Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0827-V10-2025

for

Infineon Technologies Security Controller M9905 A11 with optional ACL v2.07.003 and v2.09.002

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 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0827-V10-2025 (*)

Infineon Technologies Security Controller M9905 A11 with optional ACL v2.07.003 and v2.09.002

from	Infineon Technologies AG
PP Conformance:	Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5
valid until:	3 November 2030

INFORMATION TECHNOLOGY SECURITY
SOGIS
IT SECURITY CERTIFIED
MUTUAL RECOGNITION AGREEMENT

SOGIS
Recognition Agreement

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), CEM:2022 extended by Scheme Interpretations, and by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents as listed in the Certification Report for conformance to the Common Criteria for IT Security Evaluation (CC). CC:2022. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 5.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2 and ALC_FLR
only

Bonn, 4 November 2025

For the Federal Office for Information Security

Fabian Hodouschek
Head of Certification

L.S.

Sandro Amendola
Director-General Directorate General S

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. 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 conducts the procedure according to the criteria laid down in the following:

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BMI Regulations on Ex-parte Costs[3]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licensing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), CC:2022 [4] [1] also published as ISO/IEC 15408

[1] Act on the Federal Office for Information Security (BSI-Gesetz – BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

[2] Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung – BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

[3] 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

- Common Methodology for IT Security Evaluation (CEM), CC:2022 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

3. Recognition Agreements

In order to avoid multiple certification 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. European Recognition of CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4. For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it 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 under SOGIS-MRA for all assurance components selected.

3.2. 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 3 EAL 2+ ALC_FLR components.

[4] Proclamation of the Bundesamtes für Sicherheit in der Informationstechnik vom 14. April 2023 auf https://www.bsi.bund.de

4. Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product Infineon Technologies Security Controller M9905 A11 with optional ACL v2.07.003 and v2.09.002, has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0827-V9-2024. Specific results from the evaluation process BSI-DSZ-CC-0827-V9-2024 were re-used.

The evaluation of the product Infineon Technologies Security Controller M9905 A11 with optional ACL v2.07.003 and v2.09.002, was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 1 October 2025. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Infineon Technologies AG.

The product was developed by: Infineon Technologies AG.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the evaluated guidance documentation are observed,
- the product is operated in the environment described, 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 Certificate issued confirms the assurance of the product claimed in the Security Target. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-assessment or re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis. Therefore the BSI reserves the right to revoke the certificate, especially if a exploitable vulnerability of the certified product gets to known.

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 4 November 2025 is valid until 3 November 2030. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security

[5] Information Technology Security Evaluation Facility

Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,

2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

6. Publication

The product Infineon Technologies Security Controller M9905 A11 with optional ACL v2.07.003 and v2.09.002, has been included in the BSI list of certified products, which is published regularly in the listing found at the BSI Website https://www.bsi.bund.de/dok/Zertifizierung-Gesamtlisten. Further information can be obtained from BSI-Infoline +49 (0)228 9582-111.

Further copies of this Certification Report can be requested from the developer[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] Infineon Technologies AG
Melli-Beese-Str. 9
86159 Augsburg

B. Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1. Executive Summary

The Target of Evaluation (TOE) is the Infineon Technologies Security Controller M9905 A11 with optional ACL v2.07.003 and v2.09.002.

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 soft-ware 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.

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 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 Security Target [5] and [8] is the basis for this certification. It is based on the certified Protection Profile Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007 [7].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [5] and [8], chapter 7. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality	Addressed issue
SF_DPM	Device Phase Management
SF_PS	Protection against Snooping
SF_PMA	Protection against Modification Attacks
SF_PLA	Protection against Logical Attacks
SF_CS	Cryptographic Support

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [5] and [8], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [5] and [8], chapter 4.1.2. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [5] and [8], chapter 4.

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

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

Infineon Technologies Security Controller M9905 A11 with optional ACL v2.07.003 and v2.09.002

The following table outlines the TOE deliverables:

No.	Type	Item / Identifier	Release / Version	Form of Delivery
1	HW	M9905 A11	A11 (design step)	Customer chooses delivery method.
2	FW	Boot Software (BOS) and the Resource Management System (RMS), Flash Loader (FL) and the NRG software.	80001151 (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	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.
13	DOC	ACL97-Crypto2304T-L90 Asymmetric Crypto Library for Crypto2304T RSA/ECC/Toolbox 32-bit Security Controller User interface manual	2.09.002 / 2024-06-27	Personalized PDF via secure iShare server.

