Federal Office
for Information Security

Certification Report

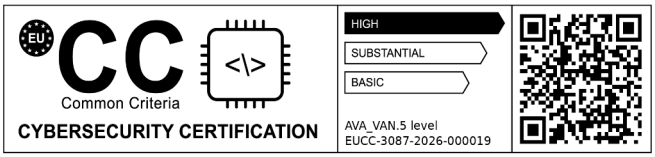
EUCC-3087-2026-0019
Administration ID
BSI-DSZ-CC-0961-V8-2026

for

Infineon 16-Bit controller IFX_CCI_0000XX with XX placeholder for the following numbers: 07h, 09h, 0Ah, 0Bh, 16h, 17h, 18h, 23h, 24h with design step G13

from

Infineon Technologies AG



BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Infoline +49 (0)228 99 9582-11

Contents

A. Certification....4
1. Preliminary Remarks....4
2. Specifications of the Certification Procedure....4
3. Recognition Agreements....5
4. Performance of Evaluation and Certification....5
5. Publication....7
B. Certification Results....8
1. Executive Summary....9
2. Identification of the TOE....10
3. Security Policy....13
4. Assumptions and Clarification of Scope....14
5. Architectural Information....15
6. Supplementary Cybersecurity Information....16
7. IT Product Testing....16
8. Evaluated Configuration....17
9. Results of the Evaluation....18
10. Obligations and Notes for the Usage of the TOE....21
11. Security Target....22
12. Regulation specific aspects (eIDAS, QES)....22
13. Bibliography....24
C. Annexes....32

A. Certification

1. Preliminary Remarks

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

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

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

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

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

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]
- BSI Certification and Approval Ordinance[3]

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

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

- 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.
- The TOE Infineon 16-Bit controller IFX_CCI_0000XX with XX placeholder for the following numbers: 07h, 09h, 0Ah, 0Bh, 16h, 17h, 18h, 23h, 24h with design step G13 has been certified by the certification body of the Federal Office for Information Security

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

(BSI) based on administration ID BSI-DSZ-CC-0961-V7-2024. Specific results from the corresponding evaluation process were re-used.

- The present evaluation of the product Infineon 16-Bit controller IFX_CCI_0000XX with XX placeholder for the following numbers: 07h, 09h, 0Ah, 0Bh, 16h, 17h, 18h, 23h, 24h with design step G13 was carried out by TÜV Informationstechnik GmbH, located at Unternehmensgruppe TÜV NORD
  Am TÜV 1
  45307 Essen.
- The evaluation was completed on 8 October 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 21 October 2026 is valid until 20 October 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 Infineon 16-Bit controller IFX_CCI_0000XX with XX placeholder for the following numbers: 07h, 09h, 0Ah, 0Bh, 16h, 17h, 18h, 23h, 24h with design step G13 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_000007h, IFX_CCI_000009h, IFX_CCI_00000Ah, IFX_CCI_00000Bh, IFX_CCI_000016h, IFX_CCI_000017h, IFX_CCI_000018h, IFX_CCI_000023h, IFX_CCI_000024h G13 including both production lines and optional software packages: Flash Loader, Asymmetric Cryptographic Library, Hardware Support Library, and CIPURSE™ Cryptographic Library.

The TOE provides a real 16-bit CPU-architecture and is compatible to the Intel 80251 architecture. The major components of the core system are the two CPUs (Central Processing Units), the MMU (Memory Management Unit), and MED (Memory Encryption/Decryption Unit). The controller can communicate using contact-based interfaces.

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

The product Infineon 16-Bit controller IFX_CCI_0000XX with XX placeholder for the following numbers: 07h, 09h, 0Ah, 0Bh, 16h, 17h, 18h, 23h, 24h with design step G13 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-0961-V7-2024. Specific results from the evaluation process BSI-DSZ-CC-0961-V7-2024 were re-used. The TOE deliverables are listed in table 1.

