Federal Office
for Information Security

Certification Report

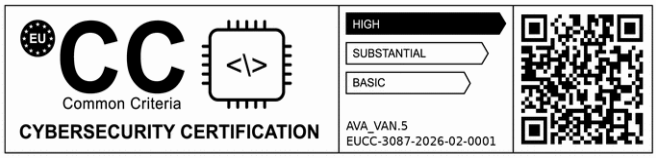
EUCC-3087-2026-02-0001
Administration ID
BSI-DSZ-CC-1272-2026

for

IFX_CCI_00007Ah/8Fh A11, R11, M11 with optional Crypto Suite

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

1. Preliminary Remarks

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

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

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

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

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

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

This Certification Report is the result of the certification activities carried out by the certification body of the BSI in conclusion of the technical evaluation. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

2. Specifications of the Certification Procedure

The certification body carries out its activities according to the criteria laid down in the following:

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

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

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

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

3. Recognition Agreements

In order to avoid multiple certifications of the same product in different countries a mutual recognition of IT security certificates – as far as such certificates are based on ITSEC or CC – under certain conditions was agreed

3.1. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The current list of signatory nations and approved certification schemes can be seen on the website: https://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 5 EAL 2 and ALC_FLR components.

4. Performance of Evaluation and Certification

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

[3] Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung – BSIZertV) of 02 December 2025, Bundesgesetzblatt 2025, no. 301

[4] BMI Regulations on Ex-parte Costs - Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) - dated 2 September 2019, Bundesgesetzblatt I p. 1365

- The TOE IFX_CCI_00007Ah/8Fh A11, R11, M11 with optional Crypto Suite, has been certified by the certification body of the Federal Federal Office for Information Security (BSI).
- The evaluation of the product IFX_CCI_00007Ah/8Fh A11, R11, M11 with optional Crypto Suite, was carried out by TÜV Informationstechnik GmbH, located at:
  Unternehmensgruppe TÜV NORD
  Am TÜV 1
  45307 Essen.
- The evaluation was completed on 18 December 2025. TÜV Informationstechnik GmbH is a notified evaluation facility (ITSEF) .
- This certification was applied for: Infineon Technologies AG.
- The assessed TOE was developed by: Infineon Technologies AG.
- The certification activities are concluded with the comparability check and the production of this Certification Report. This work was completed by the certification body of the BSI.

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

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

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

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

In order to prevent an indefinite certificate usage where evolving attack methods justify a recent reassessment of the product’s resistance, the maximum validity period of the certificate is limited. The certificate issued on 17 February 2026 is valid until 16 February 2031 and its validity can be renewed by certifying the TOE again.

The holder of this certificate is obliged:

1. to meet the obligations from the Implementing Regulation (EU) 2024/482, in particular but not exclusively to respect the rules for certificate usage, to monitor the conformity of the certified TOE, to inform the certification body about subsequently detected vulnerabilities or irregularities with relevance to the security of the TOE and to maintain vulnerability management and disclosure procedures.

Should changes be introduced into the certified version of the TOE, the validity period of its related certificate can be extended in order to cover the changed TOE, provided the holder of the certificate applies for measures under EUCC scheme’s assurance continuity

(i.e. recertification or maintenance) and the changed TOE then meets the assurance requirements.

5. Publication

The TOE IFX_CCI_00007Ah/8Fh A11, R11, M11 with optional Crypto Suite, has been notified to ENISA for publication on the website on European cybersecurity certification schemes and has also been included in BSI's list of certified products, which is published regularly (see [EUCC_CERT]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

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

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

B. Certification Results

The following chapters summarise the assessment results of the

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

1. Executive Summary

The Target of Evaluation is the Infineon Security Controller IFX_CCI_00007Ah A11 / R11 / M11, IFX_CCI_00008Fh R11 / M11 with firmware version 80.510.04.03, optional Crypto Suite 5.02.003 and user guidance documents.