No.	Type	Item / Identifier	Release / Version	Form of Delivery
		(optional)		

Table 2: Deliverables of the TOE

Note that the NRG software is not part of the certification scope.

The individual TOE hardware is uniquely identified by its identification data. The identification data contains the lot number, the wafer number and the coordinates of the chip on the wafer. Each individual TOE can therefore be traced unambiguously and thus assigned to the entire development and production process.

As the TOE is under control of the user software, the TOE Manufacturer can only guarantee the integrity up to the delivery procedure. It is in the responsibility of the Composite Product Manufacturer to include mechanisms in the implemented software (developed by the IC Embedded Software Developer) which allows detection of modifications after the delivery.

In detail, regarding identification:

The TOE can be delivered in various configurations, achieved by means of blocking and depending on the customer order.

All product derivatives of this TOE, including all configuration possibilities differentiated by the Generic Chip Identification Mode (GCIM) data and the configuration information output, are manufactured by Infineon Technologies AG. However, the Smartcard Embedded Software respectively user software is *not* part of the TOE.

New configurations can occur at any time depending on the user blocking or by different configurations applied by the manufacturer. In any case the user is able to clearly identify the TOE hardware, its configuration and proof the validity of the certificate independently, meaning without involving the manufacturer. The various blocking options, as well as the means used for the blocking, are done during the manufacturing process or at user premises. Entirely all means of blocking and the firmware respectively software parts involved in the blocking used at Infineon Technologies AG and/or the user premises, are subject of the evaluation. All resulting configurations of a TOE derivative are subject of the certificate. All resulting configurations are either at the predefined limits or within the predefined configuration ranges. For more information about blocking, see chapter 8 below.

The hardware part of the TOE is identified by M9905 A11. Another characteristic of the TOE is the chip identification data. The chip identification data is accessible via the Generic Chip Identification Mode (GCIM).

The Generic Chip Identification Mode (GCIM) can be activated on the ISO/IEC 7816-3 interfaces after power-on with a dedicated signalling sequence and is also accessible by the user software. This GCIM outputs amongst other identifiers for the platform, chip mode, ROM code, chip type, design step, fabrication facility, wafer, die position, firmware identifier, temperature range, and frequency.

For further, detailed information regarding TOE identification see [5] and [8], p.7f (remark 1).

In detail, regarding delivery:

“TOE Delivery” is uniquely used to indicate

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

Therefore three different delivering procedures have to be taken into consideration:

- Delivery of the IC dedicated software components (IC dedicated SW, guidance) from the TOE manufacturer to the IC embedded software developer.
- Delivery of the IC embedded software (ROM / Flash data, initialisation and pre-personalization data, Bundle Business package) from the IC embedded software developer to the TOE manufacturer.
- Delivery of the final TOE from the TOE manufacturer to the composite product manufacturer. After phase 3 the TOE is delivered in form of wafers or sawn wafers, after phase 4 in form of modules (with or without inlay antenna).

The TOE is delivered via the logistics sites:

- DHL Singapore,
- KWE Shanghai,
- K&N Großostheim.

3. Security Policy

The security policy enforced is defined by the selected set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

The Security Policy of the TOE is to provide basic security functionalities to be used by the smart card operating system and the smart card application, thus providing an overall smart card system security. Therefore, the TOE will implement a symmetric cryptographic block cipher 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.

The EC library is used to provide a high-level interface to Elliptic Curve cryptography implemented on the hardware component Crypto@2304T and includes countermeasures against SPA, DPA and DFA attacks.

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 two security objective for the IC Embedded Software Developer, the objectives OE.Plat-Appl and OE.Resp-Appl.

5. Architectural Information

The TOE is a SmartCard (Security IC). Detailed information on the TOE hardware architecture is to be found in [5] and [8] section 2.1.

6. Documentation

The evaluated documentation as outlined in table 2 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.

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

The developer performed five categories of tests:

- Simulation Tests (Design Verification),
- Qualification Tests / Software Verification,
- 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 evaluators were able to repeat the tests of the developer either using the library of programs, tools and prepared chip samples delivered to the evaluator or at the developer’s site. They performed independent tests to supplement, augment and to verify the tests performed by the developer. For the developer tests repeated by the evaluators other test parameters were used and the test equipment was varied. Security features of the TOE realised by specific design and layout measures were checked by the evaluators during layout inspections both in design data and on the final product.

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

For penetration testing the evaluators took all security functionalities into consideration. Intensive penetration testing was planned based on the analysis results and performed forthe 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 tests results confirm that the TOE is resistant to attackers with high attack potential in the intended environment for the TOE.

