Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0593-2009

for

Infineon Smart Card IC (Security Controller) SLE66CLX206PEM / m2084-a11, SLE66CLX206PE / m2085-a11, SLE66CLX206PES / m2086-a11, SLE66CDX206PEM / m2099-a11, SLE66CLX203PEM / m2098-a11, SLE66CLX207PEM / m2980-a11, SLE66CLX207PE / m2981-a11, SLE66CLX207PES / m2982-a11, SLE66CLX126PEM / m2087-a11, SLE66CLX126PE / m2088-a11, SLE66CLX126PES / m2089-a11, SLE66CLX127PEM / m2997-a11, SLE66CLX127PE / m2998-a11, SLE66CLX127PES / m2999-a11, all with optional libraries RSA V1.6, EC V1.1, SHA-2 V1.0 and all with specific IC dedicated software

from

Infineon Technologies AG

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0593-2009

Infineon Smart Card IC (Security Controller) SLE66CLX206PEM / m2084-a11, SLE66CLX206PE / m2085-a11, SLE66CLX206PES / m2086-a11, SLE66CDX206PEM / m2099-a11, SLE66CLX203PEM / m2098-a11, SLE66CLX207PEM / m2980-a11, SLE66CLX207PE / m2981-a11, SLE66CLX207PES / m2982-a11, SLE66CLX126PEM / m2087-a11, SLE66CLX126PE / m2088-a11, SLE66CLX126PES / m2089-a11, SLE66CLX127PEM / m2997-a11, SLE66CLX127PE / m2998-a11, SLE66CLX127PES / m2999-a11, all with optional libraries RSA V1.6, EC V1.1, SHA-2 V1.0 and all 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

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, 8 May 2009

For the Federal Office for Information Security

Bernd Kowalski L.S.
Head of Department

SOGIS - MRA

This page is intentionally left blank.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

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

Contents

A Certification

1 Specifications of the Certification Procedure

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

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)[5]
- Common Methodology for IT Security Evaluation, Version 2.3
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1 European Recognition of ITSEC/CC - Certificates

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

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

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

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

[4] Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

[5] Proclamation of the Bundesministerium des Innern of 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

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

2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria 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) SLE66CLX206PEM / m2084-a11, SLE66CLX206PE / m2085-a11, SLE66CLX206PES / m2086-a11, SLE66CDX206PEM / m2099-a11, SLE66CLX203PEM / m2098-a11, SLE66CLX207PEM / m2980-a11, SLE66CLX207PE / m2981-a11, SLE66CLX207PES / m2982-a11, SLE66CLX126PEM / m2087-a11, SLE66CLX126PE / m2088-a11, SLE66CLX126PES / m2089-a11, SLE66CLX127PEM / m2997-a11, SLE66CLX127PE / m2998-a11, SLE66CLX127PES / m2999-a11, all with optional libraries RSA V1.6, EC V1.1, SHA-2 V1.0 and all with specific IC dedicated software has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0523-2008. Specific results from the evaluation process BSI-DSZ-CC-0523-2008 were re-used.

The evaluation of the product Infineon Smart Card IC (Security Controller) SLE66CLX206PEM / m2084-a11, SLE66CLX206PE / m2085-a11, SLE66CLX206PES / m2086-a11, SLE66CDX206PEM / m2099-a11, SLE66CLX203PEM / m2098-a11, SLE66CLX207PEM / m2980-a11, SLE66CLX207PE / m2981-a11, SLE66CLX207PES / m2982-a11, SLE66CLX126PEM / m2087-a11, SLE66CLX126PE / m2088-a11, SLE66CLX126PES / m2089-a11, SLE66CLX127PEM / m2997-a11, SLE66CLX127PE / m2998-a11, SLE66CLX127PES / m2999-a11, all with optional libraries RSA V1.6, EC V1.1, SHA-2 V1.0 and all with specific IC dedicated software was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 24 April 2009. The TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Infineon Technologies AG

[6] Information Technology Security Evaluation Facility

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 please refer to the excerpts from the criteria at the end of the Certification Report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods may evolve over time, the resistance of the certified version of the product against new attack methods can be re-assessed if required and the sponsor applies for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme. It is recommended to perform a re-assessment on a regular basis.