The evaluation of the product Infineon 16-Bit controller IFX_CCI_0000XX with XX placeholder for the following numbers: 07h, 09h, 0Ah, 0Bh, 16h, 17h, 18h, 23h, 24h with design step G13 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 8 October 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 Multi-Assurance
- Global Assurance Package: EAL 5
- Augmentation: ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_FLR.3, ALC_TAT.3, ATE_FUN.2, ATE_COV.3, AVA_VAN.5
- sub-TSF assurance Package: EAL 6 augmented with ALC_FLR.3

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

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

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:

Infineon 16-Bit controller IFX_CCI_0000XX with XX placeholder for the following numbers: 07h, 09h, 0Ah, 0Bh, 16h, 17h, 18h, 23h, 24h with design step G13

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

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
Hardware				
1.	HW	IFX_CCI_000007h, IFX_CCI_000009h, IFX_CCI_00000Ah, IFX_CCI_00000Bh, IFX_CCI_000016h, IFX_CCI_000017h, IFX_CCI_000018h, IFX_CCI_000023h, IFX_CCI_000024h	Design step G13	Plain wafers, bare dies, complete modules, IC cases of any type (for example TSSOP28, VQFN32, VQFN40, CCS-modules, etc.), with or without inlay mounting, or in whatever package. The customer (recipient) chooses the delivery method.
Optional IC dedicated software				
1.	FW	Firmware including BOS, RMS, and Flash Loader	FW Identifier 80.101.07.2 or 80.101.07.1 or 80.101.07.0	On-chip software
Mandatory TOE guidance documentation				
2.	DOC	16-bit Security Controller Family - V02, Hardware Reference Manual [HRM]	5.0 2019-06-13	Personalized PDF via secured download or on demand via encrypted mail.
3.	DOC	Production and personalization, 16-bit security controller [PPUM]	3.6 2019-06-24	Personalized PDF via secured download or on demand via encrypted mail.

No	Type	Identifier	Release	Form of Delivery
4.	DOC	16-bit Security Controller, 65-nm Technology, Programmer's Reference Manual [PRM]	9.14 2019-12-03	Personalized PDF via secured download or on demand via encrypted mail.
5.	DOC	16-bit Security Controller - V02, Security Guidelines [SG]	1.01-2479 2020-03-09	Personalized PDF via secured download or on demand via encrypted mail.
6.	DOC	16-bit Security Controller - V02, Errata Sheet [ES]	7.1 2019-11-05	Personalized PDF via secured download or on demand via encrypted mail.
7.	DOC	16-bit Security Controller, Crypto@2304T V3, User Manual [Crypto_UM]	2.0 2024-06-21	Personalized PDF via secured download or on demand via encrypted mail.
Optional IC dedicated support software: ACL				
1.	SW	RSA2048	v2.09.002	Precompiled object format code – L251 file type with ending ".lib via secured download as zipped file.
2.	SW	RSA4096	v2.09.002	Precompiled object format code – L251 file type with ending ".lib via secured download as zipped file.
3.	SW	EC	v2.09.002	Precompiled object format code – L251 file type with ending ".lib via secured download as zipped file.
4.	SW	Toolbox[6]	v2.09.002	Precompiled object format code – L251 file type with ending ".lib via secured download as zipped file.
5.	DOC	ACL52-Crypto2304T-C65 Asymmetric Crypto Library RSA/ECC/Toolbox, 16-bit Security Controller, User interface manual [ACL]	v2.09.002 2026-09-02	Personalized PDF via secured download or on demand via encrypted mail.
Optional IC dedicated support software: HSL-1				
6.	SW	Hardware Support Library (HSL)	v03.12.8812	Precompiled object format code – L251 file type with ending ".lib via secured download as zipped file.
	DOC	HSL library for SLCx2 [HSL_1]	1.0 2018-11-23	CHM file via secured download or on demand via encrypted mail.
Optional IC dedicated support software: HSL-2				
	SW	Hardware Support Library (HSL)	v03.11.8339	Precompiled object format code – L251 file type with ending ".lib via secured download as zipped file.

[6]Please note that the Toolbox library is not part of the TSF.

