Federal Office
for Information Security

# Certification Report

## BSI-DSZ-CC-0437-2008

for

## SLE66CX680PE / m1534-a14,
## SLE66CX360PE / m1536-a14,
## SLE66CX482PE / m1577-a14,
## SLE66CX480PE / m1565-a14,
## SLE66CX182PE / m1564-a14,
## all optional with RSA2048 V1.5 and all with specific IC dedicated software

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-0437-2008**

**SLE66CX680PE / m1534-a14,**
**SLE66CX360PE / m1536-a14,**
**SLE66CX482PE / m1577-a14,**
**SLE66CX480PE / m1565-a14,**
**SLE66CX182PE / m1564-a14,**
**all optional with RSA2048 V1.5 and all with specific IC dedicated software**

Common Criteria Arrangement for components up to EAL 4

| | |
|---|---|
| from | Infineon Technologies AG |
| PP Conformance: | Smartcard IC Platform Protection Profile, Version 1.0, July 2001, Eurosmart, BSI-PP-0002-2001 |
| Functionality: | PP conformant plus product specific extensions Common Criteria Part 2 extended |
| Assurance: | Common Criteria Part 3 conformant EAL 5 augmented by ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4 |

Common Criteria

The IT product identified in this certificate has been evaluated at an accredited and licensed / approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 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 2.3 (ISO/IEC 15408:2005) .

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, 27. Mai 2008

For the Federal Office for Information Security

IT Security Certified
SOGIS - MRA

Irmela Ruhrmann
Head of Division

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 setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

# 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 2.3 (ISO/IEC 15408:2005)[5]
- Common Methodology for IT Security Evaluation, Version 2.3
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

## 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-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998.

This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7). The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and the United Kingdom within the terms of this Agreement.

---

2 Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

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 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 (CC-MRA). It includes also the recognition of Protection Profiles based on the CC.

As of February 2007 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, The Netherlands, New Zealand, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations resp. approved certification schemes can be seen on the web site: http://www.commoncriteriaportal.org

The Common Criteria Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement.

This evaluation contains the components ALC_DVS.2, AVA_MSU.3, and AVA_VLA.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 products SLE66CX680PE / m1534-a14, SLE66CX360PE / m1536-a14, SLE66CX482PE / m1577-a14, SLE66CX480PE / m1565-a14, SLE66CX182PE / m1564-a14, all optional with RSA2048 V1.5 and all with specific IC dedicated software have undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0322-2007. Specific results from the evaluation process BSI-DSZ-CC-0322-2007 were re-used.

The evaluation of the products SLE66CX680PE / m1534-a14, SLE66CX360PE / m1536-a14, SLE66CX482PE / m1577-a14, SLE66CX480PE / m1565-a14, SLE66CX182PE / m1564-a14, all optional with RSA2048 V1.5 and all with specific IC dedicated software was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 27 May 2008. 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

[6] Information Technology Security Evaluation Facility

- 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.

For the meaning of the assurance levels and the confirmed strength of functions, 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 products SLE66CX680PE / m1534-a14, SLE66CX360PE / m1536-a14, SLE66CX482PE / m1577-a14, SLE66CX480PE / m1565-a14, SLE66CX182PE / m1564-a14, all optional with RSA2048 V1.5 and all with specific IC dedicated software have been included in the BSI list of the certified products, which is published regularly (see also Internet: http://www.bsi.bund.de) and [5]. Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] Infineon Technologies AG
Am Campeon 1 - 12
85579 Neubiberg

# B Certification Results

The following results represent a summary of

- the security target of the sponsor for the target of evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

# 1 Executive Summary

The Target of evaluation (TOE) is SLE66CX680PE / m1534-a14, SLE66CX360PE / m1536-a14, SLE66CX482PE / m1577-a14, SLE66CX480PE / m1565-a14, SLE66CX182PE / m1564-a14, all optional with RSA2048 V1.5 and all with specific IC dedicated software. The RSA2048 library V1.5 is an improvement of the already certified RSA2048 Library V1.4 (e.g. BSI-DSZ-CC-0322-2005). The Target of Evaluation (TOE) comprises all products in unified channel programming (UCP) technology. UCP stands for an improved way of programming the EEPROM.

This TOE is intended to be used in smart cards for particularly security relevant applications, including high speed security authentication, data encryption or electronic signature. Several security features independently implemented in hardware or controlled by software will be provided to ensure proper operations and integrity and confidentiality of stored data. The TOE contains a crypto library RSA2048 and a RMS library providing some functionality via an API to the Smartcard Embedded Software and STS firmware for test purpose. The STS is implemented in a separated test-ROM being part of the TOE. The user/customer Smartcard Embedded Software (application) is not part of the TOE. The user has the possibility to tailor the software part of the TOE during the manufacturing process by deselecting the RSA library. The TOE can be delivered including the functionality of the RSA2048 crypto library or including no crypto library. The ACE (Advanced Crypto Engine) will be used for calculation of asymmetric algorithms like RSA. This module is especially designed for Chipcard applications with respect to the security and power consumption. The other module is the DDC providing the DES algorithm. This module computes the complete DES algorithm within a few clock cycles. That module is especially designed to counter attacks like DPA or EMA. The TOE includes also functionality to calculate single DES operations but only Triple-DES operations are subject of the evaluation.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Smartcard IC Platform Protection Profile, Version 1.0, July 2001, Eurosmart, BSI-PP-0002-2001 [9].