The TOE provides a 32-bit Armv8-M CPU architecture. The major components of the processor system are the CPU (Central Processing Unit), a MPU (Memory Protection Unit), a Security Attribution Unit (SAU), a Nested Vectored Interrupt Controller (NVIC), an Instruction Stream Signature (ISS) coprocessor, and a Masked Instruction Set Extension (MISE) coprocessor. The TOE can communicate using contact-based and contactless 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 IFX_CCI_00007Ah/8Fh A11, R11, M11 with optional Crypto Suite, has been certified under the EUCC scheme in accordance to the provisions of the Implementing Regulation (EU) 2024/482. The TOE deliverables are listed in table 1.

The evaluation of the product IFX_CCI_00007Ah/8Fh A11, R11, M11 with optional Crypto Suite, 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 6
- Augmentation: ALC_FLR.1 and ATE_SDP.1

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

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

Depending on the blocking configuration, the product can have different user available memory sizes and interface configurations. All products are identical regarding module design, layout, and footprint. All possible configuration options are achieved by blocking only.

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

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

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

2. Identification of the TOE

The Information and communications technology product is identified as follows:

IFX_CCI_00007Ah/8Fh A11, R11, M11 with optional Crypto Suite,

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:

#	Type	Item / identifier	Release(s) / version(s)	Form of delivery
1	HW	IFX_CCI_00007Ah A11 / R11 / M11, IFX_CCI_00008Fh R11 / M11	A11, R11, M11 (design step)	Depending on customer order. As stated in [ST, 1.4.4], the hardware can be delivered as bare dies (sawn wafer), as modules, or in an IC case.
2	FW	Firmware (BOS, ROM part of HSL, Flash Loader)	80.510.04.03 (Flash Loader version is also separately identified as version 10.09.0000)	Stored on the delivered hardware.
3	SW	HSL (NVM part)	04.07.0000	Secure download of object file via iShare.
4	SW	UMSLC library	02.01.0040	Secure download of object file via iShare.
5	SW	CryptoSuite (optional)	5.02.003	Secure download of object file via iShare.
6	DOC	*TEGRION™ SLC22 (32-bit Security Controller – V31) Hardware Reference Manual*	Rev. 3.1, 2025-04-22	Personalized PDF via secure iShare server.
7	DOC	*TEGRION™ SLx2 security controller family Programmer's Reference Manual SLx2_DFP*	Rev. 1.9.0, 2025-10-16	Personalized PDF via secure iShare server.
8	DOC	*SLC22 32-bit Security Controller – V31 Security Guidelines*	1.00-3076, 2025-04-30	Personalized PDF via secure iShare server.

#	Type	Item / identifier	Release(s) / version(s)	Form of delivery
9	DOC	*TEGRION SLC22 (32-bit Security Controller – V31) Preliminary Production and personalization manual*	Rev. 10.09, 2025-05-12	Personalized PDF via secure iShare server.
10	DOC	*Crypto2304T V4, User Manual*	v3.0, 2024-06-21	Personalized PDF via secure iShare server.
11	DOC	*CS-SLC22V31 CryptoSuite 32-bit Security Controller User interface manual*	v5.02.003, 2025-10-02	Personalized PDF via secure iShare server.
12	DOC	*TEGRION™ SLx22 (32-bit Security Controller – V31) Errata sheet*	Rev. 2.0, 2025-06-27	Personalized PDF via secure iShare server.

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 different cryptographic algorithms to ensure the authenticity, confidentiality, and integrity of data and to support secure authentication protocols it will provide a true random number generator.

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

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

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

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

4. Assumptions and Clarification of Scope

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

The objective OE.Resp-Appl states that the IC Embedded Software Developer shall treat user data (especially keys) of the composite product appropriately.

The ST includes multiple objectives for the Composite Product Integrator and Personaliser: OE.Process-Sec-IC, OE.Lim_Block_Loader, OE.Loader_Usage, OE.TOE_Auth, OE.Secure_UC_Load, OE.Secure_Delivery.

