Federal Office
for Information Security

Certification Report

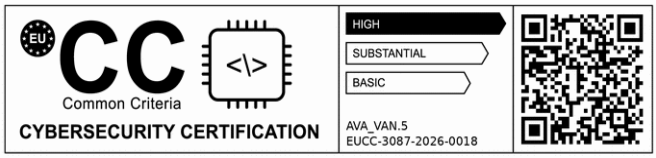
EUCC-3087-2026-0018
Administration ID
BSI-DSZ-CC-1287-2026

for

IFX_CCI_00003Fh, IFX_CCI_000059h, IFX_CCI_00005Bh, IFX_CCI_00003Ch, IFX_CCI_00003Dh, IFX_CCI_00005Ah design step G11 and H11 with optional HSL v2.01.6198, optional SCL v2.13.001, optional ACL v3.03.003, optional ACL v3.04.001, optional v3.05.002, optional HCL v1.13.001, optional RCL v1.10.006 and with specific IC-dedicated firmware identifier 80.203.003 and Flash Loader v8.06.001

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, Infoline +49 (0)228 99 9582-11

Contents

A. Certification....4
1. Preliminary Remarks....4
2. Specifications of the Certification Procedure....4
3. Recognition Agreements....5
4. Performance of Evaluation and Certification....5
5. Publication....7
B. Certification Results....8
1. Executive Summary....9
2. Identification of the TOE....11
3. Security Policy....13
4. Assumptions and Clarification of Scope....14
5. Architectural Information....15
6. Supplementary Cybersecurity Information....15
7. IT Product Testing....16
8. Evaluated Configuration....18
9. Results of the Evaluation....19
10. Obligations and Notes for the Usage of the TOE....27
11. Security Target....28
12. Regulation specific aspects (eIDAS, QES)....28
13. Bibliography....29
C. Annexes....32

A. Certification

1. Preliminary Remarks

The Implementing Regulation (EU) 2024/482 of the European Parliament and of the Council of 31 January 2024 [EUCC-VO] establishes a Union-wide cybersecurity certification scheme for TOEs and Protection Profiles for conformity assessments using the requirements of Common Criteria.

By implementing the Cybersecurity Act[1], certification activities at assurance level 'high' and in duly justified cases at assurance level 'substantial' are reserved to the National Cybersecurity Certification Agency of a Member State.

In accordance to BSIG[2] Act, the Federal Office for Information Security (BSI) issues certificates for information technology products.

Certification of a product is carried out at the request of a developer, vendor or a distributor, hereinafter called the applicant.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria referenced in the above mentioned Implementing Regulation (EU) 2024/482 as well as relevant application notes and interpretations published by the certification body of the BSI.

Evaluation facilities notified by the German National Cybersecurity Certification Authority carry out the evaluation.

This Certification Report is the result of the certification activities carried out by the certification body of the BSI in conclusion of the technical evaluation. 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 carries out its activities according to the criteria laid down in the following:

- Implementing Regulation (EU) 2024/482 of the European Parliament and of the Council of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC) [EUCC-VO]
- EUCC state-of-the-art documents of relevance to the TOE [EUCC_SOTA]
- Act on the Federal Office for Information Security[2]

[1] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

[2] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 2 December 2025, BGBl. 2025 Nr. 301, S. 2

- BSI Certification and Approval Ordinance[3]
- BMI Regulations on Ex-parte Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior and Community)
- ISO/IEC 15408 as published on the day of issuance of this certificate and as mirrored by the Common Criteria for IT Security Evaluation (CC), Version CC:2022 [CC]
- ISO/IEC 18045 as published on the day of issuance of this certificate and as mirrored by the Common Methodology for IT Security Evaluation (CEM), Version CEM:2022 [CEM]
- DIN EN ISO/IEC 17065 standard
- EUCC programme: Scheme documentation describing the certification process (EUCC) [EUCC_PROG]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [AIS]

3. Recognition Agreements

In order to avoid multiple certifications 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. 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 5 EAL 2 and ALC_FLR components.

4. Performance of Evaluation and Certification

- The certification body monitors each individual evaluation to ensure a uniform application and interpretation of the criteria as well as uniform ratings.

[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 02 December 2025, Bundesgesetzblatt 2025, no. 301

[4] 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

- The TOE IFX_CCI_00003Fh, IFX_CCI_000059h, IFX_CCI_00005Bh, IFX_CCI_00003Ch, IFX_CCI_00003Dh, IFX_CCI_00005Ah design step G11 and H11 with optional HSL v2.01.6198, optional SCL v2.13.001, optional ACL v3.03.003, optional ACL v3.04.001, optional v3.05.002, optional HCL v1.13.001, optional RCL v1.10.006 and with specific IC-dedicated firmware identifier 80.203.003 and Flash Loader v8.06.001 has been certificated.
- The evaluation of the product IFX_CCI_00003Fh, IFX_CCI_000059h, IFX_CCI_00005Bh, IFX_CCI_00003Ch, IFX_CCI_00003Dh, IFX_CCI_00005Ah design step G11 and H11 with optional HSL v2.01.6198, optional SCL v2.13.001, optional ACL v3.03.003, optional ACL v3.04.001, optional v3.05.002, optional HCL v1.13.001, optional RCL v1.10.006 and with specific IC-dedicated firmware identifier 80.203.003 and Flash Loader v8.06.001 was carried out by TÜV Informationstechnik GmbH, located at

  Unternehmensgruppe TÜV NORD
  Am TÜV 1
  45307 Essen.
- The evaluation was completed on 6 August 2026. TÜV Informationstechnik GmbH is a notified evaluation facility (ITSEF) .
- This certification was applied for: Infineon Technologies AG.
- The assessed TOE was developed by: Infineon Technologies AG.
- The certification activities are concluded with the comparability check and the production of this Certification Report. This work was completed by the certification body of the BSI.

This Certification Report applies only to the version of the TOE as identified in this document. The confirmed assurance package is valid on the condition that

- all statements and indications regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in an environment 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 issued Certificate confirms the assurance of the product claimed in the Security Target [ST] on certificate’s issuance day. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be reassessed. Therefore, the holder of the certificate should involve the assurance continuity program of the EUCC Certification Scheme (e.g. by a re-assessment or re-certification) in its obligations to monitor the certified product. Specifically, if certification results should be 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 reassessment on a regular e.g. annual basis.

In order to prevent an indefinite certificate usage where evolving attack methods justify a recent reassessment of the product’s resistance, the maximum validity period of the certificate is limited. The certificate issued on 1 October 2026 is valid until 30 September 2031 and its validity can be renewed by certifying the TOE again.

The holder of this certificate is obliged:

1. to meet the obligations from the Implementing Regulation (EU) 2024/482, in particular but not exclusively to respect the rules for certificate usage, to monitor the

conformity of the certified TOE, to inform the certification body about subsequently detected vulnerabilities or irregularities with relevance to the security of the TOE and to maintain vulnerability management and disclosure procedures.