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see part C or [3], part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 5 augmented by ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6, chapter 5.1]. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC part 2 extended.

The Security Functional Requirements (SFR) relevant for the IT-Environment of the TOE are outlined in the Security Target [6, chapter 5.2].

The TOE Security Functional Requirements are implemented by the following TOE Security Functions:

| TOE Security Function | Addressed issue |
|---|---|
| SEF1 | Operating state checking |
| SEF2 | Phase management with test mode lock-out |
| SEF3 | Protection against snooping |

| TOE Security Function | Addressed issue |
|---|---|
| SEF4 | Data encryption and data disguising |
| SEF5 | Random number generation |
| SEF6 | TSF self test |
| SEF7 | Notification of physical attack |
| SEF8 | Memory Management Unit (MMU) |
| SEF9 | Cryptographic support |

Table 1: TOE Security Functions

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

The claimed TOE's strength of functions 'high' (SOF-high) for specific functions as indicated in the Security Target [6, chapter 6] is confirmed. The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). For details see chapter 9 of this report.

The assets to be protected by the TOE are defined in the Security [6, chapter 3.1]. Based on these assets the security environment is defined in terms of assumptions, threats and policies. This is outlined in the Security Target [6 , chapter 3.2 to 3.4].

This certification covers the following configurations of the TOE:

- SLE66CX680PE / m1534-a14 with RSA2048 V1.5 (produced in Dresden/Germany)
- SLE66CX360PE / m1536-a14 with RSA2048 V1.5 (produced in Dresden/Germany)
- SLE66CX482PE / m1577-a14 with RSA2048 V1.5 (produced in Dresden/Germany)
- SLE66CX480PE / m1565-a14 with RSA2048 V1.5 (produced in Dresden/Germany)
- SLE66CX182PE / m1564-a14 with RSA2048 V1.5 (produced in Dresden/Germany)

For more details refer to chapter 8.

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:

SLE66CX680PE / m1534-a14, SLE66CX360PE / m1536-a14, SLE66CX482PE / m1577-a14, SLE66CX480PE / m1565-a14, SLE66CX182PE / m1564-a14, all optional with RSA2048 V1.5 and all with specific IC dedicated software

The following table outlines the TOE deliverables:

| No | Type | Identifier | Release | Form of delivery |
|---|---|---|---|---|
| 1 | HW | SLE66CX680PE Smart Card IC | GDS-file-ID: m1534-a14 with production line indicator: “2” (Dresden) | Wafer or packaged module |
| | | SLE66CX360PE Smart Card IC | GDS-file-ID: m1536-a14 with production line indicator: “2” (Dresden) | Wafer or packaged module |
| | | SLE66CX482PE Smart Card IC | GDS-file-ID: m1577-a14 with production line indicator: “2” (Dresden) | Wafer or packaged module |
| | | SLE66CX480PE Smart Card IC | GDS-file-ID: m1565-a14 with production line indicator: “2” (Dresden) | Wafer or packaged module |
| | | SLE66CX182PE Smart Card IC | GDS-file-ID: m1564-a14 with production line indicator: “2” (Dresden) | Wafer or packaged module |
| 2 | FW | STS Self Test Software (the IC Dedicated Test Software) | V55.0B.07 | Stored in Test ROM on the IC |
| 3 | FW | RMS Resource Management System (the IC Dedicated Support Software) | V2.5 | Stored in reserved area of User ROM on the IC |
| 4 | SW | RSA2048 library (optional) | V1.5 | Source code in electronic form |
| 5 | DOC | Data Book – SLE 66CxxxPE / MicroSlim Security Controller Family incl. the errata sheet | 07.05 | Hardcopy and pdf-file |
| 6 | DOC | Security Programmers’ Manual - SLE66C(L)xxxP(E) Controllers | 08.07 | Hardcopy and pdf-file |
| 7 | DOC | Errata & delta Sheet – SLE 66CxxxPE / MicroSlim Security Controller Family Controllers – Products and Boundout | 11.07 | Hardcopy and pdf-file |
| 8 | DOC | Security & Chip Card ICs – SLE 66CxxxPE – Instruction Set | 07.04 | Hardcopy and pdf-file |
| 9 | DOC | Security &Chip Card ICs SLE 66CxxxPE– Instruction Set and Special Function Registers – Quick Reference | 05.04 | Hardcopy and pdf-file |
| 10 | DOC | RSA 2048 bit Support SLE66C(L)XxxxPE – RSA Interface Specification for library V1.5 | 01.2007 | Hardcopy and pdf-file |
| 11 | DOC | RSA 2048 bit Support SLE66C(L)XxxxPE – Arithmetic Library for V1.5 | 01.2007 | Hardcopy and pdf-file |
| 12 | DOC | [12]..[25] Application Notes | see list in section13 | Hardcopy and pdf-file |

Table 2: Deliverables of the TOE

The hardware part of the TOE is identified by SLE66CX680PE / m1534-a14, SLE66CX360PE / m1536-a14, SLE66CX482PE / m1577-a14, SLE66CX480PE / m1565-a14 and SLE66CX182PE / m1564-a14. Another characteristic of the TOE is a serial number (chip identification number). This serial number is chip specific as the wafer, production date, chip type (chip type specifies the mask version number skipping the last digit - here e1 is issued -, whereby the assignment is done by using [11, Table 2-36 and chapter 7.9]) and the coordinates on the wafer are part of the number. The serial number, which is accessible in the chip identification mode, is linked to the version number. In the tool Workstream one can reconstruct which version number belongs to which serial number. For the format of the serial number see [11, 7.9].

