CERTIFICATION REPORT

Certification file:	**TUVIT-DSZ-CC-9246**
Product / system:	Smart Card IC (Security Controller) SLE66CLX640P / m1523a11, SLE66CLX641P / m1522a11
Product manufacturer:	Infineon Technologies AG St.-Martin-Straße 53 81669 München
Customer:	see above
Evaluation facility:	TÜViT, evaluation body for IT security
Evaluation report:	*Version 1 as of 2005-07-22* Document-number: *20676378_TÜViT_041.01* Author: Dr. Patrick Bödeker, Dr. Karsten Grans
Result:	EAL5 augmented by ALC_DVS.2, AVA_MSU.3, AVA_VLA.4
Evaluation stipulations:	14 (see chapter 10)
Certifier:	Dr. Christoph Sutter
Certification stipulations:	one (see chapter 11)

Essen, 2005-07-29

Dr. Ernst-Hermann Gruschwitz Dr. Christoph Sutter

Contents

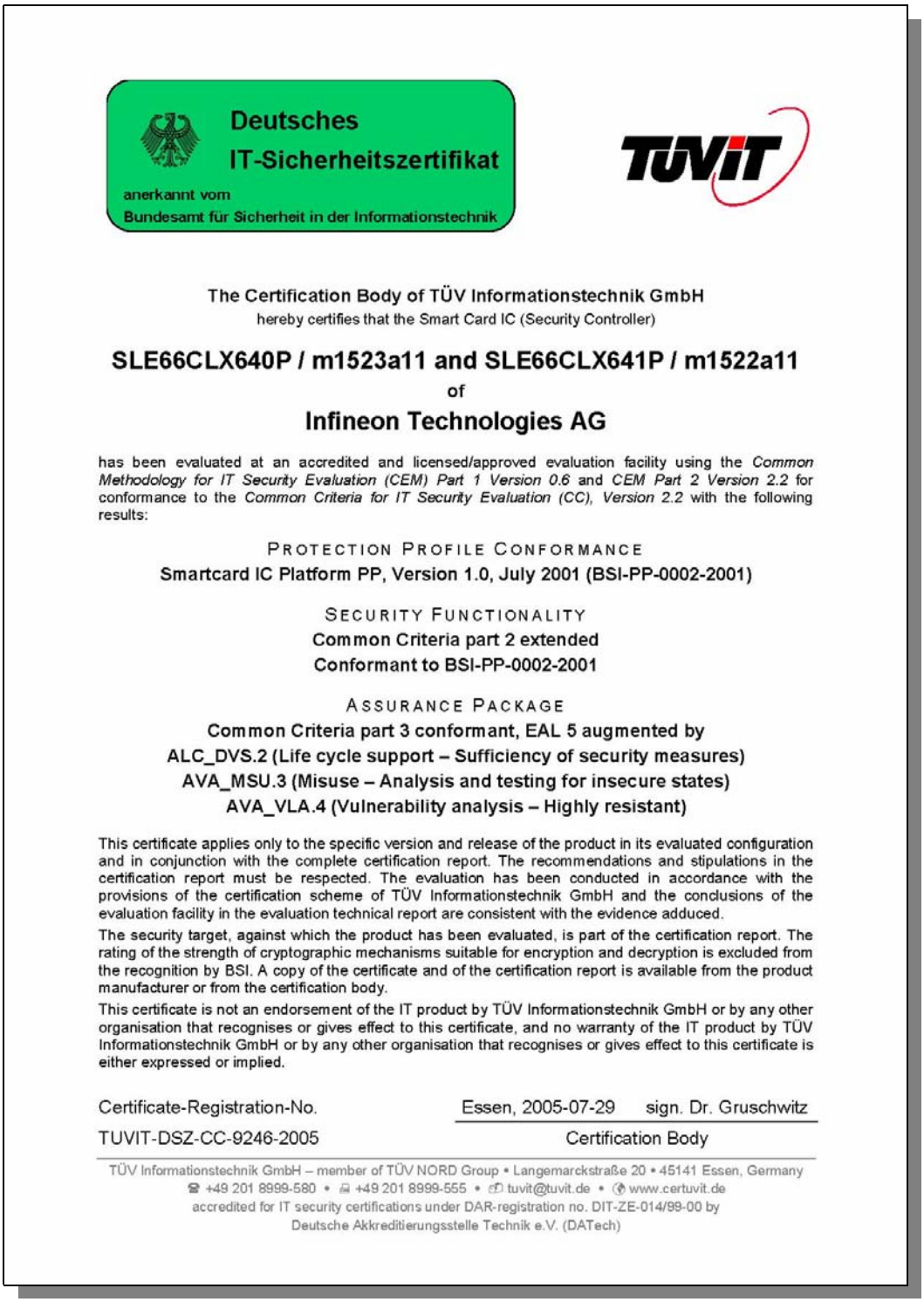
Part A

Certificate and Background of the Certification

Part A presents a copy of the issued certificate and summarizes

- information about the certification body,
- the certification procedure, and
- the performance of evaluation and certification.

1 The Certificate



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

The Certification Body of TÜV Informationstechnik GmbH
hereby certifies that the Smart Card IC (Security Controller)

SLE66CLX640P / m1523a11 and SLE66CLX641P / m1522a11
of
Infineon Technologies AG

has been evaluated at an accredited and licensed/approved evaluation facility using the *Common Methodology for IT Security Evaluation (CEM) Part 1 Version 0.6* and *CEM Part 2 Version 2.2* for conformance to the *Common Criteria for IT Security Evaluation (CC), Version 2.2* with the following results:

PROTECTION PROFILE CONFORMANCE
Smartcard IC Platform PP, Version 1.0, July 2001 (BSI-PP-0002-2001)

SECURITY FUNCTIONALITY
Common Criteria part 2 extended
Conformant to BSI-PP-0002-2001

ASSURANCE PACKAGE
Common Criteria part 3 conformant, EAL 5 augmented by
ALC_DVS.2 (Life cycle support – Sufficiency of security measures)
AVA_MSU.3 (Misuse – Analysis and testing for insecure states)
AVA_VLA.4 (Vulnerability analysis – 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 recommendations and stipulations in the certification report must be respected. The evaluation has been conducted in accordance with the provisions of the certification scheme of TÜV Informationstechnik GmbH and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The security target, against which the product has been evaluated, is part of the certification report. The rating of the strength of cryptographic mechanisms suitable for encryption and decryption is excluded from the recognition by BSI. A copy of the certificate and of the certification report is available from the product manufacturer or from the certification body.

This certificate is not an endorsement of the IT product by TÜV Informationstechnik GmbH or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Informationstechnik GmbH or by any other organisation that recognises or gives effect to this certificate is either expressed or implied.

Certificate-Registration-No. Essen, 2005-07-29 sign. Dr. Gruschwitz
TUVIT-DSZ-CC-9246-2005 Certification Body

TÜV Informationstechnik GmbH – member of TÜV NORD Group • Langemarckstraße 20 • 45141 Essen, Germany
☎ +49 201 8999-580 • 🖷 +49 201 8999-555 • 🖂 tuvit@tuvit.de • 🌐 www.certuvit.de
accredited for IT security certifications under DAR-registration no. DIT-ZE-014/99-00 by
Deutsche Akkreditierungsstelle Technik e.V. (DATech)

2 Certification Body – CERTÜVIT

CERTÜVIT, the Certification Body of *TÜV Informationstechnik GmbH*[1] – member of TÜV NORD Group – was established in 1998 and offers a variety of services in the context of security evaluation and validation.

CERTÜVIT was accredited in September 1999 for certification of IT security products according to ITSEC and Common Criteria by *Deutsche Akkreditierungsstelle für Informations- und Telekommunikationstechnik (Dekitz)* now *Deutsche Akkreditierungsstelle Technik e.V. (DATech), Frankfurt/Main* under DAR-registration no. DAT-ZE-014/99-01 and performs its projects under a quality management system certified against ISO 9001 by *Germanischer Lloyd, Hamburg*.

CERTÜVIT is accredited by *Bundesamt für Sicherheit in der Informationstechnik*[2] to issue the "German IT Security Certificate" which is recognised by BSI as equivalent to the "German IT Security Certificate" of BSI.

3 Specifications of the Certification Procedure

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

- DIN EN 45011
- TÜVIT Certification Scheme
- TÜVIT Certification Conditions
- Regulations on the "German IT Security Certificate" issued by the BSI and accepted in the contract of BSI and TÜVIT as of November 20, 2002.
- Common Criteria for Information Technology Security Evaluation (CC) part 1-3, version 2.2, January 2004.
- Common Methodology for Information Technology Security Evaluation (CEM) part 1, version 0.6, January 1997.
- Common Methodology for Information Technology Security Evaluation (CEM) part 2, version 2.2, January 2004.
- Application Notes and Interpretations of the Scheme (AIS), published by BSI.

[1] in the following termed shortly TÜVIT

[2] in the following termed shortly BSI

4 Recognition Agreements

In order to avoid multiple certification of the same product by different certification bodies a mutual recognition of IT security certificates – as far as such certificates are based on ITSEC or CC – under certain conditions was agreed. CERTÜViT certificates are German IT Security Certificates recognized by BSI – the national German certification body in international agreements – to be equivalent to its own certificates but they are not part of these international agreements.

4.1 CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4 was signed between the national participants of Australia and New Zealand, Austria, Canada, Czech Republic, Finland, France, Germany, Greece, Hungary, Israel, Italy, Japan, The Netherlands, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

4.2 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. The arrangement on the mutual recognition of IT security certificates based on the CC was extended by these participants up to and including the evaluation assurance level EAL7.

5 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure uniform procedures, interpretations of the criteria, and ratings. The Smart Card IC (Security Controller) *SLE66CLX640P / m1523a11, SLE66CLX641P / m1522a11* have undergone the certification procedure at TÜViT certification body. It was a complete re-certification of the Smart Card IC (Security Controller) *SLE66CX322P / m1484b14, SLE66CX322P / m1484f18* (BSI-DSZ-CC-0266-2005 as of 2005-04-22). Compared to the security controller *SLE66CX322P* the main differences are an additional radio frequency interface for contactless use and a bigger EEPROM memory size of 64 kBytes instead of 32 kBytes.

The evaluation of the Smart Card IC (Security Controller) SLE66CLX640P / m1523a11, SLE66CLX641P / m1522a11 was conducted by the evaluation body for IT-security of TÜViT and concluded on July 22, 2005. The TÜViT evaluation facility is recognised by BSI.

The sponsor as well as the developer is Infineon Technologies AG. Distributor of the product is Infineon Technologies AG.

The certification was concluded with

- the comparability check and
- the preparation of this certification report.

This work was concluded on July 29, 2005. The confirmation of the evaluation assurance level (EAL) only applies on the condition that

- all stipulations regarding generation, configuration and operation, as given in part B of this report, are observed,
- the product is operated – where indicated – in the environment described.

