Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1179-V5-2025

for

Infineon Technologies AG OPTIGA™ Trusted Platform Module SLB9672_2.0 v17 and SLB9673_2.0 v27 v17.10.16488.00, v17.12.16858.00, v17.13.17733.00, v27.10.16688.00, and v27.13.17770.00

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-1179-V5-2025 (*)

Trusted Platform Module

Infineon Technologies AG OPTIGA™ Trusted Platform Module SLB9672_2.0 v17 and SLB9673_2.0 v27 v17.10.16488.00, v17.12.16858.00, v17.13.17733.00, v27.10.16688.00, and v27.13.17770.00

SOGIS
Recognition Agreement

from	Infineon Technologies AG
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.1 and AVA_VAN.4
valid until:	26 July 2028

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), Version 3.1 extended by Scheme Interpretations and CC Supporting Documents as listed in the Certification Report for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. 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, 26 August 2025

For the Federal Office for Information Security

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

Fabian Hoduschek L.S.
Head of Section

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87 - D-53175 Bonn - 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

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), Version 3.1 [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), Version 3.1 [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 and ALC_FLR components.

[4] Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

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 AG OPTIGA™ Trusted Platform Module SLB9672_2.0 v17 and SLB9673_2.0 v27 v17.10.16488.00, v17.12.16858.00, v17.13.17733.00, v27.10.16688.00, and v27.13.17770.00, has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1179-V4-2023. Specific results from the evaluation process BSI-DSZ-CC-1179-V4-2023 were re-used.

The evaluation of the product Infineon Technologies AG OPTIGA™ Trusted Platform Module SLB9672_2.0 v17 and SLB9673_2.0 v27 v17.10.16488.00, v17.12.16858.00, v17.13.17733.00, v27.10.16688.00, and v27.13.17770.00, was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 22 August 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 following report, 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 26 August 2025 is valid until 26 July 2028. Validity can be re-newed by re-certification.

[5] Information Technology Security Evaluation Facility

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 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 AG OPTIGA™ Trusted Platform Module SLB9672_2.0 v17 and SLB9673_2.0 v27 v17.10.16488.00, v17.12.16858.00, v17.13.17733.00, v27.10.16688.00, and v27.13.17770.00, 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 Trusted Platform Module SLB9672_2.0 v17 and Trusted Platform Module SLB9673_2.0 v27 (or SLB9672_2.0 v17 and SLB9673_2.0 v27 in short), version v17.10.16488.00, v17.12.16858.00, v17.13.17733.00, v27.10.16688.00, and v27.13.17770.00, including related guidance documentation as described in the Security Target [6].

The OPTIGA™ Trusted Platform Module SLB9672_2.0 v17 and SLB9673_2.0 v27, called TOE or SLB9672_2.0 v17 and SLB9673_2.0 v27 in the following text, is an integrated circuit and software platform that gives users the possibility to update the product OPTIGA™ Trusted Platform Module SLB9672_2.0 v17 and SLB9673_2.0 v27 v17.10.16488.00, v17.12.16858.00, v17.13.17733.00, v27.10.16688.00, and v27.13.17770.00 to a new product version.

The security functionality of the TOE is reduced to the FieldUpgrade process. The SLB9672_2.0 uses the Serial Peripheral Interface (SPI) and the SLB9673_2.0 uses the Inter Integrated Circuit Interface (I2C) for the integration into existing PC mainboards.

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

TOE Security Functionality	Addressed issue
SF_CRY	Cryptographic Support
SF_G&T	General and Test
SF_OBH	Object Hierarchy

Table 1: TOE Security Functionalities

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

Infineon Technologies AG OPTIGA™ Trusted Platform Module SLB9672_2.0 v17 and SLB9673_2.0 v27 v17.10.16488.00, v17.12.16858.00, v17.13.17733.00, v27.10.16688.00, and v27.13.17770.00

The following table outlines the TOE deliverables:

No.	Type	Item / Identifier	Release / Version	Form of Delivery
1.	HW/SW	OPTIGA™ Trusted Platform Module SLB9672_2.0 v17 and SLB9673_2.0 v27	v17.10.16488.00, v17.12.16858.00, v17.13.17733.00, v27.10.16688.00, and v27.13.17770.00	Packaged module
2.	DOC	*OPTIGA™ TPM SLB 9672 FW17.10 Databook*	Revision 1.1, 2021-07-23	PDF-file
		OPTIGA™ TPM, SLB9672 FW17.12, Databook	Revision 1.2, 2022-03-09	PDF-file
		OPTIGA™ TPM, SLB9672 FW17.13, Databook	Revision 1.3, 2023-04-19	PDF-file
		OPTIGA™ TPM, SLB9673 FW27.10,	Revision 1.2,	PDF-file

