence for CC these are out of scope).

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.

This is a re-certification based on BSI-DSZ-CC-0961-V3-2018.

The evaluation has confirmed:

- PP Conformance: Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014 [8]
- for the Functionality: PP conformant plus product specific extensions Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant EAL 6 augmented by ALC_FLR.1

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

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

9.2. Results of cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But cryptographic functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

The following table (which originates from the ITSEF-evaluated table in [21] and in this certification report is enhanced by the 100 bit column) provides an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its rating from cryptographic point of view. Any Cryptographic Functionality that is marked in column '*Security Level above 100 Bits*' of the following table with '*no*' achieves a security level of lower than 100 Bits (in general context) only.

Purpose / Service	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
Symmetric Cryptographic Co Processor				
	TDES in modes			
	ECB	[S21], [S30]	|k| = 112, 168	No
	CBC	[S20], [S21], [S30]	|k| = 112, 168	168: Yes,

Purpose / Service	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
				112: No
	CBC-MAC	[S20], [S21], [S30], [S32]	|k| = 112, 168	No
	CBC-MAC-ELB	[S20], [S21], [S30], [S32]	|k| = 112, 168 + key length for ELB	No
	AES in modes			
	ECB	[S21], [S30], [S31]	|k| = 128, 192, 256	No
	CBC	[S21], [S30], [S31]	|k| = 128, 192, 256	Yes
	CBC-MAC	[S20], [S21], [S30], [S32]	|k| = 128, 192, 256	No
	CBC-MAC-ELB	[S20], [S21], [S30], [S32]	|k| = 128, 192, 256 + key length for ELB	No
Symmetric Cryptographic Libraries (v02.04.002 + v02.02.010)				
	AES in modes			
	ECB	[S31], modes in [S21]	|k| = 128, 192, 256	No
	CBC, CTR, CFB	[S31], modes in [S21]	|k| = 128, 192, 256	Yes
	PCBC (encryption)	[S31], [S36]	|k| = 128, 192, 256	Yes
	PCBC (authenticated enc)	[S31], [S36]	|k| = 128, 192, 256	No
	TDES / TDEA in modes			
	ECB	[S20], modes in [S21]	|k| = 112 and 168 bits	No
	CBC, CTR and CFB	[S20], modes in [S21]	|k| = 112 and 168 bits	168: Yes, 112: No
	PCBC (encryption)	[S20], [S36]	|k| = 128, 192, 256	168: Yes, 112: No
	PCBC (authenticated enc)	[S20], [S36]	|k| = 128, 192, 256	No
	CMAC			
	AES-CMAC	[S21], [S30], [S31], [S37]	|k| = 128, 192, 256	No
	TDES-CMAC	[S20], [S21], [S30], [S37]	|k| = 168	No
Random Number Generation				
	Hybrid Physical True Random Number Generation	[S13]	N/A	N/A
RSA library v2.06.003 + v2.07.003 + v2.08.007				

