Federal Office
for Information Security

Certification Report

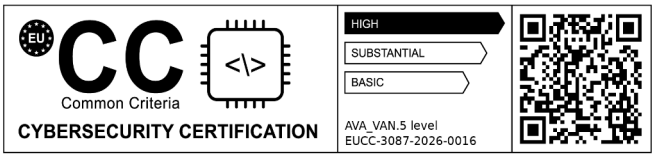
EUCC-3087-2026-0016
Administration ID
BSI-DSZ-CC-1205-V4-2026

for

IFX_CCI_00006Ah, IFX_CCI_00006Bh, IFX_CCI_00006Ch, design step S12 with firmware 80.311.04.1, optional NRG™ SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib 01.30.0695, optional SCL v2.15.000, optional ACL v3.34.000 & 3.35.001, optional RCL v1.10.007, optional HCL v1.13.002 and user guidance

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 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_00006Ah, IFX_CCI_00006Bh, IFX_CCI_00006Ch, design step S12 with firmware 80.311.04.1, optional NRG™ SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib 01.30.0695, optional SCL v2.15.000, optional ACL v3.34.000 & 3.35.001, optional RCL v1.10.007, optional HCL v1.13.002 and user guidance has been previously certified by the certification body of the Federal Office for Information Security (BSI) based on administration ID BSI-DSZ-CC-1205-V3-2025. Specific results from the corresponding evaluation process were re-used.
- The present evaluation of the product IFX_CCI_00006Ah, IFX_CCI_00006Bh, IFX_CCI_00006Ch, design step S12 with firmware 80.311.04.1, optional NRG™ SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib 01.30.0695, optional SCL v2.15.000, optional ACL v3.34.000 & 3.35.001, optional RCL v1.10.007, optional HCL v1.13.002 and user guidance was carried out by TÜV Informationstechnik GmbH, located at

  Unternehmensgruppe TÜV NORD
  Am TÜV 1
  45307 Essen.
- The evaluation was completed on 17 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 [CC] itself.

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 re-assessment 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 26 August 2026 is valid until 25 August 2031 and its validity can be renewed by certifying the TOE again.

The holder of this certificate is obliged:

- 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_00006Ah, IFX_CCI_00006Bh, IFX_CCI_00006Ch, design step S12 with firmware 80.311.04.1, optional NRG™ SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib 01.30.0695, optional SCL v2.15.000, optional ACL v3.34.000 & 3.35.001, optional RCL v1.10.007, optional HCL v1.13.002 and user guidance 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_00006Ah, IFX_CCI_00006Bh, IFX_CCI_00006Ch, design step S12 with firmware 80.311.04.1, optional NRG™ SW v05.03.4097, optional HSL v3.52.9708, UMSLC lib v01.30.0695, optional SCL v2.15.000, optional ACL v3.34.000, optional ACL v3.35.001, optional RCL v1.10.007, optional HCL v1.13.002 and user guidance.

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 is able to communicate using either the contact-based or the contactless interface.

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 TOE is the platform for the smartcard embedded software.

The product IFX_CCI_00006Ah, IFX_CCI_00006Bh, IFX_CCI_00006Ch, design step S12 with firmware 80.311.04.1, optional NRG™ SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib 01.30.0695, optional SCL v2.15.000, optional ACL v3.34.000 & 3.35.001, optional RCL v1.10.007, optional HCL v1.13.002 and user guidance 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-1205-V3-2025. Specific results from the evaluation process BSI-DSZ-CC-1205-V3-2025 were re-used. The TOE deliverables are listed in table 1.

The evaluation of the product IFX_CCI_00006Ah, IFX_CCI_00006Bh, IFX_CCI_00006Ch, design step S12 with firmware 80.311.04.1, optional NRG™ SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib 01.30.0695, optional SCL v2.15.000, optional ACL v3.34.000 & 3.35.001, optional RCL v1.10.007, optional HCL v1.13.002 and user guidance was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 17 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 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 a product can have different user available configuration by order or by BPU (please refer to [ST] chapter 1.4.7, for an identification of the components, which can be blocked via BPU).