No.	Type	Item / Identifier	Release / Version	Form of Delivery
		Databook	2022-03-09	
		OPTIGA™ TPM, SLB9673 FW27.13, Databook	Revision 1.3, 2023-04-19	PDF-file
3.	DOC	*OPTIGA™ TPM2.0, TPM 2.0 implementations according to TCG TPM Library Specification Rev. 01.59, Application Note, User Guidance*	Revision 1.04, 2021-10-06	PDF-file
4.	DOC	*OPTIGA™ TPM, SLB 9672 TPM2.0 FW17.xx, Errata and Updates*	Revision 1.4, 2023-04-21	PDF-file
		OPTIGA™ TPM, SLB 9673 TPM2.0 FW27.xx, Errata and Updates	Revision 1.2, 2023-04-21	PDF-file
5.	DOC	*Trusted Platform Module Library, Part 1: Architecture, Family "2.0" Level 00 Revision 01.59*	Revision 01.59, 2019-11-08	Public document, downloadable from https://www.trustedcomputinggroup.org
6.	DOC	*Trusted Platform Module Library, Part 2: Structures, Family "2.0" Level 00 Revision 01.59*	Revision 01.59, 2019-11-08	Public document, downloadable from https://www.trustedcomputinggroup.org
7.	DOC	*Trusted Platform Module Library, Part 3: Commands, Family "2.0" Level 00 Revision 01.59*	Revision 01.59, 2019-11-08	Public document, downloadable from https://www.trustedcomputinggroup.org
8.	DOC	*Trusted Platform Module Library, Part 4: Supporting Routines, Family "2.0" Level 00 Revision 01.59*	Revision 01.59, 2019-11-08	Public document, downloadable from https://www.trustedcomputinggroup.org
9.	DOC	*TCG PC Client Platform TPM Profile Specification for TPM 2.0*	Version 1.05, Revision 14, 2020-09-04	Public document, downloadable from https://www.trustedcomputinggroup.org
10.	DOC	*Errata for TCG Trusted Platform Module Library, Family "2.0" Level 00 Revision 1.59*	Version 1.1, 2020-06-18	Public document, downloadable from https://www.trustedcomputinggroup.org

Table 2: Deliverables of the TOE

TOE Identification

The TOE hardware and firmware is identified by name and version number as listed in the following table:

Type	Name	Version number
Security IC with integrated firmware	OPTIGA™ Trusted Platform Module SLB9672_2.0 v17 and SLB9673_2.0 v27	v17.10.16488.00, v17.12.16858.00, v17.13.17733.00, v27.10.16688.00, and v27.13.17770.00

Table 3: Identifiers of the TOE

The fabricated modules are physically labelled with the TOE reference by printing. The labelling consists of four lines:

Line	Label	Remark
0	Infineon	Logo and name of producer
1	SLB9672	–
2	AU20 yy	The <yy> is an internal FW indication (only at manufacturing due to field upgrade option)
3	<Lot number> H <datecode>	–

Line	Label	Remark
0	Infineon	Logo and name of producer
1	SLB9673	–
2	AU20 yy	The <yy> is an internal FW indication (only at manufacturing due to field upgrade option)
3	<Lot number> H <datecode>	–

Tables 4: Labelling of TOE modules

The version information of the TOE can be read out electronically with the command TPM2_GetCapability. The vendor specific return values for the TOE are defined as listed in the following tables:

