Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0315-2005

for

Infineon Smart Card IC (Security Controller) SLE66CX642P/m1485b16 with RSA 2048 V1.30 and specific IC Dedicated Software

from

Infineon Technologies AG

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 228 9582-0, Fax +49 228 9582-455, Infoline +49 228 9582-111

Deutsches
IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0315-2005

Infineon Smart Card IC (Security Controller) SLE66CX642P/m1485b16 with RSA 2048 V1.30 and specific IC Dedicated Software

from

Infineon Technologies AG

IT Security Certified

SOGIS-MRA

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, Part 1 Version 0.6*, *Part 2 Version 1.0* extended by advice of the Certification Body for components beyond EAL4 and smart card specific guidance for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC 15408:1999)* and including final interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

Evaluation Results:

PP Conformance:	**Protection Profile BSI-PP-0002-2001**
Functionality:	**BSI-PP-0002-2001 conformant plus product specific extensions Common Criteria Part 2 extended**
Assurance Package:	**Common Criteria Part 3 conformant EAL5 augmented by:** ALC_DVS.2 (Life cycle support - Sufficiency of security measures), AVA_MSU.3 (Vulnerability assessment - Analysis and testing for insecure states), AVA_VLA.4 (Vulnerability assessment - Highly resistant)

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.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 12. August 2005

The President of the Federal Office
for Information Security

Common Criteria

Dr. Helmbrecht L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 9582-0 - Fax +49 228 9582-455 - Infoline +49 228 9582-111

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 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.

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 2.1[5]
- Common Methodology for IT Security Evaluation (CEM)
  - Part 1, Version 0.6
  - Part 2, Version 1.0
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

The use of Common Criteria Version 2.1, Common Methodology, part 2, Version 1.0 and final interpretations as part of AIS 32 results in compliance of the certification results with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2 as endorsed by the Common Criteria recognition arrangement committees.

---

[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 7 July 1992, Bundesgesetzblatt I p. 1230

[4] Schedule of Cost for Official Procedures of the Federal Office for Information Security (BSI-Kostenverordnung, BSI-KostV) of 29th October 1992, Bundesgesetzblatt I p. 1838

[5] Proclamation of the Bundesministerium des Innern of 22nd September 2000 in the Bundesanzeiger p. 19445

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 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).

2.2 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 was signed in May 2000. It includes also the recognition of Protection Profiles based on the CC. The arrangement was signed by the national bodies of Australia, Canada, Finland France, Germany, Greece, Italy, The Netherlands, New Zealand, Norway, Spain, United Kingdom and the United States. Israel joined the arrangement in November 2000, Sweden in February 2002, Austria in November 2002, Hungary and Turkey in September 2003, Japan in November 2003, the Czech Republic in September 2004, the Republic of Singapore in March 2005, India in April 2005.

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) SLE66CX642P/m1485b16 with RSA 2048 V1.30 and specific IC Dedicated Software has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0266-2005.

The evaluation of the product Infineon Smart Card IC (Security Controller) SLE66CX642P/m1485b16 with RSA 2048 V1.30 and specific IC Dedicated Software was conducted by TÜV Informationstechnik GmbH Prüfstelle IT-Sicherheit. The TÜV Informationstechnik GmbH Prüfstelle IT-Sicherheit is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor, vendor and distributor is:

Infineon Technologies AG
Secure Mobile Solutions
P.O. Box 80 09 49,
81609 München, Germany

The certification is concluded with

- the comparability check and
- the production of this Certification Report.

This work was completed by the BSI on 12. August 2005.

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.

This Certification Report only applies to the version of the product indicated here. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

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.

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-28 and D1 to D-4.

The product Infineon Smart Card IC (Security Controller) SLE66CX642P/m1485b16 with RSA 2048 V1.30 and 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). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the vendor[7] of the product. The Certification Report can also be downloaded from the above-mentioned web site.

[7] Infineon Technologies AG
Secure Mobile Solutions
P.O. Box 80 09 49,
81609 München, 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 version m1485b16 of the Infineon Smart Card IC (Security Controller) SLE66CX642P with RSA 2048 V1.30 and specific IC Dedicated Software. This version provides a hardware platform for a smart card to run smart card applications executed by a smart card operating system.

The evaluation was performed as a re-evaluation process based on BSI-DSZ-CC-0266-2005.

The TOE was re-evaluated because its design was changed on module level in some points in comparison to the SLE66CX322P and for the SLE66CX642P the only production site is Dresden. The Security Target [6] was updated because of the new TOE name.

The chip version m1485b16 is manufactured in Infineons IC fabrication in Dresden, Germany, indicated by the production line indicator “2” (see part D, Annex A of this report).

The hardware part of the TOE is the complete chip, composed of a processing unit (CPU) with a memory management unit (MMU), several different memories (256 bytes of internal RAM (IRAM), 4 kBytes of extended RAM (XRAM), 208 kBytes of user ROM, 8 kByte of test ROM and 64 kBytes of EEPROM), a security logic, an interrupt module, bus system, a timer, an interrupt-controlled I/O interface, a random number generator (RNG), a checksum module (CRC module) and two modules for cryptographic operations: ACE (Advanced Crypto Engine) and the so called DDC (providing the DES algorithm and especially designed to counter attacks like DPA or EMA).

The firmware part of the TOE consists of the RMS (Resource Management System) routines for EEPROM programming and security function testing and the STS (Self Test Software) which consists of test and initialisation 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]. The RMS routines are stored by the TOE manufacturer in a reserved area of the normal user ROM. The STS routines are stored in the protected test ROM, used for testing purposes during production only and are not accessible for the user software.