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 explicitely guarantee or endorse the certified TOE.

2. Identification of the TOE

The Information and communications technology product is identified as follows:

IFX_CCI_00006Ah, IFX_CCI_00006Bh, IFX_CCI_00006Ch, design step S12 with firmware 80.311.04.1, optional NRG™ SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib 01.30.0695, optional SCL v2.15.000, optional ACL v3.34.000 & 3.35.001, optional RCL v1.10.007, optional HCL v1.13.002 and user guidance

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_00006Ah, IFX_CCI_00006Bh, IFX_CCI_00006Ch	S12 (design step)	Complete modules, wafers, IC cases or packages (see [ST, 1.4.5]).
2.	FW	BOS & RFAPI & POWS	80.311.04.1	Stored on the delivered hardware.
3.	FW	Flash Loader	v09.13.0006	Stored on the delivered hardware.
4.	SW	NRG™ SW (optional)	v05.03.4097	Secure download (L251 Library File) via iShare.
5.	SW	HSL (optional)	v3.52.9708	Secure download (L251 Library File) via iShare.
6.	SW	UMSLC	v01.30.0695	Secure download (L251 Library File) via iShare.
7.	SW	SCL (optional)	v2.15.000	Secure download (L251 Library File) via iShare.
8.	SW	ACL (optional)	v3.34.000 or 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.

No.	Type	Item / Identifier	Release / Version	Form of Delivery
11.	DOC	*SLC39 32-bit Security Controller - V23, Hardware Reference Manual*	See [AGD_HRM] in Section 13.	Personalized PDF via secure iShare server.
12.	DOC	*SLx1/SLx3 (40 nm) Security Controllers, Programmer's Reference Manual*	See [AGD_PRM] in Section 13.	Personalized PDF via secure iShare.
13.	DOC	*SLC39 32-bit Security Controller - V23, Security Guidelines*	See [AGD_SG] in Section 13.	Personalized PDF via secure iShare.
14.	DOC	*SLx3 (40nm) Security Controllers, Production and Personalization Manual*	See [AGD_PPUM] in Section 13.	Personalized PDF via secure iShare.
15.	DOC	*32-bit Security Controller Crypto2304T V3, User Manual* (optional)	See [AGD_CryptoUM] in Section 13.	Personalized PDF via secure iShare.
16.	DOC	*HSL for SLCx7 V23b, Hardware Support Library* (optional, HSL v03.52.9708)	See [AGD_HSL] in Section 13.	Personalized PDF via secure iShare.
17.	DOC	*UMSLC library for SLCx7V23b User Mode Security Life Control*	See [AGD_UMSLC] in Section 13.	Personalized PDF via secure iShare.
18.	DOC	*SCL37-SCP-v440-C40 Symmetric Crypto Library for SCP-v440 AES/DES/MAC* (optional, SCL v2.15.000)	See [AGD_SCL] in Section 13.	Personalized PDF via secure iShare.
19.	DOC	*ACL37-Crypto2304T-C40 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox* (optional, ACL v3.34.000)	See [AGD_ACL_334000] in Section 13.	Personalized PDF via secure iShare.
20.	DOC	*ACL37-Crypto2304T-C40 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox* (optional, ACL v3.35.001)	See [AGD_ACL_335001] in Section 13.	Personalized PDF via secure iShare.
21.	DOC	*RCL37-X-C40 Random Crypto Library for SCP-v440 & RNG-v3 DRBG/HWRNG 32-bit Security Controller, User interface manual* (optional, RCL v1.10.007)	See [AGD_RCL] in Section 13.	Personalized PDF via secure iShare.
22.	DOC	*HCL37-CPU-C40 Hash Crypto Library for CPU SHA 32-bit Security Controller, User interface manual* (optional, HCL v1.13.002)	See [AGD_HCL] in Section 13.	Personalized PDF via secure iShare.