Details can be found in the Security Target [ST], chapter 4.2.

5. Architectural Information

The TOE provides a 32-bit Armv8-M CPU architecture. The major components of the processor system are the CPU (Central Processing Unit), a MPU (Memory Protection Unit), a Security Attribution Unit (SAU), a Nested Vectored Interrupt Controller (NVIC), an Instruction Stream Signature (ISS) coprocessor, and a Masked Instruction Set Extension (MISE) coprocessor. The TOE can communicate using contact-based and contactless 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 smart card 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 smart card 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, 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 tests performed by the developer were divided into the following categories:

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

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

The evaluation has shown that the actual version of the TOE provides the security functionalities as specified by the developer. The test results confirm the correct implementation of the TOE security functionalities.

For penetration testing, the evaluators took all security functionalities into consideration. Intensive penetration testing was planned based on the analysis results and performed for the underlying mechanisms of security functionalities. The penetration tests considered both the physical tampering of the TOE and attacks, which do not modify the TOE physically. The penetration test results confirm that the TOE is resistant to attackers with high attack potential in the intended environment for the TOE.

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

8. Evaluated Configuration

This certificate covers the following configurations of the TOE:

The tests are performed with the chip IFX_CCI_00007Ah, produced by TSMC fab 15 in Taiwan. The identifiers IFX_CCI_00007Ah A11 / R11 / M11, IFX_CCI_00008Fh R11 / M11 may differ from each other only in terms of blocked modules: They are still physically present on the TOE, but not accessible. Thus, the tests were performed on a TOE without any blocked features. For the tests different chip types are prepared with different patches. With the loaded patch code, the defined tests could be performed. The entire functionality is the same for all chips.

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-3087-2026-02-0001, administration ID BSI-DSZ-CC-1272-2026
- was issued on: 17 February 2026
- is valid until: 16 February 2031

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

9.2. Results of cryptographic assessment

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

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

#	Purpose	Cryptographic mechanism	Implementation standard	Key size in bits	Security Level above 120 Bits
Symmetric coprocessor (SCP)					
1	Cryptographic primitive	AES	[FIPS197]	128, 192, 256	yes
2	Confidentiality	#1 in ECB mode for encryption and decryption	[NIST_SP800-38A]	128, 192, 256	no
CryptoSuite: symmetric functionality					
3	Cryptographic primitive	TDES	[NIST_SP800-67_2017]	112, 168	no
4	Cryptographic primitive	AES	[FIPS197]	128, 192, 256	yes
5	Confidentiality	#3 in ECB mode for encryption and decryption	[NIST_SP800-38A]	112, 168	no
6	Confidentiality	#3 in CBC mode for encryption and decryption	[NIST_SP800-38A]	112, 168	no
7	Confidentiality	#3 in CTR mode for encryption and decryption	[NIST_SP800-38A]	112, 168	no
8	Confidentiality	#4 in ECB mode for encryption and decryption	[NIST_SP800-38A]	128, 192, 256	no
9	Confidentiality	#4 in CBC mode for encryption and decryption	[NIST_SP800-38A]	128, 192, 256	yes
10	Confidentiality	#4 in CTR mode for encryption and decryption	[NIST_SP800-38A]	128, 192, 256	yes
11	Confidentiality	#4 in CCM mode for encryption and decryption	[NIST_SP800-38C]	128, 192, 256	yes
12	Confidentiality	#4 in GCM mode for Authenticated encryption	[NIST_SP800-38D]	128, 192, 256	yes
13	Integrity	#3 in Retail MAC mode for MAC generation	[ISO_9797-1_2011]	112	no