Property	Vendor specific value
TPM_PT_MANUFACTURER	“IFX”
TPM_PT_VENDOR_STRING_1	“SLB9”
TPM_PT_VENDOR_STRING_2	“672”
TPM_PT_VENDOR_STRING_3	NULL
TPM_PT_VENDOR_STRING_4	NULL
TPM_PT_FIRMWARE_VERSION_1	Major and minor version, e.g. 0x0011000A indicates v17.10, 0x0011000C indicates v17.12, 0x0011000D indicates v17.13
TPM_PT_FIRMWARE_VERSION_2	Build number and Common Criteria certification state (for instance, 0x00406800 or 0x00406802) Byte 1: reserved for future use (0x00) Byte 2 and 3: Build number (for instance, 0x4068) Byte 4: Common Criteria certification state/mode: 0x00 = TPM operational mode/TPM is CC certified, 0x02 = TPM operational mode/TPM is not certified, 0x60 = Manually entered TPM firmware recovery mode (triggered externally for testing purposes) 0x61 = TPM firmware recovery mode (triggered by code integrity failure detection) 0x62 = TPM firmware update mode
TPM_PT_MODES	Bit 0 (FIPS_140_2) = 1 Bits 1...31 = 0

Property	Vendor specific value
TPM_PT_MANUFACTURER	“IFX”

Property	Vendor specific value
TPM_PT_VENDOR_STRING_1	“SLB9”
TPM_PT_VENDOR_STRING_2	“673”
TPM_PT_VENDOR_STRING_3	NULL
TPM_PT_VENDOR_STRING_4	NULL
TPM_PT_FIRMWARE_VERSION_1	Major and minor version, e.g. 0x001B000A indicates v27.10, 0x001B000D indicates v27.13
TPM_PT_FIRMWARE_VERSION_2	Build number and Common Criteria certification state (for instance, 0x00413000 or 0x00413002) Byte 1: reserved for future use (0x00) Byte 2 and 3: Build number (for instance, 0x4130) Byte 4: Common Criteria certification state/mode: 0x00 = TPM operational mode/TPM is CC certified, 0x02 = TPM operational mode/TPM is not certified, 0x60 = Manually entered TPM firmware recovery mode (triggered externally for testing purposes) 0x61 = TPM firmware recovery mode (triggered by code integrity failure detection) 0x62 = TPM firmware update mode
TPM_PT_MODES	Bit 0 (FIPS_140_2) = 1 Bits 1...31 = 0

Tables 5: Vendor specific properties of TPM2_GetCapability

TOE Delivery

As the TOE is a security IC product it can be delivered only in form complete mounted IC`s. Only TOEs, which have undergone and passed all the production tests are delivered in the state user mode.

The production of the TOE wafers will be performed at TSMC Tainan (Fab14A), Taiwan (see [6], 2.2.5).

The delivery of the TOE documentation from Infineon Technologies (the TOE Manufacturer) to the Platform manufacturer is an external delivery process and done from the site IFX Munich.

The TOE is delivered via the logistics sites: DHL Singapore, KWE Shanghai, and K&N Großostheim.

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.

The delivery documentation describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the user’s site including the necessary intermediate delivery procedures.

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:

- Cryptographic Support: destruction of cryptographic keys, the generation of SHA256 and SHA512 hash values, AES256 encryption and decryption in CTR mode, key derivation using AES CTR and CMAC mode, key unwrapping in KWP_AD, and ECDSA signature verification with curve TPM_ECC_NIST_P521.
- General and Test: provision and enforcement of the TPM role model, startup- and self tests, preservation of secure state in case of failures or shutdown, and resistance to physical manipulation or probing.
- Object Hierarchy: state control on all subjects, objects and operations.

Specific details concerning the above-mentioned security policies can be found in chapter 8 of the Security Target [6].

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 Security Objectives for the Operational Environment are given in [6], 5.2:

- OE.FieldUpgradeInfo: The developer via AGD documentation will instruct the admin doing the upgrade how to do the upgrade and that the admin should inform the end user regarding the Field Upgrade process, its result, whether the installed firmware is certified or not, and the version of the certified TPM.

5. Architectural Information

The SLB9672_2.0 v17 and SLB9673_2.0 v27 consist of **hardware** and **firmware** components.

The **hardware** of the TOE consists of the following parts: Security Peripherals (filters, sensors), Core System, Memories, Coprocessors, Random number generator (RNG), Checksum module (CRC), Interrupt module (INT), Timer (TIM), Buses (BUS), Serial Peripheral Interface (SPI), GPIO interface and the Tick Counter.

The **firmware** of the TOE includes an operating system that provides the functionality specified by the Trusted Platform Module Library specification. The chip initialisation routine with security checks and identification mode as well as test routines for production testing are located in a separate test ROM. The firmware also provides the mechanism for updating the protected capabilities once the TOE is in the field as defined in the Field Upgrade procedure.

