



Certification Report

EUCC-3087-2025-12-0001

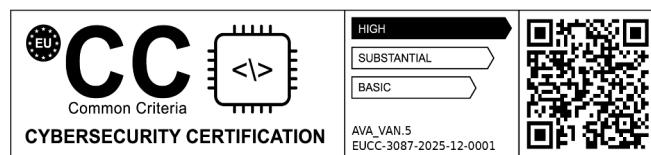
Administration ID
BSI-DSZ-CC-1079-V6-2025

for

**Infineon Security Controller IFX_CCI_00000Fh,
IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h,
IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah,
IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step
G12**

from

Infineon Technologies AG



BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-11

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.....	15
7. IT Product Testing.....	15
8. Evaluated Configuration.....	16
9. Results of the Evaluation.....	16
10. Obligations and Notes for the Usage of the TOE.....	26
11. Security Target.....	27
12. Regulation specific aspects (eIDAS, QES).....	27
13. Bibliography.....	28
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 Act¹, 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 BSIG¹ 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 Security²

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 I No. 301, p. 2

- BSI Certification and Approval Ordinance³
- BMI Regulations on Ex-parte Costs⁴
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior and Community)
- ISO/IEC 15408 as published on the day of issuance of this certificate and as mirrored by the Common Criteria for IT Security Evaluation (CC), Version CC:2022 [CC]
- ISO/IEC 18045 as published on the day of issuance of this certificate and as mirrored by the Common Methodology for IT Security Evaluation (CEM), Version CEM:2022 [CEM]
- DIN EN ISO/IEC 17065 standard
- EUCC programme: Scheme documentation describing the certification process (EUCC) [EUCC_PROG]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)

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 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

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 Infineon Security Controller IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step G12 has been certificied by the certification body of the Federal Federal Office for Information Security (BSI) based on administration ID BSI-DSZ-CC-1079-V5-2024. Specific results from the evaluation process were re-used.
- The evaluation of the product Infineon Security Controller IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step G12 was carried out by TÜV Informationstechnik GmbH. The evaluation was completed on 18 December 2025. TÜV Informationstechnik GmbH located at

Unternehmensgruppe TÜV NORD
Am TÜV 1
45307 Essen

is a notified evaluation facility (ITSEF) .

- This certification was applied for: Infineon Technologies AG.
- The assessed TOE was developed by: Infineon Technologies AG.
- The certification activities are concluded with the comparability check and the production of this Certification Report. This work was completed by the certification body of the BSI.

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

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

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

The issued Certificate confirms the assurance of the product claimed in the Security Target [ST] on certificate's issuance day. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be reassessed. Therefore, the holder of the certificate should involve the assurance continuity program of the EUCC Certification Scheme (e.g. by a re-assessment or re-certification) in its obligations to monitor the certified product. Specifically, if certification results should be used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a reassessment on a regular e.g. annual basis.

In order to prevent an indefinite certificate usage where evolving attack methods justify a recent reassessment of the product's resistance, the maximum validity period of the certificate is limited. The certificate issued on 19 December 2025 is valid until 18 December 2030 and its validity can be renewed by certifying the TOE.

The holder of this certificate is obliged:

1. to meet the obligations from the Implementing Regulation (EU) 2024/482, in particular but not exclusively to respect the rules for certificate usage, to monitor the conformity of the certified TOE, to inform the certification body about subsequently

detected vulnerabilities or irregularities with relevance to the security of the TOE and to maintain vulnerability management and disclosure procedures.

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

5. Publication

The TOE Infineon Security Controller IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step G12, 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 [or Protection Profiles], which is published regularly (see [EUCC_CERT]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

This holder of the certificate⁵ has to publish on its website this Certification Report and supplementary information. The Certification Report may also be obtained in electronic form at the internet address stated above.

⁵ Infineon Technologies AG
Am Campeon 1-15
85579 Neubiberg

B. Certification Results

The following chapters summarise the assessment results of the

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

1. Executive Summary

The Target of Evaluation (TOE) is the Infineon Technologies AG security controller (integrated circuit IC), IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch Design Step G12, including optional software libraries and dedicated firmware.

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

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 the MED (Memory Encryption/Decryption Unit). 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 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 Security Controller IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step G12 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 administration ID BSI-DSZ-CC-1079-V5-2024. Specific results from the evaluation process BSI-DSZ-CC-1079-V5-2024 were re-used. The TOE deliverables are listed in table 1.

The evaluation of the product Infineon Security Controller IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step G12 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 18 December 2025. 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: Global Assurance EAL 5

- Augmentation: Global Assurance: ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_FLR.3, ALC_TAT.3, ATE_FUN.2, ATE_COV.3, AVA_VAN.5 sub-TSF assurance level EAL6 augmented with ALC_FLR.3

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

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

Depending on the blocking configuration, an IFX_CCI_00000Fh G12 product can have e.g. different user available memory sizes and can come with or without individual accessible cryptographic coprocessors. All products are identical in regard to module design, layout, and footprint. All possible configuration options are described in Section 2..