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

With regard to the meaning of the evaluation assurance levels (EAL) and the strength of function (SoF), please refer to part C of this report.

6 Publication

The following Certification Results consist of pages B-1 to B-28. The product SLE66CLX640P / m1523a11, SLE66CLX641P / m1522a11 will be included in the BSI list of certified products which is published at regular intervals (e. g. in the Internet at http://www.bsi.bund.de) and the TÜViT certification lists (http://www.certuvit.de).

Further copies of this certification report may be ordered from the sponsor of the product. The certification report may also be obtained in electronic form at the internet address of CERTÜViT as stated above.

Part B

Certification Result

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 Result

1 Executive Summary

1.1 Target of Evaluation and Evaluation Background

The target of evaluation (TOE) is the Smart Card IC (Security Controller) in the two versions ***SLE66CLX640P / m1523a11*** and ***SLE66CLX641P / m1522a11***.

Both products are identically from hardware perspective. The difference is in the mounting step only. Regarding the ***SLE66CLX641P*** the ISO7816 pads have not been contacted, thus this chip is for contactless use only, whereas the ***SLE66CLX640P*** provides both interface types and is for dual use therefore. Both types can be distinguished by a different chip ident. The TOE is internally registered under the development code m1523a11 (for SLE66CLX640P) and m1522a11 (for the SLE66CLX641P). The term a11 describes the design status.

Both security controller are variants of the SLE66CX322P architecture and manufactured in a 0.22 µm CMOS technology. They are intended to be used as a hardware platform for smart cards for particularly security-relevant applications.

The TOE hardware consists of a dedicated microprocessor (CPU) with a MMU (Memory Management Unit), several different memories, input and security logic, a timer and an interrupt-controlled I/O interface. A RNG (Random Number Generator) and a checksum module (CRC module) are integrated on the chip. In addition the TOE is equipped with a RF interface (radio frequency power and signal interface) that enables contactless communication between a PICC (proximity integrated chip card, PICC) and a reader/writer (proximity coupling device, PCD).This is illustrated in the following figure:

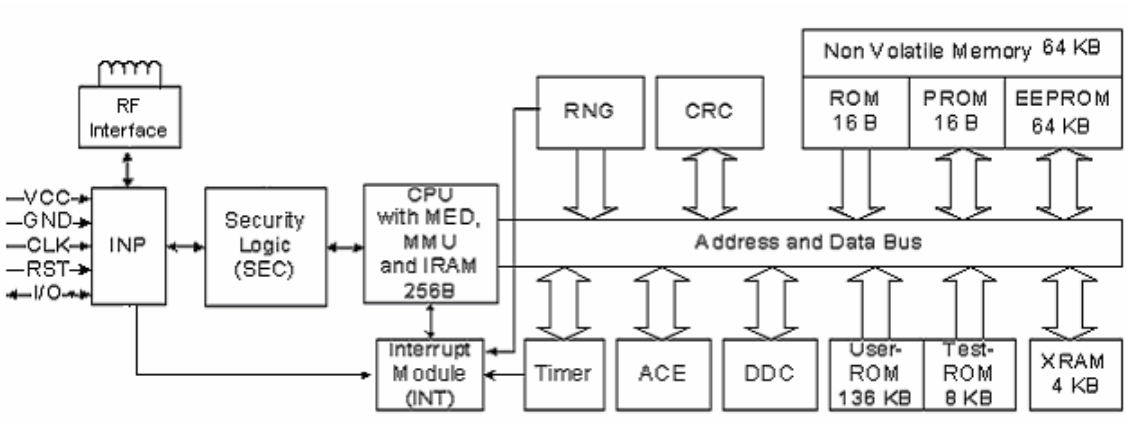


Figure 1: Block Diagram of the SLE66CLX640P / m1523a11

The CPU is compatible with the SAB 8051 instruction set and is 6 times faster than the standard processor. It provides additional instructions for smart card applications. The memory comprises 256 bytes of internal RAM (IRAM), 4 kBytes of extended RAM (XRAM), 136 kBytes of user ROM, 8 kBytes of test ROM, and 64 kBytes of EEPROM.

The CPU accesses the memory via the integrated Memory Encryption and Decryption unit (MED). The access rights of the application to the memories can be controlled with the memory management unit (MMU).

Security, sleep mode and interrupt logic as well as the RNG are specially designed for smart card applications. The sleep mode logic (clock stop mode per ISO/IEC 7816-3) is used to reduce the overall power consumption. The timer permits implementation of communication protocols such as T=1 and all other time-critical operations.

The UART-controlled I/O interface allows the smart card and terminal to be operated in parallel. The PLL unit allows operating the SLE66CLX640P / SLE66CLX641P with a multiplication factor over the external clock signal or free running with maximum frequency. The RNG does not supply a pseudorandom number sequence, but instead produces genuine random numbers under all conditions. The checksum module allows calculation of checksums per ISO 3309 (16 bit CRC).

Two modules for cryptographic operations are implemented on the TOE. The first module is the Advanced Crypto Engine (ACE) for calculation of asymmetric algorithms like RSA and elliptic curve (EC). This module is especially designed for chip card application with respect to the security and power consumption. The second module is the DDC which provides the DES algorithm and support for elliptic curve (EC) cryptography. This module computes the complete DES algorithm within a few clock cycles. That module is especially designed to counter attacks like DPA or EMA. The SLE66CLX640P and SLE66CLX641P include functionality to calculate single DES and 3DES operations. The evaluation includes the 3DES operation only.

The TOE software (firmware) required for operating the chip consists of routines for programming the EEPROM from application programs and for online testing of the security enforcing functions. These are stored in a reserved user ROM area. In addition, the chip initialization routine with security checks and identification mode as well as test routines for production testing are located in a separate test ROM.

The TOE comprises the hardware of the smart card security controller, SLE66CLX640P / m1523a11, SLE66CLX641P / m1522a11 and part of the associated firmware/software required for operation. The Smartcard Embedded Software is not part of the TOE.

The TOE is intended to be used in smart cards for particularly security-relevant applications. The term “user software” is used in the following for all operating systems and applications stored and executed on the TOE. The TOE provides the platform for the user software. The user software itself is not part of the TOE.

The TOE is conformant to the Smartcard IC Platform Protection Profile, Version 1.0, July 2001 [PP0002] and was evaluated against the claims of the Security Target[3] [ST] (attached in part D) by "*evaluation body of TÜV Informationstechnik GmbH*" (TÜViT). The evaluation was completed on July 22, 2005. TÜViT's evaluation body is recognised by BSI.

1.2 Assurance Package

The TOE security assurance requirements are based entirely on the assurance components and classes defined in Part 3 of the Common Criteria (see part C of this report or [CC] Part 3 for details). The TOE meets the assurance requirements of assurance level EAL 5 (Evaluation Assurance Level 5 – semiformally designed and tested) augmented by ALC_DVS.2 (Life cycle support – Sufficiency of security measures), AVA_MSU.3 (Misuse – Analysis and testing for insecure states), and AVA_VLA.4 (Vulnerability analysis – Highly resistant).

1.3 Strength of Functions

The TOE's strength of functions is rated "high" (SOF-high). The strength of functions rating does not include cryptographic algorithms for encryption and decryption. For more details see also chapter 9 of this report.

1.4 Functionality

Except the functional requirements, FAU_SAS.1 (Audit storage), FCS_RND.1 (Quality metric for random numbers), FMT_LIM.1 (Limited capabilities), FMT_LIM.2 (Limited availability), and FPT_TST.2 (Subset TOE testing) the TOE security functional requirements were taken from CC part 2 (i. e. the set is CC part 2 extended) [CC]. They can be categorized into the following six functional classes:

1. security audit,
2. cryptographic support,
3. user data protection,
4. security management,
5. protection of the TOE security functions, and
6. resource utilisation.

[3] hereinafter called ST

Chapter 9 lists the security functional requirements in more detail. They are met by nine suitable TOE security functions (TSF):

TSF	Short Description
1. Operating state checking	Correct function of the SLE66CLX640P / SLE66CLX641P is only given in the specified range of the environmental operating parameters. To prevent an attack exploiting those circumstances it is necessary to detect if the specified range is left. All operating signals are filtered to prevent malfunction and the operating state is monitored with sensors for the operating voltage, clock signal frequency, temperature and electromagnetic radiation.
2. Phase management with test mode lock-out	During start-up of the SLE66CLX640P / SLE66CLX641P the decision for the user mode or the test mode is taken dependent on several phase identifiers. If test mode is the active phase the SLE66CLX640P / SLE66CLX641P requests authentication before any action (test mode lock-out). The phase management is used to provide separation between test mode and user mode as well as between security enforcing functions and user software.
3. Protection against snooping	Several mechanisms protect the SLE66CLX640P / SLE66CLX641P against snooping the design or the user data during operation and even if it is out of operation (power down).
4. Data encryption and data disguising	The memory contents of the SLE66CLX640P / SLE66CLX641P are encrypted on chip to protect against data analysis on stored data as well as on internally transmitted data. To prevent interpretation of leaked processed or transferred information, randomness is inserted in the information. In addition, important parts of the CPU and the complete DES component are especially designed to counter leakage attacks like DPA or EMA. The current consumption is independent of the processed data. In order to counter fault attacks in the RSA-calculation, redundant calculations are performed.
5. Random number generation	Random data is essential for cryptography as well as for physical security mechanisms. SLE66CLX640P / SLE66CLX641P is equipped with a true random generator based on physical probabilistic controlled effects. The random data can be used from the user software as well as from the security enforcing functions. It fulfils the requirements from the functionality class P2 of [AIS31].
6. TSF self test	The TSF of the SLE66CLX640P / SLE66CLX641P has either a hardware controlled self test which can be started from the user software by a RMS function call or can be tested directly from the user software for the active shield. The tested security enforcing functions are TSF 1, 5, and 7.
7. Notification of physical attack	The entire surface of the SLE66CLX640P / SLE66CLX641P is protected with the active shield. Attacks over the surface are detected when the shield lines are cut or get contact.

TSF	Short Description
8. Memory Management Unit (MMU)	The MMU in the SLE66CLX640P / SLE66CLX641P gives the user software the possibility to define different access rights for memory areas and components. In case of an access violation the MMU will generate a non maskable interrupt (NMI). Then an interrupt service routine (ISR) can react on the access violation.
9. Cryptographic support	The TOE is equipped with several hardware accelerators to support standard cryptographic operations. The components are a hardware DES encryption unit and a combination of software and hardware unit to support RSA cryptography and RSA key generation. The key for the cryptographic 3DES operations are provided from the user software (environment).

A more detailed description of the TOE security functions can be found in chapter 6 of the public ST, which is attached as part D of this certification report.