The software part of the TOE consists of the RSA2048 library to provide a high level interface to RSA (Rivest, Shamir, Adleman) cryptography implemented on the hardware component ACE. The routines are used for the generation of RSA key pairs, the RSA signature verification, the RSA signature generation and the RSA modulus recalculation. The RSA2048 library is delivered as source code as part of the Infineon Sofware Development Kit and is to be integrated into the users embedded software.

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 provides an ideal platform for applications requiring non-volatile data storage. The TOE is intended for use in a range of high security 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. This includes for example measures for memory protection, leakage protection and sensors to allow operations only under specified conditions.

The Security Target is written using the Smartcard IC Platform Protection Profile, Version 1.0, July 2001, BSI registration ID: BSI-PP-0002-2001 [9]. With reference to this Protection Profile, the smart card product life cycle is described in 7 phases. The development, production and operational user environment are described and referenced to these phases. TOE delivery is defined at the end of phase 3 as wafers or phase 4 as modules.

The assumptions, threats and objectives defined in this Protection Profile [9] are used. To address additional security features of the TOE (e.g cryptographic services), the security environment as outlined in the PP [9] is augmented by an additional policy, an assumption and security objectives accordingly.

The IT product Infineon Smart Card IC (Security Controller) SLE66CX642P/m1485b16 with RSA 2048 V1.30 and specific IC Dedicated Software was evaluated against the claims of the Security Target [6] by TÜV Informationstechnik GmbH Prüfstelle IT-Sicherheit. The evaluation was completed on 30.6.2005. The TÜV Informationstechnik GmbH Prüfstelle IT-Sicherheit is an evaluation facility (ITSEF)[8] recognised by BSI.

The sponsor, vendor and distributor is Infineon Technologies AG.

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see Annex C or [1], part 3 for details). The TOE meets the assurance requirements of assurance level EAL5+ (Evaluation Assurance Level 5 augmented). The following table shows the augmented assurance components.

Requirement	Identifier
EAL5	TOE evaluation: Semiformally designed and tested
+: ALC_DVS.2	Life cycle support – Sufficiency of security measures
+: AVA_MSU.3	Vulnerability assessment - Analysis and testing for insecure states
+: AVA_VLA.4	Vulnerability assessment - Highly resistant

Table 1: Assurance components and EAL-augmentation

[8] Information Technology Security Evaluation Facility

1.2 Functionality

The TOE Security Functional Requirements (SFR) selected in the Security Target are Common Criteria Part 2 extended as shown in the following tables.

The following SFRs are taken from CC part 2:

Security Functional Requirement	Identifier	Source from PP or added in ST
FCS	**Cryptographic support**	
FCS_COP.1	Cryptographic operation	ST
FCS_CKM.1	Cryptographic key generation	ST
FDP	**User data protection**	
FDP_ACC.1	Subset access control	ST
FDP_ACF.1	Security attribute based access control	ST
FDP_IFC.1	Subset information flow control	PP
FDP_ITT.1	Basic internal transfer protection	PP
FMT	**Security Management**	
FMT_MSA.1	Management of security attributes	ST
FMT_MSA.3	Static attribute initialisation	ST
FPT	**Protection of the TOE Security Functions**	
FPT_FLS.1	Failure with preservation of secure state	PP
FPT_ITT.1	Basic internal TSF data transfer protection	PP
FPT_PHP.3	Resistance to physical attack	PP
FPT_SEP.1	TSF domain separation	PP
FRU	**Resource utilisation**	
FRU_FLT.2	Limited fault tolerance	PP

Table 2: SFRs taken from CC Part 2

The following CC part 2 extended SFRs are defined:

Security Functional Requirement	Identifier	Source from PP or added in ST
FAU	**Security Audit**	
FAU_SAS.1	Audit storage	PP / ST[9]
FCS	**Cryptographic support**	
FCS_RND.1	Quality metric for random numbers	PP / ST
FMT	**Security management**	
FMT_LIM.1	Limited capabilities	PP
FMT_LIM.2	Limited availability	PP
FPT	**Protection of the TOE Security Functions**	
FPT_TST.2	Subset TOE testing	ST

Table 3: SFRs CC part 2 extended

Note: Only the titles of the Security Functional Requirements are provided. For more details please refer to the Security Target [6], chapter 5.1.1 and 7.2.

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

TOE Security Functions	Description
SF1	Operating state checking
SF2	Phase management with test mode lock-out
SF3	Protection against snooping
SF4	Data encryption and data disguising
SF5	Random number generation
SF6	TSF self test
SF7	Notification of physical attack
SF8	Memory Management Unit (MMU)
SF9	Cryptographic support

Table 4: TOE Security Functions

SF1: Operating state checking

Correct function of the SLE66CX642P with RSA 2048 is only given in the specified range. To prevent an attack exploiting that circumstance, it is necessary to detect if the specified range is left.

[9] PP/ST: component is described in the PP but operations are performed in the ST.

All operating signals are filtered to prevent malfunction and the operation state is monitored with sensors for the operating voltage, clock signal, frequency, temperature and electromagnetic radiation.

SF2: Phase management with test mode lock-out

During start-up of the TOE the decision for the user mode or the test mode is taken depending on several phase identifiers. If test mode is the active phase, the TOE requests authentication before any action (test mode lock-out).

The phase management is used to provide the separation between the security enforcing functions and the user software. After TOE delivery the TOE is set to user mode.

SF3: Protection against snooping

Several mechanisms, like topological design measures for disguise, protect the TOE against snooping the design or the user data during operation and even if it is out of operation (power down).

