Federal Office
for Information Security

Certification Report

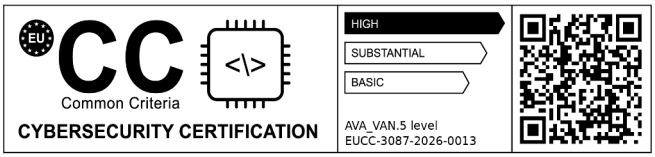
EUCC-3087-2026-0013
Administration ID
BSI-DSZ-CC-1156-V5-2026

for

IFX_CCI_00004Fh, IFX_CCI_000050h - IFX_CCI_000058h, IFX_CCI_00005Ch design step S11 with firmware 80.310.03.0 & 80.310.03.1, optional NRG™ SW 05.03.4097, opt. HSL v3.52.9708, UMSLC lib v01.30.0564, opt.SCL v2.15.000 and v2.11.003, opt. ACL v3.33.003, and v3.35.001 and v3.02.000, opt. RCL v1.10.007, opt. HCL v1.13.002

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

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 R1 [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 R1 [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_00004Fh, IFX_CCI_000050h - IFX_CCI_000058h, IFX_CCI_00005Ch design step S11 with firmware 80.310.03.0 & 80.310.03.1, optional NRG™ SW 05.03.4097, opt. HSL v3.52.9708, UMSLC lib v01.30.0564, opt.SCL v2.15.000 and v2.11.003, opt. ACL v3.33.003, and v3.35.001 and v3.02.000, opt. RCL v1.10.007, opt. HCL v1.13.002 (short Version of the TOE identifier: IFX_CCI_00004Fh S11)has been certified by the certification body of the Federal Federal Office for Information Security (BSI) based on administration ID BSI-DSZ-CC-1156-V4-2024-MA-01. Specific results from the corresponding the evaluation process were re-used.
- The present evaluation of the product IFX_CCI_00004Fh, IFX_CCI_000050h - IFX_CCI_000058h, IFX_CCI_00005Ch design step S11 with firmware 80.310.03.0 & 80.310.03.1, optional NRG™ SW 05.03.4097, opt. HSL v3.52.9708, UMSLC lib v01.30.0564, opt.SCL v2.15.000 and v2.11.003, opt. ACL v3.33.003, and v3.35.001 and v3.02.000, opt. RCL v1.10.007, opt. HCL v1.13.002 was carried out by TÜV Informationstechnik GmbH, located at
  Unternehmensgruppe TÜV NORD
  Am TÜV 1
  45307 Essen.
- The evaluation was completed on 20 July 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 [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 re-assessment of the product’s resistance, the maximum validity period of the certificate is limited. The certificate issued on 17 August 2026 is valid until 23 July 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_00004Fh, IFX_CCI_000050h - IFX_CCI_000058h, IFX_CCI_00005Ch design step S11 with firmware 80.310.03.0 & 80.310.03.1, optional NRG™ SW 05.03.4097, opt. HSL v3.52.9708, UMSLC lib v01.30.0564, opt.SCL v2.15.000 and v2.11.003, opt. ACL v3.33.003, and v3.35.001 and v3.02.000, opt. RCL v1.10.007, opt. HCL v1.13.002 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 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) is the Infineon Security Controller IFX_CCI_00004Fh, IFX_CCI_000050h, IFX_CCI_000051h, IFX_CCI_000052h, IFX_CCI_000053h, IFX_CCI_000054h, IFX_CCI_000055h, IFX_CCI_000056h, IFX_CCI_000057h, IFX_CCI_000058h, IFX_CCI_00005Ch design step S11 with firmware 80.310.03.0 and 80.310.03.1, optional NRG™ SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib v01.30.0564, optional SCL v2.11.003 and v2.15.000, optional ACL v3.02.000, v3.33.003, and v3.35.001, optional RCL v1.10.007, optional HCL v1.13.002 and user guidance.

Please refer to chapter 2 for an identification of the hardware, firmware, and software components, including the corresponding version identifier.

The TOE provides a 32-bit ARMv7-M CPU-architecture. The major components of the core system are the CPU (Central Processing Unit), an MPU (Memory Protection Unit), a Nested Vectored Interrupt Controller (NVIC), and an Instruction Stream Signature (ISS). The dual interface controller can communicate using either the contact based or the contactless inter-face.

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 product IFX_CCI_00004Fh, IFX_CCI_000050h - IFX_CCI_000058h, IFX_CCI_00005Ch design step S11 with firmware 80.310.03.0 & 80.310.03.1, optional NRG™ SW 05.03.4097, opt. HSL v3.52.9708, UMSLC lib v01.30.0564, opt.SCL v2.15.000 and v2.11.003, opt. ACL v3.33.003, and v3.35.001 and v3.02.000, opt. RCL v1.10.007, opt. HCL v1.13.002 has been certified under the EUCC scheme in accordance to the provisions of the Implementing Regulation (EU) 2024/482. This is a certification, based on BSI-DSZ-CC-1156-V4-2024-MA-01. Specific results from the evaluation process BSI-DSZ-CC-1156-V4-2024 and BSI-DSZ-CC-1156-V4-2024-MA-01 were re-used. The TOE deliverables are listed in table 1.

