Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0573-2009

for

SLB9635TT1.2 / m1566a13 HW a13 / FW 03.17.0008.00

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-0573-2009

Trusted Platform Module

SLB9635TT1.2 / m1566a13 HW a13 / FW 03.17.0008.00

from	Infineon Technologies AG
PP Conformance:	Schutzprofil PC Client Specific Trusted Platform Module TPM Family 1.2; Level 2; Version 1.1, BSI-PP-0030-2008
Functionality:	PP strict conformant; Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.1 AVA_VAN.4

Common Criteria Recognition Arrangement for components up to EAL 4

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 advice of the Certification Body for components beyond EAL 4 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, 20 November 2009

For the Federal Office for Information Security

IT Security Certified

SOGIS - MRA

Bernd Kowalski
Head of Department

L.S.

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:

- 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

The SOGIS-Mutual Recognition Agreement (MRA) for certificates based on ITSEC became initially effective in March 1998.

This agreement on the mutual recognition of IT security certificates was extended in April 1999 to include certificates based on the Common Criteria for the Evaluation Assurance Levels (EAL 1 – EAL 7). This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and United Kingdom, and from The Netherlands since January 2009 within the terms of this 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 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

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

2.2 International Recognition of CC - Certificates

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 January 2009 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 web site: 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.

This evaluation contains the components AVA_VAN.4 and ALC_FLR.1 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 SLB9635TT1.2 / m1566a13 HW a13 / FW 03.17.0008.00 has undergone the certification procedure at BSI.

The evaluation of the product SLB9635TT1.2 / m1566a13 HW a13 / FW 03.17.0008.00 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 14 October 2009. The 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, where specified in the following report and in the Security Target.

[6] Information Technology Security Evaluation Facility

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 may evolve over time, the resistance of the certified version of the product against new attack methods can be re-assessed if required and the sponsor applies for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme. It is recommended to perform a re-assessment on a regular 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 SLB9635TT1.2 / m1566a13 HW a13 / FW 03.17.0008.00 has been included in the BSI list of the 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

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 ([12], [13], [14], [15] and [16] including [17] and [18]).

The SLB9635TT1.2 Trusted Platform Module, called TPM or SLB9635TT1.2 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 SLB9635TT1.2 is a complete solution implementing the version 1.2 of the TCG Trusted Platform Module Main, Specification Version 1.2 [11] and the TCG PC Client Specific TPM Interface Specification, Version 1.2 Final, Revision 1.00 [15].

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, Version 1.1, BSI-CC-PP-0030-2008, [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 EAL4 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:

Portion of TOE Security Functionality	Addressed issue
SF_CRY - Cryptographic Support	There are several functions within the TOE related to 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.
SF_I&A - 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. This shared secret is the identification and authentication data, which is called authorization data in the TPM Main Specification. The TOE supports the management of TSF data by restricting the ability to modify and create the authentication data to different roles (e.g. TPM owner, User under physical presence, Entity owner, authorized user) based on different rules and restricting the ability to reset the TPM dictionary attack mitigation mechanism and the creation of migration tickets to the TPM owner, by using access control mechanisms during the command processing. The TOE associate user security attributes (e.g. authData, locality, physical presence, authorization handle and shared secret if the subject is a OSAP session and authorization associated with the delegation blob if the subject is a DSAP session) with subjects acting on the behalf of that user. The TOE enforces different rules, implemented in the appropriate command, on the initial association and governing changes of user security attributes

