Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0961-2017

for

IFX_CCI_000007h, IFX_CCI_000009h, IFX_CCI_00000Ah, IFX_CCI_00000Bh, IFX_CCI_000016h, IFX_CCI_000017h, IFX_CCI_000018h, design step G13 including optional software libraries and dedicated firmware

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-0961-2017 (*)

IFX_CCI_000007h, IFX_CCI_000009h, IFX_CCI_00000Ah, IFX_CCI_00000Bh, IFX_CCI_000016h, IFX_CCI_000017h, IFX_CCI_000018h, design step G13 including optional software libraries and dedicated firmware

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

SOGIS
Recognition Agreement
for components up to
EAL 4

Common Criteria

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 4

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.

Common Criteria
Recognition Arrangement
for components up to
EAL 4

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.

Bonn, 10 July 2017

For the Federal Office for Information Security

Bernd Kowalski
Head of Department

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.

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.

[1] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

Contents

A. Certification

1. 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[2]
- BSI Certification and Approval Ordinance[3]
- BSI Schedule of Costs[4]
- 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[5] [1] also published as ISO/IEC 15408.
- 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]

2. 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.

2.1. European Recognition of ITSEC/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.

[2] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

[3] 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

[4] 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

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

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). 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 new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. 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.sogisportal.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

This certificate is recognized under SOGIS-MRA for all assurance components selected.

2.2. 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 CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification) of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://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 nations listed above.

As the product certified has been accepted into the certification process before 08 September 2014, this certificate is recognized according to the rules of CCRA-2000, i.e. up to and including CC part 3 EAL 4 components. The evaluation contained the components ADV_FSP.5, ADV_IMP.2, ADV_INT.3, ADV_SPM.1, ADV_TDS.5, ALC_CMC.5, ALC_CMS.5, ALC_DVS.2, ALC_TAT.3, ATE_COV.3, ATE_DPT.3, ATE_FUN.2 and AVA_VAN.5 that are not mutually recognised in accordance with the provisions of the CCRA-2000, for mutual recognition the EAL 4 components of these assurance families are relevant.

3. 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_000007h, IFX_CCI_000009h, IFX_CCI_00000Ah, IFX_CCI_00000Bh, IFX_CCI_000016h, IFX_CCI_000017h, IFX_CCI_000018h, design step G13 including optional software libraries and dedicated firmware has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0891-2015. Specific results, mainly regarding ALC aspects of the evaluation process BSI-DSZ-CC-0891-2015 were re-used.

The evaluation of the product IFX_CCI_000007h, IFX_CCI_000009h, IFX_CCI_00000Ah, IFX_CCI_00000Bh, IFX_CCI_000016h, IFX_CCI_000017h, IFX_CCI_000018h, design step G13 including optional software libraries and dedicated firmware was conducted by T-Systems International GmbH. The evaluation was completed on 03.07.2017. T-Systems International GmbH is an evaluation facility (ITSEF)[6] 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.

4. Validity of the Certification Result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only 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 levels please refer to the excerpts from the criteria at the end of the Certification Report or in the CC itself.

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-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 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 10 July 2017 is valid until 9 July 2022. Validity can be re-newed by re-certification.

[6] 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.

5. Publication

The product IFX_CCI_000007h, IFX_CCI_000009h, IFX_CCI_00000Ah, IFX_CCI_00000Bh, IFX_CCI_000016h, IFX_CCI_000017h, IFX_CCI_000018h, design step G13 including optional software libraries and dedicated firmware 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[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] Infineon Technologies AG
Am Campeon 1-12
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 IFX_CCI_000007h, IFX_CCI_000009h, IFX_CCI_00000Ah, IFX_CCI_00000Bh, IFX_CCI_000016h, IFX_CCI_000017h, IFX_CCI_000018h, design step G13 including optional software libraries and dedicated firmware 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:

IFX_CCI_000007h, IFX_CCI_000009h, IFX_CCI_00000Ah, IFX_CCI_00000Bh, IFX_CCI_000016h, IFX_CCI_000017h, IFX_CCI_000018h, design step G13 including optional software libraries and dedicated firmware.