Should changes be introduced into the certified version of the TOE, the validity period of its related certificate can be extended in order to cover the changed TOE, provided the holder of the certificate applies for measures under EUCC scheme's assurance continuity (i.e. recertification or maintenance) and the changed TOE then meets the assurance requirements.

5. Publication

The TOE IFX_CCI_00003Fh, IFX_CCI_000059h, IFX_CCI_00005Bh, IFX_CCI_00003Ch, IFX_CCI_00003Dh, IFX_CCI_00005Ah design step G11 and H11 with optional HSL v2.01.6198, optional SCL v2.13.001, optional ACL v3.03.003, optional ACL v3.04.001, optional v3.05.002, optional HCL v1.13.001, optional RCL v1.10.006 and with specific IC-dedicated firmware identifier 80.203.003 and Flash Loader v8.06.001 has been notified to ENISA for publication on the website on European cybersecurity certification schemes and has also been included in BSI's list of certified products, which is published regularly (see [EUCC_CERT]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

This holder of the certificate[5] has to publish on its website this Certification Report and supplementary information. The Certification Report may also be obtained in electronic form at the internet address stated above.

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

B. Certification Results

The following chapters summarise the assessment results of the

- the applicant’s Security Target specified for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes, statements and indications from the certification body.

1. Executive Summary

The Target of Evaluation (TOE) consists of the hardware part, the firmware part, the software part as well as the user guidance.

In detail, the TOE is the Infineon Technologies AG security controller IFX_CCI_00003Fh, IFX_CCI_000059h, IFX_CCI_00005Bh, IFX_CCI_00003Ch, IFX_CCI_00003Dh, IFX_CCI_00005Ah in Design Steps G11 and H11 with specific IC dedicated firmware and optional software:

- Asymmetric Cryptographic Libraries (ACLs) v3.03.003, v3.04.001, and v3.05.002,
- Symmetric Cryptographic Library (SCL) v2.13.001,
- Hash Cryptographic Library (HCL) v1.13.001,
- Random Crypto Library (RCL) v1.10.006, and
- Hardware Support Library (HSL) v2.01.6198.

The firmware version of the TOE is referenced via the firmware identifier 80.203.00.3. The firmware comprises the Boot Software (BOS) and Flash Loader (FL) v8.06.001.

The TOE provides a proprietary 32-bit RISC CPU designed on the basis of the ARMv7_M architecture. The major components of the core system are the CPU (Central Processing Unit), the MPU (Memory Protection Unit) and MED (Memory Encryption / Decryption Unit).

The user has the possibility to configure the TOE, either during production or by Infineon's BPU (billing per use) concept. The options are listed in [ST, 1.4.7] and comprise for example the memory sizes of the RAM, NVM and Cache, the availability of peripherals like the cryptographic coprocessors (symmetric and asymmetric), and the availability of the communication interfaces. Especially the possibility to configure the cryptographic coprocessors is of importance to the TOE, as the presence of the coprocessor affects the provided security functionalities:

- If the symmetric cryptographic coprocessor (SCP) is not available to the user, then the TOE will not provide any AES and TDES calculations.
- A blocked asymmetric cryptographic coprocessor (Crypto2304T) means, that the user is not able to use this coprocessor for calculations, e.g. RSA and ECC calculations.

All cryptographic libraries are optional. However, the following dependencies exist:

- In case the optional SCL is part of the TOE, availability of the SCP is required.
- In case one of the optional ACLs is part of the TOE, the availability of the arithmetic coprocessor (Crypto2304T) is required.

The different identifiers used for the TOE represent the same underlying hardware; however, the IFX_CCI_00003Fh, IFX_CCI_000059h, IFX_CCI_00005Bh, IFX_CCI_00003Ch, IFX_CCI_00003Dh, and IFX_CCI_00005Ah can differ in terms of their configuration. This difference is achieved by means of blocking (i.e. the blocked modules are still physically present on the TOE, but not accessible). In addition, the products IFX_CCI_00003Ch, IFX_CCI_00003Dh, and IFX_CCI_00005Ah run through the burn-in process during the production to reduce the error rate.

The design step H11 is identical to the design step G11 except for the deactivated SPI interface. This deactivation was realized by a metal fix (i.e. physical manipulation of metal layers M1 and M2).

The security functionality can be found in chapter 7 of the ST [ST].

This TOE is intended to be used in smart cards for particularly security relevant applications and for its previous use as 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 product IFX_CCI_00003Fh, IFX_CCI_000059h, IFX_CCI_00005Bh, IFX_CCI_00003Ch, IFX_CCI_00003Dh, IFX_CCI_00005Ah design step G11 and H11 with optional HSL v2.01.6198, optional SCL v2.13.001, optional ACL v3.03.003, optional ACL v3.04.001, optional v3.05.002, optional HCL v1.13.001, optional RCL v1.10.006 and with specific IC-dedicated firmware identifier 80.203.003 and Flash Loader v8.06.001 has been certified under the EUCC scheme in accordance to the provisions of the Implementing Regulation (EU) 2024/482. The TOE deliverables are listed in table 1.

The evaluation of the product IFX_CCI_00003Fh, IFX_CCI_000059h, IFX_CCI_00005Bh, IFX_CCI_00003Ch, IFX_CCI_00003Dh, IFX_CCI_00005Ah design step G11 and H11 with optional HSL v2.01.6198, optional SCL v2.13.001, optional ACL v3.03.003, optional ACL v3.04.001, optional v3.05.002, optional HCL v1.13.001, optional RCL v1.10.006 and with specific IC-dedicated firmware identifier 80.203.003 and Flash Loader v8.06.001 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 6 August 2026. TÜV Informationstechnik GmbH is a notified evaluation facility (ITSEF).

The Evaluation Technical Report (ETR) [ETR] was provided by the ITSEF according to the Common Criteria [CC], the Methodology [CEM], the requirements of the Scheme [EUCC-VO],[EUCC_PROG].

The evaluation has confirmed:

- CC Version and Release: see [CC] and [CEM]
- PP Conformance: Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014 [PP]
- Assurance Level: EUCC High with component AVA_VAN.5
- Assurance Package: EAL 5
- Augmentation: Global Assurance: ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_FLR.3, ALC_TAT.3, ATE_FUN.2, ATE_COV.3, AVA_VAN.5; sub-TSF assurance level: EAL6 augmented with ALC_FLR.3

The Security Target [ST] 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 [PP].

A detailed description of the security functionality, addressed threats, organisational security policies and the operational environment can be found in the Security Target [ST].

Depending on the blocking configuration, the product can have e.g. different user available memory sizes and can come with or without individual accessible cryptographic coprocessors. All products are identical in regard to module design, layout, and footprint. All possible configuration options are described in Section 2.

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

The vulnerability assessment results stated in this certificate do not express an appraisal of the strength and suitability of the cryptographic algorithms implemented in the TOE (see BSIG Section 52, Para. 4, Clause 2).