SF4: Data encryption and data disguising

The memory contents of the TOE is encrypted on chip to protect against data analysis on stored data as well as on internally transmitted data. Only the key owner has the possibility to read out data. To prevent interpretation of leaked information, randomness is inserted in the information. This function is specifically effective to prevent DPA during DES calculations.

SF5: Random number generation

Random data are essential for cryptography as well as for physical security mechanisms. The TOE is equipped with a true random generator based on physical probabilistic effects. The random data can be used from the user software as well as from the security enforcing functions.

SF6: TSF self test

The TSF of the SLE66CX642P with RSA 2048 has a hardware controlled self-test which can be started from the user software or is started directly to test SF1, SF5 and SF7. Any attempt to modify the sensor devices will be detected from the test.

SF7: Notification of physical attack

The entire surface of the TOE is protected with the active shield. Attacks over the surface are detected when the shield lines are cut or get contacted.

SF8: Memory Management Unit (MMU)

The MMU in the TOE gives the user software the possibility to define different access rights for memory areas. In case of an access violation the MMU will generate a non maskable interrupt (NMI). Then an interrupt service routine can react on the access violation. The policy of setting up

the MMU and specifying the memory ranges is defined by the user software.

SF9: Cryptographic Support

Cryptographic operations are provided by the TOE. The TOE is equipped with several hardware accelerators to support the standard cryptographic operation. The components are a hardware DES encryption unit and a combination of software and hardware unit to support RSA cryptography and RSA key generation.

As the final transition from test mode to user mode is performed before TOE delivery, all TOE Security Functions are applicable from TOE delivery at the end of phase 3 or 4 (depending on when TOE delivery takes place in a specific case) to phase 7. The RSA functionality as part of SF9 is only available, if the embedded software developer implements the RSA2048 library into the embedded software.

1.3 Strength of Function

The TOE's strength of functions is claimed 'high' (SOF-high) for specific functions as indicated in the Security Target [6, chapter 6]. 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) (see Chapter 9 of this report).

1.4 Summary of threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product

The threats which were assumed for the evaluation and averted by the TOE and the organisational security policies defined for the TOE are specified in the Security Target [6] and can be summarised as follows.

It is assumed that the attacker is a human being or a process acting on behalf of him.

So called standard high-level security concerns defined in the Protection Profile [9] were derived from considering the end-usage phase (Phase 7 of the life cycle as described in the Security Target) as follows:

- manipulation of User Data and of the smart card Embedded Software (while being executed/processed and while being stored in the TOE's memories),
- disclosure of User Data and of the smart card Embedded Software (while being processed and while being stored in the TOE's memories) and
- deficiency of random numbers.

These high-level security concerns are refined in the Protection Profile [9] and used by the Security Target [6] by defining threats on a more technical level for

- Inherent Information Leakage,
- Physical Probing,
- Physical Manipulation,
- Malfunction due to Environmental Stress,
- Forced Information Leakage,
- Abuse of Functionality and
- Deficiency of Random Numbers.

Phase 1 and the Phases from TOE Delivery up to the end of Phase 6 are covered by assumptions (see below).

The development and production environment starting with Phase 2 up to TOE Delivery are covered by an organisational security policy outlining that the IC Developer / Manufacturer must apply the policy “Protection during TOE Development and Production (P.Process-TOE)” so that no information is unintentionally made available for the operational phase of the TOE. The Policy ensures confidentiality and integrity of the TOE and its related design information and data. Access to samples, tools and material must be restricted.

A specific additional security functionality for DES, Triple-DES and RSA-encryption and decryption must be provided by the TOE according to an additional security policy defined in the Security Target.

Objectives are taken from the Protection Profile plus additional ones related to the additional policy.

1.5 Special configuration requirements

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 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). At this point in time the operating system software including the RSA2048 library (IC dedicated SW part of the TOE) is already stored in the non-volatile memories of the chip and the *test mode* is disabled.

Thus, there are no special procedures for generation or installation that are important for a secure use of the TOE. The further production and delivery processes, like the Smart Card Finishing Process, Personalisation and the delivery of the smart card to an end user, have to be organised in a way that excludes all possibilities of physical manipulation of the TOE.

There are no special security measures for the start-up of the TOE besides the requirement that the controller has to be used under the well-defined operating conditions and that the requirements on the software have to be applied as described in the user documentation and chapter 10 of this Report.

1.6 Assumptions about the operating environment

Since the Security Target claims conformance to the Protection Profile [9], the assumptions defined in section 3.2 of the Protection Profile are valid for the Security Target of this TOE. With respect to the life cycle defined in the Security Target, Phase 1 and the Phases from TOE Delivery up to the end of Phase 6 are covered by these assumptions from the PP:

The developer of the smart card Embedded Software (Phase 1) must ensure:

- the appropriate “Usage of Hardware Platform (A.Plat-Appl)” while developing this software in Phase 1. Therefore, it has to be ensured, that the software fulfils the assumptions for a secure use of the TOE. In particular the assumptions imply that developers are trusted to develop software that fulfils the assumptions.
- the appropriate “Treatment of User Data (A.Resp-Appl)” while developing this software in Phase 1. The smart card operating system and the smart card application software have to use security relevant user data of the TOE (especially keys and plain text data) in a secure way. It is assumed that the Security Policy as defined for the specific application context of the environment does not contradict the Security Objectives of the TOE. Only appropriate secret keys as input for the cryptographic function of the TOE have to be used to ensure the strength of cryptographic operation.

