Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1056-2018

for

Infineon Technologies AG Trusted Platform Module SLB9665_2.0 v5.63.3144.00, v5.63.3149.00, v5.63.3353.00, v5.63.3355.00

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-1056-2018 (*)

Trusted Platform Module

Infineon Technologies AG Trusted Platform Module SLB9665_2.0,
v5.63.3144.00, v5.63.3149.00, v5.63.3353.00, v5.63.3355.00

SOGIS
Recognition Agreement

from	Infineon Technologies AG
PP Conformance:	Protection Profile, TPM Library specification Family “2.0”, Level 0 Revision 1.16, December 10, 2014, Version 1.0, Trusted Computing Group
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.1 and AVA_VAN.4

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 4

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, 30 April 2018

For the Federal Office for Information Security

Joachim Weber
Head of Branch

L.S.

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

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....6

1. Preliminary Remarks....6
2. Specifications of the Certification Procedure....6
3. Recognition Agreements....7
4. Performance of Evaluation and Certification....8
5. Validity of the Certification Result....8
6. Publication....9

B. Certification Results....10

1. Executive Summary....11
2. Identification of the TOE....12
3. Security Policy....15
4. Assumptions and Clarification of Scope....16
5. Architectural Information....16
6. Documentation....19
7. IT Product Testing....19
8. Evaluated Configuration....24
9. Results of the Evaluation....24
10. Obligations and Notes for the Usage of the TOE....25
11. Security Target....26
12. Definitions....26
13. Bibliography....27

C. Excerpts from the Criteria....30

D. Annexes....31

A. Certification

1. Preliminary Remarks

Under the BSIG1 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]
- BSI Schedule of 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]
- 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 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

- 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.sogisportal.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: http://www.commoncriteriaportal.org.

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

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2+ ALC_FLR components.

[4] Proclamation of the 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 Trusted Platform Module SLB9665_2.0, v5.63.3144.00, v5.63.3149.00, v5.63.3353.00, v5.63.3355.00 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1020-V2-2017. Specific results from the evaluation process BSI-DSZ-CC-1020-V2-2017 were re-used.

The evaluation of the product Infineon Technologies AG Trusted Platform Module SLB9665_2.0, v5.63.3144.00, v5.63.3149.00, v5.63.3353.00, v5.63.3355.00 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 18 April 2018. 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 maximum validity of the certificate has been limited. The certificate issued on 30 April 2018 is valid until 29 April 2023. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

[5] Information Technology Security Evaluation Facility

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 Trusted Platform Module SLB9665_2.0, v5.63.3144.00, v5.63.3149.00, v5.63.3353.00, v5.63.3355.00 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
Alter Postweg 101
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 SLB9665_2.0, versions v5.63.3144.00 and v5.63.3149.00 and v5.63.3353.00 and v5.63.3355.00, including related guidance documentation as described in the Security Target. The versions v5.63.3144.00 and v5.63.3149.00 and the versions v5.63.3353.00 and v5.63.3355.00 include the identical source code, where the versions v5.63.3149.00 and v5.63.3355.00 are used for field upgrade.

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 SLB9665_2.0 is a complete solution implementing the version 2.0 of the TCG Trusted Platform Module Library Family “2.0” Specification and the TCG PC Client Specific Platform TPM Profile (PTP) Family “2.0” Specification.

The SLB9665_2.0 uses the Low Pin Count Interface (LPC) as defined by Intel for the integration into existing PC mainboards. The SLB9665_2.0 is basically a secure controller with the following added functionalities:

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

The TOE is delivered in different variants. The hardware and firmware/software of the variants are identical, the only difference between the derivatives are the temperature range (standard or enhanced temperature range) and the package.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Protection Profile, TPM Library specification Family “2.0”, Level 0 Revision 1.16, December 10, 2014, Version 1.0, Trusted Computing Group [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
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; all taken from the underlying PP [8]. 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.

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

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

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

Infineon Technologies AG Trusted Platform Module SLB9665_2.0,

v5.63.3144.00, v5.63.3149.00, v5.63.3353.00, v5.63.3355.00

The following table outlines the TOE deliverables:

No.	Type	Item / Identifier	Release / Version	Form of Delivery
1	HW	Trusted Platform Module SLB9665_2.0	v5.63.3144.00, v5.63.3149.00, v5.63.3353.00, v5.63.3355.00	Packaged module
2	DOC	*OPTIGA™ TPM 2.0 Trusted Platform Module Application Note User Guidance*	Revision 1.90, 2018-02-28	Hardcopy or pdf-file
3	DOC	*OPTIGA™ Trusted Platform Module Databook*	Revision 2.9, 2017-08-01	Hardcopy or pdf-file
4	DOC	*OPTIGA™ TPM SLB9665 TPM 2.0 Errata and Updates*	Revision 2.3, 2017-11-03	Hardcopy or pdf-file
5	DOC	*OPTIGA™ TPM SLB9665 TPM 2.0 Errata and Updates*	Revision 2.4, 2018-02-02	Hardcopy or pdf-file
6	DOC	*TPM Library Part 1 Architecture, Family "2.0", Level 00*	Revision 01.16, 2014-10-30	Public document, downloadable from https://www.trustedco

