Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1206-V2-2024

for

IFX_CCI_000068h, IFX_CCI_000080h design step G12 with firmware v80.505.04.1, optional CryptoSuite v04.05.007, optional HSL v04.05.0040, optional UMSLC v02.01.0040, optional NRG™ v06.10.0002, optional Ascon-128 MISE v1.1.2, optional SHA256 MISE v1.1.1 and user guidance documents

from

Infineon Technologies AG

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

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1206-V2-2024 (*)

IFX_CCI_000068h, IFX_CCI_000080h design step G12 with firmware v80.505.04.1, optional CryptoSuite v04.05.007, optional HSL v04.05.0040, optional UMSLC v02.01.0040, optional NRG™ v06.10.0002, optional Ascon-128 MISE v1.1.2, optional SHA256 MISE v1.1.1 and user guidance documents

from	Infineon Technologies AG
PP Conformance:	Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 6 augmented by ALC_FLR.1
valid until:	19 March 2029

SOGIS
Recognition Agreement

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 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, 20 March 2024

For the Federal Office for Information Security

Matthias Intemann
Head of Section

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 BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

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

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

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

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

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

2. Specifications of the Certification Procedure

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

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BMI Regulations on Ex-parte Costs [3]
- Special decrees issued by the Bundesministerium des Innern und für Heimat (Federal Ministry of the Interior and Community)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408

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

2 Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

3 BMI Regulations on Ex-parte Costs - Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) - dated 2 September 2019, Bundesgesetzblatt I p. 1365

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

3. Recognition Agreements

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

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

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

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

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

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

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

3.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The current list of signatory nations and approved certification schemes can be seen on the website: https://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2 and ALC_FLR components.

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

4. Performance of Evaluation and Certification

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

The product IFX_CCI_000068h, IFX_CCI_000080h design step G12 with firmware v80.505.04.1, optional CryptoSuite v04.05.007, optional HSL v04.05.0040, optional UMSLC v02.01.0040, optional NRG™ v06.10.0002, optional Ascon-128 MISE v1.1.2, optional SHA256 MISE v1.1.1 and user guidance documents has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1206-2023. Specific results from the evaluation process BSI-DSZ-CC-1206-2023 were re-used.

The evaluation of the product IFX_CCI_000068h, IFX_CCI_000080h design step G12 with firmware v80.505.04.1, optional CryptoSuite v04.05.007, optional HSL v04.05.0040, optional UMSLC v02.01.0040, optional NRG™ v06.10.0002, optional Ascon-128 MISE v1.1.2, optional SHA256 MISE v1.1.1 and user guidance documents was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 29 February 2024. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

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

The product was developed by: Infineon Technologies AG.

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

5. Validity of the Certification Result

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

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

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

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

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the

[5] Information Technology Security Evaluation Facility

maximum validity of the certificate has been limited. The certificate issued on 20 March 2024 is valid until 19 March 2029. 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 IFX_CCI_000068h, IFX_CCI_000080h design step G12 with firmware v80.505.04.1, optional CryptoSuite v04.05.007, optional HSL v04.05.0040, optional UMSLC v02.01.0040, optional NRG™ v06.10.0002, optional Ascon-128 MISE v1.1.2, optional SHA256 MISE v1.1.1 and user guidance documents has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

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

[6] Infineon Technologies AG
Melli-Beese-Str. 9
86159 Augsburg

B. Certification Results

The following results represent a summary of

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

1. Executive Summary

The Target of Evaluation (TOE) is the Infineon Security Controller IFX_CCI_000068h, IFX_CCI_000080h design step G12 with firmware version 80.505.04.1, optional CryptoSuite version 04.05.007, optional HSL version 04.05.0040, optional UMSLC version 02.01.0040, optional NRG™ version 06.10.0002, optional Ascon-128 MISE version 1.1.2, optional SHA-256 MISE version 1.1.1 and user guidance documents.

The TOE provides a 32-bit Arm v8-M CPU architecture. The major components of the processor system are the CPU (Central Processing Unit), a MPU (Memory Protection Unit), a Security Attribution Unit (SAU), a Nested Vectored Interrupt Controller (NVIC), an Instruction Stream Signature (ISS) coprocessor, and a Masked Instruction Set Extension (MISE) coprocessor and additional software libraries as indicated in the TOE name. The TOE can communicate using contact-based interfaces.

This TOE is intended to be used in smart cards for particular security relevant applications and as a developing platform for smart card operating systems. The term smartcard embedded software is used in the following for all operating systems and applications stored and executed on the TOE. The TOE is the platform for the smartcard embedded software.

