Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0629-2010

for

Infineon Smart Card IC (Security Controller) SLE66CX162PE / m1531-a25 and SLE66CX80PE / m1533-a25 all with optional libraries RSA V1.6, EC V1.1, SHA-2 V1.0 and both 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-0629-2010

Infineon Smart Card IC (Security Controller) SLE66CX162PE / m1531-a25 and SLE66CX80PE / m1533-a25 all with optional libraries RSA V1.6, EC V1.1, SHA-2 V1.0 and both with specific IC dedicated software

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 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, 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, 11 June 2010
For the Federal Office for Information Security

SOGIS IT SECURITY CERTIFIED

Bernd Kowalski L.S.
Head of Department

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 2.3 (ISO/IEC 15408:2005)[5] [1]
- Common Methodology for IT Security Evaluation, Version 2.3 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]
- 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 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

2.1 European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and in addition at higher recognition levels for IT-Products related to certain technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic).

The new agreement was initially signed by the national bodies of Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the the United Kingdom.

Within the terms of this agreement the German Federal Office for Information Security (BSI) recognises

- for the basic recognition level certificates issued as of April 2010 by the national certification bodies of France, The Netherlands, Spain and United Kingdom.
- for the higher recognition level in the technical domain Smart card and similar Devices certificates issued as of April 2010 by the national certification bodies of France, The Netherlands and the United Kingdom.

In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

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

Historically, the first SOGIS-Mutual Recognition Agreement Version 1 (ITSEC only) became initially effective in March 1998. It was extended in 1999 to include certificates based on the Common Criteria (MRA Version 2). Recognition of certificates previously issued under these older versions of the SOGIS-Mutual Recognition Agreement is being continued.

2.2 International Recognition of CC – Certificates (CCRA)

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

As of 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 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 product Infineon Smart Card IC (Security Controller) SLE66CX162PE / m1531-a25 and SLE66CX80PE / m1533-a25 all with optional libraries RSA V1.6, EC V1.1, SHA-2 V1.0 and both with specific IC dedicated software has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0470-2008. Specific results from the evaluation process BSI-DSZ-CC-0470-2008 were re-used.

The evaluation of the product Infineon Smart Card IC (Security Controller) SLE66CX162PE / m1531-a25 and SLE66CX80PE / m1533-a25 all with optional libraries RSA V1.6, EC V1.1, SHA-2 V1.0 and both with specific IC dedicated software was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 18 May 2010. 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.

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 evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification).

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

---

[6] Information Technology Security Evaluation Facility

5 Publication

The product Infineon Smart Card IC (Security Controller) SLE66CX162PE / m1531-a25 and
SLE66CX80PE / m1533-a25 all with optional libraries RSA V1.6, EC V1.1, SHA-2 V1.0 and both with specific IC dedicated software 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

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 Infineon Smart Card IC (Security Controller) SLE66CX162PE / m1531-a25 and SLE66CX80PE / m1533-a25 all with optional libraries RSA V1.6, EC V1.1, SHA-2 V1.0 and both with specific IC dedicated software . Compared to the successfully certified forerunner process BSI-DSZ-CC-0470-2008 this TOE comprises the same hardware design as no changes have been introduced. This recertification is processed due to new RSA, EC and SHA-2 libraries.

The ICs consists of a dedicated non standard microprocessor (CPU) with a MMU (Memory Management Unit), several different memories, security logic, a timer, an interrupt-controlled I/O interface, a AIS31 compatible RNG (Random Number Generator), and a checksum module (CRC module) and further components are integrated on the chip too. For fast asymmetric cryptographic calculation performance the TOE has the Advanced Cryptographic Engine (ACE) component implemented. The TOE's block diagram is shown in [6], Figure 1.

This TOE is intended to be used in smart cards particularly for security relevant applications, including high speed security authentication, data encryption or electronic signature. The TOE offers a new, improved standard of integrated security features, thereby meeting the requirements of all smart card applications with contact-based interface such as information integrity, access control, mobile telephone, as well as uses in electronic funds transfer and healthcare systems. 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.