The certification results apply only to the version of the product indicated in the certificate and on the condition that all the statements and indications are kept as detailed in this Certification Report. Neither the BSI nor any other organisation that recognises or gives effect to this certificate implicitly or explicitly guarantee or endorse the certified TOE.

2. Identification of the TOE

The Information and communications technology product is identified as follows:

IFX_CCI_00003Fh, IFX_CCI_000059h, IFX_CCI_00005Bh, IFX_CCI_00003Ch, IFX_CCI_00003Dh, IFX_CCI_00005Ah design step G11 and H11 with optional HSL v2.01.6198, optional SCL v2.13.001, optional ACL v3.03.003, optional ACL v3.04.001, optional v3.05.002, optional HCL v1.13.001, optional RCL v1.10.006 and with specific IC-dedicated firmware identifier 80.203.003 and Flash Loader v8.06.001

Holder of the certificate: Infineon Technologies AG
Am Campeon 1-15
85579 Neubiberg
https://www.infineon.com/product-information/cybersecurity-information

The following table outlines the TOE deliverables:

TOE Component	Release / Date	Form of Delivery	Comment
Hardware			
IFX_CCI_00003Fh, IFX_CCI_000059h, IFX_CCI_00005Bh, IFX_CCI_00003Ch, IFX_CCI_00003Dh, IFX_CCI_00005Ah	G11 and H11	Customer chooses delivery method (see [ST, 1.4.5]).	–
Firmware			
BOS	80.203.00.3	Stored on the delivered hardware.	–
Flash Loader	v8.06.001	Stored on the delivered hardware.	–
Software			
ACL: RSA2048 Library	3.03.003 or 3.04.001 or 3.05.002	Secured download (L251 Library File (object code)) via ishare.	Optional; depending on order
ACL: RSA4096 Library	3.03.003 or 3.04.001 or 3.05.002	Secured download (L251 Library File (object code)) via ishare.	Optional; depending on order
ACL: EC Library	3.03.003 or 3.04.001 or 3.05.002	Secured download (L251 Library File (object code)) via ishare.	Optional; depending on order

TOE Component	Release / Date	Form of Delivery	Comment
ACL: Toolbox Library	3.03.003 or 3.04.001 or 3.05.002	Secured download (L251 Library File (object code)) via ishare.	Optional; depending on order
ACL: Base Library	3.03.003 or 3.04.001 or 3.05.002	Secured download (L251 Library File (object code)) via ishare.	Optional; depending on presence of RSA, EC and Toolbox
SCL	2.13.001	Secured download (L251 Library File (object code)) via ishare.	Optional; depending on order. Consists of four library files
HCL	1.13.001	Secured download (L251 Library File (object code)) via ishare.	Optional; depending on order. Consists of two library files
RCL	1.10.006	Secured download (L251 Library File (object code)) via ishare.	Optional; depending on order. Consists of three library files
HSL	2.01.6198	Secured download (L251 Library File (object code)) via ishare.	Optional; depending on order
Guidance Documentation for IFX_CCI_00003Fh, IFX_CCI_000059h, and IFX_CCI_00005Bh			
32-bit Security Controller – V20 Hardware Reference Manual	See [AGD_HRM_V20] in 13.2.	Secured download (personalized PDF) via ishare.	Document depends on derivate ordered.
32-bit Security Controller - V20 Security Guidelines	See [AGD_Sec_V20] in Section 13.2.	Secured download (personalized PDF) via ishare.	Document depends on derivate ordered.
32-bit Security Controller – V20 Errata Sheet	See [AGD_ES_V20] in Section 13.2.	Secured download (personalized PDF) via ishare.	Document depends on derivate ordered.
Guidance Documentation for IFX_CCI_00003Ch, IFX_CCI_00003Dh, and IFX_CCI_00005Ah			
32-bit Security Controller – V21 Hardware Reference Manual	See [AGD_HRM_V21] in Section 13	Secured download (personalized PDF) via ishare.	Document depends on derivate ordered.
32-bit Security Controller - V21 Security Guidelines	See [AGD_Sec_V21] in Section 13	Secured download (personalized PDF) via ishare.	Document depends on derivate ordered.
32-bit Security Controller – V21 Errata Sheet	See [AGD_ES_V21] in Section 13	Secured download (personalized PDF) via ishare.	Document depends on derivate ordered.
Guidance Documentation valid for all TOE Variants			
ARMv7-M Architecture Reference Manual	DDI 0403D ID0 21310 / 2010-02-12	Secured download (personalized PDF) via ishare.	–
Production and personalization 32-bit ARM-based security controller User´s Manual	3.5 / 2021-12-17	Secured download (personalized PDF) via ishare.	–

TOE Component	Release / Date	Form of Delivery	Comment
32-bit Security Controller SLC37 (65 nm Technology) Programmer's Reference Manual	5.3 / 2022-07-08	Secured download (personalized PDF) via ishare.	–
32-bit Security Controller Crypto@2304T V3 User Manual	3.0 / 2024-06-21	Secured download (personalized PDF) via ishare.	Optional; delivered if the Crypto2304T is available on the TOE.
ACL37-Crypto2304T-C65 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox 32-bit Security Controller User interface manual	3.03.003 / 2026-05-11 3.04.001 / 2026-05-11 3.05.002 / 2026-05-11	Secured download (personalized PDF) via ishare.	Optional; delivered if one of the Asymmetric Crypto Libraries (ACL) is available on the TOE.
SCL37-SCP-v4-C65 Symmetric Crypto Library for SCP-v4 AES/DES/MAC 32-bit Security Controller User interface manual	2.13.001 / 2024-07-25	Secured download (personalized PDF) via ishare.	Optional; delivered if the Symmetric Crypto Library (SCL) is available on the TOE.
RCL37-X-C65 Random Crypto Library for SCP-v4 & HRNG-v2 DRBG/HWRNG 32-bit Security Controller User interface manual	1.10.006 / 2020-06-16	Secured download (personalized PDF) via ishare.	Optional; delivered if the Random Crypto Library (RCL) is available on the TOE.
HCL37-CPU-C65 Hash Crypto Library for CPU SHA 32-bit Security Controller User interface manual	1.13.001 / 2020-03-11	Secured download (personalized PDF) via ishare.	Optional; delivered if the Hash Crypto Library (HCL) is available on the TOE.
SLxx7-C65 Hardware Support Library	02.01.6198 / 2019-07-05	Secured download (personalized CHM) via ishare.	Optional; delivered if the Hardware Support Library (HSL) is available on the TOE.

Table 1: Deliverables of the TOE

3. Security Policy

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

The security policy enforced is defined by the selected set of security functional requirements and implemented by the TOE. It covers the following issues:

The security policy of the TOE is to provide basic security functionalities to be used by the smart card operating system and the smart card application, thus providing an overall smart card system security. Therefore, the TOE will implement a symmetric cryptographic block cipher algorithm (Triple-DES and AES) to ensure the confidentiality of plain text data by encryption and to support secure authentication protocols. This functionality is provided by the Symmetric Co-Processor (SCP) and the Symmetric Cryptographic Library (SCL).