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

5 Publication

The product Infineon Smart Card IC (Security Controller) SLE66CLX206PEM / m2084-a11, SLE66CLX206PE / m2085-a11, SLE66CLX206PES / m2086-a11, SLE66CDX206PEM / m2099-a11, SLE66CLX203PEM / m2098-a11, SLE66CLX207PEM / m2980-a11, SLE66CLX207PE / m2981-a11, SLE66CLX207PES / m2982-a11, SLE66CLX126PEM / m2087-a11, SLE66CLX126PE / m2088-a11, SLE66CLX126PES / m2089-a11, SLE66CLX127PEM / m2997-a11, SLE66CLX127PE / m2998-a11, SLE66CLX127PES / m2999-a11, all with optional libraries RSA V1.6, EC V1.1, SHA-2 V1.0 and all with specific IC 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 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
CCS M PS
Am Campeon 1-12
85579 Neubiberg

This page is intentionally left blank.

B Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1 Executive Summary

The Target of Evaluation (TOE) is the Infineon Smart Card IC (Security Controller) SLE66CLX206PEM / m2084-a11, SLE66CLX206PE / m2085-a11, SLE66CLX206PES / m2086-a11, SLE66CDX206PEM / m2099-a11, SLE66CLX203PEM / m2098-a11, SLE66CLX207PEM / m2980-a11, SLE66CLX207PE / m2981-a11, SLE66CLX207PES / m2982-a11, SLE66CLX126PEM / m2087-a11, SLE66CLX126PE / m2088-a11, SLE66CLX126PES / m2089-a11, SLE66CLX127PEM / m2997-a11, SLE66CLX127PE / m2998-a11, SLE66CLX127PES / m2999-a11, all with optional libraries RSA V1.6, EC V1.1, SHA-2 V1.0 and all with specific IC dedicated software. All products of this TOE were already successfully CC EAL5+ certified in the different design version by the BSI. The direct recertification reference for this TOE is the BSI process BSI-DSZ-CC-523-2008 including the library versions RSA Version 1.5 and EC Version 1.1. The main differences to the forerunner (SLE66CLX1600PEx) are the different implemented memory sizes, the new RSA library version and the SHA-2 library for computing hash values.

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, an AIS31-compliant RNG (Random Number Generator), and a checksum module (CRC module). Further components are integrated on the chip too. For fast asymetric cryptographic operations performance the TOE has the Advanced Cryptographic Engine (ACE) component implemented. The TOE's block diagram is shown in Figure 1 of the Security Target [6, chapter 2.1].

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 and contactless 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 crypto library RSA, the crypto library EC, the RMS library and the SHA-2 library provide some functionality via an API to the Smartcard Embedded Software and STS firmware for test purpose. The STS is implemented in a separated Test-ROM being part of the TOE. The RSA library supports operation size from 512 bits to 2048 bits. Only key sizes from 1024 bits up to 2048 bits are within the scope of this evaluation. The EC library can perform EC operations on elliptic curve parameters with key lengths up to 533 bits. Included in the evaluation are only operations with key length of 192 to 521 bits.

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. Two modules for cryptographic operations are implemented on the TOE: The well known Advanced Crypto Engine (ACE) for calculation of asymmetric algorithms like RSA and elliptic curve (EC) and the Cryptographic Unit (DDES) for Dual Key DES calculations. These modules are especially designed for Chipcard applications with respect to the security and power consumption. The DDES module computes the complete DES algorithm within a few clock cycles and is especially designed to counter attacks like DPA or EMA. The TOE includes also functionality to calculate single DES operations, but part of the evaluation is the triple-DES operation only. For more detail please refer to the Security Target [6, chapter 2.1].

