Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0844-2014

for

SLB96xx

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-0844-2014

Trusted Platform Module

SLB96xx

from	Infineon Technologies AG
PP Conformance:	PC Client Specific Trusted Platform Module Family 1.2; Level 2, Revision 116, Version 1.2, 6 October 2011, BSI-CC-PP-0030-2008-MA-01
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented with ALC_FLR.1 and AVA_VAN.4

Common Criteria
Recognition
Arrangement
for components up
to EAL 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 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

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.

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.

Bonn, 28 February 2014

For the Federal Office for Information Security

Joachim Weber
Head of Division

L.S.

SOGIS Recognition
Agreement

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....................7

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

B Certification Results....................11

1 Executive Summary....................12
2 Identification of the TOE....................13
3 Security Policy....................14
4 Assumptions and Clarification of Scope....................14
5 Architectural Information....................15
6 Documentation....................16
7 IT Product Testing....................16
8 Evaluated Configuration....................17
9 Results of the Evaluation....................17
10 Obligations and Notes for the Usage of the TOE....................20
11 Security Target....................20
12 Definitions....................20
13 Bibliography....................22

C Excerpts from the Criteria....................25

CC Part 1:....................25
CC Part 3:....................26

D Annexes....................35

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- 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 technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic). In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

[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 a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

[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

As of September 2011 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. Details on recognition and the history of the agreement can be found at https://www.bsi.bund.de/zertifizierung.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

2.2 International Recognition of CC – Certificates (CCRA)

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of September 2011 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. 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.

This evaluation contains the components ALC_FLR.1 and AVA_VAN.4 that are not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL4 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 SLB96xx has undergone the certification procedure at BSI.

The evaluation of the product SLB96xx was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 24. January 2014. 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,

[6] Information Technology Security Evaluation Facility

- 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.

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 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 SLB96xx 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
Alter Postweg 101
86159 Augsburg

This page is intentionally left blank.

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 TOE is a Security IC with integrated firmware (operating system) and guidance documentation ([9], [10], [11], [12], [13], [14]), which is named SLB96xx, internally registered under the development code v04.40.0119.00.

The TOE (SLB96xx) comprises different derivates. The hardware and the firmware/software of the derivates are identical. The only difference between the derivates is the temperature range, the packaging and the own intermediated IFX certificate. The derivates are listed in the document TPM Trusted Platform Module Version 1.2 SLB9660 Errata and Updates [13]. There is no impact on the security policy of the TOE.

The SLB96xx Trusted Platform Module, called TPM or SLB96xx in the following text, 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 SLB96xx is a complete solution implementing the version 1.2 of the TCG Trusted Platform Module Main, Specification Version 1.2 [16] and the TCG PC Client Specific TPM Interface Specification, Version 1.21 Final, Revision 1.00 [12].

The SLB96xx is basically a secure controller with the following added functionality:

- Random number generator (DRNG)
- 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 Security Target [6] is the basis for this certification. It is based on the certified Protection Profile PC Client Specific Trusted Platform Module Family 1.2; Level 2, Revision 116, Version 1.2, 6 October 2011, BSI-CC-PP-0030-2008-MA-01 [7].

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

SLB96xx

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	SLB96xx Security IC with integrated firmware (operating system)	FW v04.40.0119.00	Packaged module
2	DOC	Trusted Computing Group TPM Main Specification [16]	Version 1.2, Revision 116	Hardcopy and pdf-file
3	DOC	TCG PC Client Specific TPM Interface Specification (TIS) for TPM Family 1.2; Level 2 [12]	Version 1.21 FINAL, Revision 1.00	Hardcopy and pdf-file
4	DOC	TPM Trusted Platform Module SLB9660 TCG Rev 116 Databook including Errata and Updates for TPM V1.2 SLB9660 (Revision 1.3, 2013-10-25) [13]	Version 1.1	Hardcopy and pdf-file

No	Type	Identifier	Release	Form of Delivery
5	DOC	TPM Trusted Platform Module Version 1.2 SLB9660 Application Note Basic Platform Manufacturer Guideline [14]	Version 1.00	Hardcopy and pdf-file

Table 2: Deliverables of the TOE

The user identifies the evaluated TOE by the data code printed on the chip package (cf. [13], 6.3 / 7.3) and the FW version “04.40.0119.00”, which can be read out as described in the guidance documentation (cf. [14], Annex D).