The SCP as well as the SCL implement countermeasures against SPA, DPA, and DFA attacks.

The TOE hardware is also equipped with a HRNG module, which can be configured to different random number generators following [AIS20] and [AIS31]. Additionally, the TOE can come with the Random Cryptographic Library (RCL) which implements a [N890A]-conformant DRBG. All RNG implementations are protected against leakage attacks as well as fault injec-tion.

The RSA library is used to provide a high-level interface to RSA (Rivest, Shamir, Adleman) cryptography implemented on the hardware component Crypto2304T and includes counter-measures against SPA, DPA and DFA attacks. The EC library is used to provide a high-level interface to Elliptic Curve cryptography implemented on the hardware component Crypto2304T and includes countermeasures against SPA, DPA and DFA attacks.

The Hash Cryptographic Library (HCL) implements functionality for SHA-1/2 digest computation over user-provided data. The HCL implements countermeasures against side-channel attacks as well as fault attacks.

Besides that, the TOE can come with the optional Hardware Support Library (HSL), which provides a simplified interface for NVM management and provides the possibility to write tearing safe into the NVM.

As the TOE is a hardware security platform, the security policy of the TOE is also to provide protection against leakage of information (e.g. to ensure the confidentiality of cryptographic keys during AES, Triple-DES, RSA and EC cryptographic functions performed by the TOE), against physical probing, against malfunctions, against physical manipulations and against abuse of functionality. Hence, the TOE shall

- maintain the integrity and the confidentiality of data stored in the memory of the TOE and
- maintain the integrity, the correct operation and the confidentiality of security functionalities (security mechanisms and associated functions) provided by the TOE.

Specific details concerning the above-mentioned security policies can be found in Chapters 6 and 7 of the Security Target [ST].

4. Assumptions and Clarification of Scope

The assumptions defined in the Security Target and some aspects of threats and organisational security policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled and measures to be taken by the IT environment, the user or the risk manager. The following topics are of relevance:

The ST includes the following security objective for the IC embedded software developer: OE.RespAppl.

The objective OE.Resp-Appl states that the IC embedded software developer shall treat user data (especially keys) of the composite product appropriately. The IC embedded software developer gets sufficient information on how to protect user data adequately in the security guidelines [AGD_Sec].

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

The objective OE.Process-Sec-IC requires the protection of the TOE, as well as of its manufacturing and test data up to the delivery to the end-consumer. As defined in [ST, 2.2.5] the TOE can be delivered to the composite product manufacturer after phase 3 or after phase 4 (as complete modules, plain wafers, bare dies, in any IC case, or in any type of package). However, the single chips are identical in all cases. This means that the test mode is deactivated and the TOE is locked in the user mode. Therefore, it is not necessary to distinguish between these forms of delivery. Since Infineon has no information about the security requirements of the implemented IC embedded software it is not possible to define any concrete security requirements for the environment of the composite product manufacturer.

The objective OE.TOE_Auth requires that the environment has to support the authentication and verification mechanism and has to know the corresponding authentication reference data. The composite product manufacturer receives sufficient information with regard to the authentication mechanism in [AGD_PPUM, 4].

The objective OE.Loader_Usage requires that the authorised user has to support the trusted communication with the TOE by protecting the confidentiality and integrity of the loaded data and he has to meet the access conditions defined by the flash loader. [AGD_PPUM, 4] provides sufficient information regarding this topic.

The objective OE.Lim_Block_Loader requires the composite product manufacturer to protect the loader against misuse, to limit the capability of the loader and to terminate the loader irreversibly after the intended usage. The permanent deactivation of the flash loader is de-scribed in [AGD_PPUM, 4]. This objective for the environment originates from the “Package 1: Loader dedicated for usage in secured environment only”. However, this TOE also implements “Package 2: Loader dedicated for usage by authorized users only” and thus, the flash loader can also be used in an unsecure environment and is able to protect itself against misuse if the authentication and download keys are handled appropriately.

The objective OE.Secure_Delivery complements the second item of the previous OE in case the TOE is ordered with a (temporarily) deactivated Flash Loader but already flashed customer software. In this case, the customer is required to implement mechanisms to prevent attacks during TOE transport as required by the security needs of the loaded IC Embedded Software. This requirement is provided to the user as part of [AGD_PPUM, 3] describing the relevant scenario:

> *Scenario 2: The customer orders Flash Loader chips and asks Infineon to fill the NVM with the appropriate application code and data. […] On delivery, the customer application is active and responsible for transport protection.*

As Infineon has no information about the security requirements of the implemented IC em-bedded software, it is not possible for the guidance to define any concrete security requirements for the environment of the IC Embedded Software Developer or Composite Product Manufacturer.

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

5. Architectural Information

Detailed information in the TOE architecture is to be found in the [ST].

6. Supplementary Cybersecurity Information

The evaluated documentation as outlined in table 1 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.

The developers website as stated in chapter 2 provides the following supplementary information:

- the period during which support is offered (esp. security related updates)
- contact information of the manufacturer or provider and accepted methods for receiving vulnerability information from end users and security researchers
- a reference to online repositories listing publicly disclosed vulnerabilities related to the TOE/ICT, ICT service or ICT process and to any relevant cybersecurity advisories.

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

7. IT Product Testing

All tests have been carried out by ITSEF:

TÜV Informationstechnik GmbH,
Unternehmensgruppe TÜV NORD
Am TÜV 1
45307 Essen
under the responsibility of certification Body

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87
Postfach 20 03 63
D-53175 Bonn

Please refer to chapter 1 for details on assurance levels or packages involved into testing.

The following State-of-the-art-documents were applied:

Refer to chapter 9.1.

The developers' testing effort can be summarised in the following aspects.

TOE test configuration:

The tests are performed with the TOE, an emulator and a simulator.

Developer's testing approach:

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

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

- Simulation tests (design verification)
- Qualification test
- Verification test
- Security Evaluation tests
- Production tests

Amount of developer testing performed:

The tests are performed on security mechanism-, subsystem- and module-level.

As demonstrated during ATE_COV.3 the developer has tested all security mechanisms and TSFIs as given in [ADV_FSP] and [ADV_ARC].

As demonstrated during ATE_DPT.3 the developer has tested all TSF subsystems and modules against the TOE design as given in [ADV_TDS] and against the security architecture description as given in [ADV_ARC].

TOE security functionality tested:

The following TOE security functionalities were tested:

- SF_DPM: Device Phase Management,
- SF_PS: Protection against Snooping,
- SF_PMA: Protection against Modifying Attacks,
- SF_PLA: Protection against Logical Attacks,
- SF_CS: Cryptographic Support.

Overall developer testing results:

The TOE has passed all tests defined in the developer’s test plan so that all TSFs have been successfully tested considering [ADV_FSP], [ADV_TDS] and [ADV_ARC].

