Federal Office
for Information Security

# Certification Report

# BSI-DSZ-CC-1178-V3-2022

for

# Infineon Technologies AG OPTIGA™ Trusted Platform Module SLB9672_2.0 v16 and SLB9673_2.0 v26, version v16.10.16488.00, v16.12.16858.00 and v26.10.16688.00

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-1178-V3-2022** (*)

Trusted Platform Module

**Infineon Technologies AG OPTIGA™ Trusted Platform Module SLB9672_2.0 v16 and SLB9673_2.0 v26, version v16.10.16488.00, v16.12.16858.00 and v26.10.16688.00**

| | |
|---|---|
| from | Infineon Technologies AG |
| PP Conformance: | Protection Profile PC Client Specific TPM, TPM Library specification Family “2.0”, Level 0 Revision 1.59, Version: 1.3, Date: 2021-09-29, ANSSI-CC-PP-2021/02 |
| Functionality: | PP conformant<br>Common Criteria Part 2 extended |
| Assurance: | Common Criteria Part 3 conformant<br>EAL 4 augmented by ALC_FLR.1 and AVA_VAN.4 |

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), 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, 29 April 2022

For the Federal Office for Information Security

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

Sandro Amendola L.S.
Head of Division

**Bundesamt für Sicherheit in der Informationstechnik**
Godesberger Allee 185-189 - 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 licencing process (CC-Stellen) [3]

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 Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408.
- 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.

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

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. 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 v16 and SLB9673_2.0 v26, version v16.10.16488.00, v16.12.16858.00 and v26.10.16688.00, has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1178-V2-2022. Specific results from the evaluation process BSI-DSZ-CC-1178-V2-2022 were re-used.

The evaluation of the product Infineon Technologies AG OPTIGA™ Trusted Platform Module SLB9672_2.0 v16 and SLB9673_2.0 v26, version v16.10.16488.00, v16.12.16858.00 and v26.10.16688.00, was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 27 April 2022. 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 at the date of certification. 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.

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

[5] Information Technology Security Evaluation Facility

maximum validity of the certificate has been limited. The certificate issued on 29 April 2022 is valid until 28 April 2027. 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 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 v16 and SLB9673_2.0 v26, version v16.10.16488.00, v16.12.16858.00 and v26.10.16688.00, has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 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
Am Campeon 1-15
85579 Neubiberg

# 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 v16 and Trusted Platform Module SLB9673_2.0 v26 (or SLB9672_2.0 v16 and SLB9673_2.0 v26 in short), version v16.10.16488.00, v16.12.16858.00 and v26.10.16688.00, including related guidance documentation as described in the Security Target [6].

The TOE is an integrated circuit and software platform that provides computer manufacturers with the core components of a subsystem used to assure authenticity, integrity and confidentiality in e-commerce and internet communications within a Trusted Computing Platform. The SLB9672_2.0 v16 and SLB9673_2.0 v26 is a complete solution implementing the version 2.0 of the TCG Trusted Platform Module Library Family “2.0” Revision 01.59 Specification and the TCG PC Client Platform TPM Profile Specification for TPM 2.0.

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 SLB9672_2.0 v16 and SLB9673_2.0 v26 are basically secure controllers with the following added functionality:

- Random number generator (DRBG),
- Asymmetric key generation (RSA keys with key length 1024, 2048, 3072 and 4096 bits, EC keys with key length 256 bits and 384 bits),
- Symmetric key generation (AES keys with 128, 192 and 256 bits),
- Symmetric and asymmetric key procedures (encryption/decryption, generation and verification of digital signatures),
- Hash algorithms (SHA-1, SHA-256, SHA-384) and MAC (HMAC),
- Secure key and data storage,
- Identification and Authorization mechanisms.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Protection Profile PC Client Specific TPM, TPM Library specification Family “2.0”, Level 0 Revision 1.59, Version: 1.3, Date: 2021-09-29, ANSSI-CC-PP-2021/02 [8].