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 and IFX_CCI_000018h design step G13. Firmware includes BOS, Flash Loader (with SCL), and RMS.	HW-Version: G13 FW-Version 80.101.07.0	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): RSA2048, RSA4096, EC, Toolbox, HSL.	 V2.06.003, V2.06.003, V2.06.003, V2.06.003, V01.22.4346.	Object code (electronic data in lib format)
3	Doc	16-bit Security Controller – V02 Errata sheet [13]	Rev. 2.2, Infineon, 14th March 2016	Document in electronic form
4	Doc	16-bit Security Controller – V02 Hardware Reference Manual [12]	Rev. 4.2, Infineon, 15th November 2016	Document in electronic form
5	Doc	16-Bit Security Controller - V02, Security Guidelines [11]	Rev. 1.00-1545, Infineon, 01st December 2016	Document in electronic form
6	Doc	CL52 Asymmetric Crypto Library for Crypto@2304T RSA/ECC/Toolbox with included Errata Sheet of 10th May 2017 [14]	Rev. 2.06.003, Infineon, 12th December 2016	Document in electronic form

No	Type	Identifier	Release	Form of Delivery
7	Doc	Crypto@2304TV3 User manual [15]	Rev. 1.4.1, Infineon, 10th November 14	Document in electronic form
8	Doc	Hardware Support Library (HSL) [18]	Rev. 01.22.4346, 2016, Infineon	Document in electronic form
9	Doc	Production and Personalization, 16-bit Security Controller in 65 nm [17]	Rev. 3.2, Infineon, 05th August 2016	Document in electronic form
10	Doc	16-bit Security Controller 65-nm Technology, Programmer's Reference Manual [16]	Rev. 9.1, Infineon, 11th February 2016	Document in electronic form

Table 2: Deliverables of the TOE

The delivery procedures follow the user demands, meaning that the user defines the procedures applied for delivery. These procedures include, but are not limited to, selection of the carrier, packing requirements, labelling, delivery documentation and information. The delivery to the user is always via the regional distribution centres, which are also audited.

Regarding identification of the TOE, at TOE start-up a special mode can be chosen by applying special signalling in contact based communication and the TOE subsequently outputs the generic chip identification data. A user can identify these data, interpret it and retrieve the respective TOE versioning information.

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.

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

The software part of the TOE consists of the cryptographic RSA- and EC- 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 to the final user the Flash Loader shall be locked by the by the user.

For more details please refer to the Security Target [6] and [9], chapters 1.2 and 2.

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, G13 with firmware and optional software libraries (RSA2048 2k and 4k, EC, Toolbox, HSL) with revisions as stated in table 2 above. The flash loader (part of FW) was enabled on evaluated derivative. All hardware modules and all interfaces including options were activated and the ranges of available memories was not limited (i.e. maximum size was available). The BPU feature was not used.

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 IFX_CCI_000007h, G13 (with all further identifiers, all identifiers represent the equal hardware platform and the differences are achieved by configuration and blocking options) of the TOE. The firmware and optional software libraries (RSA2048 2k and 4k, EC, Toolbox, HSL libraries) were examined in those revisions, which are stated in table 2 (above).

The evaluation results are valid for all configurations and blocking options of the hardware stated in 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 another 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:

- Functionality Classes and Evaluation Methodology for Deterministic Random Number Generators, Part of AIS20, Version 2.0, 02.12.1999
- The Application of CC to Integrated Circuits, Part of AIS25, JIL, version 3.0, February 2009
- JIL-HW-ADV_ARC Security Architecture requirements (ADV_ARC) for smart cards and similar devices, Version 2.0, JIL, January 2012,
- Application of Attack Potential to Smartcards, Version 2.9, JIL, January 2013,
- Attack Methods for Smartcards and Similar Devices, Version 2.2, JIL, January 2013,
- A proposal for: Functionality classes and evaluation methodology for true (physical) random number generators, Part of AIS31, Version 3.1, BSI, 25.09.2001,
- A proposal for: Functionality classes for random number generators, Part of AIS31, Version 2.00, BSI, 18.09.2011,
- Composite product evaluation for Smart Cards and similar devices, Part of AIS36, Version 1.2, JIL, January 2012,
- 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, 04.12.2007,
- Minimum Requirements for Evaluating Side-Channel Attack Resistance of Elliptic Curve Implementations, Part of AIS46, Version 1.0.4, BSI, 01.07.2011,
- Methodology for cryptographic rating of memory encryption schemes used in smartcards and similar devices, Part of AIS46, Version 1.0, BSI, 31.10.2013,
- Minimum Requirements for Evaluating Side-Channel Attack Resistance of RSA, DSA and Diffie-Hellman Key Exchange Implementations, Part of AIS46, Version 1.0, BSI, 14.01.2013.

