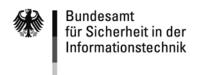# Certification Report

BSI-DSZ-CC-0430-2008

for

Infineon Smart Card IC (Security Controller) SLE66CLX800PE / m1581-e12, SLE66CLX800PEM / m1580-e12, SLE66CLX800PES / m1582-e12, SLE66CLX360PE / m1587-e12, SLE66CLX360PEM / m1588-e12, SLE66CLX360PES / m1589-e12, SLE66CX800PE / m1599-e12 all with RSA 2048 V1.5 and ECC V1.1 and specific Dedicated Software

from

Infineon Technologies AG

Deutsches IT-Sicherheitszertifikat
erteilt vom   Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0430-2008

Smart Card with Signature Application

Infineon Smart Card IC (Security Controller)
SLE66CLX800PE / m1581-e12, SLE66CLX800PEM / m1580-e12,
SLE66CLX800PES / m1582-e12, SLE66CLX360PE / m1587-e12,
SLE66CLX360PEM / m1588-e12, SLE66CLX360PES / m1589-e12,
SLE66CX800PE / m1599-e12 all with RSA 2048 V1.5 and ECC V1.1 and
specific Dedicated Software

from	Infineon Technologies AG
PP Conformance:	Protection Profile BSI-PP-0002-2001
Functionality:	BSI-PP-0002-2001 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, AVA_VLA.4

Common Criteria
Arrangement
for components
up to EAL 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, 15. May 2008
For the Federal Office for Information Security

IT
Security
Certified

SOGIS - MRA

Bernd Kowalski
Head of Department

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)

* 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]   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

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.

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 product Infineon Smart Card IC (Security Controller) SLE66CLX800PE / m1581-e12, SLE66CLX800PEM / m1580-e12, SLE66CLX800PES / m1582-e12, SLE66CLX360PE / m1587-e12, SLE66CLX360PEM / m1588-e12, SLE66CLX360PES / m1589-e12, SLE66CX800PE / m1599-e12 all with RSA 2048 V1.5 and ECC V1.1 and specific Dedicated Software has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-

0399-2007. Specific results from the evaluation process based on BSI-DSZ-CC-0399-2007 were re-used.

The evaluation of the product Infineon Smart Card IC (Security Controller) SLE66CLX800PE / m1581-e12, SLE66CLX800PEM / m1580-e12, SLE66CLX800PES / m1582-e12, SLE66CLX360PE / m1587-e12, SLE66CLX360PEM / m1588-e12, SLE66CLX360PES / m1589-e12, SLE66CX800PE / m1599-e12 all with RSA 2048 V1.5 and ECC V1.1 and specific Dedicated Software was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 13.03.2008. 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

- 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.

---

[6]   Information Technology Security Evaluation Facility

5 Publication

The following Certification Results contain pages B-1 to B-24 and D1 to D-4.

The product Infineon Smart Card IC (Security Controller) SLE66CLX800PE / m1581-e12, SLE66CLX800PEM / m1580-e12, SLE66CLX800PES / m1582-e12, SLE66CLX360PE / m1587-e12, SLE66CLX360PEM / m1588-e12, SLE66CLX360PES / m1589-e12, SLE66CX800PE / m1599-e12 all with RSA 2048 V1.5 and ECC V1.1 and specific Dedicated Software has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). 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
D-85579 Neubiberg, Germany

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.

