Federal Office
for Information Security

Certification Report

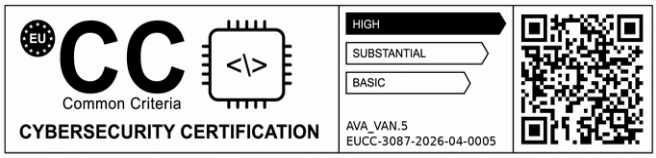
EUCC-3087-2026-04-0005
Administration ID
BSI-DSZ-CC-0827-V11-2026

for

Infineon Technologies Security Controller M9900 A22/C22/D22, M9905 A11, M9906 A11

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 Infineon Technologies Security Controller M9900 A22/C22/D22, M9905 A11, M9906 A11, has been re-certified by the certification body of the Federal Federal Office for Information Security (BSI) based on administration ID BSI-DSZ-CC-0827-V10-2025. Comprehensive results from the evaluation process were re-used.
- The evaluation of the product Infineon Technologies Security Controller M9900 A22/C22/D22, M9905 A11, M9906 A11 was carried out by TÜV Informationstechnik GmbH, located at:
  Unternehmensgruppe TÜV NORD
  Am TÜV 1
  45307 Essen.
- The evaluation was completed on 19 February 2026. TÜV Informationstechnik GmbH is a notified evaluation facility (ITSEF) .
- This certification was applied for: Infineon Technologies AG.
- The assessed TOE was developed by: Infineon Technologies AG.
- The certification activities are concluded with the comparability check and the production of this Certification Report. This work was completed by the certification body of the BSI.

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

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

For the meaning of the assurance components and assurance levels please refer to CC 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 13 April 2026 is valid until 14 April 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 Infineon Technologies Security Controller M9900 A22/C22/D22, M9905 A11, M9906 A11, 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 (TOE) is the Infineon smart card IC (Security Controller) M9900 A22/C22/D22, M9905 A11, M9906 A11 with optional Software Libraries EC, Toolbox, Base and with specific IC dedicated software.

This TOE is intended to be used in smart cards for particularly security relevant applications and for its previous use as developing platform for smart card operating systems. The TOE is the platform for the Smart card Embedded Software.

The product Infineon Technologies Security Controller M9900 A22/C22/D22, M9905 A11, M9906 A11 has been certified under the EUCC scheme in accordance to the provisions of the Implementing Regulation (EU) 2024/482. This is a re-certification based on BSI-DSZ-CC-0827-V10-2025 (BSI administration ID). Results from the evaluation process BSI-DSZ-CC-0827-V10-2025 were re-used. The TOE deliverables are listed in table 1.

The evaluation of the product Infineon Technologies Security Controller M9900 A22/C22/D22, M9905 A11, M9906 A11 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 19 February 2026. TÜV Informationstechnik GmbH is a notified evaluation facility (ITSEF).

The Evaluation Technical Report (ETR) [ETR] was provided by the ITSEF according to the Common Criteria [CC], the Methodology [CEM], the requirements of the Scheme [EUCC-VO],[EUCC_PROG].

The evaluation has confirmed:

- CC Version and Release: see [CC] and [CEM]
- PP Conformance: Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014 [PP]
- Assurance Level: EUCC High with component AVA_VAN.5
- Assurance Package: EAL 5
- Augmentation: ALC_DVS.2 and AVA_VAN.5

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 TOE can have different user available configuration. Despite these variation possibilities, all products are derived from the same hardware design results.