The chip type byte identifies the different versions in the following manner:

- 91 hex for version m1534-a1(x),
- 93 hex for version m1536-a1(x),
- AE hex for version m1577-a1(x),
- AD hex for version m1565-a1(x),
- A1 hex for version m1564-a1(x).

Using the additional detailed production parameter bytes, one can reconstruct the last character (x) of the version number of a specific chip via a data base system at Infineon Logistic Department. The first nibble of the batch number [11, 7] gives the production line indicator which is "2" for chip version manufactured in Infineons IC fabrication in Dresden, Germany.

The RSA2048 library, as separate software part of the TOE, as well as RMS and STS, as firmware parts of the TOE, are identified by their unique version numbers. Note: The TOE can be delivered with or without the RSA library. As the RMS is part of the ROM mask, one can get the RMS version number for a specific chip by using the ROM type bytes and asking the data base system at Infineon Logistic Department.

# 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:

The security policy of the TOE is to provide basic Security Functions to be used by the smart card operating system and the smart card application thus providing an overall smart card system security. Therefore, the TOE will implement an algorithm to ensure the confidentiality of plain text data by encryption and to support secure authentication protocols and it will provide a random number generator.

As the TOE is a hardware security platform, the security policy of the TOE is also to provide protection against leakage of information (e.g. to ensure the confidentiality of cryptographic keys during Triple-DES cryptographic functions performed by the TOE), against physical probing, against malfunctions, against physical manipulations and against abuse of functionality. Hence the TOE shall

- maintain the integrity and the confidentiality of data stored in the memory of the TOE and
- maintain the integrity, the correct operation and the confidentiality of Security Functions (security mechanisms and associated functions) provided by the TOE.

# 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: Usage of Hardware Platform, Treatment of User Data, Protection during TOE Development and Production, Protection during Packaging, Finishing and Personalisation. Details can be found in the Security Target [6, chapter 4.2].

# 5 Architectural Information

The Infineon Smart Card ICs (Security Controller) SLE66CX680PE / m1534-a14, SLE66CX360PE / m1536-a14, SLE66CX482PE / m1577-a14, SLE66CX480PE / m1565-a14, SLE66CX182PE / m1564-a14, all optional with RSA2048 V1.5 and all with specific IC dedicated software are integrated circuits (IC) providing a platform to a smart card operating system and smart card application software. A top level block diagram and a list of subsystems can be found within the TOE description of the Security Target. The complete hardware description and the complete instruction set of the TOE is to be found in the Data Book [11] and other guidance documents delivered to the customer, see table 2.

For the implementation of the TOE Security Functions basically the central processing unit (CPU) with memory management unit (MMU), RAM, ROM, EEPROM, security logic, interrupt module, bus system, Random Number Generator (RNG) and the cryptographic operations of the chip are used. Security measures for physical protection are realised within the layout of the whole circuitry.

The Special Function Registers, the CPU instructions and the various on-chip memories provide the interface to the software using the Security Functions of the TOE.

The TOE IC Dedicated Test Software (STS), stored on the chip, is used for testing purposes during production only and is completely separated from the use of the embedded software by disabling before TOE delivery.

The TOE IC Dedicated Support Software (RMS), stored on the chip, is used for EEPROM programming and Security Function testing. It is stored by the TOE manufacturer in a reserved area of the normal user ROM and can be used by the users embedded software.

The software part of the TOE consists of the RSA2048 library. The TOE includes also functionality to calculate single DES operations, but part of the evaluation is the Triple-DES operation only.

# 6 Documentation

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

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

# 7 IT Product Testing

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

- Simulation tests: These tests are performed before starting the production to develop the technology for the production and to define the process parameters.
- Qualification tests: These tests are performed after the first production of chips. The tests are performed in test mode. With these tests the influence of temperature, frequency, and voltage on the security functions are tested in detail.
- Verification tests: These tests are performed in normal mode and check the functionality in the end user environment. The results of the qualification and verification tests are the basis on which it is decided, whether the TOE is released to production.
- Security evaluation tests: These tests are performed in normal mode and check the security mechanisms aiming on the security functionality and the effectiveness of the mechanisms. The random numbers are tested as required by AIS 31 and fulfill the criteria.
- Production tests: These tests are performed at each TOE before delivery. The aim of the production tests is to check whether each chip is functioning correctly.
- Penetration Tests: Penetration Tests are performed to find security flaws in the product.

The developer tests cover all Security Functions and all security mechanisms as identified in the functional specification, the high level design and the low level design. Chips from the production site in Dresden (see part D, annex A of this report) were used for tests.