No	Type	Identifier	Release	Form of Delivery
	DOC	HSL library for SLCx2 [HSL_2]	1.0 2018-07-12	CHM file via secured download or on demand via encrypted mail.
Optional IC dedicated support software: HSL-3				
	SW	Hardware Support Library (HSL)	v02.01.6634	Precompiled object format code – L251 file type with ending ".lib via secured download as zipped file.
	DOC	Hardware Support Library for SLCx2 [HSL_3]	02.01.6634 2017-03-01	CHM file via secured download or on demand via encrypted mail.
Optional IC dedicated support software: HSL-4				
	SW	Hardware Support Library (HSL)	v01.22.4346	Precompiled object format code – L251 file type with ending ".lib via secured download as zipped file.
	DOC	Hardware Support Library for SLCx2 [HSL_4]	01.22.4346 2016	CHM file via secured download or on demand via encrypted mail.
Optional IC dedicated support software: CIPURSE™ CL: CCL				
	SW	Crypto Library (CIPURSE™ CL)	V02.00.0004	Precompiled object format code – L251 file type with ending ".lib via secured download as zipped file.
	DOC	CIPURSE™ Crypto Library, CCLX2xCIP v02.00.0004, CIPURSE™ V2, Compliant to OSPT™ Alliance CIPURSE™ V2 Cryptographic Protocol, User Interface	1.6 2018-02-02	Personalized PDF via secured download or on demand via encrypted mail.

Table 1: Deliverables of the TOE

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 send 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).

Respective distribution centers are listed in Appendix B.

In the field, the IC embedded software developer can identify a product in question using the Generic Chip Identification Mode (GCIM) and the user guidance. Furthermore, the RMS function IFX_ConfigurationRead can be used to retrieve further information. Thereby, the exact and distinct identification of any product with its exact configuration of this TOE is given.

The bytes 45, 46 and 47 of the GCIM include the Common Criteria Certification Identifier, which can be used to uniquely identify the certified TOE. This identifier reflects the name of the TOE as given in the ST and includes the hexadecimal values listed behind the “IFX_CCI_” part of the TOE name. Thus, this TOE is identified by the Common Criteria Certification Identifiers 0x000007, 0x000009, 0x00000A, 0x00000B, 0x000016, 0x000017, 0x000018, 0x000023, and 0x000024. These identifiers are used by the developer only for this TOE and reflect the same underlying basic hardware.

The design step of the TOE is indicated by byte 11 and 12 of the GCIM. The G13 is coded as 0x060D, where 0x06 stands for G and 0x0D for 13.

The GCIM can be activated after power-on with a dedicated signalling sequence and is also accessible by the user software. This GCIM outputs amongst other identifiers for the platform, chip mode, ROM code, chip type, design step, fabrication facility, wafer, die position, firmware, and the CCI. The interpretation of the chip identification data is described in [HRM, 6.5].

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 versions for the individual firmware parts can be received by the mapping given in [ALC_CMS].

The optional software parts of the TOE are identified by their unique version numbers. The user can verify that he received the correct version by calculating the hash signatures of the provided library files. The mapping of these hash signatures to the version numbers is provided in [ST, 10]. The version numbers of firmware and software are listed in Table 1.

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 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.

Furthermore, the TOE also contains a CIPURSE™ Cryptographic Library (CCL), which can be used to implement a CIPURSE™ V2 conformant protocol in the IC embedded software.

Besides that, the TOE can come with the optional Hardware Support Library (HSL in four alternative versions) 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 Chapters 7 and 8 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 respectively by the Composite Manufacturer. They are in particular: OE.Resp-Appl., OE.Process-Sec-IC, OE.Lim_Block_Loader, OE.Loader_Usage, OE.TOE_Auth and OE.Secure_Delivery.

OE.Resp-Appl. 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 [SG].

OE.Process-Sec-IC. This objective requires the protection of the TOE, as well as of its manufacturing and test data up to the delivery to the end-consumer. As defined in [ST, 2.2.5] the TOE can be delivered to the composite product manufacturer after phase 3 or after phase 4. 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.

OE.Lim_Block_Loader This objective 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 [PPUM, 4.5.3]. 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 authorised 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.
OE.Loader_Usage	This objective 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. [PPUM, 4] provides sufficient information regarding this topic.
OE.TOE_Auth	This objective requires that the environment has to support the authentication and verification mechanism and has to know the corresponding authentication reference data. The composite product manufacturer receives sufficient information with regard to the authentication mechanism in [PPUM, 4.2.2].
OE.Secure_Delivery	This objective requires an alternative transport protection in case the Flash Loader is disabled. Technical and / or organisational security procedures (e.g. a custom mutual authentication mechanism or a security transport) should be put in place by the customer (recipient) to secure the personalised TOE during delivery as required by the security needs of the loaded IC Embedded Software.