1.5 Summary of Threats and Organisational Security Policies (OSPs)

The primary assets for the TOE are user data, smartcard embedded software (program code), the correct operation of the TOE, and random numbers generated by the TOE. Secondary assets are logical and physical design data, IC Dedicated Software, initialization Data and pre-personalization Data, TSF data, specific development aids, test and characterizations related data, material for software development support, and photomasks as defined in section 3.1 of [PP0002].

Any human user or TOE external process acting on his behalf is regarded as an attacker.

All threats were taken over from [PP0002] and are based on the following three standard high-level security concerns:

- manipulation of user data and of the smartcard embedded software (while being executed/processed and while being stored in the TOE's memories),
- disclosure of user data and of the smartcard embedded software (while being processed and while being stored in the TOE's memories), and
- deficiency of random numbers.

The seven threats deal with:

- physical manipulation,
- physical probing,
- malfunction due to environmental stress,
- inherent information leakage,
- forced information leakage,

- abuse of functionality, and
- deficiency of Random Numbers.

One organisational security policy P.Process TOE from [PP0002] requires protection during TOE development and production and one additional OSP P.Add-Functions require:

- Area based Memory Access Control,
- Triple Data Encryption Standard (3DES), and
- Rivest-Shamir-Adleman (RSA)

as additional TOE functionality.

A more detailed description of the threats and organisational security policies can be found in sections 3.3 and 3.4 of [PP0002] and in sections 3.3 and 3.4 of the public ST, which is attached as part D of this certification report.

1.6 Special Configuration Requirements

The TOE is delivered in one fixed configuration. It has two different operating modes: *user mode* and *test mode*. The user software being executed on the TOE cannot use the *test mode*. The TOE is delivered as a hardware unit either at the end of the IC manufacturing process or at the end of IC packaging. At this point the operating system software is already stored in the non-volatile memories of the IC and *test mode* is disabled.

1.7 Assumptions about the Operating Environment

The life-cycle of the TOE is defined in the underlying protection profile [PP0002] which distinguishes three distinct development and manufacturing stages with 5 phases and two additional stages and corresponding phases:

1. development stage:
   - smartcard embedded software development (phase 1),
   - integrated circuit (hereafter “IC”) design, IC dedicated software development, integration and photomask fabrication (phase 2),
2. IC production stage:
   - IC manufacturing, testing, preparation and shipping to the IC assembly line (phase 3),
3. smartcard production stage:
   - smartcard IC packaging (and testing) (phase 4),
   - smartcard product finishing process, printing (and testing), smartcard preparation and shipping to the personalisation line (phase 5),

In addition, two important stages have to be considered in the smartcard life cycle:

- smartcard personalisation and testing stage where the user data is loaded into the smartcard's memory (phase 6),
- smartcard usage by its issuers and end-user (phase 7) which may include loading and other management of applications in the field.

The assumptions from section 3.2 of [PP0002]

- A.Process-Card,
- A.Plat-Appl, and
- A.Resp-Appl

are valid for this ST and concern phase 1 and phases from TOE delivery up to the end of phase 6. Furthermore, the additional assumption A.Key-Function was defined in ST. The description of all assumptions can be found in chapter 4.

1.8 Independence of the Certifier

Within the last two years, the certifier did not render any consulting- or other services for the company ordering the certification and there was no relationship between them that might have an influence on his assessment.

The certifier did not participate at any time in test procedures for the product, which forms the basis of the certification.

1.9 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 with regard to generation, configuration and operation as detailed in this certification report. This certificate is not an endorsement of the IT product by TÜV Informationstechnik GmbH or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Informationstechnik GmbH 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 the Smart Card IC (Security Controller) *SLE66CLX640P / m1523a11, SLE66CLX641P / m1522a11*. The delivered ICs contain the actual TOE (version m1523a11 or m1522a11) and the operating system. They are delivered either in form of wafers or in form of modules at end of phase 3 or at the end of phase 4, respectively. The delivery of the TOE to the customer (card manufacturer) is done in one of the following three allowed ways:

1. Personal pick-up at the sales warehouse in Regensburg (Germany) or Wuxi (China)
2. Secure transport by specific haulage companies *directly* to the customer
3. Secure transport by specific haulage companies to the customer via the distribution centers DC E (Europe) or DC A (Asia)

The delivered TOE contains the software parts of the TOE: STS (version 53.36.31), RMS (version 0.5), and RSA2048 library (version 1.30).

The following TOE deliverables are provided:

No	Type	Identifier	Release	Form of delivery
1	HW	**SLE66CLX640P / m1523a11** or:	GDS-file-ID: m1523a11 with production line indicator: "2" (Dresden)	Wafer or packaged module
		SLE66CLX641P / m1522a11	GDS-file-ID: m1522a11 with production line indicator: "2" (Dresden)	
2	SW	STS Self Test Software *(the IC Dedicated Test Software)*	V53.36.31	Stored in Test ROM on the IC
3	SW	RMS-E Resource Management System *(the IC Dedicated Support Software)*	V0.5	Stored in reserved area of User ROM on the IC
4	SW	RSA2048 library	V1.30	Source code in electronic form
5	DOC	Data Book – SLE 66CxxxP Security Controller Family	08.04	Hardcopy and pdf-file
6	DOC	Confidential Errata & Information Sheet – SLE 66CxxxP Products and Boundout	05.05	Hardcopy and pdf-file
7	DOC	Security & Chip Card ICs – SLE 66CxxxP – Instruction Set	05.01	Hardcopy and pdf-file
8	DOC	RSA 2048 bit Support - RSA Interface Specification for library V1.30	12.2004	Hardcopy and pdf-file
9	DOC	RSA 2048 bit Support – Arithmetic Library for V1.30	12.2004	Hardcopy and pdf-file
10	DOC	Application Notes [Appl_N]		Hardcopy and pdf-file

Table 1: Deliverables of the TOE

The hardware part of the TOE is identified by *SLE66CLX640P / m1523a11* and *SLE66CLX641P / m1522a11* resp. and is indicated as a chip type identifier in the EEPROM (chip type 8Ah for 640P and 89h for 641P). It is produced in Dresden, indicated by the production line number '2' within the chip identification number in the EEPROM. The firmware parts *RMS* and *STS* (required for the operation of the chip) and the separate software part *RSA2048 library* are identified by their unique version numbers. The STS version number can be obtained from three additional control bytes of the chip identification number. The RMS is part of the ROM mask. The version number can be obtained from the ROM type bytes using the data base system at Infineon Logistic Department.

The chip type byte identifies different versions in the following manner: 8Ah for versions m1523a1(x); 89h for versions m1522a1(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.

TOE documentation is delivered either as hardcopy or as softcopy (encrypted) according to defined mailing procedures. The software components RMS and RSA2048 library are sent encrypted to the Smartcard Embedded Software Developer in phase 1 of the life-cycle.

For RMS and STS, defined procedures at the development and production sites guarantee that the right versions are implemented into the TOE ICs.

3 Security Policy

Within the security target two security policies are defined:

Policy Name	Description
Memory Access Control Policy	The TOE shall control read, write, delete, execute accesses of software running at two different modes (system mode active during interrupt execution or application mode active during other executing) on data and code stored in memory areas.
Data Processing Policy	User data and TSF data shall not be accessible from the TOE except when the smartcard embedded software decides to communicate the user data via an external interface. The protection shall be applied to confidential data only but without the distinction of attributes controlled by the smartcard embedded software.

A more detailed description of the security policies can be found in section 5.1.1 of [PP0002] and section 5.1.1.2 of the public ST, which is attached as part D of this certification report.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The only assumptions defined in the ST are assumptions about the environment of use (see following section). There is no usage assumption defined in the ST.

4.2 Environmental Assumptions

The following four assumptions about the environment of use are defined in the ST and must be regarded when using the TOE.

Assumption	Description
A.Process-Card	Protection during Packaging, Finishing and Personalisation 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).
A.Plat-Appl	Usage of Hardware Platform The smartcard embedded software is designed so that the requirements from the following documents are met: (i) TOE guidance documents (refer to the Common Criteria assurance class AGD) such as the hardware data sheet, and the hardware application notes, and (ii) findings of the TOE evaluation reports relevant for the smartcard embedded software.
A.Resp-Appl	Treatment of User Data All user data are owned by smartcard embedded software. Therefore, it must be assumed that security relevant user data (especially cryptographic keys) are treated by the smartcard embedded software as defined for the specific application context.
A.Key-Function	Usage of Key-dependent Functions Key-dependent functions (if any) shall be implemented in the smartcard embedded software in a way that they are not susceptible to leakage attacks (as described under threats T.Leak Inherent and T.Leak Forced).

4.3 Clarification of Scope

The smartcard operating system and the application software stored in user ROM and in EEPROM are not part of the TOE. The certification is only valid for TOE chips produced in Dresden (production line indicator: “2”).

5 Architectural Information

The TOE can be divided into 6 hardware components illustrated in figure 1 above and indicated in the following table:

name	description
Input logic (INP)	manages input data, contains the UART-controlled I/O interface and a PLL unit to allow a multiplication factor between the external and internal clock frequencies
Security logic (SEC)	manages security relevant events
Central Processing Unit (CPU)	Microcontroller type ECO 2000 with the subcomponents memory encryption and decryption unit (MED), memory management unit (MMU) and 256 bytes of internal RAM (IRAM)
External memory	comprising of: - 4 kBytes extended RAM (XRAM) - 136 kBytes user ROM, including the routines for chip management (RMS) - 8 KB test ROM containing the test routines (STS), and - a total of 64 kBytes non-volatile memory (EEPROM)
Random number generator (RNG)	provides true random numbers
Checksum module (CRC)	calculates checksums
Interrupt module (INT)	manages interrupts
Timer (TIM)	responsible for timing
Advanced Crypto Engine (ACE)	Provides long integer modulo calculations used in asymmetric algorithms like RSA
DES accelerator (DDC)	provides fast calculations of DES and EC2 support.
Address and data bus (BUS)	connects different components

and three additional software/firmware components:

name	description
IC dedicated test software (STS)	consists of test and initialization routines (Self Test Software)
IC dedicated support software (RMS)	used for EEPROM programming and security functions testing (Resource Management System)

name	description
RSA2048 library	Functions for generating RSA key pairs, RSA en-/decryption, RSA signature verification/generation, and RSA modulus calculation

6 Documentation

The following documentation is provided with the product by the developer to the consumer as indicated in table 1 above:

- Data Book – SLE 66CxxxP Security Controller Family, release 08.04
- Confidential Errata & Information Sheet – SLE 66CxxxP Products and Boundout, release 05.05
- Security and Chip Card ICs – SLE66CxxxP – Instruction Set, release 05.01
- Security & Chip Card ICs – SLE 66CxxxP – Instruction Set, release 12.2004
- RSA 2048 bit Support – RSA Interface Specification for library V1.30, release 12.2004
- Application Notes [Appl_N]

7 IT Product Testing

The developer tested the TOE Security Functions (TSF) systematically against the Functional Specification (FSP), the High-Level Design (HLD), and the Low-Level Design (LLD) with the result that all TSF behave as specified. The developer's tests can be divided into six categories:

1. analog and digital simulation tests which results are used in further tests,
2. qualification tests after the first production with a new mask,
3. verification tests for each mask version to decide whether the TOE is released to production,
4. security evaluation tests to check security mechanism and functionality,
5. chip production tests on every chip before delivery, and
6. layout tests for the optical verification of parts of the implementation.