The TOE or parts of it are delivered between the following two parties (defined in [7]):

- TOE Manufacturer (comprises all roles before TOE delivery)
- Platform Manufacturer (comprises all roles after TOE delivery)

Therefore two different delivering procedures have to be taken into consideration as described in (cf. [15], 6.2):

- 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 enforcement of user access to cryptographic IT assets in accordance with the following security function policies (SFP):

- TPM Mode Control SFP (MCT-SFP),
- Delegation (Del-SFP),
- Key Management SFP (KeyM-SFP),
- Key Migration SFP (Kmig-SFP),
- Measurement and Reporting SFP (M&R-SFP),
- Non-volatile Storage SFP (NVS-SFP),
- Monotonic Counter SFP (MC-SFP),
- Export and Import of Data SFP (EID-SFP) and
- Direct Anonymous Attestation Protocol SFP (DAA-SFP)

to meet the security functional requirements. These policies include different operational roles, subjects, objects and operations which are described in [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.
- 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.
- The IT environment must protect the integrity of sealed data blobs.
- The IT environment must create credentials by trustworthy procedures.
- 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 Direct Anonymous Attestation (DAA) Protocol issuer must support a procedure for attestation without revealing the attestation information based on the DAA Protocol.

Details can be found in the Security Target [6] chapter 4.3 and the Protection Profile [7] chapter 4.3.

5 Architectural Information

The Target of Evaluation (TOE) is the SLB96xx consisting of the following hardware and firmware components.

The hardware of the SLB96xx is based on the SLE70-Family architecture with additional components and is manufactured by the Infineon Technologies AG.

The IC consists of a dedicated microprocessor (CPU) with a MMU (Memory Management Unit), several different memories, security logic, shield, a timer, an interrupt-controlled I/O interface and a RNG (Random Number Generator). Additionally, a hardware hash accelerator and a specialized interface, the Low Pin Count interface (LPC), have been added. This LPC interface is the main interface of the chip.

The CPU is a real 16-bit CPU-architecture and is compatible to the Intel 80251 architecture. The major components of the core system are the CPU (Central Processing Unit), the MMU (Memory Management Unit) and MED (Memory Encryption/Decryption Unit). The CPU control each other in order to detect faults and serve by this for data integrity. The TOE implements a full 16 MByte linear addressable memory space for each privilege level, a simple scalable Memory Management concept and a scalable stack size. The flexible memory concept consists of ROM- and Flash-memory as part of the non volatile memory (NVM), respectively EEPROM. For the EEPROM memory the Unified Channel Programming (UCP) memory technology is used.

The SLB96xx uses an external clock of 33 MHz which is compliant to the definition of the LPC interface. The PLL unit allows operating the core controller of the SLB96xx with a multiplication factor over the divided external clock signal or free running with maximum frequency. The checksum module allows simple calculation of checksums per ISO 3309 (16 bit CRC).

Three modules for cryptographic operations are implemented on the TOE. The two cryptographic co-processors serve the needs of modern cryptography:

- The symmetric co-processor (SCP) for AES hardware acceleration.
- The Asymmetric Crypto Co-processor, called Crypto2304T in the following, is used for RSA-2048 bit (4096-bit with CRT).
- The third module named HASH provides the Secure Hash Algorithm-1 (SHA-1).

The firmware required for operating the chip includes an operating system that provides the TCG functionality specified in the TPM Main Specification. The chip initialisation routine with security checks and identification mode as well as test routines for production testing is 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 TPM Main Specification. The field upgrade can only be downloaded to the chip if it has been encrypted and signed by the manufacturer Infineon Technologies AG.

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 configuration under evaluation has the identification SLB96xx (cf. [13], 6.3 and [14], Annex D). The test configuration, in particular the test environment, is described in detail within the documents [18], [19], [20] and [21].

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

1. Technology development tests as the earliest tests to check the technology against the specification and to get the technology parameters used in simulations of the circuitry (this testing is not strictly related to Security Functionalities);
2. Tests which are performed in a simulation environment with different tools for the analogue circuitries and for the digital parts of the TOE;
3. Regression tests of the hardware within a simulation environment based on special software dedicated only for the regression tests;
4. Regression tests which are performed for the IC Dedicated Test Software and for the Operating System on the final product of the TOE;
5. Characterisation and verification tests to release the TOE to production:

   a) used to determine the behaviour of the chip with respect to different operating conditions and varied process parameters (often also referred to as characterisation tests);

   b) special verification tests for Security Functionalities which were done with samples of the TOE (referred also as developers security evaluation) and which include also layout tests by automatic means and optical control, in order to verify statements concerning the layout;

6. Functional production tests, which are done for every chip to check its correct functionality as a last step of the production process (phase 3).