Table 1: Deliverables of the TOE

If the user software (operating system) is loaded on the delivered TOE, the TOE is under the control of the user software and the TOE Manufacturer (Infineon Technologies AG) can only guarantee the integrity up to the delivery process. In this case, the user software is responsible for the integrity of the TOE and thus a transport protection is optional (see [AGD_PPUM], chapter 4: "On delivery, if the application is active, then the application is responsible for transport protection").

In detail, regarding identification:

The hexadecimal values listed behind the “IFX_CCI_” are part of the TOE name IFX_CCI_00006Ah, IFX_CCI_00006Bh, IFX_CCI_00006Ch. These identifiers are used by the developer only for this TOE. Different underlying basic hardware configurations are achieved only by the means of blocking; the actual hardware is always present and thus identical but may not be accessible to the user. The design step of the TOE is indicated by byte 11 and 12 of the GCIM. The GCIM is described in [AGD_HRM] chapter 5.6.

In addition to the hardware part, the TOE consists of firmware parts and software parts:

The firmware part of the TOE is identified also via the GCIM: Bytes 31 to 34 contain the firmware identifier. The optional software consists of the libraries ACL, SCL, HSL, RCL, HCL, and NRG. The UMSLC library is always part of the TOE.

These libraries are identified by their version numbers. The user can identify the versions by calculating the hash value of the provided library files and compare them to the hash values provided in [ST] chapter 9 to 15.

In detail, regarding delivery:

According to the PP [PP] chapter 1.2.3 the lifecycle of the TOE consists of 7 phases. TOE Delivery is uniquely used to indicate

- after Phase 3 (or before Phase 4) if the TOE is delivered in form of wafers or sawn wafers (dice) or,
- after Phase 4 (or before Phase 5) if the TOE is delivered in form of packaged products.

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

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

Therefore, three different delivery procedures have to be taken into consideration:

1. Delivery of the IC dedicated software components (IC dedicated SW, guidance) from the TOE Manufacturer to the IC Embedded Software Developer.
2. Delivery of the IC Embedded Software (ROM / Flash data, initialisation and prepersonalisation data) from the IC Embedded Software Developer to the TOE Manufacturer.
3. 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).

The TOE is delivered via the distribution centers:

- DHL Singapore (Distribution Center Asia),
- KWE Shanghai,
- K&N Großostheim (Distribution Center Europe).

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 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 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 Crypto@2304T and includes countermeasures against SPA, DPA, and DFA attacks. The EC library is used to provide a high-level interface to Elliptic Curve cryptography implemented on the hardware component Crypto@2304T 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 Chapter 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 uncovered aspects need to be provided for by specific security objectives that have to be met by the TOE environment. They are in particular:

Therefore the ST includes the following security objectives for the operational environment, which are relevant for the Composite Product Manufacturer:

- OE.Resp-Appl
- OE.Process-Sec-IC,

- OE.Lim_Block_Loader,
- OE.Loader_Usage,
- OE.TOE_Auth,
- OE.Secure_Delivery
- and OE.Prevent_Masquerade.

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_SG].

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 the Security Target [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 has to support the authentication and verification mechanism and has to know the corresponding authentication reference data. The composite product manufacturer receives sufficient information regarding to the authentication mechanism in [AGD_PPUM], section 2.1.5. Please note that this objective is only valid in case the Flash Loader 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 ordered with External Authentication (EA) instead of mutual authentication. In this case, customers need to take care that no masquerading attacks can be performed. The objective replaces OE.Loader_Usage. A description of the External Authentication is given in [AGD_PPUM] section 2.1.5 and the ST highlights the risks of masquerading attacks when using this order option of the flash loader:

> *The objective OE.Prevent_Masquerade requires measures by customers to ensure the authenticity of the TOE.*

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] chapter 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 described 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, 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 requires the customers to provide transport protection in case the TOE is delivered (i) with flash loader deactivated or (ii) if external authentication is available. In the latter case O.Authentication is not available and needs to be compensated by customer measures.

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

5. Architectural Information

The TOE hardware consists basically of a core, a memory system, and peripherals. There are two separate bus entities: a memory bus and a peripheral bus for high-speed communication with the peripherals. In more detail, the TOE hardware can be further divided into Major core components:

- CPU, MPU, NVIC, ISS.