Protection during Packaging, Finishing and Personalisation (A.Process-Card) is assumed after TOE Delivery up to the end of Phase 6, as well as during the delivery to Phase 7.

The following additional assumption is assumed in the Security Target:

- Key-dependent functions (if any) shall be implemented in the smart card Embedded Software in a way that they are not susceptible to leakage attacks (A.Key-Function).

1.7 Disclaimers

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 following TOE deliverables are provided for a customer who purchases the TOE (version m1485b16):

No	Type	Identifier	Release	Date	Form of Delivery
1	HW	SLE66CX642P Smart Card IC	GDS-file-ID: m1485b16 with production line indicator: “2” (Dresden)		Wafer or packaged module
2	SW	STS Self Test Software *(the IC Dedicated Test Software)*	V53.10.13		Stored in Test ROM on the IC
3	SW	RMS Resource Management System *(the IC Dedicated Support Software)*	V1.5		Stored in reserved area of User ROM on the IC
4	SW	RSA2048 library	V1.30		Source code in electronic form

Table 5: Delivered hardware and software of the TOE, version m1485b16

No	Type	Identifier	Release	Date	Form of Delivery
5	DOC	SLE66CxxxP Security Controller Family, Data Book [10]	08.04	August 2004	Hardcopy and pdf-file
6	DOC	Confidential Errata and Information Sheet-SLE66CxxxP Products and Bondout [11]	07.04	July 2004	Hardcopy and pdf-file
7	DOC	SLE66CxxxP Security Controller Family, Confidential Instruction Set [12]	05.01	May 2001	Hardcopy and pdf-file
9	DOC	RSA 2048 bit Support, RSA Interface Specification for Library V1.30 [13]	12.04	Dec. 2004	Hardcopy and pdf-file
10	DOC	RSA 2048 bit Support, Arithmetic Library for V1.30 [14]	12.04	Dec. 2004	Hardcopy and pdf-file
11	DOC	Application Notes [15] – [28]	See chapter 14 below		Hardcopy and pdf-file

Table 6: Delivered documents of the TOE for version m1485b16

The hardware part of the version of the TOE is identified by SLE66CX642P m1485b16 and the GDS-file. For identification of a specific chip, the Chip Identification Number stored in the EEPROM can be used (see [10, chapter 7] and [11, table 2-8]):

- The chip type byte identifies the different versions in the following manner:
  7C hex for version m1485b1(x).
  Using the additional detailed production parameter bytes, one can reconstruct the last character (x) of the version number of a specific chip via a data base system at Infineon Logistic Department.
- The STS is identified by its unique version number which is stored in three additional control bytes of the Chip Identification Number.
- The RMS is identified by its unique version number. As the RMS is part of the ROM mask, one can get the RMS version number for a specific chip by using the ROM type bytes and asking the data base system at Infineon Logistic Department.
- The first nibble of the batch number gives the production line indicator which is “2” for the chip version 1485b16 manufactured in Infineons IC fabrication in Dresden, Germany.

The RSA2048 library, as a separate software part of the TOE is identified by its unique version number.

The delivery process from Infineon to their customers (to Phase 5 or Phase 6 of the life- cycle) guarantees, that the customer is aware of the exact versions of the different parts of the TOE as outlined above.

To ensure that the customer receives the evaluated version of the chip, either

- he has to personally pick up the TOE (IC on Wafers or as Modules) at the Infineon Warehouse in Regensburg (VKL-Rgb) (see part D, annex A of this report) or
- the TOE (IC on Wafers or as Modules) is sent as a secured transport by specific haulage companies from the Infineon Warehouse in Regensburg (VKL-Rgb) directly or via one of three distribution centers (DC E for Europe, DC A for Asia and DC U for the United States) to the customer. The sender informs the receiver that a delivery was started; after the delivery was received it has to be checked according to the consignment notes and the sender is to be informed immediately about result of the check.

TOE documentation is delivered either as hardcopy or as softcopy (encrypted) according to defined mailing procedures.

The TOE RSA2048 software is delivered as softcopy (encrypted source code) to the embedded software developer according to defined mailing procedures usually as part of the Infineon Software Development Kit for this chip. After implementation of the RSA2048 functionality into the embedded software, this is

delivered back as part of the customers deliverables (e.g. ROM-code) into the chip production of Infineon.

Defined procedures at the development and production sites guarantee that the right versions of the RMS and STS are implemented into a specific ROM mask for a TOE IC.

3. Security Policy

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 a symmetric cryptographic block cipher 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. Additionally, a combination of software and hardware parts of the TOE implement RSA cryptography and RSA key generation.

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 DES, Triple-DES and RSA 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 smart card operating system and the application software stored in the User ROM and in the EEPROM are not part of the TOE. The code in the Test ROM of the TOE (IC Dedicated Test Software) is used by the TOE manufacturer to check the chip function before TOE delivery. This was considered as part of the evaluation under the CC assurance aspects ALC for relevant procedures and under ATE for testing.

The TOE is delivered as a hardware unit at the end of the chip manufacturing process (phase 3 of the life cycle defined) or at the end of the IC packaging into modules (phase 4 of the life cycle defined). At these specific points in time the operating system software is already stored in the non-volatile memories of the chip and the test mode is completely disabled.

The smart card applications need the Security Functions of the smart card operating system based on the security features of the TOE. With respect to

security the composition of this TOE, the operating system, and the smart card application is important. Within this composition the security functionality is only partly provided by the TOE and causes dependencies between the TOE Security Functions and the functions provided by the operating system or the smart card application on top. These dependencies are expressed by environmental and secure usage assumptions as outlined in the user documentation.