#	Purpose	Cryptographic mechanism	Implementation standard	Key size in bits	Security Level above 120 Bits
14	Integrity	#3 in CBC MAC mode for MAC generation	[ISO_9797-1_2011] padding method 2	112, 168	no
15	Integrity	#4 in CMAC mode for MAC generation	[NIST_SP800-38B]	128, 192, 256	yes
16	Integrity	#4 in CBC MAC mode for MAC generation	[ISO_9797-1_2011] padding method 2	128, 192, 256	no
CryptoSuite: asymmetric functionality					
17	N/A	Certified FFC domain parameters: • 1024-bit MODP Group with 160-bit Prime Order Subgroup • 2048-bit MODP Group with 224-bit Prime Order Subgroup • 2048-bit MODP Group with 256-bit Prime Order Subgroup	[RFC5114]	N/A	--
18	Key agreement	Finite-Field Diffie-Hellman computation using domain parameters listed in #17	[NIST_SP800-56A, 5.7.1.1] without step 2,	1024-2048	
19	Key generation	Finite-Field key generation for domain parameters listed in #17	[NIST_SP800-56A, 5.6.1.1]	1024-2048	
20	N/A	Certified Montgomery elliptic curves: • Curve25519, Curve448	[RFC7748]	N/A	--
21	Key agreement	X25519 using Curve25519	[RFC7748, 5]	256	--
22	Key agreement	X448 using Curve448	[RFC7748, 5]	448	--

#	Purpose	Cryptographic mechanism	Implementation standard	Key size in bits	Security Level above 120 Bits
23	Confidentiality	RSA encryption	[PKCS#1_2012, 5.1.1], [NIST_SP800-56B, 7.1.1]	1024 – 4224	yes for >= 2800 bit only
24	Confidentiality	RSA decryption	[PKCS#1_2012, 5.1.2 2a], [NIST_SP800-56B, 7.1.2.1]	1024 – 2112	no
25	Confidentiality	RSA decryption with CRT	[PKCS#1_2012, 5.1.2 2b], [NIST_SP800-56B, 7.1.2.3]	1024 – 4224	yes for >= 2800 bit only
26	Authenticity	RSA signature generation[6]	[PKCS#1_2012, 5.2.1 2a]	1024 – 2112	no
27	Authenticity	RSA signature generation with CRT[6]	[PKCS#1_2012, 5.2.1 2b]	1024 – 4224	yes for >= 2800 bit only
28	Authenticity	RSA signature verification[6]	[PKCS#1_2012, 5.2.2]	1024 – 4224	yes for >= 2800 bit only
29	Key generation	Generation of probably random primes p and q for RSA keys	[FIPS186-5, A.1.3] without step 1 Note: only conformant for prime Bitlength >= 2048; in case prime Bitlength < 2048 identical algorithm is used, but considered proprietary	1024 – 4128	--
30	Key generation	Generation of RSA's N and d parameters from p, q	[FIPS186-5, A.1.1], [PKCS#1_2012, 3.1 / 3.2(1)],	1024 – 4224	--
31	Key generation	Generation of RSA CRT parameters from p, q	[FIPS186-5, A.1.1], [PKCS#1_2012, 3.1 / 3.2(2)]	1024 – 4224	--
32	Primality testing	Miller-Rabin primality test	[FIPS186-5, B.3.1]	512 – 2064 (prime length)	--
33	Primality testing	Enhanced Miller-Rabin primality test	[FIPS186-5, B.3.2]	512 – 2064 (prime length)	--