This TOE is intended to be used in smart cards particularly for security relevant applications, including high speed security authentication, data encryption or electronic signature. The TOE offers a new, improved standard of integrated security features, thereby meeting the requirements of all smart card applications with contact-based interface such as information integrity, access control, mobile telephone, as well as uses in electronic funds transfer and healthcare systems. 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 consists of the hardware part as described in [6] chapter 2.2.1, the firmware parts and the software parts as listed in [6] Table 3: Firmware and Library Versions. The RSA, EC, SHA-2 cryptographic and the RMS libraries provide functionality via an API to the Smartcard Embedded Software. The STS firmware for test purposes has an API to the Smartcard Embedded Software as well. The STS is implemented in a separated Test-ROM being part of the TOE. The Smartcard Embedded Software is not part of the TOE.

The user has the possibility to tailor the software part of the TOE during the manufacturing process. Thus the TOE can be delivered including - in free combinations - or not including any of the functionality of the EC crypto library, the RSA crypto library and the SHA-2 crypto library. If the user decides not to use one or all of the crypto library(s) the specific library(s) is (are) not delivered to the user and the accompanying —Additional Specific Security Functionality (O.Add-Functions) Rivest-Shamir-Adleman (RSA) and/ or EC and/or SHA-2 is/are not provided by the TOE. Deselecting one of the libraries does not include the code implementing functionality, which the user decided not to use. Not including the code of the deselected functionality has no impact of any other security policy of the TOE;

it is exactly equivalent to the situation where the user decides just not to use the functionality. The RSA, EC and SHA-2 libraries can be implemented together with the Smartcard Embedded Software in the User-ROM mask. All other Smartcard Embedded Software does not belong to the TOE and is not subject of the evaluation.

The TOE includes also functionality to calculate single DES operations, but part of the evaluation is the triple-DES operation only. For more details and used key lengths please refer to [6], chapter 2.2.2.

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 (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the Assurance Requirements of the Evaluation Assurance Level EAL 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 all 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
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) or 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 9, Para. 4, Clause 2). For details see chapter 9 of this report.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. 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 3.2 to 3.4.

This certification covers the following configurations of the TOE:

- SLE66CX162PE / m1531-a25 with/or without RSA and/or EC and/or SHA-2 (produced in Dresden),
- SLE66CX80PE / m1533-a25 with/or without RSA and/or EC and/or SHA-2 (produced in Dresden).

For more details please 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:

Infineon Smart Card IC (Security Controller) SLE66CX162PE / m1531-a25 and SLE66CX80PE / m1533-a25 all with optional libraries RSA V1.6, EC V1.1, SHA-2 V1.0 and both with specific IC dedicated software

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of delivery
1a	HW	SLE66CX162PE Smart Card IC	GDS-file-ID: m1531-a25 with production line indicator: “2” (Dresden)	Wafer or packaged module
1b	HW	SLE66CX80PE Smart Card IC	GDS-file-ID: m1533-a25 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)*	2.5	Stored in reserved area of User ROM on the IC
4	SW	RSA library (optional)	V1.6	Source code in electronic form
5	SW	EC library (optional)	V1.1	Source code in electronic form
6	SW	SHA-2 library (optional)	V1.0	Source code in electronic form
7	DOC	Data Book – SLE66CxxxPE /MicroSlim Security Controller Family [22]	05.07	Hardcopy and pdf-file
8	DOC	Errata Sheet - SLE66CxxxPE Controllers - Product and Boundout [23]	2009-07-15	Hardcopy and pdf-file
9	DOC	Security Programmers’ Manual - SLE66C(L)xxxP(E) Controllers [27]	2009-03-27	Hardcopy and pdf-file
10	DOC	Security & Chip Card ICs – SLE 66CxxxPE – Instruction Set [25]	07.2004	Hardcopy and pdf-file
11	DOC	Chip Card & Security ICs - SLE66CxxxP – Instruction Set and Special Function Registers – Quick Reference [26]	05.2004	Hardcopy and pdf-file

No	Type	Identifier	Release	Form of delivery
12	DOC	RSA 2048 bit Support SLE66C(L)XxxxPE RSA Interface Specification for library V1.6 (optional) [29]	12.2009	Hardcopy and pdf-file
13	DOC	RSA 2048 bit Support SLE66C(L)XxxxPE – Arithmetic Library for V1.6 (optional) [28]	09.2008	Hardcopy and pdf-file
14	DOC	Elliptic Curve GF(P) Support SLE66C(L)XxxxPE Interface Specification ECC-Library V 1.1 [24]	12.2009	Hardcopy and pdf-file
15	DOC	Application Notes [11]...[21]	see list in section 13	Hardcopy and pdf-file