Contents of the certification results

1   Executive Summary

The Target of Evaluation (TOE) is the Infineon Smart Card IC (Security Controller) SLE66CLX800PE / m1581-e12, SLE66CLX800PEM / m1580-e12, SLE66CLX800PES / m1582-e12, SLE66CLX360PE / m1587-e12, SLE66CLX360PEM / m1588-e12, SLE66CLX360PES / m1589-e12, SLE66CX800PE / m1599-e12 all with RSA 2048 V1.5 and ECC V1.1 and specific Dedicated Software. For this evaluation specific results from the evaluation process based on BSI-DSZ-CC-0399-2007 were re-used. Compared to the product SLE66CLX800PE / m1581-e12, SLE66CLX800PEM / m1580-e12, SLE66CLX800PES / m1582-e12, SLE66CLX360PE / m1587-e12, SLE66CLX360PEM / m1588-e12, SLE66CLX360PES / m1589-e12 with specific IC Dedicated Software (BSI-DSZ-CC-0399-2007) the TOE includes a RSA2048 library and a ECC library. The ECC library is completely new, whereby the RSA2048 library V1.5 is an improvement of the already certified RSA2048 Library V1.4 (e.g. BSI-DSZ-CC-0322-2005). The hardware of the TOE is unchanged. In addition the derivate SLE66CX800PE / m1599-e12 is included. This derivate is the same hardware as the SLE66CLX800PE / m1581-e12 with the exception that all contactless communication types are blocked during the production process. The TOE is implemented with UCP (Unified Channel Programming) technology. UCP is a way of programming the non volatile memory (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 user has the possibility to tailor the software part of the TOE during the manufacturing process by deselecting one or both crypto libraries. The TOE can be delivered including the functionality of the ECC crypto library or including the functionality of the RSA2048 crypto library or including the functionality of the ECC and RSA2048 crypto libraries or including no crypto library.

If the user decides not to use one or both of the crypto libraries 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 *ECC* is/are not provided by the TOE. Deselecting one or two crypto libraries does not include the code implementing functionality, which the user decided not to use. Excluding 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 chip versions of the TOE are manufactured in Infineons IC fabrication in Corbeil Essonnes (Altis), France, indicated by the first nibble of the batch number which gives the production line indicator "5" (see part D, Annex A of this report).

The differences in the contactless interface area are responsible for the different naming extensions "M", "S" or coming without extension. The derivates without extension communicate with the contact-based interface according to ISO 7816/ETSI/EMV and with the contactless interface according to ISO 14443 type A and type B. The extended "M" is used for the Mifare contactless interface protocol and related memory management (classic 1k emulation), whereas the "S" nominates the derivates with the ISO 18092 passive mode. The TOE will be identified by SLE66CLX800PEx if we speak of the three derivates SLE66CLX800PE / m1581-e12, SLE66CLX800PEM / m1580-e12, SLE66CLX800PES / m1582-e12 with an EEPROM of 80 kBytes. The same applies for SLE66CLX360PEx (stand for the three derivates SLE66CLX360PE / m1587-e12, SLE66CLX360PEM / m1588-e12, SLE66CLX360PES / m1589-e12 with an EEPROM of 36 kBytes).

All seven products are identically from hardware perspective and produced with the same masks with the exception of the first metal mask (called M1 mask) which contains the derivate specific information (e. g. development code, design step, memory size).

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile BSI-PP-0002-2001 [9]

The hardware part of the TOE is the complete chip, composed of hardware, firmware and software parts:

The TOE Hardware consists of:

- Microcontroller type ECO 2000 (CPU) with the subcomponents memory encryption and decryption unit (MED), memory management unit (MMU) and 256 bytes of internal RAM (IRAM)

- Security logic (SEC), Memory Control Unit (MCU) with FCURSE distributes the data to and from memory components while the FCURSE provides camouflage access operation, True random number generator (RNG), Checksum module (CRC), Advanced Crypto Engine (ACE) for long integer modulo calculations, Dual Key DES and Cryptographic Unit (DDC), Interrupt module (INT), Input Logic (INP), Timer (TIM)

- The external memory comprises 6 kBytes RAM (XRAM), 128 Bits PROM, 1280 x 6 Bits Map-RAM, 240 kBytes user ROM, including the routines for the chip management (RMS) (the derivates SLE66CLX800PEM and SLE66CLX360PEM have 236 kBytes), 16 kBytes test ROM containing the test routines (STS) (the derivates SLE66CLX800PEM and SLE66CLX360PEM have 20 kBytes), and 80 kBytes non-volatile memory (EEPROM) for the derivates SLE66CLX800PEx and SLE66CX800PE with error detection (EDC) and error correction (ECC) (the derivates SLE66CLX360PEx have 36 kBytes)

- The RF interface (radio frequency power and signal interface) enables contactless communication between a PICC (proximity integrated chip card, PICC) and a reader/writer (proximity coupling device, PCD). The power

supply and data are received by an antenna which consists of a coil with a few turns directly connected to the IC.