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 4 augmented by ALC_FLR.1 and AVA_VAN.4.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 7.2. 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_CRY | Cryptographic Support |
| SF_I&A | Identification and Authentication |

| TOE Security Functionality | Addressed issue |
|---|---|
| SF_G&T | General and Test |
| SF_OBH | Object Hierarchy |
| SF_TOP | TOE Operation |

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 8.1.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 4.1. 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 [6], chapters 4.1, 4.2 and 4.3.

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

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms 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 AG OPTIGA™ Trusted Platform Module SLB9672_2.0 v16 and SLB9673_2.0 v26, version v16.10.16488.00, v16.12.16858.00 and v26.10.16688.00**

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 v16 and SLB9673_2.0 v26 | v16.10.16488.00 and v16.12.16858.00 and v26.10.16688.00 | Packaged module |
| 2. | DOC | *OPTIGA™ TPM SLB 9672 FW16.10 Databook* | Revision 1.1, 2021-07-22 | PDF-file |
| | | *OPTIGA™ TPM SLB 9672 FW16.12 Databook* | Revision 1.2, 2022-03-09 | PDF-file |
| | | *OPTIGA™ TPM, SLB9673 FW26.10, Databook* | Revision 1.2, 2022-03-09 | 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 FW16.xx, Errata and Updates* | Revision 1.3, 2022-03-24 | PDF-file |

| No. | Type | Item / Identifier | Release / Version | Form of Delivery |
|---|---|---|---|---|
| | | *OPTIGA™ TPM, SLB 9673 TPM2.0 FW26.xx, Errata and Updates* | Revision 1.0, 2021-10-21 | 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 v16 and SLB9673_2.0 v26 | v16.10.16488.00, v16.12.16858.00 and v26.10.16688.00 |

Table 3: Identifiers of the TOE

The fabricated modules are physically labelled with the TOE reference by printing. The labelling consists of four lines (for SLB9672_2.0 v16 and SLB9673_2.0 v26, resp.):

| Line | Label | Remark |
|---|---|---|
| 0 | Infineon | Logo and name of producer |
| 1 | SLB9672 | – |
| 2 | XU20 yy or 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 | XU20 yy or AU20 yy | The <yy> is an internal FW indication (only at manufacturing due to field upgrade option) |
| 3 | <Lot number> H <datecode> | – |

Table 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 (SLB9672_2.0 v16 and SLB9673_2.0 v26, resp.):

| 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. 0x0010000A indicates v16.10, 0x0010000C indicates v16.12 |
| TPM_PT_FIRMWARE_VERSION_2 | Build number and Common Criteria certification state (for instance, 0x00406800 or 0x00406802)<br>Byte 1: reserved for future use (0x00)<br>Byte 2 and 3: Build number (for instance, 0x4068)<br>Byte 4: Common Criteria certification state/mode:<br>0x00 = TPM operational mode/TPM is CC certified,<br>0x02 = TPM operational mode/TPM is not certified,<br>0x60 = Manually entered TPM firmware recovery mode (triggered externally for testing purposes)<br>0x61 = TPM firmware recovery mode (triggered by code integrity failure detection)<br>0x62 = TPM firmware update mode |
| TPM_PT_MODES | Bit 0 (FIPS_140_2) = 1<br>Bits 1...31 = 0 |

| Property | Vendor specific value |
|---|---|
| TPM_PT_MANUFACTURER | “IFX” |
| TPM_PT_VENDOR_STRING_1 | “SLB9” |

| Property | Vendor specific value |
|---|---|
| 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. 0x001A000A indicates v26.10 |
| TPM_PT_FIRMWARE_VERSION_2 | Build number and Common Criteria certification state (for instance, 0x00413000 or 0x00413002)<br>Byte 1: reserved for future use (0x00)<br>Byte 2 and 3: Build number (for instance, 0x4130)<br>Byte 4: Common Criteria certification state/mode:<br>0x00 = TPM operational mode/TPM is CC certified,<br>0x02 = TPM operational mode/TPM is not certified,<br>0x60 = Manually entered TPM firmware recovery mode (triggered externally for testing purposes)<br>0x61 = TPM firmware recovery mode (triggered by code integrity failure detection)<br>0x62 = TPM firmware update mode |
| TPM_PT_MODES | Bit 0 (FIPS_140_2) = 1<br>Bits 1...31 = 0 |

Table 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 TOE is delivered in form of complete chips which include the hardware, the firmware, the Endorsement Primary Seed, two RSA Endorsement Key, two ECC Endorsement Keys and four Endorsement Certificates. The delivery of the TOE is done from a distribution centre by postal transfer or delivery courier.