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

5. Architectural Information

The TOE consists of the following hardware:

- Core System:
  - Proprietary dual CPU implementation being comparable to the 80251 microcontroller architecture from functional perspective and with enhanced MCS®251 instruction set,
  - Cache with Post Failure Detection,
  - Memory Encryption/Decryption Unit (MED), and
  - Memory Management Unit (MMU).
- Memories:
  - Read-Only Memory (ROM), not available for the user,
  - Random Access Memory (RAM), and
  - SOLID FLASH™ NVM, the flash cell based non-volatile memory.
  - Memory Bus and Peripheral Bus.
- Coprocessors:
  - Crypto2304T for asymmetric algorithms like RSA and EC (optionally blocked) and

- Symmetric Crypto Coprocessor for DES and AES Standards (optionally blocked).

- Control:
  - Interface Management Module (IMM),
  - Interrupt and Peripheral Event Channel Controller (ITP),
  - Clock & Power Management, and
  - Control.
- System Peripherals:
  - Sensors & Filters and
  - User mode Security Life Control (UmSLC).
- Peripherals:
  - Different Hybrid Random Number Generator (HRNG):
  - Cyclic Redundancy Check module (CRC),
  - Universal Asynchronous Receiver/Transmitter (UART),
  - Inter-Integrated Circuit module (I2C), and
  - General Purpose Input Output (GPIO).

Further, more detailed information is readily available in the Security Target [ST], section 2.2.1.

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 five categories:

- Simulation tests (design verification),
- Qualification tests,
- Verification Tests,
- Security Evaluation Tests,
- 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 a subset of the tests of the developer by using the library of programs, tools, and prepared chip samples delivered to the evaluator 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 function-alities 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 functionality in scope of the current reevaluation into consideration (see Section 8). Penetration testing was planned based on the analysis results and performed for the underlying mechanisms of security functionalities on the lead platform (see Section 8). 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_000007h, IFX_CCI_000009h, IFX_CCI_00000Ah, IFX_CCI_00000Bh, IFX_CCI_000016h, IFX_CCI_000017h, IFX_CCI_000018h, IFX_CCI_000023h, IFX_CCI_000024h G13.

Depending on the blocking configuration, a product can have different user available configuration by order or by BPU (please refer to [ST, 1.1] 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 20/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-3087-2026-0019, administration ID BSI-DSZ-CC-0961-V8-2026
- was issued on: 21 October 2026
- is valid until: 20 October 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 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. For Reference of Legislatives and Standards quoted above see section 13.2.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits
Symmetric Coprocessor (SCP)					
1	Cryptographic	TDES	[NIST SP800-67],	112, 168	-

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits
	primitive		[ISO_18033-3]		
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	Yes
7	Integrity protection	#1 in CBC-MAC and CBC-MAC-ELB mode for MAC generation	[ISO_9797-1]	112, 168	No
8	Integrity protection	#2 in CBC-MAC and CBC-MAC-ELB mode for MAC generation	[ISO_9797-1]	128, 192, 256	No
Asymmetric Cryptographic Library (ACL)					
9	Confidentiality	RSA encryption	[PKCS #1, 5.1.1] [IEEE_P1363, 8.2.2]	1024 – 2112	No
10	Confidentiality	RSA decryption	[PKCS #1, 5.1.2] [IEEE_P1363, 8.2.1 (I) / 8.2.3]	1024 – 2112	No
11	Confidentiality	RSA decryption with CRT	[PKCS #1, 5.1.2] [IEEE_P1363, 8.2.1 (II) / 8.2.3]	1024 – 4224	Yes >= 2800 bit
12	Authenticity	RSA signature generation	[PKCS #1, 5.2.1] [IEEE_P1363, 8.2.1 (I) / 8.2.4]	1024 – 2112	No
13	Authenticity	RSA signature generation with CRT	[PKCS #1, 5.2.1] [IEEE_P1363, 8.2.1 (II) / 8.2.4]	1024 – 4224	No
14	Authenticity	RSA signature verification	[PKCS #1, 5.2.2] [IEEE_P1363, 8.2.5]	1024 – 4224	n/a
15	Key generation	RSA key generation utilizing the preparative function “CryptoGeneratePrime()” or the function “CryptoRSAKeyGen()	Proprietary The generated keys meet [PKCS #1], Sections 3.1 and 3.2 and [IEEE_P1363],	1024 – 4224	Yes >=2800bit