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 [7].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 5 augmented by ALC_DVS.2 - Sufficiency of security measures, AVA_MSU.3 - Validation of analysis and AVA_VLA.4 - Highly resistant.

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 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:

- SLE66CLX206PEM / m2084-a11 with/or without RSA and/or EC and/or SHA-2 (produced in Dresden),
- SLE66CLX206PE / m2085-a11 with/or without RSA and/or EC and/or SHA-2 (produced in Dresden),
- SLE66CLX206PES / m2086-a11 with/or without RSA and/or EC and/or SHA-2 (produced in Dresden),

- SLE66CDX206PEM / m2099-a11 with/or without RSA and/or EC and/or SHA-2 (produced in Dresden),
- SLE66CLX203PEM / m2098-a11 with/or without RSA and/or EC and/or SHA-2 (produced in Dresden),
- SLE66CLX207PEM / m2980-a11 with/or without RSA and/or EC and/or SHA-2 (produced in Dresden),
- SLE66CLX207PE / m2981-a11 with/or without RSA and/or EC and/or SHA-2 (produced in Dresden),
- SLE66CLX207PES / m2982-a11 with/or without RSA and/or EC and/or SHA-2 (produced in Dresden),
- SLE66CLX126PEM / m2087-a11 with/or without RSA and/or EC and/or SHA-2 (produced in Dresden),
- SLE66CLX126PE / m2088-a11 with/or without RSA and/or EC and/or SHA-2 (produced in Dresden),
- SLE66CLX126PES / m2089-a11 with/or without RSA and/or EC and/or SHA-2 (produced in Dresden).
- SLE66CLX127PEM / m2997-a11 with/or without RSA and/or EC and/or SHA-2 (produced in Dresden).
- SLE66CLX127PE / m2998-a11 with/or without RSA and/or EC and/or SHA-2 (produced in Dresden).
- SLE66CLX127PES / m2999-a11 with/or without RSA and/or EC and/or SHA-2 (produced in Dresden).

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

Infineon Smart Card IC (Security Controller) SLE66CLX206PEM / m2084-a11, SLE66CLX206PE / m2085-a11, SLE66CLX206PES / m2086-a11, SLE66CDX206PEM / m2099-a11, SLE66CLX203PEM / m2098-a11, SLE66CLX207PEM / m2980-a11, SLE66CLX207PE / m2981-a11, SLE66CLX207PES / m2982-a11, SLE66CLX126PEM / m2087-a11, SLE66CLX126PE / m2088-a11, SLE66CLX126PES / m2089-a11, SLE66CLX127PEM / m2997-a11, SLE66CLX127PE / m2998-a11, SLE66CLX127PES / m2999-a11, all with optional libraries RSA V1.6, EC V1.1, SHA-2 V1.0 and all with specific IC dedicated software