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

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

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

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

TOE Security Functionality	Addressed issue
SF_DPM	Device Phase Management
SF_PS	Protection against Snooping
SF_PMA	Protection against Modification Attacks
SF_PLA	Protection against Logical Attacks
SF_HC	Hardware provided Cryptography
SF_CS	CryptoSuite Services

Table 1: TOE Security Functionalities

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

The assets to be protected by the TOE are derived from the Protection Profile. 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], chapter 3.

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

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

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

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

IFX_CCI_000068h, IFX_CCI_000080h design step G12 with firmware v80.505.04.1, optional CryptoSuite v04.05.007, optional HSL v04.05.0040, optional UMSLC v02.01.0040, optional NRG™ v06.10.0002, optional Ascon-128 MISE v1.1.2, optional SHA256 MISE v1.1.1 and user guidance documents.

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	IFX_CCI_000068h, IFX_CCI_000080h	G12 (design step)	Postal transfer in cages as bare dies (sawn wafer), PG-X2QFN-20 packages, or in chip-scale packaging (CSP).
2	FW	BOS, ROM part of HSL, Flash Loader	80.505.04.1 (Flash Loader version is also separately identified as version 10.01.0001)	Stored on the delivered hardware.
3	SW	NRG™ SW library (optional; non-TOE)	06.10.0002	Secure download of object file via iShare.
4	SW	HSL (NVM part) (optional)	04.05.0040	Secure download of object file via iShare.
5	SW	UMSLC library (optional)	02.01.0040	Secure download of object file via iShare.
6	SW	CryptoSuite (optional)	v04.05.007	Secure download of object file via iShare.
7	SW	Ascon-128 MISE	1.1.2 (sw library) For documentation see #16 below (or [20]).	Secure download of object file via iShare.
8	SW	SHA256 MISE	1.1.1 (sw library) For documentation see #17 below (or [21]).	Secure download of object file via iShare.
9	DOC	TEGRION™ SLC21 (32-bit Security Controller – V24), Hardware Reference Manual	See [12] (or [AGD_HRM]) in section Bibliography.	Personalized PDF via secure iShare server.

No	Type	Identifier	Release	Form of Delivery
10	DOC	TEGRION™ SLx2 security controller family, Programmer's Reference Manual, SLx2_DFP	See [13] (or [AGD_PRM]) in section Bibliography.	Personalized PDF via secure iShare server.
11	DOC	SLC21, 32-bit Security Controller – V24, Security Guidelines	See [14] (or [AGD_SG]) in section Bibliography.	Personalized PDF via secure iShare server.
12	DOC	SLC21 (32-bit Security Controller – V24), Production and personalization manual, Flash Loader V10	See [15] (or [AGD_PPM]) in section Bibliography.	Personalized PDF via secure iShare server.
13	DOC	Crypto2304T V4, User Manual	See [16] (or [AGD_CryptoUM]) in section Bibliography.	Personalized PDF via secure iShare server.
14	DOC	CS-SLC21V24 CryptoSuite 32-bit Security Controller, User interface manual	See [19] (or [AGD_CS]) in section Bibliography.	Personalized PDF via secure iShare server.
15	DOC	TEGRION™ SLC21 (32-bit Security Controller – V24) Errata sheet	See [17] (or [AGD_ES]) in section Bibliography.	Personalized PDF via secure iShare server.
16	DOC	Ascon-128 MISE Application Note (document only)	See [20] (or [AGD_ASCON]) in section Bibliography.	ASCII text files available as a secure download via iShare. The README files are part of the respective application note package, which also contains the source files of the library.
17	DOC	SHA256 MISE Application Note (document only)	See [21] (or [AGD_SHA]) in section Bibliography.	

Table 2: Deliverables of the TOE

Regarding TOE delivery:

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

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

Therefore, three different delivery procedures must 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 (e.g. 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).

To determine the necessary procedures to maintain security when distributing versions of the TOE the assumptions, threats, organisational security policies, and security objectives identified in the ST must be considered for an appropriate level of protection on delivery.

- The internal delivery procedures of the TOE Manufacturer comprise all deliverables among the several TOE Manufacturer sites themselves. These deliverables consist of electronic as well as paper documents and physical items like wafers or masks. The corresponding security procedures guarantee an integer and confidential transfer. These internal procedures are evaluated within the ALC_DVS evaluation activity.
- Delivery from the TOE Manufacturer to the IC Embedded Software Developer:
  The delivery from Infineon Technologies (the TOE Manufacturer) to the IC Embedded Software Developer is an external delivery process. This is not a delivery of the final TOE. The delivered items are the optional software libraries and the user guidance. For these items the integrity, confidentiality, and authenticity must be maintained. The delivered items are either of type documentation or software. As such, they are delivered electronically in encrypted form.
- Delivery from the IC Embedded Software Developer to the TOE Manufacturer:
  The delivery procedures from the IC Embedded Software Developer to the TOE Manufacturer (i.e. IFX) are described in a specific developer document.
- Delivery from the TOE Manufacturer to the Composite Product Manufacturer:
  The deliverables and the way of protection are described in a separate document as well as above. The delivered TOEs contain the actual TOE and the embedded software.