- Address and data bus (ADBUS), SFR bus (SBUS), Memory bus (MBUS)

The firmware and software part of the TOE consists of:

- The RMS (Resource Management System) routines stored in a reserved area of the normal user ROM for EEPROM programming, security function testing, random number online testing and Mifare protocol (only the derivates SLE66CLX800PEM and SLE66CLX360PEM) and consists of STS (Self Test Software) stored in the especially protected test ROM consisting of test and initialization routines. The RMS is part of the IC Dedicated Support Software and the STS is part of the IC Dedicated Test Software as defined in Protection Profile [9].

- RSA2048 (optional) providing high level interface to RSA (Rivest, Shamir, Adleman) and an ECC library (optional) providing a high level interface to Elliptic Curve Cryptography. The TOE can be delivered without the RSA2048 library and / or ECC library.

The smart card operating system and the application stored in the User ROM and in the EEPROM are not part of the TOE.

The TOE security assurance requirements 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, 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
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 6.1.

The claimed TOE's strength of functions 'high (SOF-high) for specific functions as indicated in the Security Target [6], chapter 6.1 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 Target [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.

The TOE has two different operating modes, user mode and test mode. The application software being executed on the TOE can not use the test mode. The TOE has seven evaluated configurations (see for more details chapter 8):

- SLE66CLX800PE / m1581-e12 with/or without RSA 2048 and/or ECC

- SLE66CLX800PEM / m1580-e12 with/or without RSA 2048 and/or ECC

- SLE66CLX800PES / m1582-e12 with/or without RSA 2048 and/or ECC

- SLE66CLX360PE / m1587-e12 with/or without RSA 2048 and/or ECC

- SLE66CLX360PEM / m1588-e12 with/or without RSA 2048 and/or ECC

- SLE66CLX360PES / m1589-e12 with/or without RSA 2048 and/or ECC

- SLE66CX800PE / m1599-e12 with/or without RSA 2048 and/or ECC

The TOE is delivered as a hardware unit at the end of the IC manufacturing process (Phase 3) or at the end of IC Packaging (Phase 4). 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) SLE66CLX800PE / m1581-e12, SLE66CLX800PEM / m1580-e12, SLE66CLX800PES / m1582-e12, SLE66CLX360PE / m1587-e12, SLE66CLX360PEM / m1588-e12, SLE66CLX360PES / m1589-e12, SLE66CX800PE / m1599-e12 all with RSA 2048 V1.5 and ECC V1.1 and specific Dedicated Software

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	SLE66CLX800PE Smart Card IC	GDS-file-ID: m1581-e12 with production line indicator: "5" (Altis)	Wafer or packaged module
		SLE66CLX800PEM Smart Card IC	GDS-file-ID: m1580-e12 with production line indicator: "5" (Altis)	Wafer or packaged module
		SLE66CLX800PES Smart Card IC	GDS-file-ID: m1582-e12 with production line indicator: "5" (Altis)	Wafer or packaged module
		SLE66CLX360PE Smart Card IC	GDS-file-ID: m1587-e12 with production line indicator: "5" (Altis)	Wafer or packaged module
		SLE66CLX360PEM Smart Card IC	GDS-file-ID: m1588-e12 with production line indicator: "5" (Altis)	Wafer or packaged module
		SLE66CLX360PES Smart Card IC	GDS-file-ID: m1589-e12 with production line indicator: "5" (Altis)	Wafer or packaged module
		SLE66CX800PE Smart Card IC	GDS-file-ID: m1599-e12 with production line indicator: "5" (Altis)	Wafer or packaged module
2	FW	STS Self Test Software (the IC Dedicated Test Software)	V57.08.07	Stored in Test ROM on the IC
3	FW	RMS Resource Management System *(the IC Dedicated Support Software)*	RMS_E V06	Stored in reserved area of User ROM on the IC
4	SW	RSA2048 library (optional)	V1.5	Source code in electronic form
5	SW	ECC library (optional)	V1.1	Source code in electronic form
6	DOC	Data Book [23]	10.06	Hardcopy and pdffile