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

#	Purpose	Cryptographic mechanism	Implementation standard	Key size in bits	Security Level above 120 Bits
34	N/A	Certified Weierstrass elliptic curves: • all NIST curves over prime fields in [NIST_SP800-186], • all Brainpool curves of [RFC5639], • secp160k1, secp160r1, secp160r2, secp256k1 of [SEC2_2010], • ANSII FRP256V1 of [ANSSI], • BN P256 of [ISO_15946-5_2022], and • W-25519, W-448 of [NIST_SP800-186].	[NIST_SP800-186], [RFC5639], [SEC2_2010], [ANSSI], [ISO_15946-5_2022]		"No" for BN P256 in [ISO_15946, 7.3] in general case, "not rated w.r.t. 120 bits" in specific cases.
35	Authenticity	ECDSA signature generation on curves listed in #34[6]	[FIPS186-5, 6.4.1]	160 – 521	key sizes >=250: yes
36	Authenticity	ECDSA signature verification on curves listed in #34[6]	[FIPS186-5, 6.4.2]	160 – 521	key sizes >=250: yes
37	Key agreement	Elliptic Curve Diffie-Hellman (ECDH) key agreement on curves listed in #34	[NIST_SP800-56A, 5.7.1.2] without cofactor multiplication	160 – 521	key sizes >=250: yes
38	N/A	PACE integrated mapping on curves listed in #34	[ICAO_11, Appendix B.2]	160 – 521	--
39	Key generation	ECDSA key generation on curves listed in #34	[FIPS186-5, A.2.1]	160 – 521	key sizes >=250: yes
40	Authenticity	ECSDSA signature generation on curves listed in #34	[ISO_14888-3_2018, 6.10.4], [TR-03111_2018, 4.2.3],	160 – 521	key sizes >=250: yes
41	Authenticity	ECSDSA signature verification on curves listed in #34	[ISO_14888-3_2018, 6.10.5], [TR-03111_2018, 4.2.3]	160 – 521	key sizes >=250: yes

#	Purpose	Cryptographic mechanism	Implementation standard	Key size in bits	Security Level above 120 Bits
42	Key generation	ECSDSA key generation on curves listed in #34	[ISO_14888-3_2018, 6.10.3]	160 – 521	key sizes >=250: yes
43	N/A	Certified Edwards curves: • Ed25519, Ed448	[NIST_SP800-186]	N/A	--
44	Authenticity	EdDSA signature generation on curves listed in #43	[FIPS186-5, 7.6]	256, 456	--
45	Authenticity	EdDSA signature verification on curves listed in #43	[FIPS186-5, 7.7]	256, 456	--
46	Authenticity	EdDSA pre-hash signature generation[6] on curves listed in #43	[FIPS186-5, 7.8.1]	256, 456	--
47	Authenticity	EdDSA pre-hash signature verification[6] on curves listed in #43	[FIPS186-5, 7.8.2]	256, 456	--
48	Key generation	Elliptic Curve key generation on curves listed in #43	[FIPS186-5, A.2.3]	256, 456	--
49	Key generation	ML-KEM key generation with random seed	[FIPS203, 6.1]	ML-KEM-512, ML-KEM-768, ML-KEM-1024	Not rated, Yes, Yes
50	Key generation	ML-KEM key generation with provided seed	[FIPS203, 6.1], Proprietary implementation	ML-KEM-512, ML-KEM-768, ML-KEM-1024	Not rated, Yes, Yes
51	Key generation	ML-DSA key generation with random seed	[FIPS204, 5.1]	ML-DSA-44, ML-DSA-65, ML-DSA-87	Not rated, Yes, Yes
52	Key generation	ML-DSA key generation with provided seed	[FIPS204, 5.1], Proprietary implementation	ML-DSA-44, ML-DSA-65, ML-DSA-87	Not rated, Yes, Yes