No.	Type	Item / Identifier	Release / Version	Form of Delivery
				mputinggroup.org
7	DOC	*TPM Library Part 2 Structures, Family "2.0", Level 00*	Revision 01.16, 2014-10-30	Public document, downloadable from https://www.trustedcomputinggroup.org
8	DOC	*TPM Library Part 3 Commands, Family "2.0", Level 00*	Revision 01.16, 2014-10-30	Public document, downloadable from https://www.trustedcomputinggroup.org
9	DOC	*TPM Library Part 4 Supporting Routines, Family "2.0", Level 00*	Revision 01.16, 2014-10-30	Public document, downloadable from https://www.trustedcomputinggroup.org
10	DOC	*ERRATA, Errata Version 1.5, September 21, 2016 FOR TCG Trusted Platform Module Library, Specification Version 2.0, Revision 1.16, October 30, 2014, TCG Published*	Version 1.5, 2016-09-21	Public document, downloadable from https://www.trustedcomputinggroup.org
11	DOC	*TCG PC Client Specific Platform TPM Profile for TPM TPM 2.0 (PTP), Family "2.0", Level 00*	Revision 00.43, 2015-01-26	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	Trusted Platform Module SLB9665_2.0	v5.63.3144.00 and v5.63.3149.00 and v5.63.3353.00 and v5.63.3355.00

Table 3: Identifiers of the TOE

The fabricated modules are physically labelled with the TOE reference by printing. The following table lists the labelling for the package TSSOP-28-2:

Line	Content	Remark
1	SLB9665TT20 or SLB9665XT20	SLB9665TT20: Standard temperature range, SLB9665XT20: Enhanced temperature range.
2	G <datecode> KMC	<K> indicates assembly site code, <MC> indicates mold compound code
3	00 <Lot number>	The 00 is an internal FW indication (only at manufacturing due to field upgrade option).

Table 4: Labelling of TOE module

The following table lists the labelling for the package VQFN-32-13:

Line	Content	Remark
0	Infineon	—
1	SLB9665	—
2	VQ20yy or XQ20 yy	VQ20: Standard temperature range, XQ20: Enhanced temperature range. The <yy> is an internal FW indication (only at manufacturing due to field upgrade option).
3	<Lot number> H <datecode>	—

Table 4a: Labelling of TOE module for VQFN-32-13

The version information of the TOE can be read out electronically with the command TPM2_GetCapability. In the Databook [10] chapter 4.6.2 the vendor specific return values for the TOE are defined as listed in the following table:

Property	Vendor specific value
TPM_PT_MANUFACTURER	“IFX”
TPM_PT_VENDOR_STRING_1	“SLB9”
TPM_PT_VENDOR_STRING_2	“665”
TPM_PT_VENDOR_STRING_3	NULL
TPM_PT_VENDOR_STRING_4	NULL
TPM_PT_FIRMWARE_VERSION_1	Major and minor version (for instance, 0x0005003F indicates V5.63)
TPM_PT_FIRMWARE_VERSION_2	Build number and Common Criteria certification state (for instance, 0x000C4800 or 0x000C4802) Byte 1: reserved for future use (0x00) Bytes 2 and 3: Build number (for instance, 0x0C48) Byte 4: Common Criteria certification state, 0x00 means TPM is CC certified, 0x02 means TPM is not certified

Table 5: Vendor specific properties of TPM2_GetCapability

TOE Delivery

The TOE is a Trusted Platform Module and will be delivered only in form of complete mounted ICs. Only TOEs which have undergone and passed all the production tests are delivered. At the delivery they are in user mode, the test mode is locked and not accessible.

The production of the TOE wafers will be performed at IFX Dresden.

The production site sends the TOE to one of the distribution centers: DHL Singapore (DC-A: Distribution Center Asia), K&N Großostheim (DC-E: Distribution Center Europe), K&N Hayward (DC-U: Distribution Center USA), G&D Neustadt (backup distribution center), IFX Morgan Hill (backup distribution center).

The real shipment is done in the following manner:

1. The customer picks up the TOE directly at one of the distribution centers. After a positive check of the proof of the identity of the recipient (the customer has to announce the recipient and Infineon Technologies checks the identity of the recipient controlling the consignment notes and the passport of the recipient) is done, the TOE is delivered to the recipient (e.g. Transport Company of the

customer). The recipient has to sign an acknowledgement of receipt that contains the date of the delivery, the number of parts, the specific product name (TOE) and the name of the recipient. The customer can choose the transport company and is responsible for the transport security.