The evaluation of the product IFX_CCI_00004Fh, IFX_CCI_000050h - IFX_CCI_000058h, IFX_CCI_00005Ch design step S11 with firmware 80.310.03.0 & 80.310.03.1, optional NRG™ SW 05.03.4097, opt. HSL v3.52.9708, UMSLC lib v01.30.0564, opt.SCL v2.15.000 and v2.11.003, opt. ACL v3.33.003, and v3.35.001 and v3.02.000, opt. RCL v1.10.007, opt. HCL v1.13.002 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 20 July 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] and 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 6
- Augmentation: 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, an IFX_CCI_00004Fh S11 product can have e.g. different user available memory sizes and can come with or without individual accessible cryptographic coprocessors. All products are identical regarding module design, layout, and footprint. All possible configuration options are achieved by blocking only and are described in the security target [ST] section 1.4.7.

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_00004Fh, IFX_CCI_000050h - IFX_CCI_000058h, IFX_CCI_00005Ch design step S11 with firmware 80.310.03.0 & 80.310.03.1, optional NRG™ SW 05.03.4097, opt. HSL v3.52.9708, UMSLC lib v01.30.0564, opt.SCL v2.15.000 and v2.11.003, opt. ACL v3.33.003, and v3.35.001 and v3.02.000, opt. RCL v1.10.007, opt. HCL v1.13.002

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:

No.	Type	Item / Identifier	Release / Version	Form of Delivery
1.	HW	IFX_CCI_00004Fh, IFX_CCI_000050h, IFX_CCI_000051h, IFX_CCI_000052h, IFX_CCI_000053h, IFX_CCI_000054h, IFX_CCI_000055h, IFX_CCI_000056h, IFX_CCI_000057h, IFX_CCI_000058h, IFX_CCI_00005Ch	S11 (design step)	The customer chooses delivery method (the ST describes under which circumstances transport protection is provided by the TOE).

No.	Type	Item / Identifier	Release / Version	Form of Delivery
2.	FW	BOS & POWS	80.310.03.0 and 80.310.03.1	Stored on the delivered hardware.
3.	FW	Flash Loader	09.12.0003	Stored on the delivered hardware.
4.	SW	NRG™ SW (optional)	05.03.4097	Secure download (L251 Library File) via ishare.
5.	SW	HSL (optional)	v3.52.9708	Secure download (L251 Library File) via ishare.
6.	SW	UMSLC	v01.30.0564	Secure download (L251 Library File) via ishare.
7.	SW	SCL (optional)	v2.11.003 and v2.15.000	Secure download (L251 Library File) via ishare.
8.	SW	ACL (optional)	v3.02.000, v3.33.003, and v3.35.001	Secure download (L251 Library File) via ishare.
9.	SW	RCL (optional)	v1.10.007	Secure download (L251 Library File) via ishare.
10.	SW	HCL (optional)	v1.13.002	Secure download (L251 Library File) via ishare.
11.	DOC	SLC36 32-bit Security Controller – V16, Hardware Reference Manual	5.2 / 2020-12-21	Personalized PDF via secure iShare server
12.	DOC	Security Controllers, SLx1/SLx3 Controller Family, Programmer's Reference Manual	5.8 / 2024-05-24	Personalized PDF via secure iShare server
13.	DOC	SLC36 32-bit Security Controller – V16, Security Guidelines	1.00-3157 / 2026-02-17	Personalized PDF via secure iShare server
14.	DOC	Production and Personalization Manual, 32-bit security controller	09.12 / 2023-03-02	Personalized PDF via secure iShare server
15.	DOC	32-bit Security Controller, Crypto2304T V3, User Manual (optional)	3.0 / 2024-06-21	Personalized PDF via secure iShare server
16.	DOC	HSL for SLCx7V16, Hardware Support Library (optional)	03.52.9708 / 2021-01-25	Personalized PDF via secure iShare server
17.	DOC	UMSLC library for SLCx7 in 40nm, User Mode Security Life Control	01.30.0564 / 20219-08-30	Personalized PDF via secure iShare server
18.	DOC	SCL37-SCP-v440-C40 Symmetric Crypto Library for SCP-v440 AES/DES/MAC (optional, SCL v2.11.003)	2.11.003 / 2021-06-16	Personalized PDF via secure iShare server
19.	DOC	SCL37-SCP-v440-C40 Symmetric Crypto Library for SCP-v440 AES/DES/MAC (optional, SCL v2.15.000)	2.15.000 / 2023-07-20	Personalized PDF via secure iShare server
20.	DOC	ACL37-Crypto2304T-C40 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox (optional, ACL v3.02.000)	3.02.000 / 2026-04-23	Personalized PDF via secure iShare server

No.	Type	Item / Identifier	Release / Version	Form of Delivery
21.	DOC	ACL37-Crypto2304T-C40, Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox (optional, ACL v3.33.003)	3.33.003 / 2026-04-23	Personalized PDF via secure iShare server
22.	DOC	ACL37-Crypto2304T-C40, Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox (optional, ACL v3.35.001)	3.35.001 / 2026-04-23	Personalized PDF via secure iShare server
23.	DOC	RCL37-X-C40 Random Crypto Library for SCP-v440 & RNG-v3 DRBG/HWRNG 32-bit Security Controller, User interface manual (optional)	1.10.007 / 2020-06-16	Personalized PDF via secure iShare server
24.	DOC	HCL37-CPU-C40 Hash Crypto Library for CPU SHA 32-bit Security Controller, User interface manual (optional)	1.13.002 / 2020-05-07	Personalized PDF via secure iShare server

Table 1: Deliverables of the TOE

Please note that NRG™ and the toolbox are out of scope of this evaluation, hence no evaluated TOE guidance documentation applies. Except for the function listed in the ST [ST] section 6.1.6. However, see respective developer provided documentation is available.

The delivery documentation describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the user's site including the necessary intermediate delivery procedures.