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits
			Section 8.1.3.1		
16	N/A	Supported elliptic curves: - All curves in [FIPS186-4], - All curves in [RFC5639].	[FIPS186-4] [RFC5639]	N/A	-
17	Authenticity	ECDSA signature generation on curves listed in #16	[ANS X9.62, 7.3] [ISO_14888-3, 6.4.3] [IEEE_P1363, 7.2.7]	160 – 521	N/A
18	Authenticity	ECDSA signature verification on curves listed in #16	[ANS X9.62, 7.4.1] [ISO_14888-3, 6.4.4] [IEEE_P1363, 7.2.8]	160 – 521	Key sizes 160, 163, 192, 224: No Key sizes >= 250: Yes
19	Key generation	Elliptic Curve key generation on curves listed in #16	[ANS X9.62, A.4.3] [ISO_14888-3, 6.4.2] [IEEE_P1363, A.16.9]	160 – 521	Key sizes 160, 163, 192, 224: No Key sizes >= 250: Yes
20	Key agreement	Elliptic Curve Diffie-Hellman (ECDH) key agreement on curves listed in #16	[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
Random Number generation (Hardware)					
21	RNG	Physical RNG	PTG.2 in [AIS31]	N/A	N/A
22	RNG	Hybrid RNG	corresponds to PTG.3 in [AIS31]	N/A	N/A
23	RNG	Deterministic RNG	corresponds to DRG.3 in [AIS20]	N/A	N/A
24	RNG	Deterministic RNG	corresponds to DRG.2 in [AIS20]	N/A	N/A
CIPURSE™ Cryptographic Library (CCL)					
25	Key Agreement	CIPURSE™ Session Key Agreement (using #2)	[CIPURSE-1, 5.3], [NIST SP800-38A]	128	–
26	Authentication	CIPURSE™ Authentication (using #2)	CIPURSE-1, 5.3 / 6.3], [NIST SP800-38A]	128	–
27	Confidentiality	CIPURSE™ Security Messaging for	[CIPURSE-1, 6.4],	128	–

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits
		Confidentiality (using #2)	[NIST SP800-38A]		
28	Integrity protection	CIPURSE™ Secure Messaging for Integrity (using #2)	[CIPURSE-1, 6.3], [CIPURSE-2, P.2], [NIST SP800-38A]	128	–

Table 2: TOE cryptographic functionality

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

Please note, that this holds true also for those algorithms, where no cryptographic 120-Bit-Level assessment was given. Consequently, the targeted Evaluation Assurance Level has been achieved for those functionalities as well.

The developer evidence [CR_MECH] lists the cryptographic functionalities used and provided by the TOE.

The strength of the these cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 52, Para. 4, Clause 2).

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 and/or 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.

In addition, the following aspects need to be fulfilled when using 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 [SG], [HRM], [PRM], [ES], [ACL], [HSL_1], [HSL_2], [HSL_3], [HSL_4], [CCL], and [Crypto_UM] 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 [PPUM] have to be considered.

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

- The security IC embedded software developer can deliver his software either to Infineon to let them implement it in the TOE (in the Flash memory) or to the composite product manufacturer to let him download the software in the Flash memory.
- The delivery procedure from the security IC embedded software developer to the composite product manufacturer is not part of this evaluation and a secure delivery is required.

The fulfilment of security objectives for the environment from the Security Target, [ST] shall be ensured as well.

11. Security Target

For the purpose of publishing, the public 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

BSI Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany

BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ICT	Information and communications technology
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

12.2. Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

Extension - The addition to an ST or PP of functional requirements not contained in CC part 2 and/or assurance requirements not contained in CC part 3.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Package - Named set of either security functional or security assurance requirements

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

13. Bibliography

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

[CC] ISO 15408:2022, Common Criteria for Information Technology Security Evaluation
- Part 1: Introduction and general model
- Part 2: Security functional components
- Part 3: Security assurance components
- Part 4: Framework for the specification of evaluation methods and activities
- Part 5: Pre-defined packages of security requirements
https://www.iso.org/standard/72891.html
https://www.iso.org/standard/72892.html
https://www.iso.org/standard/72906.html
https://www.iso.org/standard/72913.html
https://www.iso.org/standard/72917.html

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 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