Purpose / Service	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
	RSA encryption	[S22], [S29]	Modulus length 1976 – 4096 (please note specifics for the RSA2k and RSA4k libraries)	Yes
	RSA decryption with and without CRT	[S22], [S29]	Modulus length 1976 – 4096 (please note specifics for the RSA2k and RSA4k libraries)	Yes
	RSA signature generation with and without CRT	[S22], [S29]	Modulus length 1976 – 4096 (please note specifics for the RSA2k and RSA4k libraries)	Yes
	RSA signature verification (only modular exponentiation part)	[S22], [S29]	Modulus length 1976 – 4096 (please note specifics for the RSA2k and RSA4k libraries)	Yes
EC libraries v2.06.003 + v2.07.003 + v2.08.007				
	ECDSA signature generation and verification	[S19], [S23], [S26], [S27], [S29]	Key sizes corresponding to the used elliptic curves [S26]: P-{192, 224, 256, 384, 521}, K-{163, 233, 283, 409}, B-{163, 233, 283, 409}; [S19]: P{160, 192, 224, 256, 320, 384, 512}t1, P{160, 192, 224, 256, 320, 384, 512}r1	Generation: No Verification: Yes
	ECDH key agreement	[S19], [S24], [S26], [S28], [S29]	Key sizes corresponding to the used elliptic curves [S26]: P-{192, 224, 256, 384, 521}, K-{163, 233, 283, 409}, B-{163, 233, 283, 409}; [S19]: P{160, 192, 224, 256, 320, 384, 512}t1, P{160, 192, 224, 256, 320, 384, 512}r1	Yes
CIPURSE™				
	CIPURSE™ Session Key Agreement AES	[S35-1], [S35-2] Sections 5.2 and 6.2	AES $\|K_0\|$ = 128 bits	Yes
	CIPURSE™ Authentication AES	[S21], [S31], [S35-1], [S35-2] Section 5.3	AES $\|K_0\|$ = 128 bits	Yes
	CIPURSE™ Secure Messaging for Integrity	[S21], [S31], [S35-1], [S35-2] Sections 5.3 and 6.3	MAC based on AES $\|K_0\|$ = 128 bits	No
	CIPURSE™ Secure Messaging for Confidentiality	[S21], [S31], [S35-1], [S35-2] Section 6.3	AES $\|K_0\|$ = 128 bits	Yes

Table 3: TOE cryptographic functionality

In addition to, the following rating applies regarding RSA key generation:

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
Key Generation (ACL v2.07.003 + v2.08.007)	RSA Key Generation in ACL v2.07.003 + v2.08.007, utilizing the preparative function “CryptoGeneratePrime()” or the function “CryptoRSAKeyGen()”	n/a	1976 - 4096	Yes

Table 4: TOE cryptographic functionality

For the Cryptographic Functionalities

- CryptoGeneratePrimeMask() which might be used in conjunction with RSA Key Generation in ACL **v2.07.003** and **v2.08.007**,
- CryptoRSAKeyGen(), CryptoGeneratePrime() or CryptoGeneratePrimeMask() of ACL **v2.06.003**

no statement on the respective cryptographic strength is given.

Please note that in ACL v2.06.003 the function CryptoGeneratePrime() is not in scope of the evaluation and thus not included in the certificate.

The Flash Loader's cryptographic strength was also not assessed by BSI. However, the evaluation according to the TOE's Evaluation Assurance Level did not reveal any implementation weaknesses.

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

The developer evidence [21] lists the cryptograhic functionalities used and provided by the TOE.

Reference of Legislatives and Standards quoted above:

[S19] RFC 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, IETF Trust and the persons identified as the document authors, March 2010

[S20] National Institute of Standards and Technology (NIST), Special Publication 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Revised January 2012, Technology Administration, U.S. Department of Commerce, 2012-01, 800-67 Rev. 1

[S21] National Institute of Standards and Technology(NIST), Technology Administration, US Department of Commerce, NIST Special Publication SP 800-38A (for AES and DES), SP800-38A, 2001-12

[S22] PKCS #1 v2.2: RSA Cryptography Standard, RSA Laboratories, PKCS #1 v2.2, 2012-10-27

[S23] American National Standard for Financial Services ANSI X9.62-2005, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital

Signature Algorithm (ECDSA), American National Standards Institute, ANSI X.9.62, 2005-11-16

[S24] ANSI X.9.63, 2011-12-21, 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, American National Standards Institute

[S26] FIPS Pub 186-4, 2013-07, Federal Information Processing Standards Publication, FIPS PUB 186-4, Digital Signature Standard (DSS), U.S. Department of Commerce, National Institute of Standards and Technology (NIST)

[S27] ISO/IEC 14888-3 2006, published 2009-02-15, INTERNATIONAL STANDARD ISO/IEC 14888-3:2006, TECHNICAL CORRIGENDUM 2, Published 2009-02-15, Information technology — Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms

[S28] ISO/IEC 11770-3 2008, published 2009-09-15, INTERNATIONAL STANDARD ISO/IEC 11770-3:2008, TECHNICAL CORRIGENDUM 1, Published 2009-09-15, Information technology — Security techniques —Key management — Part 3: Mechanisms using asymmetric techniques

[S29] IEEE 1363 2000-01-30 (approved), IEEE Standard Specification for Public key Crytography, IEEE Standards Board. The standard covers specification for public key cryptography including mathematical primitives for secret value deviation, public key encryption and digital signatures and cryptographic schemes based on those primitives.