Portion of TOE Security Functionality	Addressed issue
	with subjects acting on the behalf of users.
SF_ACC – Access Control	The TOE provides the security function policies TPM Mode Control SFP (MCT_SFP), Delegation SFP (Del_SFP), Key Management SFP (KeyM_SFP), Key Migration SFP (KMig_SFP), Measurement And Reporting SFP (M&R_SFP), Non-volatile Storage SFP (NVS_FSP), Monotonic Counter SFP (MC-SFP), Export and Import of Data (EID_SFP) and Direct Anonymous Attestation Protocol SFP (DAA_SFP) to protect the sensitive subjects, objects and operations of the TOE. The security policies are described in section 8.2 and in the PP [7], section 6.1.
SF_GEN – General	The TOE provides the roles: TPM owner, Entity owner, Delegated entity, Entity user, User using operatorAuth and “World” and associates users with roles. The role is bound always on specific authentication token The TOE performs the following management functions: - Management of the TPM modes of operation, - Management of Delegation Tables and Family Tables, - Management of security attributes of keys, - Management of security attributes of PCR, - Management of security attributes of NV storage areas, - Management of security attributes of monotonic counters and - Reset the Action Flag of TPM dictionary attack mitigation mechanism. The TOE provides an authentication functionality to consistently interpret authentication reference data of the TPM owner, delegated entities, owner of entities, user of entities and User using operatorAuth, when shared between the TSF and another trusted IT product and uses roles when interpreting the TSF data from another trusted IT product. The TOE provides the transmission and reception of user data in encrypted manner, to protect the user data from unauthorized disclosure. The TOE provides the transmission and reception of user data in encrypted and signed manner, to protect the user data from undiscovered modification, deletion, insertion and replay errors (only required for sessions). The TOE provides the generation of an audit record of the event Transport session including different information (e.g. type and outcome of event). The TOE provides reliable time stamps as number of ticks since start of the tick session. The TOE provides the generation of evidence of origin for transmitted data at the request of the originator and is able to verify the evidence of origin of transmitted data to recipient, by calculation and verifying a digital signature of the data.
SF_P&T – Protection and Test	The TOE preserves a secure state when a failure of any crypto operations including RSA encryption, RSA decryption, SHA-1, RNG, RSA signature generation, HMAC generation or failure of any commands or internal operations (including AES and Tripple-DES encryption/ decryption) and authorization occurs. The TOE supports a suite of self tests during startup and at the request of an authorized user to demonstrate the correct operation of the TSF and to verify the integrity of stored TSF executable code. The TOE supports the Direct Anonymous Attestation Protocol. The TOE resists physical manipulation and physical probing to the TSF by responding automatically such that the SFRs are always enforced.

Table 1: Portions of TOE Security Functionality

For more details please refer to the Security Target [6], chapter 8.1 at which the portions of the TOE Security Functionality as depicted in Table 1 correspond to the SF (Security Features) in Security Target [6].

The assets to be protected by a TOE are defined in the Protection Profile [7], chapter 1.3.4. Based on these assets the TOE Security Environment 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 specified 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:

SLB9635TT1.2 / m1566a13 HW a13 / FW 03.17.0008.00

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	Security IC with integrated firmware (operating system)	SLB9635TT1.2 / m1566a13 HW a13 / FW 03.17.0008.00, ROM CRC 9AE5	Packaged module
2	DOC	Trusted Computing Group TPM Main Specification [11]	Version 1.2, Revision 94	Hardcopy and pdf-file
3	DOC	TCG PC Client Specific TPM Interface Specification (TIS) for TPM Family 1.2; Level 2 [15]	Version 1.2 FINAL, Revision 1.00	Hardcopy and pdf-file
4	DOC	TPM SLB9635TT1.2 TCG Rev 103 Trusted Platform Module Databook [16]	Version 1.3	Hardcopy and pdf-file
5	DOC	Errata and Updates for TPM V1.2 SLB9635TT1.2 [17]	Version 3.2	Hardcopy and pdf-file
6	DOC	Basic Platform Manufacturer Guideline for TPM 1.2 [18]	Version 1.0	Hardcopy and pdf-file

Table 2: Deliverables of the TOE

The delivery of the Security IC is done in the following manner:

1. The customer picks up the TOE directly in Großostheim (DC-E), Singapore (DC-A), Wuxi (DC-C), Tokyo (DC-J) or Hayward (DC-U).

After a positive check of the proof of the identity of the recipient (the customer has to announce the recipient and Infineon Technologies checks the identity of the recipient controlling the consignment notes and the passport of the recipient) is done, the TOE is delivered to the recipient (e.g. Transport Company of the customer). The recipient has to sign an acknowledgement of receipt that contains the date of the delivery, the number of parts, the specific product name (TOE) and the name of the recipient. The customer can choose the transport company and is responsible for the transport security.

2. The distribution centers (DC-E for Europe, DC-C for China, DC-A for Asia, DC-J for Japan and DC-U for the United States) send the TOE to the customer.

The transport is secured by the following process:

For the transport only evaluated haulage companies are used, which are chosen by the Infineon Technologies AG. The assessment and approvement of the used haulage companies is done by a department of the Infineon Technologies AG.

The sender informs the receiver (other DC or customer) that a delivery was started. After the delivery was received the delivery is checked according to the consignment notes. If any delay or failure occurs the receiver has to inform the sender about this fact. This process is integrated in an electronic process and controlled by the system Assist4. Manipulation of the TOE is not possible without destroying it.