No	Type	Identifier	Release	Form of Delivery
7	DOC	Security Programmers' Manual [20]	08.07	Hardcopy and pdffile
8	DOC	Instruction Set [21]	07.04	Hardcopy and pdffile
9	DOC	Instruction Set and Special Function Registers – Quick Reference [22]	11.06	Hardcopy and pdffile
10	DOC	RSA Interface Specification for library V1.5 [27]	01.2007	Hardcopy and pdffile
11	DOC	RSA Arithmetic Library for V1.5 [26]	01.2007	Hardcopy and pdffile
12	DOC	Functional Specification ECC Library [25]	04	Hardcopy and pdffile
13	DOC	Errata & delta Sheet [24]	10.06	Hardcopy and pdffile
14	DOC	Application Notes [11], [12], [14]-[19], [29]-[40]	chapter 13	Hardcopy and pdffile

Table 2: Deliverables of the TOE

The hardware part of the TOE is identified by SLE66CLX800PE / m1581-e12, SLE66CLX800PEM / m1580-e12, SLE66CLX800PES / m1582-e12, SLE66CLX360PE / m1587-e12, SLE66CLX360PEM / m1588-e12 SLE66CLX360PES / m1589-e12 or SLE66CX800PE / m1599-e12. For identification of a specific chip, the Chip Identification Number stored in the EEPROM can be used (see [23, chapter 7.9]).

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

- A4 hex for version m1581e1(x),

- A2 hex for version m1580e1(x),

- B9 hex for version m1582e1(x),

- B6 hex for version m1587e1(x),

- B7 hex for version m1588e1(x),

- B8 hex for version m1589e1(x).

- BA hex for version m1599e1(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 database system at Infineon Logistic Department.

The first nibble of the batch number [23, chapter 7] gives the production line indicator which is "5" for all chip versions manufactured in Infineons IC fabrication in Corbeil Essonnes (Altis), France.

The RSA2048 library and the ECC 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. Note: The TOE can be delivered with or without the RSA library and / or the ECC 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 Infineon Smart Card IC (Security Controller) SLE66CLX800PE / m1581-e12, SLE66CLX800PEM / m1580-e12, SLE66CLX800PES / m1582-e12, SLE66CLX360PE / m1587-e12, SLE66CLX360PEM / m1588-e12, SLE66CLX360PES / m1589-e12, SLE66CX800PE / m1599-e12 all with RSA 2048 V1.5 and ECC V1.1 and specific 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 [23] and other guidance documents delivered to the customer, see table 2.

For the implementation of the TOE Security Functions basically the components 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 software part of the TOE consists of the RSA2048 library and the ECC 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 documentations [10] – [24] are provided with the products by the developer to the customer for secure usage of the TOE in accordance with the Security Target.

Note that the customer who buys the TOE is normally the developer of the operating system and/or application software which will use the TOE as hardware computing platform to implement the software (operating system / application software) which will use the TOE.

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 Altis (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 "5" (Altis) 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

The TOE has seven evaluated configurations:

- SLE66CLX800PE / m1581-e12 with/or without RSA 2048 and/or ECC

- SLE66CLX800PEM / m1580-e12 with/or without RSA 2048 and/or ECC

- SLE66CLX800PES / m1582-e12 with/or without RSA 2048 and/or ECC

- SLE66CLX360PE / m1587-e12 with/or without RSA 2048 and/or ECC

- SLE66CLX360PEM / m1588-e12 with/or without RSA 2048 and/or ECC

- SLE66CLX360PES / m1589-e12 with/or without RSA 2048 and/or ECC

- SLE66CX800PE / m1599-e12 with/or without RSA 2048 and/or ECC

All with the specific IC Dedicated Software and with production line indicator "5" (Altis). 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.

Every information of how to use the TOE and its Security Functions by the software is provided within the user documentation.

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.