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

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

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

2. Identification of the TOE

The Target of Evaluation (TOE) is identified as follows:

Infineon Security Controller IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step G12

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	Identifier	Release	Form of Delivery
1	HW	IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch	G12	Customer chooses delivery method for complete modules, with or without inlay mounting, with or without inlay antenna mounting, in form of plain wafers, in any IC case (for example TSSOP28, VQFN32, VQFN40, CCS-modules, etc.), in no IC case or package, simply as bare dies, or in whatever type of package. (refer to [ST, 2.2.5]).
2	FW	Boot Software (BOS)	80.102.06.0 or 80.102.06.1	Stored on the delivered hardware.

No	Type	Identifier	Release	Form of Delivery
3	FW	Flash Loader (FL) - Optional; depending on order	80.102.06.0 or 80.102.06.1	Stored on the delivered hardware.
4	FW	NRG ROM part - NRG is not part of the TOE Security Functionality (TSF)	80.102.06.0 or 80.102.06.1	Stored on the delivered hardware.
5	FW	Radio Frequency Application Interface (RFAPI) - The RFAPI functions are not part of the TOE Security Functionality (TSF)	80.102.06.0 or 80.102.06.1	Stored on the delivered hardware.
6	FW	Resource Management System (RMS)	80.102.06.0 or 80.102.06.1	Stored on the delivered hardware.
7	SW	RSA2048 Libraries - Optional; depending on order	v2.07.003, v2.08.007, v2.09.002	Secure download (precompiled object code – L251 file) via ishare.
8	SW	RSA4096 Libraries - Optional; depending on order	v2.07.003, v2.08.007, v2.09.002	Secure download (precompiled object code – L251 file) via ishare.
9	SW	EC Libraries - Optional; depending on order	v2.07.003, v2.08.007, v2.09.002	Secure download (precompiled object code – L251 file) via ishare.
10	SW	Toolbox Libraries - None of the Toolbox libraries is part of the TOE Security Functionality (TSF) - Optional; depending on order	v2.07.003, v2.08.007, v2.09.002	Secure download (precompiled object code – L251 file) via ishare.
11	SW	Base Libraries - Optional; depending on presence of RSA, EC, and Toolbox	v2.07.003, v2.08.007, v2.09.002	Secure download (precompiled object code – L251 file) via ishare.
12	SW	Symmetric Cryptographic Libraries (SCL) - Optional; depending on order	v2.04.002 or v2.13.001	Secure download (precompiled object code – L251 file) via ishare.
13	SW	Hash Cryptographic Library (HCL) - Optional; depending on order	v1.12.001	Secure download (precompiled object code – L251 file) via ishare.
14	SW	CIPURSE™ library (CCL) - Optional; depending on order	v02.00.0004	Secure download (precompiled object code – L251 file) via ishare.
15	SW	Hardware Support Libraries (HSL) - Optional; depending on order	v03.11.8339 or v03.12.8812	Secure download (precompiled object code – L251 file) via ishare.
16	SW	NRG Software Library (NRGS) - Optional; depending on order	v02.03.3446	Secure download (precompiled object code – L251 file) via ishare.
17	DOC	16-bit Security Controller Family – V05, Hardware Reference Manual	5.0 / 2019-06-14	Secured download (personalized PDF) via ishare or on demand via encrypted email.
18	DOC	Production Personalization, Security Controller and 16-bit	3.6 / 2019-06-24	Secured download (personalized PDF) via ishare or on demand via encrypted email.