Furthermore, the delivery documentation describes in a sufficient manner how the various procedures and technical measures provide for the detection of modifications and any discrepancies between the TOE respective parts of it sent by the TOE Manufacturer and the version received by the Composite Product Manufacturer.

Three different delivery procedures have to be taken into consideration:

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

Respective distribution centers are listed in Appendix B (see end of document).

The individual TOE hardware is uniquely identified by its identification data. Each individual TOE can therefore be traced unambiguously and thus assigned to the entire development and production process.

The hardware part of the TOE is identified by IFX_CCI_00004Fh, IFX_CCI_000050h, IFX_CCI_000051h, IFX_CCI_000052h, IFX_CCI_000053h, IFX_CCI_000054h, IFX_CCI_000055h, IFX_CCI_000056h, IFX_CCI_000057h, IFX_CCI_000058h, IFX_CCI_00005Ch design step S11.

Another characteristic of the TOE are the chip identification data. These chip identification data are accessible via the Generic Chip Identification Mode (GCIM) (see [AGD_HRM], section 5.6).

At TOE start-up the so called GCIM can be chosen by applying special signalling in contactless or contact based communication and the TOE outputs then the generic chip identification data (unless another configuration option is chosen). This data contains the firmware identifier accompanied with the certification identifier, the design step and even more tracking information. In combination with [AGD_HRM] (section 5.6) the user can identify the data, interpret it and retrieve the TOE versioning information. This information includes also the required mapping of firmware identifier and certification identifier.

The optional software libraries can be identified by their unique version numbers and by calculating a hash value (e.g. SHA-256) over the delivered lib-files (.lib) and comparing the calculated values to the values stated in Security Target [ST], chapters 9 - 15.

3. Security Policy

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 algorithms (Triple-DES and AES) to ensure the confidentiality of plain text data by encryption and to support secure authentication protocols and it will provide different random number generators.

The RSA library is used to provide a high-level interface to RSA (Rivest, Shamir, Adleman) cryptography implemented on the hardware component 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 optional Hash Crypto Library provides a high-level interface for performing cryptographic hash functions and includes countermeasures against SPA, DPA, and DFA attacks. The RCL provides a high-level interface for obtaining random data. This can be deterministic data from an AES CTR_DRBG or non-deterministic data that is provided by the underlying hardware. The RCL includes countermeasures against SPA, DPA, and DFA attacks.
Besides that, the TOE can come with the optional Hardware Support Library (HSL) providing a simplified interface for NVM management and provides the possibility to write tearing safe into the NVM.
As the TOE is a hardware security platform, the security policy of the TOE is also to provide protection against leakage of information (e.g. to ensure the confidentiality of cryptographic keys during AES, Triple-DES, RSA, and EC cryptographic functions performed by the TOE), against physical probing, against malfunctions, against physical manipulations, and against abuse of functionality. Hence, the TOE shall

- maintain the integrity and the confidentiality of data stored in the memory of the TOE, and

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

Specific details concerning the above-mentioned security policies can be found in [ST] chapter 6 / 7.

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 uncovered aspects need to be provided for by specific security objectives that have to be met by the TOE environment. They are in particular:

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 guidance documents listed in Table 4.

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

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

The objective OE.TOE_Auth requires that the environment must support the authentication and verification mechanism and must know the corresponding authentication reference data. The composite product manufacturer receives sufficient information about the authentication mechanism in [AGD_PPUM] chapter 4. Please note that this objective is only valid in case the Flash Loader is active and the TOE is ordered with mutual authentication (i.e., option External Authentication is unavailable).

The objective OE.Prevent_Masquerade is valid in case the Flash Loader is active and the Flash Loader is ordered with External Authentication (EA) instead of mutual authentication. It addresses two aspects:

- the support of a trusted communication channel identical to OE.Loader_Usage, however, with reference to the one-way authentication (external authentication), and
- the user is required to implement mechanisms to prevent masquerading attacks as no mutual authentication is enforced by the TOE itself.

The first item is addressed in [AGD_PPUM] chapter 4 just as OE.Loader_Usage. The second item is addressed in [AGD_PPUM] section 2.1.5 with a description of the External Authentication. Note that this objective replaces OE.TOE_Auth when the TOE is ordered with EA available.

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. 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] chapter 4:

> On delivery, if the application is active, then the application is responsible for transport protection.

The objective OE.Loader_Usage requires that the authorised user must 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] section 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] section 2.1.2.2. This objective for the environment originates from the “Package 1: Loader dedicated for usage in secured environment only”. However, the TOE also implements “Package 2: Loader dedicated for usage by authorised users only” and thus the Flash Loader can also be used in insecure environments before phase 7 and is able to protect itself against misuse if the authentication and download keys are handled appropriately.

Details can be found in the Security Target [ST], chapter 3 and 4.

5. Architectural Information

For further information on the TOE architecture, see Security Target [ST], chapter 1 (especially sections 1.3 and 1.4).

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 [ST].

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.

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 of this report for details on assurance levels or packages involved into testing.
The tests performed by the developer were divided into the following categories:

- Simulation tests (design verification),
- Qualification/verification tests, and
- Production Tests.

The developer tests cover all security functionalities and all security mechanisms as identified in the functional specification.
The evaluators were able to repeat the tests of the developer by using the library of programs, tools, and prepared chip samples delivered to the evaluators or at the developer's site. They performed independent tests to supplement, augment, and to verify the tests performed by the developer. For the developer tests repeated by the evaluators, other test parameters were used, and the test equipment was varied. Security features of the TOE realised by specific design and layout measures were checked by the evaluators during layout inspections both in design data and on the final product.
The evaluation has shown that the actual version of the TOE provides the security functionalities as specified by the developer. The test results confirm the correct implementation of the TOE security functionalities.
For penetration testing, the evaluators took all security functionalities into consideration. In-tensive 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.