For components beyond EAL 4 the evaluation methodology applied was defined in co-ordination with the Certification Body [4] (AIS 34).

The evaluation methodology CEM [2] was used for those components used up to EAL 4 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product.

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 package as defined in the CC (see also part C of this report)

- The components ALC_DVS.2, AVA_MSU.3, 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-0399-2007 , re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on changed hardware and technology.

The evaluation has confirmed:

- Conformance to the PP: Protection Profile BSI-PP-0002-2001 [9]

- For the functionality: BSI-PP-0002-2001 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, 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

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 the following TOE Security Functions:

− SEF9 implements 3DES and Elliptic Curve Diffie-Hellman (ECDH) key agreement

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

- algorithms for the encryption and decryption:

  RSA, ECDSA

This holds for the TOE Security Function SEF9 implementing:

- RSA encryption and decryption

- RSA key generation

- Signature creation and verification according to ECDSA standard

- Elliptic Curve (EC) key generation

The strength of the cryptographic algorithms was not rated in the course of this evaluation (see BSIG Section 4, Para. 3, Clause 2). The commitment of each algorithm as per [28]. The validity period of each algorithm and its bitlenght is recommended in the official catalogue [28].

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

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.

- All security hints described in [20], [23] and the delivered application notes [10] – [23] have to be considered.

- Especially the recommendation in [20, 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 3DES: "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

  - For ECC (if the ECC 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 3DES, RSA (optional) and ECC (optional)) and

  - "Secure security attributes" resulting from FMT_MSA.2 (for 3DES, RSA (optional) and ECC (optional)).

  - RE.Phase-1: Design and Implementation of the Smartcard Embedded Software

  - RE.Process-Card: Protection during Packaging, Finishing and Personalisation

  - RE.Cipher: Cipher Schemas

- 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 configure the ranges of encryption,

- if the SW comparison of random numbers to/with regard to the active shielding is correctly implemented [38],

- 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 [23, 19.9], [20], and [37].

- 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 [29].

  - 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.

  - As the bit length of the randomisation by the scalar multiplication and inversion is adjusted to be 24 bit or 533 – "bit length of the curve" bit, it is strongly recommended that only curves with bit length up to 521 bit are used, because only for these curves it is examined that the randomisation is sufficient to counter attacks.

- Recommendation resulting from ADV_LLD:

  - Because of the possibility to overwrite functions of the RSA2048 and ECC library (delivered to the smartcard embedded software developer in form of source code or object code), it is pointed out that only the usage of the original RSA2048 library V1.5 and ECC library V1.1 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 [28, dated 5th February 2008] 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 [28].

  - 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 [28].

  This data is deplaced by a new version of [28].

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
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
PP	Protection Profile
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest, Shamir, Adelmann – a public key encryption algorithm
SEF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function

ST   Security Target

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

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 require-ments 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. specifically:

-       AIS 25, Version 3, 6 August 2007 for: CC Supporting Document, - The Application of CC to Integrated Circuits, Version 2.0, CCDB-2006-04-003, April 2006

-       AIS 26, Version 3, 6 August 2007 for: CC Supporting Document, - Application of Attack Potential to Smartcards, Version 2.3, CCDB-2007-04-001, April 2007

-       AIS 31, Version 1, 25 Sept. 2001 for: Functionality classes and evaluation methodology of physical random number generators

-       AIS 34, Version 1.00, 1 June 2004, Evaluation Methodology for CC Assurance Classes for EAL5+

-       AIS 36, Version 2, 12 November 2007 for: CC Supporting Document, ETR template for composite evaluation of Smart Cards and similar devices, Version 1.0 Revision 1, September 2007 and CC Supporting Document, Composite product evaluation of Smart Cards and similar devices, Version 1.0, September 2007

[5]   German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Web-site

[6]   Security Target, Infineon Technologies AG, Security and Chipcard ICs, SLE66CLX800PE / m1581-e12, SLE66CLX800PEM / m1580-e12, SLE66CLX800PES / m1582-e12, SLE66CLX360PE / m1587-e12, SLE66CLX360PEM / m1588-e12, SLE66CLX360PES / m1589-e12, SLE66CLX800PE / m1599-e12 all with RSA2048 V1.5 and ECC V1.1 and specific Dedicated Software, 15. January 2008, Version 0.5