Table 2: Deliverables of the TOE

The hardware part of the TOE is identified by SLE66CX162PE / m1531-a25 or SLE66CX80PE / m1533-a25. Another characteristic of the TOE is a serial number (chip identification number). This serial number is chip specific as the chip type, lot number, wafer, chip coordinates on the wafer, production date, production site (e.g. upper nibble of (08000AH) “2” stands for Infineon‟s IC fabrication in Dresden/Germany “a”) and design step (e.g. “19” at address (080009H) stands for design step “25”) are part of the number. The serial number, which is accessible in the chip identification mode, is linked to the version number. For the format of the serial number see [Databook, 7.3.5] and [DB_ErrSh, 6.7].

Type	Name	Version number	Chip type
Target of Evaluation	SLE66CX162PE	m1531-a25	94
	SLE66CX80PE	m1533-a25	96
Hardware	Dresden	A25	
Firmware	RMS library	2.5	
	STS	55.0B.07	
Software	RSA library (optional)	V1.6	
	EC library (optional)	V1.1	
	SHA-2 library (optional)	V1.0	

The RSA library, the EC library and the SHA-2 library, as separate software parts of the TOE, as well as RMS and STS, as firmware parts of the TOE, are identified by their unique version numbers.

The TOE can be delivered with or without the RSA library and / or the EC library and / or the SHA-2 library.

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 TOEs 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 two modules for 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 cryptographic libraries RSA, EC and SHA-2 are delivery options. Therefore the TOE may come with free combinations of or without these libraries. In the case of coming without one or any combination of these libraries the TOE does not provide the Additional Specific Security Functionality Rivest-Shamir-Adleman Cryptography (RSA) and/or Elliptic Curve Cryptography (EC) and/or SHA-2.

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 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 (Germany) 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-0470-2008 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 expert know-how. Specific additional penetration attacks were performed in the course of this evaluation.

8 Evaluated Configuration

The SLE66CX162PE and the SLE66CX80PE are identically from hardware perspective. The difference is that in the SLE66CX80PE the memory is blocked to smaller size. All types can be distinguished by a different chip identification. The difference in the memory size does not influence the security of the TOE as neither an asset nor a security enforcing function is affected. Therefore the products are certified together.

This certification covers the above mentioned configurations (see chapter 1) 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 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:

- The Application of CC to Integrated Circuits
- The Application of Attack Potential to Smartcards
- Functionality classes and evaluation methodology of physical random number generators

(see [4], AIS 25, AIS 26, AIS 31)

To support composite evaluations according to AIS 36 the document ETR for composite evaluation [10] was provided and approved. This document provides details of this platform evaluation that have to be considered in the course of a composite evaluation on top. The approval is limited to the end of 2010 if resistance against high attack potential is required and if no attack has been published.

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 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.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0470-2008, re-use of specific evaluation tasks was possible.

The evaluation has confirmed:

- PP Conformance: Smartcard IC Platform Protection Profile, Version 1.0, July 2001, Eurosmart, BSI-PP-0002-2001 [10]
- 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:
- 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.

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.

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

9.2 Results of cryptographic assessment

The following cryptographic algorithms are used by the TOE to enforce its security policy:

- hash functions: SHA-2
- algorithms for the encryption and decryption: RSA, EC, Triple-DES
- This holds for the following security functions: SEF9

The strength of the cryptographic algorithms was not rated in the course of this evaluation (see BSIG Section 9, Para. 4, Clause 2). But Cryptographic functions with a security level of 80 bits or lower can no longer be regarded as secure against attacks with high attack potential without considering the application context. Therefore for these functions it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (www.bsi.bund.de).

The cryptographic functions 2-key Triple DES (2TDES), RSA 1024, provided by the TOE achieve a security level of maximum 80 Bits (in general context).

10 Obligations and Notes for the Usage of the TOE

The operational documents as outlined in Table 4, deliverables of the TOE, contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate. This is specifically the case as the approval of the document ETR for composite evaluation [10] is limited to the end of 2010.