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

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

Evaluator Tests

Independent Testing according to ATE_IND:

Testing approach:

The evaluator’s testing effort can be summarised in the way described in the following:

The evaluator's objective regarding this aspect was to test the functionality of the TOE as described in [ST], [ADV_FSP], [ADV_ARC] and [ADV_TDS], and to verify the developer's test results by repeating developer's tests contained, respectively referenced, in [ATE] and to add independent tests.

In the course of 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,
- Optional library tests.

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

TOE test configuration:

The tests are performed with the chips IFX_CCI_00003Fh uniquely identified by the chip identification data. Different chip types are prepared for the tests. One of these types is the

configuration, which is delivered to the user. The others enable the download of test programs or may include deactivated security mechanisms. The remaining functionality is the same for all chips.

Selection criteria:

All security mechanisms and security features (portions of the TSF) and related interfaces were tested. Therefore, no selection criteria are applied. All security mechanisms and related interfaces are tested regarding their functional behaviour. The tests were chosen to perform at minimum one test for each security mechanism of TSF and related interfaces.

Interfaces tested:

The evaluator included all security mechanisms and security features and related interfaces into the testing subset. Portions of TSF and related interfaces, as identified in the functional specification, which are tested:

- SF_DPM: Device phase management,
- SF_PS: Protection against snooping,
- SF_PMA: Protection against modifying attacks,
- SF_PLA: Protection against logical attacks,
- SF_CS: Cryptographic Support.

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.

8. Evaluated Configuration

This certificate covers the following configurations of the TOE:

Smartcard IC IFX_CCI_00003Fh, IFX_CCI_000059h, IFX_CCI_00005Bh, IFX_CCI_00003Ch, IFX_CCI_00003Dh, IFX_CCI_00005Ah G11 and H11 (Tainan).

TOE Configurations:

The user has the possibility to configure the TOE, either during production or by Infineon's BPU or PIN-Letter concepts[6]. The options are listed in [ST, 1.4.7] and comprise e.g. the memory sizes of the RAM, NVM and Cache, the availability of the cryptographic coprocessors (symmetric and asymmetric), and the availability of the communication interfaces.

Especially the possibility to configure the cryptographic coprocessors is of importance to the TOE, as their presence affects the provided security functionalities.

If the symmetric cryptographic co-processor (SCP) is not available to the user, then the TOE will not provide any AES, TDES, or MAC calculations.

A blocked asymmetric cryptographic co-processor (Crypto2304T) means, that the user is not able to use the optional RSA, EC, and Toolbox libraries.

The different Common Criteria Identifiers (CCIs), which are used for the TOE, are all TOE derivatives derived from the equal hardware design results. The firmware also remains entirely equal throughout all derivatives. The different identifiers represent different configuration options available. This differences are achieved by means of blocking (i.e. the blocked modules are still physically present on the TOE, but not accessible). The

[6]Please note that the BPU and PIN-Letter process require an active Flash Loader.

products IFX_CCI_00003Ch, IFX_CCI_00003Dh and IFX_CCI_00005Ah run through the Burn-In process during the production to reduce the error rate. The TOE IFX_CCI_00003Dh is not available for customers and used by Infineon Technologies AG only. The difference between the design steps is that the design step H11 does not support the SPI interface.

TOE Optional Software Libraries

The TOE can be delivered with optional software libraries, as described in [ST, 1.2 / 1.4.1.2].

All other Smartcard Embedded Software does not belong to the TOE and is not subject of the evaluation.

The RSA, EC, and Toolbox libraries are parts of the Asymmetric Cryptographic Library (ACL). Additionally a Base library is part of the ACL. If at least one of the RSA, EC, and Toolbox libraries is selected by the user, the Base library is automatically included. All parts of the ACL have to be of the same version number. The following optional ACL versions are available:

- v3.03.003 (ACL-1),
- v3.04.001 (ACL-2), and
- v3.05.002 (ACL-3),

If the user decides not to use an optional software library, the library is not delivered to the user and the accompanying additional specific security functionality is not provided by the TOE. Deselecting an optional software library excludes the code implementing the corresponding functionality, which the user decided not to use. Excluding the code of the deselected functionality has no impact on any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use the functionality.

TOE Firmware Components

The firmware of the TOE is represented by the firmware identifier 80.203.00.3. The firmware components comprise the BOS and the flash loader version 8.06.001.

TOE User Guidance

The user guidance is part of the TOE. Parts of the user guidance relate to optional configuration options, and are, as such, also optional. These documents are only delivered if the corresponding optional component is ordered. The user guidance is addressed in [ST, 1.2 / 1.4.1.3].

9. Results of the Evaluation

9.1. CC specific results

The ITSEF produced and provided the Evaluation Technical Reports (ETR) [ETR] according to the the requirements of the Scheme [EUCC-VO],[EUCC_PROG], the Common Criteria [CC], the Common Evaluation Methodology [CEM], and all relevant interpretations and guidelines of the Scheme (AIS) [AIS].

For the evaluation from component level AVA_VAN.4 onwards the following state-of-the-art documents and supporting documents were applied:

- 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 Informations-technik.
- 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 4, 2025-04-11, Bundesamt für Sicherheit in der Informationstechnik, Bundesamt für Sicherheit in der Informationstechnik.
- Updates to the Developer Evidence and ETR Templates for the Evaluation of Random Number Generators, Version 1.0, 2025-07-04, Bundesamt für Sicherheit in der Informationstechnik.
- 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.
- 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.
- 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.
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 31, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 4, 2025-04-11, Bundesamt für Sicherheit in der Informationstechnik.
- Updates to the Developer Evidence and ETR Templates for the Evaluation of Random Number Generators, Version 1.0, 2025-07-04, Bundesamt für Sicherheit in der Informationstechnik.
- Developer evidence for the evaluation of a physical true random number 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.
- 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.
- 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.
- Guideline for the Development and Evaluation of formal security pol-icy models in the scope of ITSEC and Common Criteria, Version 2.0, 2007-12-04, 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.
- Application Notes and Interpretation of the Scheme (AIS) – AIS 42, Guidelines for the Developer Documentation, Version 1, 2008-05-21, 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.
- Guidelines for Evaluating Machine-Learning based Side-Channel At-tack Resistances, Version 2024-01, 2024-02-29, Bundesamt für Sicherheit in der Informationstechnik.
- Review-Protokoll zum (Krypto-)AVA-KickOff, 2019-08-23, Bundesamt für Sicherheit in der Informationstechnik.
- Guidelines for Evaluating Side-Channel and Fault Attack Resistance of Elliptic Curve Implementations, Version 3.0, 2024-02-29, Bundesamt für Sicherheit in der Informationstechnik.
- Methodology for cryptographic rating of memory encryption schemes used in smartcards and similar devices, Version 1.0, 2013-10-31, Bundesamt für Sicherheit in der Informationstechnik.