The evaluators testing effort can be summarised into the following classes of tests: Module tests, Simulation tests, Emulation tests, Tests in user mode, Tests in test mode and Hardware tests. The evaluators performed independent tests to supplement, augment and to verify the tests performed by the developer by sampling. Besides repeating exactly the developers tests, test parameters were varied and additional analysis was done. With these kind of tests performed in the developer's testing environment the entire security functionality of the TOE was verified. Overall the evaluators have tested the TSF systematically against the functional specification, the high-level design and the low-level design.

The evaluators supplied evidence that the current version of the TOE with production line indicator "2" for Dresden provides the Security Functions as specified.

For this re-evaluation the evaluators re-assessed the penetration testing and confirmed the results from the previous certification procedure BSI-DSZ-CC-0399-2007 where they took all Security Functions into consideration. Intensive penetration testing was performed at that time to consider the physical tampering of the TOE using highly sophisticated equipment and expertised know-how. Specific additional penetration attacks were performed in the course of this evaluation.

# 8 Evaluated Configuration

This certification covers the following configurations of the TOE:

- SLE66CX680PE / m1534-a14 with RSA2048 V1.5 library (produced in Dresden),
- SLE66CX360PE / m1536-a14 with RSA2048 V1.5 library (produced in Dresden),
- SLE66CX482PE / m1577-a14 with RSA2048 V1.5 library (produced in Dresden),
- SLE66CX480PE / m1565-a14 with RSA2048 V1.5 library (produced in Dresden),

- SLE66CX182PE / m1564-a14 with RSA2048 V1.5 library (produced in Dresden).

All with the specific IC Dedicated Software and with production line indicator “2” for Dresden, Germany. After delivery the TOE only features one fixed configuration (user mode), which cannot be altered by the user. The TOE was tested in this configuration. All the evaluation and certification results therefore are only effective for this version of the TOE. For all evaluation activities performed in test mode, there was a rationale why the results are valid for the user mode, too.

# 9 Results of the Evaluation

## 9.1 CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The evaluation methodology CEM [2] was used for those components used 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).

The following guidance specific for the technology was used:

(i) The Application of CC to Integrated Circuits

(ii) The Application of Attack Potential to Smartcards

(iii) Functionality classes and evaluation methodology of physical random number generators

(see [4], AIS 25, AIS 26, AIS 31) were used.

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

- All components of the class ASE
- All components of the EAL 5 augmented package as defined in the CC (see also part C of this report)
- The components ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4 augmented for this TOE evaluation.
- All components claimed in the Security Target [6, chapter 6] and defined in the CC (see also part C of this report)

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0322-2007, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on changed Hardware and implemented cryptolibrary RSA2048 .

The evaluation has confirmed:

- for PP Conformance Smartcard IC Platform Protection Profile, Version 1.0, July 2001, Eurosmart, BSI-PP-0002-2001 [9]
- for the functionality: PP conformant plus product specific extensions
  Common Criteria Part 2 extended

- for the assurance: Common Criteria Part 3 conformant
  EAL 5 augmented by
  ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4
- The following TOE Security Functions fulfil the claimed Strength of Function: high

  SEF2 – Phase management with test mode lock-out,
  SEF3 – Protection against snooping,
  SEF4 – Data encryption and data disguising,
  SEF5 – Random number generation

In order to assess the strength of function the scheme interpretations AIS 25,26 and AIS 31 (see [4]) were used. 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 rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). This holds for: SEF9.

The TOE is equipped with several hardware accelerators to support the standard cryptographic operations. This security enforcing function is introduced to include the cryptographic operation in the scope of the evaluation as the cryptographic function itself is not used from the TOE security policy. On the other hand these functions are of special interest for the use of the hardware as platform for the software. The components are a hardware DES encryption unit and a combination of software and hardware unit to support RSA cryptography and RSA key generation. The key for the cryptographic Triple-DES operations are provided from the Smartcard Embedded Software.

The strength of the cryptographic algorithms was not rated in the course of this evaluation (see BSIG Section 4, Para. 3, Clause 2). The validity period of each algorithm and its bitlength is recommended in the official catalogue [26].

## 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. The TOE is delivered to the Smartcard Embedded Software Developer and the Card Manufacturer. The actual end user obtains the TOE from the Card Manufacturer together with the application which runs on the TOE. The Smartcard Embedded Software Developer receives all necessary recommendations and hints to develop his software in form of the delivered application notes. In addition, the following aspects need to be fulfilled when using the TOE:

- All security hints described in [11], [27]..[29] and the delivered application notes [12].. [25] have to be considered.
- Especially the recommendation in [27, chapter 4] should be followed.

In addition the following assumptions and requirements concerning external security measures, explicitly documented in the singles evaluation reports, have to be fulfilled:

- Requirement resulting from ADO_DEL:

  - As the TOE is under control of the user software, the chip manufacturer can only guarantee the integrity up to the delivery procedure. It is in the responsibility of the Smartcard Embedded Software Developer to include mechanisms in the implemented software which allows detection of modifications after the delivery.
  - The Smartcard Embedded Software Developer should not accept deliverables from Infineon he had not requested. All confidential information sent in electronic form has to be accepted only in encrypted form.
- Requirement resulting from AGD_ADM and AGD_USR:
  In the environment the following assumption has to be fulfilled:
  - “Protection during packaging, finishing and personalisation” resulting from A.Process-Card: It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end-user to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use). This means that the Phases after TOE Delivery are assumed to be protected appropriately.
  - In addition the development environment of the operating system developer has to be protected adequately, in order to be able to guarantee the security of the TOE on the whole.
- Requirement resulting from AGD_ADM and AGD_USR:
  The following requirements of the environment defined in [6] has to be taken into consideration from the Smartcard Embedded Software Developer:
  - For Triple-DES: “Cryptographic key generation“ resulting from FCS_CKM.1, or “Import of user data without security attributes” resulting from FDP_ITC.1, or “Import of user data with security attributes” resulting from FDP_ITC.2
  - For RSA (if the RSA library is selected): “Cryptographic key generation“ resulting from FCS_CKM.1 (optional), or “Import of user data without security attributes” resulting from FDP_ITC.1, or “Import of user data with security attributes” resulting from FDP_ITC.2
  - “Cryptographic key destruction“ resulting from FCS_CKM.4 (for Triple-DES, RSA (optional) and
  - “Secure security attributes” resulting from FMT_MSA.2 (for Triple-DES, RSA (optional)).
- Requirement resulting from AVA_MSU:
  During development of the Smartcard Embedded Software the correct configuration of the following parameters has to be checked:
  - Wait states functionality is activated for all operations of the Embedded Software critical for side channel attacks (e.g. SPA/DPA),
  - FCURSE functionality is activated for all operations of the Embedded Software critical for side channel attacks (e.g. SPA/DPA),
  - parameters for memory encryption E0ADR, E2ADR and E2ENC (XKEY) which the ranges of of encryption are configured correct,

  - The SW comparison of random numbers to/with regard to the active shielding is correctly implemented,
  - MMU is configured correct,
  - calls of the self test of the TSF implemented in the RMS routines to detect failures of the sensors are implemented. Depending on the application (e.g. time between possible resets) the developer of the Smartcard Embedded Software has to decide how often this function has to be executed during normal operation. The self test shall be executed at least once during security relevant operation (e.g. key generation).
  - call of the test of the random number generation to detect failures of the RNG is implemented.
  - Application of the security advices given in [11, chapter 19.9], [27], and [20].
- Recommendation resulting from AVA_VLA
  - The TOE has implemented a hardware DES accelerator. In case the keys necessary for the calculation of the DES are transferred into the DES accelerator, these keys can be spied out by means of a SPA/DPA. In order to prevent this, the transfer of the keys has to be protected using the measures described in [13].
  - The TOE does not implement a padding scheme for the RSA signature creation/verification. This has to be implemented by the embedded software. To counter known attacks against incorrect padding a complete check of padding regarding correctness is mandatory.
  - If the key parameters of the signature generation are stored in the RAM, a Bellcore attack is possible. Therefore the embedded software has to check the consistency of the key parameters handed over by the RSA signature generation function after call of the function, e.g. by means of a CRC.
- Recommendation resulting from ADV_LLD:
  - Because of the possibility to overwrite functions of the RSA2048 library (delivered to the smartcard embedded software developer in form of source code), it is pointed out that only the usage of the original RSA2048 library V1.5 is evaluated. For example the function AceGetRnd_sec can be overwritten with another function which uses not the true random number generator (K3) but pseudorandom numbers.
- Periodically a new official catalogue is published on the homepage of the German Federal Network Agency. The current version of the catalogue holds for the strength of the TOE`s cryptographic signature algorithms. The user is obliged to take the information of the current version of [26, published February 5th, 2008, page 376] into account. The periods of the recommended usage of the TOEs algorithms for encryption and decryption listed in 9.2 are
  - Signature creation and verification using RSA encryption, decryption and key generation with a keylength from 1024 to 2048 bits. A usage of 2048 bits is recommended. From 1974 bits keylenght the current recommended period of usage is by the end of 2014 [26].

- Signature creation and verification according to ECDSA and Elliptic Curve (EC) key generation standard with 192 - 521 bits key sizes. From 224 bits keylenght the current recommended period of usage is by the end of 2014 [26].

This data is deplaced by a new version of [26].

# 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

**ACE** Advanced Crypto Engine

**API** Application Programming Interface

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

**CBC** Cipher Block Chaining

**CC** Common Criteria for IT Security Evaluation

**CRC** Checksum module

**CPU** Central Processing Unit

**DES** Data Encryption Standard; symmetric block cipher algorithm

**DDC** DES accelerator

**DPA** Differential Power Analysis

**EAL** Evaluation Assurance Level

**ECB** Electrical Code Block

**ECC** Elliptic Curve Cryptography

**EEPROM** Electrically Erasable Programmable Read Only Memory

**EMA** Electro magnetic analysis

**ETR** Evaluation Technical Report

**IC** Integrated Circuit

**IT** Information Technology

**ITSEF** Information Technology Security Evaluation Facility

**MED** Memory Encryption and Decryption unit

**MMU** Memory Management Unit

**PP** Protection Profile

**RAM** Random Access Memory

**RNG** Random Number Generator

**ROM** Read Only Memory

| | |
|---|---|
| **RSA** | Rivest, Shamir, Adleman – a public key encryption algorithm |
| **RMS** | Resource Management System |
| **SEF** | Security Function |
| **SFP** | Security Function Policy |
| **SFR** | Security Functional Requirement |
| **SOF** | Strength of Function |
| **SPA** | Simple power analysis |
| **ST** | Security Target |
| **STS** | Self Test Software |
| **SW** | Software |
| **TOE** | Target of Evaluation |
| **Triple-DES** | Symmetric block cipher algorithm based on the DES |
| **TSC** | TSF Scope of Control |
| **TSF** | TOE Security Functions |
| **TSP** | TOE Security Policy |
| **TSS** | TOE Summary Specification |
| **UCP** | Unified Channel Programming |

## 12.2 Glossary

**Augmentation** - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance 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 entity within the TSC that contains or receives information and upon which subjects perform operations.