The delivery 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 is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

- Cryptographic Support: generation of random numbers, generation of asymmetric key pairs, RSA and ECC digital signature (generation and verification), RSA, ECC and AES data encryption and decryption, key destruction, the generation of hash values and the generation and verification of MAC values.
- Identification and Authentication: mechanisms for the identification and authentication capability to authorize the use of a Protected Object and Protected Capability using authentication values or policies.
- 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, modification of security attributes, provision of TPM hierarchy model, monitoring of data storage, enforcement of object hierarchy.
- TOE Operation: access control on different subjects, objects and operations, enforcement of different rules of operation and interaction between subjects and objects, enabling and disabling of functions, enforcement of NVM restrictions, and creation of evidence of origin.

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 topics are of relevance: (Details can be found in chapter 5.2 of the ST [6])

- OE.Configuration: The TOE must be installed and configured properly for starting up the TOE in a secure state. The security attributes of subjects and objects shall be managed securely by the authorised user.
- OE.Locality: The developer of the host platform must ensure that trusted processes indicate their correct locality to the TPM and untrusted processes are able to assert just the locality 0 or Legacy only to the TPM.
- OE.Credential: The IT environment must create EK and AK credentials by trustworthy procedures for the root of trust for reporting.
- OE.Measurement: The platform part of the root of trust for measurement provides a representation of embedded data or program code (measured values) to the TPM for measurement.
- 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.

- OE.ECDAA: The ECDAA issuer must support a procedure for attestation without revealing the attestation information based on the ECDAA signing operation.

# 5. Architectural Information

The SLB9672_2.0 v16 and SLB9673_2.0 v26 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) (used only in SLB9672_2.0 v16), Inter Integrated Circuit (I2C) (used only in SLB9673_2.0 v26), 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 in the Trusted Platform Module Library specification and User Guidance.

The entire firmware of the TOE as defined in the PP [8] is comprised of: Boot Software (BOS), Professional Secure Operating System (PSOS), Cryptographic Libraries (ACL, SCL, HCL, RCL), Hardware Support Library (HSL), FieldUpgrade (CFUL), TPM2.0 Application (APP).

# 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 the ST [6] and the design documentation, 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.

TOE test configuration:

The tests are performed with the chips OPTIGA™ Trusted Platform Module SLB9672_2.0 v16 and OPTIGA™ Trusted Platform Module SLB9673_2.0 v26, uniquely identified by their serial numbers and version information. For the tests different chip types are prepared. One of these types is the configuration which is finally delivered to the user. The others contain special download functionality for test programs or have some security mechanisms deactivated. The entire functionality is the same for all chips.

All security features (portions of the TSF) and related interfaces were tested. Therefore no selection criteria are applied. All security features and related interfaces are tested regarding their functional behavior. The tests were chosen to perform at minimum one test for each security feature of TSF and related interfaces.

Verdict for the activity:
The results of the specified and conducted independent evaluator tests confirm the TOE functionality as described. The TSF and the interfaces were found to behave as specified. The results of the developer tests, which have been repeated by the evaluator, matched the results the developer stated. 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.

**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.

Systematic search for potential vulnerabilities and known attacks in public domain sources has been conducted, using a list of vulnerabilities [4, AIS26], and from a methodical analysis of the evaluation documents. Analysis has been carried out why these vulnerabilities are not exploitable in the intended environment of the TOE. If the rationale is suspect in the opinion of the evaluator penetration tests are devised. Even if the rationale is convincing in the opinion of the evaluator penetration tests are devised for some vulnerabilities, especially to support the argument of non-practicability of the exploiting time in case of SPA, DPA and FI attacks.

For implementation attacks the following test resources were used by the evaluator: Digital Oscilloscope, Passive Probe, Active Differential Probe, EM Probe, Delay Generator, Laser Fault Injection System and proprietary measuring/analyzing software.