Please refer to chapter 8 for complete and precise information on settings and configuration of the TOE during the evaluation, including relevant operational notes and observations.

8. Evaluated Configuration

This certificate covers the following configurations of the TOE:

- Smartcard IC IFX_CCI_00004Fh, IFX_CCI_000050h, IFX_CCI_000051h, IFX_CCI_000052h, IFX_CCI_000053h, IFX_CCI_000054h, IFX_CCI_000055h, IFX_CCI_000056h, IFX_CCI_000057h, IFX_CCI_000058h, IFX_CCI_00005Ch S11 (Global Foundries Fab 7).

Depending on the blocking configuration a product can have different user available configuration: they can be choosen by order or by BPU (please refer to [ST] section 1.1 for an identification of the components which can be blocked via BPU).

As stated and detailed in the ETR [ETR], developer and evaluator tested the TOE in those configurations in which the TOE is delivered and which are described in the Security Target [ST].

9. Results of the Evaluation

9.1. CC specific results

The ITSEF produced and provided the Evaluation Technical Reports (ETR) [ETR] according to 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,
- 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,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 20, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 4, 2013-05-15, Herausgeber: Zertifizierungsstelle des BSI im Rahmen des Zertifizierungsschemas,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 20, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3, 2013-05-15,
- 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.
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 23, Zusammentragen von Nachweisen der Entwickler, Version 4, 2017-03-15
- Application Notes and Interpretation of the Scheme (AIS) – AIS 25, Anwendungen der CC auf integrierte Schaltungen, Version 9, 2017-03-15,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 26, Evaluationsmethodologie für in Hardware Integrierte Schaltungen, Version 10, 2017-07-03,
- Application Notes and Interpretation of the Scheme (AIS) – AIS 27, Transition from ITSEC to CC, Version 5, 2010-08-17,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 31, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3, 2013-05-15,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 32, CC-Interpretationen im deutschen Zertifizierungsschema, Version 7, 2011-06-08,

- Application Notes and Interpretation of the Scheme (AIS) – AIS 34, Evaluation Methodology for CC Assurance Classes for EAL5+ (CC v2.3 & v3.1) and EAL6 (CC v3.1), Version 3, 2009-09-03,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 35, Öffentliche Fassung eines Security Target (ST-lite), Version 2, 2007-11-12,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 36, Kompositionsevaluierung, Version 5, 2017-03-15,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 37, Terminologie und Vorbereitung von Smartcard-Evaluierun-gen, Version 3, 2010-05-17,
- Application Notes and Interpretation of the Scheme (AIS) – AIS 38, Reuse of evaluation results, Version 2, 2007-09-28,
- Application Notes and Interpretation of the Scheme (AIS) – AIS 39, Formal Methods, Version 3, 2008-10-24,
- Application Notes and Interpretation of the Scheme (AIS) – AIS 41, Guidelines for PPs and STs, Version 2, 2011-01-31,
- Application Notes and Interpretation of the Scheme (AIS) – AIS 42, Guidelines for the Developer Documentation, Version 1, 2008-05-21,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 46, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren, Version 3, 2013-12-04,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 47, Regelungen zu Site Certification, Version 1.1, 2013-12-04,
- Guidance for Site Certification, Version 1.1, 2013-12-04,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 48, Anforderungen an die Prüfung von Sicherheitsetiketten, Version 1.0, 2015-04-30,

are considered.

Additionally the EUCC Supporting Mandatory Technical Documents are considered.

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 [ETRRfCOMP] 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 assurance components that are identified in chapter 1 of this report and claimed by the Security Target [ST] for the corresponding TOE which is identified in chapter 2 of this report.

The certificate

- is uniquely identified by: EUCC-3087-2026-0013, administration ID BSI-DSZ-CC-1156-V5-2026
- was issued on: 17.August.2026
- is valid until: 23 July 2031

The results of the evaluation are only applicable to the TOE as defined in chapter 1, 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 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.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size |k| in Bits	Comments	Security Level above 120 Bits
Symmetric Coprocessor (SCP)						
1	Cryptographic primitive	TDES	[NIST SP800-67], [ISO_18033-3]	112, 168	-	-
2	Cryptographic primitive	AES	[FIPS197], [ISO_18033-3]	128, 192, 256	-	-
3	Confidentiality	#1 in ECB mode for encryption and decryption	[NIST SP800-38A]	112, 168	-	No
4	Confidentiality	#1 in CBC mode for encryption and decryption	[NIST SP800-38A]	112, 168	-	No
5	Confidentiality	#2 in ECB mode for encryption and decryption	[NIST SP800-38A]	128, 192, 256	-	No
6	Confidentiality	#2 in CBC mode for encryption and decryption	[NIST SP800-38A]	128, 192, 256	-	No
Symmetric Cryptographic Libraries (both SCLs)						
7	Cryptographic primitive	TDES	[NIST SP800-67]	112, 168	-	-
8	Cryptographic primitive	AES	[FIPS197]	128, 192, 256	-	-
9	Confidentiality	#7 in ECB mode for encryption and decryption	[NIST SP800-38A]	112, 168	-	No