Memory system components:

- ROM, Cache, RAM, NVM, ICS, CPAU,

Memory bus and peripherals such as

- SPAU, SCP, RNG, CRC module.

Further, more detailed information is readily available in the Security Target [ST] section 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. Intensive penetration testing was planned based on the analysis results and performed for the underlying mechanisms of security functionalities. The penetration tests considered both the physical tampering of the TOE and attacks, which do not modify the TOE physically. The penetration test results confirm that the TOE is resistant to attackers with high attack potential in the intended environment for the TOE.

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 certification covers the following configurations of the TOE:

- Smartcard IC IFX_CCI_00006Ah, IFX_CCI_00006Bh, IFX_CCI_00006Ch S12 (Global Foundries Fab 7)

Depending on the blocking configuration a product can have different user available configuration by order or by BPU (please refer to [ST] section 1.4.7, for an identification of the components, which can be blocked via BPU).

As stated and detailed in the [ETR], developer and evaluator tested the TOE in those configurations/identifiers 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 the state-of-the-art documents and supporting documents listed in section 13.1 were applied.

For RNG assessment the scheme interpretations AIS 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 [ST] 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 identified in chapter 2 of this report.

The certificate

- is uniquely identified by: EUCC-3087-2026-0016, administration ID BSI-DSZ-CC-1205-V4-2026
- was issued on: 26 August 2026
- is valid until: 25 August 2031

The results of the evaluation are only applicable to the TOE as defined in chapter 1 and 2 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

The following table gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines the standard of application where its specific appropriateness is stated.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments	Security Level above 120 Bits
Symmetric Co-Processor (SCP)						
1	Cryptographic primitive	TDES	[NIST SP800-67], [ISO18033-3]	112, 168	-	-
2	Cryptographic primitive	AES	[FIPS197], [ISO18033-3]	128, 192, 256	-	-
3	Confidentiality	#1 in ECB mode for encryption and decryption	[NIST SP800-38A]	112, 168	-	No

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments	Security Level above 120 Bits
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	-	Yes
Symmetric Cryptographic Libraries						
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
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

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments	Security Level above 120 Bits
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) v3.34.000 and v3.35.001						
20	Confidentiality	RSA Encryption	[PKCS #1, 5.1.1] [IEEE_P1363, 8.2.2]	512 – 4224	-	Yes >= 2800 bit
21	Confidentiality	RSA Decryption	[PKCS #1, 5.1.2] [IEEE_P1363, 8.2.1 (I) / 8.2.3]	512 – 2112	-	Yes >= 2800 bit
22	Confidentiality	RSA Decryption with CRT	[PKCS #1, 5.1.2] [IEEE_P1363, 8.2.1 (II) / 8.2.3]	512 – 4224	-	Yes >= 2800 bit
23	Authenticity	RSA Signature generation	[PKCS #1, 5.2.1] [IEEE_P1363, 8.2.1 (I) / 8.2.4]	512 – 2112	-	No
24	Authenticity	RSA Signature generation with CRT	[PKCS #1, 5.2.1] [IEEE_P1363, 8.2.1 (II) / 8.2.4]	512 – 4224	-	No
25	Authenticity	RSA Signature verification	[PKCS #1, 5.2.2] [IEEE_P1363, 8.2.5]	512 – 4224	-	n/a
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]	512 – 4224	Method CRT	>=2800bit Yes
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]	512 – 2112	Method n_d	n/a
28	Key generation	RSA key generation returning key representation p, q and d (prime generation included)	[IEEE_P1363, 8.1.3.1]	512 – 2047	Method p_q_d; Prime generation method follows [FIPS186-4, B.3.3] with random primes instead of “primes with condition”	No