The transport of the TOE from the distribution center to the customer is done with the same process used for the transport between the DCs.

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

A processing step during production testing incorporates the chip-individual features into the hardware of the TOE. The individual TOE hardware is uniquely identified by its serial number. The serial number comprises the lot number, the wafer number and the coordinates of the chip on the wafer. Each individual TOE can therefore be traced unambiguously and thus assigned to the entire development.

The delivery of the TOE related documentation is done from the Infineon Technologies department AE at the site München-Campeon (MchC).

All confidential electronic documents are delivered encrypted by using PGP tools within an already established PKI, so the confidentiality and integrity of the documentation is ensured during the whole life cycle because only the good recipient is able to decrypt the code. The detection of modification is reached by the functionality of the PGP tools. Deliverables send in paper form are personalised as described in [10], chapter 3, and only send on request by the Smartcard Embedded Software Developer. This personalisation consists of a serial number which is printed as a watermark in the document. This serial number is administered by Infineon and linked to the customer the document is delivered to. Furthermore the envelopes are secured by a seal and signature.

All paper documents are send personalised (if they are not personally handed over) as described in [10], chapter 3, in two envelopes, plus seal and signature one marked with “personally”. With these procedures an integer and confidential transfer is guaranteed.

TOE identification

The user identifies the evaluated TOE by the data code printed on the chip package [17], chapter 2, and the FW version “03.17” and ROM CRC “9AE5” which can be read out as described in the guidance documentation [18], Annex D. The HW version of the TOE can

be unambiguously identified by the FW version “03.17” and ROM CRC “9AE5” as listed in [17], chapter 2.

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:

- Security management,
- Cryptographic support,
- TPM Operational Modes,
- Identification, Authentication and Binding,
- Delegation,
- Key management,
- Key Migration,
- Measurement and Reporting,
- Non-volatile Storage,
- Counter,
- Data Import and Export,
- Direct Anonymous Attestation and TSF Protection.

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: Configuration, Locality, Physical Presence, Integrity of Sealed Data Blobs, Credential, Measurement and Direct Anonymous Attestation. Details can be found in the Security Target [6], chapter 4.3, and Protection Profile [7], chapter 5.2.

5 Architectural Information

The TOE is the “Infineon SLB9635TT1.2 Trusted Platform Module, which comprises the hardware of the security controller, type SLB9635TT1.2, and the associated firmware required for operation provided in ROM and EEPROM.

All hardware parts constituting the TOE are listed below:

- Security logic (SEC)
- Microcontroller type ECO2000 (CPU) with the subcomponents memory encryption and decryption unit (MED), memory management unit (MMU) and 256 bytes of internal RAM(IRAM)
- External memory comprising:
    - 12 kByte extended RAM (XRAM)
    - 196 kByte user ROM, including the routines for chip management (RMS)

  - 8 KB test ROM containing the test routines (STS), and
  - a total of 68 kByte non-volatile memory (EEPROM)
- Random number generator (RNG)
- Checksum module (CRC)
- Interrupt module (INT)
- Timer (TIM)
- Address and data bus (BUS)
- ACE for long integer modulo calculations, which are used in asymmetric algorithms like RSA
- DES accelerator (DDC) used for fast calculations of the DES algorithm
- Low Pin Count interface (LPC)
- Hash accelerator (HASH) for the algorithms SHA-1
- Tick Counter
- Input logic (INP)

The entire firmware of the TOE consists of two different parts. The one is the operating system called firmware in the following document. The firmware includes operating system and the Endorsement Key and is used to operate the IC. The firmware includes also the capability for updating the protected capabilities once the TOE is in the field (TPM_FieldUpgrade). Note that it is possible to update an old TPM firmware version e.g. v3.16 to a certified firmware version v3.17.0008.00.

The other is the Self Test Software (STS). The STS routines are stored in the especially protected test ROM and are not accessible for the user software (application).