In general, the TOE is delivered via the logistics sites (see Table 8):

- DHL Singapore,
- KWE Shanghai, and
- K&N Großostheim.

Regarding TOE identification:

Depending on the blocking configuration, a TOE can have different sizes of the available NVM. In the field, the IC Embedded Software Developer can identify a product in question using the Generic Chip Identification Mode (GCIM), which is described in [13] (or [AGD_PRM]) section 8.4. This information can also be read out using the IFX mailbox area (see [13] or [AGD_PRM] sections 8.9 and 8.10). Thereby, the exact and distinct identification of any product with its exact configuration of this TOE is given.

In addition to the hardware part, the TOE consists of firmware parts and software parts. The firmware part of the TOE is identified also via the GCIM.

The optional libraries comprise the HSL (NVM part), UMSLC, and NRG™ SW (not part of the TSF), Crypto Suite, Ascon-128- and SHA-256 MISE libraries. These libraries are identified by their version numbers. The user can identify the versions by calculating the hash value of the provided library files and compare them to the hash values provided in [6], section 8.

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

- 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.

Details concerning the above-mentioned security policies can be found in sections 6 and 7 of the Security Target [6].

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. Details can be found in the Security Target [6].

5. Architectural Information

Detailed information on the architectural information can be found in the Security Target (see [6]).

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

Developer's Test according to ATE_FUN

Developer’s testing approach:

All TSFs and related security mechanisms, subsystems and modules are tested to assure complete coverage of all SFRs.

Different classes of tests are performed to test the TOE in a sufficient manner:

- Functional verification is done using simulation tests and formal verification during TOE development. The simulation tests result in CRC checksums that are used for further testing to check that a processed TOE matches the expected results from simulation.
- Post-silicon product qualification tests are conducted in Test Mode and User Mode after production of the TOE. Here, the CRC checksums derived in simulation are used to verify the design of the processed TOE. In addition, regression tests are conducted as characterization of firmware parts of the TOE.
- For each produced TOE, production testing is conducted and aims to check the correct functionality of each produced IC.

The TOE has passed all tests defined in the developer’s test plan so that all TSFs have been tested successfully.

The developer’s testing results demonstrate that the TSFs behave as specified.

The developer’s testing results demonstrate that the TOE behaves as expected.

Independent Evaluator Testing according to ATE_IND:

The evaluator's objective regarding this aspect was to test the functionality of the TOE and to verify the developer's test results by repeating developer's tests and to add independent tests. During the evaluation of the TOE, the following classes of tests were carried out:

- Module tests,
- Simulation tests,
- Emulation tests,
- Tests in user mode,
- Tests in test mode,
- Hardware tests, and
- Optional library tests.

The results of the specified and conducted independent evaluator tests confirm the TOE’s functionality. The TSF and the interfaces were found to operate as specified.

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

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

Penetration Testing according to AVA_VAN:

All configurations of the TOE being intended to be covered by the current evaluation were tested.

The overall test result is that no deviations were found between the expected and the actual test results; moreover, no attack scenario with the attack potential high was successful in the TOE’s operational environment as defined in [6], provided that all measures required by the developer are applied.

The embedded software must implement the security advice given in [12] (or [AGD_HRM]), [13] (or [AGD_PRM]), [14] (or [AGD_SG]), [15] (or [AGD_PPM]), [16] (or [AGD_CryptoUM]), [17] (or [AGD_ES]), [19] (or [AGD_CS]), [20] (or [AGD_Ascon]) and [21] (or [AGD_SHA]).

Testing Summary:

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

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

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

The evaluators were able to repeat the tests of the developer by using the library of programs, tools, and prepared chip samples delivered to the evaluators or at the developer’s site. They performed independent tests to supplement, augment, and to verify

the tests performed by the developer. For the developer tests, repeated by the evaluators, other test parameters were used and the test equipment was varied. Security features of the TOE realised by specific design and layout measures were checked by the evaluators during layout inspections both in design data and on the final product.

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

For penetration testing, the evaluators took all security functionalities into consideration. Intensive penetration testing was planned based on the analysis results and performed for the underlying mechanisms of security functionalities. The penetration tests considered both the physical tampering of the TOE and attacks, which do not modify the TOE physically. The penetration test results confirm that the TOE is resistant to attackers with high attack potential in the intended environment for the TOE.