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-0961-V8-2026, Version 3.9, 2026-09-02, Common Criteria Confidential Security Target IFX_CCI_000007h, IFX_CCI_000009h, IFX_CCI_00000Ah, IFX_CCI_00000Bh, IFX_CCI_000016h, IFX_CCI_000017h, IFX_CCI_000018h, IFX_CCI_000023h, IFX_CCI_000024h Design step G13, Infineon Technologies AG
Security Target lite, Version 3.9, 2026-09-02, Common Criteria Security Target Lite IFX_CCI_000007h, IFX_CCI_000009h, IFX_CCI_00000Ah, IFX_CCI_00000Bh, IFX_CCI_000016h, IFX_CCI_000017h, IFX_CCI_000018h, IFX_CCI_000023h, IFX_CCI_000024h Design step G13, 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 for the Product Infineon 16-Bit controller IFX_CCI_0000XX with XX placeholder for the following numbers: 07h, 09h, 0Ah, 0Bh, 16h, 17h, 18h, 23h, 24h with design step G13, Version 1,2026-09-11, EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY) , TÜV Informationstechnik GmbH, (confidential document)

[ETRfCOMP] ETR for composite evaluation for the Product Infineon 16-Bit controller IFX_CCI_0000XX with XX placeholder for the following numbers: 07h, 09h, 0Ah, 0Bh, 16h, 17h, 18h, 23h, 24h with design step G13, Version 1, 2026-09-11, EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION (ETR COMP), TÜV Informationstechnik GmbH (confidential document)

[HRM] Guidance documentation for the TOE, Version 5.0, 2019-06-13, 16-bit Security Controller Family – V02, Hardware Reference Manual, Infineon Technologies AG

[PPUM] Guidance documentation for the TOE, 3.6, 2019-06-24, Production and Personalization, 16-bit Security Controller in 65nm, Infineon Technologies AG

[PRM] Guidance documentation for the TOE, Version 9.14, 2019-12-03, 16-bit Security Controller 65-nm Technology, Programmer's Reference Manual, Infineon Technologies AG

[SG] Guidance documentation for the TOE, Version 1.01-2479, 2020-03-09, 16-bit Security Controller – V02 Security Guidelines, Infineon Technologies AG

[ES] Guidance documentation for the TOE, Version 7.1, 2019-11-05, 16-bit Security Controller – V02, Errata Sheet, Infineon Technologies AG

[Crypto_UM] Guidance documentation for the TOE, Version 2, 2024-06-21, 16-bit Security Controller, Crypto@2304T V3, User Manual, Infineon Technologies AG

[ACL] Guidance documentation for the TOE, Version 2.09.002, 2026-09-02, ACL52-Crypto2304T-C65 Asymmetric Crypto Library RSA / ECC / Toolbox 16-bit Security Controller User Interface, Infineon Technologies AG

[HSL_1] Guidance documentation for the TOE, Version 1.0, 2018-11-23 , HSL library for SLCx2, Version 03.12.8812, Infineon Technologies AG

[HSL_2] Guidance documentation for the TOE, Version 1.0, 2018-07-12, HSL library for SLCx2, Version 03.11.8339, Infineon Technologies AG

[HSL_3] Guidance documentation for the TOE, Version 02.01.6634, 2017-03-01, Hardware Support Library for SLCx2, Version 02.01.6634, Infineon Technologies AG

[HSL_4] Guidance documentation for the TOE, Version 01.22.4346, 2016, Hardware Support Library for SLCx2, Version 01.22.4346, Infineon Technologies AG

[CCL] Guidance documentation for the TOE, Version 1.6, 2018-02-02, CIPURSE™ Crypto Library, CCLX2xCIP v02.00.0004, CIPURSE™ V2, Compliant to OSPT™ Alliance CIPURSE™ V2 Cryptographic Protocol, User Interface, Infineon Technologies AG

[ALC_CMS] Life Cycle Support Configuration Management IFX_CCI_000007h with options Including optional Software Libraries 1.8 2024-08-12, Infineon Technologies AG

[CR_MECH] Documentation for the TOE, Version, 2026-09-03, Cryptographic Mechanisms 7h with options, Infineon Technologies AG

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.

[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.

[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.

[EUCC-ADV-ARC] EUCC Scheme State-of-The-Art Document - Security Architecture requirements (ADV_ARC) for smart cards and similar devices extended to Secure Sub Systems in SoCs, Version 1.1, 2023-10, ENISA.

[EUCC-AP-SC] EUCC Scheme State-of-The-Art Document - Application of Attack Potential to Smartcards and Similar Devices, Version 2, 2025-02, ENISA.