**Protection Profile** - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

**Security Function** - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

**Security Target** - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

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

**Strength of Function** - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

**SOF-basic** - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

**SOF-medium** - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

**SOF-high** - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

**Subject** - An entity within the TSC that causes operations to be performed.

**Target of Evaluation** - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

**TOE Security Functions** - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

**TOE Security Policy** - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

**TSF Scope of Control** - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

# 13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

[2] Common Methology for Information Technology Security Evaluation (CEM), Evaluation Methology, Version 2.3, August 2005

[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 on the BSI Website

[6] Security Target BSI-DSZ-CC-0437, SLE66CX680PE / m1534-a14, SLE66CX360PE / m1536-a14, SLE66CX482PE / m1577-a14, SLE66CX480PE / m1565-a14, SLE66CX182PE / m1564-a14, All Products with RSA2048 library, Version 1.3, 2007-03-22, Infineon AG

[7] Evaluation Technical Report, Version 3, 2008-04-02, 8102967591 / BSI-DSZ-CC-0437, Product: SLE66CX680PE / m1534-a14, SLE66CX360PE / m1536-a14, SLE66CX482PE / m1577-a14, SLE66CX480PE / m1565-a14, SLE66CX182PE / m1564-a14, All Products with RSA2048 V1.5 library, TÜViT (confidential document)

[8] Configuration list for the TOE, Configuration Management Scope (ACM_SCP), SLE66CX680PE / m1534-a14, SLE66CX360PE / m1536-a14, SLE66CX482PE / m1577-a14, SLE66CX480PE / m1565-a14, SLE66CX182PE / m1564-a14, all Products with RSA2048 V1.5, Version 1.4, 10.08.2007 Infineon (confidential document)

[9] Smart card IC Platform Protection Profile, Version 1.0, July 2001, BSI registration ID: BSI-PP-0002-2001, developed by Atmel Smart Card ICs, Hitachi Ltd., Infineon Technologies AG, Philips Semiconductors

[8] specifically

- AIS 25, Version 3, 6 August 2007, Anwendung der CC auf Integrierte Schaltungen including JIL Document resp. CC Supporting Document
- AIS 26, Version 3, 6 August 2007, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document resp. 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 1.00, 1 June 2004, 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 resp. CC Supporting Document and CCRA policies
- AIS 36, Version 2, 12 November 2007, Kompositionsevaluierung including JIL Document resp. CC Supporting Document
- AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results

[10] ETR for composite evaluation according to AIS 36, 8102967591 / BSI-DSZ-CC-0437, SLE66CX680PE / m1534-a14, SLE66CX360PE / m1536-a14, SLE66CX482PE / m1577-a14, SLE66CX480PE / m1565-a14, SLE66CX182PE / m1564-a14, all products with RSA2048 V1.5 library, Version 1, 2008-04-01, Infineon Technologies AG, TÜViT, (confidential document)

[11] Data Book – SLE 66CxxxPE / MicroSlim Security Controller Family, incl. the errata sheet [DB_ErrSh], Version 07.05, 01.07.2005, Infineon.

[12] Application Note, SLE66CXxxS Using CRC (PDF+SW),Version 03.01, 03.2001 Infineon

[13] Application Note, SLE66CxxxP, DDES - EC2 Accelerator including complementary, Version 04.02, 2004-02 and Application Note SLE 66CxxxPE DDES Accelerator, Version 07.05, 2005-07, Infineon

[14] Application Note, SLE66CxxxPE, Using MicroSlim NVM (cLib), confidential, version 05.05, 05.2005, Infineon

[15] Application Note, SLE66CxxxP/PE, Memory Encryption Decryption, confidential Version 11.04, 11.2004, Infineon

[16] Application Note, SLE66CxxxPE, MMU-Memory Management Unit (PDF+SW), confidential, Version 12.04, 12.2004, Infineon

[17] Application Note, SLE66CxxxP, MMU Security Issues (PDF) confidential, Version 01.02, 01.2002, Infineon

[18] Application Note, SLE66CxxxP/PE, Testing the RNG, confidential, Version 11.04, 11.2004 Infineon

[19] Application Note, SLE66CxxxP/PE, Using RNG a.t. FIPS140 (PDF+SW), confidential, Version 02.04, 02.2004, Infineon

[20] Application Note, SLE66CxxxPE, Security Advice, (PDF+SW) confidential, Version 05.04, 05.2004, Infineon

[21] Application Note, SLE 66CxxS, Secure Hash Algorithm SHA-, confidential, Version 01.98, 01.1998, Infineon

[22] Application Note, SLE66CxxxPE, Using the active shield, confidential, Version 12.04, 12.2004, Infineon

[23] Application Note, SLE66CxxxP, UART (PDF+SW), confidential, Version 10.03, 10.2003, Infineon