8. Evaluated Configuration

The evaluation tests are performed with the chip IFX_CCI_000068h, produced by TSMC fab 15 in Taiwan. The identifiers IFX_CCI_000068h and IFX_CCI_000080h may differ from each other only in terms of blocked modules: They are still physically present on the TOE, but not accessible. Thus, the tests were performed on a TOE without any blocked features.

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

For specific configuration options, see [6], section 1.4.6.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used for those components up to EAL 5 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the technology was used:

- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 1, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers, Version 14, 2017-10-11, Bundesamt für Sicherheit in der Informationstechnik.
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 14, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 7, 2010-08-03, Bundesamt für Sicherheit in der Informationstechnik.
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 19, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 9, 2014-11-03, Bundesamt für Sicherheit in der Informationstechnik.

- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 20, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3, 2013-05-15, Herausgeber: Zertifizierungsstelle des BSI im Rahmen des Zertifizierungsschemas, Bundesamt für Sicherheit in der Informationstechnik.
- A proposal for: Functionality classes for random number generators, W. Killmann, W. Schindler, Version 2.0, 2011-09-18, T-Systems GEI GmbH and Bundesamt für Sicherheit in der Informationstechnik. (same as [KS2011])
- Developer evidence for the evaluation of a deterministic random number generator, Version 0.9, 2013-02-28, Bundesamt für Sicherheit in der Informationstechnik.
- Evaluation Report as part of the Evaluation Technical Report, Part B – ETR-Part Deterministic Random Number Generator, Template-Version 0.10, 2013-02-28, Bundesamt für Sicherheit in der Informationstechnik.
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 23, Zusammentragen von Nachweisen der Entwickler, Version 4, 2017-03-15, Bundesamt für Sicherheit in der Informationstechnik.
- CC Supporting Document Guidance – Collection of Developer Evidence, Version 1.5, April 2012, CCDB-2012-04-005.
- Joint Interpretation Library – Collection of Developer Evidence, Version 1.5, January 2012.
- Application Notes and Interpretation of the Scheme (AIS) – AIS 25, Anwendungen der CC auf integrierte Schaltungen, Version 9, 2017-03-15, Bundesamt für Sicherheit in der Informationstechnik.
- CC Supporting Document Mandatory Technical Document – Security Architecture requirements (ADV_ARC) for smart cards and similar devices, Version 2.1, April 2014, CCDB-2012-04-004.
- CC Supporting Document Guidance – Security Architecture requirements (ADV_ARC) for smart cards and similar devices – Appendix 1, Version 2.0, April 2012.
- CC Supporting Document Mandatory Technical Document – The Application of CC to Integrated Circuits, Version 3.0, Revision 1, March 2009, CCDB-2009-03-002.
- Joint Interpretation Library – Security Architecture requirements (ADV_ARC) for smart cards and similar devices – Appendix 1, Version 2.0, January 2012.
- Joint Interpretation Library – The Application of CC to Integrated Circuits, Version 3.0, February 2009.
- Joint Interpretation Library – Security requirements for post-delivery code loading, Version 1.0, February 2016.
- Validity of conducted tests on Security Smart Card ICs in dependence of test date, Version 1, 2017-03-15, Bundesamt für Sicherheit in der Informationstechnik.
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 26, Evaluationsmethodologie für in Hardware Integrierte Schaltungen, Version 10, 2017-07-03, Bundesamt für Sicherheit in der Informationstechnik.
- Auswahl geeigneter Chips für DPA-Messungen, Version 1.1, 2008-12-07, Bundesamt für Sicherheit in der Informationstechnik.

- Special Attack Methods for Smartcards and Similar Devices, Version 1.4, 2011-06-08, Bundesamt für Sicherheit in der Informationstechnik.
- CC Supporting Document Mandatory Technical Document – Requirements to perform Integrated Circuit Evaluations, Version 1.1, May 2013, CCDB-2013-05-001.
- Joint Interpretation Library – Application of Attack Potential to Smartcards, Version 3.2, November 2022.
- Joint Interpretation Library – Attack Methods for Smartcards and Similar Devices, Version 2.4, 2020, confidential.
- Joint Interpretation Library – Requirements to perform Integrated Circuit Evaluations, Version 1.1, February 2013.
- Application Notes and Interpretation of the Scheme (AIS) – AIS 27, Transition from ITSEC to CC, Version 5, 2010-08-17, Bundesamt für Sicherheit in der Informationstechnik.
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 31, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3, 2013-05-15, Bundesamt für Sicherheit in der Informationstechnik.
- Developer evidence for the evaluation of a physical true random generator, Version 0.8, 2013-02-28, Bundesamt für Sicherheit in der Informationstechnik.
- Evaluation Report as part of the Evaluation Technical Report, Part B – ETR-Part True Physical and Hybrid Random Number Generator, Template-Version 0.7, 2013-02-28, Bundesamt für Sicherheit in der Informationstechnik.
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 32, CC-Interpretationen im deutschen Zertifizierungsschema, Version 7, 2011-06-08, Bundesamt für Sicherheit in der Informationstechnik.
- Application Notes and Interpretation of the Scheme (AIS) – AIS 34, Evaluation Methodology for CC Assurance Classes for EAL5+ (CC v2.3 & v3.1) and EAL6 (CC v3.1), Version 3, 2009-09-03, Bundesamt für Sicherheit in der Informationstechnik.
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 35, Öffentliche Fassung eines Security Target (ST-lite), Version 2, 2007-11-12, Bundesamt für Sicherheit in der Informationstechnik.
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 36, Kompositionsevaluierung, Version 5, 2017-03-15, Bundesamt für Sicherheit in der Informationstechnik.
- CC Supporting Document Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, Version 1.4, December 2015, CCDB-2015-12-001.
- Joint Interpretation Library – Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018.
- CC Supporting Document Guidance – ETR template for composite evaluation of Smart Cards and similar devices, Version 1.1, December 2015, CCDB-2015-12-002.
- Joint Interpretation Library – ETR template for composite evaluation of Smart Cards and similar devices, Version 1.1, August 2015.

