Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0958-V2-2017

for

Infineon Technologies AG Trusted Platform Module SLB9670_1.2 v6.43.0243.00, v6.43.0244.00, v6.43.0245.00 and v6.43.0246.00

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-0958-V2-2017 (*)

Trusted Platform Module

Infineon Technologies AG Trusted Platform Module SLB9670_1.2 v6.43.0243.00, v6.43.0244.00, v6.43.0245.00 and v6.43.0246.00

from	Infineon Technologies AG
PP Conformance:	Trusted Computing Group Protection Profile, PC Client specific Trusted Platform Module TPM Family 1.2; Level 2, Revision 116, Version 1.3, 14 July 2014, BSI-CC-PP-0030-2008-MA-02
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

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 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 for components up to EAL 4

Bonn, 8 August 2017

For the Federal Office for Information Security

Bernd Kowalski
Head of Department

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.

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.

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

Contents

A. Certification

1. 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[2]
- BSI Certification and Approval Ordinance[3]
- BSI Schedule of Costs[4]
- 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[5] [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]

2. 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.

2.1. European Recognition of ITSEC/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.

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

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

[4] 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

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

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). 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 new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. 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 nations listed above.

This certificate is recognized under SOGIS-MRA for all assurance components selected.

2.2. 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 CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification) of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

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 nations listed above.

As this certificate is a re-certification of a certificate issued according to CCRA-2000 this certificate is recognized according to the rules of CCRA-2000, i.e. up to and including CC part 3 EAL 4 components. The evaluation contained the components ALC_FLR.1 and AVA_VAN.4 that are not mutually recognised in accordance with the provisions of the CCRA-2000, for mutual recognition the EAL 4 components of these assurance families are relevant.

3. 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 SLB9670_1.2 v6.43.0243.00, v6.43.0244.00, v6.43.0245.00 and v6.43.0246.00 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0958-2015. Specific results from the evaluation process BSI-DSZ-CC-0958-2015 were re-used.

The evaluation of the product Infineon Technologies AG Trusted Platform Module SLB9670_1.2 v6.43.0243.00, v6.43.0244.00, v6.43.0245.00 and v6.43.0246.00 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 1 August 2017. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] 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.

4. Validity of the Certification Result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only 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 levels please refer to the excerpts from the criteria at the end of the Certification Report or in the CC itself.

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-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 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 8 August 2017 is valid until 7 August 2022. 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

[6] Information Technology Security Evaluation Facility

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

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

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

5. Publication

The product Infineon Technologies AG Trusted Platform Module SLB9670_1.2 v6.43.0243.00, v6.43.0244.00, v6.43.0245.00 and v6.43.0246.00 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[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] Infineon Technologies AG
Am Campeon 1-12
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 SLB9670_1.2” (or SLB9670_1.2 in short), versions v6.43.0243.00, v6.43.0244.00, v6.43.0245.00 and v6.43.0246.00, including related guidance documentation as described in the Security Target. The versions v6.43.0243.00 and v6.43.0244.00 and v6.43.0245.00 and v6.43.0246.00 include the identical source code, where the v6.43.0244.00 and v6.43.0245.00 and v6.43.0246.00 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 as defined in the TPM Main Specification. The SLB9670_1.2 is a complete solution implementing the TCG TPM Main Specification, Version 1.2, Revision 116, and the TCG PC Client Specific TPM Interface Specification (TIS), Version 1.3.

The SLB9670_1.2 uses the Serial Peripheral Interface (SPI) for the integration into existing PC mainboards. The SLB9670_1.2 is basically a secure controller with the following added functionality:

- Random number generator (DRBG),
- Asymmetric key generation (RSA keys with key length up to 2048 bit),
- Symmetric key generation (AES keys, for internal use only),
- Symmetric and asymmetric key procedures (encryption/decryption, generation and verification of digital signatures),
- Hash algorithms (SHA-1) and MAC (HMAC),
- Secure key and data storage,
- Identification and Authentication mechanisms,
- Tick and Monotonic Counter.

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

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Trusted Computing Group Protection Profile, PC Client specific Trusted Platform Module TPM Family 1.2; Level 2, Revision 116, Version 1.3, 14 July 2014, BSI-CC-PP-0030-2008-MA-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 7.1. 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	Authentication and Identification
SF_ACC	Access Control
SF_GEN	General
SF_P&T	Protection and Test

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.

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 SLB9670_1.2 v6.43.0243.00, v6.43.0244.00, v6.43.0245.00 and v6.43.0246.00.