(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, where it has to be noticed that these are only relevant in the GBIC context and not in the CC context.

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-0891-2015 in the sense that specific results, mainly regarding ALC aspects of the evaluation process BSI-DSZ-CC-0891-2015 were re-used.

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).

A table of cryptographic functionalities of the TOE can be found in table 19 of the Security Target [6] and [9], where all Cryptographic Functionality that is marked in column '*Security Level above 100 Bits*' of table 19 with '*no*' achieves a security level of lower than 100 Bits (in general context).

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.

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 IC Dedicated Support Software and/or Embedded Software using the TOE.

For this reason the TOE includes guidance documentation (see table 2) which contains obligations and guidelines for the developer of the product layer on top on how to securely use this certified TOE and which measures have to be implemented in order to fulfil the security requirements of the Security Target of the TOE. In the course of the evaluation of the composite product or system it must be examined if the required measures have been correctly and effectively implemented by the product layer on top. Additionally, the evaluation of the composite product or system must also consider the evaluation results as outlined in the document ETR for composite evaluation [10].

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] – [18].

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. Definitions

12.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
BOS	Boot Operating System
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
cPP	Collaborative Protection Profile
DRNG	Deterministic random number generator
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FW	Firmware
GBIC	German Banking Industry Committee
HRNG	Hybrid random number generator
HSL	Hardware Support Library

HW	Hardware
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
NVM	Non volatile memory
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
SCL	Symmetric cryptographic library
SCP	Symmetric cryptographic processor
TOE	Target of Evaluation
TRNG	True random number generator
TSF	TOE Security Functionality

12.2. 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.

13. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012
http://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012, http://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] Confidential Security Target BSI-DSZ-CC-0961-2017, Version 0.9, 22.05.2017, “Confidential Security Target IFX_CCI_000007h, IFX_CCI_000009h, IFX_CCI_00000Ah, IFX_CCI_00000Bh, IFX_CCI_000016h, IFX_CCI_000017h, IFX_CCI_000018h, design step G13”, Infineon Technologies AG (confidential document)

[8] specifically

- AIS1, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers, Version 13, 14.08.2008,
- AIS14, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 7, 03.08.2010,
- AIS19, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria) und ITSEC, Version 9, 03.11.2014,
- AIS20, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3.0, 15.05.2013,
- AIS25, Anwendung der CC auf Integrierte Schaltungen, Version 8, 12.02.2013,
- AIS26, Evaluationsmethodologie für in Hardware integrierte Schaltungen, Version 9, 21.03.2013,
- AIS31, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3.0, 15.05.2013,
- AIS32, CC-Interpretationen im deutschen Zertifizierungsschema, Version 6, 08.07.2011,
- AIS34, Evaluation Methodology for CC Assurance Classes for EAL5+, Version 3, 03.09.2009,
- AIS35, Öffentliche Fassung eines Security Target (ST-lite), Version 2, 12.11.2007,
- AIS36, Kompositionsevaluierung, Version 4, 15.05.2013,
- AIS38, Wiederverwendung von Evaluationsergebnissen, Version 2, 28.09.2007,
- AIS39, Formal Method, Version 3.0, 24.10.2008,
- AIS46, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren, Version 3, 04.12.2013.

[7] Evaluation Technical Report for the Product BSI-DSZ-CC-0961-2017, 1.01, 03.07.2017, “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-0961-2017, Version 0.3, 22.05.2017, “Public Security Target IFX_CCI_000007h, IFX_CCI_000009h, IFX_CCI_00000Ah, IFX_CCI_00000Bh, IFX_CCI_000016h, IFX_CCI_000017h, IFX_CCI_000018h, design step G13”, Infineon Technologies AG (sanitised public document)

[10] ETR for composite evaluation according to AIS 36 for the Product BSI-DSZ-CC-0961-2017, Version 1.13, 27.06.2017, ETR for composite evaluation (EFC), T-Systems International GmbH (confidential document)

[11] 16-Bit Security Controller - V02, Security Guidelines, Rev. 1.00-1545, Infineon, 01.12.2016

[12] 16-bit Security Controller – V02 Hardware Reference Manual, Rev. 4.2, Infineon, 15.11.2016

[13] 16-bit Security Controller – V02 Errata sheet, Rev. 2.2, Infineon, 14.03.2016

[14] CL52 Asymmetric Crypto Library for Crypto@2304T RSA/ECC/Toolbox with included Errata Sheet of 10th May 2017, Rev. 2.06.003, Infineon, 12.12.2016

[15] Crypto@2304TV3 User manual, Rev. 1.4.1, Infineon, 10.11.2014

[16] 16-bit Security Controller 65-nm Technology, Programmer's Reference Manual, Rev. 9.1, Infineon, 11.02.2016

[17] Production and Personalization, 16-bit Security Controller in 65 nm, Rev. 3.2, Infineon, 05.08.2016

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

This page is intentionally left blank.