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of delivery
1a	HW	SLE66CLX206PEM Smart Card IC	GDS-file-ID: m2084-a11 with production line indicator: “2” (Dresden)	Wafer or packaged module
1b	HW	SLE66CLX206PE Smart Card IC	GDS-file-ID: m2085-a11 with production line indicator: “2” (Dresden)	Wafer or packaged module
1c	HW	SLE66CLX206PES Smart Card IC	GDS-file-ID: m2086-a11 with production line indicator: “2” (Dresden)	Wafer or packaged module
1d	HW	SLE66CDX206PEM Smart Card IC	GDS-file-ID: m2099-a11 with production line indicator: “2” (Dresden)	Wafer or packaged module
1e	HW	SLE66CLX203PEM Smart Card IC	GDS-file-ID: m2098-a11 with production line indicator: “2” (Dresden)	Wafer or packaged module
1f	HW	SLE66CLX207PEM Smart Card IC	GDS-file-ID: m2980-a11 with production line indicator: “2” (Dresden)	Wafer or packaged module
1g	HW	SLE66CLX207PE Smart Card IC	GDS-file-ID: m2981-a11 with production line indicator: “2” (Dresden)	Wafer or packaged module
1h	HW	SLE66CLX207PES Smart Card IC	GDS-file-ID: m2982-a11 with production line indicator: “2” (Dresden)	Wafer or packaged module
1i	HW	SLE66CLX126PEM Smart Card IC	GDS-file-ID: m2087-a11 with production line indicator: “2” (Dresden)	Wafer or packaged module
1j	HW	SLE66CLX126PE Smart Card IC	GDS-file-ID: m2088-a11 with production line indicator: “2” (Dresden)	Wafer or packaged module
1k	HW	SLE66CLX126PES Smart Card IC	GDS-file-ID: m2089-a11 with production line indicator: “2” (Dresden)	Wafer or packaged module
1l	HW	SLE66CLX127PEM Smart Card IC	GDS-file-ID: m2997-a11 with production line indicator: “2” (Dresden)	Wafer or packaged module
1m	HW	SLE66CLX127PE Smart Card IC	GDS-file-ID: m2998-a11 with production line indicator: “2” (Dresden)	Wafer or packaged module
1n	HW	SLE66CLX127PES Smart Card IC	GDS-file-ID: m2999-a11 with production line indicator: “2” (Dresden)	Wafer or packaged module
2	FW	STS Self Test Software *(the IC Dedicated Test Software)*	V57.09.08	Stored in Test ROM on the IC
3	FW	RMS-E Resource Management System *(the IC Dedicated Support Software)*	RMS_E V07	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
1	DOC	Data Book – SLE66C(L)(X)xxxPE(M/S) Security Controller Family	2008-09-03	Hardcopy and pdf-file
8	DOC	Errata Sheet - SLE66CxxxPE Controllers - Product and Boundout	2009-02-04	Hardcopy and pdf-file

No	Type	Identifier	Release	Form of delivery
9	DOC	Security Programmers' Manual - SLE66C(L)xxxP(E) Controllers	2009-03-27	Hardcopy and pdf-file
10	DOC	Security & Chip Card ICs – SLE66CxxxPE – Instruction Set	07.04	Hardcopy and pdf-file
11	DOC	Chip Card & Security ICs - SLE66CL(X)xxxPE(M/S) – Instruction Set and Special Function Registers – Quick Reference	11.06	Hardcopy and pdf-file
12	DOC	RSA 2048 bit Support SLE66C(L)XxxxPE RSA Interface Specification for library V1.6 (optional)	02.2009	Hardcopy and pdf-file
13	DOC	RSA 2048 bit Support SLE66C(L)XxxxPE Arithmetic Library for V1.6 (optional)	09.2008	Hardcopy and pdf-file
14	DOC	Elliptic Curve GF(P) Support SLE66C(L)XxxxPE Interface Specification ECC-Library V 1.1 (optional)	2009-03-03	Hardcopy and pdf-file
15	DOC	Application Notes [17]..[32]	see list in section 13	Hardcopy and pdf-file

Table 2: Deliverables of the TOE

The hardware part of the TOE is identified by SLE66CLX206PEM / m2084-a11, SLE66CLX206PE / m2085-a11, SLE66CLX206PES / m2086-a11, SLE66CDX206PEM / m2099-a11, SLE66CLX203PEM / m2098-a11, SLE66CLX207PEM / m2980-a11, SLE66CLX207PE / m2981-a11, SLE66CLX207PES / m2982-a11, SLE66CLX126PEM / m2087-a11, SLE66CLX126PE / m2088-a11, SLE66CLX126PES / m2089-a11, SLE66CLX127PEM / m2997-a11 or SLE66CLX127PE / m2998-a11, SLE66CLX127PES / m2999-a11. 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. "0B" at address (080009H) stands for design step "11") 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 [12, chapter 6.16.2.6] and [11, chapter 6.7].

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 chip type byte identifies the different versions in the following Table 3.