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	SLB9670_1.2 Security IC with integrated firmware and operating system	v6.43.0243.00, v6.43.0244.00, v6.43.0245.00 and v6.43.0246.00	Packaged module
2	DOC	Trusted Computing Group TPM Main Specification [16] including: TPM Main Part 1 Design Principles, TPM Main Part 2 TPM Structures, TPM Main Part 3 Commands	Version 1.2, Revision 116	Public document, downloadable from https://www.trustedcomputinggroup.org
3	DOC	TCG PC Client Specific TPM Interface Specification (TIS) [12]	Version 1.3	Hardcopy and pdf-file
4	DOC	OPTIGA™ TPM SLB 9670 TPM1.2 Databook [13]	Revision 1.9	Hardcopy and pdf-file

No	Type	Identifier	Release	Form of Delivery
5	DOC	TPM Trusted Platform Module Version 1.2, Application Note Basic Platform Manufacturer Guideline [14]	Version 1.00	Hardcopy and pdf-file
6	DOC	OPTIGA™ TPM SLB 9670 TPM1.2 Errata and Updates [15]	Revision 1.9	Hardcopy and pdf-file

Table 2: Deliverables of the TOE

TOE identification

The TOE is identified by identifiers of the product and version numbers for the hardware and firmware as listed in the following table.

Type	Name	Version number
Target of Evaluation	SLB9670_1.2	
Firmware		v6.43.0243.00, v6.43.0244.00, v6.43.0245.00 and v6.43.0246.00

Table 3: Version number of hardware and firmware parts of the TOE

The fabricated modules are physically labelled with the TOE reference by printing. The labelling consists of three lines, which differ depending on the package [13, 6.3]:

Line	Content	Remark
1	SLB9670	
2	VQ12 <yy>	<yy> is an internal FW indication (only at manufacturing due to field upgrade option)
3	XXH <xxxxr>	<Lot number> H <datecode>

Table 4: Labelling of TOE module (VQFN)

The TPM version and the firmware version can be read out electronically with the command TPM_GetCapability, which is described in [13, 4.7.4].

TOE Delivery

The TOE or parts of it are delivered between the following two parties:

- The TPM developer (identical to the TOE developer / manufacturer) comprises all roles before TOE delivery,
- the authorized user (i.e. the platform manufacturer and the application developer) comprises all relevant roles after TOE delivery.

The following different delivering procedures have to be taken into consideration:

- Internal delivery among the several TOE manufacturer sites themselves,
- Delivery of the final TOE from the TOE Manufacturer to the Platform Manufacturer,
- Delivery of documentation accompanying the final TOE from the TOE manufacturer.

The internal delivery procedures of the TOE Manufacturer comprise all deliverables among the several TOE Manufacturer sites themselves. These deliverables consist of electronic as well as paper documents and physical items like wafers or masks. The corresponding security procedures guarantee an integer and confidential transfer. These internal procedures are evaluated within the ALC_DVS evaluation activity.

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 digital signature (generation and verification), data encryption and decryption, key destruction, the generation of hash values and the generation and verification of MAC values.
- Authentication and Identification: The TPM provides four protocols for authentication and identification to authorize the use of entities without revealing the authorization data (AuthData) on the network or the connection to the TPM. The basic premise is to prove knowledge of a shared secret.
- Access Control: TPM Mode Control, Delegation, Key Management, Key Migration, Measurement and Reporting, Non-volatile Storage, Monotonic Counter, Export and Import of Data, and Direct Anonymous Attestation Protocol.
- General: Operational Roles, management of operational modes, delegation tables, security attributes, and security flags.
- Protection and Test: Preserving of a secure state in case of a failure, self tests during start-up and on demand, resistance to physical manipulation and probing.

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:

- 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 authorized user.
- 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.
- The developer of the host platform must ensure that physical presence indicated to the TOE implies interaction by an operator and is difficult or impossible to spoof by rogue software or remote attackers.
- The IT environment must protect the integrity of sealed data blobs.
- The IT environment must create EK and AIK credentials by trustworthy procedures for the root of trust for reporting.
- 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.
- The DAA issuer must support a procedure for attestation without revealing the attestation information based on the Direct Anonymous Attestation Protocol.

Details can be found in the Security Target [6], chapter 5.2.

5. Architectural Information

The SLB9670_1.2 consists of hardware and firmware components.