The limited validity for the usage of cryptograhic algortithms as outlined in chapter 9 has to be considered by the user and his system risk management process.

Some security measures are partly implemented in the hardware and require additional configuration or control or measures to be implemented by the IC Dedicated Support Software or Embedded Software.

For this reason the TOE includes guidance documentation (see table 2) which contains guidelines for the developer of the IC Dedicated Support Software and Embedded Software on how to securely use the microcontroller chip and which measures have to be implemented in the software in order to fulfil the security requirements of the Security Target of the TOE.

In the course of the evaluation of the composite product or system it must be examined if the required measures have been correct and effectively implemented by the software. Additionally, the evaluation of the composite product or system must also consider the evaluation results as outlined in the document ETR for composite evaluation [10].

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

All security hints described in the user guidance documentation [22], [27], [28], [29], [24] and the delivered application notes [11]...[21] have to be considered. For secure usage of the TOE the fulfilment of the assumptions about the environment in the Security Target [ST] and especially the recommendations of the Security Programmers Manual [27] have to be taken into account.

Due to the possible probing attack on not encrypted CPU BUS lines, the embedded software developer has to make sure that appropriate software countermeasures are implemented to achieve resistance against high attack potential. The efficiency of the additional countermeasures has to be checked by the embedded software evaluator in view of the application (if required in the context of embedded software application).

Specific care should be taken to the viewpoint of randomization of the BUS:

- Enabling hardware supported countermeasures (RWS = Random Wait States, FCURSE = Functional CURrent Scrambling Engine (dummy operation) or Bus Confusion and the use of these features in the application context.
- Special countermeasures in view of the application developed by the embedded software developer.

11 Security Target

For the purpose of publishing, the Security Target [9] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4])

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
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
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 Book
EC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
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
SAR	Security Assurance Requirement
SEF	Security Function
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
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 Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, 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, SLE66CX162PE / m1531-a25, SLE66CX80PE / m1533-a25 all with op-tional libraries RSA V1.6 and EC V1.1 and SHA-2 V1.0 1.3 2009-10-07, Infineon Technologies AG (Public document)

[7] Evaluation Technical Report – Summary (ETR SUMMARY), BSI-DSZ-CC-0629, SLE66CX162PE / m1531-a25 SLE66CX80PE / m1533-a25 all with optional libraries RSA V1.6 and EC V1.1 and SHA-2 V1.0, Version 3 from 2010-04-27, Evaluation Body for IT Security of TÜV Informationstechnik GmbH (confidential document)

[8] Configuration Management Scope (ACM_SCP), SLE66CX162PE / m1531-a25, SLE66CX80PE / m1533-a25 all with optional libraries RSA V1.6 and EC V1.1 and SHA-2 V1.0 1.1 2010-01-21, Infineon Technologies AG (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

[10] ETR for composition according to AIS 36 for the Product SLE66CX162PE / m1531-a25 SLE66CX80PE / m1533-a25 all with optional libraries RSA V1.6 and EC V1.1

[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, 7 May 2009, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 1, 25 September 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

and SHA-2 V1.0, Version 3 from 2010-04-27, Evaluation Body for IT Security of TÜV Informationstechnik GmbH (confidential document)

[11] Application Note, SLE66CxxxP, DDES - EC2 Accelerator including complementary Application Note SLE 66CxxxPE DDES Accelerator, 04.02/07.05, 2004-02/2005-07

[12] Application Note, SLE66CxxxPE, Using MicroSlim NVM (cLib), confidential, 05.05, 2005-05

[13] Application Note, SLE66CxxxP/PE, Memory Encryption Decryption confidential, 11.04, 2004-11

[14] Application Note, SLE66CxxxPE, MMU-Memory Management Unit (PDF+SW) confidential, 12.04, 2004-12

[15] SLE66C(L)xxxPE - Optimized Usage of Data NVM Above 64k, 08.05, 2005-08

[16] Application Note, SLE66CxxxP/PE, Testing the RNG, confidential, 11.04, 2004-11

[17] Application Note, SLE66CxxxP/PE, Using RNG a.t. FIPS140 (PDF+SW), confidential, 02.04, 2004-02