#	Purpose	Cryptographic mechanism	Implementation standard	Key size in bits	Security Level above 120 Bits
53	Key encapsulation	ML-KEM key encapsulation	[FIPS203, 6.2]	ML-KEM-512, ML-KEM-768, ML-KEM-1024	Not rated, Yes, Yes
54	Key decapsulation	ML-KEM key decapsulation	[FIPS203, 6.3]	ML-KEM-512, ML-KEM-768, ML-KEM-1024	Not rated, Yes, Yes
55	Authenticity	ML-DSA signature generation	[FIPS204, 5.2 / 5.4]	ML-DSA-44, ML-DSA-65, ML-DSA-87	Not rated, Yes, Yes
56	Authenticity	ML-DSA signature verification	[FIPS204, 5.3 / 5.4]	ML-DSA-44, ML-DSA-65, ML-DSA-87	Not rated, Yes, Yes
CryptoSuite: hashing functionality					
57	Hash	SHA-1	[FIPS180-4]	N/A	--
58	Hash	SHA2-256, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	[FIPS180-4]	N/A	--
59	Hash	SHA3-224, SHA3-256, SHA3-384, SHA3-512	[FIPS202, 6.1]	N/A	--
60	XOF	SHAKE-128, SHAKE-256	[FIPS202, 6.2]	N/A	--
61	HMAC	HMAC generation using SHA-1, SHA2-256, SHA2-384, SHA2-512	[FIPS180-4], [FIPS198-1]	160, 256, 384, 512	“No” is for SHA-1 mode in general for all implementations and certification procedures.
Hardware RNG					
62	RNG	Physical RNG	N/A; corresponds to PTG.2 in [KS2011]	N/A	--

#	Purpose	Cryptographic mechanism	Implementation standard	Key size in bits	Security Level above 120 Bits
CryptoSuite: RNG functionality					
63	RNG	Physical RNG	N/A; corresponds to class PTG.2 in [KS2011]	N/A	--
64	RNG	Physical RNG with cryptographic post-processing	Post-processing based on [NIST_SP800-90A] CTR_DRBG; corresponds to PTG.3 in [KS2011] and [NIST_SP800-90A]	CTR_DRBG uses AES-128 or AES-256	--
65	RNG	Deterministic RNG	CTR_DRBG as specified in [NIST_SP800-90A]; corresponds to DRG.3 in [KS2011]	CTR_DRBG uses AES-128 or AES-256	--
66	RNG	Hybrid deterministic RNG	Post-processing based on [NIST_SP800-90A] CTR_DRBG; corresponds to DRG.4 in [KS2011] and [NIST_SP800-90A]	CTR_DRBG uses AES-128 or AES-256	--
67	RNG	Physical RNG with cryptographic post-processing	Proprietary Post-processing; corresponds to PTG.3 in [KS2011]	uses AES-128	--
68	RNG	Physical RNG with cryptographic post-processing	Proprietary Post-processing; corresponds to DRG.4 in [KS2011]	uses AES-128	--
Flash Loader					
69	Cryptographic primitive	AES	[FIPS197]	128	--
70	Authenticated encryption	#69 in CCM mode	[NIST_SP800-38C]	128	--
71	Authentication	#69 in CMAC mode	[NIST_SP800-38B]	128	--
72	Key derivation	KDF in counter mode with AES CMAC as PRF	[NIST_SP800-108, 4.1], [NIST_SP800-38B, 6.2]	128	--

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:

[ANSSI] *Avis relatif aux paramètres de courbes elliptiques définis par l'Etat français*, 2011-10-16, Journal Officiel de la République Française (JORF).
[FIPS140-2] *FIPS PUB 140-2, Security Requirements for Cryptographic Modules*, 2001-05-25, National Institute of Standards and Technology (NIST).
[FIPS180-4] *FIPS PUB 180-4 Federal Information Processing Standards Publication Secure Hash Standard (SHS)*, 2015-08, 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 PUB 197, Advanced Encryption Standard (AES)*, Updated Version, 2023-05-09, National Institute of Standards and Technology (NIST).
[FIPS198-1] *FIPS PUB 198-1 Federal Information Processing Standards Publication, The Keyed-Hash Message Authentication Code (HMAC)*, 2008-07, National Institute of Standards and Technology (NIST).
[FIPS202] *FIPS PUB 202 Federal Information Processing Standards Publication, SHA-3 Standard: Permutation-Based Hash and Extendable-Out-put Functions*, 2015-08, National Institute of Standards and Technology (NIST).
[FIPS203] *FIPS PUB 203 Federal Information Processing Standards Publication, Module-Lattice-Based Key-Encapsulation Mechanism Standard*, 2024-08, National Institute of Standards and Technology (NIST).
[FIPS204] *FIPS PUB 204 Federal Information Processing Standards Publication, Module-Lattice-Based Digital Signature Standard*, 2024-08, National Institute of Standards and Technology (NIST).
[ICAO_11] ICAO Doc 9303, Machine Readable Travel Document, eighth edition, 2021, Part 11: Security Mechanisms for MRTDs.
[ISO_14888-3_2018] *ISO/IEC 14888-3, IT Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms*, 2018-11, ISO/IEC.
[ISO_15946-5_2022] *ISO/IEC 15946-5: Information security — Cryptographic techniques based on elliptic curves Part 5: Elliptic curve generation*, 2022-02, ISO/IEC.
[ISO_9797-1_2011] *Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher*, 2011-03, ISO/IEC.
[NIST_SP800-186] *NIST Special Publication 800-186 – Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters* 2023-02, National Institute of Standards and Technology (NIST).
[NIST_SP800-22] *NIST Special Publication 800-22 Revision 1a – A Statistical Test Suite for Random and Pseudorandom Number Generators for Crypto-graphic Applications*, 2010-04, National Institute of Standards and Technology (NIST).
[NIST_SP800-38A] *NIST Special Publication 800-38A – Recommendation for Block Cipher Modes of Operation – Methods and Techniques*, 2001-12, National Institute of Standards and Technology (NIST).
[NIST_SP800-38B] *NIST Special Publication 800-38B – Recommendation for Block Cipher Modes of Operation – The CMAC Mode for Authentication*, Up-dated Version, 2016-10-06, National Institute of Standards and Technology (NIST).
[NIST_SP800-38C] *NIST Special Publication 800-38C – Recommendation for Block Cipher Modes of Operation – The CCM Mode for Authentication and Confidentiality*, Errata

Updated Version, 2007-07-20, National Institute of Standards and Technology (NIST).
[NIST_SP800-38D] *NIST Special Publication 800-38D – Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*, 2007-11, National Institute of Standards and Technology (NIST).
[NIST_SP800-56A] *NIST Special Publication 800-56A – Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography*, 2018-04, National Institute of Standards and Technology (NIST).
[NIST_SP800-56B] *NIST Special Publication 800-56B Revision 2 – Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography*, 2019-03, National Institute of Standards and Technology (NIST).
[NIST_SP800-67_2017] *NIST Special Publication 800-67 – Revision 2 – Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, rev. 2, 2017-11, National Institute of Standards and Technology (NIST).
[NIST_SP800-90A] *NIST Special Publication 800-90A – Revision 1 – Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, rev. 1, 2015-06, National Institute of Standards and Technology (NIST).
[NIST_SP800-90B] *NIST Special Publication 800-90B – Recommendation for the Entropy Sources Used for Random Bit Generation*, 2018-01, National Institute of Standards and Technology (NIST).
[PKCS#1_2012] *PKCS #1: RSA Cryptography Standard*, Version 2.2, 2012-10-17, RSA Laboratories.
[RFC5114] *RFC 5114 - Additional Diffie-Hellman Groups for Use with IETF Standards*, 2008-01, The Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc5114.txt.
[RFC5639] *RFC 5639 - Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation*, 2010-03, The Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc5639.txt.
[RFC7748] *RFC 7748 - Elliptic Curves for Security*, 2016-01, The Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc7748.txt.
[SEC_2_2010] *Standards For Efficient Cryptography – SEC 2: Recommended Ellip-tic Curve Domain Parameters*, Version 2.0, 2010, Certicom Research.
[TR-02102-1_2014] *BSI - Technische Richtlinie TR-02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen*, Version 2014-01, 2014-02-10, Bundesamt für Sicherheit in der Informationstechnik.
[TR-03111_2018] *BSI - Technical Guideline BSI TR-03111 - Elliptic Curve Cryptography*, Version 2.10, 2018-06-01, Bundesamt für Sicherheit in der Informationstechnik.