The TOE consists of the following hardware:

- 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),
  - EEPROM Flash memory,
- Coprocessors,
  - Crypto2304T for asymmetric algorithms like RSA,
  - Symmetric Crypto Co-processor AES standard (SCP),
  - Hash accelerator (HASH) for the algorithms SHA-1,
  - Checksum module (CRC),
- Random number generator (RNG),
- Interrupt module (INT),
- Timer (TIM),
- Buses (BUS),
  - AXI™ Memory Bus,
  - APB Peripheral B,
- Serial Peripheral Interface (SPI),
- Tick Counter.

The firmware of the TOE consists of two parts. One part consists of the Self Test Software (STS), the Service Algorithm Minimal (SAM), the Resource Management System (RMS) and the Flash Loader. The STS routines are stored in the especially protected test ROM and are not accessible for the user software (application).

The other firmware part is the operating system and is comprised of:

- Communication System,
- System Management including:

  - GPIO System,
  - Crypto,
  - Locality System,
  - PKCS#1,
  - RND (DRNG),
  - RMS Int,
  - OS Startup,
  - Control,
  - System Selftest,
  - Security System,
  - Data & Power,
  - Field Upgrade,
- Transportation,
- TPM-Dispatcher,
- System Startup,
- State-Machine,
- Authorization,
- Dictionary Attack Logic,
- TPM-Command,
- TcpaFlags,
- Locality,
- Test,
- RSA2048,
- Memory Components,
- AES,
- Archive,
- Tick Counter,
- PCR,
- Key Class,
- FW-Upgrade,
- DAA.

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

The developer’s testing effort can be summarised as follows:

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 one module that is 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_ACC: Access Control (HW interfaces, External Software Interfaces),
- SF_GEN: General (HW interfaces, External Software Interfaces),
- SF_P&T: Protection and Test (HW interfaces, External Software Interfaces).

Overall developer testing results:

The TOE has passed all tests defined in the developer’s test plan so that all TSF has been successfully tested against FSP, TDS and ARC.

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

7.2. Evaluator Testing

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 performed with the TOE version v6.43.0243.02 where 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 TPM_GetCapability command with TPM_CAP_VERSION_VAL as capability name. The command returned the following values:

- Version = 1.2.6.43,
- tpmVendorID = IFX,
- vendorSpecific (including TOE software version) = 6.43.243.02 tpms10.

TOE test configuration:

The tests are performed with the chips Trusted Platform Module SLB9670_1.2 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 except the version number. The samples tested have the version number v6.43.0243.02 where the last digit 02 indicates a not certified product. With the end of the certification process the version number becomes v6.43.0243.00 indicating a certified product. There are no other differences between the configuration delivered to the user and the configuration tested. The versions v6.43.0243.00 and v6.43.0244.00 and v6.43.0245.00 and v6.43.0246.00 include the identical source code, where the versions v6.43.0244.00 and v6.43.0245.00 and v6.43.0246.00 are used for field upgrade, therefore the test results of the tested configuration are also applicable to the configuration delivered to the user. The others chip types contain special download functionality for test programs or have some security mechanisms deactivated.

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_ACC: Access Control (HW interfaces, External Software Interfaces),
- SF_GEN: General (HW interfaces, External Software Interfaces),

- SF_P&T: Protection and Test (HW interfaces, External Software Interfaces).

Developer tests performed:

The evaluator has re-implemented and performed a subset of developer's test cases including at least one test case for each TOE Security Feature.

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.

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:

- Raspberry PI 3 Model B (Revision: a02082),
- TOE Adapter TPM,
- 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,
- Card Reader: Infineon Generic Transparent Reader Signal Generator,
- Delay Generator,
- Laser Fault Injection System,
- Proprietary measuring/analyzing software,
- Standard PC.
- Attack scenarios having been tested:
- Statistical tests of the TOE TRNG and DRNG random number generators according to [4, AIS20] and [4, AIS31] requirements.
- Find undocumented capabilities which are sent by the TOE as response to TPM_GetCapabilitiy command.
- Try to circumvent access control by injecting faults through laser light (LFI attack).
- Buffer overflow attack through sending commands with correct layout, but randomly filled, to the TOE.
- 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.

SFRs penetration tested:

The SFRs accessible via 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_ACC (INT 2.3),
- SF_GEN (INT 2.4),
- SF_P&T (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 SLB9670_1.2 in version v6.43.0243.00, v6.43.0244.00, v6.43.0245.00 and v6.43.0246.00 as described in [6], [13] and [15].

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.

The following guidance specific for the technology was used:

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

(ii) Evaluation Methodology for Hardware Integrated Circuits.

(see [4], AIS 25 and AIS 26). 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-0958-2015, re-use of specific evaluation tasks was possible.