Within this evaluation of the TOE several aspects were specifically considered to support a composite evaluation of the TOE together with an embedded smart card application software (i.e. smart card operating system and application). This was necessary as Infineon Technologies AG is the TOE developer and manufacturer and responsible for specific aspects of handling the embedded smart card application software in its development and production environment. For those aspects refer to part B, chapter 9.2 of this report.

The full evaluation results are applicable only for TOE chips from the semiconductor factory in Dresden, labelled by the production line indicator „2“.

5. Architectural Information

The Infineon Smart Card IC (Security Controller) SLE66CX642P/m1485b16 with RSA 2048 V1.30 and specific IC Dedicated Software are integrated circuits (IC) plus supporting software for RSA calculations 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 SLE66CX642P/m1485b16 is to be found in the Data Book [10] and other guidance documents delivered to the customer, e.g. Confidential Instruction Set [12].

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 (ACE and DDC) 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 software for RSA calculations uses the defined TOE hardware interfaces and is to be implemented by the embedded software developer as outlined in the RSA Interface Specification [13]. It provides a high level software interface to the users operating system and application.

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.

6. Documentation

The documentation [10] – [28] is provided with the product 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:

(i) tests which are performed in a simulation environment for analogue and for digital simulations;

(ii) functional production tests, which are done as a last step of the production process (phase 3) and, in case TOE delivery is at the end of phase 4, additionally done as a last step of IC Packaging. These tests are done for every chip to check its correct functionality;

(iii) qualification tests to release the TOE to production to determine the behaviour of the chip with respect to different operating conditions (often also referred to as characterisation tests);

(iv) special verification tests on functionality of the chip which were done with samples of the TOE in user mode;

(v) special verification tests on Security Functions which were done with samples of the TOE in user mode;

(vi) layout tests as part of the design and release process by testing the implementation by optical control, in order to verify statements concerning the layout design.

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

The evaluators confirmed test results from the previous certification procedure BSI-DSZ-CC-0266-2005 where they could repeat the tests of the developer either using the library of programs and tools delivered to the evaluator or at the developers site and where they 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. Security features of the TOE realised by specific design and layout measures were checked by the evaluators during layout inspections at that time.

For this re-evaluation, the developer provided test evidence for chips from the production site Dresden. The test results confirm the correct implementation of the TOE Security Functions.

The evaluators supplied evidence that the actual version of the TOE SLE66CX642P/m1485b16 with RSA 2048 with production line indicator “2” (Dresden) provides the Security Functions as specified.

For this re-evaluation the evaluators re-assessed the penetration testing and confirmed the results from the previous certification procedure BSI-DSZ-CC-0266-2005 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.

8. Evaluated Configuration

The TOE is identified by the version Infineon Smart Card IC (Security Controller) SLE66CX642P/m1485b16 with RSA 2048 V1.30 and specific IC Dedicated Software with production line indicator “2” (Dresden). The TOE has only one fixed evaluated configuration at the time of delivery.

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

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*. Thus, the evaluation was mainly performed in the *user mode*. 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 Evaluation of the TOE

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

The evaluation methodology CEM [2] was used for those components identical with EAL4. For components beyond EAL4 the methodology was defined in co-ordination with the Certification Body [4, AIS 34]). For smart card IC specific methodology the CC supporting documents

(i) The Application of CC to Integrated Circuits

(ii) Application of Attack Potential to Smartcards and

(see [4, AIS 25 and AIS 26]) and [4, AIS 31] (*Functionality classes and evaluation methodology for physical random number generators)* were used. The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

The verdicts for the CC, Part 3 assurance components (according to EAL5 augmented and the class ASE for the Security Target evaluation) are summarised in the following table.

Assurance classes and components		**Verdict**
Security Target evaluation	CC Class ASE	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	PASS
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration management	CC Class ACM	PASS
Partial CM automation	ACM_AUT.1	PASS
Generation support and acceptance procedures	ACM_CAP.4	PASS
Development tools CM coverage	ACM_SCP.3	PASS
Delivery and operation	CC Class ADO	PASS
Detection of modification	ADO_DEL.2	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC Class ADV	PASS
Semiformal functional specification	ADV_FSP.3	PASS
Semiformal high-level design	ADV_HLD.3	PASS
Implementation of the TSF	ADV_IMP.2	PASS
Modularity	ADV_INT.1	PASS
Descriptive low-level design	ADV_LLD.1	PASS
Semiformal correspondence demonstration	ADV_RCR.2	PASS
Formal TOE security policy model	ADV_SPM.3	PASS
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS

Assurance classes and components		Verdict
Life cycle support	CC Class ALC	PASS
Sufficiency of security measures	ALC_DVS.2	PASS
Standardised life-cycle model	ALC_LCD.2	PASS
Compliance with implementation standards	ALC_TAT.2	PASS
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: low-level design	ATE_DPT.2	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing – sample	ATE_IND.2	PASS
Vulnerability assessment	CC Class AVA	PASS
Covert channel analysis	AVA_CCA.1	PASS
Analysis and testing for insecure states	AVA_MSU.3	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Highly resistant	AVA_VLA.4	PASS

Table 7: Verdicts for the assurance components

The evaluation has shown that:

- the TOE is conform to the Smartcard IC Platform Protection Profile, BSI-PP-0002-2001 [9]
- Security Functional Requirements specified for the TOE are Common Criteria Part 2 extended
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL5 augmented by ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4
- The following TOE Security Functions fulfil the claimed Strength of Function:
  SF 2 (Phase management with test mode lock-out),
  SF 3 (Protection against snooping),
  SF 4 (Data encryption and data disguising) and
  SF 5 (Random number generation)
  Therefore the scheme interpretations AIS 26 and AIS 31 (see [4]) were used.