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size |k| in Bits	Comments	Security Level above 120 Bits
10	Confidentiality	#7 in CBC mode for encryption and decryption	[NIST SP800-38A]	112, 168	-	No
11	Confidentiality	#7 in CTR mode for encryption and decryption	[NIST SP800-38A]	112, 168	-	No
12	Confidentiality	#7 in CFB mode for encryption and decryption	[NIST SP800-38A]	112, 168	-	No
13	Integrity protection	#7 in CMAC mode for MAC generation	[NIST SP800-38B]	112, 168	-	No
14	Integrity protection	#7 in Retail MAC (Algorithm 3) for MAC generation	[ISO9797-1]	112	-	No
15	Confidentiality	#8 in ECB mode for encryption and decryption	[NIST SP800-38A]	128, 192, 256	-	No
16	Confidentiality	#8 in CBC mode for encryption and decryption	[NIST SP800-38A]	128, 192, 256	-	Yes
17	Confidentiality	#8 in CTR mode for encryption and decryption	[NIST SP800-38A]	128, 192, 256	-	Yes
18	Confidentiality	#8 in CFB mode for encryption and decryption	[NIST SP800-38A]	128, 192, 256	-	Yes
19	Integrity protection	#8 in CMAC mode for MAC generation	[NIST SP800-38B]	128, 192, 256	-	Yes
Asymmetric Cryptographic Library (ACL) v3.02.000						
20	Confidentiality	encryption	[PKCS #1, 5.1.1], [IEEE_P1363, 8.2.2]	1024 – 2112	-	No
21	Confidentiality	decryption	[PKCS #1, 5.1.2], [IEEE_P1363, 8.2.1 (I) / 8.2.3]	1024 – 2112	-	No
22	Confidentiality	decryption with CRT	[PKCS #1, 5.1.2], [IEEE_P1363, 8.2.1 (II) / 8.2.3]	1024 – 4224	-	Yes >= 2800 bit
23	Authenticity	signature generation	[PKCS #1, 5.2.1], [IEEE_P1363, 8.2.1 (I) / 8.2.4]	1024 – 2112	-	No

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size |k| in Bits	Comments	Security Level above 120 Bits
24	Authenticity	signature generation with CRT	[PKCS #1, 5.2.1], [IEEE_P1363, 8.2.1 (II) / 8.2.4]	1024 – 4224	-	Yes >= 2800 bit
25	Authenticity	signature verification	[PKCS #1, 5.2.2], [IEEE_P1363, 8.2.5]	1024 – 4224	-	Yes >= 2800 bit
26	Key generation	RSA key generation returning CRT key components dp, dq and qinv (prime generation not included)	[PKCS #1, 3.1 / 3.2], [IEEE_P1363, 8.1.3.1]	1024 – 4224	Method CRT	Yes >= 2800 bit
27	Key generation	RSA key generation returning key representation n and d (prime generation not included)	[PKCS #1, 3.1 / 3.2], [IEEE_P1363, 8.1.3.1]	1024 – 2112	Method n_d	No
28	Key generation	RSA key generation returning key representation p, q and d (prime generation included)	[IEEE_P1363, 8.1.3.1]	1024 – 2047	Method p_q_d; Prime generation method follows [FIPS186-4, B.3.3] but due to key size considered proprietary.	No
29	Key generation	RSA key generation returning key representation p, q and d (prime generation included)	[IEEE_P1363, 8.1.3.1] [FIPS186-4, B.3.3]	2048 – 2112	Method p_q_d	No
30	Cryptographic primitive	Primality test	-	length of prime: 512 – 2112 Bits	Method PRIME_CHECK; Proprietary primality test	N/A
31	Cryptographic primitive	Primality test	[FIPS186-4, C.3.1 / C.3.2]	length of prime: 512 – 2064 Bits	Method PRIME_CHECK_ MASK	N/A
32	N/A	Supported elliptic curves: - All curves in	[FIPS186-4] [RFC5639]	N/A	–	N/A

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size |k| in Bits	Comments	Security Level above 120 Bits
		[FIPS186-4], - All curves in [RFC5639].				
33	Authenticity	ECDSA signature generation on curves listed in #32	[ANS X9.62, 7.3], [IEEE_P1363, 7.2.7]	160 – 521	hash calculation of ECDSA is not implemented by the library and lies in the responsibility of the user.	Key sizes 160, 163, 192, 224:No Key sizes >= 250: Yes
34	Authenticity	ECDSA signature verification on curves listed in #32	[ANS X9.62, 7.4.1] [IEEE_P1363, 7.2.8]	160 – 521	hash calculation of ECDSA is not implemented by the library and lies in the responsibility of the user.	Key sizes 160, 163, 192,224 : No Key sizes >= 250: Yes
35	Key agreement	Elliptic Curve Diffie-Hellman (ECDH) key agreement on curves listed in #32	[ANS X9.63, 5.4.1] [ISO_11770-3, D.6] [IEEE_P1363, 7.2.1]	160 – 521	–	Key sizes 160, 163, 192, 224: No Key sizes >= 250: Yes
36	Key generation	Elliptic Curve key generation on curves listed in #32	[ANS X9.62, A.4.3] [IEEE_P1363, A.16.9]	160 – 521	–	Key sizes 160, 163, 192, 224: No Key sizes >= 250: Yes
Asymmetric Cryptographic Libraries (ACLs) v3.33.003 and v3.35.001						
37	Confidentiality	RSA encryption	[PKCS #1, 5.1.1] [IEEE_P1363, 8.2.2]	1024 – 4224	–	Yes >= 2800 bit
38	Confidentiality	RSA decryption	[PKCS #1, 5.1.2] [IEEE_P1363, 8.2.1 (I) / 8.2.3]	1024 – 2112	–	No
39	Confidentiality	RSA decryption with CRT	[PKCS #1, 5.1.2] [IEEE_P1363, 8.2.1 (II) / 8.2.3]	1024 – 4224	–	Yes >= 2800 bit
40	Authenticity	RSA signature generation	[PKCS #1, 5.2.1] [IEEE_P1363, 8.2.1 (I) / 8.2.4]	1024 – 2112	–	No
41	Authenticity	RSA signature generation with CRT	[PKCS #1, 5.2.1] [IEEE_P1363, 8.2.1	1024 – 4224	–	Yes >= 2800 bit