10. Obligations and Notes for the Usage of the TOE

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

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

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

Some security measures are partly implemented in this certified TOE, but require additional configuration or control or measures to be implemented by a product layer on top, e.g. the IC Dedicated Support Software using the TOE. For this reason the TOE includes guidance documentation (see table 1) which contains obligations and guidelines for the developer of the product layer on top on how to securely use this certified TOE and which measures have to be implemented in order to fulfil the security requirements of the Security Target of the TOE. In the course of the evaluation of the composite product or system it must be examined if the required measures have been correctly and effectively implemented by the product layer on top. Additionally, the evaluation of the composite product or system must also consider the evaluation results as outlined in the document "ETR for composite evaluation" [ETRfCOMP].

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

The security IC embedded software developer can deliver their software either to Infineon to let them implement it in the TOE (in the NVM) or to the composite product manufacturer to let them download the software into the NVM.

- 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 may be required. (cf. OE.Secure-Delivery in [ST], 4.2])
- 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.
- The delivery procedure from the TOE manufacturer (IFX) to the composite product manufacturer is not part of this evaluation. However, for security reasons, a form of transport protection might be required depending on the order option. The applied transport protection mechanisms must be considered during the composite evaluation considering the security needs of any pre-loaded IC Embedded Software that is active during delivery.

11. Security Target

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

For the purpose of publishing, the Security Target [ST] of the 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 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
https://www.commoncriteriaportal.org

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

https://www.iso.org/standard/72889.html
as mirrored by CCRA's edition:
CEM:2022 R1, Common Methodology for Information Technology Security Evaluation
https://www.commoncriteriaportal.org

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

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

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

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

[ST] Security Target BSI-DSZ-CC-1272-2026, Rev. 1.0, 2025-10-31, Confidential Security Target "IFX_CCI_00007Ah/8Fh A11/R11/M11 with optional Crypto Suite", Infineon Technologies AG (confidential document)
Security Target lite, Rev. 1.0, 2025-10-31, Public Security Target "IFX_CCI_00007Ah/8Fh A11/R11/M11 with optional Crypto Suite", Infineon Technologies AG

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

[ETR] Evaluation Technical Report, Version 2, 2025-12-15, EVALUATION TECHNICAL REPORT SUMMARY, TÜV Informationstechnik GmbH, (confidential document)

[ETRfCOMP] „Evaluation Technical for Composite Evaluation (ETR COMP) for the IFX_CCI_00007Ah A11 / R11 / M11, IFX_CCI_00008Fh R11 / M11", Version 2, 2025-12-15, TÜV Informationstechnik GmbH, (confidential document)

[CSCV] Cryptographic Standards Compliance Verification, Version 2, 2025-10-28, TÜV Informationstechnik GmbH (confidential document)

[7] See section 9.1 for detailed list of used AIS

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-1272-2026

Evaluation results regarding development and production environment

The IT product IFX_CCI_00007Ah/8Fh A11, R11, M11 with optional Crypto Suite, (Target of Evaluation, TOE, also named as ICT product) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM) [CEM].

As a result of the TOE certification, dated 17 February 2026, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support as claimed by the ST [ST] and that are stated in chapter 1 of this report are fulfilled for the development and production sites of the TOE. Listed below are the Distribution Centres:

Site ID	Company name and address	Functions of site
Distribution Sites		
DHL Singapore	DHL Supply Chain Singapore Ptd Tampinese LogisPark 1 Greenwich Drive Singapore 533865	• Distribution
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	• Distribution
K&N Großostheim	Kühne & Nagel Stockstädter Strasse 10 63762 Großostheim Germany	• Distribution

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