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

The evaluators were able to repeat the tests of the developer either using the library of programs, tools and prepared chip samples delivered to the evaluator or at the developers site. They performed independent tests to supplement, augment and to verify the tests performed by the developer. The tests of the developer were repeated by sampling, by repetition of complete regression tests and by software routines developed by the evaluators and computed on samples with an evaluation operating system. For the developer tests repeated by the evaluators other test parameters were used and the test equipment was varied. Security features of the TOE realised by specific design and layout measures were checked by the evaluators during layout inspections both in design data and on the final product.

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

For penetration testing the evaluators took all security functionalities into consideration. Intensive penetration testing was planned based on the analysis results and performed for the underlying mechanisms of security functionalities using bespoke equipment and expert know how. 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.

8 Evaluated Configuration

This certification covers the following configurations of the TOE: The configuration under evaluation has the identification SLB96xx (cf. [13], 6.3 and [14], Annex D).

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [8] 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).

For RNG assessment the scheme interpretations AIS 20 and AIS 31 were used (cf. [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.

The evaluation has confirmed:

- PP Conformance: PC Client Specific Trusted Platform Module Family 1.2; Level 2, Revision 116, Version 1.2, 6 October 2011, BSI-CC-PP-0030-2008-MA-01 [7]
- for the Functionality: PP conformant
Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
EAL 4 augmented by ALC_FLR.1 and AVA_VAN.4

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

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

9.2 Results of cryptographic assessment

The 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
Key Generation	RSA	P1363 [22]	|Modulus| = 512, 1024, 2048	TPM [16]
Authenticity	RSA signature generation / verification (RSASSA-PKCS1-v1_5)	PKCS#1 [23]	|Modulus| = 512, 1024, 2048	TPM [16]
Authentication	HMAC with SHA-1	RFC2104 [24], FIPS180-2 [25]	|k| = 160	TPM [16]
Key Agreement	RSA decryption (RSAES-OAEP)	PKCS#1 [23]	|Modulus|=512, 1024, 2048	TPM [16]
Integrity	HMAC with SHA-1	RFC2104 [24], FIPS180-2 [25]	|k| = 160	TPM [16]
Confidentiality	AES in CBC and CTR mode	FIPS197 [26], NIST SP800-38A [27]	|k| = 128	TPM [16]
	RSA encryption / decryption (RSAES- OAEP, RSAES-PKCS1-v1_5)	PKCS#1 [23]	|Modulus| = 512, 1024, 2048	TPM [16]
	MGF1	PKCS#1 [23], TPM [16]	|k| = 160	TPM [16]

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application
Cryptographic Primitive	SHA-1	FIPS180-2 [25]	None	TPM [16]
	Deterministic RNG DRG.3	AIS20 [28]	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 3: 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 key generation, 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 [23], ADV_TDS_TPMFU [29]	|Modulus| = 2048	yes	TPM-Field Upgrade
Key Agreement	HMAC with SHA-256	RFC2104 [24], FIPS180-2 [25], NIST SP800-108 [30], ADV_TDS_TPMFU [29]	|k| = 256	yes	TPM-Field Upgrade
Integrity	HMAC with SHA-256	RFC2104 [24], FIPS180-2 [25], NIST SP800-108 [30], ADV_TDS_TPMFU [29]	|k| = 256	yes	TPM-Field Upgrade
Confidentiality	AES in CBC mode	FIPS197 [26], NIST SP800-38A [27],	|k| = 128	yes	TPM-Field Upgrade

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
		ADV_TDS_TPMFU [29]			

Table 4: 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

AES	Advanced Encryption Standard
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
CRT	Chinese Remainder Theorem
DRNG	Deterministic Random Number Generator
EAL	Evaluation Assurance Level

EEPROM	Electrically Erasable Programmable Read Only Memory
ETR	Evaluation Technical Report
HMAC	Keyed-Hash Message Authentication Code
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	Information Technology Security Evaluation Facility
PLL	Phase Locked Loop
PP	Protection Profile
RSA	Rivest, Shamir, Adleman Public Key Encryption
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.

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

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.

Protection Profile - An implementation-independent statement of security needs for a TOE type.

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 - A set of software, firmware and/or hardware possibly accompanied by guidance.

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

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012

[3] BSI certification: Procedural Description (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[8].

[5] German IT Security Certificates (BSI 7148), periodically updated list published also in the BSI Website

[6] Security Target BSI-DSZ-CC-0844-2014, Version 1.1, 02 December 2013, SLB96xx Security Target, Infineon Technologies AG (public version)

[7] PC Client Specific Trusted Platform Module Family 1.2; Level 2, Revision 116, Version 1.2, 6 October 2011, BSI-CC-PP-0030-2008-MA-01

[8] Evaluation Technical Report 0844, Version 4, 24 January 2014, TÜV Informationstechnik GmbH (confidential document)

[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.