8. Evaluated Configuration

The M9905 A11 is produced at IFX Dresden.

The TOE hardware offers different configuration options, which a customer can choose. The mechanism to choose a configuration can be done by the following methods:

- by product selection or dialog-based in Tools,
- via Bill-per-Use (BpU) and Flash Loader (FL),

The degree of freedom for configuring the TOE is predefined by Infineon Technologies AG. The list of TOE configurations is given in the confidential ST.

Beside fix TOE configurations, which can be ordered as usual, this TOE implements optionally the so called Bill-Per-Use (BPU) ability. This solution enables the customer to tailor the product on his own to the required configuration by blocking parts of the chip on demand into the final configuration at his own premises, without further delivery or involving support by Infineon Technology AG. Customers, who are intended to use this feature receiving the TOE in a predefined configuration including the Flash Loader software, enhanced with the BPU blocking software. The blocking information is part of a chip configuration area and can be modified by customers using specific APDUs. Once a final blocking is done, further modifications are disabled.

The BPU software part is only present on the products which have been ordered with the BPU option. In all other cases this software is not present on the product.

The hardware of this TOE can be delivered with the following configuration options:

- both crypto co-processors accessible
- with a blocked Crypto2304T

In the case the Crypto2304T is blocked, no EC computation supported by hardware is possible. No accessibility of the deselected cryptographic co-processors is without impact on any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use the cryptographic co-processors.

The TOE can be delivered with the following optional libraries

- ECC
- Asymmetric Base library for ECC

In case of deselecting one or several of these libraries the TOE does not provide the respective functionality.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [6] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used for those components up to EAL 5 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product [4] (AIS 34).

For RNG assessment the scheme interpretations AIS 20/31 was used (see [4]).

To support composite evaluations according to AIS 36 the document ETR for composite evaluation [9] 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 of it.

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 following assurance components:

- All components of the EAL 5 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_DVS.2 and AVA_VAN.5 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0827-V9-2024, re-use of specific evaluation tasks was possible.

The focus of this re-evaluation was on change to the new CC-version 2022, user guidance updates and scope reduction. More precisely:

- *The re-evaluation is done according to CC:2022 instead of CC v3.1.*
- *For the M9905 A11 there are no changes to the hardware of the TOE. The derivates M9900 A22/C22/D22/G11 and M9906 A11 were removed from the certification scope.*

The following changes to the software and firmware are described:

- *The asymmetric library (ACL) in version 2.09.002 is added,*
- *All PSL, SCL and HCL library versions are removed,*
- *The ACL in version 2.05.005 is removed,*
- *The Flash Transition Layer is removed,*
- *The Security claims for RSA are removed for both ACL,*
- *The Security claims for ECDSA Verify are removed for both ACL.*

There are changes to guidance documents.

The evaluation has confirmed:

● PP Conformance:	Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007 [7]
● for the Functionality:	PP conformant Common Criteria Part 2 extended
● for the Assurance:	Common Criteria Part 3 conformant EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5

For specific evaluation results regarding the development and production environment see annex B in part D of this report.

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

9.2. Results of cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, 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-{192, 224, 256, 384, 521}, K-{163, 233, 283, 409}, B-{163, 233, 283, 409} [FIPS186-4]; brainpool: P{160, 192, 224, 256, 320, 384, 512}t1, P{160, 192, 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] [FIPS186-4] [RFC5639]	Key sizes corresponding to the used elliptic curves NIST: P-{192, 224, 256, 384, 521}, K-{163, 233, 283, 409}, B-{233, 283, 409} [FIPS186-4]; brainpool: P{160, 192, 224, 256, 320, 384, 512}t1, P{160, 192, 224, 256, 320	Key sizes 160, 163, 192, 224: no Key sizes >= 256 : yes
	Physical True RNG PTG.2	[AIS31]	N/A	n/a
Key	ECC	[X962, A.4.3]	Key sizes	Key sizes

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits
Generation		[FIPS186-4] [RFC5639]	corresponding to the used elliptic curves NIST: P-{192, 224, 256, 384, 521}, K-{163, 233, 283, 409}, B-{233, 283, 409} [FIPS186-4]; brainpool: P{160, 192, 224, 256, 320, 384, 512}t1, P{160, 192, 224, 256, 320	160, 163, 192, 224: no Key sizes >= 256 : yes

Table 3: TOE cryptographic functionality

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process, too.