2. The distribution centers send the TOE to the customer (Platform Manufacturer). The transport is secured by the following process: For the transport only evaluated haulage companies are used, which are chosen by the Infineon Technologies AG. The assessment and approvement of the used haulage companies is done by a department of the Infineon Technologies AG. The sender informs the receiver (other distribution center or customer) that a delivery was started. After the delivery was received the delivery is checked according to the consignment notes. If any delay or failure occurs the receiver has to inform the sender about this fact. This process is integrated in an electronic process. Manipulation of the TOE is not possible without destroying it. This is assured by the TOE itself which is – in this stage – already in user mode. The transport of the TOE from the distribution center to the customer is done with the same process used for the transport between the DCs.

The assessment and approvement of the used haulage companies is done by a department of the Infineon Technologies AG.

The delivery of the TOE related documentation is done from the Infineon Technologies department AE at the site Munich.

The dispatch of TOE-related components and documents (e.g. guidance documentation, applications notes, errata sheet, Security Target) are subject to regulations. This covers in particular the precise tracking and delivery only after signing a non-disclosure agreement (NDA) and explicitly ordering.

They range from delivery with regular mail to personal delivery. Most of the deliverables are classified as confidential and therefore only delivered to persons with special legitimacy.

All confidential electronic documents are delivered encrypted by using PGP tools within an already established PKI, so the confidentiality and integrity of the documentation is ensured during the whole life cycle because only the good recipient is able to decrypt the code. The detection of modification is reached by the functionality of the PGP tools. Deliverables send in paper form are personalised and only send on request by the Platform Manufacturer. This personalisation consists of a serial number which is printed as a watermark in the document. This serial number is administered by Infineon and linked to the customer the document is delivered to. Furthermore the envelopes are secured by a seal and signature.

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 an 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 by the TOE-Environment. The following topics are of relevance: (Details can be found in the PP [8], chapters 4.4 and 5.2)

- 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 SLB9665_2.0 consists of hardware and firmware components.

The hardware of the TOE consists of the following parts:

- Security Peripherals (filters, sensors),

- Core System:
  - with proprietary CPU implementation of the Intel MCS251 standard architecture from functional perspective,
  - Cache with post failure detection,
  - Memory Encryption/Decryption Unit (MED),
  - Memory Management Unit (MMU);
- Memories:
  - Read-Only Memory (ROM),
  - Random Access Memory (RAM),
  - SOLID FLASH™ NVM;
- Coprocessors:
  - Crypto2304T for asymmetric algorithms like RSA and ECC,
  - Symmetric Crypto Co-processor AES standard (SCP),
  - Hash accelerator (HASH) for the SHA-1 and SHA-256 algorithms,
  - Checksum module (CRC);
- Random number generator (RNG),
- Interrupt module (INT),
- Timer (TIM),
- Buses (BUS):
  - Memory Bus,
  - Peripheral Bus;
- Low Pin Count Interface (LPC),
- 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 TPM_FieldUpgrade command of the Trusted Platform Module Library specification.

One part is the operating system which includes the TPM application, the System Management, the Endorsement Primary Seed (EPS) and the Endorsement Keys and is used to operate the IC. The operating system includes also the capability for updating the protected capabilities once the TOE is in the field (TPM_FieldUpgrade).

The entire operating system of the TOE is comprised of:

- TPM Secure Operating System:
  - ComSys,
  - DataStore,

  - DevCtrl,
  - ECC,
  - FieldUpgrade,
  - GPIO,
  - HashSys,
  - Locality,
  - MACSys,
  - OSStartup,
  - PKcs1,
  - PowMan,
  - RandData,
  - RMSInt,
  - RSA,
  - SymEnc,
  - SysMan,
  - SysSec,
  - SelfTest,
  - TaskCtrl,
  - TimCtrl,
  - Cryptographic Library;
- OS Abstraction Layer,
- Crypto Engine,
- Platform,
- Storage,
- Support,
- TPM Commands,
- PCR,
- Authorization,
- Attack Logic,
- Command Execution Engine.

The other firmware/software parts are:

- Self Test Software (STS) stored in the especially protected test ROM,
- Service Algorithm Minimal (SAM),
- Resource Management System (RMS),

- Flash Loader.

6. Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7. IT Product Testing

The tests performed by the **developer** were divided into six categories:

- Simulation Tests (design verification):

  In the course of the development of the TOE simulation tests are carried out. These simulation tests yield CRC sums, which are used in the further testing.

- Qualification Tests:

  For each mask version a qualification test is performed. Via the results of these tests a qualification report is generated. The positive result of the qualification is one part of the necessary testing results documented with the qualification report. The qualification report is completed after the verification testing (see below) and the security evaluation (see below) are performed successfully. The tests performed and their results are listed in the qualification report. The results of the tests are the basis on which it is decided, whether the TOE is released to production.

- Verification Tests:

  With these tests in user mode the functionality in the end user environment is checked.