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size |k| in Bits	Comments	Security Level above 120 Bits
			(II) / 8.2.4]			
42	Authenticity	RSA signature verification	[PKCS #1, 5.2.2] [IEEE_P1363, 8.2.5]	1024 – 4224	–	Yes >= 2800 bit
43	Key agreement	Diffie-Hellman (DH) key agreement	[FIPS186-4, 5.5] [PKCS #1, 5.1.2 / 5.2.1] [IEEE_P1363, 8.2.3 / 8.2.4]	1024 – 4224	–	Yes >= 2800 bit
44	Key generation	RSA key generation returning CRT key components dp, dq and qinv (prime generation not included)	[PKCS #1, 3.1 / 3.2] [IEEE_P1363, 8.1.3.1]	1024 – 4224	Method CRT	Yes >= 2800 bit
45	Key generation	RSA key generation returning key representation n and d (prime generation not included)	[PKCS #1, 3.1 / 3.2] [IEEE_P1363, 8.1.3.1]	1024 – 2112	Method n_d	No
46	Key generation	RSA key generation returning key representation p, q and d (prime generation included)	[IEEE_P1363, 8.1.3.1]	1024 – 2047	Method p_q_d; Prime generation method follows [FIPS186-4, B.3.3] but due to key size considered proprietary.	No
47	Key generation	RSA key generation returning key representation p, q and d (prime generation included)	[IEEE_P1363, 8.1.3.1] [FIPS186-4, B.3.3]	2048 – 2112	Method p_q_d	No
48	Cryptographic primitive	Generation of probable primes, Miller Rabin test	[FIPS186-4, B.3.3 / C.3.1]	length of prime: 512 – 2064 Bits	Method 2PRIME_GEN	N/A
49	Cryptographic primitive	Primality test	–	length of prime: 512 – 2112 Bits	Method PRIME_CHECK; Proprietary primality test	N/A

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size |k| in Bits	Comments	Security Level above 120 Bits
50	Cryptographic primitive	Primality test	[FIPS186-4, C.3.1 / C.3.2]	length of prime: 512 – 2064 Bits	Method PRIME_CHECK_ MASK	N/A
51	N/A	Supported elliptic curves: - All curves in [FIPS186-4], - All curves in [RFC5639].	[FIPS186-4], [RFC5639]	N/A	–	N/A
52	Authenticity	ECDSA signature generation on curves listed in #51	[ANS X9.62, 7.3] [IEEE_P1363, 7.2.7]	160 – 521	hash calculation of ECDSA is not implemented by the library and lies in the responsibility of the user.	N/A
53	Authenticity	ECDSA signature verification on curves listed in #51	[ANS X9.62, 7.4.1] [IEEE_P1363, 7.2.8]	160 – 521	hash calculation of ECDSA is not implemented by the library and lies in the responsibility of the user.	Key sizes 160, 163, 192, 224: No Key sizes >= 250: Yes
54	Key agreement	Elliptic Curve Diffie-Hellman (ECDH) key agreement on curves listed in #51	[ANS X9.63, 5.4.1] [ISO_11770-3, D.6] [IEEE_P1363, 7.2.1]	160 – 521	–	Key sizes 160, 163, 192, 224: No Key sizes >= 250: Yes
55	Key generation	Elliptic Curve key generation on curves listed in #51	[ANS X9.62, A.4.3] [IEEE_P1363, A.16.9]	160 – 521	–	Key sizes 160, 163, 192, 224: No Key sizes >= 250: Yes
56	PACE integrated mapping	Point encoding for the ECDH-integrated mapping on curves listed in #51	[ICAO_11, B.2]	160 – 521	–	Key sizes 160, 163, 192, 224: No Key sizes >= 250: Yes
Additionally only for Asymmetric Cryptographic Library (ACL) v3.35.001						
57	Cryptographic primitive	Prime number generation	–	length of prime: 512 – 2112 Bits	Method PRIME_GEN; Proprietary prime number generation	N/A

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size |k| in Bits	Comments	Security Level above 120 Bits
					method, which follows [PrimeGen]	
Flash Loader						
58	Confidentiality	#2 in CCM mode for encryption and decryption	[NIST SP800-38C]	128	–	Not rated
59	Authenticity	#2 in CCM mode for MAC verification	[NIST SP800-38C]	128	–	Not rated
60	Authentication	Mutual authentication protocol based on #59	[AGD_PPUM, 2.1.5]	128	–	Not rated
61	Authentication	External authentication protocol based on #5	[AGD_PPUM, 2.1.5]	128	–	Not rated
Random Number generation (Hardware)						
62	RNG	Physical RNG	PTG.2 in [AIS31]	N/A	–	N/A
63	RNG	Hybrid RNG	corresponds to PTG.3 in [AIS31]	N/A	–	N/A
64	RNG	Deterministic RNG	corresponds to DRG.3 in [AIS20]	N/A	–	N/A
65	RNG	Deterministic RNG	corresponds to DRG.4 in [AIS31]	N/A	–	N/A
Random Crypto Library (RCL) v1.10.007						
66	RNG	Physical RNG	PTG.2 in [AIS31]	N/A	The RCL acts as interface to the PTG.2 hardware RNG	N/A
67	RNG	Deterministic RNG	corresponds to DRG.3 in [AIS20] [NIST SP800-90A]	128, 256	CTR_DRBG	N/A
68	RNG	Deterministic RNG	corresponds to DRG.4 in [AIS31] [NIST SP800-90A]	128, 256	CTR_DRBG	N/A
Hash Crypto Library (HCL) v1.13.002						
69	Hash	SHA-1	[FIPS180-4]	N/A	–	N/A