[S30] ISO/IEC 18033 2005, ISO/IEC 18033-3: 2005, Information technology – Security techniques - Encryption algorithms - Part 3: Block ciphers [18033]

[S31] FIPS 197 2001-11-26, Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTION STANDARD (AES), U.S. DEPARTMENT OF COMMERCE / National Institute of Standards and Technology, November 26, 2001

[S32] ISO/IEC 9797-1 2011-03-01, ISO/IEC 9797-1: 2011, Information technology – Security techniques - Message Authentication Codes (MACs) Part 1 Mechanisms using a block cipher

[S36] PCBC mode, 1996, Bruce SCHNEIER, Applied Cryptography, Second Edition, John Wiley & Sons,1996

[S37] SP800-38B 2005 with update 2016-10-03, National Institute of Standards and Technology(NIST), Technology Administration, US Department of Commerce, NIST Special Publication SP 800-38B (for CMAC Mode for Authentication)

[S35-1] CIPURSE™ V2 Cryptographic Protocol issued by the OSPT™ Alliance, v1.0, 2012-09-28

[S35-2] CIPURSE™ V2 Cryptographic Protocol issued by the OSPT™ Alliance with Errata and Precision List, v1.1, 2014-09-19

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 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, all the instructions in the following user guidance documents shall be considered when using the TOE (see also section 13 below, bibliography):

- see documents [11] – [20].

The fulfilment of security objectives for the environment from the Security Target, [6] and [9] shall be ensured as well.

11. Security Target

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

12. Regulation specific aspects (eIDAS, QES)

None

13. Definitions

13.1. Acronyms

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

13.2. Glossary

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

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

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

14. Bibliography

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

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

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

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[7] https://www.bsi.bund.de/AIS

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

[6] Confidential Security Target for BSI-DSZ-CC-0961-V4-2019, Version 2.1, 2019-07-22, “Confidential Security Target IFX_CCI_000007h, IFX_CCI_000009h, IFX_CCI_00000Ah, IFX_CCI_00000Bh, IFX_CCI_000016h, IFX_CCI_000017h, IFX_CCI_000018h, IFX_CCI_000023h, IFX_CCI_000024h, design step G13”, Infineon Technologies AG (confidential document)

[7] Evaluation Technical Report for the Product BSI-DSZ-CC-0961-V4-2019, v4.00, 2019-08-15, “Evaluation Technical Report - Summary”, T-Systems International GmbH, (confidential document)

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

[9] Public Security Target BSI-DSZ-CC-0961-V4-2019, Version 1.7, 2019-07-22, “Public Security Target IFX_CCI_000007h, IFX_CCI_000009h, IFX_CCI_00000Ah, IFX_CCI_00000Bh, IFX_CCI_000016h, IFX_CCI_000017h, IFX_CCI_000018h, IFX_CCI_000023h, IFX_CCI_000024h, design step G13”, Infineon Technologies AG (sanitised public document)

[7] See section 9.1 for details on used AIS

[10] ETR for composite evaluation according to AIS 36 for BSI-DSZ-CC-0961-V4-2019, Version 4.00, 2019-08-06, ETR for composite evaluation (EFC), T-Systems International GmbH (confidential document)

[11] 16-Bit Security Controller - V02, Security Guidelines, Rev. 1.01-1958, Infineon Technologies AG, 2018-10-24

[12] 16-bit Security Controller – V02 Hardware Reference Manual, Rev. 5, Infineon Technologies AG, 2019-06-13

[13] 16-bit Security Controller – V02 Errata sheet, Rev. 6.0, Infineon Technologies AG, 2019-06-19