[24] Application Note, SLE66CxxxPE - UART basic (PDF), Version 02.07, 02.2007, Infineon

[25] Application Note, SLE66CxxxPE - Static UART (PDF), Version 01.07, 02.2007, Infineon

[26] Regulierungsbehörde für Telekommunikation und Post: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), German "Bundesanzeiger Nr. 19", published February 5th, 2008, page 376

[27] Security Programmers' Manual, SLE66C(L)xxxP(E) Controllers, Version 08.07, 08.2007, Infineon

[28] RSA 2048 bit Support SLE66C(L)XxxxPE RSA Interface Specification for library V1.5, 01.2007 2007-01 Infineon

[29] RSA 2048 bit Support SLE66CXxxxPE– Arithmetic Library for V1.5, 01.2007, Infineon

# C Excerpts from the Criteria

CC Part1:

**Conformance results** (chapter 7.4)

„The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to CC Part 2 (functional requirements), CC Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

- **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.
- **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

- **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.
- **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

- **Package name Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.
- **Package name Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

- **PP Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.“

CC Part 3:

**Protection Profile criteria overview** (chapter 8.2)

“The goal of a PP evaluation is to demonstrate that the PP is complete, consistent, technically sound, and hence suitable for use as a statement of requirements for one or more evaluatable TOEs. Such a PP may be eligible for inclusion within a PP registry.”

| **“Assurance Class** | **Assurance Family** |
|---|---|
| Class APE: Protection Profile evaluation | TOE description (APE_DES) |
| | Security environment (APE_ENV) |
| | PP introduction (APE_INT) |
| | Security objectives (APE_OBJ) |
| | IT security requirements (APE_REQ) |
| | Explicitly stated IT security requirements (APE_SRE) |

Table 3 - Protection Profile families - CC extended requirements ”

**Security Target criteria overview** (Chapter 8.3)

“The goal of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.”

| **“Assurance Class** | **Assurance Family** |
|---|---|
| Class ASE: Security Target evaluation | TOE description (ASE_DES) |
| | Security environment (ASE_ENV) |
| | ST introduction (ASE_INT) |
| | Security objectives (ASE_OBJ) |
| | PP claims (ASE_PPC) |
| | IT security requirements (ASE_REQ) |
| | Explicitly stated IT security requirements (ASE_SRE) |
| | TOE summary specification (ASE_TSS) |

Table 5 - Security Target families - CC extended requirements ”

**Assurance categorisation** (chapter 7.5)

“The assurance classes, families, and the abbreviation for each family are shown in Table 1.

| Assurance Class | Assurance Family |
|---|---|
| ACM: Configuration management | CM automation (ACM_AUT) |
| | CM capabilities (ACM_CAP) |
| | CM scope (ACM_SCP) |
| ADO: Delivery and operation | Delivery (ADO_DEL) |
| | Installation, generation and start-up (ADO_IGS) |
| ADV: Development | Functional specification (ADV_FSP) |
| | High-level design (ADV_HLD) |
| | Implementation representation (ADV_IMP) |
| | TSF internals (ADV_INT) |
| | Low-level design (ADV_LLD) |
| | Representation correspondence (ADV_RCR) |
| | Security policy modeling (ADV_SPM) |
| AGD: Guidance documents | Administrator guidance (AGD_ADM) |
| | User guidance (AGD_USR) |
| ALC: Life cycle support | Development security (ALC_DVS) |
| | Flaw remediation (ALC_FLR) |
| | Life cycle definition (ALC_LCD) |
| | Tools and techniques (ALC_TAT) |
| ATE: Tests | Coverage (ATE_COV) |
| | Depth (ATE_DPT) |
| | Functional tests (ATE_FUN) |
| | Independent testing (ATE_IND) |
| AVA: Vulnerability assessment | Covert channel analysis (AVA_CCA) |
| | Misuse (AVA_MSU) |
| | Strength of TOE security functions (AVA_SOF) |
| | Vulnerability analysis (AVA_VLA) |

Table 1: Assurance family breakdown and mapping”

**Evaluation assurance levels** (chapter 11)

“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 11.1)

“Table 6 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 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 extended with explicitly stated assurance requirements.