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments	Security Level above 120 Bits
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	Yes
30	Key agreement	RSA Diffie-Hellman (DH) key agreement	[FIPS186-4, 5.5] [PKCS #1, 5.2.1 / 5.1.2] [IEEE_P1363, 8.2.4 / 8.2.3]	512 - 4224	Method RSA_DH	>=2800bit Yes
31	Cryptographic primitive (only for ACL v3.35.001)	Prime number generation	-	length of prime: 512 – 2112 Bits	Method PRIME_GEN; Proprietary prime number generation method, which follows [PrimeGen]	Not rated
32	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 [N186-4] B.3.3: (only for prime Bitlength >= 1024; in case prime Bitlength < 1024 identical algorithm is used, but considered proprietary) [N186-4] C.3.1	Not rated
33	Cryptographic primitive	Primality test	-	length of prime: 512 – 2112 Bits	Method PRIME_CHECK; Proprietary primality test	not rated
34	Cryptographic primitive	Primality test	[FIPS186-4, C.3.1 / C.3.2]	length of prime: 512 – 2064 Bits	Method PRIME_CHECK_MASK	n/a
35	N/A	Supported elliptic curves: • All curves in	[FIPS186-4] [RFC5639]	N/A	-	n/a

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments	Security Level above 120 Bits
		[FIPS186-4], • All curves in [RFC5639].				
36	Cryptographic primitive	EC point addition on curves listed in #35	N/A	160 – 521	-	n/a
37	Authenticity	ECDSA signature generation on curves listed in #35[6]	[ANS X9.62, 7.3] [IEEE_P1363, 7.2.7]	160 – 521	-	n/a
38	Authenticity	ECDSA signature verification on curves listed in #35	[ANS X9.62, 7.4.1] [IEEE_P1363, 7.2.8]	160 – 521	-	Key sizes 160, 163, 192, 224: No Key sizes >= 250: Yes
39	Key agreement	Elliptic Curve Diffie-Hellman (ECDH) key agreement on curves listed in #35	[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
40	Key generation	Elliptic Curve key generation on curves listed in #35	[ANS X9.62, A.4.3] [IEEE_P1363, A.16.9]	160 – 521	-	Key sizes 160, 163, 192, 224: No Key sizes >= 250: Yes
41	PACE integrated mapping	Point encoding for the ECDH-integrated mapping on curves listed in #35	[ICAO_11, B.2]	160 – 521	-	Key sizes 160, 163, 192, 224: No Key sizes >= 250: Yes
Flash Loader						
42	Confidentiality	#2 in CCM mode for encryption and decryption	[NIST SP800-38C]	128	-	Not rated

[6] Note that the hash calculation of ECDSA s not implemented by the library and lies in the responsibility of the user.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments	Security Level above 120 Bits
43	Authenticity	#2 in CCM mode for MAC verification	[NIST SP800-38C]	128	-	Not rated
44	Authentication	Mutual authentication protocol based on #43	[AGD_PPUM, 2.1.5]	128	-	Not rated
45	Authentication	External authentication protocol based on #5	[AGD_PPUM, 2.1.5]	128	-	Not rated
Random Number generation (Hardware)						
46	RNG	Physical RNG	PTG.2 in [AIS31]	N/A	-	n/a
47	RNG	Hybrid RNG	Corresponds to PTG.3 in [AIS31]	N/A	-	n/a
48	RNG	Deterministic RNG	Corresponds to DRG.3 in [AIS20]	N/A	-	n/a
49	RNG	Deterministic RNG	Corresponds to DRG.4 in [AIS31]	N/A	-	n/a
Random Crypto Library (RCL) v1.10.007						
50	RNG	Physical RNG	PTG.2 in [AIS31]	N/A	The RCL acts as interface to the PTG.2 hardware RNG	n/a
51	RNG	Deterministic RNG	Corresponds to DRG.3 in [AIS20] [NIST SP800-90A]	128, 256	CTR_DRBG	n/a
52	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						
53	Hash calculation	SHA-1	[FIPS180-4]	N/A	-	n/a (keyless operation)
54	Hash calculation	SHA-224	[FIPS180-4]	N/A	-	n/a (keyless operation)
55	Hash calculation	SHA-256	[FIPS180-4]	N/A	-	n/a (keyless operation)
56	Hash calculation	SHA-384	[FIPS180-4]	N/A	-	n/a (keyless operation)

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments	Security Level above 120 Bits
57	Hash calculation	SHA-512	[FIPS180-4]	N/A	-	n/a (keyless operation)
58	Hash calculation	SHA-512/224	[FIPS180-4]	N/A	-	n/a (keyless operation)
59	Hash calculation	SHA-512/256	[FIPS180-4]	N/A	-	n/a (keyless operation)

Table 2: TOE cryptographic functionality

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

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.