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size |k| in Bits	Comments	Security Level above 120 Bits
	calculation					
70	Hash calculation	SHA-224	[FIPS180-4]	N/A	–	N/A
71	Hash calculation	SHA-256	[FIPS180-4]	N/A	–	N/A
72	Hash calculation	SHA-384	[FIPS180-4]	N/A	–	N/A
73	Hash calculation	SHA-512	[FIPS180-4]	N/A	–	N/A
74	Hash calculation	SHA-512/224	[FIPS180-4]	N/A	–	N/A
75	Hash calculation	SHA-512/256	[FIPS180-4]	N/A	–	N/A

Table 2: TOE cryptographic functionality

The TOE's memory encryption, named ICS ("ICS-C8") and not separately listed above, was successfully evaluated according to BSI's "Methodology for cryptographic rating of memory encryption schemes used in smartcards and similar devices" (Version 1.0, 2013-10-31).

Where no cryptographic 120-Bit-Level assessment was given at all (i.e where "N/A" was stated), nevertheless the targeted CC Evaluation Assurance Level has been achieved for those functionalities as well.

Further conformance evaluation and assessment to claimed cryptographic functionality standards is documented in the confidential report "Cryptographic Standards Compliance Verification" [27].

Reference of Legislatives and Standards quoted above:

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

[AIS31] Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 31, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3, 2013-05-15, Bundesamt für Sicherheit in der Informationstechnik

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

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

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

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

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

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

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

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

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

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

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

[NIST SP800-38C] NIST SP800-38C, Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality, 2004-05 with updates as of 2007-07-20, National Institute of Standards and Technology (NIST)

[NIST SP800-67] NIST Special Publication 800-67 – Revision 2, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher – Revised November 2017, National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce

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

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

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 reassessed.

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 using the TOE. For this reason the TOE includes guidance documentation (see table 1) 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, re-certifications or maintenance result available for the product.

Furthermore:

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 in [AGD_ACL], [AGD_SCL], [AGD_RCL], [AGD_HCL], [AGD_SG], [AGD_HSL], [AGD_PPUM], [AGD_PRM], [AGD_HRM], [AGD_UMSLC], and [AGD_CryptoUM]
- 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 TOE manufacturer (Infineon) to the composite product manufacturer is not part of this evaluation. However, for security reasons, a form of transport protection might be required depending on the order option (see section 2.1 for details). The applied transport protection mechanisms must be considered during the composite evaluation considering the security needs of any pre-loaded IC Embedded Software that is active during delivery.

- The TOE can come with a pre-loaded image called Performance Flash Loader, which is a non-TOE component. Using the PFL results in a non-certified product.
- The TOE does not implement key generation (FCS_CKM.1), key derivation (FCS_CKM.5), or key insertion (FDP_ITC.1/2) as required by the FCS_COP.1 and FCS_CKM.6 iterations (dependency) used in the ST for the symmetric cryptography. The IC Embedded Software must provide this functionality instead. The same applies to the key destruction required by the FCS_COP.1 and FCS_CKM.1 iterators used in the ST for the asymmetric cryptography.

11. Security Target

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

SHA256 hash of the ST:

```
b23aff95311c5d5a4f82d8d6bc94f9c359054c845e5c43f3d6e638860bdf967f
```

SHA256 hash of the ST lite:

```
e75061583160e46ca0ae54dac657ea3be10be16bcd40824df1c3c53e6cc5f5e2
```

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

BPU	Bill per use
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
DPA	Differential Power Analysis
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ICT	Information and communications technology
IFX	Infineon

IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
NVM	None Volatile Memory
PFL	Performance Flash Loader
PP	Protection Profile
RCL	Random Crypto Library
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SPA	Simple Power Analysis
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

as mirrored by CCRA's edition:
CC:2022 R1, 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.commoncriteriaportal.org
amended by:
CCMB Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.2, 15 October 2025, CCRA
https://www.commoncriteriaportal.org

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

as mirrored by CCRA's edition:
CEM:2022 R1, Common Methodology for Information Technology Security Evaluation
https://www.commoncriteriaportal.org

[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[6] https://www.bsi.bund.de/AIS

[ST] Security Target BSI-DSZ-CC-1156-V5-2026, Version 7.2, 2026-05-04, IFX_CCI_00004Fh, IFX_CCI_000050h, IFX_CCI_000051h, IFX_CCI_000052h, IFX_CCI_000053h, IFX_CCI_000054h, IFX_CCI_000055h, IFX_CCI_000056h, IFX_CCI_000057h, IFX_CCI_000058h, IFX_CCI_00005Ch, S11 Security Target, Developer Name
Security Target lite, Version 7.2, 2026-05-04, IFX_CCI_00004Fh, IFX_CCI_000050h, IFX_CCI_000051h, IFX_CCI_000052h, IFX_CCI_000053h, IFX_CCI_000054h, IFX_CCI_000055h, IFX_CCI_000056h, IFX_CCI_000057h, IFX_CCI_000058h, IFX_CCI_00005Ch, S11 Security Target Lite, 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 2, 2026-06-29, EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY), TÜV Informationstechnik GmbH, (confidential document)