Amongst others, the following attack scenarios have been tested: Statistical tests of the TOE DRNG according to AIS 20 requirements, undocumented capabilities which are sent by the TOE as response to TPM2_GetCapabilitiy command, circumvention of access control by injecting faults through laser light (LFI attack), effectiveness of filters and detectors, effectiveness of bus and memory encryption, Differential Fault Analysis, Simple and Differential Power Analysis, EMA / SEMA / DEMA Attacks, effectiveness of deactivation of test functions, bypass of PIN counter, intentional misuse of TPM commands.

Verdict for the sub-activity:

The evaluator has performed penetration testing based on the systematic search for potential vulnerabilities and known attacks in public domain sources and from the methodical analysis of the evaluation documents. During the evaluator's penetration testing of potential vulnerabilities the TOE operated as specified. All potential vulnerabilities are not exploitable in the intended environment for the TOE. The TOE is resistant to attackers with **moderate attack potential** in the intended environment for the TOE.

# 8. Evaluated Configuration

This certification covers the following configurations of the TOE:

Trusted Platform Module SLB9672_2.0 v16 and Trusted Platform Module SLB9673_2.0 v26 (or SLB9672_2.0 v16 and SLB9673_2.0 v26 in short), version v16.10.16488.00, v16.12.16858.00 and v26.10.16688.00, including related guidance documentation as described in the Security Target [6].

# 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-1178-V2-2022, re-use of specific

evaluation tasks was possible. The TOE's hardware and firmware of the new version v16.12.16858.00 remain unchanged in comparison to the forerunner certification. *Within the course of this re-certification process, the following changes are relevant to the TOE:*

*i. There are changes in the software version v16.12.16858.00 compared to the version v16.10.16488.00, namely an update of the Operating System; moreover, in warm reset mode the tick counter interrupts are disabled.*

*ii. A new Databook for the TOE version v16.12.16858.00 was added, the Databook for the version v26.10.16688.00 was updated.*

*iii. The Errata and Updates document was updated.*

The evaluation has confirmed:

- PP Conformance: Protection Profile PC Client Specific TPM, TPM Library specification Family "2.0", Level 0 Revision 1.59, Version: 1.3, Date: 2021-09-29, ANSSI-CC-PP-2021/02 [8]
- for the Functionality: PP conformant
  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). But cryptographic functionalities with a security level of lower than 100 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 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 and outlines its rating from cryptographic point of view. Any Cryptographic Functionality that is marked in column '*Security Level above 100 Bits*' of the following table with '*no*' achieves a security level of lower than 100 Bits (in general context) only.

Detailed results on conformance and non-conformance have been compiled into the report [17].

## 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.

Especially the following notice from the Security Target [6] should be taken into account:

*The TPM includes two ECC Endorsement Keys (EK) and two RSA Endorsement Keys (EK) and the Endorsement Primary Seed (EPS), which can be used to generate additional EKs alternatively. The two ECC Endorsement Keys, the two RSA Endorsement Keys and the Endorsement Primary Seed are generated outside the TPM with the TPM Personalization Certification Authority (TPM-CA) located within the secure production area of the TOE in a secure room. The RSA Endorsement Key is generated from a proved random number generator by the HSM-PDG and not derived from the Endorsement Seed.*

*The Endorsement Keys RSA EK and ECC EK, personalized by the TPM vendor, are not visible and changeable for the user, but can be deactivated with the TPM2_EvictControl() and TPM2_FlushContext commands, and can be activated again with the TPM2_CreatePrimary command by the user. As these personalized Endorsement Keys should be used only for the identification of the TPM vendor, the user shall not use these keys for other functions.*

*During the production phase the so called unique ID is computed, which is unique across all Infineon TPMs and stored as NV index in a reserved Infineon NV index handle area for TPM OEMs. The TPM unique ID can not be changed and is preserved across field upgrades.*

# 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 |
| **EAL** | Evaluation Assurance Level |
| **ETR** | Evaluation Technical Report |
| **I2C** | Inter Integrated Circuit Interface |
| **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 |
| **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.