- Joint Interpretation Library – Certification of “open” smart card products, Version 1.1 (for trial use), 2013-02-04.
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 37, Terminologie und Vorbereitung von Smartcard-Evaluierungen, Version 3, 2010-05-17, Bundesamt für Sicherheit in der Informationstechnik.
- CC Supporting Document Guidance – Smartcard Evaluation, Version 2.0, February 2010, CCDB-2010-03-001.
- Application Notes and Interpretation of the Scheme (AIS) – AIS 38, Reuse of evaluation results, Version 2, 2007-09-28, Bundesamt für Sicherheit in der Informationstechnik.
- Application Notes and Interpretation of the Scheme (AIS) – AIS 39, Formal Methods, Version 3, 2008-10-24, Bundesamt für Sicherheit in der Informationstechnik.
- Application Notes and Interpretation of the Scheme (AIS) – AIS 41, Guidelines for PPs and STs, Version 2, 2011-01-31, Bundesamt für Sicherheit in der Informationstechnik.
- Guidance Document – The PP/ST Guide, Version 2, Revision 0, 2010-08, Bundesamt für Sicherheit in der Informationstechnik.
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 46, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren, Version 3, 2013-12-04, Bundesamt für Sicherheit in der Informationstechnik.
- Review-Protokoll zum (Krypto-)AVA-KickOff, Template-Version/Date: 2019-08-23, Bundesamt für Sicherheit in der Informationstechnik.
- Minimal Requirements for Evaluating Side-Channel Attack Resistance of Elliptic Curve Implementations, Version 1.0.4, 2011-07-01, BSI.
- Methodology for cryptographic rating of memory encryption schemes used in smartcards and similar devices, Version 1.0, 2013-10-31, BSI.
- Minimum Requirements for Evaluating Side-Channel Attack Resistance of RSA, DSA and Diffie-Hellman Key Exchange Implementations, Version 1.0, 2013-01-14, BSI.
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 47, Regelungen zu Site Certification, Version 1.1, 2013-12-04, Bundesamt für Sicherheit in der Informationstechnik.
- Guidance for Site Certification, Version 1.1, 2013-12-04, Bundesamt für Sicherheit in der Informationstechnik.
- Joint Interpretation Library – Minimum Site Security Requirements, Version 3.0, 02/2020.

(see [4] for respective AIS references).

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

To support composite evaluations according to AIS 36 the document ETR for composite evaluation [10] was provided and approved. This document provides details of this platform evaluation that have to be considered in the course of a composite evaluation on top.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 6 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_FLR.1 augmented for this TOE evaluation.

The evaluation has confirmed:

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

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

9.2. Results of cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But cryptographic functionalities with a security level of lower than 120 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

The following table gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its rating from cryptographic point of view. Any Cryptographic Functionality that is marked in column '*Security Level above 120 Bits*' of the following table with '*no*' achieves a security level of lower than 120 Bits (in general context) only.

No.	Purpose	Cryptographic Mechanism	Implementation Standard	Key Size in Bits	Security Level above 120 Bits	Comments
Symmetric Co-Processor (SCP)						
1	Cryptographic Primitive	AES	[FIPS197]	128, 192, 256	--	Cryptographic Primitives might have various use case scenarios not explicitly specified on HW platform level (e.g. confidentiality, integrity, authenticity etc.). Hence no rating on “security level > 120 bits” but considered according to AVA_VAN.5 penetration testing..