No	Type	Identifier	Release	Form of Delivery
19	DOC	16-bit Security Controller, 65nm-Technology, Programmer's Reference Manual	9.14 / 2019-12-03	Secured download (personalized PDF) via ishare or on demand via encrypted email.
20	DOC	16-bit Security Controller – V05, Security Guidelines	1.01-3119 / 2025-09-02	Secured download (personalized PDF) via ishare or on demand via encrypted email.
21	DOC	16-bit Security Controller – V05, Errata Sheet	10.0 / 2021-02-25	Secured download (personalized PDF) via ishare or on demand via encrypted email.
22	DOC	CL52 Asymmetric Crypto Library for Crypto@2304T, RSA/ECC/Toolbox, 16-bit Security Controller, User Interface, Version 2.07.003 - Optional; delivered if RSA, EC, or Toolbox library version v2.07.003 is ordered.	2.07.003 / 2025-09-15	Secured download (personalized PDF) via ishare or on demand via encrypted email.
23	DOC	ACL52-Crypto2304T-C65 Asymmetric Crypto Library, RSA / ECC / Toolbox, 16-bit Security Controller, User Interface, Version 2.08.007 - Optional; delivered if RSA, EC, or Toolbox library version v2.08.007 is ordered.	2.08.007 / 2025-09-15	Secured download (personalized PDF) via ishare or on demand via encrypted email.
24	DOC	ACL52-Crypto2304T-C65 Asymmetric Crypto Library, RSA / ECC / Toolbox, 16-bit Security Controller, User Interface, Version 2.09.002 - Optional; delivered if RSA, EC, or Toolbox library version v2.09.002 is ordered.	2.09.002 / 2024-06-27	Secured download (personalized PDF) via ishare or on demand via encrypted email.
25	DOC	Hardware Support Library for SLCx2 Version 03.12.8812 - Optional; delivered if HSL is ordered	1.1 / 2019-07-08	Secured download (personalized PDF) via ishare or on demand via encrypted email.
26	DOC	Hardware Support Library for SLCx2 Version 03.11.8339 - Optional; delivered if HSL is ordered	1.0 / 2018-07-12	Secured download (personalized PDF) via ishare or on demand via encrypted email.
27	DOC	SCL52-SCP-v4-C65 Symmetric Crypto Library for SCP-v4 DES / AES 16-bit Security Controller, User Interface, Version 2.04.002 - Optional; delivered if SCL version v2.04.002 is ordered.	2.04.002 / 2018-05-22	Secured download (personalized PDF) via ishare or on demand via encrypted email.

No	Type	Identifier	Release	Form of Delivery
28	DOC	SCL52-SCP-v4-C65 Symmetric Cryptographic Library for SCP-v4 AES/DES/MAC, 16-bit Security Controller, User Interface, Version 2.13.001 - Optional; delivered if SCL version v2.13.001 is ordered.	2.13.001 / 2020-11-05	Secured download (personalized PDF) via ishare or on demand via encrypted email.
29	DOC	HCL52-CPU-C65 Hash Crypto Library for CPU SHA 16-bit Security Controller, User interface manual - Optional; delivered if HCL is ordered.	1.12.001 / 2020-01-14	Secured download (personalized PDF) via ishare or on demand via encrypted email.
30	DOC	CIPURSE™ Crypto Library, CCLX2xCIP v02.00.0004, CIPURSE™ V2, Compliant to OSPT™ Alliance CIPURSE™ V2 Cryptographic Protocol, User Interface Optional; delivered if CCL is ordered.	1.6 / 2018-02-02	Secured download (personalized PDF) via ishare or on demand via encrypted email.
31	DOC	16-bit Security Controller, Crypto@2304T V3, User Manual - Optional; delivered if the Crypto2304T is available on the TOE.	2.0 / 2024-06-21	Secured download (personalized PDF) via ishare or on demand via encrypted email.

Table 1: Deliverables of the TOE

3. Security Policy

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 a 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.

Furthermore, the TOE also contains the optional 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), which provides a simplified interface for NVM management and provides the possibility to write tearing safe into the NVM.

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

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

Specific details concerning the above-mentioned security policies can be found in Chapter 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 aspects lead to specific security objectives to be fulfilled and measures to be taken by the IT environment, the user or the risk manager. The following topics are of relevance:

The ST includes the following security objective for the IC embedded software developer: OE.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 [SEC].

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

The objective OE.Process-Sec-IC requires the protection of the TOE, as well as of its manufacturing and test data up to the delivery to the end-consumer. As defined in [ST, 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.

The objective OE.TOE_Auth requires that the environment has to support the authentication and verification mechanism and has to know the corresponding authentication reference data. The composite product manufacturer receives sufficient information with regard to the authentication mechanism in [PPUM, 3.2.2].

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. [PPUM, 3] 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 [PPUM, 3.5.3]. 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 authorized users only” and thus the flash loader can also be used in an unsecure environment and is able to protect itself against misuse if the authentication and download keys are handled appropriately.

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

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

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

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

5. Architectural Information

This ETR abbreviates the TOE as IFX_CCI_00000Fh for the sake of a better readability.

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 the MED (Memory Encryption/Decryption Unit). 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 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.

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

6. Supplementary Cybersecurity Information

The evaluated documentation as outlined in table 1 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

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

- the period during which support is offered (esp. security related updates)
- contact information of the manufacturer or provider and accepted methods for receiving vulnerability information from end users and security researchers

- a reference to online repositories listing publicly disclosed vulnerabilities related to the TOE/ICT product, 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 for details on assurance levels or packages involved into testing.

The developer performed five categories of tests:

- Simulation Tests (Design Verification),
- Qualification Tests,
- Verification Tests,
- Security Evaluation Test,
- Production Tests.