C. Excerpts from the Criteria

CC Part 1:

Conformance Claim (chapter 10.4)

“The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - **CC Part 3 extended** - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

Table 3: APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

Table 4: ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model

Assurance Class	Assurance Components
	ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Table 5: Assurance class decomposition

Evaluation assurance levels (chapter 8)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next Section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC Part 3. More precisely, each EAL includes no more than one

component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.

Evaluation assurance level 1 (EAL 1) - functionally tested (chapter 8.3)

“Objectives

EAL 1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL 1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL 1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL 1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.”

Evaluation assurance level 2 (EAL 2) - structurally tested (chapter 8.4)

“Objectives

EAL 2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time.

EAL 2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL 3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL 3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL 3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering."

Evaluation assurance level 4 (EAL 4) - methodically designed, tested, and reviewed (chapter 8.6)

"Objectives

EAL 4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL 4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL 4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs."

Evaluation assurance level 5 (EAL 5) - semiformally designed and tested (chapter 8.7)

"Objectives

EAL 5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL 5 assurance. It is likely that the additional costs attributable to the EAL 5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL 5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques."

Evaluation assurance level 6 (EAL 6) - semiformally verified design and tested (chapter 8.8)

"Objectives

EAL 6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL 6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs."

Evaluation assurance level 7 (EAL 7) - formally verified design and tested (chapter 8.9)

"Objectives

EAL 7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL 7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis."

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 6: Evaluation assurance level summary”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

“Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

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

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0961-2017

Evaluation results regarding development and production environment

The IT product IFX_CCI_000007h, IFX_CCI_000009h, IFX_CCI_00000Ah, IFX_CCI_00000Bh, IFX_CCI_000016h, IFX_CCI_000017h, IFX_CCI_000018h, design step G13 including optional software libraries and dedicated firmware (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 10 July 2017, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.5, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.3) are fulfilled for the development and production sites of the TOE listed below:

Type of site	Site
Development	Infineon Technologies AG, Am Campeon 1-12, 85579 Neubiberg, Germany
	Infineon Technologies Austria AG, Development Center Graz, Babenbergerstr. 10, 8020 Graz Austria
	Infineon Technologies AG, Alter Postweg 101, 86159 Augsburg, Germany
	Infineon Technologies AG DC Bucharest, Novopark Blvd., Dimitrie Pompei Nr. 6, Section 2, 020335 Bucharest, Romania
Production / Testing / Packaging / Delivery	Taiwan Semiconductor Manufacturing Company Ltd., 1, Nan-Ke North Rd., Tainan Science Park, Tainan 741-44, Taiwan
	Ardentec Corporation, No. 3, Gungye 3rd Rd., Hsin-Chu Industrial Park, Hu-Kou, Hsin-Chu Hsien, Taiwan 30351, R.O.C., Taiwan
	Amkor Technology Philippines, Km. 22 East Service Rd., South Superhighway, Muntinlupa City 1702, Philippines
	Amkor Technology Philippines, 119 North Science Avenue, Laguna Technopark, Binan, Laguna 4024, Philippines
	Infineon Technologies AG, Wernerwerkstraße 2, 93049 Regensburg, Germany
	Infineon Technology AG, DCE, Kühne & Nagel, Stockstädter Strasse 10 – Building 8A, 63762 Großostheim, Germany

Type of site	Site
	Infineon Technologies AG, Wernerwerkstraße 2, 93049 Regensburg, Germany
	Kuehne & Nagel, 30805 Santana Street, Hayward, CA 94544, USA
	Excel Singapure PTE Ltd., DHL Exel Supply Chain, Greenwich Drive 1, Singapore 489949, Singapore
	Infineon Technologies (Wuxi) Co. Ltd., No. 118, Xing Chuang San Lu, Wuxi 214028, Jiangsu, P.R. China

Table 7: List of relevant sites

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6] and [9]. Within the baseline certification and re-considered via re-use in the AIS38-sense in this certification, 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.