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:

Infineon Technologies Security Controller M9900 A22/C22/D22, M9905 A11, M9906 A11

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

The following table outlines the TOE deliverables:

No.	Type	Item / Identifier	Release / Version	Form of Delivery
1	HW	M9900 A22/C22/D22, M9905 A11, M9906 A11	A11/A22/C22/D22 (de-sign step)	Customer chooses delivery method.
2	FW	Boot Software (BOS) and the Resource Management System (RMS), Flash Loader (FL) and the NRG software.	For M9900 A22/C22/D22: 80001141 (BOS-V1), or 80001142 (BOS-V2) For M9905 A11: 80001151 (BOS-V1) For M9906 A11: 80001150 (BOS-V1)	Stored on the delivered hardware.
3	SW	NRG Management (optional)	01.03.0927	Secure download of object file via iShare.
4	SW	NRG Reader (optional)	01.02.0800	Secure download of object file via iShare.
5	SW	ACL (optional)	2.07.003 or 2.09.002	Secure download of object file via iShare.
6	DOC	32-bit Security Controller M9900 Hardware Reference Manual	3.0 / 2019-08-28	Personalized PDF via secure iShare server.
7	DOC	M9900 Security Guidelines User´s Manual	2025-06-06	Personalized PDF via secure iShare server.
8	DOC	ARMv7-M Architecture Reference Manual, ARM DDI 0403E.e	DDI 0403E.e / 2021-02-15	Personalized PDF via secure iShare server.
9	DOC	SLE97 security controllers Programmer's Reference Manual SLCx7_DFP Document release reference: Z8F80731571-A	5.9 / 2024-11-25	Personalized PDF via secure iShare server.
10	DOC	SLE97 / SLC14 Family Production and Personalization User´s Manual	2014-08-10	Personalized PDF via secure iShare server.
11	DOC	M9905 M9906 Errata Sheet	3.1 / 2019-09-05	Personalized PDF via secure iShare server.
12	DOC	M9900 Errata Sheet	4.1 / 2019-09-24	Personalized PDF via secure iShare server.
13	DOC	CL97 Asymmetric Crypto Library for Crypto@2304T RSA / ECC / Toolbox, User Interface (optional)	2.07.003 / 2024-08-26	Personalized PDF via secure iShare server.
14	DOC	ACL97-Crypto2304T-L90 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox 32-bit Security	2.09.002 / 2024-06-27	Personalized PDF via secure iShare server.

No.	Type	Item / Identifier	Release / Version	Form of Delivery
		Controller User interface manual (optional)		

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

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, 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 only includes one security objective for the IC Embedded Software Developer, the objective OE.Resp-Appl.

The objective OE.Resp-Appl states that the IC Embedded Software Developer shall treat user data (especially keys) appropriately. The IC Embedded Software Developer gets sufficient information on how to protect user data adequate in the security guidelines.

The ST only includes two security objectives for the operational environment (for the Composite Product Manufacturer), the objectives OE.Process-Sec-IC and OE.Secure_Delivery.

OE.Process-Sec-IC states that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use). This means that the phases after TOE delivery are assumed to be protected appropriately.

The Composite Product Manufacturer therefore has to be informed only about the general requirement resulting from OE.Process-Sec-IC.

OE.Secure_Delivery states that the TOE does not provide 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.

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

5. Architectural Information

The TOE provides a real 32-bit CPU-architecture and is compatible to the ARMv7-M instruction set. The major components of the core system are the 32-bit CPU (Central Processing Unit), the Cache system, the MPU (Memory Protection Unit) and MED (Memory Encryption/Decryption Unit).

The TOE consists of the hardware part, the firmware parts and the software parts. The software parts are differentiated into the asymmetric cryptographic libraries EC, Toolbox and Base, all in two different versions. The firmware of the TOE comprises the Boot Software (BOS), Resource Management System (RMS), the high-level firmware Flash Loader (FL) and the NRG 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 following State-of-the-art-documents were applied:

The tests performed by the developer were divided into the following categories:

- Simulation tests (design verification),
- Qualification / verification tests,
- Security Evaluation 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 M9905 A11 from Dresden. For the tests different samples are prepared with different patch. With the loaded patch code the defined tests could be performed.