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

(i) the TOE Security Function SF9 -- which is

a) DES encryption and decryption by the hardware co-processor and

b) RSA encryption, decryption and key-generation by the combination of hardware co-processor and RSA2048 Software -- and

(ii) for other usage of encryption and decryption within the TOE.

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

The code in the Test ROM of the TOE (IC Dedicated Test Software) is used by the TOE manufacturer to check the chip function before TOE delivery. This was considered as part of the evaluation under the CC assurance aspects ALC for relevant procedures and under ATE for testing.

The results of the evaluation are only applicable to the SLE66CX642P/m1485b16 with RSA 2048 produced in the semiconductor factory in Dresden, labelled by the production line indicator „2“ within the chip identification number in the EEPROM, and the firmware and software versions as indicated in table 5.

The validity can be extended to new versions and releases of the product or to chips from other production and manufacturing sites, provided the sponsor applies for re-certification or assurance continuity of the modified product, in accordance with the procedural requirements, and the evaluation of the modified product does not reveal any security deficiencies.

9.2 Additional Evaluation Results

- The evaluation confirmed specific results of a previous smart card IC evaluation regarding assurance aspects for the development and production environment. This is outlined in part D of this report, annex A.
- To support a composite evaluation of the TOE together with a specific smart card embedded software additional evaluator actions were performed during the TOE evaluation. The results are documented in the ETR-lite [8] according to [4, AIS 36]. Therefore, the interface between the smart card embedded software developer and the developer of the TOE was examined in detail.

10. Comments/Recommendations

1. The operational documents [10] - [28] contain necessary information about the usage of the TOE and all security hints therein have to be considered.
2. In the following, specific items are listed:

   - In the operational environment of the TOE the following assumptions about the environment as outlined in the Security Target have to be fulfilled:
     “Protection during packaging, finishing and personalisation” resulting from the assumption A.Process-Card of the Security Target: *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.
The assumptions on the usage of the hardware platform (A.Plat-Appl), treatment of user data (A.Resp-Appl) and on usage of key-dependent functions (A.Key-Function) have to be fulfilled (see part B, chapter 1.6 of this report). For measures important for A.Key-Function refer to [17].

- The functional requirements for the environment defined in the Security Target [6, chapter 5.2] have to be taken into consideration by the Smartcard Embedded Software Developer.

- The Embedded Software
has to activate Wait states and CURSE functionality for all operations of the Embedded Software critical for side channel attacks (e.g. SPA / DPA),
has to use parameters for memory encryption E0ADR, E2ADR and XKEY which configure the ranges of encryption,
has to configure the MMU correct,
has to call the self tests of the TSF implemented in the RMS routines in order to detect failures of the sensors. This self test is executed automatically after each reset. 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 to avoid attacks on the composite product.

- It is possible to store data in the EEPROM without encryption, which might constitute a risk in case an attacker is given the possibility to read out this data. The operating system developer is responsible for the use of all security functionality made available by the TOE and controllable by him in such a way, that secure operation is guaranteed. These are the parameters for memory encryption determining areas for the encryption. In the data book [10, chapter 19] it is pointed out to the operating system developer, which effects on the security not proper use of this functionality might have, and it is described in detail, how to use effectively the security mechanisms made available by the TOE.

- In case an alarm is triggered, the content of the XRAM is not being deleted. In order to prevent an attacker from reading out this data, the embedded software has to delete explicitly the XRAM after each reset (see [10, chapter 7]).

- The delivered MMU is set so, that SLE66CX642P/m1485b16 is compatible with SLECX160S, i.e. all ROM areas are mapped. Since the movec blockade of the SLE66CX160S is no longer implemented, in this setting reading out of the ROM by a programme in the EEPROM is possible. In order to avoid this, the operating system developer has to programme the MMU in a way that reading out is impossible. This fact is pointed out in the data book [10, chapter 19].
- ROM contents of chips, being manufactured with the same user mask are identically encrypted. This leads to the possibility to carry out ROM read out attacks using as many samples as available and combining all results. Therefore, it is recommended to store security critical data (e.g. identification and authentication data) not in the ROM, but in the EEPROM (this is encrypted chip individually). This fact is pointed out to the operating system developer in application note [18].
- 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 might be observable by means of a SPA / DPA. In order to prevent this, the transfer of the keys have to be protected using the measures described in application note [17].
- The TOE has an active shielding for the identification of attacks by means of physical probing. It is possible for the operating system developer to configure the active shielding (see application note [19]). It is recommended to change the configuration of the active shielding before any security critical operation and to compare the returned values with the expected values accordingly.
- The TOE is protected by light sensors against DFA light attacks. Within the delivered RSA2048 library countermeasures against DFA attacks are implemented.
  The Smartcard Embedded Software Developer has to implement sufficient countermeasures in his software to counter such attacks, too. An example of a possible implementation of such a countermeasure is given in application note [23]. Furthermore the Smartcard Embedded Software Developer has to calculate DES encryption and decryption or decryption and encryption respectively and compare the results as described in application note [17].
- In order to protect the TOE against attacks on power consumption (e.g. DPA), the wait states functionality in connection with the random number generator and additional features to modify the current profile have to be used by the operating system developer, together with additional software measures, as described in [10, chapter 19].
- For the fulfilment of the Strength of Function “medium” or "high" for the Random Number Generator according to [4, AIS31] specific guidance has to be followed by the Smartcard Embedded Software