The entire firmware of the TOE is comprised of:

- I/O-Interface
- Transportation
- TPM-Dispatcher
- State-Machine
- Authorization
- Dictionary Attack Logic
- TPM-Command
- HASH
- HMAC
- 3DES
- AES
- RSA2048
- MGF1
- Memory

- Security
- Archive
- Test
- Tick Counter
- DAA
- RND
- PCR
- Field-Upgrade
- TcpaFlags
- Locality
- Key Class
- System Startup

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

Description of the Test configuration

The test configuration used for independent testing is as follows:

- PC with Intel Pentium 4 CPU 2.8 GHZ, 1 GB RAM
- Windows 2000 Service Pack 4
- ifxtpm.dll driver with date 6th August 2008
- TOE with hardware tag SLB9635TT12, GE913KIV (corresponds to HW a13 according to [18], chapter 2); firmware 03.17.0008.00 and ROM CRC 9AE5

The test environment to repeat developer tests consists of

- PC with Intel Pentium 4 CPU, 2.8 GHz
- Windows XP Professional Service Pack 3
- TOE with hardware tag SLB9635TT12, GE913KIV (corresponds to HW a13 according to [18], chapter 2); with firmware 03.17.0008.00 and ROM CRC 9AE5

I) Developer's Test according to ATE_FUN

The developer tests of the Infineon SLB9635TT1.2/m1566a13 are separated in several categories:

- Technology development

- Production technology development and testing

  The process technology for the products is defined and its properties ensured by testing

- Circuit development
  - Design verification by simulation

    The simulation checks if the design under development produces the intended behaviour
  - Qualification testing (test mode for full access to parameters)

    After sample production it is tested if the device fulfils the specification (whole range of parameters is verified)
  - Verification testing (user mode)

    Tests functionality available to the user
  - Security evaluation

    The resistance against relevant attack scenarios is tested
- Production testing
  - Initial testing

    Functionality of the IC is tested
  - Final testing

    Functionality testing under stress conditions, sensor calibration and user mode activation

The overall goal of the tests is to show that the TOE implements the TSF as described by the security target, the functional specification and the design documentation. As shown in the test categories above, testing covers the different configurations of the TOE. The software tests cover the TOE in an activated state, which represents the usual state in which the TOE is used by end users.

II) Independent Testing according to ATE_IND (Evaluator Tests)

Subset size chosen

The evaluator performed twelve automated tests using a Java-based test system. Each security feature defined in the [6], chapter 8, was covered with at least one test. The testing included positive and negative tests.

Selection criteria for the interfaces that compose the subset

The following test strategy was applied for independent testing:

- Cover all security features of the TOE with at least one test.
- Specifically target the cryptographic features of the TOE.
- If possible, design test cases in a way that they test behaviour which is not specifically covered by a developer test. Also, skip some features which are considered to be sufficiently covered by developer tests.

Interfaces tested

The following interfaces were directly stimulated by the tests:

- INT 2.1
- INT 2.2
- INT 2.3
- INT 2.4
- INT 2.5

Developer tests performed

The evaluators independently repeated a subset of the developer tests. This subset includes all automated tests in [19]. It covers all security functions and contains a large part of all developer tests.

The sample results in a total number of 132921 checked test instructions in the developer test cases.

Verdict for the activity

During the evaluator's TSF subset testing, the TOE operated as specified. Therefore the TOE passed the evaluators testing. The tests confirm the TOE functionality as described in the developer documents.

III) Penetration Testing according to AVA_VAN (Evaluator Tests)

The penetration testing was performed using developer's testing tools and 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

The penetration tests consist of manual and automated tests. The manual tests were executed using the DLLTest.exe tool provided by the developer. The automated tests were either executed using the developer's test suite with modified test scripts or proprietary test suite/ tools of the evaluation lab.

TOE test configurations

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

- Test tool by TÜViT to implement most of the test cases
- Java J2SE JRE version 5.0
- Windows 2000
- Installed and working driver for the TOE: "ifxtpm.dll" library in Windows system32 directory
- DLLTest.exe tool provided by the developer to execute raw packets/byte strings
- Additional Software: Microsoft Windows XP Professional, Version 2002, Service Pack 3, developer's test suite for TOE

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

- Oscilloscope and Laser equipment
- Proprietary measuring/analysing software
- Standard PC

SFRs penetration tested

The following TSF interfaces have been tested:

- 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.

8 Evaluated Configuration

This certification covers the following configurations of the TOE: The configuration under evaluation has the identification SLB9635TT1.2 / m1566a13 HW a13 / FW 03.17.0008.00, ROM CRC 9AE5.

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [9] 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 for those components up to EAL4 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product [4] (AIS 34).