- Guidelines for Evaluating Side-Channel-Attack Resistance of RSA, DSA and Diffie-Hellman Key Exchange Implementations, Version 2024-01, 2024-02-29, Bundesamt für Sicherheit in der Informationstechnik.
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 47, Regelungen zu Site Certification, Version 1.1, 2013-12-04, Bundesamt für Sicherheit in der Informationstechnik.
- CC Supporting Document Guidance – Site Certification, Version 1.0, Revision 1, 2007-10, CCDB-2007-11-001.
- Details for the structure and content of the ETR for Site Certification, Version 1.0, 2010, Bundesamt für Sicherheit in der Informationstechnik.
- Guidance for Site Certification, Version 1.1, 2013-12-04, Bundesamt für Sicherheit in der Informationstechnik.
- Transition Policy to CC:2022 and CEM:2022, 2023-04-20, Common Criteria Recognition Arrangement Management Committee, CCMC-2023-04-001.
- EUCC Scheme State-of-The-Art Document - Security Architecture requirements (ADV_ARC) for smart cards and similar devices extended to Secure Sub Systems in SoCs, Version 1.1, 2023-10, ENISA.
- EUCC Scheme State-of-The-Art Document - Application of Attack Potential to Smartcards and Similar Devices, Version 2, 2025-02, ENISA.
- EUCC Scheme State-of-The-Art Document - ETR for Composite Evaluation Template, Version 1, 2025-09, ENISA.
- EUCC Scheme State-of-The-Art Document - The Application of CC to Integrated Circuits, Version 2, 2024-12, ENISA.
- EUCC Scheme State-of-The-Art Document - Minimum ITSEF requirements for security evaluations of Smart Cards and similar devices, Version 1.1, 2023-10, ENISA.
- EUCC Scheme State-of-The-Art Document - Minimum Site Security Requirements, Version 2, 2025-02, ENISA.
- EUCC Scheme State-of-The-Art Document - Certification of “open” smart card products, Version 1.1, 2023-10, ENISA.
- EUCC Scheme State-of-The-Art Document - ADV_SPM.1 interpretation for CC:2022 transition, Version 1.1, 2025-10, ENISA.
- EUCC Scheme State-of-The-Art Document - STAR methodology, Version 1, 2025-02, ENISA.
- Attack Methods for Smartcards and Similar Devices, Version 2.5 (confidential), 2022-05, Joint Interpretation Working Group.
- Collection of Developer Evidence, Version 1.5, 2012-01, Joint Interpretation Library.
- Security requirements for post-delivery code loading, Version 2.0, 2024-09, Joint Interpretation Working Group.
- Remaining Strength of Asymmetric Cryptographic Mechanisms after Partial Key Leakage, Version 1.0 (confidential), 2020-06, Joint Interpretation Working Group.

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

On advise by the Certification Body and consent by the certificate holder the following guidance further specific for the technology of the product [AIS] (AIS 34) was applied:

For RNG assessment the scheme interpretations AIS 20/31 was used (see [AIS]).

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

The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

As a result of the evaluation, the verdict PASS is confirmed for the assurance components that are identified in chapter 1 of this report and claimed by the Security Target [ST] for the corresponding TOE. The corresponding TOE is identified in chapter 2 of this report.

The certificate

- is uniquely identified by: EUCC-3087-2026-0018, administration ID BSI-DSZ-CC-1287-2026
- was issued on: 1 October 2026
- is valid until: 30 September 2031

The results of the evaluation are only applicable to the TOE as defined in chapter 1 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 52, Para. 4, Clause 2). But cryptographic functionalities with a security level of lower than 120 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

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

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits
Symmetric Co-Processor (SCP)				
Cryptographic primitive Confidentiality Integrity	TDES in modes ECB, CBC CBC-MAC, CBC-MAC-ELB	[N867] [N838A] [ISO_9797-1]	|k| = 112 (for legacy use only, see [N867]), |k| = 168	No
Cryptographic primitive Confidentiality Integrity	AES in modes ECB, CBC CBC-MAC, CBC-MAC-ELB	[FIPS197] [N838A] [ISO_9797-1]	|k| = 128, 192, 256	ECB: No CBC, CBC-MAC: Yes
HRNG				
RNG	Physical True RNG PTG.2	[AIS31]	N/A	N/A
	Hybrid Random Number Generator PTG.3	[AIS31]	N/A	N/A
	Deterministic Random Number Generation DRG.3	[AIS31]	N/A	N/A
	Key Stream Generation DRG.2	[AIS31], [ADV_TDS _Achterbahn]	N/A	N/A
Random Cryptographic Library (RCL)				
RNG	Deterministic Random Number Generation DRG.3	[AIS31], [N890A]	N/A	N/A
Symmetric Cryptographic Library (SCL)				
Cryptographic primitive Confidentiality Integrity Integrity Confidentiality	TDES in modes ECB, CBC, CTR, CFB CMAC Retail-MAC PCBC	[N867] [N838A] [N838B] [ISO_9797-1] [Schneider]	|k| = 112 (for legacy use only, see [N867]), |k| = 168	No No
Cryptographic primitive Confidentiality Integrity Confidentiality	AES in modes ECB, CBC, CTR, CFB CMAC PCBC	[FIPS197] [N838A] [N838B] [Schneider]	|k| = 128, 192, 256	ECB: No CBC, CTR, CFB, CMAC: Yes
Asymmetric Cryptographic Libraries (ACL 3.03.003, 3.04.001, and 3.05.002)				
Confidentiality	RSAEP encryption	[PKCS #1, 5.1.1]	512 – 2112	
Confidentiality	IFEP-RSA encryption	[IEEE_P1363, 8.2.2]	512 – 2112	No
Confidentiality	RSADP decryption	[PKCS #1, 5.1.2]	512 – 2112	No
Confidentiality	IFDP-RSA decryption	[IEEE_P1363, 8.2.1 (I) / 8.2.3]	512 – 2112	No

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits
Authenticity	RSASP1 signature generation	[PKCS #1, 5.2.1]	512 – 2112	No
Authenticity	IFSP-RSA1 signature generation	[IEEE_P1363, 8.2.1 (I) / 8.2.4]	512 – 2112	No
Authenticity	RSAVP1 signature verification	[PKCS #1, 5.2.2]	512 – 4224	No, <2800 Yes, >= 2800
Authenticity	IFVP-RSA1	[IEEE_P1363, 8.2.5]	512 – 4224	No, <2800 Yes, >= 2800
Key generation	Proprietary RSA key-pair generation	[PKCS #1, 3.1 / 3.2] [IEEE_P1363, 8. 1.3.1]	512 – 4224	No, <2800 Yes, >= 2800
Authenticity	ECDSA signature generation	[ANS X9.62, 7.3], [ISO_14888-3, 6.4.3], [IEEE_P1363, 7. 2.7]	160 – 521	No, <240 Yes, >=240
Authenticity	ECDSA signature verification	[ANS X9.62, 7.4. 1], [ISO_14888-3, 6.4.4], [IEEE_P1363, 7. 2.8]	160 – 521	No, <240 Yes, >=240
Key generation	Elliptic Curve key generation	[ANS X9.62, A.4. 3], [ISO_14888-3, 6.4.2], [IEEE_P1363, A. 16.9]	160 – 521	No, <240 Yes, >=240
Key agreement	Elliptic Curve Diffie-Hellman (ECDH) key agreement	[ANS X9.63, 5.4.1], [ISO_11770-3, D. 6] [IEEE_P1363, 7. 2.1]	160 – 521	No, <240 Yes, >=240
Hash Cryptographic Library (HCL)				
Digest computation	SHA-1	[FIPS180-4]	160	No
Digest computation	SHA-224, SHA-256, SHA-384, SHA-512, SHA-512, SHA-512/224, SHA512/256	[FIPS180-4]	224 - 512	N/A