The evaluation body repeated the tests of the developer for all TSF and security mechanism and performed independent penetration testing. The testing confirmed that all obvious vulnerabilities were considered and that the TOE does not feature any exploitable

vulnerability within the intended operational environment with respect to attackers possessing high attack potential, if all the measures required are taken into consideration.

8 Evaluated Configuration

The TOE *SLE66CLX640P / m1523a11, SLE66CLX641P / m1522a11* is delivered in one fixed configuration (either *SLE66CLX640P / m1523a11 or SLE66CLX641P / m1522a11* resp.) and no further generation takes place. Therefore, the evaluated configuration is identical to the TOE, which can be identified as described in chapter 2 of this certification report.

9 Results of the Evaluation

The Evaluation Technical Report [ETR] was provided by TÜViT's evaluation body according to the requirements of the Scheme, the Common Criteria [CC], the Methodology [CEM] and the Application Notes and Interpretations of the Scheme [AIS]. Especially, the following Application Notes and Interpretations of the Scheme were used in the present certification:

- [AIS 25], [AIS 26], and [AIS 36] for smart card IC specific methodology,
- [AIS 31] for the assessment of the random number generator, and
- [AIS 34] for assurance components beyond EAL4.

The verdicts for the CC, part 3 assurance classes and components (according to EAL5 augmented by ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4 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
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	ATE_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 of insecure states	AVA_MSU.3	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Highly resistant	AVA_VLA.4	PASS

All assurance components were assessed with the verdict PASS. This includes that all evaluator action elements being part of the assurance components are also assessed with PASS. Therefore, the TOE as defined in the security target is considered to be Part 3 conformant.

Section 5.1 of the public ST, which is attached as part D of this certification report, lists the following TOE security functional requirements.

ID	**Class**/Component	**Source**
FAU	**Security audit**	
FAU_SAS.1	*Audit Storage*	[PP0002]
FCS	**Cryptographic support**	
FCS_COP.1	Subset access control	added in ST
FCS_CKM.1	Cryptographic key generation	added in ST
FCS_RND.1	*Quality metric for random numbers*	[PP0002]
FDP	**User data protection**	
FDP_ACC.1	Subset access control	added in ST
FDP_ACF.1	Security attribute based access control	added in ST
FDP_IFC.1	Subset information flow control	[PP0002]

ID	**Class**/Component	**Source**
FDP_ITT.1	Basic internal transfer protection	[PP0002]
FDP_SDI.1	Stored data integrity monitoring	added in ST
FMT	**Security management**	
FMT_LIM.1	*Limited capabilities*	[PP0002]
FMT_LIM.2	*Limited availability*	[PP0002]
FMT_MSA.1	Management of security attributes	added in ST
FMT_MSA.3	Static attribute initialisation	added in ST
FMT_SMF.1	Specification of management functions	added in ST
FPT	**Protection of TOE Security Functions**	
FPT_FLS.1	Failure with preservation of secure state	[PP0002]
FPT_ITT.1	Basic internal TSF data transfer protection	[PP0002]
FPT_PHP.3	Resistance to physical attack	[PP0002]
FPT_SEP.1	TSF domain separation	[PP0002]
FPT_TST.2	*Subset TOE testing*	added in ST
FRU	**Resource utilisation**	
FRU_FLT.2	Limited fault tolerances	[PP0002]

Apart from *FAU_SAS.1*, *FCS_RND.1*, *FMT_LIM.1*, *FMT_LIM.2*, and *FPT_TST.2* (marked in italics in the table above) the security functional requirements were taken from [CC] part 2, i. e. the TOE is [CC] part 2 extended.

The TOE is conformant to the Smartcard IC Platform Protection Profile [PP0002].

The evaluation performed in accordance to EAL5 augmented by ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4 has shown that the TOE security functional requirements are correctly realised by the TOE security functions. Thus, in realising these functional requirements, it is assured that the TOE will meet the security objectives claimed in the ST.

TSF 2 (Phase management with test mode lock-out), TSF 3 (Protection against snooping), TSF 4 (Data encryption and data disguising), and TSF 5 (Random number generation) fulfil the SOF-rating high (SOF-high). The strength of function rating for the RNG was performed according to [AIS 31]. The strength of functions rating does not include cryptographic algorithms for encryption and decryption, like 3DES and RSA in TSF 9 (cryptographic support).

The sponsor must advise the certification authority about any modification of the TOE or its guidance documentation. The certification authority will then check whether the certification results are still valid and, if necessary, initiate all further steps concerning a re-evaluation. The results of the evaluation are only applicable to the product "*SLE66CLX640P / m1523a11, SLE66CLX641P / m1522a11*". 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 of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

9.1 Additional evaluation results for a subsequent composite evaluation

The evaluation confirmed the following results regarding the development and production environment. The Common Criteria assurance requirements:

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

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

- Infineon Technologies AG, Königsbrücker Straße 180, 01099 Dresden, Germany (semiconductor factory)
- Infineon Technologies AG, St.-Martin-Straße 76, 81541 München, Germany (development center)
- Infineon Technologies AG, Leibnizstraße 6, 93055 Regensburg, Germany (IC packaging into modules and warehouse and delivery center)
- Infineon Technologies AG, Development Center Graz, Babenbergerstraße 10, 8020 Graz, Austria (development center)
- Du Pont Photomasks France S.A., 224, bd John Kennedy, F-91105 Corbeil Essonnes, France (mask center)
- Infineon Technologies AG, Alter Postweg 101, 86159 Augsburg, Germany (development center)
- Infineon Technologies Asian Pacific, Exel Singapure Pte. Ltd, 81 ALPS Avenue, Exel Supply Chain Hub, Singapore 498803 (distribution center)
- Infineon Technologies (Wuxi) Co. Ltd., No. 118, Xing Chuang San Lu, Wuxi-Singapore Industrial Park, Wuxi 214028, Jiangsu, P.R. China (module mounting)

For all sites listed above, the requirements have been specifically applied in accordance with the Security Target "*SLE66CLX640P / m1523-a11, SLE66CLX641P / m1522-a11, Both with RSA2048 V1.3* – Security Target", Version 1.2, as of 2005-06-03 [ST]. The evaluators verified, that the threats are countered and the security objectives for the life cycle phases 2, 3, and 4 up to the delivery at the end of phase 3 or 4 as state in [ST] are fulfilled by the procedures of these sites.

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. These results are documented in the evaluation report [ETR-lite] according to

[AIS 36]. Therefore, the interface between the smart card embedded software developer and the developer of the TOE was examined in detail. These composition related action comprised the following tasks:

- Examination of the integration of the embedded software in the configuration management system of the IC manufacturer for the TOE. This comprises the handling of the ROM-code, the related acceptance and verification procedures with the customer and the assignment to a unique commercial type identifier as well as the handling of different ROM-code masks for the same smart card IC.
- Examination of consistency of delivery and pre-personalisation procedures. This comprises the handling of (specific delivery procedures) and pre-personalisation data with respect to the physical, technical and organisational measures to protect these data as well as the procedures to ensure the correct configuration of the TOE. In addition, the production test related to customer specific items including the integrity check of the customer ROM-code and the personalisation process were checked.
- Examination of the separation based on the unique commercial type identifier and the related test and delivery procedures.
- Examination, that (the hardware manufacturer) has implemented procedures to provide a customer product related configuration list based on the general configuration list provided for evaluation of the TOE supplemented by the customer specific items including ROM-mask labeling, specific development tools for embedded software development and related customer specific deliveries and the corresponding verification data generated by (the hardware manufacturer) to be sent to customer. In the course of the TOE evaluation a specific customer product related configuration list was checked.
- Examination of aspects relevant for the user guidance documentation of the TOE to use the TOE for a product composition.
- Examination of a list of TOE security mechanisms including a rating to be used within a composite product vulnerability assessment.

10 Evaluation Stipulations, Comments, and Recommendations

The Evaluation Technical Report [ETR] contains the following stipulation:

1. The following assumptions and requirements concerning external security measures have to be considered:
   - All security hints described in [DB] and the delivered application notes [Appl_N] have to be considered.
   - As the TOE is under control of the user software, the chip manufacturer can only guarantee the integrity up to the delivery procedure. It is in the responsibility of the Smartcard Embedded Software Developer to include mechanisms in the implemented software which allows detection of modifications after the delivery.
   - The Smartcard Embedded Software Developer should not accept deliverables from Infineon he had not requested. All confidential information sent in electronic form has to be accepted only in encrypted form.
   - In the environment the following assumption has to be fulfilled (see [ST]):
     - "Protection during packaging, finishing and personalisation" resulting from A.Process-Card (*It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end-user to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use). This means that the Phases after TOE Delivery (refer to Sections 2.1 and 8.1) 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 following functional requirements of the environment defined in [ST] have to be taken into consideration from the Smartcard Embedded Software Developer:
     - "Cryptographic key generation" resulting from FCS_CKM.1 (for 3DES and optional for RSA), or "Import of user data without security attributes" resulting from FDP_ITC.1 (for 3DES and RSA), or "Import of user data with security attributes" resulting from FDP_ITC.2 (for 3DES and RSA),
     - "Cryptographic key destruction" resulting from FCS_CKM.4 (for 3DES and RSA), and
     - "Secure security attributes" resulting from FMT_MSA.2 (for 3DES and RSA).

- During an evaluation of the Smartcard Embedded Software the correct configuration of the following parameters has to be checked:
  - Wait states functionality is activated for all operations of the Embedded Software critical for side channel attacks (e.g. SPA/DPA),
  - CURSE functionality is activated for all operations of the Embedded Software critical for side channel attacks (e.g. SPA/DPA),
  - parameters for memory encryption E0ADR, E2ADR and XKEY which configure the ranges of encryption,
  - if the SW comparison of random numbers to/with regard to the active shielding is correctly implemented (in case it is implemented [App_Shield]),
  - MMU is configured correctly,
  - calls of the self test of the TSF implemented in the RMS routines to detect failures of the sensors are implemented. Depending on the application (e. g. time between possible resets) the developer of the Smartcard Embedded Software has to decide how often this function has to be executed during normal operation. The self-test shall be executed at least once during security relevant operation (e. g. key generation).
  - call of the test of the random number generation to detect failures of the RNG is implemented (see below).
- According to section 16.3.5 of the databook [DB] the user of the TOE (the Smartcard Embedded Software Developer) must perform the online test via the RMS function SleRngAIS 31AnalogTest at start-up or at least before using the RNG for security relevant operation. As this is not sufficient, the Smartcard Embedded Software Developer has to follow the following advice:

  A RNG live test (one call of SleRngAIS 31AnalogTest) 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 recommended that latest before any operation is executed which shall be protected by chip internal randomisation mechanisms (CURSE, Random Waite States, Bus Confusion), the RNG live test is executed [App_RNG].
- 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 functionalities 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 of the encryption. In chapter 19 of [DB] 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 to him in detail how to use effectively the security mechanisms made available by the TOE.