No.	Purpose	Cryptographic Mechanism	Implementation Standard	Key Size in Bits	Security Level above 120 Bits	Comments
2	Confidentiality	#1 in ECB mode for encryption and decryption	[NIST SP800-38A]	128, 192, 256	No	“No” is for ECB mode in general for all implementations and certification procedures.
Flash Loader						
3	Cryptographic primitive	AES	[FIPS197]	128	--	--
4	Authenticated encryption	#3 (AES) in CCM mode for encryption and decryption	[NIST SP800-38C]	128	--	Not rated w.r.t. “security level > 120 bits” but considered according to AVA_VAN.5 penetration testing.
5	Key derivation	KDF in counter mode with AES-CMAC as PRF	[NIST SP800-108, 5.1] [NIST SP800-38B, 6.2]	128	--	Not rated w.r.t. “security level > 120 bits” but considered according to AVA_VAN.5 penetration testing.
CryptoSuite: Symmetric Functionality						
6	Cryptographic primitive	AES	[FIPS197]	128, 192, 256	--	--
7	Confidentiality	#6 in ECB mode for encryption and decryption	[NIST SP800-38A]	128, 192, 256	No	“No” is for ECB mode in general for all implementations and certification procedures.
8	Confidentiality	#6 in CBC, CTR, CFB mode for encryption and decryption	[NIST SP800-38A]	128, 192, 256	Yes	--
9	Integrity	#3 in CMAC mode for MAC generation	[NIST SP800-38B]	128, 192, 256	No	--
CryptoSuite: Asymmetric Functionality						
10	Key agreement	Finite field Diffie-Hellman	[PKCS#3, 7.2]	1024-2048	N/A	--
11	Confidentiality	RSA Encryption	[PKCS #1, 5.1.1]	1024 – 4224	Yes for >= 2800 bit	--

No.	Purpose	Cryptographic Mechanism	Implementation Standard	Key Size in Bits	Security Level above 120 Bits	Comments
12	Confidentiality	RSA Decryption	[PKCS #1, 5.1.2, 2a]	1024 – 2112	Yes for >= 2800 bit	--
13	Confidentiality	RSA Decryption with CRT	[PKCS #1, 5.1.2, 2b]	1024 – 4224	Yes for >= 2800 bit	--
14	Authenticity	RSA Signature generation	[PKCS #1, 5.2.1, 2a]	1024 – 2112	For Keysize >=2000 bit: security level >=100bit	--
15	Authenticity	RSA Signature generation with CRT	[PKCS #1, 5.2.1, 2b]	1024 – 4224	Yes for >= 2800 bit	--
16	Authenticity	RSA Signature verification	[PKCS #1, 5.2.2]	1024 – 4224	Yes for >= 2800 bit	--
17	Key generation	RSA key generation returning probably random primes p and q.	--	1024 – 2047	N/A	Prime generation method follows [FIPS186-4, B.3.3] but due to key size considered proprietary. Method: “Ccc_Rsa_KeyGen PQ”.
18	Key generation	RSA key generation returning probably random primes p and q.	[FIPS 186-4, B.3.3] [FIPS 186-4, C.3.1]	2048 – 4128	N/A	Step 1 not implemented Method: “Ccc_Rsa_KeyGen PQ”
19	Key generation	Calculation of RSA key components (N, d) from p, q	[FIPS 186-4, B.3.1] [PKCS#1, 3.1 / 3.2(1)]	1024 – 2112	N/A	Method: “Ccc_Rsa_KeyGen PQ + Ccc_Rsa_KeyGenN + Ccc_Rsa_KeyGenD ”
20	Key generation	Calculation of RSA CRT parameters from p, q	[FIPS 186-4, B.3.1] [PKCS#1, 3.1 / 3.2(2)]	1024 – 4224	N/A	Method: “Ccc_Rsa_KeyGen PQ + Ccc_Rsa_KeyGenC