Table 2: TOE cryptographic functionality

Legislatives and Standards:

- IEEE Graphic Symbols for Logic Functions (Including and incorporating IEEE Std 91a-1991, Supplement to IEEE Standard Graphic Symbols for Logic Functions), 1991-06-27, American National Standards Institute.

- American National Standard for Financial Services ANS X9.62-2005, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), 2005-11-16, American National Standards Institute.

● American National Standard for Financial Services X9.63-2011, Public Key Cryptography for the Financial Services Industry - Key Agreement and Key Transport Using Elliptic Curve Cryptography, 2011-12-21, American National Standards Institute.

● ECC Brainpool Standard Curves and Curve Generation, Version 1.0, 2005, M. Lochter, https://web.archive.org/web/20170921224120/http://www.ecc-brainpool.org/download/Domainparameters.pdf.

● FIPS PUB 180-4 Federal Information Processing Standards Publication Secure Hash Standard (SHS), 2015-08, National Institute of Standards and Technology (NIST).

● Federal Information Processing Standards Publication FIPS PUB 186-4, Digital Signature Standard (DSS), 2013-07, National Institute of Standards and Technology (NIST).

● Federal Information Processing Standards Publication FIPS PUB 186-5, Digital Signature Standard (DSS), 2023-02-03, National Institute of Standards and Technology (NIST).

● Federal Information Processing Standards Publication PUB 197, Advanced Encryption Standard (AES), Updated Version, 2023-05-09, National Institute of Standards and Technology (NIST).

● IEEE P1363. Standard specifications for public key cryptography, 2000, IEEE.

● ISO/IEC 11770-3: Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques, 2008-07, ISO/IEC. Including Technical Corrigendum 1, published 2009-09-15

● ISO/IEC 14888-3, IT Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms, 2006, ISO/IEC, including Technical Corrigendum 2, published 2009-02-15.

● ISO 18033-3: Information technology - Security techniques – Encryption algorithms – Part 3: Block ciphers, 2010, ISO/IEC.

● Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher, 2011-03, ISO/IEC.

● NIST Special Publication 800-38A – Recommendation for Block Cipher Modes of Operation – Methods and Techniques, 2001-12, National Institute of Standards and Technology (NIST).

● NIST Special Publication 800-38B – Recommendation for Block Cipher Modes of Operation – The CMAC Mode for Authentication, Up-dated Version, 2016-10-06, National Institute of Standards and Technology (NIST).

● NIST Special Publication 800-67 – Revision 2 – Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, rev. 2, 2017-11, National Institute of Standards and Technology (NIST).

● NIST Special Publication 800-90A – Revision 1 – Recommendation for Random Number Generation Using Deterministic Random Bit Generators, rev. 1, 2015-06, National Institute of Standards and Technology (NIST).

● PKCS #1: RSA Cryptography Standard, Version 2.2, 2012-10-17, RSA Laboratories.

● RFC 5639 - Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, 2010-03, The Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc5639.txt.

10. Obligations and Notes for the Usage of the TOE

Table 1: Deliverables of the TOE outlines the documents that contain necessary information on the intended use of the TOE including all security related information, conditions and instructions to be taken into account by the user. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target and not covered by the TOE itself need to be met by the operational environment of the TOE.

The customer or user of the TOE shall take the statements of this certificate into account in its system risk management process. The user should define measures in its risk management that respond to emerging and new attack methods and techniques to the TOE until the TOE has been re-assessed.

The user also has to consider in its risk management the limited validity for the usage of cryptographic algorithms as outlined in chapter 9.

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" [ETRfCOMP].

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.

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 which 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 [AGD_Sec], [AGD_HRM], [AGD_ES], [AGD_PRM], [AGD_Crypto], [AGD_ACL], [AGD_SCL], [AGD_HCL], [AGD_HSL], and [AGD_RCL] have to be considered.

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

- All security hints described in [AGD_PPUM] have to be considered.

In addition, the following hint resulting from the evaluation of the ALC evaluation aspect has to be considered:

- The security IC embedded software developer can deliver his software either to Infineon to let them implement it in the TOE (in the Flash memory) or to the composite product manufacturer to let him download the software in the Flash memory.

- The delivery procedure from the security IC embedded software developer to the composite product manufacturer is not part of this evaluation and a secure delivery can be required (cf. OE.Secure_Delivery as well as Sections 2.1 and 4.2 above).
- 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 [ST] of the Information and communications technology (ICT) product is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the provisions of the EUCC certification scheme policy (see Implementing Regulation (EU) 2024/482, Annex V, V.2).

For the purpose of publishing, the Security Target [ST] of the TOE / Information and communications technology (ICT) product is provided within a separate document as Annex A of this report.

12. Regulation specific aspects (eIDAS, QES)

None

12.1. Acronyms

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
ICT	Information and communications technology
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

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

[EUCC-VO] Implementing Regulation (EU) 2024/482 of the European Parliament and of the Council of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)
and
Implementation Regulation (EU) 2025/2462 of 8 December 2025 amending Implementing Regulation (EU) 2024/482 as regards definitions, ICT product series certification, assurance continuity and state-of-the-art document

[CC] ISO 15408:2022, Common Criteria for Information Technology Security Evaluation
- Part 1: Introduction and general model
- Part 2: Security functional components
- Part 3: Security assurance components
- Part 4: Framework for the specification of evaluation methods and activities
- Part 5: Pre-defined packages of security requirements
https://www.iso.org/standard/72891.html

https://www.iso.org/standard/72892.html
https://www.iso.org/standard/72906.html
https://www.iso.org/standard/72913.html
https://www.iso.org/standard/72917.html

[CEM] ISO 18045:2022: Information technology Security techniques Methodology for IT security evaluation
https://www.iso.org/standard/72889.html

[EUCC_SOTA] EUCC state-of-the-art documents:
https://certification.enisa.europa.eu/publications/eucc-state-art-documents_en

[EUCC_PROG] EUCC program of the BSI: Scheme documentation describing the certification process (EUCC), https://www.bsi.bund.de/zertifizierung

[EUCC_CERT] EUCC Certificates, periodically updated list published on ENISA's website on European cybersecurity certification schemes (https://certification.enisa.europa.eu/) but also on BSI's website (https://www.bsi.bund.de/zertifizierungsreporte)