Type	Name	Version number	Chip type
Target of Evaluation	SLE66CLX206PEM	m2084-a11	D3h
	SLE66CLX206PE	m2085-a11	D4h
	SLE66CLX206PES	m2086-a11	D5h
	SLE66CDX206PEM	m2099-a11	DFh
	SLE66CLX203PEM	m2098-a11	D2h
	SLE66CLX207PEM	m2980-a11	D6h
	SLE66CLX207PE	m2981-a11	D7h
	SLE66CLX207PES	m2982-a11	D8h
	SLE66CLX126PEM	m2087-a11	D9h
	SLE66CLX126PE	m2088-a11	DAh
	SLE66CLX126PES	m2089-a11	DBh
	SLE66CLX127PEM	m2997-a11	DCh
	SLE66CLX127PE	m2998-a11	DDh
	SLE66CLX127PES	m2999-a11	DEh
Hardware	Dresden	A11	
Firmware	RMS-E library STS	RMS_E V07 57.09.08	
Software	RSA library (optional) EC library (optional) SHA-2 library (optional)	V1.6 V1.1 V1.0	

Table 3: TOE identification

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 [6, chapter 2.1]. The complete hardware description and the complete instruction set of the TOE is to be found in the Data Book [12] 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. The SHA-2 library consists of routines for initialization, compression and finalisation of SHA-256 and SHA-512 hash computation. 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 RSA library, the EC library and the SHA-2 library. The RSA library and the EC library are delivered as source code and in this way integrated in the user software. The SHA-library is delivered as source code and is in this way available for the user software, too. 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 provided together with the product. 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-0523-2008 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 expertised know-how. Specific additional penetration attacks were performed in the course of this evaluation.

8 Evaluated Configuration

The SLE66CL/DX206PEx, the SLE66CLX207PEx, the SLE66CLX203PEM, the SLE66CLX126PEx and the SLE66CLX127PEx are identically from hardware perspective. The difference is that in the SLE66CLX126PEx and the SLE66CLX127PEx the memory is blocked to a 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 evaluated together.

Therefore the TOE is delivered in the fixed configurations listed chapter 1 of this report. For more details please refer to chapter 1.

This certification covers the above mentioned configurations 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) [8] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used 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) were used.

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

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

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0523-2008, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on implemented memory sizes, the STS update and the new RSA library version.

The evaluation has confirmed:

● PP Conformance:	Smartcard IC Platform Protection Profile, Version 1.0, July 2001, Eurosmart, BSI-PP-0002-2001 [7]
● for the Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
● for the Assurance:	Common Criteria Part 3 conformant EAL 5 augmented by ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4

- The following TOE Security Functions fulfil the claimed Strength of Function : high
  SEF2 – Phase management with test mode lock-out,
  SEF3 – Protection against snooping,
  SEF4 – Data encryption and data disguising,
  SEF5 – Random number generation

In order to assess the strength of function the scheme interpretations AIS 25, 26 and AIS 31 (see [4]) were used. For specific evaluation results regarding the development and production environment see annex B in part D of this report.

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

9.2 Results of cryptographic assessment

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

- algorithms for the encryption and decryption: RSA, EC, Triple-DES
- This holds for the following security functions: SF9

The strength of the cryptographic algorithms was not rated in the course of this evaluation (see BSIG Section 4, Para. 3, 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) [33]

The cryptographic functions 2-key Triple DES (2TDES) and RSA 1024 provided by the TOE have got 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 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered.

The operational documents as outlined in Table 2, deliverables of the TOE, 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:

All security hints described in the user guidance documentation [12]..[16] and the delivered application notes [17]..[32] 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 [13] have to be taken into account.

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 for the EC library 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.

Because of a possible fault injection attack on the ECDSA signature verification, the operating system developer has to check the verify result by e.g. performing the verify function twice, if the verification result is used for a security critical operation.

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
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 Block
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 requirement(s) to a package.

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

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - An passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

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

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

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

Subject - An active entity in the TOE that performs operations on objects.