**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.

# 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-1178-V3-2022, Version 2.3, March 30, 2022, “Security Target OPTIGA™ Trusted Platform Module SLB9672_2.0 v16 SLB9673_2.0 v26”, Infineon Technologies AG (public document)

[7] Evaluation Technical Report, Version 2, April 06, 2022, ”Evaluation Technical Report Summary”, TÜV Informationstechnik GmbH, (confidential 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

[8] Protection Profile PC Client Specific TPM, TPM Library specification Family “2.0”, Level 0 Revision 1.59, Version: 1.3, Date: 2021-09-29, ANSSI-CC-PP-2021/02

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

[10] OPTIGA™ TPM, SLB9672 FW16.10, Databook, Revision 1.1, July 22, 2021, Infineon Technologies AG

OPTIGA™ TPM, SLB9673 FW26.10, Databook, Revision 1.2, March 09, 2022, Infineon Technologies AG

OPTIGA™ TPM, SLB9672 FW16.12, Databook, Revision 1.2, March 09, 2022, Infineon Technologies AG

[11] OPTIGA™ TPM, SLB 9672 TPM2.0 FW16.xx, Errata and Updates, Revision 1.3, March 24, 2022

OPTIGA™ TPM, SLB 9673 TPM2.0 FW26.xx, Errata and Updates, Revision 1.0, Oct 21, 2021

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

[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)

[17] SINGLE EVALUATION REPORT ADDENDUM to ETR-Part ASE, Cryptographic Standards Compliance Verification (CSCV); Version 1, July 19, 2021, TÜV Informationstechnik GmbH, (confidential document)

# 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-1178-V3-2022

## Evaluation results regarding development and production environment

The IT product Infineon Technologies AG OPTIGA™ Trusted Platform Module SLB9672_2.0 v16 and SLB9673_2.0 v26, version v16.10.16488.00, v16.12.16858.00 and v26.10.16688.00, (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 29 April 2022, 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<br>Tampines LogisPark<br>1 Greenwich Drive<br>Singapore 533865 |
| K&N Großostheim | Kühne & Nagel<br>Stockstädter Strasse 10<br>63762 Großostheim<br>Germany |
| KWE Shanghai | KWE Kintetsu World Express (China) Co., Ltd.<br>Shanghai Pudong Airport Pilot Free Trade Zone<br>No. 530 Zheng Ding Road<br>Shanghai,<br>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-1178-V3-2022

## Overview and rating of cryptographic functionalities implemented in the TOE

| No. | Cryptographic Mechanism | Standard of Implementation | Key Size in Bits | Comments | Security Level above 100 Bits |
|---|---|---|---|---|---|
| 1. | Authenticity RSA signature generation / verification | [RFC3447] | \|Modulus\| = 1024 | [Main_1, B.1 – B.7] and [Main_3, 20.2] | no |
| | RSASSA-PKCS1-v1_5 | [RFC3447, 8.2] | | | no |
| | RSASSA_PSS | [RFC3447, 8.1] | | | no |
| | SHA-1, SHA-256, SHA-384 | [FIPS180-4] | | | no |
| 2. | Authenticity RSA signature generation / verification | [RFC3447] | \|\|Modulus\| = 2048<br>\|Modulus\| = 3072<br>\|Modulus\| = 4096 | [Main_1, B.1 – B.7] and [Main_3, 20.2] | yes |
| | RSASSA-PKCS1-v1_5 | [RFC3447, 8.2] | | | yes |
| | RSASSA_PSS | [RFC3447, 8.1] | | | yes |
| | SHA-1, SHA-256, SHA-384 | [FIPS180-4] | | | no, yes, yes |
| 3. | Authenticity EC signature generation/ verification according to | [FIPS186-4] | \|k\| = 256<br>\|k\| = 384 | [Main_1, C.4.2] | yes |
| | ECDSA | [ISO_14888-3] | ECC_NIST_P256<br>ECC_NIST_P384 | | yes |
| | SHA-1, SHA-256, SHA-384 | [FIPS180-4] | | | no, yes, yes |
| 4. | Authenticity EC signature generation according to | [ISO_15946-5] | \|k\| = 256<br>\| | [Main_1, C.4.2] | yes |
| | ECDAA | [Main_1, C.4.2] | ECC_BN_P256 | | |
| | SHA-1, SHA-256, SHA-384 | [ISO_10118-3] | | | no, yes, yes |
| 5. | EC signature verification ECDSA | [FIPS186-4] | \|k\| = 521<br>ECC_NIST_P521 | TPM-FieldUpgrade | yes |
| | SHA-512 | [FIPS180-4] | | | |