[14] “CL52 Asymmetric Crypto Library for Crypto@2304T RSA/ECC/Toolbox” with included Errata Sheet of 10th May 2017, Rev. 2.06.003, Infineon Technologies AG, 2019-04-25

and

“CL52 Asymmetric Crypto Library for Crypto@2304T RSA/ECC/Toolbox”, Rev. 2.07.003, Infineon Technologies AG, 2019-04-25

and

“ACL52-Crypto2304T-C65 Asymmetric Crypto Library RSA / ECC / Toolbox”, Rev.2.08.007, Infineon Technologies AG, 2019-04-25

[15] Crypto@2304T V3 User manual, Rev. 1.4.1, Infineon Technologies AG, 2014-11-10

[16] 16-bit Security Controller 65-nm Technology, Programmer's Reference Manual, Rev. 9.12, Infineon Technologies AG, 2019-07-14

[17] Production and Personalization, 16-bit Security Controller in 65 nm, Rev. 3.6, Infineon Technologies AG, 2019-06-24

[18] Hardware Support Library (HSL), chm-file, Rev. 01.22.4346 (as of 2016), Infineon Technologies AG

and

Hardware Support Library (HSL), chm-file, Rev. 02.01.6634 (as of 2017), Infineon Technologies AG

and

Hardware Support Library (HSL), chm-file, Rev. 03.11.8339 (as of 2018-07-12), Infineon Technologies AG

and

Hardware Support Library (HSL), chm-file, Rev. 03.12.8812 (as of 2018-11-23), Infineon Technologies AG

[19] “CIPURSE™ Crypto Library, CCL52_SCP_v4 v2.0.0004, CIPURSE™ V2, Compliant to OSPT™ Alliance CIPURSE™ V2 Cryptographic Protocol, User Interface”, Version 1.6, Infineon Technologies AG, 2018-02-02

[20] “SCL52 Symmetric Cryptogaphic Library for DES / AES, 16-bit Security Controller, User Interface”, Version 2.02.010, 2016-12-09, Infineon Technologies AG

and

“SCL52 Symmetric Cryptogaphic Library for DES / AES, 16-bit Security Controller, User Interface”, Version 2.04.002, 2018-01-15, Infineon Technologies AG

[21] “Cryptographic Mechnisms 7h with options”, 2018-08-14, 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 detailled 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-0961-V4-2019

Evaluation results regarding development and production environment

The IT product Infineon smart card IC (Security Controller) IFX_CCI_000007h, 000009h, 00000Ah, 00000Bh, 000016h, 000017h, 000018h, 000023h, 000024h, design step G13 with optional libraries CCL V02.00.0004, RSA2048/4096 V2.08.007 / V2.07.003 / V2.06.003, EC V2.08.007 / V2.07.003 / V2.06.003, Toolbox V2.08.007 / V2.07.003 / V2.06.003, HSL V03.12.8812 / V03.11.8339 / V02.01.6634 / V01.22.4346, SCL V2.04.002 / V2.02.010 and with specific IC dedicated software (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations 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 18 December 2019, 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) are fulfilled for the development and production sites of the TOE.

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

Distribution Center name	Address
Kühne & Nagel	Stockstädter Straße 10 – Building 8A, 63762 Großostheim, Germany
DCH KWE Kintetsu World Express	DCH KWE Kintetsu World Express (China) Co., Ltd., Building A5 Unit 1/6 & 1/9, Infineon Distribution Center China, Shanghai Pudong Airport Pilot Free Trade Zone, No.530 Zheng Ding Road, Shanghai, P.R. China
IFX Morgan Hill	Infineon Technologies North America Corp., 18275 Serene Drive, Morgan Hill, CA 95037, USA
DHL Singapore	DHL Supply Chain Singapore Pte. Ltd., Infineon Distribution Center Asia, Tampines LogisPark, 1 Greenwich Drive, Singapore 533865

Distribution Center name	Address
G&D Neustadt	DHL Supply Chain Singapore Pte. Ltd., Infineon Distribution Center Asia, Tampines LogisPark, 1 Greenwich Drive, Singapore 533865

Table 5: TOE Distribution Centers

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