In course of the evaluation process, a source code analysis was performed to compare the TOE implementation of the cryptographic functionality with the preconditions and steps defined in the referenced standards. The results of this analysis, including the deviations found by the evaluator and the conformance verification results were summarized in the [CSCV] report. For the deviations, which are stated to be conformant to the referenced specifications, the evaluator confirms that the implementation is conformant with the referenced standard in the boundary conditions and operational environment of the TOE and in sense of equivalent process as specified by Federal Information Processing Standards Publications, cf. [FIPS186-4]:

> Equivalent process: Two processes are equivalent if, when the same values are input to each process (either as input parameters or as values made available during the process or both), the same output is produced.

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 in bibliography

[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)*

[PrimeGen] Details about Prime Number Generation, Infineon CCS Statement, Version 0.2, 2017-12-13

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 Embedded 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, recertifications or maintenance result available for the product.

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.

In addition, the following aspects need to be fulfilled when using the TOE:

- 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.
- Depending on the chosen Flash Loader status, a secure delivery procedure from the security IC embedded software developer to the composite product manufacturer might be required. See also OE.Secure_Delivery for further details.
- The firmware flash loader requires either mutual authentication to establish a secure channel or a one-way authentication of the user without establishing a secure channel even though the communication is encrypted and integrity protected. This latter configuration does not satisfy the Loader Package 2.

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. 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

3DES / TDES	Triple DES
ACL	Asymmetric Cryptographic Library
AES	Advanced Encryption Standard
AIS	Application Notes and Interpretations of the Scheme
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
CPU	Central Processing Unit
cPP	Collaborative Protection Profile
CRC	cyclic redundancy check
DES	Data Encryption Standard
DFA	Dependent Failure Analysis
DPA	Differential Power Analysis
DRNG	Deterministic RNG
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ISS	Instruction Stream Signature Checking
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
MPU	Memory Protection Unit
NVIC	Nested Vectored Interrupt Controller
NVM	SOLID FLASH™ Memory
PFL	Performance Flash Loader
PP	Protection Profile
RAM	Read-Only Memory

RNG	Random Number Generator
ROM	Read only Memory
SAR	Security Assurance Requirement
SCP	Symmetric Cryptographic Processor
SFP	Security Function Policy
SFR	Security Functional Requirement
SPA	Simple Power Analysis
SPAU	System Peripheral Access Unit
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, Information security, cybersecurity and privacy protection — Evaluation criteria for IT security
- 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
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 security, cybersecurity and privacy protection — Evaluation criteria for IT security — 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

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

[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, see chapter 13.1 or https://www.bsi.bund.de/AIS

[ST] Security Target BSI-DSZ-CC-1205-V4-2026, Version 7.0, 2026-06-08, IFX_CCI_00006Ah, IFX_CCI_00006Bh, IFX_CCI_00006Ch S12 Security Target, Infineon Technologies AG (confidential document)
Security Target lite, Version 7.0, 2026-06-08, IFX_CCI_00006Ah, IFX_CCI_00006Bh, IFX_CCI_00006Ch S12 Security Target, Infineon Technologies AG

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

[ETR] Evaluation Technical Report, Version 1, 2026-07-30, EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY), TÜV Informationstechnik GmbH, (confidential document)

[ETRfCOMP] ETR for composite evaluation according to AIS 36 for the Product IFX_CCI_00006Ah, IFX_CCI_00006Bh, IFX_CCI_00006Ch S12, Version 1, 2026-07-30, EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION (ETR COMP), TÜV Informationstechnik GmbH (confidential document)