| No. | Cryptographic Mechanism | Standard of Implementation | Key Size in Bits | Comments | Security Level above 100 Bits |
|---|---|---|---|---|---|
| | XMSS<br>SHA-256 | [N8208]<br>[FIPS180-4] | - | | yes |
| 6. | Authentication HMAC with SHA-1 | [ISO_9797-2]<br>[ISO_10118-3] | \|k\| = 160 | [Main_1, 11.4.3] | no |
| | ECDEC | [N856, 6.2.2.2] | \|k\| = 256<br>\|k\| = 384 | [Main_1, C7] | yes |
| | | [FIPS186-4] | ECC_NIST_P256<br>ECC_NIST_P384 | | |
| | RSA decryption RSAES-PKCS1-v1_5 | [RFC3447, 7.2] | \|Modulus\| = 2048 | | yes |
| | AES decryption in CFB mode | [ISO_18033-3],<br>[ISO_10116] | \|k\| = 128<br>\|k\| = 192<br>\|k\| = 256 | | yes |
| 7. | Authentication HMAC with SHA-256 and SHA-384 | [ISO_9797-2],<br>[ISO_10118-3] | \|k\| = 256<br>\|k\| = 384 | [Main_1, 11.4.3] | yes |
| | ECDEC | [N856, 6.2.2.2] | \|k\| = 256<br>\|k\| = 384 | [Main_1, C7] | yes |
| | | [FIPS186-4] | ECC_NIST_P256<br>ECC_NIST_P384 | | |
| | RSA decryption RSAES-PKCS1-v1_5 | [RFC3447, 7.2] | \|Modulus\| = 2048<br>\|Modulus\| = 3072<br>\|Modulus\| = 4096 | | yes |
| | AES decryption in CFB mode | [ISO_18033-3],<br>[ISO_10116] | \|k\| = 128<br>\|k\| = 192<br>\|k\| = 256 | | yes |
| 8. | Key Agreement Diffie-Hellmann (ECDH) | [N856, 6.2.2.2] | \|k\| = 256<br>\|k\| = 384 | [Main_1, 11.4.9.3] | yes |
| | | [FIPS186-4] | ECC_NIST_P256<br>ECC_NIST_P384 | | yes |
| | KDFe | [N856] | | [Main_1, C7] | yes |
| | HMAC with SHA-256, SHA-384 and | [ISO_9797-2],<br>[ISO_10118-3] | \|k\| = 256<br>\|k\| = 384 | | yes |
| | SHA-1 | | \|k\| = 160 | | no |
| 9. | Key Agreement KDFa | [Main_1, 11.4.9.1],<br>[N808] | | [Main_1, 11.4.9.1] | yes |
| | HMAC with SHA-256, SHA-384 and | [ISO_9797-2],<br>[ISO_10118-3] | \|k\| = 256<br>\|k\| = 384 | | yes |
| | SHA-1 | | \|k\| = 160 | | no |
| 10. | Key Agreement AES CMAC | [N808]<br>[ISO_18033-3],<br>[ISO_9797-1] | \|k\| = 256 | TPM-FieldUpgrade | yes |