- Security Evaluation Tests:

  In the context of security evaluation testing the security mechanisms is tested again in the user mode only focusing on security. Here is not only verified that the security functionality is working as this was already tested on every single TOE during production, but also it is tested how well the security functionality is working and the effectiveness is calculated. This step is necessary as the mechanisms work together and that must be evaluated in the user mode.

- Production Tests:

  Before delivery on every chip production tests are performed. These tests use the CRC checksums attained by the simulation tests. The aim of these tests is to check whether each chip is functioning correctly.

- Software Tests:

  The firmware and software of the TOE is developed and tested with software tools like simulator, emulator and on hardware tools during the development phase.

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

The evaluators were able to repeat the tests of the developer, either using the tools and TOE samples delivered to the evaluator, or at the developer's site.

They performed independent tests to supplement, augment and verify the tests performed by the developer. The evaluator included all security features and related interfaces into the testing subset. For the developer tests repeated by the evaluators other test parameters were used and the test equipment was varied.

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

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

7.1. Developer's Test according to ATE_FUN

TOE test configuration:

The tests are either performed with the TOE itself, or with a simulated or emulated representation of the TOE, as appropriate for the respective test.

Developer's testing approach:

All TSF and related security mechanisms, subsystems and modules, except those that are not used by the TOE and internally blocked, are tested in order to assure complete coverage of all SFR.

Amount of developer testing performed:

The tests are performed on security mechanisms and subsystem and module level.

TOE security functionality tested:

- SF_CRY: Cryptographic Support,
- SF_I&A: Identification and Authentication,
- SF_G&T: General and Test,
- SF_OBH: Object Hierarchy,
- SF_TOP: TOE Operation.

Overall developer testing results:

The TOE has passed all tests except such tests which were waived by the developer. For these tests the developer provided a sufficient justification why the tests were waived. The evaluator analyzed the impact on the TOE and comes to the conclusion that all of these tests will not have any impact on the security and functionality of the TOE, so that all TSF has been successfully tested regarding FSP, TDS and ARC.

The developer's testing results demonstrate that the TSFs behave as specified.

7.2. Evaluator Tests

Independent Testing according to ATE_IND

The evaluator's testing effort is described as follows, outlining the testing approach, configuration, depth and results:

Testing approach:

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,
- Software tests.

With this kind of tests the entire security functionality of the TOE was tested.

All functional tests were re-performed with the TOE version v5.63.3144.02 and v5.63.3353.02 except fuzzy-tests which were performed with version v5.63.3144.02 only. The last digit 02 indicates a not certified product. For the certified product this digit is 00. The TOE version was identified by performing the TPM2_GetCapability command with TPM_CAP_TPM_PROPERTIES as capability name. The command returned the following values:

TPM_PT_MANUFACTURER = IFX, TPM_PT_VENDOR_STRING = SLB9665, TPM_PT_FIRMWARE_VERSION = 5 63 3144.02, respectively

TPM_PT_FIRMWARE_VERSION = 5 63 3353.02.

TOE test configuration:

The tests are performed with the chips Trusted Platform Module SLB9665_2.0 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 samples tested have their version numbers ending on ".02" where the last digit 02 indicates a not certified product. With the end of the certification process the version number ending becomes ".00" indicating a certified product. The entire functionality is the same for all chips.

Selection criteria:

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.

Interfaces tested:

The evaluator included all security features and related interfaces into the testing subset. Portions of the TSF and related interfaces (in brackets) tested:

- SF_CRY: Cryptographic Support (HW interfaces, External Software Interfaces),
- SF_I&A: Identification and Authentication (HW interfaces, External Software Interfaces),
- SF_G&T: General and Test (HW interfaces, External Software Interfaces).

- SF_OBH: Object Hierarchy (HW interfaces, External Software Interfaces),
- SF_TOP: TOE Operation (HW interfaces, External Software Interfaces).

Developer tests performed:

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 covers all portions of the TSF (security features) 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 evaluator's effort for penetrating testing can be summarised as follows:

Overview:

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.

Penetration testing approach:

Systematic search for potential vulnerabilities and known attacks in public domain sources, use of a list of vulnerabilities [4, AIS26], and from a methodical analysis of the evaluation documents.

Analysis 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.

TOE test configurations:

For tests of the TOE firmware the following test resources were used:

- HW: Raspberry PI 3 Model B (Revision: a02082), TOE Adapter TPM.
- SW: Raspbian GNU/Linux 8 (jessie), Python 2.7.9, TUViT TPM 2.0 TestSuite Version 1.4 (implemented in Python).

For LFI, side channel attacks and DPA measurements the following test resources were used by the evaluator in the technical security laboratory of the evaluation lab:

- Digital Oscilloscope,
- Passive Probe,
- Active Differential Probe,
- EM Probe,
- Delay Generator,
- Laser Fault Injection System,
- Proprietary measuring/analyzing software,
- Windows PC,
- Raspberry PI 3 Model B (Revision: a02082), using the same software as for tests of the TOE firmware.