- In case an alarm is triggered, the contents of the XRAM are not being deleted. In order to prevent an attacker from reading out this data, the user operating system has to delete explicitly the XRAM after each reset. This fact is pointed out to the operating system developer in chapter 7 of [DB].
- The delivered MMU is set thus, that SLE66CLX640P / m1523a11, SLE66CLX641P / m1522a11 are compatible with SLECX160S, i. e. all ROM areas are mapped. Since the MOVC blockade of the SLE66CX160S is no longer implemented, in this setting reading out of the ROM by a program in the EEPROM is possible. In order to avoid this, the operating system developer has to program the MMU in a way that reading out is impossible. This fact is pointed out in the chapter 19 of [DB].
- ROM contents of chips, being drawn up with the same mask, are identically encrypted. This leads to the possibility of the attacker to carry out attacks on the ROM at as many patterns as he likes. Independent of the rating of the strength of mechanisms, preventing such attacks, 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 an application note [Appl_MED].
- The TOE has implemented a hardware DES accelerator. In case the keys necessary for the calculation of the DES are transferred unencrypted into the DES accelerator, these keys could be spied out by means of a SPA/DPA. In order to prevent this, the transfer of the keys has to be protected using the measures described in [Appl_DES].
- 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 change the current pattern. [Appl_Shield] describes to him how to realise this. Moreover it is recommended to change the current pattern before any security critical operation and to compare the returned values with the expected values accordingly frequently with regard to the software.
- The TOE is protected by light sensors against DFA light attacks (e. g. with laser). Nevertheless the performed penetration tests show that it is still possible to manipulate a running program with a focussed laser. 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 [App_Sec]. 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 [App_DES].

11 Certification Stipulations and Notes

The stipulation of the evaluation report (see chapter 10) is applicable. There are no additional notes or stipulations resulting from the certification report.

12 Security Target

The security target [ST] for the Smart Card IC (Security Controller) *SLE66CLX640P / m1523a11, SLE66CLX641P / m1522a11* is included in part D of this certification report.

13 Definitions

13.1 Acronyms

ADM	Administrator Guidance
CC	Common Criteria for Information Technology Security Evaluation (referenced to as [CC])
CEM	Common Methodology for Information Technology Security Evaluation (referenced to as [CEM])
CM	Configuration Management
CMOS	Complementary Metal-Oxide Semiconductor
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
DDC	DES accelerator
DOC	Documentation
DPA	Differential Power Analysis
EAL	Evaluation Assurance Level
EEPROM	Electrical Erasable and Programmable Read Only Memory
FSP	Functional Specification
HLD	High-level Design
HW	Hardware
IC	Integrated Circuit
IF	Interface
IGS	Installation, Generation and Start-up
IRAM	Internal Random Access Memory
MED	Memory Encryption and Decryption Unit
MMU	Memory Management Unit
OSP	Organisational Security Policy
PLL	Phase Lock Loop
PP	Protection Profile
PROM	Programmable Read Only Memory
RAM	Random Access Memory
RMS	Resource Management System
RNG	Random Number Generator
ROM	Read Only Memory
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SIF	Sub-interface

SOF	Strength of Function
SPA	Simple Power Analysis
SS	Sub-system
ST	Security Target
STS	Self Test Software
SW	Software
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Function Interfaces
TSP	TOE Security Policy
UART	Universal Asynchronous Receiver Transmitter
USR	User Guidance
VLA	Vulnerability Analysis
XRAM	Extended Random Access Memory

13.2 Glossary

Augmentation – The addition of one or more assurance component(s) from 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

[AIS] Application Notes and Interpretations of the Scheme (AIS), published by BSI

[AIS 25] AIS 25, Version 2, as of 2002-07-29 including the CC supporting document: “The Application of CC to Integrated Circuits”, Version 1.2, 07’2002

[AIS 26] AIS 26, Version 2, as of 2002-08-06 including the CC supporting document: “Application of Attack Potential to Smartcards”, Version 1.1, 07’2002

[AIS 31] AIS 31, Version 1, 2001-09-25 “Functionality classes and evaluation methodology for physical random number generators”

[AIS 34] AIS 34, Version 1.00, 2004-06-01 “Evaluation Methodology for CC Assurance Classes for EAL5+”

[AIS 36] AIS 36, Version 1, as of 2002-07-29 including the CC supporting documents: “ETR-lite for Composition”, Version 1.1, 07’2002 and “ETR-lite for composition: Annex A Composite smartcard evaluation : Recommended best practice”, Version 1.2, 03’2002

[Appl_N] comprises the following application notes from Infineon Technologies AG:

- *Application Note, SLE66CLxxxP - Anticollision Type A, version 03.03*
- *Application Note, SLE66CLxxxP - Anticollision Type B, version 03.03*
- *Application Note, SLE66CLxxxP - Card Coil Design Guide, version 05.05*
- *Application Note, SLE66CLxxxP - Contactless Protocol, version 03.03*
- *Application Note, SLE 66CxxxP, Using the CRC, version 03.01*
- *Application Note, SLE 66CxxxP, Infineon Chipcard Crypto API, version 05.02*
- **[Appl_DES]** *Application Note, SLE 66CxxxP, DDES - EC2*, version 02.04
- **[Appl_MED]** *Application Note, SLE66CxxxP/SLE66CxxxPE, Memory Encryption Decryption*, version 11.04
- *Application Note, SLE 66CxxxP, MMU-Memory Management Unit*, version 08.00
- *Application Note, SLE 66CxxxP, MMU Security Issues*, version 01.02
- *Application Note, SLE 66CxxxP, Optimized CL-Energy performance, version 06.05*
- *Application Note, PLL Fast Switch*, version 03.03
- *Application Note, SLE 66CxxxP, RF Interface Porting from SLE66CL160S, version 03.03*
- **[Appl_RNG]** *Application Note, SLE 66CxxxP, Testing the Random Number Generator*, version 11.04
- *Application Note, SLE 66CxxxP/PE, Using RNG a.t. FIPS140, version 02.04*
- **[Appl_SEC]** *Application Note, SLE 44CxxxS, SLE 11/22/66CxxxS, SLE 66CxxxP Security Advice concerning Program Flow Manipulation*, version 10.00
- *Application Note, SLE 66CxxxS, Secure Hash Algorithm SHA-1*, version 01.98
- **[Appl_Shield]** *Application Note, SLE 66CxxxP, Using the Active Shield security feature*, version 01.02
- *Application Note, DES – software version, version 09.97*
- *Application Note, SLE 66CxxxP, Transfer of a ROM Mask from SLE 66CxxS*, version 06.01
- *Application Note, SLE 66CxxxP, UART*, version 10.03

[CC] Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004,
Part 1: Introduction and general model
Part 2: Security functional requirements
Part 3: Security assurance requirements

[CEM] Common Methodology for Information Technology Security Evaluation,
Part 1: Introduction and general model, version 0.6, revision 11.01.1997,
Part 2: Evaluation Methodology, Version 2.2, January 2004

[DB] Data Book - SLE 66CxxxP Security Controller Family, release 08.04 and Confidential Errata & Information Sheet - SLE 66CxxxP Products and Boundout, release 05.05

[ETR] Evaluation Technical Report, TÜV Informationstechnik GmbH,
version 1, 2005-07-22, document-number: 20676378_TÜViT_041.01

[ETR-lite] ETR-LITE FOR COMPOSITION (ETR-LITE), TÜV Informationstechnik GmbH,
version 1, 2005-07-22, document-number: 20676378_TÜViT_037.01

[PP0002] Smartcard IC Platform Protection Profile, Version 1.0, July 2001
(certified on 2001-07-11 by BSI under certification ID: BSI-PP-0002-2001)

[ST] SLE66CLX640P / m1523-a11, SLE66CLX641P / m1522-a11, Both with RSA2048 V1.3 – Security Target, Version 1.2, 2005-06-03

Part C

Excerpts from the Criteria

The excerpts from the criteria are dealing with

- conformance results
- assurance categorization
- evaluation assurance levels
- strength of security function
- vulnerability analysis

CC Part 1:

Conformance results (section 5.4 of CC part 1 with 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 predefined 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.“

CC Part 3:

Assurance categorisation

The assurance classes, families, and the abbreviation for each family are shown in *Table 2*.

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: 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

„Table 3 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 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 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_IMT					**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 3: Evaluation assurance level summary

Evaluation assurance level 1 (EAL1) - functionally tested

“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

“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

“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

“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

“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

“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

“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)

AVA_SOF Strength of TOE security functions

“Strength of function analysis addresses TOE security functions that are realised by a probabilistic or permutational mechanism (e.g. a password or hash function). Even if such functions cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat them by direct attack. A level or a specific metric may be claimed for the strength of each of these functions. Strength of function analysis is performed to determine whether such functions meet or exceed the claim. For example, strength of function analysis of a password mechanism can demonstrate that the password function meets the strength claim by showing that the password space is sufficiently large.”

Three levels exist: SOF-basic, SOF-medium, and SOF-high.

Vulnerability analysis (AVA_VLA)

AVA_VLA Vulnerability analysis

"Vulnerability analysis consists of the identification of flaws potentially introduced in the different refinement steps of the development. It results in the definition of penetration tests through the collection of the necessary information concerning: (1) the completeness of the TSF (does the TSF counter all the postulated threats?) and (2) the dependencies between all security functions. These potential vulnerabilities are assessed through penetration testing to determine whether they could, in practice, be exploitable to compromise the security of the TOE."

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.

The intent of the developer analysis is to confirm that no identified security vulnerabilities can be exploited in the intended environment for the TOE and that the TOE is resistant to obvious penetration attacks.

Obvious vulnerabilities are considered to be those that are open to exploitation that requires a minimum of understanding of the TOE, skill, technical sophistication, and resources. These might be suggested by the TSF interface description. Obvious vulnerabilities include those in the public domain, details of which should be known to a developer or available from an evaluation authority.

Performing a search for vulnerabilities in a systematic way requires that the developer identify those vulnerabilities in a structured and repeatable way, as opposed to identifying them in an ad-hoc fashion. The associated evidence that the search for vulnerabilities was systematic should include identification of all TOE documentation upon which the search for flaws was based.