[AGD_HRM] Guidance documentation for the TOE, Version 2.0, 2022-06-15, SLC39 32-bit Security Controller - V23, Hardware Reference Manual Infineon Technologies AG

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

[AGD_SG] Guidance documentation for the TOE, Version 1.00-3156, 2026-02-17, SLC39 32-bit Security Controller - V23, Security Guidelines, Infineon Technologies AG

[AGD_PPUM] Guidance documentation for the TOE, Version 09.13, 2023-05-15, SLx3 (40nm) Security Controllers, Production and Personalization Manual, Infineon Technologies AG

[AGD_CryptoUM] Guidance documentation for the TOE, Version 3, 2024-06-21, 32-bit Security Controller Crypto2304T V3 User Manual, Infineon Technologies AG

[AGD_HSL] Guidance documentation for the TOE, Version v3.52.9708, 2022-06-22, HSL for SLCx7 V23b, Hardware Support Library, Infineon Technologies AG

[AGD_UMSLC] Guidance documentation for the TOE, Version 01.30.0695, 2022-07-04, UMSLC library for SLCx7V23b User Mode Security Life Control, Infineon Technologies AG

[AGD_SCL] 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, Infineon Technologies AG

[AGD_ACL_334000] Guidance documentation for the TOE, Version 3.34.000, 2026-04-23, ACL37-Crypto2304T-C40 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox, 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, 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

[CSCV] SINGLE EVALUATION REPORT ADDENDUM to ETR-Part ASE, Cryptographic Standards Compliance Verification, Version 2, 2024-08-27, TÜVInformationstechnik GmbH (confidential document)

13.1. Application Notes, Interpretations of the Scheme (AIS) and Supporting Documents

[AIS1] 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.

[AIS14] 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.

[AIS19] 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.

[AIS20] 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.

[AIS20_DEV_ETR] 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.

[AIS20_DEV_EV] Developer evidence for the evaluation of a deterministic random number generator, Version 0.9, 2013-02-28, Bundesamt für Sicherheit in der Informationstechnik.

[AIS20_EVL-DRNG] 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.

[AIS20_PS2024] A proposal for: Functionality classes for random number generators, Version 3.0, 2024-09-10, M. Peter, W. Schindler, Bundesamt für Sicherheit in der Informationstechnik.

[AIS20_TP] Transition Policy to Version 3.0 of the Mathematical/Technical Reference, Version 1.0, 2025-04-15, Bundesamt für Sicherheit in der Informationstechnik.

[AIS20_V3] 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, Bundesamt für Sicherheit in der Informationstechnik.

[AIS23] Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 23, Zusammentragen von Nachweisen der Entwickler, Version 4, 2017-03-15, Bundesamt für Sicherheit in der Informationstechnik.

[AIS25] 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.

[AIS25_Test-Valid] 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.

[AIS26] 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.

[AIS31] 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.

[AIS31_DEV_ETR] 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.

[AIS31_DEV_EV] Developer evidence for the evaluation of a physical true random number generator, Version 0.8, 2013-02-28, Bundesamt für Sicherheit in der Informationstechnik.

[AIS31_EVL-PTRNG] 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.

[AIS31_KS2011] 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.

[AIS31_PS2024] A proposal for: Functionality classes for random number generators, Version 3.0, 2024-09-10, M. Peter, W. Schindler, Bundesamt für Sicherheit in der Informationstechnik.

[AIS31_TP] Transition Policy to Version 3.0 of the Mathematical/Technical Reference, Version 1.0, 2025-04-15, Bundesamt für Sicherheit in der Informationstechnik.

[AIS31_V3] 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.

[AIS32] Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 32, CC-Interpretationen im deutschen Zertifizierungsschema, Version 7, 2011-06-08, Bundesamt für Sicherheit in der Informationstechnik.

[AIS34] 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.

[AIS35] 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.

[AIS36] Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 36, Kompositionsevaluierung, Version 5, 2017-03-15, Bundesamt für Sicherheit in der Informationstechnik.

[AIS37] 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.

[AIS38] 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.