Attack scenarios having been tested:

- Statistical tests of the TOE DRNG according to [4, AIS20] requirements.
- Find undocumented capabilities which are sent by the TOE as response to TPM2_GetCapabilitiy command.
- Try to circumvent access control by injecting faults through laser light (LFI attack).
- Effectiveness of the TOE security functionality.
- 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 dictionary attack counter.
- Intentional misuse of TPM commands.
- Brute force of authValues.
- Tearing on LPC communication interface.

SFRs penetration tested:

The following TSF interfaces have been tested:

- Electrical interface (INT 1.2),
- Data Interface (INT 1.3),
- SF_CRY (INT 2.1),
- SF_I&A (INT 2.2),
- SF_G&T (INT 2.3),
- SF_OBH (INT 2.4),

- SF_TOP (INT 2.5).

All security features of the TOE have been addressed by penetration testing.

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.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

Trusted Platform Module SLB9665_2.0 in version v5.63.3144.00 and v5.63.3149.00 and v5.63.3353.00 and v5.63.3355.00 as described in [6] and [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-1020-V2-2017, re-use of specific evaluation tasks was possible.

The evaluation has confirmed:

- PP Conformance: Protection Profile, TPM Library specification Family "2.0", Level 0 Revision 1.16, December 10, 2014, Version 1.0, Trusted Computing Group [8]
- for the Functionality: PP conformant plus product specific extensions 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.

Table 8 in annex C of part D lists the cryptographic functionalities inside the TOE whose cryptographic strength has not been rated.

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.

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.

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

The ECC Endorsement Key, the RSA Endorsement Key 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 by Infineon.

Moreover:

The RSA Endorsement Key (personalized during production) is generated from a proved random number generator by a Hardware Security Module outside the TOE and not derived from the Endorsement Seed.

The personalized Endorsement Keys RSA EK and ECC EK and the personalized EPS (Endorsement Primary Seed) are not visible, changeable and erasable from the user.

- In particular Annex G from [14] needs to be observed.

In addition, the following aspects need to be fulfilled when using the TOE:

- In order to fulfil the “Key Requirements” as formulated in [9], the Annex D from [14] must be followed.

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. Definitions

12.1. 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
EK	Endorsement Key
EPS	Endorsement Primary Seed
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
SAR	Security Assurance Requirement

SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

12.2. Glossary

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

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

Extension - The addition to an ST or PP of functional requirements not contained in CC part 2 and/or assurance requirements not contained in CC part 3.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Package - named set of either security functional or security assurance requirements

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

13. Bibliography

[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
http://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017,
http://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-1056-2018, Version 1.7, February 28, 2018, „Security Target, Trusted Platform Module, SLB9665_2.0“, Infineon Technologies AG (public document)

[7] Evaluation Technical Report, Version 4, March 2, 2018, ”Evaluation Technical Report Summary”, TÜV Informationstechnik GmbH, (confidential document)

[8] Protection Profile, TPM Library specification Family “2.0”, Level 0 Revision 1.16, December 10, 2014, Version 1.0, Trusted Computing Group

[9] Key Requirements on “Trusted Computing” and “Secure Boot”, by the German Federal Government, August 2012

[10] OPTIGA™ SLB 9665 TPM2.0 Databook, Version 2.9, August 1, 2017, Infineon Technologies AG

[11] OPTIGA™ SLB 9665 TPM 2.0 Errata and Updates, Version 2.3, November 3, 2017

OPTIGA™ SLB 9665 TPM 2.0 Errata and Updates, Version 2.4, February 2, 2018

[12] NIST Special Publication SP 800-108: Recommendation for Key Derivation Using Pseudorandom Functions (revised), October 2009, National Institute of Standards and Technology (NIST).

[13] NIST SP800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, (revised), May 2013, National Institute of Standards and Technology (NIST).

[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 9, 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 38, Version 2, Reuse of evaluation results

[14] OPTIGA™ TPM 2.0 Trusted Platform Module Application Note User Guidance, Revision 1.90, February 28, 2018, Infineon Technologies AG (confidential developer document)

[15] Trusted Platform Module Library Part 1: Architecture, Family “2.0”, Level 00 Revision 01.16, October 30, 2014, Trusted Computing Group (TCG).

[16] Trusted Platform Module Library Part 2: Structures, Family “2.0”, Level 00 Revision 01.16, October 30, 2014, Trusted Computing Group (TCG).

[17] Trusted Platform Module Library Part 3: Commands, Family “2.0”, Level 00 Revision 01.16, October 30, 2014, Trusted Computing Group (TCG).

[18] Trusted Platform Module Library Part 4: Supporting Routines, Family “2.0”, Level 00 Revision 01.16, October 30, 2014, Trusted Computing Group (TCG).