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

The evaluator was able to repeat 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 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 that do not modify the TOE physically. The penetration tests 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_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch G12 (Tainan).

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

As stated and detailed in the ETR [ETR], developer and evaluator tested the TOE in those configurations/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 the requirements of the Scheme [EUCC-VO],[EUCC_PROG], the Common Criteria [CC], the Common Evaluation Methodology [CEM], and all relevant interpretations and guidelines of the Scheme (AIS) [AIS].

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

The following guidance specific for the technology was used:

- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 1, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers, Version 14, 2017-10-11,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 14, Anforderungenan Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nachCC (Common Criteria), Version 7, 2010-08-03,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 19, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 9, 2014-11-03,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 20,Funktionalitätsklassen und Evaluationsmethodologie für deterministischeZufallszahlengeneratoren, Version 4, 2025-04-11, Herausgeber: Zertifizierungsstelle des BSI im Rahmen des Zertifizierungsschemas,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 23,Zusammentragen von Nachweisen der Entwickler, Version 4, 2017-03-15,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 26, Evaluationsmethodologie für in Hardware integrierte Schaltungen, Version 10, 2017-07-03,
- Attack Methods for Smartcards and Similar Devices, Version 2.5, 2022-05, Joint Interpretation Working Group (confidential),

- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 31, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 4, 2025-04-11
- Developer evidence for the evaluation of a physical true random number generator, Version 0.8, 2013-02-28, Bundesamt für Sicherheit in der Informationstechnik.
- Evaluation Report as part of the Evaluation Technical Report, Part B – ETR-Part True Physical and Hybrid Random Number Generator, Template-Version 0.7, 2013-02-28, Bundesamt für Sicherheit in der Informationstechnik.
- Application Notes and Interpretation of the Scheme (AIS) – AIS 34, Evaluation Methodology for CC Assurance Classes for EAL5+ (CC v2.3 & v3.1) and EAL6 (CC v3.1), Version 3, 2009-09-03,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 35, Öffentliche Fassung eines Security Target (ST-lite), Version 2, 2007-11-12
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 36, Kompositionsevaluierung, Version 5, 2017-03-15,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 37, Terminologie und Vorbereitung von Smartcard-Evaluierungen, Version 3, 2010-05-17,
- Application Notes and Interpretation of the Scheme (AIS) – AIS 38, Reuse of evaluation results, Version 2, 2007-09-28,
- Application Notes and Interpretation of the Scheme (AIS) – AIS 39, Formal Methods, Version 3, 2008-10-24, Bundesamt für Sicherheit in der Informationstechnik.
- Application Notes and Interpretation of the Scheme (AIS) – AIS 41, Guidelines for Pps and STs, Version 2, 2011-01-31,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 46, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren, Version 3, 2013-12-04,
- Anwendungshinweise und Interpretationen zum Schema (AIS) – AIS 47, Regelungen zu Site Certification, Version 1.1, 2013-12-04

are considered.

Additionally the CC Supporting Mandatory Technical Documents

- Joint Interpretation Library – Application of Attack Potential to Smartcards, Version 3.2.1, 2024-02 and
- Joint Interpretation Library – ETR template for composite evaluation of Smart Cards and similar devices, Version 1.1, August 2015
- Transition Policy to CC:2022 and CEM:2022, 2023-04-20, Common Criteria Recognition Arrangement Management Committee, CCMC-2023-04-001.
- EUCC Scheme State-of-The-Art Document - Security Architecture requirements (ADV_ARC) for smart cards and similar devices extended to Secure Sub Systems in SoCs, Version 1.1, 2023-10, ENISA.
- EUCC Scheme State-of-The-Art Document - Application of Attack Potential to Smartcards and Similar Devices, Version 1.2, 2023-08, ENISA.