No.	Purpose	Cryptographic Mechanism	Implementation Standard	Key Size in Bits	Security Level above 120 Bits	Comments
						rt”
21	Key generation (primality test)	Miller-Rabin primality test	[FIPS 186-4], C.3.1	512 – 2064	N/A	(Prime candidate length)
22	Key generation (primality test)	Enhanced Miller-Rabin primality test	[FIPS 186-4], C.3.2	512 – 2064	N/A	(Prime candidate length)
23	ECC	Supported elliptic curves: NIST curves over prime fields in [FIPS186-4], Brainpool curves in [RFC5639], ANSII FRP256V1 in [ANSSI_EC], BN P256 in [ISO_15946, 7.3], W-25519 in [NIST SP800-186].	FIPS186-4] [RFC5639] [ANSSI_EC] [ISO_15946] [NIST SP800-186]	160-521	“No” for BN P256 in [ISO_15946, 7.3] in general case, “not rated w.r.t. 120 bits” in specific cases.	--
24	Authenticity	ECDSA signature generation on curves listed in #23	[FIPS186-4, 6.4]	160-521	Key size 160,163,192, 224: No Key sizes >=250: Yes	(Note that the hash calculation of ECDSA s not implemented by the library and lies in the responsibility of the user.)
25	Authenticity	ECDSA signature verification on curves listed in #23	[FIPS186-4, 6.4]	160-521	Key size 160,163,192, 224: No Key sizes >=250: Yes	(Note that the hash calculation of ECDSA s not implemented by the library and lies in the responsibility of the user.)
26	Key agreement	Elliptic Curve Diffie-Hellman (ECDH) key agreement on curves listed in #23	[NIST SP800-56A, 5.7.1.2]	160-521	Key size 160,163,192, 224: No Key sizes >=250: Yes	
27	Key generation	Elliptic Curve key generation on curves listed in #23	[FIPS186-4, B.4.1]	160-521	N/A	--

No.	Purpose	Cryptographic Mechanism	Implementation Standard	Key Size in Bits	Security Level above 120 Bits	Comments
CryptoSuite: Hash Functionality						
28	Hash	SHA-1	[FIPS180-4]	N/A	N/A	--
29	Hash	SHA-2	[FIPS180-4]	N/A	N/A	
MISE: ASCON						
30	Authenticated encryption	Ascon-128	[ASCON, 2.4]	128	N/A	Please note: ASCON is final candidate but standard not yet not finalized (as of date of certification end).
MISE: Hash Functionality						
31	Hash	SHA-256	[FIPS180-4]	N/A		
Random Number generation (Hardware)						
32	RNG	Physical RNG	According to PTG.2 in [KS2011]	N/A	N/A	--
CryptoSuite: RNG Functionality						
33	RNG	Physical RNG	Corresponds to PTG.2 in [KS2011]	N/A	N/A	
34	RNG	Physical RNG with cryptographic post-processing	Corresponds to PTG.3 in [KS2011] and [NIST SP800-90A]	N/A	N/A	Post-processing based on [NIST SP800-90A] CTR_DRBG.
35	RNG	Deterministic RNG	Corresponds to DRG.3 in [KS2011] and [NIST SP800-90A]	N/A	N/A	Implementation according to CTR_DRBG specified in [NIST SP800-90A]
36	RNG	Hybrid deterministic RNG	Corresponds to DRG.4 in [KS2011] and [NIST SP800-90A]	N/A	N/A	Post-processing based on [NIST SP800-90A] CTR_DRBG.

Table 3: TOE cryptographic functionality

Please take into account the following additional information:

- Conformance evaluation and assessment to claimed cryptographic functionality standards, as required by Common Criteria Part 1 section A.13, is documented in the confidential report “Cryptographic Standards Compliance Verification” [18].
- The Flash Loader's cryptographic strength was also not assessed by BSI. However, the evaluation of the Flash Loader’s implementation strength according to the TOE's

Evaluation Assurance Level (including AVA_VAN.5) did not reveal any implementation weaknesses.

- A BSI-assessment of the memory encryption MCICE, based the public MemEnc-Guide ("Methodology for cryptographic rating of memory encryption schemes used in smartcards and similar devices", v1.0, 31.10.2013), was positive.

The references within table 3 are as follows:

[ASCON] Ascon v1.2 Submission to NIST, 2021-05-31

[FIPS197] FIPS 197, Federal Information Processing Standards Publication, Advanced Encryption Standard (AES), Published 2001-11-26, Updated 2023-05-09, National Institute of Standards and Technology (NIST).

[FIPS180-4] FIPS PUB 180-4 Federal Information Processing Standards Publication Secure Hash Standard (SHS), August 2015, Information Technology Laboratory National Institute of Standards and Technology

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

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

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

[NIST SP800-38C] NIST SP800-38C, Recommendation for Block Cipher Modes of Operation, The CCM Mode for Authentication and Confidentiality, May 2004 (errata update 07-20-2007), National Institute of Standards and Technology (NIST).

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

[ISO_9798-2] ISO/IEC 9798-2: 2008 - Information Technology - Security techniques - Entity authentication - Part 2: Mechanisms using authenticated encryption. Fourth edition 2019-06

[NIST SP800-90A] NIST Special Publication 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015, National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce

[NIST SP800-108] NIST Special Publication, NIST SP 800-108r1, Recommendation for Key Derivation Using Pseudorandom Functions, August 2022, National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce.

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

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

[KS2011] A proposal for: Functionality classes for random number generators, W. Killmann, W. Schindler, Version 2.0, 2011-09-18, T-Systems GEI GmbH and Bundesamt für Sicherheit in der Informationstechnik.