[19] ERRATA, Errata Version 1.5, September 21, 2016 FOR TCG Trusted Platform Module Library, Specification Version 2.0, Revision 1.16, October 30, 2014, TCG Published.

For references corresponding to cryptographic standards listed in Table 7 please refer to Annex C.

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 detailled 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 http://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-1056-2018

Evaluation results regarding development and production environment

The IT product Infineon Technologies AG Trusted Platform Module SLB9665_2.0, v5.63.3144.00, v5.63.3149.00, v5.63.3353.00, v5.63.3355.00 (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 30 April 2018, 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_LCD.1, ALC_TAT.1, ALC_FLR.1)

are fulfilled for the development and production sites of the TOE listed below:

Site ID	Company name and address	Functions of site
Development		
IFX Augsburg	Infineon Technologies AG Alter Postweg 101 86159 Augsburg Germany	Development
IFX Bangalore	Infineon Technologies India Pvt. Ltd. Mahatma Gandhi (M.G) Road No. 11, Bangalore-560001 India	Development
IFX Bucharest	Infineon Technologies Romania Blvd. Dimitrie Pompeiu Nr. 6 Sector 2 020335 Bucharest Romania	Development
IFX Milpitas	Infineon Technologies AG Chip Card and Security 640 North McCarthy Blvd Milpitas, CA 95035 USA	Development
IFX Munich	Infineon Technologies AG Am Campeon 1-12 85579 Neubiberg Germany	Development IT

Site ID	Company name and address	Functions of site
IFX Graz	Infineon Technologies Austria AG Development Center Graz Babenbergerstr. 10 8020 Graz Austria	Development
IFX Villach	Infineon Technologies Austria AG Siemensstr. 2 9500 Villach Austria	IT (Datacenter)
IFX Klagenfurt	Infineon Technologies Austria AG Lakeside B05 9020 Klagenfurt Austria	IT (Support)
IFX Melaka	Infineon Technologies Sdn. Bhd. Batu Berendam FTZ 75350, Melaka Malaysia	IT (Support)
Production		
Amkor Manila	Amkor Technology Philippines Km. 22 East Service Rd. South Superhighway Muntinlupa City 1702 Philippines	Pre-assembly Module assembly Module test
	Amkor Technology Philippines 119 North Science Avenue Laguna Technopark, Binan Laguna 4024 Philippines	
ARDT Hsin-Chu	Ardentec Corporation T site No. 3, Gungye 3rd Rd., Hsin-Chu Industrial Park, Hu-Kou, Hsin-Chu Hsien Taiwan 30351, R.O.C.	Wafer test
ARDT Singapore	Ardentec Singapore Pte. Ltd. 12 Woodlands Loop #02-00 Singapore 738283	Wafer test
DHL Singapore	DHL Exel Supply Chain Richland Business Centre 11 Bedok North Ave 4, Level 3, Singapore 489949	Distribution Center

Site ID	Company name and address	Functions of site
Disco Kirchheim	DISCO HI-TEC EUROPE GmbH Liebigstrasse 8 85551 Kirchheim Germany	Pre-assembly
DNP Agrate	DNP Photomask Europe S.p.A. Via C. Olivetti 2/A 20041 Agrate Brianza Italy	Mask production
G&D Neustadt	Giesecke & Devrient Secure Data Management GmbH Austraße 101b 96465 Neustadt bei Coburg Germany	Distribution Center
IFX Dresden	Infineon Technologies Dresden GmbH & Co. OHG Königsbrücker Str. 180 01099 Dresden Germany	Wafer production Wafer test
IFX Morgan Hill	Infineon Technologies North America Corp. 18275 Serene Drive Morgan Hill, CA 95037 USA	Inlay test Distribution
IFX Regensburg	Infineon Technologies AG Wernerwerkstraße 2 93049 Regensburg Germany	Pre-assembly Assembly Module test Scrap
IFX Singapore	Infineon Technologies Asia Pacific PTE Ltd. 168 Kallang Way Singapore 349253	Module test
IFX Wuxi	Infineon Technologies (Wuxi) Co. Ltd. No. 118, Xing Chuang San Lu Wuxi-Singapore Industrial Park Wuxi 214028, Jiangsu P.R. China	Module assembly Module test
K&N Großostheim	Kühne & Nagel Stockstädter Strasse 10 – Building 8A 63762 Großostheim Germany	Distribution Center

Site ID	Company name and address	Functions of site
K&N Hayward	Kuehne & Nagel 30805 Santana Street Hayward, CA 94544 USA	Distribution Center
Toppan Dresden	Toppan Photomask, Inc Rähnitzer Allee 9 01109 Dresden Germany	Mask production

Table 6: List of relevant TOE 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-1056-2018