| No. | Cryptographic Mechanism | Standard of Implementation | Key Size in Bits | Comments | Security Level above 100 Bits |
|---|---|---|---|---|---|
| 11. | Integrity HMAC with SHA-256, SHA-384 and<br>SHA-1 | [ISO_9797-2], [ISO_10118-3] | \|k\| = 256<br>\|k\| = 384<br>\|k\| = 160 | [Main_1, 11.4.3] | yes<br>no |
| 12. | Integrity XMSS with SHA-256 | [N8208] [ISO_10118-3] | - | TPM-FieldUpgrade | yes |
| 13. | Confidentiality AES in CFB mode | [ISO_18033-3], [ISO_10116] | \|k\| = 128<br>\|k\| = 192<br>\|k\| = 256 | [TPM] | yes |
| 14. | Confidentiality RSA encryption / decryption<br>RSAES -PKCS1-v1_5<br>RSAES-OAEP | [RFC3447]<br>[RFC3447, 7.2]<br>[RFC3447, 7.1] | \|Modulus\| = 1024 | [Main_1, B.1 – B.7]<br>[Main_3, 14] | no<br>no<br>no |
| 15. | Confidentiality RSA encryption / decryption<br>RSAES -PKCS1-v1_5<br>RSAES-OAEP | [RFC3447]<br>[RFC3447, 7.2]<br>[RFC3447, 7.1] | \|Modulus\| = 2048<br>\|Modulus\| = 3072<br>\|Modulus\| = 4096 | [Main_1, B.1 – B.7]<br>[Main_3, 14] | yes<br>yes<br>yes |
| 16. | Cryptographic Primitive SHA-384 | [FIPS180-4] | none | [Main_1, 11.4.2] | yes |
| 17. | Cryptographic Primitive SHA-256 | [FIPS180-4] | none | [Main_1, 11.4.2] | yes |
| 18. | Cryptographic Primitive SHA-1 | [FIPS180-4] | none | [Main_1, 11.4.2] | no |
| 19. | Cryptographic Primitive HMAC with SHA-1 | [ISO_9797-2], [ISO_10118-3] | \|k\| = 160 | [Main_1, 11.4.3] | no |
| 20. | Cryptographic Primitive HMAC with SHA-256 | [ISO_9797-2], [ISO_10118-3] | \|k\| = 256 | [Main_1, 11.4.3] | yes |
| 21. | Cryptographic Primitive HMAC with SHA-384 | [ISO_9797-2], [ISO_10118-3] | \|k\| = 384 | [Main_1, 11.4.3] | yes |
| 22. | Cryptographic Primitive Deterministic RNG DRG.3 | [AIS20], [N890A] | CTR_DRBG implemented | [Main_1, 11.4.10] | yes |
| 23. | Trusted Channel HMAC with SHA-256 and SHA-384 | [ISO_9797-2], [ISO_10118-3] | \|k\| = 256<br>\|k\| = 384 | [TPM] | yes |
| 24. | Trusted Channel AES in CFB mode | [ISO_18033-3], [ISO_10116] | \|k\| = 128<br>\|k\| = 192<br>\|k\| = 256 | [TPM] | yes |

| No. | Cryptographic Mechanism | Standard of Implementation | Key Size in Bits | Comments | Security Level above 100 Bits |
|---|---|---|---|---|---|
| | RSA | [RFC3447] | \|k\| = 1024,<br>\|k\| = 2048<br>\|k\| = 3072<br>\|k\| = 4096 | | no (1024),<br>yes, yes, yes |
| | ECC | [FIPS186-4], [N856] | ECC_NIST_P256,<br>ECC_NIST_P384,<br>\|k\| = 256<br>\|k\| = 384 | | yes |
| | HMAC with SHA-256, SHA-384 and | [ISO_9797-2], [ISO_10118-3] | \|k\| = 256<br>\|k\| = 384 | | yes |
| | SHA-1 | | \|k\| = 160 | | no |
| 25. | Key Generation RSA primary keys | [TPM], [FIPS186-4], [N890A] using CRT_DRBG | \|k\| = 2048<br>\|k\| = 3072<br>\|k\| = 4096 | – | yes |
| 26. | Key Generation RSA | [TPM], [FIPS186-4], [N890A] using CRT_DRBG | \|k\| = 2048<br>\|k\| = 3072<br>\|k\| = 4096 | | yes |
| 27. | Key Generation RSA | [TPM], | \|k\| = 1024 | Infineon key generation method “TPM_RSA GEN2” | *Not rated* |
| 28. | Key Generation ECC | [TPM], [FIPS186-4], [N890A] using CRT_DRBG | \|k\| = 256<br>\|k\| = 384 | – | yes<br>yes |
| | ECC_NIST_P256<br>ECC_NIST_P384 | [FIPS186-4] | | | yes |
| | ECC_BN_P256 | [ISO_15946-5] | | | no |
| 29. | Key Generation AES | [TPM], [N8133], [N808], [N890A] | \|k\| = 128<br>\|k\| = 192<br>\|k\| = 256 | – | yes |