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

- All components of the EAL4 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, Version 1.1, BSI-CC-PP-0030-2008 [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
AVA_VAN.4

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:

- RSA signature scheme with cryptographic key sizes 512, 1024, 2048 bits according to [20],
- RSA encryption scheme with cryptographic key sizes 512, 1024, 2048 bits according to [20],
- encryption scheme 3DES with cryptographic mode of operation CBC and with cryptographic key sizes 112 bits and 168 bits according to [21],
- encryption scheme AES with cryptographic mode of operation CTR and with cryptographic key size 128 bits according to [22],
- encryption scheme TPM_ALG_XOR with MGF1 [20] and with cryptographic key size of variable bit length according to TPM main specification [13],
- hash function SHA-1 according to [23],
- authentication scheme HMAC with hash algorithm SHA-1 [23] and with cryptographic key size 160 bits according to [24].

This holds for the following security features:

- SF_CRY - Cryptographic Support

The strength of the cryptographic algorithms was not rated in the course of this evaluation (see BSIG Section 9, Para. 4, Clause 2). According to [11] the algorithms are suitable for using in services required for a TPM in the TCG Trusted Platform Module Main Specification, version 1.2, [12], [13], [14] and additional services that are optional in the main TPM specification but mandatory in the PC client specific interface specification [15].

10 Obligations and notes for the usage of the TOE

The operational documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered.

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

3DES Triple Data Encryption Standard

AES Advanced Encryption Standard

BSI Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany

BSIG	BSI-Errichtungsgesetz
CBC	Cipher Block Chaining
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CTR	Counter
DES	Data Encryption Standard
DFA	Differential Fault Attack
EAL	Evaluation Assurance Level
FW	Firmware
HMAC	Hash-based Message Authentication Code
HW	Hardware
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	Information Technology Security Evaluation Facility
MGF	Mask Generation Function
RNG	Random Number Generator
PP	Protection Profile
RSA	Rivest, Shamir and Adleman
SAR	Security Assurance Requirement
SF	Security Feature
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
ST	Security Target
SW	Software
TCG	Trusted Computing Group
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.

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 - An 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 - A set consisting of all hardware, software, and firmware of the 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 1, September 2006
Part 2: Security functional components, Revision 2, September 2007
Part 3: Security assurance components, Revision 2, September 2007

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 2, September 2007

[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, BSI 7149), periodically updated list published also in the BSI Website

[6] Security Target BSI-DSZ-CC-0573, Version 1.0, September 28, 2009, Security Target of SLB9635TT1.2 / m1566a13, Infineon Technologies AG

[7] Protection Profile PC Client Specific Trusted Platform Module Family 1.2; Level 2, BSI-CC-PP-0030-2008, Version 1.1, July 10, 2008, Trusted Computing Group

[8] Evaluation Technical Report, Version 2, November 18, 2009, ETR Summary, TÜV Informationstechnik GmbH (confidential document)

[9] Configuration list for the TOE (confidential document):
SLB9635TT1.2 / m1566a13, FW_Configurationlist, Version 0.3, 2009-09-28
SLB9635TT1.2 / m1566a13, Configuration Management Scope (ALC_SCP), Version 0.2 2009-09-29

[10] Security Management SMS Allgemeiner Teil, Version 9.0, September 01, 2004

[11] Trusted Computing Group TPM Main Specification, consisting of [12], [13] and [14]

---

[8] specifically

- AIS 20, Version 1, 2. December 1999, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 6, 7 September 2009, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 6, 07 May 2009, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 1, 25 Sept. 2001 Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 1, 2 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema.
- AIS 34, Version 2, 24 October 2008, Evaluation Methodology for CC Assurance Classes for EAL5+
- AIS 35, Version 2.0, 12 November 2007, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 2, 12 November 2007, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results

[12] TPM Main Part 1 Design Principles, Specification Version 1.2, Revision 94, 29 March 2006, Trusted Computing Group, Incorporated

[13] TPM Main Part 2 TPM Structures, Specification Version 1.2, Revision 94, 29 March 2006, Trusted Computing Group, Incorporated

[14] TPM Main Part 3 Commands, Specification Version 1.2, Revision 94, 29 March 2006, Trusted Computing Group, Incorporated

[15] TCG PC Client Specific TPM Interface Specification (TIS) for TPM Family 1.2; Level 2, Version 1.2 FINAL, Revision 1.00, July 11, 2005

[16] TPM SLB9635TT1.2 TCG Rev 103 Trusted Platform Module Databook Version 1.3 January 22, 2008, Infineon Technologies AG