Overview and rating of cryptographic functionalities implemented in the TOE

No.	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
1.	Authenticity RSA signature generation / verification	[RFC3447]	|Modulus| = 1024	no	[Main_1, B.1 – B.7] and [Main_3, 20.2]
	RSASSA-PKCS1-v1_5	according Section 8.2			
	RSASSA_PSS	according Section 8.1			
	SHA-256	[FIPS180-4]			
	SHA-1				
2.	Authenticity RSA signature generation / verification	[RFC3447]	|Modulus| = 2048	yes	[Main_1, B.1 – B.7] and [Main_3, 20.2]
	RSASSA-PKCS1-v1_5	[RFC3447, 8.2]			
	RSASSA_PSS	[RFC3447, 8.1]			
	SHA-256	[FIPS180-4]		yes	
	SHA-1			no	
3.	Authenticity EC signature generation/ verification according to	[FIPS186-4]	|k| = 256 ECC_NIST_P 256	yes	[Main_Errata, 2.29]
	ECDSA	[ISO_14888-3]			
	ECDAA	[Main_Errata, 2.29]			
	SHA-256	[FIPS180-4]		yes	
	SHA-1			no	
4.	Authenticity EC signature generation/ verification according to	[ISO_15946-5]	|k| = 256 ECC_BN_P25 6	no	[Main_Errata, 2.29]
	ECDAA	[Main_Errata, 2.29]			
	SHA-1, SHA-256	[FIPS180-4]			
5.	Authenticity RSA signature verification (RSASSA-PKCS1-v1_5)	[RFC3447] [ADV_IMP_FU]	|Modulus|= 2048	yes	TPM-FieldUpgrade
	SHA-256	[FIPS180-4]		yes	
	SHA-1			no	
6.	Authentication HMAC with SHA-1	[ISO_9797-2] [ISO_10118-3]	|k| = 160	no	[Main_1, 11.4.3]
	ECDEC	[N856, 6.1.1.2]	|k| = 256	yes	[Main_1, C7]
		[FIPS186-4]	ECC_NIST_P 256	yes	

No.	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
	RSA decryption RSAES-PKCS1-v1_5	[RFC3447, 7.2]	|Modulus| = 2048	yes	
	AES decryption in CFB mode	[ISO_18033-3], [ISO_10116]	|k| = 128	yes	
7.	Authentication HMAC with SHA-256	[ISO_9797-2], [ISO_10118-3]	|k| = 256	yes	[Main_1, 11.4.3]
	ECDEC	[N856, 6.1.1.2]	|k| = 256		[Main_1, C7]
		[FIPS186-4]	ECC_NIST_P 256		
	RSA decryption RSAES-PKCS1-v1_5	[RFC3447, 7.2]	|Modulus| = 2048		
	AES decryption in CFB mode	[ISO_18033-3], [ISO_10116]	|k| = 128		
8.	Key Agreement Diffie-Hellmann (ECDH)	[N856, 6.1.1.2] [FIPS186-4]	|k| = 256 ECC_NIST_P 256	yes	[Main_1, 11.4.9.3]
	KDFe	[N856]			[Main_1, C7]
	HMAC with SHA-256 and	[ISO_9797-2], [ISO_10118-3]	|k| = 256		
	SHA-1		|k| = 160		
9.	Key Agreement KDFa	[Main_1, 11.4.9.1], [N808]	|Modulus| = 2048	yes	[Main_1, 11.4.9.1]
	HMAC with SHA-256 and	[ISO_9797-2], [ISO_10118-3]	|k| = 256		
	SHA-1		|k| = 160		
10.	Key Agreement HMAC with SHA-256	[ISO_9797-2], [FIPS180-4] [N808], [ADV_IMP_FU]	|k| = 256	yes	TPM-FieldUpgrade
11.	Integrity HMAC with SHA-256 and	[ISO_9797-2], [ISO_10118-3]	|k| = 256	yes	[Main_1, 11.4.3]
	SHA-1		|k| = 160	no	
12.	Integrity HMAC with SHA-256	[ISO_9797-2], [ISO_10118-3], [N808], [ADV_IMP_FU]	|k| = 256	yes	TPM-FieldUpgrade
13.	Confidentiality AES in CFB mode	[ISO_18033-3], [ISO_10116]	|k| = 128	yes	[TPM]
14.	Confidentiality RSA encryption / decryption	[RFC3447]	|Modulus| = 1024	no	[Main_1, B.1 – B.7]
	RSAES-PKCS1-v1_5	[RFC3447, 7.2]			[Main_3, 14]
	RSAES-OAEP	[RFC3447, 7.1]			