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. To accomplish this intent, the evaluator first assesses the exploitability of all identified vulnerabilities. This is accomplished by conducting penetration testing. The evaluator

should assume the role of an attacker with a low (for AVA_VLA.2), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential when attempting to penetrate the TOE. Any exploitation of vulnerabilities by such an attacker should be considered by the evaluator to be “obvious penetration attacks” (with respect to the AVA_VLA.*.2C elements) in the context of the components AVA_VLA.2 through AVA_VLA.4.”

Part D

Security Target

Attached is the Security Target *SLE66CLX640P / m1523-a11, SLE66CLX641P / m1522-a11, Both with RSA2048 V1.3 – Security Target*

Author: Infineon Technologies AG

Date: 2005-06-03

Version: 1.2

Public

Infineon Technologies AG
Security and Chipcard ICs

Evaluation Documentation

SLE66CLX640P / m1523-a11
SLE66CLX641P / m1522-a11
Both with
RSA2048 V1.3

Security Target

Version **1.2**
Date **2005-06-03**
Author **H.-J. Novinsky, H.-U. Buchmüller**

Filename: **SLE66CLX640P+CLX641P_SecurityTarget_1.2.doc**

TABLE OF CONTENTS

List of figures:

List of tables:

1 Introduction

1.1 Security Target Identification

The Security Target has the revision 1.2 and is dated 2005-06-03.

The Security Target is based on the Protection Profile “Smartcard IC Platform Protection Profile”.

The Protection Profile and the Security Target are built with Common Criteria V2.1. The ST takes into account all relevant current final interpretations.

Table 1: Identification

	Version number	Date	Registration
Smartcard IC Platform Protection Profile	1.0	July 2001	BSI-PP-0002
Common Criteria	2.1	August 1999	ISO15408

1.2 Security Target Overview

The Target of Evaluation (TOE), comprise two smart card ICs (Security Controllers) meeting the highest requirements in terms of performance and security. Both are manufactured by Infineon Technology AG in a 0.22 µm CMOS technology. The products are intended to be used in smart cards for particularly security-relevant applications.

The TOE includes a crypto library RSA2048 and a RMS library which provide some functionality via an API to the Smartcard Embedded Software and STS firmware for test purpose (see chapter 2.2.2).

Table 2: TOE identification

Name	Version number	Design Status	Firmware RMS Lib	Firmware STS	Software RSA Lib
SLE66CLX640P	m1523	a11	RMS_E V05	53.36.31	1.3
SLE66CLX641P	m1522	a11	RMS_E V05	53.36.31	1.3

The listed RSA2048 and RMS libraries are implemented together with the Smartcard Embedded Software in the User-ROM mask. The Smartcard Embedded Software is not part of the TOE.

The STS is implemented in a separated test-ROM part of the TOE.

Both products are identically from hardware perspective. The difference is in the mounting step only. Regarding the SLE66CLX641P the ISO7816 pads have not been contacted, thus this chip is for contactless use only, whereas the SLE66CLX640P provides both interface types and is for dual use therefore. Both types can be distinguished by a different chip ident. The difference in the mounting step does not influence the security of the TOE as neither an asset nor a security enforcing function is affected. Therefore both products are evaluated together.

The main security features implemented in the SLE66CLX640P / m1523-a11 and SLE66CLX641P / m1522-a11 are:

- a SAB 8051 compatible instruction set and some additional powerful instructions needed for smart card applications,

- data encryption according to single-DES and 3DES standard (single DES is out of scope of the evaluation),
- data encryption according to RSA standard with 512 to 2048 bits key length (key length below 1024 bit are out of scope of the evaluation),
- security sensors and physical countermeasures (e.g. shielding),
- true random number generation (AIS31 compliant),
- control of access rights to the memory by the memory management unit (MMU),
- access to the memory via the integrated Memory Encryption and Decryption (MED),
- countermeasures against SPA, DPA, EMA, and DFA attacks.

In this security target the TOE (target of evaluation) is described and a summary specification is given. The security environment of the TOE during its different phases of the lifecycle is defined. The assets are identified which have to be protected through the security policy. The threats against these assets are described. The security objectives as the objectives of the security policy are defined as well as the security requirements. The requirements are built up of the security functional requirements as part of the security policy and the security assurance requirements as the steps during the evaluation and certification to show the TOE meets its requirements. The functionality of the TOE to meet the requirements is described.

The assets, threats, security objectives and the security functional requirements are defined in the Smartcard IC Platform Protection Profile and are referenced here. These requirements build up a minimal standard common for all Smartcards.

The security enforcing functions are defined here in the security target as property of this specific TOE. Here it is shown how this specific TOE fulfils the requirements for the standard defined in the Protection Profile.

1.3 CC Conformance

This security target is conformant to Common Criteria V2.1 (ISO15408) part 2 extended, part 3 conformant and conformant to the Smartcard IC Platform Protection Profile. The assurance level is EAL5 augmented with components ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4.

The security requirements of the TOE according to the Smartcard IC Platform Protection Profile are listed in Table 9. The augmented security functional requirements (see Table 10) are listed and described in section 5.1.

2 Description of the Target of Evaluation (TOE)

The TOE description helps to understand the specific security environment and the security policy. In this context the assets, threats, security objectives and security functional requirements can be employed. The following is a more detailed description of the TOE than in the Smartcard IC Platform Protection Profile as it belongs to the specific TOE.

2.1 Product Type

The Target of Evaluation (TOE), the SLE66CLX640P / m1523-a11 and SLE66CLX641P / m1522-a11, is a smart card IC (Security Controller) meeting the highest requirements in terms of performance and security. It is manufactured by Infineon Technologies AG in a 0.22 µm CMOS technology. The IC is intended to be used in smart cards for particularly security-relevant applications. That is based on its previous use as developing platform for smart card operating systems according to the lifecycle model (in Smartcard IC Platform Protection Profile).

The term Smartcard Embedded Software is used in the following for all operating systems and applications stored and executed on the TOE. The TOE is the platform for the Smartcard Embedded Software. The Smartcard Embedded Software itself is not part of the TOE.

The TOE products are variants of the SLE66CX322P architecture. The distinguishing feature is the additional contactless interface. Apart from this addition most components are unchanged.

The IC, whose block diagram is shown in Figure 1, consists of a dedicated microprocessor (CPU) with a MMU (Memory Management Unit), several different memories, security logic, a timer and an interrupt-controlled I/O interface. A RNG (**R**andom **N**umber **G**enerator) and a checksum module (CRC module) are integrated on the chip. In addition the TOE is equipped with a RF interface (radio frequency power and signal interface) that enables contactless communication between a PICC (proximity integrated chip card, PICC) and a reader/writer (proximity coupling device, PCD).

The CPU is compatible with the SAB 8051 instruction set and is 6 times faster than the standard processor. It provides additional powerful instructions for smart card applications. The memory comprises 256 bytes of internal RAM (IRAM), 4 kBytes of extended RAM (XRAM), 136 kBytes of user ROM, 8 kByte of test ROM and 64 kByte of EEPROM. It thus meets the requirements of the new generation of operating systems. The CPU accesses the memory via the integrated **M**emory **E**ncryption and **D**ecryption unit (MED). The access rights of the application to the memories can be controlled with the memory management unit (MMU). Security, sleep mode and interrupt logic as well as the RNG are specially designed for smart card applications. The sleep mode logic (clock stop mode per ISO/IEC 7816-3) is used to reduce the overall power consumption. The timer permits easy implementation of communication protocols such as T=1 and all other time-critical operations. The UART-controlled I/O interface allows the smart card and terminal to be operated in parallel. The PLL unit allows operating the SLE66CLX640P / m1523-a11 and SLE66CLX641P / m1522-a11 with a multiplication factor over the external clock signal or free running with maximum frequency. The RNG does not supply a pseudorandom number sequence, but instead produces genuine random numbers under all conditions. The checksum module allows simple calculation of checksums per ISO 3309 (16 bit CRC).

Two modules for cryptographic operations are implemented on the TOE. The well known ACE (Advanced Crypto Engine) for calculation of asymmetric algorithms like RSA and elliptic curve (EC). This module is especially designed for chip card application with respect to the security and power consumption. The other module is the DDC which provides the DES algorithm and support for elliptic curve (EC) cryptography. This module computes the complete DES algorithm within a few clock cycles. That module is especially designed to counter attacks like DPA or EMA. The SLE66CLX640P / m1523-a11 and SLE66CLX641P / m1522-a11 include functionality to calculate single DES operations. The evaluation includes the triple-DES operation only.

The software (firmware) required for operating the chip consists of routines for programming the EEPROM from application programs and for online testing of the security enforcing functions.

These are stored in a reserved user ROM area. In addition, the chip initialisation routine with security checks and identification mode as well as test routines for production testing are located in a separate test ROM.

The TOE offers a new, improved standard of integrated security features, thereby meeting the requirements of all smart card applications such as information integrity, access control, mobile telephone, as well as uses in electronic funds transfer and healthcare systems.

To sum up, the TOE is a powerful smart card IC with a large amount of memory and special peripheral devices with both improved performance and optimised power consumption at minimal chip size. It therefore constitutes the basis for future smart card applications.

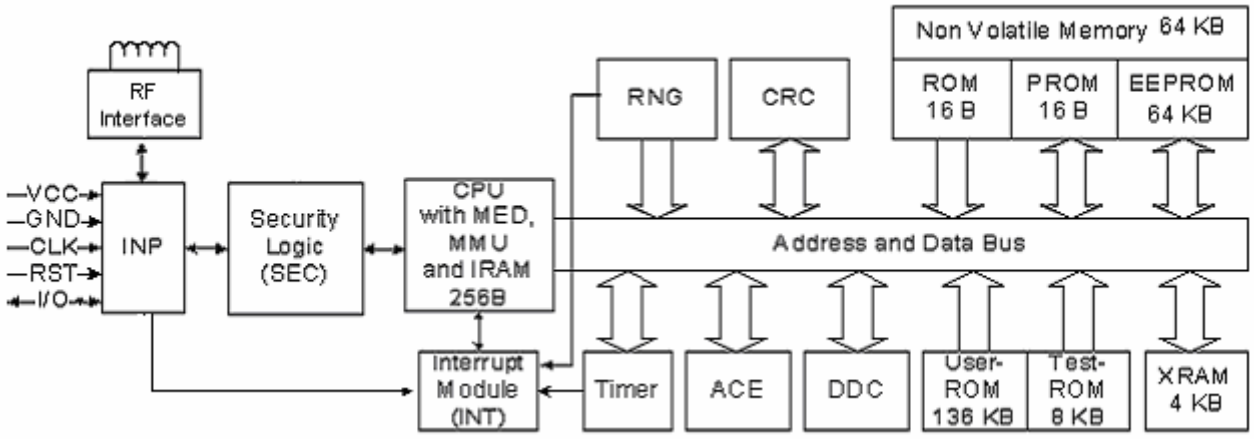


Figure 1: Block diagram of the SLE66CLX640P and SLE66CLX641P

2.2 Scope of the TOE

The TOE comprises the *hardware* of two smart card security controllers, SLE66CLX640P / m1523-a11 and SLE66CLX641P / m1522-a11, manufactured by Infineon Technologies AG, and part of the associated *firmware*/*software* required for operation. The documents described in section 2.2.3 and listed in Annex 9.1 are supplied as a manual. In the following description, the term “manufacturer” is short for Infineon Technologies AG, the manufacturer of the TOE. The Smartcard Embedded Software is not part of the TOE.