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

[ST] Security Target BSI-DSZ-CC-1287-2026, Version 3.6, 2026-05-28, "Confidential Security Target IFX_CCI_00003Fh IFX_CCI_000059h IFX_CCI_00005Bh IFX_CCI_00003Ch IFX_CCI_00003Dh IFX_CCI_00005Ah G11 and H11 including optional software libraries: Flash Loader according Package1 and Package2, HCL, RCL, HSL, ACL and SCL, Resistance to attackers with HIGH attack potential", Infineon Technologies AG (confidential document)
Security Target lite, Version 3.6 2026-05-28, "Public Security Target IFX_CCI_00003Fh IFX_CCI_000059h IFX_CCI_00005Bh IFX_CCI_00003Ch IFX_CCI_00003Dh IFX_CCI_00005Ah G11 and H11 including optional software libraries: Flash Loader according Package1 and Package2, HCL, RCL, HSL, ACL and SCL, Resistance to attackers with HIGH attack potential", Infineon Technologies AG

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

[ETR] Evaluation Technical Report, Version 3, 2026-09-29, „EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY) Common Criteria CC:2022 (Multi-Assurance with global assurance level EAL5 augmented with ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_FLR.3, ALC_TAT.3, ATE_FUN.2, ATE_COV.3, AVA_VAN.5 and sub-TSF assurance level EAL6 augmented with ALC_FLR.3)", TÜV Informationstechnik GmbH, (confidential document)

[ETRfCOMP] ETR for composite evaluation for the Product IFX_CCI_00003Fh, IFX_CCI_000059h, IFX_CCI_00005Bh, IFX_CCI_00003Ch, IFX_CCI_00003Dh, IFX_CCI_00005Ah G11 and H11, Version 3, 2026-09-29, „EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION (ETR COMP) Common Criteria CC:2022 (Multi-Assurance with global assurance level EAL5 augmented with ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_FLR.3, ALC_TAT.3, ATE_FUN.2, ATE_COV.3, AVA_VAN.5 and

[7] specifically

- See section 9.1 for detailed list of used AIS

sub-TSF assurance level EAL6 augmented with ALC_FLR.3)“, TÜV Informationstechnik GmbH (confidential document)

[AGD_Sec] 32-bit Security Controller – V20 Security Guidelines for IFX_CCI_00003Fh, IFX_CCI_000059h, IFX_CCI_00005Bh, 1.00-3147, 2026-02-02, Infineon Technologies AG
32-bit Security Controller – V21 Security Guidelines for IFX_CCI_00003Ch, IFX_CCI_00003Dh, IFX_CCI_00005Ah, 1.00-3148, 2026-02-02, Infineon Technologies AG

[AGD_HRM] 32-bit Security Controller – V20 Hardware Reference Manual, 4.0, 2021-06-29, Infineon Technologies AG
32-bit Security Controller – V21 Hardware Reference Manual, 4.0, 2021-06-29, Infineon Technologies AG

[AGD_ES] 32-bit Security Controller – V20 Errata Sheet, 5.1, 2023-08-04, Infineon Technologies AG
32-bit Security Controller – V21 Errata Sheet, 5.1, 2023-08-04, Infineon Technologies AG

[AGD_PRM] SLC37 (65 nm) Security Controllers Programmer's Reference Manual, 5.3, 2022-07-08, Infineon Technologies AG

[AGD_Crypto] 32-bit Security Controller Crypto2304T V3 User Manual, 3.0, 2024-06-21, Infineon Technologies AG

[AGD_ACL] ACL37-Crypto2304T-C65 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox 32-bit Security Controller User interface manual, 3.03.003, 2026-05-11, Infineon Technologies AG
ACL37-Crypto2304T-C65 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox 32-bit Security Controller User interface manual, 3.04.001, 2026-05-11, Infineon Technologies AG
ACL37-Crypto2304T-C65 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox 32-bit Security Controller User interface manual, 3.05.002, 2026-05-11, Infineon Technologies AG

[AGD_SCL] SCL37-SCP-v4-C65 Symmetric Crypto Library for SCP-v4 AES/DES/MAC 32-bit Security Controller User interface manual, 2.13.001, 2024-07-25, Infineon Technologies AG

[AGD_HCL] HCL37-CPU-C65 Hash Crypto Library for CPU SHA 32-bit Security Controller User interface manual, 1.13.001, 2020-03-11, Infineon Technologies AG

[AGD_HSL] SLxx7-C65 Hardware Support Library, 02.01.6198, 2019-07-05, Infineon Technologies AG

[AGD_RCL] RCL37-X-C65 Random Crypto Library for SCP-v4 & HRNG-v2 DRBG/HWRNG 32-bit Security Con-troller User interface manual, 1.10.006, 2020-06-16, Infineon Technologies AG

[AGD_PPUM] Production and personalization 32-bit Arm®-based security controller, 3.5, 2021-12-17, Infineon Technologies AG

[ADV_TDS] TOE Design IFX_CCI_3Fh, 1.2, 2026-05-18, Infineon Technologies AG

[ADV_ARC] Security Architecture IFX_CCI_3Fh, 1.2, 2026-05-21, Infineon Technologies AG

[ADV_FSP] Functional Specification IFX_CCI_3Fh, 1.3, 2026-05-21, Infineon Technologies AG

C. 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-1287-2026

Evaluation results regarding development and production environment

The IT product IFX_CCI_00003Fh, IFX_CCI_000059h, IFX_CCI_00005Bh, IFX_CCI_00003Ch, IFX_CCI_00003Dh, IFX_CCI_00005Ah design step G11 and H11 with optional HSL v2.01.6198, optional SCL v2.13.001, optional ACL v3.03.003, optional ACL v3.04.001, optional v3.05.002, optional HCL v1.13.001, optional RCL v1.10.006 and with specific IC-dedicated firmware identifier 80.203.003 and Flash Loader v8.06.001 (Target of Evaluation, TOE, also named as ICT product) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM) [CEM].

As a result of the TOE certification, dated 1 October 2026, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support as claimed by the ST [ST] and that are stated in chapter 1 of this report are fulfilled for the development and production sites of the TOE listed below are the Distribution Centres:

Site ID	Company name and address
DHL Singapore	DHL Supply Chain Singapore Pte Ltd., Advanced Regional Center Tampines LogisPark 1 Greenwich Drive Singapore 533865
K&N Großostheim	Kühne & Nagel Stockstädter Strasse 10 63762 Großostheim Germany
KWE Shanghai	KWE Kintetsu World Express (China) Co., Ltd. Building A5 Unit 1/6 & 1/9, Infineon Distribution Center China, Shanghai Pudong Airport Pilot Free Trade Zone No. 530 Zheng Ding Road Shanghai, P.R. China

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [ST]. 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 [ST]) are fulfilled by the procedures of these sites.

Note: End of report