No.	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
15.	Confidentiality RSA encryption / decryption	[RFC3447]	|Modulus| = 2048	yes	[Main_1, B.1 – B.7]
	RSAES -PKCS1-v1_5	[RFC3447, 7.2]			[Main_3, 14]
	RSAES-OAEP	[RFC3447, 7.1]			
16.	Confidentiality AES in PCBC mode	[ISO_18033-3], [N808], [ADV_IMP_FU]	|k| = 128	yes	TPM-FieldUpgrade
17.	Cryptographic Primitive SHA-256	[FIPS180-4]	none	yes	[Main_1, 11.4.2]
18.	Cryptographic Primitive SHA-1	[FIPS180-4]	none	no	[Main_1, 11.4.2]
19.	Cryptographic Primitive HMAC with SHA-1	[ISO_9797-2], [ISO_10118-3]	|k| = 160	no	[Main_1, 11.4.3]
20.	Cryptographic Primitive HMAC with SHA-256	[ISO_9797-2], [ISO_10118-3]	|k| = 256	yes	[Main_1, 11.4.3]
21.	Cryptographic Primitive Deterministic RNG DRG.3	[AIS20], [N890]	CTR_DRGB implemented	yes	[Main_1, 11.4.10]
22.	Trusted Channel HMAC with SHA-256	[ISO_9797-2], [ISO_10118-3]	|k| = 256	yes	[TPM]
23.	Trusted Channel AES in CFB mode	[ISO_18033-3], [ISO_10116]	|k| = 128	yes	[TPM]
	RSA	[RFC3447], [ISO_15946-1], [N808]	|k| = 1024, |k| = 2048	no yes	
	ECC	[FIPS186-4]	ECC_NIST_P256, |k| = 256		
	HMAC (SHA-256)	[ISO_9797-2], [ISO_10118-3]	|k| = 256		
24.	Key Generation ECC primary keys	[Main_1, C.5 / C.6 / C.8], [N808], [ISO_15946-1, 6.1] (not Section 6.1.1)	|k| = 256		–
	ECC_NIST_P256	[FIPS186-4]		yes	
	ECC_BN_P256	[ISO_15946-5]		no	
25.	Key Generation ECC	[Main_1, C.5 / C.8], [N808], [ISO_15946-1, 6.1] (not Section 6.1.1)	|k| = 256		–
	ECC_NIST_P256	[FIPS186-4]		yes	
	ECC_BN_P256	[ISO_15946-5]		no	
26.	Key Generation AES	[TPM], [N8133], [N808]	|k| = 128	yes	–

Table 7: TOE cryptographic functionality

Reference of Legislatives and Standards specified in Table 7 above:

[FIPS180-4] *FIPS PUB 180-4 Federal Information Processing Standards Publication Secure Hash Standard (SHS),* August 2015, Information Technology Laboratory National Institute of Standards and Technology.

[FIPS186-4] *Federal Information Processing Standards Publication FIPS PUB 186-4, Digital Signature Standard (DSS),* July 2013, 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*, 2003, 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_15946-1] *ISO 15946-1: Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General*, 2002, 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*, 2010, ISO/IEC.

[ISO_9797-2] *Information technology - Security techniques- Message Authentication Codes (MACs) - Part 2: Mechanisms using a dedicated hash-function*, 2011-06, ISO/IEC.

[Main_1] *Trusted Platform Module Library Part 1: Architecture, Family "2.0", Level 00 Revision 01.16*, 2014-10-30, Trusted Computing Group (TCG).

[Main_2] *Trusted Platform Module Library Part 2: Structures, Family "2.0", Level 00 Revision 01.16*, 2014-10-30, Trusted Computing Group (TCG).

[Main_3] *Trusted Platform Module Library Part 3: Commands, Family "2.0", Level 00 Revision 01.16*, 2014-10-30, Trusted Computing Group (TCG).

[Main_4] *Trusted Platform Module Library Part 4: Supporting Routines, Family "2.0", Level 00 Revision 01.16*, 2014-10-30, Trusted Computing Group (TCG).

[Main_Errata] *ERRATA, Errata Version 1.5, September 21, 2016 FOR TCG Trusted Platform Module Library,* Specification Version 2.0, Revision 1.16, October 30, 2014, TCG Published.

[N808] *NIST Special Publication SP 800-108: Recommendation for Key Derivation Using Pseudorandom Functions* (revised), October 2009, National Institute of Standards and Technology (NIST).

[N8133] NIST Special Publication 800-133, *Recommendation for Cryptographic Key Generation;* December 2012

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

[N890] *NIST Special Publication 800-90A: Recommendation for Random Number Generation Using Deterministic Random Bit Generators*. January 2012, National Institute of Standards and Technology (NIST).

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

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

For the Cryptographic Functionality TPM_RSAGEN1 used in conjunction with “Key Generation RSA Primary Keys” and “Key Generation RSA” listed in Table 8 below no statement on the respective cryptographic strength can be given:

No.	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Comments
1.	Key Generation RSA primary keys	[TPM], TPM_RSAGEN1, [N808]	|k| = 2048	TPM_RSAGEN1 is a proprietary Infineon prime number generation method
2.	Key Generation RSA	[TPM], TPM_RSAGEN1	|k| = 1024 |k| = 2048	TPM_RSAGEN1 is a proprietary Infineon prime number generation method

Table 8: TOE cryptographic functionality not rated

Note: End of report