[AGD_PPM] See [15].

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 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].

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.

Requirements for the Usage of the Evaluated Product:

The TOE is delivered to the composite product manufacturer and to the security IC embedded software developer. The actual end-consumer obtains the TOE from the composite product issuer together with the application that runs on the TOE.

The security IC embedded software developer receives all necessary recommendations and hints to develop his software in form of the delivered documentation.

- All security hints described in the delivered documents in [12] - [21] must be considered.

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

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

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

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

11. Security Target

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

12. Regulation specific aspects (eIDAS, QES)

None.

13. Definitions

13.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
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] Security Target BSI-DSZ-CC-1206-V2-2024, Version 1.4.4, 2024-02-26, "IFX_CCI_000068h/80h G12 Security Target", Infineon Technologies AG (public document)

[7] Evaluation Technical Report, Version 2, 2024-02-27, "EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY)", TÜV Informationstechnik, (confidential document)

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

[9] (not used) - see [6]

[10] ETR for composite evaluation according to AIS 36 for the Product, Version 2, 2024-02-27, "ETR for Composite Evaluation", TÜV Informationstechnik GmbH (confidential document)

[11] Configuration list for the TOE, Version 0.4, 2024-01-25 (confidential document)

[12] also referred to as [AGD_HRM], "TEGRION™ SLC21 (32-bit Security Controller – V24), Hardware Reference Manual", Version 5.0, 2023-12-11, Infineon Technologies AG (confidential document)

[13] also referred to as [AGD_PRM], "TEGRION™ SLx2 security controller family, Programmer's Reference Manual, SLx2_DFP", Version 1.3.0, 2023-10-19, Infineon Technologies AG (confidential document)

[14] also referred to as [AGD_SG], "SLC21, 32-bit Security Controller – V24, Security Guidelines", Version 1.00-3001, 2023.07-26, Infineon Technologies AG (confidential document)

[15] also referred to as [AGD_PPM], "SLC21 (32-bit Security Controller – V24), Production and personalization manual, Flash Loader V10", Version 10.01, 2023-06-28, Infineon Technologies AG (confidential document)

[16] also referred to as [AGD_CryptoUM], "Crypto2304T V4, User Manual", Version 2.0, 2023-07-14, Infineon Technologies AG (confidential document)

[17] also referred to as [AGD_ES], "TEGRION™ SLC21 (32-bit Security Controller – V24) Errata sheet", Version 3.0, 2024-01-09, Infineon Technologies AG (confidential document)

[18] "SINGLE EVALUATION REPORT ADDENDUM to ETR-Part ADV Cryptographic Standards Compliance Verification", Version 4, 2024-02-27, TÜV Informationstechnik GmbH (confidential document)

[19] also referred to as [AGD_CS], "CS-SLC21V24 CryptoSuite 32-bit Security Controller User interface manual", Version 4.05.007, 2023-11-08, Infineon Technologies AG (confidential document)

[7] See section 9.1 on usage of specific AIS.

[20] also referred to as [AGD_ASCON], “Ascon-128 MISE Application Note (ReadMe_AsconMise-v1.1.3.md)”, Version 1.1.3, 2023-09-13, Infineon Technologies AG (confidential document)

[21] also referred to as [AGD_SHA], “SHA256 MISE Application Note (ReadMe_ShaMise-v1.1.2.md)”, Version 1.1.2, 2023-09-13, Infineon Technologies AG (confidential document)

C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria can be followed:

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12
- On the detailed definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17
- The table in CC part 3 , Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published at https://www.commoncriteriaportal.org/cc/

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development and production environment

Annex B of Certification Report BSI-DSZ-CC-1206-V2-2024

Evaluation results regarding development and production environment

The IT product IFX_CCI_000068h, IFX_CCI_000080h design step G12 with firmware v80.505.04.1, optional CryptoSuite v04.05.007, optional HSL v04.05.0040, optional UMSLC v02.01.0040, optional NRG™ v06.10.0002, optional Ascon-128 MISE v1.1.2, optional SHA256 MISE v1.1.1 and user guidance documents (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations, 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 20 March 2024, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.5, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_FLR.1, ALC_TAT.3)

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

Distribution Center name	Address
DHL Singapore	DHL Supply Chain Singapore Pte Ltd., Advanced Regional Center Tampines LogisPark 1 Greenwich Drive Singapore 533865
KWE Shanghai	KWE Kintetsu World Express (China) Co., Ltd. Shanghai Pudong Airport Pilot Free Trade Zone No. 530 Zheng Ding Road Shanghai, P.R. China
K&N Großostheim	Kühne & Nagel Stockstädter Strasse 10 63762 Großostheim Germany

Table 4: 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]) are fulfilled by the procedures of these sites.

Note: End of report