[18] SLE66C(L)xxxPE Family - Secure Hash Algorithm SHA-2 (SHA 256/224, SHA 512/384) Library Version V1.0, 04.2009, 2009-04

[19] Application Note, SLE66CxxxPE, Using the active shield, confidential, 12.04, 2004-12

[20] Application Note, SLE66CxxxPE - UART basic (PDF), 02.07, 2007-02

[21] Application Note, SLE66CxxxPE - Static UART (PDF), 01.07, 2007-01

[22] Data Book – SLE66CxxxPE /MicroSlim Security Controller Family incl. the errata sheet [23], 05.07, 2005-07-01

[23] Errata Sheet - SLE66CxxxPE Controllers - Product and Boundout, 2009-07-15, 2009-07-15

[24] Elliptic Curve GF(P) Support SLE66C(L)XxxxPE Interface Specification ECC-Library V 1.1, 12.2009 from 2009-12

[25] Security & Chip Card ICs – SLE 66CxxxPE – Instruction Set, 07.04, 2004-07

[26] Chip Card & Security ICs - SLE66CxxxP – Instruction Set and Special Function Registers – Quick Reference, 05-2004, 2004-05

[27] Security Programmers' Manual - SLE66C(L)xxxP(E) Controllers, 2009.03, 2009-03-27

[28] RSA 2048 bit Support SLE66C(L)XxxxPE Arithmetic Library for V1.6, 09.2008, 2008-09

[29] RSA 2048 bit Support SLE66C(L)XxxxPE RSA Interface Specification for library V1.6, 12.2009 2009-12

This page is intentionally left blank.

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-0629-2010

Evaluation results regarding development and production environment

The IT product Infineon Smart Card IC (Security Controller) SLE66CX162PE / m1531-a25 and
SLE66CX80PE / m1533-a25 all with optional libraries RSA V1.6, EC V1.1, SHA-2 V1.0 and both with specific IC dedicated software (Target of Evaluation, TOE) has been evaluated at an 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 11 June 2010, the following results regarding the development and production environment apply. The Common Criteria Security 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:

Site	Address	Function
Altis	Altis Semiconductor S.N.C. Boulevard John Kennedy 224 91105 Corbeil Essonnes France	Production Initialisation and Pre-personalisation
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

Site	Address	Function
Augsburg	Infineon Technologies AG Alter Postweg 101 86159 Augsburg Germany	Development
Bangalore	Infineon Technologies India Pvt. Ltd. 13th Floor, Discoverer Building International Technology Park Whitefield Road Bangalore, India - 560066	Software development and testing
Bangkok	Smartrac Technology, 142 Moo 1 Hi-Tech industrial Estate, Ban Laean, Bang, Pa-In Phra na korn Si Ayatthaya, 13160 Thailand	Inlay antenna mounting
Bukarest	Infineon Technologies Romania Blvd. Dimitrie Pompeiu Nr. 6 Sector 2 020335 Bucharest, Romania	Development
Burlington	IBM Corporation IBM Systems and Technology Group 1000 River St., Essex Junction, Vermont 05452 U.S.A.	Production Initialisation and Pre-personalisation Mask Center
Chanhassen	Smartrac Technology US Inc. 1546 Lake Drive West Chanhassen, MN 55317 USA	Inlay antenna mounting
Dresden	Infineon Technologies Dresden GmbH & Co. OHG Königsbrücker Str. 180 01099 Dresden Germany	Production Initialisation and Pre-personalisation
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

Site	Address	Function
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
Kulim	Infineon Technologies (Kulim) Sdn. Bhd. Lot 10 &11, Julan Hi-Tech 7 Industrial Zone Phase II Kulim Hi-Tech Park 09000 Kulim, Kedah Darul Aman Malaysia	Production Initialisation and Pre-personalisation
Munich	Infineon Technologies AG Am Campeon 1-12 85579 Neubiberg Germany Infineon Technologies AG Otto-Hahn-Ring 6 81739 München (Perlach) Germany	Development
Razan Toppan	Toppan Printing Co., Ltd. 6-2, Hanami-Dai, Ranzan-Machi, Hiki-Gun, Saitama 355-0204 Japan	Inlay antenna mounting
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
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

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.