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

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

13 Bibliography

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

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

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

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

[5] German IT Security Certifcates (BSI 7148, BSI 7149), periodically updated list published also in the BSI Website

[6] Security Target SLE66CLX206PEM / m2084-a11SLE66CLX206PE / m2085-a11, SLE66CLX206PES / m2086-a11, SLE66CDX206PEM / m2099-a11, SLE66CLX203PEM / m2098-a11, SLE66CLX207PEM / m2980-a11, SLE66CLX207PE / m2981-a11, SLE66CLX207PES / m2982-a11, SLE66CLX126PEM / m2087-a11, SLE66CLX126PE / m2088-a11, SLE66CLX126PES / m2089-a11, SLE66CLX127PEM / m2997-a11SLE66CLX127PE / m2998-a11SLE66CLX127PES / m2999-a11 all with optional libraries RSA V1.6, EC V1.1 and SHA-2 V1.0 from 2009-03-05, Infineon AG

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

[8] Evaluation Technical Report – Summary (ETR SUMMARY), SLE66CLX206PEM / m2084-a11SLE66CLX206PE / m2085-a11, SLE66CLX206PES / m2086-a11, SLE66CDX206PEM / m2099-a11, SLE66CLX203PEM / m2098-a11, SLE66CLX207PEM / m2980-a11, SLE66CLX207PE / m2981-a11, SLE66CLX207PES / m2982-a11, SLE66CLX126PEM / m2087-a11, SLE66CLX126PE / m2088-a11, SLE66CLX126PES / m2089-a11,

[8] specifically

- AIS 20, Version 1, 2. December 1999, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 3, 6 August 2007, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 3, 6 August 2007, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 1, 25 Sept. 2001 Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 1, 2 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema.
- AIS 34, Version 1.00, 1 June 2004, Evaluation Methodology for CC Assurance Classes for EAL5+
- AIS 35, Version 2.0, 12 November 2007, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document 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

SLE66CLX127PEM / m2997-a11SLE66CLX127PE / m2998-a11SLE66CLX127PES / m2999-a11 all with optional libraries RSA V1.6, EC V1.1 and SHA-2 V1.0, Version 2 from 2009-04-09, Evaluation Body for IT Security of TÜV Informationstechnik GmbH (confidential document)

[9] ETR for composition according to AIS 36 for the Products SLE66CLX206PEM / m2084-a11SLE66CLX206PE / m2085-a11, SLE66CLX206PES / m2086-a11, SLE66CDX206PEM / m2099-a11, SLE66CLX203PEM / m2098-a11, SLE66CLX207PEM / m2980-a11, SLE66CLX207PE / m2981-a11, SLE66CLX207PES / m2982-a11, SLE66CLX126PEM / m2087-a11, SLE66CLX126PE / m2088-a11, SLE66CLX126PES / m2089-a11, SLE66CLX127PEM / m2997-a11SLE66CLX127PE / m2998-a11SLE66CLX127PES / m2999-a11 all with optional libraries RSA V1.6, EC V1.1 and SHA-2 V1.0, Version 1 from 2009-04-09, Evaluation Body for IT Security of TÜV Informationstechnik GmbH (confidential document)

[10] Configuration Management Scope (ACM_SCP), SLE66CLX206PEM / m2084-a11SLE66CLX206PE / m2085-a11, SLE66CLX206PES / m2086-a11, SLE66CDX206PEM / m2099-a11, SLE66CLX203PEM / m2098-a11, SLE66CLX207PEM / m2980-a11, SLE66CLX207PE / m2981-a11, SLE66CLX207PES / m2982-a11, SLE66CLX126PEM / m2087-a11, SLE66CLX126PE / m2088-a11, SLE66CLX126PES / m2089-a11, SLE66CLX127PEM / m2997-a11SLE66CLX127PE / m2998-a11SLE66CLX127PES / m2999-a11 all with optional libraries RSA V1.6, EC V1.1 and SHA-2 V1.0, Version 1.0 from 2009-01-20, Infineon AG (confidential document)