- EUCC Scheme State-of-The-Art Document - Application of Attack Potential to Smartcards and Similar Devices, Version 2.0 (DRAFT), 2025-02, ENISA.
- EUCC Scheme State-of-The-Art Document - Composite product evaluation and certification for CC: 2022, Version 1.0 (DRAFT), 2025-02, ENISA.
- EUCC Scheme Guideline on Cryptography, Version 2, 2025-05, ENISA.
- 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), 2024-01-31, ENISA.
- EUCC Scheme State-of-The-Art Document - The Application of CC to Integrated Circuits, Version 1.1, 2023-10, ENISA.
- EUCC Scheme State-of-The-Art Document - The Application of CC to Integrated Circuits, Version 2.0 (DRAFT), 2024-12, ENISA.
- EUCC Scheme State-of-The-Art Document - Minimum ITSEF requirements for security evaluations of Smart Cards and similar devices, Version 1.1, 2023-10, ENISA.
- EUCC Scheme State-of-The-Art Document - Minimum Site Security Requirements, Version 1.1, 2023-10, ENISA.
- EUCC Scheme State-of-The-Art Document - Minimum Site Security Requirements, Version 2.0 (DRAFT), 2025-02, ENISA.
- EU Commission Implementing Regulation 2024/482, 2024-01-31, EU
- EUCC Scheme State-of-The-Art Document - STAR methodology, Version 1.0 (DRAFT), 2025-02, ENISA.
- Remaining Strength of Asymmetric Cryptographic Mechanisms after Partial Key Leakage, Version 1.0 (confidential), 2020-06, Joint Interpretation Working Group.
- Joint Interpretation Library – Assurance Continuity - Practical Cases for Smart Cards and similar devices, Version 1.1, 2024-04, Joint Interpretation Working Group.
- ETR for composite evaluation TD SC & SD, Version 1.2, 2024-04, Joint Interpretation Working Group.
- ADV_SPM.1 interpretation for [CC:2022] transition, Joint Interpretation Library, Version 1.0, 2024-05

are considered.

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

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

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

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

The certificate

- is uniquely identified by: EUCC-3087-2025-12-0001, administration ID BSI-DSZ-CC-1079-V6-2025
- was issued on: 19 December 2025
- is valid until: 18 December 2030

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

9.2. Results of cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 52, Para. 4, Clause 2). But cryptographic functionalities with a security level of lower than 120 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (<https://www.bsi.bund.de>).

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

Purpose	Cryptographic Mechanism	Standard Implementation	Key Size in Bits	Category according to [EUCC-Crypto]	Security Level above 120 Bits
Key Agreement	ECDH (ACL v2.07.003, v2.08.007, and v2.09.002)	[ANS_X9.63], [IEEE_P1363], [ISO_11770-3]	The used elliptic curves NIST: P-{256, 384, 521} [FIPS186-5]; brainpool: P{256, 384, 512}r1 [RFC5639]	Recommended	Key size < 250: No Key sizes >=250: Yes
			The used elliptic curves NIST: P-{192, 224}, K-{163, 233, 283, 409}, B-{233, 283, 409} [FIPS186-4]; brainpool: P{160, 192, 224, 320, 384, 512}t1, P{160, 192, 224, 320}r1 [RFC5639]	NONE	
	CIPURSE™ Session Agreement (using AES) (CCL v02.00.0004)	Key5.3, [FIPS197], [NIST SP800-38A]	k = 128	NONE	--

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Category according to [EUCC-Crypto]	Security Level above 120 Bits
Cryptographic Primitive	TDES in modes ECB, CBC (SCP, SCL v2.04.002, v2.13.001) CTR, CFB (SCL v2.04.002, v2.13.001) CBC-MAC, CBC-MAC-ELB (SCP) PCBC (SCL v2.04.002, v2.13.001) BLD (blinding) and Recrypt (SCP) CMAC (SCL v2.04.002, v2.13.001) Retail-MAC (SCL v2.13.001)	[NIST SP800-67], [ISO_18033-3] [NIST SP800-38A] [ISO_9797-1] [ISO_9797-1] [PCBC] proprietary implementation [NIST SP800-38B] [ISO_9797-1]	$ k = 112, 168$ $ k = 112$	Legacy for $ k = 168$ NONE for $ k = 112$	No
RSA encryption decryption signature generation verification (only modular exponentiation part) (ACL v2.07.003, v2.08.007, and v2.09.002)	[PKCS #1], [IEEE_P1363]	Modulus length ⁶ = 1976 – 4224	RSA encryption is only in the scope of the for n ≥ 3000 evaluation up to 2112 bits.	Legacy for n ≥ 1900 and log2(e) > 16 Recommended for n ≥ 3000 and log2(e) > 16	Yes for 2800 bit only.
ECDSA signature generation (ACL v2.07.003, v2.08.007, and v2.09.002)	[ANS X9.62], [IEEE_P1363], [ISO_14888-3]	The used elliptic curves NIST: P{256, 384, 521} [FIPS186-5]; brainpool: P{256, 384, 512}r1 [RFC5639]	Recommended	Key size < 250: No Key sizes >=250: Yes	

⁶ Please note that the RSA library supports key lengths from 65 to 4224 bits; however, key lengths below 1976 bits are not included in the certificate.