The evaluation has confirmed:

- PP Conformance: Trusted Computing Group Protection Profile, PC Client specific Trusted Platform Module TPM Family 1.2; Level 2, Revision 116, Version 1.3, 14 July 2014, BSI-CC-PP-0030-2008-MA-02 [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 following cryptographic algorithms are used by the TOE to enforce its security policy:

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application
Authenticity	RSA signature generation / verification (RSASSA-PKCS1-v1_5)	[PKCS#1]	|Modulus| = 512, 1024, 2048	TPM [16]
Authentication	HMAC with SHA-1	[RFC2104], [FIPS180-4]	|k| = 160	TPM [16]
Key Agreement	RSA decryption (RSAES-OAEP)	[PKCS#1]	|Modulus|=512, 1024, 2048	TPM [16]
Integrity	HMAC with SHA-1	[RFC2104], [FIPS180-4]	|k| = 160	TPM [16]
Confidentiality	AES in CBC and CTR mode	[FIPS197], [SP800-38A]	|k| = 128	TPM [16]
	RSA encryption / decryption (RSAES- OAEP, RSAES-PKCS1-v1_5)	[PKCS#1]	|Modulus| = 512, 1024, 2048	TPM [16]
	MGF1	[PKCS#1], TPM [16]	|k| = 160	TPM [16]
Cryptographic Primitive	SHA-1	[FIPS180-4]	None	TPM [16]
	Deterministic RNG DRG.3	[4, AIS20]	None	TPM [16]
Trusted Channel	Transport Session	TPM [16]	n.a.	TPM [16]
	OIAP	TPM [16]	n.a.	TPM [16]
	OSAP	TPM [16]	n.a.	TPM [16]
	DSAP	TPM [16]	n.a.	TPM [16]

Table 5: TOE cryptographic functionality (Part I)

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2).

According to [16] the algorithms are suitable for authenticity, authentication, key agreement, integrity and confidentiality. An explicit validity period is not given.

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).

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).

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
Authenticity	RSA signature verification (RSASSA-PKCS1-v1_5)	[PKCS#1], [FUP]	|Modulus|= 2048	yes	TPM-FieldUpgrade
Key Derivation	KDF based on HMAC with SHA-256	[RFC2104], [FIPS180-4], [SP800-108], [FUP]	|k| = 256	yes	TPM-FieldUpgrade
Integrity	HMAC with SHA-256	[RFC2104], [FIPS180-4], [SP800-108], [FUP]	|k| = 256	yes	TPM-FieldUpgrade
Confidentiality	AES in CBC mode	[FIPS197], [SP800-38A], [FUP]	|k| = 128	yes	TPM-FieldUpgrade

Table 6: TOE cryptographic functionality (Part II)

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.

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.

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
EEPROM	Electrically Erasable Programmable Read Only Memory
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
SPI	Serial Peripheral Interface
ST	Security Target
TOE	Target of Evaluation
TPM	Trusted Platform Module
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 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012
http://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012, 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[8] 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-0958-V2-2017, Version 1.3, 14 July 2017, Security Target, Trusted Platform Module, SLB9670_1.2, Infineon Technologies AG

[7] Evaluation Technical Report, Version 2, 31 July 2017, Evaluation Technical Report Summary, TÜV Informationstechnik GmbH – Evaluation Body for IT Security, (confidential document)

[8] Trusted Computing Group Protection Profile, PC Client specific Trusted Platform Module TPM Family 1.2; Level 2, Revision 116, Version 1.3, 14 July 2014, BSI-CC-PP-0030-2008-MA-02

[9] TPM Main Part 1 Design Principles, Specification Version 1.2, Revision 116, 1 March 2011, Trusted Computing Group Inc.

[10] TPM Main Part 2 TPM Structures, Specification Version 1.2, Revision 116, 1 March 2011, Trusted Computing Group Inc.

[11] TPM Main Part 3 Commands, Specification Version 1.2, Revision 116, 1 March 2011, Trusted Computing Group Inc.

[8] 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 38, Version 2, Reuse of evaluation results

[12] TCG PC Client Specific TPM Interface Specification (TIS), Version 1.3, 21 March 2013, Trusted Computing Group Inc.

[13] OPTIGA™ TPM SLB 9670 TPM1.2 Databook, Version 1.9, 27 June 2017, Infineon Technologies AG

[14] TPM Trusted Platform Module Version 1.2, Application Note Basic Platform Manufacturer Guideline, Version 1.00, September 2014, Infineon Technologies AG

[15] OPTIGA™ TPM SLB 9670 TPM1.2 Errata and Updates, Version 1.9, 14 July 2017, Infineon Technologies AG

[16] Trusted Computing Group TPM Main Specification, consisting of [9], [10] and [11]

[17] Implementation standards:

[P1363] IEEE P1363-2000, Standard Specifications for Public Key Cryptography, Institute of Electrical and Electronics Engineers, Inc.