[12] PC Client Specific TPM Interface Specification (TIS) for TPM Family 1.2; Level 2, Version 1.21 FINAL, Revision 1.00, May 2011, Trusted Computing Group Inc.

[8] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 8, 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 EAL5+ (CCv2.3 & CCv3.1) and EAL6 (CCv3.1)
- AIS 35, Version 2, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 4, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2, Reuse of evaluation results

[13] TPM Trusted Platform Module SLB9660 TCG, Rev 116, Databook Including Errata and Updates for TPM V1.2 SLB9660 (Revision 1.3, 2013-10-25), Version 1.1, 06 August 2013, Infineon Technologies AG

[14] TPM Trusted Platform Module, Version 1.2, SLB9660 Application Note Basic Platform Manufacturer Guideline, March 2013, Infineon Technologies AG

[15] Development and Production, Version 3.7, 28 January 2013, Infineon Technologies AG

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

[17] TCG PC Client Specific TPM Interface Specification (TIS) for TPM Family 1.2; Level 2, Version 1.21 FINAL, Revision 1.00, May 2011

[18] Confidential partial evaluation report on the assurance classes ATE and AVA according to AIS 14 and as Annex of the Evaluation Technical Report [8]

[19] Confidential partial evaluation report on the assurance classes ATE and AVA according to AIS 14 and as Annex of the Evaluation Technical Report [8]

[20] Confidential partial evaluation report on the assurance classes ATE and AVA according to AIS 14 and as Annex of the Evaluation Technical Report [8]

[21] Confidential partial evaluation report on the assurance classes ATE and AVA according to AIS 14 and as Annex of the Evaluation Technical Report [8]

[22] IEEE P1363-2000, Standard Specifications for Public Key Cryptography, Institute of Electrical and Electronics Engineers, Inc. (reaffirmation PAR is actual running)

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

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

[25] Federal Information Processing Standards Publication 180-2, Secure Hash Standard (SHS), 1 August 2002, Information Technology Laboratory National Institute of Standards and Technology

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

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

[28] Anwendungshinweise und Interpretationen zum Schema, AIS 20, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3.0, 15 May 2013, Bundesamt für Sicherheit in der Informationstechnik

[29] TPMv12 Field Upgrade, Doxygen documentation, Version 778, 11 October 2013, Infineon Technologies AG

[30] 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

Assurance Class	Assurance Components
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 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.

Assurance Class	**Assurance Family**	**Assurance Components by Evaluation Assurance Level**						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
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
	ASR_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”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)

“Objectives

EAL1 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.

EAL1 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.

EAL1 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 EAL1 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 (EAL2) - structurally tested (chapter 8.4)

“Objectives

EAL2 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.

EAL2 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 (EAL3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL3 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 (EAL4) - methodically designed, tested, and reviewed (chapter 8.6)

“Objectives

EAL4 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. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 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 (EAL5) - semiformally designed and tested (chapter 8.7)

“Objectives

EAL5 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 EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 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 (EAL6) - semiformally verified design and tested (chapter 8.8)

“Objectives

EAL6 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.

EAL6 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 (EAL7) - formally verified design and tested (chapter 8.9)

“Objectives

EAL7 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 EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.”

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.”

This page is intentionally left blank

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-0844-2014

Evaluation results regarding development and production environment

The IT product SLB96xx (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 28 February 2014, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.1, ALC_FLR.1, ALC_LCD.1, ALC_TAT.1) are fulfilled for the development and production sites of the TOE listed below:

The following table outlnes the TOE deliverables:

No.	Site	Task within the evaluation
1.	Agrate DNP Photomask Europe S.p.A. Via C. Olivetti 2/A 20041 Agrate Brianza Italy	Mask house site Phase 1
2.	Augsburg Infineon Technologies AG Alter Postweg 101 86159 Augsburg Germany	Development Phase 1
3.	ASK-intTag LLC 1000 River St.Building 966 Essex Junction, VT, 05452 USA	Phase 3
4.	Infineon Technologies India Private Limited Kalyani Platina, Sy. No. 6 & 24 Kundanahalli Village Krishnaraja Puram Hobli Bangalore, India, 560066	Development Phase 1
5.	Bangkok SMARTRAC TECHNOLOGIES Ltd. 142 and 121 and 115 Moo, Hi-Tech Industrial Estate Tambon Ban Laean, Amphor Bang-Pa-In 13160 Ayutthaya Thailand	Inlay antenna mounting site Phase 3