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Category according to [EUCC-Crypto]	Security Level above 120 Bits
			The used elliptic curves NIST: P-{192, 224}, K-{163, 233, 283, 409}, B-{233, 283, 409} [FIPS186-4]; brainpool: P{160, 192, 224, 320, 384, 512}t1, P{160, 192, 224, 320}r1 [RFC5639]	NONE	
ECDSA signature verification (ACL v2.07.003, v2.08.007, and v2.09.002)	[ANS_X9.62], [IEEE_P1363], [ISO_14888-3]		The used elliptic curves NIST: P-{256, 384, 521} [FIPS186-5]; brainpool: P{256, 384, 512}r1 [RFC5639]	Recommended	Key size < 250: No Key sizes >=250: Yes
			The used elliptic curves NIST: P-{192, 224}, K-{163, 233, 283, 409}, B-{233, 283, 409} [FIPS186-4]; brainpool: P{160, 192, 224, 320, 384, 512}t1, P{160, 192, 224, 320}r1 [RFC5639]	NONE	
Random Number Generator	Physical RNG PTG.2	True	[AIS31]	N/A [EUCC-Crypto]: Note 67- No Direct Random Source. Since true random sources may produce outputs with statistical defects, their use should be limited to providing (re)seed material or additional input for deterministic	--

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Category according to [EUCC-Crypto]	Security Level above 120 Bits
				random bit generators. The direct use of a pure true random generator is not agreed.	
	Hybrid Random Number Generator PTG.3	[AIS31]	N/A	NONE	--
	Deterministic Random Number Generation DRG.2	[AIS31]	N/A	NONE	--
	Deterministic Random Number Generation DRG.3	[AIS31]	N/A	NONE	--
Key Generation	RSA key Generation using CryptoGenerateKeyPrime (ACL v2.09.002)	Proprietary The generated keys meet [PKCS #1, 3.1 / 3.2] and [IEEE_P1363, 8.1.3.1]	1976 - 4096	NONE	Yes >= 2800 bit only.
	EC key generation using ECC_ECDSAKeyGen (ACL v2.07.003, v2.08.007, and v2.09.002)	[ISO_14888-3, 6.4.2] [IEEE_P1363, A.16.9]	Key sizes corresponding to the used elliptic curves NIST: P-{192, 224, 256, 384, 521}, K-{163, 233, 283, 409}, B-{233, 283, 409} [FIPS186-4]; brainpool: P{160, 192, 224, 256, 320, 384, 512}r1, P{160, 192, 224, 256, 320, 384, 512}r1 [RFC5639]	Recommended	Key size < 250: No Key sizes >=250: Yes
	EC key generation using ECC_ECDSAKeyGenMask (ACL v2.07.003, v2.08.007, and v2.09.002)	[ANS_X9.62, 4.3] [ISO_14888-3, 6.4.2] [IEEE_P1363, A.16.9]	Key sizes corresponding to the used elliptic curves NIST: P-{192, 224, 256, 384, 521}, K-{163, 233, 283, 409}, B-{233, 283, 409} [FIPS186-4];	Recommended	Key size < 250: No Key sizes >=250: Yes

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Category according to [EUCC-Crypto]	Security Level above 120 Bits
			brainpool: P{160, 192, 224, 256, 320, 384, 512}t1, P{160, 192, 224, 256, 320, 384, 512}r1 [RFC5639]		
Authentication	CIPURSE™ Authentication (using AES) (CCL v02.00.0004)	[CIPURSE-1, 5.3 / 6.3], [FIPS197], [NIST SP800-38A]	k = 128	NONE	--
Confidential communication	CIPURSE™ Secure Messaging for Confidentiality (using AES) (CCL v02.00.0004)	[CIPURSE-1, 6.4], [FIPS197], [NIST SP800-38A]	k = 128	NONE	--
Integrity protected communication	CIPURSE™ Secure Messaging for Integrity (using AES) (CCL v02.00.0004)	[CIPURSE-1, 6.3], [CIPURSE-2, P. 2], [FIPS197], [NIST SP800-38A]	k = 128	NONE	--
Digest computation	SHA-1 and SHA-2 hash digest computation (HCL v1.12.001)	[FIPS180-4]	N/A	NONE for SHA1 Recommended for SHA2 with digest ≥ 256 bits Legacy for SHA2 with digest < 256 bits	

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.

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. Detailed results on conformance have been compiled into the report [CSCV].

Reference of Legislatives and Standards quoted above:

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

[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 SP 800-38B] NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication, 2005-05, National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Commerce.

[FIPS197] Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTION STANDARD (AES), November 2001, U.S. department of Commerce / National Institute of Standards and Technology (NIST).

[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, 2011-12-21, American National Standards Institute.

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

[ISO_11770-3] International Standard ISO/IEC 11770-3: 2008, Technical Corrigendum 1, Information technology - Security techniques – Key management Part 3: Mechanisms using asymmetric techniques, 2009-09-15.