[PKCS#1] PKCS #1, RSA Cryptography Standard, v2.0, 01 October 1998, RSA Laboratories

[RFC2104] RFC 2104, HMAC: Keyed-Hashing for Message Authentication, http://www.ietf.org/rfc/rfc2104.txt

[FIPS180-4] Federal Information Processing Standards Publication FIPS PUB 180 4, Secure Hash Standard (SHS), March 2012, Information Technology Laboratory National Institute of Standards and Technology

[FIPS197] Federal Information Processing Standards Publication 197, 26 November 2001, Announcing the ADVANCED ENCRYPTION STANDARD (AES), National Institute of Standards and Technology

[SP800-38A] NIST Special Publication 800-38A, 2001 Edition, Recommendation for Block Cipher Modes of Operation Methods and Techniques

[FUP] TPM-FieldUpgrade 16baff5, Doxygen documentation, 05 March 2015, Infineon Technologies AG

[SP800-108] NIST Special Publication SP 800-108, October 2009, Recommendation for Key Derivation Using Pseudorandom Functions

This page is intentionally left blank.

C. Excerpts from the Criteria

CC Part 1:

Conformance Claim (chapter 10.4)

“The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - **CC Part 3 extended** - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model

Assurance Class	Assurance Components
	ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next Section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC Part 3. More precisely, each EAL includes no more than one

component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.

Evaluation assurance level 1 (EAL 1) - functionally tested (chapter 8.3)

“Objectives

EAL 1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL 1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL 1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL 1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.”

Evaluation assurance level 2 (EAL 2) - structurally tested (chapter 8.4)

“Objectives

EAL 2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time.

EAL 2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL 3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL 3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL 3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering."

Evaluation assurance level 4 (EAL 4) - methodically designed, tested, and reviewed (chapter 8.6)

"Objectives

EAL 4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL 4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL 4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs."

Evaluation assurance level 5 (EAL 5) - semiformally designed and tested (chapter 8.7)

"Objectives

EAL 5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL 5 assurance. It is likely that the additional costs attributable to the EAL 5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL 5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques."

Evaluation assurance level 6 (EAL 6) - semiformally verified design and tested (chapter 8.8)

"Objectives

EAL 6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL 6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs."

Evaluation assurance level 7 (EAL 7) - formally verified design and tested (chapter 8.9)

"Objectives

EAL 7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL 7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis."

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

“Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

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

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0958-V2-2017

Evaluation results regarding development and production environment

The IT product Infineon Technologies AG Trusted Platform Module SLB9670_1.2 v6.43.0243.00, v6.43.0244.00, v6.43.0245.00 and v6.43.0246.00 (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 8 August 2017, 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 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)

Site ID	Company name and address	Functions of site
IFX Bangalore	Infineon Technologies India Pvt. Ltd. Kalyani Platina, Sy. No. 6 & 24 Kundanahalli Village Krishnaraja Puram Hobli Bangalore India – 560066 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	• Development
IFX Munich	Infineon Technologies AG Am Campeon 1-12 85579 Neubiberg Germany	• Development • IT
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

Site ID	Company name and address	Functions of site
DHL Singapore	DHL Exel Supply Chain Richland Business Centre 11 Bedok North Ave 4, Level 3, Singapore 489949	• Distribution Center Asia (DC-A)
Disco Kirchheim	DISCO HI-TEC EUROPE GmbH Liebigstrasse 8 D-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 Nitra	Giesecke & Devrient Slovakia, s.r.o. Dolné Hony 11 94901 Nitra Slovakia	• 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 • IT
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 • Distribution Center China (DC-C)

Site ID	Company name and address	Functions of site
K&N Großostheim	Infineon Technology AG Distribution Center Europe (DCE) Kühne & Nagel Stockstädter Strasse 10 – Building 8A 63762 Großostheim Germany	• Distribution Center Europe (DC-E)
K&N Hayward	Kuehne & Nagel 30805 Santana Street Hayward, CA 94544 USA	• Distribution Center USA (DC-U)
Toppan Dresden	Toppan Photomask, Inc (AMTC) Rähnitzer Allee 9 01109 Dresden Germany	• Mask production

Table 7: Relevant development and production 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.