| Assurance Class | Assurance Family | Assurance Components by Evaluation Assurance Level | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | EAL1 | EAL2 | EAL3 | EAL4 | EAL5 | EAL6 | EAL7 |
| Configuration management | ACM_AUT | | | | 1 | 1 | 2 | 2 |
| | ACM_CAP | 1 | 2 | 3 | 4 | 4 | 5 | 5 |
| | ACM_SCP | | | 1 | 2 | 3 | 3 | 3 |
| Delivery and operation | ADO_DEL | | 1 | 1 | 2 | 2 | 2 | 3 |
| | ADO_IGS | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Development | ADV_FSP | 1 | 1 | 1 | 2 | 3 | 3 | 4 |
| | ADV_HLD | | 1 | 2 | 2 | 3 | 4 | 5 |
| | ADV_IMP | | | | 1 | 2 | 3 | 3 |
| | ADV_INT | | | | | 1 | 2 | 3 |
| | ADV_LLD | | | | 1 | 1 | 2 | 2 |
| | ADV_RCR | 1 | 1 | 1 | 1 | 2 | 2 | 3 |
| | ADV_SPM | | | | 1 | 3 | 3 | 3 |
| Guidance documents | AGD_ADM | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | AGD_USR | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Life cycle support | ALC_DVS | | | 1 | 1 | 1 | 2 | 2 |
| | ALC_FLR | | | | | | | |
| | ALC_LCD | | | | 1 | 2 | 2 | 3 |
| | ALC_TAT | | | | 1 | 2 | 3 | 3 |
| Tests | ATE_COV | | 1 | 2 | 2 | 2 | 3 | 3 |
| | ATE_DPT | | | 1 | 1 | 2 | 2 | 3 |
| | ATE_FUN | | 1 | 1 | 1 | 1 | 2 | 2 |
| | ATE_IND | 1 | 2 | 2 | 2 | 2 | 2 | 3 |
| Vulnerability assessment | AVA_CCA | | | | | 1 | 2 | 2 |
| | AVA_MSU | | | 1 | 2 | 2 | 3 | 3 |
| | AVA_SOF | | 1 | 1 | 1 | 1 | 1 | 1 |
| | AVA_VLA | | 1 | 1 | 2 | 3 | 4 | 4 |

Table 6: Evaluation assurance level summary”

**Evaluation assurance level 1 (EAL1) - functionally tested** (chapter 11.3)

“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 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, and that it provides useful protection against identified threats.”

**Evaluation assurance level 2 (EAL2) - structurally tested** (chapter 11.4)

“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 practice. 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 11.5)

“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 practices.

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 11.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices 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 11.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices 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 11.8)

“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 11.9)

“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.“

**Strength of TOE security functions (AVA_SOF)** (chapter 19.3)

“Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim."

**Vulnerability analysis (AVA_VLA)** (chapter 19.4)

"Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users."

"Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis."

"Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential."

# 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 37

This page is intentionally left blank.

# Annex B of Certification Report BSI-DSZ-CC-0437-2008

## Evaluation results regarding development and production environment

The IT products SLE66CX680PE / m1534-a14, SLE66CX360PE / m1536-a14, SLE66CX482PE / m1577-a14, SLE66CX480PE / m1565-a14, SLE66CX182PE / m1564-a14, all optional with RSA2048 V1.5 and all with specific IC dedicated software (Target of Evaluation, TOE) have been evaluated at an accredited and licensed / approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 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 2.3 (ISO/IEC 15408:2005) .

As a result of the TOE certification, dated 27 May 2008, the following results regarding the development and production environment apply. The Common Criteria assurance requirements

- **ACM – Configuration management (i.e. ACM_AUT.1, ACM_CAP.4, ACM_SCP.3),**
- **ADO – Delivery and operation (i.e. ADO_DEL.2, ADO_IGS.1) and**
- **ALC – Life cycle support (i.e. ALC_DVS.2, ALC_LCD.2, ALC_TAT.2),**

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

a) Infineon Technologies Dresden GmbH & Co. OHG, Königsbrücker Str. 180, 01099 Dresden, Germany

b) Amkor Technology Philippines, Km. 22 East Service Rd., South Superhighway, Muntinlupa City 1702, Philippines and Amkor Technology Philippines, 119 North Science Avenue, Laguna Technopark, Binan, Laguna 4024, Philippines (Module Mounting)

c) Infineon Technologies AG, Secure Mobile Solutions, Alter Postweg 101, 86159 Augsburg, Germany (Development)

d) Toppan Photomask Inc. (former DuPont), Rähnitzer Allee 9, 01109 Dresden, Germany (Mask Center)

e) Assa Abloy Identification Technologies GmbH (former Sokymat GmbH), In den Weiden 4b, 99099 Erfurt, Germany (Distribution Center)

f) Infineon Technologies Austria AG, Development Center Graz, Babenbergerstr. 10, 8020 Graz, and Infineon Technologies Austria AG, Siemensstr. 2, 9500 Villach, Austria Infineon Technologies Austria AG Lakeside B05, 9020 Klagenfurt, Austria (Development)

g) Infineon Technology AG, DCE, Kühne & Nagel, Stockstädter Strasse 10 - Building 8A, 63762 Grossostheim (Distribution center)

h) Kuehne & Nagel, 30805 Santana Street, Hayward, CA 94544, U.S.A. (Distribution Center)

i) Infineon Technologies AG, Am Campeon 1-12, 85579 Neubiberg, and Infineon Technologies AG, Otto-Hahn-Ring 6, 81739 Munich (Perlach), Germany (Development)

j) Infineon Technologies AG, Wernerwerkstr. 2, 93049 Regensburg, Germany (Module Mounting with inlay antenna mounting)

k) Exel Singapore Pte Ltd, Exel Supply Chian Hub, 81, ALPS Avenue, Singapore (Distribution Center)

l) Kintetsu World Express, Inc., Tokyo Import Logistics Center, Narita Terminal, Tokyo, Japan (Distribution Center)

m) Infineon Technologies (Wuxi) Co. Ltd., No. 118, Xing Chuang San Lu, Wuxi-Singapore Industrial Park, Wuxi 214028, Jiangsu, P.R. China (Module Mounting)

The chip versions of the TOE are manufactured in Infineons IC fabrication in Dresden, Germany, indicated by the first nibble of the batch number which gives the production line indicator "2" for Dresden.

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.