[ETRfCOMP] ETR for composite evaluation for the Product BSI-DSZ-CC-1156-V5-2026, Version 2, 2026-06-29, EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION (ETR COMP), TÜV Informationstechnik GmbH (confidential document)

[ALC] Evaluation Documentation Life Cycle Sup-port M5283, Version 2.0, 2021-04-19, Infineon Technologies AG (confidential document)

[AGD_HRM] Guidance documentation for the TOE, Version 5.2, 2020-12-21, SLC36 32-bit Security Con-troller – V16, Hardware Reference Manual, Infineon Technologies AG

[AGD_PRM] Guidance documentation for the TOE, Version 5.8, 2024-05-24, SLx1/SLx3 (40nm) security controllers Programmer's Reference Manual, Infineon Technologies AG

[AGD_SG] Guidance documentation for the TOE, Version 1.00-3157, 2026-02-17, SLC36 32-bit Security Controller – V16 Security Guidelines, Infineon Technologies AG

[AGD_PPUM] Guidance documentation for the TOE, Version 9.12, 2023-03-02, Production and personalization 32-bit security controller, Infineon Technologies AG

[6]specifically

- see section 9.1.

[AGD_CryptoUM] Guidance documentation for the TOE, Version 3.0, 2024-06-21, 32-bit Security Controller Crypto2304T V3 User Manual, Infineon Technologies AG

[AGD_HSL] Guidance documentation for the TOE, Version 03.52.9708, 2021-01-25, HSL for SLCx7V16 Hardware Support Library, Infineon Technologies AG

[AGD_UMSLC] Guidance documentation for the TOE, Version 01.30.0564, 2019-08-30, UMSLC library for SLCx7 in 40nm User Mode Security Life Control, Infineon Technologies AG

[AGD_SCL_211003] Guidance documentation for the TOE, Version, Date, SCL37-SCP-v440-C40 Symmetric Crypto Library for SCP-v440 AES/DES/MAC 32-bit Security Controller User interface manual, Version 2.11.003, 2021-06-16, Infineon Technologies AG

[AGD_SCL_215000] Guidance documentation for the TOE, Version 2.15.000, 2023-07-20 , SCL37-SCP-v440-C40 Symmetric Crypto Library for SCP-v440 AES/DES/MAC 32-bit Security Controller User interface manual, Infineon Technologies AG

[AGD_ACL_302000] Guidance documentation for the TOE, Version 3.02.000, 2026-04-23, ACL37-Crypto2304T-C40 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox 32-bit Security Controller User interface manual, Infineon Technologies AG

[AGD_ACL_333003] Guidance documentation for the TOE, Version 3.33.003, 2026-04-23, ACL37-Crypto2304T-C40 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox 32-bit Security Controller User interface manual, Infineon Technologies AG

[AGD_ACL_335001] Guidance documentation for the TOE, Version 3.35.001, 2026-04-23, ACL37-Crypto2304T-C40 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox 32-bit Security Controller User interface manual, Infineon Technologies AG

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

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

[IFX_DHL_SIN] SITE TECHNICAL AUDIT REPORT (STAR) DHL Supply Chain Singapore Pte Ltd., Advanced Regional Center, Version 1, 2026-02-23, TÜV Informationstechnik GmbH *SHA256-hash: 654c0a3e193e351985fa8566f610d5e0c98b7f369fb44e9730ce50096ee42f7a*

[IFX_RGB] Site Technical Audit Report (STAR) Infineon Technologies AG, Regensburg, Germany, Infineon Technologies AG, Version 1, 2026-02-18, TÜV Informationstechnik GmbH *SHA256-hash:* 61aa1612ab916794ce5aaff0ea21dff76b668c1e113633098b13d4c99fb8ce7c

[IFX_SIN]	SITE TECHNICAL AUDIT REPORT (STAR) Infineon Technologies Asia Pacific Pte Ltd., Singapore, Version 2, 2026-03-10,TÜV Informationstechnik GmbH *SHA256-hash:* *cb34c35883212be675d6604ff6cb83a42139d0fac274af0d87c3b6e392e993e9*
[PACT_NAU]	SITE TECHNICAL AUDIT REPORT (STAR) PacTech - Packaging Technologies GmbH, Version 1, 2026-02-18, TÜV Informationstechnik GmbH *SHA256-hash:* *43f9ba890210b51a653377e8f6f9ba098595a709b19ffa54eed17cedb0fdf084*

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-1156-V5-2026

Evaluation results regarding development and production environment

The IT product IFX_CCI_00004Fh, IFX_CCI_000050h - IFX_CCI_000058h, IFX_CCI_00005Ch design step S11 with firmware 80.310.03.0 & 80.310.03.1, optional NRG™ SW 05.03.4097, opt. HSL v3.52.9708, UMSLC lib v01.30.0564, opt.SCL v2.15.000 and v2.11.003, opt. ACL v3.33.003, and v3.35.001 and v3.02.000, opt. RCL v1.10.007, opt. HCL v1.13.002 (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 17.August.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:

Distribution Center name	Address
DHL Singapore	DHL Exel 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	Infineon Technology AG Distribution Center Europe (DCE) Kühne & Nagel Stockstädter Strasse 10 – Building 8A 63762 Großostheim Germany

Also in this Certification the STAR [IFX_DHL_SIN], [IFX_RGB], [IFX_SIN], [PACT_NAU] has been approved.

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