2.2.1 Hardware of the TOE

The *hardware part* of the TOE (see Figure 1) as defined in Smartcard IC Platform Protection Profile is comprised of:

- Security logic (SEC)
- Microcontroller type ECO 2000 (CPU) with the subcomponents memory encryption and decryption unit (MED), memory management unit (MMU) and 256 bytes of internal RAM (IRAM)
- The RF interface (radio frequency power and signal interface) enables contactless communication between a PICC (proximity integrated chip card, PICC) and a reader/writer (proximity coupling device, PCD). The power supply and data are received by an antenna which consists of a coil with a few turns directly connected to the IC.
- External memory comprising:
  - 4 kBytes extended RAM (XRAM)
  - 136 kBytes user ROM, including the routines for chip management (RMS)
  - 8 KB test ROM containing the test routines (STS), and
  - a total of 64 kBytes non-volatile memory (EEPROM).

- True random number generator (RNG)
- Checksum module (CRC)
- Interrupt module (INT)
- Input Logic (INP)
- Timer (TIM)
- Address and data bus (BUS)
- Advanced Crypto Engine (ACE) for long integer modulo calculations, which are used in asymmetric algorithms like RSA
- DES accelerator (DDC), used for fast calculations of the DES algorithm and provides EC2 support.

2.2.2 Firmware and software of the TOE

The entire firmware of the products consists of two different parts. One part is the RMS routines for EEPROM programming, the security function tests, and the random number online testing (**R**esource **M**anagement **S**ystem, IC Dedicated Support Software in the Smartcard IC Platform Protection Profile). The RMS routines are stored from Infineon Technologies AG in a reserved area of the normal user ROM. The other part is the STS consisting of test and initialization routines (**S**elf **T**est **S**oftware, IC Dedicated Test Software in Smartcard IC Platform Protection Profile).The STS routines are stored in the especially protected test ROM and are not accessible for the user software.

The software part of the TOE consists of the RSA2048 library. The RSA2048 library is used to provide a high level interface to RSA (Rivest, Shamir, Adleman) cryptography implemented on the hardware component ACE and includes countermeasures against SPA, DPA and DFA attacks. The routines are used for the generation of RSA Key Pairs (RsaKeyGen), the RSA signature verification (RsaVerify), the RSA signature generation (RsaSign) and the RSA modulus recalculation (RsaModulus). The hardware ACE unit provides the basic long number calculations (add, subtract, multiply, square with 1100 bit numbers) with high performance. The RSA2048 library is delivered as source code and in this way integrated in the user software. The RSA2048 library can perform RSA operations from 512 to 2048 bits. Included in the evaluation are only operations with key length of 1024 to 2048.

The above demarcations of the TOE result in the interfaces described below.

2.2.2.1 Interfaces of the TOE

- The physical interface of the TOE to the external environment is the entire surface of the IC.
- The electrical interface of the TOE to the external environment is constituted by the pads of the chip, particularly the contacted RES, I/O, CLK lines and supply lines VCC and GND, as well as by the contactless RF interface.

  The RF interface (radio frequency power and signal interface) enables contactless communication between a PICC (proximity integration chip card, PICC) and a reader/writer (proximity coupling device, PCD). The power supply and data are received by an antenna which consists of a coil with a few turns directly connected to the IC. The RF interface offers three communication protocols: Type A (ISO/IEC 14443), Type B (ISO/IEC 14443), and FeliCa (Sony-Interface). In both products the FeliCa interface protocol is deactivated.

Different anti-collision procedures can be implemented in software supported by on-chip hardware (e.g 16-bit timer, bitgrid logic).

- The data-oriented I/O interface to the TOE is formed by the I/O pad and the antenna of the RF interface.
- The interface to the firmware is constituted by special registers used for hardware configuration and control (Special Function Registers, SFR).
- The interface of the TOE to the operating system is constituted on the one hand by the RMS routine calls and on the other by the instruction set of the TOE.
- The interface of the TOE to the test routines is formed by the STS test routine call, i.e. entry to test mode (STS TM entry).
- The interface to the RSA calculations is defined from the RSA2048 library interface.

Table 3: TOE difference overview

Type / Feature	**SLE66CLX640P**	**SLE66CLX641P**
ISO7816 contact pads	Yes	No
Type A and B RF interface	Yes	Yes
FeliCa (Sony) RF interface	Inactive	Inactive

2.2.3 Guidance documentation

The guidance documentation consists of the [Databook] (and additional errata sheets) which contains the description of all interfaces of the software to the hardware relevant for programming the TOE.

In addition programming examples for more specific topics like secure use of cryptography are documented in form of application notes. The application notes are part of the development kit provided to the software developer. The monthly updated list of application notes is provided from Infineon Technologies AG [Status].

Finally the certification report will contain an overview of the recommendations to the software developer regarding the secure use of the platform SLE66CLX640P / m1523-a11 and SLE66CLX641P / m1522-a11. These recommendations are also included in the ordinary documentation.

The list of guidance documentation is given in Annex 9.1.

2.2.4 Forms of delivery

Both products can be delivered as complete modules or in form of plain wafers. The delivery can therefore be at the end of phase 3 or at the end of phase 4 according to Smartcard IC Platform Protection Profile. Nevertheless in both cases the TOE is finished and the extended test features are removed. In this document are always both cases mentioned to avoid incorrectness but from the security policy point of view the two cases are identically.

The delivery to the software developer (phase 2 -> phase 1) contains the development package which is delivered in form of documentation as described above, data carriers, containing the tools and emulators, as development and debugging tool.

2.2.5 Production sites

The TOE will be produced in Dresden only. To identify the production site the chip identification number is coded as shown in Table 4. The exact coding of the chip identification data is described in [Databook] section 7.3.3.

Table 4: Production site in chip identification

Production Site	Product name	Chip Identification (first nibble, hex format)
Dresden	SLE66CLX640P / m1523-a11	2
Dresden	SLE66CLX641P / m1522-a11	2

3 TOE Security Environment

For this chapter the Smartcard IC Platform Protection Profile can be applied completely. A summary is given in the following.

3.1 Definition of Assets

The primary assets concern the User Data which includes the data as well as program code (Smartcard Embedded Software). This asset has to be protected while being executed and on the other hand when the TOE is not in operation. This leads to the three primary assets

- User Data
- Smartcard Embedded Software
- TOE's correct operation

The specific functions of the TOE introduce additional assets.

- the random numbers generated by the TOE

The class of secondary assets consists of the following.

- logical design data,
- physical design data,
- IC Dedicated Software, Initialisation Data and Pre-personalisation Data, TSF data
- specific development aids,
- test and characterisation related data,
- material for software development support, and
- photo masks and products in any form

For details see Smartcard IC Platform Protection Profile section 3.1.

3.2 Assumptions

The assumptions defined in the Smartcard IC Platform Protection Profile concern the phases where the TOE has left the chip manufacturer.

A.Process-Card	Protection during Packaging, Finishing and Personalisation
A.Plat-Appl	Usage of Hardware Platform
A.Resp-Appl	Treatment of User Data

The support of cipher schemas needs to make a additional assumption.

The developer of the Smartcard Embedded Software must ensure the appropriate “Usage of Key-dependent Functions (A.Key-Function)” while developing this software in Phase 1 as specified below.

A.Key-Function Usage of Key-dependent Functions

Key-dependent functions (if any) shall be implemented in the Smartcard Embedded Software in a way that they are not susceptible to leakage attacks (as described under T.Leak-Inherent and T.Leak-Forced).

Note that here the routines which may compromise keys when being executed are part of the Smartcard Embedded Software. In contrast to this the threats T.Leak-Inherent and T.Leak-Forced address (i) the cryptographic routines which are part of the TOE and (ii) the processing of User Data including cryptographic keys.

For details see Smartcard IC Platform Protection Profile section 3.2.

3.3 Threats

The threats are directed against the assets. The threat is a general description of “What one wants to do” and might contain several specific attacks (“How one wants to do it”). The more detailed description of specific attacks is given later on in the process of evaluation and certification. An overview on attacks is given in Smartcard IC Platform Protection Profile.

Table 5: Threats to Smartcards according to the Protection Profile

T.Phys-Manipulation	Physical Manipulation
T.Phys-Probing	Physical Probing
T.Malfunction	Malfunction due to Environmental Stress
T.Leak-Inherent	Inherent Information Leakage
T.Leak-Forced	Forced Information Leakage
T.Abuse-Func	Abuse of Functionality
T.RND	Deficiency of Random Numbers

For details see Smartcard IC Platform Protection Profile section 3.2.

3.4 Organisational Security Policies

Both products of the TOE have to be protected during the first phases of his lifecycle (phases 2-TOE delivery)[1]. Later on the TOE has to protect itself. The organisational security policy covers this aspect.

P.Process-TOE Protection during TOE Development and Production

[1] The TOE can be delivered either after phase 3 or after phase 4.

See Smartcard IC Platform Protection Profile for a detailed description.

Due to the augmentations of the Smartcard IC Platform Protection Profile an additional policy is introduced.

3.4.1 Augmented organisational security policy

The TOE provides specific security functionality which can be used by the Smartcard Embedded Software. In the following specific security functionality is listed which is not derived from threats identified for the TOE's environment because it can only be decided in the context of the smartcard application, against which threats the Smartcard Embedded Software will use the specific security functionality.

The IC Developer / Manufacturer must apply the policy "Additional Specific Security Functionality (P.Add-Functions)" as specified below.

P.Add-Functions Additional Specific Security Functionality

The TOE shall provide the following specific security functionality to the Smartcard Embedded Software:

- *Area based Memory Access Control*
- *Triple Data Encryption Standard (3DES),*
- *Rivest-Shamir-Adleman (RSA),*

4 Security objectives

For this chapter the Smartcard IC Platform Protection Profile can be applied completely. Only a short overview is given in the following.

4.1 Security objectives for the TOE

See Smartcard IC Platform Protection Profile.

Table 6: Objectives for Smartcards according to the Protection Profile

O.Phys-Manipulation	Protection against Physical Manipulation
O.Phys-Probing	Protection against Physical Probing
O.Malfunction	Protection against Malfunction due to Environmental Stress
O.Leak-Inherent	Protection against Inherent Information Leakage
O.Leak-Forced	Protection against Forced Information Leakage
O.Abuse-Func	Protection against Abuse of Functionality
O.Identification	TOE Identification
O.RND	Random Numbers

The TOE shall provide “Additional Specific Security Functionality (O.Add-Functions)” as specified below.