Developer:
In [10, chapter 16.3.5] the user of the TOE (the Smartcard Embedded Software Developer) is recommended to perform the online test via the RMS function *SleRngAIS31AnalogTest* at start-up or at least before using the RNG.
In [10, chapter 6.11.21], [16, chapter 2.2] and [13] it is stated that the operating system should generate one ore more keys and then perform the online test via the RMS function *SleRngAIS31AnalogTest* until the final test results are obtained (SLE_AIS31_PASS). This online test is mandated and the keys can be used if the test has passed, but must be discarded if the test fails.
In addition the evaluator came to the conclusion that a RNG live test (one call of *SleRngAIS31AnalogTest*) shall be executed at least once after power up and latest before usage of the RNG data for security relevant operation (e.g. key generation).
Furthermore, it is strongly recommended to call the live test (one call of *SleRngAIS31AnalogTest*) latest before any operation is executed that shall be protected by chip internal randomisation mechanisms (CURSE, Random Wait States, Bus Confusion).
Random numbers used for RNG tests performed by the Embedded Software shall be kept confidential by the application software.
For further advice see data book [10, chapter 16 and 6.11.21] and application note [16].

3. Depending on the security policy of the complete smart card product and on the specific usage of the RSA-Functionality of this TOE in combination with RSA supporting functionality provided by the environment (see Security Target [6, chapter 5.2]) SPA/DPA analysis for RSA-Functionality must be part of the smart card composite product evaluation.

4. As an outcome of this evaluation, the customer has to follow the evaluated delivery procedures (see chapter 2 above). In case of differing delivery procedures, these have to be evaluated in the course of the operating system evaluation or the smart card composite product evaluation.
In the following, specific items regarding delivery are listed:

   - 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. Deliverables send in electronic form (i.e. guidance documents, RSA library) have to be send and accepted only in encrypted form.

11. Annexes

Annex A: Evaluation results regarding the development and production environment (see part D of this report).

12. Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document.

13. Definitions

13.1 Acronyms

ACE	Advanced Crypto Engine
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
DES	Data Encryption Standard; symmetric block cipher algorithm
DPA	Differential Power Analysis
EAL	Evaluation Assurance Level
ECB	Electrical Code Block
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
PP	Protection Profile
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest, Shamir, Adelmann – a public key encryption algorithm
SF	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

13.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

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

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

Informal - Expressed in natural language.

Object - An entity within the TSC that contains or receives information and upon which subjects perform operations.

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

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

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

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

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

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

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or

intentional breach of TOE security by attackers possessing a moderate attack potential.

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

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

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

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

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

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

14. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999

[2] Common Methodology for Information Technology Security Evaluation (CEM), Part 1, Version 0.6; Part 2: Evaluation Methodology, Version 1.0, August 1999

[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 2, 29 July 2002 for: CC Supporting Document, - The Application of CC to Integrated Circuits, Version 1.2, July 2002
- AIS 26, Version 2, 6 August 2002 for: CC Supporting Document, - Application of Attack Potential to Smartcards, Version 1.1, July 2002
- AIS 31, Version 1, 25 Sept. 2001 for: Functionality classes and evaluation methodology of physical random number generators
- AIS 32, Version 1, 02 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungs-schema.

- AIS 34, Version 1.00, 1 June 2004, Evaluation Methodology for CC Assurance Classes for EAL5+
- AIS 36 Version 1, 29 July 2002 for CC Supporting Document, ETR-lite for Composition, Version 1.1, July 2002 and CC Supporting Document, ETR-lite for Composition: Annex A Composite smartcard evaluation, Version 1.2, March 2002

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

[6] Infineon Technologies AG, Security and Chipcard ICs, Security Target, SLE66CX642P/m1485b16, with RSA2048 V1.30, 20. April 2004, Version 1.2

[7] Evaluation Technical Report, Version 3, 27. June 2005, for the Product Smart Card IC (Security Controller) SLE66CX642P/m1485b16, with RSA2048 V1.30, (confidential document)

[8] ETR-lite for composition, according to AIS 36, Version 3.0, 27.06.2005, for the Product Smart Card IC (Security Controller) SLE66CX642P/m1485b16, with RSA2048 V1.30, (confidential document)

[9] Smartcard 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] Infineon Technologies AG, Security and Chipcard ICs, SLE66CxxxP, Security Controller Family, Data Book Version 08.04, (confidential document)

[11] Confidential Errata and Information Sheet- SLE66CxxxP Products and Bondout, Version 05.05, (confidential document)

[12] SLE66CxxxP, Security Controller Family, Confidential Instruction Set, 05.01, (confidential document)

[13] RSA 2048 bit Support, SLE66CX642P, RSA Interface Specification for Library V1.30, Version 12.04, (confidential document)

[14] RSA 2048 bit Support, SLE66CX642P, Arithmetic Library for V1.30, Version 12.04 (confidential document)

[15] Confidential Application Note, SLE66CxxxP, Transfer of a ROM Mask from SLE66CxxS to SLE66CxxxP, Version 06.01

[16] Confidential Application Note, SLE 66CxxxP and SLE 66CxxxPE, Testing the Random Number Generator, Version 11.04

[17] Confidential Application Note, SLE66xxxP, DDES – EC2, Accellerator, Version 02.04

[18] Confidential Application Note, SLE66CxxxP, Memory Encryption Decryption, Version 11.04

[19] Confidential Application Note, SLE66CxxxP, Using the active shield security feature, Version 01.02

[20] Confidential Application Note, SLE66CxxxP, Issues concerning EEPROM, Version 08.00