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

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

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

The certificate

- is uniquely identified by: EUCC-3087-2026-04-0005, administration ID BSI-DSZ-CC-0827-V11-2026
- was issued on: 13 April 2026
- is valid until: xx Month 20xx (Datum der Ausstellung plus x Jahre - 1Tag)

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 of Implementation	Key Size in Bits	Security Level above 120 Bits
Key Agreement	ECDH	[X963, 5.4.1] [FIPS186-4] [RFC5639]	Key sizes corresponding to the used elliptic curves NIST: P-{224, 256, 384, 521}, K-{233, 283, 409}, B-{163, 233, 283, 409} [FIPS186-5] / [NIST SP800-186]; brainpool: P{224, 256, 320, 384, 512}t1, P{224, 256, 320, 384, 512}r1 [RFC5639]	Key sizes 160, 163, 192, 224: no Key sizes >= 256 : yes
Cryptographic Primitive	3DES in modes ECB, CBC	[NIST SP800-67] [NIST SP800-38A]	|k| = 112 , 168	no
	AES in modes ECB, CBC	[FIPS197] [NIST SP800-38A]	|k| = 128, 192, 256	CBC: yes
	ECDSA signature generation	[X962, 7.3] [FIPS186-5] [RFC5639]	Key sizes corresponding to the used elliptic curves NIST: P-{224, 256, 384, 521}, K-{233, 283, 409}, B-{233, 283, 409} [FIPS186-5] / [NIST SP800-186]; brainpool: P{224, 256, 320, 384, 512}t1, P{224, 256, 320, 384,	Key sizes 160, 163, 192, 224: no Key sizes >= 256 : yes

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits
			512}r1 [RFC5639]	
	Physical True RNG PTG.2	[AIS31]	N/A	n/a
Key Generation	ECC	[X962, A.4.3] [FIPS186-5] [RFC5639]	Key sizes corresponding to the used elliptic curves NIST: P-{224, 256, 384, 521}, K-{233, 283, 409}, B-{163, 233, 283, 409} [FIPS186-5] / [NIST SP800-186]; brainpool: P{224, 256, 320, 384, 512}t1, P{224, 256, 320, 384, 512}r1 [RFC5639]	160, 163, 192, 224: no Key sizes >= 256 : yes

Table 2: TOE cryptographic functionality

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 Composite Product Manufacturer receives all necessary recommendations and hints to develop his software in form of the delivered documentation.

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

- The 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 IC Embedded Software Developer to the Composite Product Manufacturer is not part of this evaluation and a secure delivery is required.
- It should be noted that NRG is not within the scope of evaluation of this product.

11. Security Target

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

For the purpose of publishing, the Security Target [ST] of the TOE 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 https://www.bsi.bund.de/AIS

[ST] Security Target BSI-DSZ-CC-0827-V11-2026, Rev. 7.1, 2026-01-20, Confidential Security Target "Security Target M9900/M9905/M9906 with optional ACL Software Libraries", Infineon Technologies AG (confidential document)
Security Target lite, Rev. 7.1, 2026-01-20, Public Security Target "Security Target Lite M9900/M9905/M9906 with optional ACL Software Libraries", 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, 2026-03-02, EVALUATION TECHNICAL REPORT SUMMARY, TÜV Informationstechnik GmbH, (confidential document)

[ETRfCOMP] „Evaluation Technical for Composite Evaluation (ETR COMP) for the M990x A11/A22/C22/D22“, Version 4, 2026-03-02, TÜV Informationstechnik GmbH, (confidential document)

[CSCV] Cryptographic Standards Compliance Verification, Version 1, 2025-07-07, 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-0827-V11-2026

Evaluation results regarding development and production environment

The IT product Infineon Technologies Security Controller M9900 A22/C22/D22, M9905 A11, M9906 A11, (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 13 April 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
DHL Singapore	DHL Supply Chain Singapore Ptd Tampines LogisPark 1 Greenwich Drive Singapore 533865
KWE Shanghai	KWE Kintetsu World Express (China) Co., Ltd. Shanghai Pudong Airport Pilot Free Trade Zone No. 530 Zheng Ding Road Shanghai P.R. China
K&N Großostheim	Kühne & Nagel Stockstädter Strasse 10 63762 Großostheim Germany

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