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

7.1. Developer's Test according to ATE_FUN

The tests performed by the **developer** according to ATE_FUN were divided into six categories: Simulation Tests (design verification), Qualification Tests, Verification Tests, Security Evaluation Tests, Production Tests, and Software Tests.

The evaluator has checked the simulation tests, qualification tests, and security evaluation tests of the developer by sampling. The evaluator’s sample of developer tests performed covers all portions of the TSF (security features) and related interfaces.

Overall the TSF have been tested against the functional specification, the TOE design and the security architecture description. The tests demonstrate that the TSF performs as specified.

7.2. Evaluator Tests – Independent Testing according to ATE_IND

The **evaluator’s** testing effort according to ATE_IND is described as follows, outlining the testing approach, configuration, depth and results.

The evaluator's objective regarding this aspect was to test the functionality of the TOE as described in [6], and to verify the developer's test results by repeating developer's tests and additionally add independent tests. In the course of the evaluation of the TOE the following classes of tests were carried out: Module tests, Simulation tests, Emulation tests, Tests in user mode, Tests in test mode, Hardware tests, and Software tests. With this kind of tests the entire security functionality of the TOE was tested.

Penetration Testing according to AVA_VAN:
The penetration testing was partially performed using the developer’s testing environment, partially using the test environment of the evaluation body. All configurations of the TOE being intended to be covered by the current evaluation were tested. The overall test result is that no deviations were found between the expected and the actual test results; moreover, no attack scenario with the attack potential **Moderate** was actually successful.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

OPTIGA™ Trusted Platform Module SLB9672_2.0 v17 and SLB9673_2.0 v27 in version v17.10.16488.00, v17.12.16858.00, v17.13.17733.00, v27.10.16688.00, and v27.13.17770.00 as described in the ST [6] and Databook [10].

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [7] 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 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the technology was used:

(i) The Application of Common Criteria to Integrated Circuits.

(ii) For RNG assessment the scheme interpretations AIS 20 and AIS 31 were used (see [4]).

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_FLR.1 and AVA_VAN.4 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-1179-V4-2023, re-use of specific evaluation tasks was possible.

The current evaluation is a re-evaluation with scope reduction of a TOE previously certified under the certification ID BSI-DSZ-CC-1179-V4-2023.

Recently acquired new knowledge requires reducing the scope of security functionality of the TOE. Therefore, the current evaluation is a re-evaluation with scope reduction of OPTIGA™ Trusted Platform Module SLB9672_2.0 v17 and SLB9673_2.0 v27 v17.10.16488.00, v17.12.16858.00, v17.13.17733.00, v27.10.16688.00, and v27.13.17770.00. *The evaluation scope was reduced by removing the conformance claim to the Protection Profile PC Client Specific TPM, TPM Library Specification Family "2.0" Level 0 Revision 1.59 [PP] and reducing the TSF to the Field Upgrade functionality only. By performing a firmware update to FW 17.24/27.24 the CC Certificate with Cert ID BSI-DSZ-CC-1246 immediately becomes active.* Therefore, compared to the previously certified product, the developer uses a reduced security problem definition, reduced security objectives for the TOE and operational environment, and reduced security functional requirements. Compared to the previously certificated product, the user guidance was not updated.

The TOE hardware, firmware and software are identical compared to BSI-DSZ-CC-1179-V4-2023.

- PP Conformance: None
- for the Functionality: Product specific Security Target
Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
EAL 4 augmented by ALC_FLR.1 and AVA_VAN.4

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).

The table 7 in annex C of part D of this report gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy.

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.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

11. Security Target

For the purpose of publishing, the Security Target [6] 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.

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
cPP	Collaborative Protection Profile
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
TPM	Trusted Platform Module
TSF	TOE Security Functionality

13.2. 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.

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.

14. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017,
https://www.commoncriteriaportal.org

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

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

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website, https://www.bsi.bund.de/zertifizierungsreporte

[6] Security Target BSI-DSZ-CC-1179-V5-2025, Version 3.5, Aug. 21, 2025, “Security Target OPTIGA™ Trusted Platform Module SLB9672_2.0 v17 SLB9673_2.0 v27”, Infineon Technologies AG (public document)

[7] Evaluation Technical Report, Version 3, Aug. 21, 2025, ”Evaluation Technical Report Summary”, TÜV Informationstechnik GmbH, (confidential document)

[8] None

[9] “Eckpunkte der Bundesregierung zu Trusted Computing”, by the German Federal Government, April 2017

[10] OPTIGA™ TPM, SLB9672 FW17.10, Databook, Revision 1.1, 2021-07-23

OPTIGA™ TPM, SLB9673 FW27.10, Databook, Revision 1.2, 2022-03-09

OPTIGA™ TPM, SLB9672 FW17.12, Databook, Revision 1.2, 2022-03-09

OPTIGA™ TPM, SLB9672 FW17.13, Databook, Revision 1.3, 2023-04-19

OPTIGA™ TPM, SLB9673 FW27.13, Databook, Revision 1.3, 2023-04-19

[11] OPTIGA™ TPM, SLB 9672 TPM2.0 FW17.xx, Errata and Updates, Revision 1.4, 2023-04-21

OPTIGA™ TPM, SLB 9673 TPM2.0 FW27.xx, Errata and Updates, Revision 1.2, 2023-04-21

[12] OPTIGA™ TPM2.0, TPM 2.0 implementations according to TCG TPM Library Specification Rev. 01.59, Application Note, User Guidance 1.04 2021-10-06, Infineon Technologies AG (confidential developer document)

[7] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 9, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 10, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 35, Version 2, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 5, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2, Reuse of evaluation results

[13] Trusted Platform Module Library Part 1: Architecture, Family “2.0”, Level 00 Revision 01.59, 2019-11-08, Trusted Computing Group (TCG)

[14] Trusted Platform Module Library Part 2: Structures, Family “2.0”, Level 00 Revision 01.59, 2019-11-08, Trusted Computing Group (TCG)

[15] Trusted Platform Module Library Part 3: Commands, Family “2.0”, Level 00 Revision 01.59, 2019-11-08, Trusted Computing Group (TCG)

[16] Trusted Platform Module Library Part 4: Supporting Routines, Family “2.0”, Level 00 Revision 01.59, 2019-11-08, Trusted Computing Group (TCG)

C. Excerpts from the Criteria

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

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12
- On the detailed definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17
- The table in CC part 3, Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published at https://www.commoncriteriaportal.org/cc/

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 C: Overview and rating of cryptographic functionalities implemented in the TOE

Annex B of Certification Report BSI-DSZ-CC-1179-V5-2025

Evaluation results regarding development and production environment

The IT product Infineon Technologies AG OPTIGA™ Trusted Platform Module SLB9672_2.0 v17 and SLB9673_2.0 v27 v17.10.16488.00, v17.12.16858.00, v17.13.17733.00, v27.10.16688.00, and v27.13.17770.00, (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations and CC Supporting Documents for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 26 August 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.4, ALC_DEL.1, ALC_DVS.1, ALC_FLR.1, ALC_LCD.1, ALC_TAT.1) are fulfilled for the development and production sites.

Besides the production and development sites, the relevant TOE distribution centers are as listed below:

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

Table 6: List of relevant TOE distribution sites

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]. 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 [6]) are fulfilled by the procedures of these sites.

Annex C of Certification Report BSI-DSZ-CC-1179-V5-2025

Overview and rating of cryptographic functionalities implemented in the TOE

No.	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments
1.	EC signature verification ECDSA	[FIPS186-4]	|k| = 521 ECC_NIST_P 521	TPM-FieldUpgrade
	SHA-512	[FIPS180-4]		
2.	Integrity XMSS with XMSS-SHA2_10_256	[N8208]	None	TPM-FieldUpgrade
3.	Key Agreement	[N808]		TPM-FieldUpgrade
	AES	[ISO_18033-3]	|k| = 256	
	CTR	[ISO_10116]		
	CMAC	[ISO_9797-1]		
4.	Integrity			TPM-FieldUpgrade
	SHA-256	[FIPS180-4]	None	
	SHA-512	[FIPS180-4]	None	
5.	Decryption			TPM-FieldUpgrade
	AES	[ISO_18033-3]	|k| = 256	
	CTR	[ISO_10116]		
6.	Key Unwrapping			TPM-FieldUpgrade
	AES	[ISO_18033-3]	|k| = 256	
	KWP-AD	[N383F]		

Table 7: TOE cryptographic functionality

Note: End of report