[AIS39] Application Notes and Interpretation of the Scheme (AIS) – AIS 39, Formal Methods, Version 3, 2008-10-24, Bundesamt für Sicherheit in der Informationstechnik.

[AIS39_FM-Guide] Guideline for the Development and Evaluation of formal security policy models in the scope of ITSEC and Common Criteria, Version 2.0, 2007-12-04, Bundesamt für Sicherheit in der Informationstechnik.

[AIS41] 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.

[AIS41_PP-ST-2] Guidance Document – The PP/ST Guide, Version 2, Revision 0, 2010-08, Bundesamt für Sicherheit in der Informationstechnik.

[AIS42] 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.

[AIS46] 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.

[AIS46_AI-Guide] Guidelines for Evaluating Machine-Learning based Side-Channel Attack Resistances, Version 2024-01, 2024-02-29, Bundesamt für Sicherheit in der Informationstechnik.

[AIS46_AVATMP] Review-Protokoll zum (Krypto-)AVA-KickOff, 2019-08-23, Bundesamt für Sicherheit in der Informationstechnik.

[AIS46_ECC-Guide] 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.

[AIS46_ME-Guide] 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.

[AIS46_RSA-Guide] 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.

[AIS47] Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 47, Regelungen zu Site Certification, Version 1.1, 2013-12-04, Bundesamt für Sicherheit in der Informationstechnik.

[AIS47_CCDB-SC] CC Supporting Document Guidance – Site Certification, Version 1.0, Revision 1, 2007-10, CCDB-2007-11-001.

[AIS47_SC-ETR] Details for the structure and content of the ETR for Site Certification, Version 1.0, 2010, Bundesamt für Sicherheit in der Informationstechnik.

[AIS47_SC-GD] Guidance for Site Certification, Version 1.1, 2013-12-04, Bundesamt für Sicherheit in der Informationstechnik.

[AIS48] Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 48, Anforderungen an die Prüfung von Sicherheitsetiketten, Version 1.0, 2015-04-30, Bundesamt für Sicherheit in der Informationstechnik.

[CCMC_Trans-Policy] Transition Policy to CC:2022 and CEM:2022, 2023-04-20, Common Criteria Recognition Arrangement Management Committee, CCMC-2023-04-001.

[CRA_EUCC_Ann] Cyber Resilience Act implementation via EUCC and its applicable technical elements - Annexes, 2025-01-27, ENISA.

[JIL-AssCont_CC2022] Joint Interpretation Library – Assurance Continuity - Practical Cases for Smart Cards and similar devices, Version 1.1, 2024-04, Joint Interpretation Working Group.

[JIL-ATT-SC] Attack Methods for Smartcards and Similar Devices, Version 2.5 (confidential), 2022-05, Joint Interpretation Working Group.

[JIL-COMP_CC2022] Composite product evaluation for Smart Cards and similar devices, Version 1.6, 2024-04, Joint Interpretation Working Group.

[JIL-COMP-ETR_CC2022] ETR for composite evaluation TD SC & SD, Version 1.2, 2024-04, Joint Interpretation Working Group.

[JIL-SC-EVAL_CC2022] Guidance for smartcard evaluation, Version 3.0, 2024-04, Joint Interpretation Working Group.

[JIL-SoACM] Remaining Strength of Asymmetric Cryptographic Mechanisms after Partial Key Leakage, Version 1.0 (confidential), 2020-06, Joint Inter-pretation Working Group.

[KS2011] 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.

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-1205-V4-2026

Evaluation results regarding development and production environment

The IT product IFX_CCI_00006Ah, IFX_CCI_00006Bh, IFX_CCI_00006Ch, design step S12 with firmware 80.311.04.1, optional NRG™ SW 05.03.4097, optional HSL v3.52.9708, UMSLC lib 01.30.0695, optional SCL v2.15.000, optional ACL v3.34.000 & 3.35.001, optional RCL v1.10.007, optional HCL v1.13.002 and user guidance (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 26 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	Company name and address
DHL Singapore	DHL Supply Chain Singapore Ptd Tampinese 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. 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