[EUCC-COMP-ETR] EUCC Scheme State-of-The-Art Document - ETR for Composite Evaluation Template, Version 1, 2025-09, ENISA.

[EUCC-COMP_CC2022] EUCC Scheme State-of-The-Art Document - Composite prod-uct evaluation and certification for CC: 2022, Version 1, 2025-02, ENISA.

[EUCC-IC-CC] EUCC Scheme State-of-The-Art Document - The Application of CC to Integrated Circuits, Version 2, 2024-12, ENISA.

[EUCC-ITSEF_SC] EUCC Scheme State-of-The-Art Document - Minimum ITSEF requirements for security evaluations of Smart Cards and similar devices, Version 1.1, 2023-10, ENISA.

[EUCC-MSSR] EUCC Scheme State-of-The-Art Document - Minimum Site Security Requirements, Version 2, 2025-02, ENISA.

[EUCC-OPEN-SC] EUCC Scheme State-of-The-Art Document - Certification of “open” smart card products, Version 1.1, 2023-10, ENISA.

[EUCC-Reg] COMMISSION IMPLEMENTING REGULATION (EU) 2024/482 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)*, 2024-02-07, Official Journal of the European Union.

[EUCC-SPM] EUCC Scheme State-of-The-Art Document - ADV_SPM.1 interpretation for CC:2022 transition, Version 1.1, 2025-10, ENISA.

[EUCC-STAR] EUCC Scheme State-of-The-Art Document - STAR methodology, Version 1, 2025-02, ENISA.

[EUCC-SPM] EUCC Scheme State-of-The-Art Document - ADV_SPM.1 interpretation for CC:2022 transition, Version 1.1, 2025-10, ENISA.

[EUCC-STAR] EUCC Scheme State-of-The-Art Document - STAR methodology, Version 1, 2025-02, ENISA.

13.2. Legislatives and Standards

[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.

[CIPURSE-1] CIPURSETM V2 Cryptographic Protocol issued by OSPTTM Alliance, 2012-09-28.

[CIPURSE-2] CIPURSETM V2 Cryptographic Protocol issued by OSPTTM Alliance, 2014-09-18 (with errata and precision list).

[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).

[FIPS186-5] Federal Information Processing Standards Publication FIPS PUB 186-5, Digital Signature Standard (DSS), 2023-02-03, 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_11770-3] ISO 11770-3: Information technology - Security techniques – Key management Part 3: Mechanisms using asymmetric techniques, ISO/IEC 11770-3:2008.

[ISO_14888-3] ISO 14888-3: Information technology - Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms, ISO/IEC 14888-3:2006.

[ISO_18033-3] ISO 18033-3: Information technology - Security techniques – Encryption algorithms – Part 3: Block ciphers, ISO/IEC 18033, 2010.

[ISO_9797-1] Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher, 199912, ISO/IEC.

[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 SP800-38A, Recommendation for Block Cipher Modes of Operation, The CMAC Mode for Authentication, 2005-05, 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.

[PCBC] Bruce Schneier, Applied Cryptography, Second Edition, John Wiley & Sons, 1996.

[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).

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-0961-V8-2026

Evaluation results regarding development and production environment

The IT product Infineon 16-Bit controller IFX_CCI_0000XX with XX placeholder for the following numbers: 07h, 09h, 0Ah, 0Bh, 16h, 17h, 18h, 23h, 24h with design step G13 (Tar get 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 21 October 2026, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support as claimed by the ST [ST] and that are stated in chapter 1 of this report are fulfilled for the development and production sites of the TOE.

Besides the relevant TOE distribution centers are as follows:

Distribution Center name	Address
DCE Infineon Technology AG, Kühne & Nagel	Stockstädter Straße 10 – Building 8A, 63762 Großostheim, Germany
DCH KWE Kintetsu World Express	DCH KWE Kintetsu World Express (China) Co., Ltd., Shanghai Pudong Airport Pilot Free Trade Zone, No.530 Zheng Ding Road, Shanghai, P.R. China, Building A5 Unit 1/6 & 1/9, Infineon Distribution Center China
DHL Singapore	DHL Supply Chain Singapore Pte. Ltd., Infineon Distribution Center Asia, Tampines LogisPark, 1 Greenwich Drive, Singapore 533865

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