[21] Confidential Application Note, MMU-Memory Management Unit, Version 12.04

[22] Confidential Application Note, SLE66CxxxP, Fast Switching of PLL, Version 03.03

[23] Confidential Application Note, Security Advice concerning Program Flow Manipulation – SLE11/22/44/66CxxxS/ 66CxxxP, Version 10.00

[24] Confidential Application Note, SLE66CxxS, Secure Hash Algorithm SHA-1, Version 01.98

[25] Confidential Application Note, SLE66CxxxP, UART, Version 10.03

[26] Confidential Application Note, SLE66CxxS, SLE66CxxxP, Using the CRC, Version 03.01

[27] Application Note, SLE66CxxxP, MMU Security Issues, Version 01.02

[28] Application Note, SLE66CXxxP, Infineon Chipcard Crypto API, Version 05.02

[29] Infineon Technologies AG, Secure Mobile Solutions, SLE66CX642P/m1485b16 with RSA 2048 V1.30; Configuration Management Scope (ACM_SCP), Version 1.1, 14. June 2005 (i.e. TOE Configuration List, confidential document)

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part 1:

Caveats on evaluation results (chapter 5.4) / **Final Interpretation 008**

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 Part 2 (functional requirements), 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:

Part 2 conformant - A PP or TOE is Part 2 conformant if the functional requirements are based only upon functional components in Part 2

Part 2 extended - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2

plus one of the following:

Part 3 conformant - A PP or TOE is Part 3 conformant if the assurance requirements are based only upon assurance components in Part 3

Part 3 extended - A PP or TOE is Part 3 extended if the assurance requirements include assurance requirements not in 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:

Assurance categorisation (chapter 2.5)

„The assurance classes, families, and the abbreviation for each family are shown in Table 2.1.

Assurance Class	Assurance Family	Abbreviated Name
Class ACM: Configuration management	CM automation	ACM_AUT
	CM capabilities	ACM_CAP
	CM scope	ACM_SCP
Class ADO: Delivery and operation	Delivery	ADO_DEL
	Installation, generation and start-up	ADO_IGS
Class 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
Class AGD: Guidance documents	Administrator guidance	AGD_ADM
	User guidance	AGD_USR
Class ALC: Life cycle support	Development security	ALC_DVS
	Flaw remediation	ALC_FLR
	Life cycle definition	ALC_LCD
	Tools and techniques	ALC_TAT
Class ATE: Tests	Coverage	ATE_COV
	Depth	ATE_DPT
	Functional tests	ATE_FUN
	Independent testing	ATE_IND
Class AVA: Vulnerability assessment	Covert channel analysis	AVA_CCA
	Misuse	AVA_MSU
	Strength of TOE security functions	AVA_SOF
	Vulnerability analysis	AVA_VLA

Table 2.1 -Assurance family breakdown and mapping“

Evaluation assurance levels (chapter 6)

„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 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 6.1)

Table 6.1 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 2 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 CC 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 6.1 - Evaluation assurance level summary“

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 6.2.1)

„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 6.2.2)

„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 6.2.3)

„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 6.2.4)

„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 6.2.5)

„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 6.2.6)

„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 6.2.7)

„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 14.3)

AVA_SOF Strength of TOE security functions

„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 14.4)

AVA_VLA Vulnerability analysis

„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), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential.“

This page is intentionally left blank.

D Annexes

List of annexes of this certification report

This page is intentionally left blank.

Annex A of Certification Report BSI-DSZ-CC-0315-2005

Evaluation results regarding development and production environment

The IT product, Infineon Smart Card IC (Security Controller) SLE66CX642P/m1485b16 with RSA 2048 V1.30 and 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, Part 1 Version 0.6, Part 2 Version 1.0, extended by advice of the Certification Body for components beyond EAL4 and smart card specific guidance, for conformance to the Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC15408: 1999) and including final interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

As a result of the TOE certification, dated 12. August 2005, the following results regarding the development and production environment apply. The Common Criteria assurance requirements

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

are fulfilled for the development and production sites of the TOE listed below ((a) – (g)):

(a) **Infineon Technologies AG, Königsbrücker Str. 180, 01099 Dresden, Germany (semiconductor factory)**

(b) **Infineon TechnologiesAG, St.-Martin-Straße 76, 81541 München, Germany (development center)**

(c) **Infineon Technologies AG, Leibnizstraße 6, D-93055 Regensburg, Germany (IC packaging into modules and warehouse and delivery center)**

(d) **Infineon Technologies AG, Development Center Graz, Babenbergerstr. 10, A-8020 Graz, Austria (development center)**

(e) **Infineon Technologies Asian Pacific, Exel Singapure Pte. Ltd., 81 ALPS Avenue, Exel Supply Chain Hub, Singapure 498803**

(f) **Du Pont Photomasks France S.A., 224, bd John Kennedy, F-91105 Corbeil Essonnes, France (mask shop)**

(g) **Infineon Technologies AG, Alter Postweg 101, D-86159 Augsburg (development center)**

The hardware part of the TOE produced in the semiconductor factory in Dresden is labelled by the production line indicator „2“.

For all sites listed above, the requirements have been specifically applied for each site and in accordance with the Infineon Technologies AG, Security and Chipcard ICs, Security Target, SLE66CX642P/m1485b16, with RSA2048 V1.30, 20. April 2004, Version 1.2 [6]. The evaluators verified, that the threats are countered and the

security objectives for the life cycle phases 2, 3 and 4 up to delivery at the end of phase 3 or 4 as stated in the TOE Security Target are fulfilled by the procedures of these sites.