[7]   Evaluation Technical Report, Version 3, 07. March 2008, for the Product Smart Card IC (Security Controller) SLE66CLX800PE / m1581-e12, SLE66CLX800PEM / m1580-e12, SLE66CLX800PES / m1582-e12, SLE66CLX360PE / m1587-e12, SLE66CLX360PEM / m1588-e12, SLE66CLX360PES / m1589-e12, SLE66CLX360PES / m1589-e12, SLE66CLX800PE / m1599-e12 all with RSA2048 V1.5 and ECC V1.1 and specific Dedicated Software (confidential document)

[8]   ETR for composite evaluation, according to AIS 36, Version 1, 07. March 2008, for the Product Smart Card IC (Security Controller) SLE66CLX800PE / m1581-e12, SLE66CLX800PEM / m1580-e12, SLE66CLX800PES / m1582-e12, SLE66CLX360PE / m1587-e12, SLE66CLX360PEM / m1588-e12, SLE66CLX360PES / m1589-e12, SLE66CLX360PES / m1589-e12, SLE66CLX800PE / m1599-e12 all with RSA2048 V1.5 and ECC V1.1 and specific Dedicated Software (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]   SLE66CLxxxP - Anticollision Type A, Version 03.03, March 2003, Infineon Technologies AG

[11]   SLE66CLxxxP - Anticollision Type B, Version 03.03, March 2003 Infineon Technologies AG

[12]   SLE66CLxxxP - Card Coil Design Guide, Version 10.05, October 2005, Infineon Technologies AG

[13]   SLE66CLXxxxPE – Implementation of Transmission Protocol according to ISO/IEC 14443 Part 3 and 4, Version 02.06, February 2006, Infineon Technologies AG

[14]   SLE66CLxxxP - Implementation of Transmission Protocol according to ISO/IEC 14443 Part 4, Version 03.03, March 2003, Infineon Technologies AG

[15]   Application Note, SLE66CXxxS Using CRC (PDF+SW), Version 03.01, March 2001, Infineon Technologies AG

[16]   Application Note, SLE66CXxxP, Infineon Chipcard Crypto API (PDF+SW), Version 05.02, May 2002, Infineon Technologies AG

[17]   SLE66CLxxxPE(M) – Contactless Anticollision & Protocol (source v0.88), Ver. 01.07, Januar 2007, Infineon Technologies AG

[18] SLE66CLxxxP - Optimized Contactless Energy performance, Version 01.07, January 2007, Infineon Technologies AG

[19] SLE66C(L)xxxPE - Optimized Usage of Data NVM Above 64k, Version 08.05, August 2005, Infineon Technologies AG

[20] Security Programmers' Manual - SLE66C(L)xxxP(E) Controllers, Version 08.07, August 2007

[21] Security & Chip Card ICs – SLE66CxxxPE – Instruction Set, Version 07.04, July 2004, Infineon Technologies AG

[22] Chip Card & Security ICs - SLE66CL(X)xxxPE(M/S) – Instruction Set and Special Function Registers – Quick Reference, Version 11.06, November 2006, Infineon Technologies AG

[23] Data Book – SLE66CL(X)xxxPE(M/S) Security Controller, Version 10.06, 31 October 2006, Infineon Technologies AG

[24] Errarta & delta Sheet – SLE66CL(X)xxxPE(M/S) Controllers – Products and Boundout, Version 10.06, October 2006, Infineon Technologies AG

[25] Functional Specification ECC Library for SLE66CxxxPE, Version 04, April 2007, Infineon Technologies AG

[26] RSA 2048 bit Support – SLE66C(L)XxxxPE Arithmetic Library for V1.5, Version 01.2007, January 2007, Infineon Technologies AG

[27] RSA 2048 bit Support – SLE66C(L)XxxxPE RSA Interface Specification for library, Version 01.2007, January 2007, Infineon Technologies AG