No.	Site	Task within the evaluation
6.	Corbeil-Essones Altis Semiconductor S.N.C. Boulevard John Kennedy 224 91105 Corbeil-Essonnes France	Production site Phase 3, 4 and 6
7.	Corbeil-Essones Toppan Photomask, Inc. European Technology Center Boulevard John Kennedy 224 91105 Corbeil-Essonnes Cedex France	Mask house site Phase 3
8.	Bucharest Infineon Technologies AG DC Bukarest Novopark Blvd. Dimitrie Pompei Nr. 6 Section 2, Bucharest Romania	Development site Phase 1 and 2
9.	Chanhassen Smartrac Technology US Inc. 1546 Lake Drive West Chanhassen, MN 55317 USA	Inlay antenna mounting site Phase 3
10.	Dresden Toppan Photomask, Inc Rähnitzer Allee 9 01109 Dresden Germany	Mask house site Phase 3
11.	Infineon Technologies Dresden GmbH & Co. OHG Königsbrücker Str. 180 01099 Dresden Germany	Production site Phase 3, 5 and 6
12.	Galway HID Global Ireland Teoranta Pairc Tionscail na Tulaigh Baile na hAbhann Co. Galway Ireland	Inlay antenna mounting site Phase 3
13.	Graz Infineon Technologies Austria AG Development Center Graz Babengergerstr. 10 8020 Graz Austria	Development site Phase 1 and 2
14.	Grossostheim Infineon Technology AG Kühne & Nagel Stockstädter Strasse 10 - Building 8A	Distribution Phase 4

No.	Site	Task within the evaluation
	63762 Grossostheim Germany	
15.	Hayward Kuehne & Nagel 30805 Santana Street Hayward, CA 94544 USA	Distribution Center Phase 4
16.	Klagenfurt Infineon Technologies Austria AG Lakeside B05 9020 Klagenfurt Austria	Development site Phase 1 und 2
17.	Kulim Infineon Technologies (Kulim) Sdn. Bhd. Lot 10 &11,Julan Hi-Tech 7 Industrial Zone Phase II Kulim Hi-Tech Park 09000 Kulim, Kedah Darul Aman Malaysia	Production site Phase 3 und 4
18.	Manila Amkor Technology Philippines Km. 22 East Service Rd. South Superhighway Muntinlupa City 1702 Philippines	Module mounting site Phase 4
19.	Manila Amkor Technology Philippines 119 North Science Avenue Laguna Technopark, Binan Laguna 4024 Philippines	Module mounting site Phase 4
20.	Morgan Hill Infineon Technologies North America Corp. 18275 Serene Drive Morgan Hill, CA 95037 USA	Inlay testing site Phase 3
21.	Munich Infineon Technologies AG Am Campeon 1-12 85579 Neubiberg Germany	Development site Phase 1 and 2

No.	Site	Task within the evaluation
22.	Saitama Toppan Printing Co., LTD. Ranzan-Machi 6-2, Hanamidai Hiki-Gun, Saitama 355-0204 Japan	Inlay antenna mounting site Phase 4
23.	Regensburg-West Infineon Technologies AG Wernerwerkstraße 2 93049 Regensburg Germany	Module mounting and distribution site Phase 3, 4 and 6
24.	Round Rock Toppan Printing Company America, Inc. Round Rock Site 2175 Greenhill Drive Round Rock, Texas 78664 USA	Inlay antenna mounting site Phase 3
25.	Excel Singapure PTE Ltd. DHL Exel Supply Chain Richland Business Centre 11 Bedok North Ave 4, Level 3, Singapore 489949	Distribution center Phase 4
26.	Infineon Technologies Asia Pacific PTE Ltd. 168 Kallang Way Singapore 349253	Module testing site Phase 4
27.	Taiwan Semiconductor Manufacturing Company Ltd. 1, Nan-Ke North Rd. Tainan Science Park Tainan 741-44	Production and mask house site Phase 3, 4 and 6
28.	Ardentec Corporation No. 3, Gungye 3rd Rd., Hsin-Chu Industrial Park, Hu-Kou, Hsin-Chu Hsien, Taiwan 30351	Wafer testing site Phase 3
29.	Villach Infineon Technologies Austria AG Siemensstrasse 2 9500 Villach Austria	Development site Phase 1 and 2
30.	Wuxi Infineon Technologies (Wuxi) Co. Ltd. 118, Xing Chuang San Lu Wuxi 214028, Jiangsu P.R. China	Module mounting and distribution site Phase 4

Table 5: Addresses development/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.

This page is intentionally left blank.