[17] Errata and Updates for TPM V1.2 SLB9635TT1.2, Version 3.2, September 2009, Infineon Technologies AG

[18] Basic Platform Manufacturer Guideline for TPM 1.2, Version 1.0, July 24, 2009, Infineon Technologies AG

[19] Test Plan TPM 1.2 ROM3 3.17.0008.00, Version 1.2, September 24, 2009, Infineon Technologies AG (confidential document)

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

[21] FIPS PUB 46-3, Data Encryption Standard (DES), October 25, 1999, U.S. Department of Commerce / National Institute of Standards and Technology, Information Technology Laboratory (ITL)

[22] FIPS PUB 197, Advanced Encryption Standard (AES), November 26, 2001, U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL)

[23] FIPS PUB 180-2, Secure Hash Standard, August 1, 2002, U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL)

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

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

C Excerpts from the Criteria

CC Part1:

Conformance Claim (chapter 9.4)

„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 A.

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 decompositon.

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-

Assurance Class	Assurance Components
	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 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_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
ATE: Tests	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	2	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 3: 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 39

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0573-2009

Evaluation results regarding development and production environment

The IT product SLB9635TT1.2 / m1566a13 HW a13 / FW 03.17.0008.00 (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 advice of the Certification Body for components beyond EAL 4 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 20 November 2009, 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_LCD.1, ALC_FLR.1, ALC_TAT.1) are fulfilled for the development and production sites of the TOE listed below:

Site	Adress	Function
Altis-Toppan	Toppan Photomask, Inc. European Technology Center Boulevard John Kennedy 224 91105 Corbeil Essonnes France	Mask Center
Amkor	Amkor Technology Philippines Km. 22 East Service Rd. South Superhighway Muntinlupa City 1702 Philipines Amkor Technology Philippines 119 North Science Avenue Laguna Technopark, Binan Laguna 4024 Philipines	Module Mounting
Augsburg	Infineon Technologies AG Alter Postweg 101 86159 Augsburg Germany	Development
Bukarest	Infineon Technologies Romania Blvd. Dimitrie Pompeiu Nr. 6 Sector 2 020335 Bucharest, Romania	Development
Dresden	Infineon Technologies Dresden GmbH & Co. OHG Königsbrücker Str. 180 01099 Dresden Germany	Production

Site	Adress	Function
Dresden-Toppan	Toppan Photomask, Inc Rähnitzer Allee 9 01109 Dresden Germany	Mask Center
Graz / Villach/ Klagenfurt	Infineon Technologies Austria AG Development Center Graz Babenbergerstr. 10 8020 Graz Austria Infineon Technologies Austria AG Siemensstr. 2 9500 Villach Austria Infineon Technologies Austria AG Lakeside B05 9020 Klagenfurt Austria	Development
Großostheim	Infineon Technology AG DCE Kühne & Nagel Stockstädter Strasse 10 - Building 8A 63762 Großostheim Germany	Distribution Center
Hayward	Kuehne & Nagel 30805 Santana Street Hayward, CA 94544 U.S.A.	Distribution Center
Lustenau	New Logic Technologies AG - A Wipro Company, Millenium Park 6, 6890 Lustenau, Austria	Development
Munich	Infineon Technologies AG Am Campeon 1-12 85579 Neubiberg Infineon Technologies AG Otto-Hahn-Ring 6 81739 München (Perlach) Germany	Development
Regensburg-West	Infineon Technologies AG Wernerwerkstraße 2 93049 Regensburg Germany Smartrac Technology GmbH, Wernerwerkstraße 2 93049 Regensburg Germany	Module Mounting Inlay antenna mounting Distribution Center
Singapore	Exel Singapore Pte Ltd DHL Exel Supply Chian 81, ALPS Avenue Singapore 498803	Distribution Center
Singapore Kallang	Infineon Technologies AG 168 Kallang Way Singapore 349253	Module Mounting

Site	Adress	Function
Tokyo	Kintetsu World Express, Inc. Tokyo Import Logistics Center Narita Terminal Tokyo Japan	Distribution Center
Wuxi	Infineon Technologies (Wuxi) Co. Ltd. No. 118, Xing Chuang San Lu Wuxi-Singapore Industrial Park Wuxi 214028, Jiangsu P.R. China	Module Mounting Distribution Center

Table 4: Identification of deliveries

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.