[28] 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

[29] Application Note, SLE66CxxxP, DDES – EC2, confidential document, Ver. 02.04, February 2004, Infineon Technologies AG

[30] Complementary Application Note, SLE66CxxxP, DDES – EC2, confidential document, Ver. 07.05, July 2005, Infineon Technologies AG

[31] Application Note, SLE66CxxxP, Using MicroSlim NVM (cLib), confidential document, Ver. 05.05, May 2005, Infineon Technologies AG

[32] Application Note, SLE66CxxxP/PE, Memory Encryption Decryption, confidential document, Ver. 11.04, November 2004, Infineon Technologies AG

[33] Application Note, SLE66CxxxPE, MMU Memory Management Unit, confidential document, Ver. 12.04, December 2004, Infineon Technologies AG

[34] Application Note, SLE66CxxxP, MMU Security Issues (PDF), confidential document, Ver. 01.02, January 2001, Infineon Technologies AG

[35]   Application Note, SLE66CxxxP/PE, Testing the RNG, confidential
        document, Ver. 11.04, November 2004, Infineon Technologies AG

[36]   Application Note, SLE66CxxxP/PE, Using RNG a.t. FIPS140 (PDF+SW),
        confidential document, Ver. 2.04, February 2004, Infineon Technologies
        AG

[37]   Application Note, SLE66CxxxPE, Security Advice 05.04 (PDF+SW),
        confidential document, Ver. 05.04, May 2004, Infineon Technologies AG

[38]   Application Note, SLE66CxxxPE, Using the active shield, confidential
        document, Ver. 12.04, December 2004, Infineon Technologies AG

[39]   Application Note, DES – software version (PDF+SW), confidential
        document, Ver. 09.97, September 1997, Infineon Technologies AG

[40]   Application Note, SLE66CxxxP, UART (PDF+SW), confidential
        document, Ver. 10.03, December 2003, Infineon Technologies AG

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
	TOE description (APE_DES)
	Security environment (APE_ENV)
Class APE: Protection Profile evaluation	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
	TOE description (ASE_DES)
	Security environment (ASE_ENV)
	ST introduction (ASE_INT)
Class ASE: Security Target evaluation	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   D-3

D-2

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0430-2007

Evaluation results regarding development and production environment

The IT product Infineon Smart Card IC (Security Controller) SLE66CLX800PE / m1581-e12, SLE66CLX800PEM / m1580-e12, SLE66CLX800PES / m1582-e12, SLE66CLX360PE / m1587-e12, SLE66CLX360PEM / m1588-e12, SLE66CLX360PES / m1589-e12, SLE66CX800PE / m1599-e12 all with RSA 2048 V1.5 and ECC V1.1 and specific Dedicated Software (Target of Evaluation, TOE) 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)* .

As a result of the TOE certification, dated 07. April 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 fulfiled for the development and production sites <u>of the TOE</u> listed below:

a) Altis Semiconductor S.N.C., Boulevard John Kennedy 224,, 91105 Corbeil Essonnes, France (Production)

b) Altis Toppan (former DuPont), Toppan Photomask, Inc, European Technology Center, Boulevard John Kennedy 224, 91105 Corbeil-Essonnes Cedex, France (Mask Center)

c) 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)

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

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

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

g) Infineon Technologies Austria AG, Development Center Graz, Babenbergerstr. 10, 8020 Graz, Austria, and Infineon Technologies Austria AG, Siemensstr. 2, 9500 Villach, Austria (Development)

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

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

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

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

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

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

n) 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 Corbeil Essonnes (Altis), France, indicated by the first nibble of the batch number which gives the production line indicator "5".

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target, Infineon Technologies AG, Security and Chipcard ICs, SLE66CLX800PE / m1581-e12, SLE66CLX800PEM / m1580-e12, SLE66CLX800PES / m1582-e12, SLE66CLX360PE / m1587-e12, SLE66CLX360PEM / m1588-e12, SLE66CLX360PES / m1589-e12, SLE66CLX800PE / m1599-e12 all with RSA2048 V1.5 and ECC V1.1 and specific Dedicated Software, 15. January 2008, Version 0.5 [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.