[11] Errata Sheet - SLE66CxxxPE Controllers - Product and Boundout, Version 2009-02-04 from 2009-02-04, Infineon AG

[12] Databook, Data Book – SLE66C(L)(X)xxxPE(M/S), Security Controller Family, Version 2008.09 from 2008-09-03, Infineon AG

[13] Security Programmers' Manual - SLE66C(L)xxxP(E) Controllers, Version 2009.03 from 2009-03-27, Infineon AG

[14] RSA 2048 bit Support SLE66C(L)XxxxPE Arithmetic Library for V1.6, Version 09.2008 from 2008-09, Infineon AG

[15] RSA 2048 bit Support SLE66C(L)XxxxPE RSA Interface Specification for library V1.6, Version 02.2009 from 2009-02, Infineon AG

[16] Elliptic Curve GF(P) Support SLE66C(L)XxxxPE Interface Specification ECC-Library V 1.1, 2009-03-03, Infineon AG

[17] SLE66CL(X)xxxPE(M/S) – Contactless Protocol Type A Type B (source v18092), Version 2008-07 from 2008-07, Infineon AG

[18] SLE 66CL(X)xxxPE(M/S) - Contactless Card Coil Design Guide, Version 2008-10 from 2008-10-03, Infineon AG

[19] SLE 66CL(X)xxxPE(M/S) – Contactless Performance for Payment Applications, Version 2008-10 from 2008-10-03, Infineon AG

[20] SLE 66CL(X)xxxPE(M/S) – Optimized Contactless Energy Performance, Version 2008-12 from 2008-12-11, Infineon AG

[21] SLE 66CLXxxxPE - Implementation of Transmission Protocol according to ISO/IEC 14443 Part 3 and 4, Version 2006-02 from 2006-02-23, Infineon AG

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

[23] Application Note, SLE66CxxxPE, Using MicroSlim NVM (cLib), Version 05.05 from 2005-05, Infineon AG (confidential document)

[24] Application Note, SLE66CxxxP/PE, Memory Encryption Decryption, Version 11.04 from 2004-11, Infineon AG (confidential document)

[25] Application Note, SLE66CxxxPE, MMU-Memory Management Unit (PDF+SW), Version 12.04 from 2004-12, Infineon AG (confidential document)

[26] LE66C(L)xxxPE - Optimized Usage of Data NVM Above 64k, Version 08.05 from 2005-08, Infineon AG

[27] Application Note, SLE66CxxxP/PE, Testing the RNG, Version 11.04 from 2004-11, Infineon AG (confidential document)

[28] Application Note, SLE66CxxxP/PE, Using RNG a.t. FIPS140 (PDF+SW), Version 02.04 from 2004-02, Infineon AG (confidential document)

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

[30] Application Note, SLE66CxxxPE, Using the active shield, Version 12.04 From 2004-12, Infineon AG (confidential document)

[31] Application Note, SLE66CxxxPE - UART basic (PDF), Version 02.07 from 2007-02, Infineon AG

[32] Application Note, SLE66CxxxPE - Static UART (PDF), Version 01.07 from 2007-01

[33] BSI-Technische Richtlinie - Kryptographische Verfahren: Empfehlungen und Schlüssellängen (BSI TR-02102), Version: 1.0, 2008-06-20, Certification body of the BSI.

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance Claim (chapter 9.4)

„The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - **CC Part 3 extended** - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex A.

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decompositon.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-

Assurance Class	Assurance Components
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
ATE: Tests	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“ The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next Section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.