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 [Auswahl im Einzelfall: IC Dedicated Support Software and/or Embedded Software] using the TOE. For this reason the TOE includes guidance documentation (see table 2) which contains obligations and guidelines for the developer of the product layer on top on how to securely use this certified TOE and which measures have to be implemented in order to fulfil the security requirements of the Security Target of the TOE. In the course of the evaluation of the composite product or system it must be examined if the required measures have been correctly and effectively implemented by the product layer on top. Additionally, the evaluation of the composite product or system must also consider the evaluation results as outlined in the document "ETR for composite evaluation" [9].

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 (listed in Table 2) have to be considered.
- The Composite Product Manufacturer receives all necessary recommendations and hints to develop his software in form of the delivered documentation.

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.

11. Security Target

For the purpose of publishing, the Security Target [8] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target [5] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

12. Regulation specific aspects (eIDAS, QES)

None.

13. Definitions

13.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
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
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

13.2. Glossary

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

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.

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.

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.

14. Bibliography

[1] Common Criteria for Information Technology Security Evaluation/CC
ISO-Version:
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
CCRA-Version:
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 requirement

https://www.commoncriteriaportal.org

[2] Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology
ISO-Version:
ISO 18045:2022: Information technology Security techniques Methodology for IT security evaluation
https://www.iso.org/standard/72889.html
CCRA-Version:
CEM:2022 R1, Common Methodology for Information Technology Security Evaluation
https://www.commoncriteriaportal.

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licensing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

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

[5] Confidential Security Target BSI-DSZ-CC-0827-V10-2025, Version 6.2, 2025-07-18, “Security Target M9905 with optional ACL Software Libraries”, Infineon (*confidential document*)

[6] Evaluation Technical Report, BSI-DSZ-CC-0827-V10-2025, Version 3, 2025-09-26, “EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY)”, TÜV Informationstechnik GmbH, *(confidential document)*

[7] Security IC Platform Protection Profile, Version 1.0, 15 June 2007, BSI-CC-PP-0035-2007

[8] Security Target Lite for BSI-DSZ-CC-0827-V10-2025, Version 6.2, 2025-07-18, “Security Target Lite M9905 with optional ACL Software Libraries”, Infineon (sanitised public document)

[9] Evaluation Technical Report for Composite Evaluation for the M9905 A11, Version 3, 2025-09-26, “EVALUATION TECHNICAL REPORT FOR COMPOSITE EVALUATION (ETR COMP)”, TÜV Informationstechnik GmbH (confidential document)

[10] Configuration list for the TOE, Version 1.6, 2025-06-23, “Configuration Management Scope M9905 including optional Software Libraries EC”, Infineon (confidential document)

[11] “Site Technical Audit Report (STAR) Infineon Technologies IT Services GmbH, Klagenfurt”, version 2, 2025-09-26, TÜV Informationstechnik GmbH (confidential document)

[12] “Site Technical Audit Report (STAR) DNP Photomask Europe S.p.A., Agrate, Italy”, version 1, 2025-05-30, TÜV Informationstechnik GmbH (confidential document)

[13] “Impact Analysis for Common Criteria with Evaluation Assurance Level EAL5 augmented (EAL5+) M990X Including optional Software Libraries – EC”, Version 2.2, 2025-10-21, Infineon (confidential document)

C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria in its CCRA Documents can be followed:

- On conformance claim definitions and descriptions refer to CC:2022 part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC:2022 Part 3 chapter 6.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CCRA CC:2022 Part 5.
- On the assurance class ASE for Security Target evaluation refer to CC:2022 Part 3 chapter 9
- On the detailed definitions of the assurance components for the TOE evaluation refer to CC:2022 Part 3 chapters 7 to 15
- The table 1 in CC:2022 part 5, Chapter 4.2 summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published as the CCRA Version at
https://www.commoncriteriaportal.org/cc/index.cfm

The CC are published as the ISO/IEC Version at
https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

D. 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-V10-2025

Evaluation results regarding development and production environment

The IT product Infineon Technologies Security Controller M9905 A11 with optional ACL v2.07.003 and v2.09.002, (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), CEM:2022 extended by Scheme Interpretations and by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents for conformance to the Common Criteria for IT Security Evaluation (CC), CC:2022.

As a result of the TOE certification, dated 4 November 2025, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.2)

are fulfilled for the development and production sites of the TOE.

For the sites, the requirements have been specifically applied in accordance with the Security Target [5] and [8]. 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 [5] and [8]) are fulfilled by the procedures of these sites.

Note: End of report