[CIPURSE-1] CIPURSE™ V2 Cryptographic Protocol issued by OSPT™ Alliance, 2012-09-28

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

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

[ISO_9797-1]	Information technology – Security techniques – Message Authentication Codes (MACs), Part 1: Mechanisms using a block cipher, 2011-03-01, ISO/IEC.
[Schneier]	Applied Cryptography, Second Edition, B. Schneier, John Wiley & Sons, 1996
[PKCS-1]	PKCS #1: RSA Cryptography Standard, Version 2.2, 2012-10-27, RSA Cryptographic Standard, RSA Laboratories.
[ISO_14888-3]	International Standard ISO/IEC 14888-3: 2006, Technical Corrigendum 2: Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms, 2009-02-15.
[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, 2011-12-21, American National Standards Institute.

10. Obligations and Notes for the Usage of the TOE

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

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

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

Some security measures are partly implemented in this certified TOE, but require additional configuration or control or measures to be implemented by a product layer on top, e.g. the IC Dedicated Support Software using the TOE. For this reason the TOE includes guidance documentation (see table 2) which contains obligations and guidelines for the developer of the product layer on top on how to securely use this certified TOE and which measures have to be implemented in order to fulfil the security requirements of the Security Target of the TOE. In the course of the evaluation of the composite product or system it must be examined if the required measures have been correctly and effectively implemented by the product layer on top. Additionally, the evaluation of the composite product or system must also consider the evaluation results as outlined in the document "ETR for composite evaluation" [ETRfCOMP].

At the point in time when evaluation and certification results are reused there might be an update of the document "ETR for composite evaluation" available. Therefore, the certified products list on the BSI website has to be checked for latest information on reassessments, recertifications or maintenance result available for the product.

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

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

- All security hints described in the delivered documents [SEC], [HRM], [PRM], [Crypto_UM], [ES], [SCL-1], [SCL-2], [ACL-1], [ACL-2], [ACL-3], [HCL], [HSL-1], [HSL-2], and [CCL] 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.

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

- OE.Secure_Delivery - Secure Delivery of the TOE in case of deactivated flash loader
When the TOE is ordered with a disabled Flash Loader, it does not provide full transport protection. Therefore, 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 to secure the personalized TOE during delivery as required by the security needs of the loaded IC Embedded Software.

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

11. Security Target

For the purpose of publishing, the Security Target [ST] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the provisions of the EUCC certification scheme policy (see Implementing Regulation (EU) 2024/482, Annex V, V.2).

SHA256 hash of the ST:

e100b350a75dc6986be6e4919732628f44e93d625a20409877fd15fa5b5672c7

SHA256 hash of the ST lite:

603eb7c8e8096bfea2964fc3fbf9cb0e5e34cfab1693dec890ee5aa2cec54526

For the purpose of publishing, the Security Target [ST] of the Target of Evaluation (TOE) 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 Technologies
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

<https://www.commoncriteriaproject.org>

[CEM]

ISO 18045:2022: Information technology Security techniques
Methodology for IT security evaluation

<https://www.iso.org/standard/72889.html>

as mirrored by CCRA's edition:

CEM:2022 R1, Common Methodology for Information Technology

	Security Evaluation https://www.commoncriteriaprofile.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 TOE⁷ https://www.bsi.bund.de/AIS
[ST]	Security Target BSI-DSZ-CC-1079-V6-2025, Version 3.7, 2025-11-28, Confidential Security Target IFX_CCI_00000Fh IFX_CCI_000010h IFX_CCI_000026h IFX_CCI_000027h IFX_CCI_000028h IFX_CCI_000029h IFX_CCI_00002Ah IFX_CCI_00002Bh IFX_CCI_00002Ch G12, Infineon Technologies AG (confidential document) Security Target lite, Version 3.7, 2025-11-28, Public Security Target IFX_CCI_00000Fh IFX_CCI_000010h IFX_CCI_000026h IFX_CCI_000027h IFX_CCI_000028h IFX_CCI_000029h IFX_CCI_00002Ah IFX_CCI_00002Bh IFX_CCI_00002Ch G12, Infineon Technologies AG
[PP]	Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014
[ETR]	Evaluation Technical Report, Version 4, 2025-12-18, EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY) Common Criteria CC:2022 (Multi-Assurance with global assurance level EAL5 augmented with ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_FLR.3, ALC_TAT.3, ATE_FUN.2, ATE_COV.3, AVA_VAN.5 and sub-TSF assurance level EAL6 augmented with ALC_FLR.3), TÜV Informationstechnik GmbH, (confidential document)
[ETRfCOMP]	ETR for composite evaluation for the Product IFX_CCI_00000Fh IFX_CCI_000010h IFX_CCI_000026h IFX_CCI_000027h IFX_CCI_000028h IFX_CCI_000029h IFX_CCI_00002Ah IFX_CCI_00002Bh IFX_CCI_00002Ch G12, Version 4, 2025-12-18, Evaluation Technical for Composite Evaluation (ETR COMP) for the IFX_CCI_00000Fh G12, TÜV Informationstechnik GmbH (confidential document)
[ConfList]	Life Cycle Support Configuration Management for Common Criteria with Evaluation Assurance Level EAL6 augmented (EAL6+) IFX_CCI_00000Fh with options Including optional Software Libraries Flash Loader – 3x ACL – 2xHSL – 2x SCL HCL – CCL – NRG, Version 1.0, 2025-09-18, Infineon Technologies AG (confidential document)
[HRM]	16-bit Security Controller Family – V05, Hardware Reference Manual, Version 5.0, 2019-06-14, Infineon Technologies AG
[PPUM]	Production and Personalization, 16-bit Security Controller, Version 3.6, 2019-06-24, Infineon Technologies AG