Assurance Class	**Assurance Family**	**Assurance Components by Evaluation Assurance Level**						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

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

“Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 8.4)

“Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 8.5)

“Objectives

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

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 8.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 8.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 8.8)

“Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 8.9)

“Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

"Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

This page is intentionally left blank

D Annexes

List of annexes of this certification report

Annex A:	Security Target provided within a separate document.
Annex B:	Evaluation results regarding development and production environment

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0593-2009

Evaluation results regarding development and production environment

The IT product Infineon Smart Card IC (Security Controller) SLE66CLX206PEM / m2084-a11, SLE66CLX206PE / m2085-a11, SLE66CLX206PES / m2086-a11, SLE66CDX206PEM / m2099-a11, SLE66CLX203PEM / m2098-a11, SLE66CLX207PEM / m2980-a11, SLE66CLX207PE / m2981-a11, SLE66CLX207PES / m2982-a11, SLE66CLX126PEM / m2087-a11, SLE66CLX126PE / m2088-a11, SLE66CLX126PES / m2089-a11, SLE66CLX127PEM / m2997-a11, SLE66CLX127PE / m2998-a11, SLE66CLX127PES / m2999-a11, all with optional libraries RSA V1.6, EC V1.1, SHA-2 V1.0 and all with specific IC 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 8 May 2009, the following results regarding the development and production environment apply. The Common Criteria assurance requirements

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

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

Site	Address	Function
Altis-Toppan	Toppan Photomask, Inc. European Technology Center Boulevard John Kennedy 224 91105 Corbeil Essonnes France	Mask Center
Amkor	Amkor Technology Philippines Km. 22 East Service Rd. South Superhighway Muntinlupa City 1702 Philipines Amkor Technology Philippines 119 North Science Avenue Laguna Technopark, Binan Laguna 4024 Philipines	Module Mounting

Site	Address	Function
Augsburg	Infineon Technologies AG Alter Postweg 101 86159 Augsburg Germany	Development
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
Chanhassen	Smartrac Technology US Inc. 1546 Lake Drive West Chanhassen, MN 55317 USA	Inlay antenna mounting
Dresden-Toppan	Toppan Photomask, Inc Rähnitzer Allee 9 01109 Dresden, Germany	Mask Center
Dresden	Infineon Technologies Dresden GmbH & Co. OHG Königsbrücker Str. 180 01099 Dresden Germany	Production
Erfurt	Assa Abloy Identification Technologies GmbH (former Sokymat GmbH) In den Weiden 4b, 99099 Erfurt	Module Mounting with Inlay Antenna Mounting
Graz / Villach / Klagenfurt	Infineon Technologies Austria AG Development Center Graz Babenbergerstr. 10 8020 Graz, Austria Infineon Technologies Austria AG Siemensstr. 2 9500 Villach, Austria Infineon Technologies Austria AG Lakeside B05 9020 Klagenfurt, Austria	Development
Großostheim	Infineon Technology AG, DCE, Kühne & Nagel Stockstädter Strasse 10 - Building 8A 63762 Großostheim, Germany	Distribution Center
Hayward	Kuehne & Nagel 30805 Santana Street Hayward, CA 94544 U.S.A.	Distribution Center
Lustenau	New Logic Technologies AG, - A Wipro Company, Millenium Park 6, 6890 Lustenau, Austria	Development

Site	Address	Function
Munich	Infineon Technologies AG Am Campeon 1-12 85579 Neubiberg, Germany Infineon Technologies AG Otto-Hahn-Ring 6 81739 München (Perlach), Germany	Development
Regensburg-West	Infineon Technologies AG Wernerwerkstraße 2 93049 Regensburg, Germany Smartrac Technology GmbH, Wernerwerkstraße 2 93049 Regensburg, Germany	Module Mounting Inlay Antenna Mounting, Distribution Center
Singapore	Exel Singapore Pte Ltd DHL Exel Supply Chian 81, ALPS Avenue Singapore 498803	Distribution Center
Singapore Kallang	Infineon Technologies AG 168 Kallang Way Singapore 349253	Module Mounting
Tokyo	Kintetsu World Express, Inc. Tokyo Import Logistics Center Narita Terminal Tokyo, Japan	Distribution Center
Wuxi	Infineon Technologies (Wuxi) Co. Ltd. No. 118, Xing Chuang San Lu Wuxi-Singapore Industrial Park Wuxi 214028, Jiangsu, P.R. China	Module Mounting, Distribution Center

Table 4: TOE identification

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.