Table 7: TOE cryptographic functionality

**Reference of Legislatives and Standards specified in Table 7 above:**

[FIPS180-4] *Federal Information Processing Standards Publication, Secure Hash Standard (SHS)*, 2015-08, U.S. department of Commerce / National Institute of Standards and Technology (NIST).

[FIPS186-4] *Federal Information Processing Standards Publication FIPS PUB 186-4, Digital Signature Standard (DSS)*, 2013-07, U.S. department of Commerce / National Institute of Standards and Technology (NIST).

[FIPS186-5] *Federal Information Processing Standards Publication FIPS PUB 186-5 (Draft), Digital Signature Standard (DSS),* 2019-10, U.S. department of Commerce / National Institute of Standards and Technology (NIST).

[ISO_10116] ISO/IEC 10116: *Information technology - Security techniques – Modes of operation for an n-bit block cipher,* 2006, ISO/IEC.

[ISO_10118-3] ISO 10118-3: *Information technology - Security techniques – Hash-functions – Part 3: Dedicated hash-functions*, 2004, ISO/IEC.

[ISO_14888-3] ISO 14888-3: *Information technology - Security techniques – Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms*, 2006, ISO/IEC.

[ISO_15946-5] ISO 15946-5: *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 5: Elliptic curve generation*, 2009, ISO/IEC.

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

[ISO_9797-2] Information technology - *Security techniques- Message Authentication Codes (MACs) - Part 2: Mechanisms using a dedicated hash-function*, 2011-05, ISO/IEC.

[Main_1] *Trusted Platform Module Library Part 1: Architecture, Family "2.0"*, Level 00 Revision 01.59, 2019-11-08, Trusted Computing Group (TCG).

[Main_2] *Trusted Platform Module Library Part 2: Structures, Family "2.0"*, Level 00 Revision 01.59, 2019-11-08, Trusted Computing Group (TCG).

[Main_3] *Trusted Platform Module Library Part 3: Commands, Family "2.0",* Level 00 Revision 01.59, 2019-11-08, Trusted Computing Group (TCG).

[Main_4] *Trusted Platform Module Library Part 4: Supporting Routines, Family "2.0"*, Level 00 Revision 01.59, 2019-11-08, Trusted Computing Group (TCG).

[N8133] NIST Special Publication 800-133 Revision 1, *Recommendation for Cryptographic Key Generation,* 2019-03, National Institute of Standards and Technology (NIST).

[N8133_2012] NIST Special Publication 800-133, *Recommendation for Cryptographic Key Generation*, 2012-12, National Institute of Standards and Technology (NIST).

[N8208] Draft NIST Special Publication 800-208, *Recommendation for Stateful Hash-Based Signature Schemes,* 2019-12, National Institute of Standards and Technology (NIST).

[N856] NIST SP800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, (revised), Revision 1, 2007-03, National Institute of Standards and Technology (NIST).

[N890A] NIST Special Publication 800-90A: *Recommendation for Random Number Generation Using Deterministic Random Bit Generators,* 2015-06, National Institute of Standards and Technology (NIST).

[RFC3447] RFC 3447 - P*ublic-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications,* Version 2.1, published by The Internet Society, 2003-02, http://www.ietf.org/rfc/rfc3447.

[RFC8391] RFC 8391 – *XMSS: eXtended Merkle Signature Scheme, 2018-05, Internet Research Task Force (IRTF)*, http://www.ietf.org/rfc/rfc8391

[TPM] *Trusted Platform Module Library*, consisting of [Main_1], [Main_2], [Main_3] and [Main_4].

Note: End of report