⁷See section 9.1 for detailed list of used AIS

[PRM]	16-bit Security Controller, 65nm-Technology, Programmer's Reference Manual, Version 9.14, 2019-12-03, Infineon Technologies AG
[SEC]	16-bit Security Controller – V05, Security Guidelines, Version 1.01-3119, 2025-09-02, Infineon Technologies AG
[ES]	16-bit Security Controller – V05, Errata Sheet, Version 10.0, 2021-02-25, Infineon Technologies AG
[ACL-1]	ACL52 Asymmetric Crypto Library for Crypto@2304T, RSA/ECC/Toolbox, 16-bit Security Controller, User Interface, Version 2.07.003, 2025-09-15, Infineon Technologies AG
[ACL-2]	ACL52-Crypto2304T-C65 Asymmetric Crypto Library, RSA / ECC / Toolbox, 16-bit Security Controller, User Interface, Version 2.08.007, 2025-09-15, Infineon Technologies AG
[ACL-3]	ACL52-Crypto2304T-C65 Asymmetric Crypto Library, RSA / ECC / Toolbox, 16-bit Security Controller, User Interface, Version 2.09.002, 2024-06-27, Infineon Technologies AG
[HSL-1]	Hardware Support Library for SLCx2 Version 03.12.8812, 2019-07-08, Version 1.1, Infineon Technologies AG
[HSL-2]	Hardware Support Library for SLCx2 Version 03.11.8339, Version 1.0, 2018-07-12, Version 1.0, Infineon Technologies AG
[SCL-1]	SCL52-SCP-v4-C65 Symmetric Crypto Library for SCP-v4 DES / AES 16-bit Security Controller, User Interface, Version 2.04.002, 2018-05-22, Infineon Technologies AG
[SCL-2]	SCL52-SCP-v4-C65 Symmetric Cryptographic Library for SCP-v4 AES/DES/MAC, 16-bit Security Controller, User Interface, Version 2.13.001, 2020-11-05, Infineon Technologies AG
[HCL]	HCL52-CPU-C65 Hash Crypto Library for CPU SHA 16-bit Security Controller, User interface manual, Version 1.12.001, 2020-01-14, Infineon Technologies AG
[CCL]	CIPURSE™ Crypto Library, CCLX2xCIP v02.00.0004, CIPURSE™ V2, Compliant to OSPT™ Alliance CIPURSE™ V2 Cryptographic Protocol, User Interface, Version 1.6, 2018-02-02, Infineon Technologies AG
[Crypto UM]	16-bit Security Controller, Crypto@2304T V3, User Manual, Version 2, 2024-06-21, Infineon Technologies AG
[CSV]	Cryptographic Standards Compliance Verification, Version 1, 2024-09-12, TÜV Informationstechnik GmbH (confidential document)
[STAR Dresden]	„Site Technical Audit Report (STAR) Infineon Technologies GmbH & Co. KG, Dresden“, Version 2, 2025-12-15, TÜV Informationstechnik GmbH (confidential document)
[STAR München]	„Site Technical Audit Report (STAR) Infineon Technologies AG, Munich“, Version 5, 2025-06-04, TÜV Informationstechnik GmbH (confidential document)

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-1079-V6-2025

Evaluation results regarding development and production environment



Common Criteria

The IT product Infineon Security Controller IFX_CCI_00000Fh, IFX_CCI_000010h, IFX_CCI_000026h, IFX_CCI_000027h, IFX_CCI_000028h, IFX_CCI_000029h, IFX_CCI_00002Ah, IFX_CCI_00002Bh, IFX_CCI_00002Ch in the design step G12 (Target of Evaluation, TOE) 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 19 December 2025, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support as claimed by the ST [ST] and that are stated in chapter 1 of this report are fulfilled for the development and production sites of the TOE listed below are the Distribution Centres:

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

The Site Technical Audit Reports (STAR) ([STAR München], [STAR Dresden]) are part of this certification procedure.

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