O.Add-Functions Additional Specific Security Functionality

The TOE must provide the following specific security functionality to the Smartcard Embedded Software:

- *Area based Memory Access Control*
- *Triple Data Encryption Standard (3DES),*
- *Rivest-Shamir-Adleman (RSA),*

Table 7: Additional objectives due to TOE specific functions and augmentations

O.Add-Functions	Additional specific security functionality

4.2 Security objectives for the environment

The detailed description of the environmental security objectives is given in the Smartcard IC Platform Protection Profile. The list of objectives is in Table 8.

Table 8: Security objectives for the environment

Phase 1	OE.Plat-Appl	Usage of Hardware Platform

	OE.Resp-Appl	Treatment of User Data
Phase 2 up to TOE delivery	OE.Process-TOE	Protection during TOE Development and Production
TOE delivery up to end of phase 6	OE.Process-Card	Protection during Packaging, Finishing and Personalisation

4.2.1 Clarification of "Usage of Hardware Platform (OE.Plat-Appl)"

Regarding the cryptographic services this objective of the environment has to be clarified. The TOE supports cipher schemes as additional specific security functionality. If required the Smartcard Embedded Software shall use these cryptographic services of the TOE and their interface as specified. When key-dependent functions implemented in the Smartcard Embedded Software are just being executed, the Smartcard Embedded Software must provide protection against disclosure of confidential data (User Data) stored and/or processed in the TOE by using the methods described under "Inherent Information Leakage (T.Leak-Inherent)" and "Forced Information Leakage (T.Leak-Forced)".

Regarding the area based access control this objective of the environment has to be clarified. For the separation of different applications the Smartcard Embedded Software (Operating System) may implement a memory management scheme based upon security mechanisms of the TOE.

4.2.2 Clarification of "Treatment of User Data (OE.Resp-Appl)"

Regarding the cryptographic services this objective of the environment has to be clarified. By definition cipher or plain text data and cryptographic keys are User Data. The Smartcard Embedded Software shall treat these data appropriately, use only proper secret keys (chosen from a large key space) as input for the cryptographic function of the TOE and use keys and functions appropriately in order to ensure the strength of cryptographic operation.

This means that keys are treated as confidential as soon as they are generated. The keys must be unique with a very high probability, as well as cryptographically strong. For example, it must be ensured that it is beyond practicality to derive the private key from a public key if asymmetric algorithms are used. If keys are imported into the TOE and/or derived from other keys, quality and confidentiality must be maintained. This implies that appropriate key management has to be realised in the environment.

Regarding the area based access control this objective of the environment has to be clarified. The treatment of User Data is also required when a multi-application operating system is implemented as part of the Smartcard Embedded Software on the TOE. In this case the multi-application operating system should not disclose security relevant user data of one application to another application when it is processed or stored on the TOE.

5 IT security requirements

For this chapter the Smartcard IC Platform Protection Profile can be applied completely.

5.1 TOE security requirements

See Smartcard IC Platform Protection Profile.

The following tables provide an overview of the used functional security requirements. Requirements which are not drawn from CC Part 2 are marked in italics.

Table 9: Security functional requirements defined in Smartcard IC Platform Protection Profile

Security Functional Requirement		Refined in [PP]
FRU_FLT.2	"Limited fault tolerance"	Yes
FPT_FLS.1	"Failure with preservation of secure state"	Yes
FPT_SEP.1	"TSF domain separation"	Yes
FMT_LIM.1	*"Limited capabilities"*	
FMT_LIM.2	*"Limited availability"*	
FAU_SAS.1	*"Audit storage"*	
FPT_PHP.3	"Resistance to physical attack"	Yes
FDP_ITT.1	"Basic internal transfer protection"	Yes
FDP_IFC.1	"Subset information flow control"	
FPT_ITT.1	"Basic internal TSF data transfer protection"	Yes
FCS_RND.1	*"Quality metric for random numbers"*	

Table 10: Augmented security functional requirements

Security Functional Requirement
FPT_TST.2 "Subset TOE security testing"
FDP_ACC.1 "Subset access control"
FDP_ACF.1 "Security attribute based access control"
FMT_MSA.3 "Static attribute initialisation"
FMT_MSA.1 "Management of security attributes"
FMT_SMF.1 "Specification of Management functions"
FCS_COP.1 "Cryptographic support"
FCS_CKM.1 "Cryptographic key generation"
FDP_SDI.1 "Stored data integrity monitoring"

5.1.1 TOE security functional requirements

The detailed description of the security functional requirements is given in the Smartcard IC Platform Protection Profile. These security functional requirements are listed in Table 9. In the last

column it is marked if the requirement is refined in the [PP]. The refinements are also valid for this ST. The additional security functional requirements are listed in Table 10. The necessary assignments are done in section 7.2. The description of the additional security functional requirements is given in the following.

5.1.1.1 Subset TOE security testing (FPT_TST.2)

The security is strongly dependent on the correct operation of the security functions. Therefore, the TOE shall support that particular security functions or mechanisms are tested in the operational phase (Phase 7). The tests can be initiated by the Smartcard Embedded Software and/or by the TOE.

Part 2 of the Common Criteria provides the security functional component “TSF testing (FPT_TST.1)”. The component FPT_TST.1 provides the ability to test the TSF’s correct operation.

For the user it is important to know which security functions or mechanisms can be tested. The functional component FPT_TST.1 does not mandate to explicitly specify the security functions being tested. In addition, FPT_TST.1 requires the verification of the integrity of TSF data and stored TSF executable code which might violate the security policy. Therefore, the security functional component **Subset TOE security testing (FPT_TST.2)** has been newly created. This component allows that particular parts of the security mechanisms and functions provided by the TOE are tested.

FPT_TST.2

The security functional component Subset TOE security testing (FPT_TST.2) has been newly created (Common Criteria Part 2 extended). This component allows that particular parts of the security mechanisms and functions provided by the TOE can be tested after TOE Delivery. This security functional component is used instead of the functional component FPT_TST.1 from Common Criteria Part 2. For the user it is important to know which security functions or mechanisms can be tested. The functional component FPT_TST.1 does not mandate to explicitly specify the security functions being tested. In addition, FPT_TST.1 requires verifying the integrity of TSF data and stored TSF executable code which might violate the security policy.

The TOE shall meet the requirement “Subset TOE testing (FPT_TST.2)” as specified below (Common Criteria Part 2 extended).

FPT_TST.2	Subset TOE testing
Hierarchical to:	No other components.
FPT_TST.2.1	The TSF shall run a suite of self tests[2] *at the request of the authorised user*[3] to demonstrate the correct operation of the *environmental sensor mechanisms:* o Frequency Monitoring, o Voltage Sensor, o Light Detection and o Temperatur Sensor,

[2] The definition of the self test function (SleSlcTest) can be found in [Databook] chapter 6

[3] The term “authorized user” refers to the Smartcard Embedded Software running on the TOE

- *the RNG with help of the live test*
- *and of the active shield*.

Dependencies: FPT_AMT.1 Abstract machine testing

5.1.1.2 Memory access control

Usage of multiple applications in one Smartcard often requires separating code and data in order to prevent that one application can access code and/or data of another application. To support this feature the TOE provides Area based Memory Access Control. The underlying memory management unit (MMU) is documented in section 5 of the [DataBook].

Remember that the expression TOE always comprises the two products SLE66CLX640P / m1523-a11 and SLE66CLX641P / m1522-a11 when used in the following.

The security service being provided is described in the Security Function Policy (SFP) **Memory Access Control Policy**. The security functional requirement **"Subset access control (FDP_ACC.1)"** requires that this policy is in place and defines the scope were it applies. The security functional requirement **"Security attribute based access control (FDP_ACF.1)"** defines addresses security attribute usage and characteristics of policies. It describes the rules for the function that implements the Security Function Policy (SFP) as identified in FDP_ACC.1. The decision whether an access is permitted or not is taken based upon attributes allocated to the software. The Smartcard Embedded Software defines the attributes and memory areas. The corresponding permission control information is evaluated "on-the-fly" by the hardware so that access is granted/effective or denied/inoperable.

The security functional requirement **"Static attribute initialisation (FMT_MSA.3)"** ensures that the default values of security attributes are appropriately either permissive or restrictive in nature. Alternative values can be specified by any subject provided that the **Memory Access Control Policy** allows that. This is described by the security functional requirement **"Management of security attributes (FMT_MSA.1)"**. The attributes are determined during TOE manufacturing (FMT_MSA.3) or set at run-time (FMT_MSA.1).

From TOE´s point of view the different roles in the Smartcard Embedded Software can be distinguished according to the memory based access control. However the definition of the roles belongs to the user software.

The following Security Function Policy (SFP) **Memory Access Control Policy** is defined for the requirement "Security attribute based access control (FDP_ACF.1)":

Memory Access Control Policy

The TOE shall control *read, write, delete, execute accesses* of *software running at two different modes (system mode active during interrupt execution or application mode active during other executing)* on *data and code stored in memory areas*.

The TOE shall restrict the ability to define, to change or at least to finally accept the applied rules (as mentioned in FDP_ACF.1) to *software running at interrupt level (in the system mode)*.

The TOE shall meet the requirement "Subset access control (FDP_ACC.1)" as specified below.

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1 The TSF shall enforce the *Memory Access Control Policy* on *all subjects (software running at system mode active during interrupt execution or application mode active during other executing), all objects (data including code stored in memories) and all the operations defined in the Memory Access Control Policy*.

Dependencies: FDP_ACF.1 Security attribute based access control

The TOE shall meet the requirement "Security attribute based access control (FDP_ACF.1)" as specified below.

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1[4] The TSF shall enforce the *Memory Access Control Policy* to objects based on the following:
Subject:
- *software running at system mode active during interrupt execution or application mode active during other executing*

attributes:
- *the interrupt execution level where the software is executed (interrupt / non-interrupt) and/or*

Object:
- *data including code stored in memories*

attributes:
- *the memory area where the access is performed to and/or*
- *the operation to be performed*.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *evaluate the corresponding permission control information before the access so that accesses to be denied can not be utilised by the subject attempting to perform the operation*.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the *following additional rules: none*.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

The TOE shall meet the requirement "Static attribute initialisation (FMT_MSA.3)" as specified below.

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

---

[4] *The following element is changed as a result of Interpretation 103.*
FDP_ACF.1.1 The TSF shall enforce the [assignment*: access control SFP*] to objects based on the following: [assignment*: list of subjects and objects controlled under the indicated SFP, and. for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*].

FMT_MSA.3.1 The TSF shall enforce the *Memory Access Control Policy* to provide *well defined*[5] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow *any subject (provided that the Memory Access Control Policy is enforced and the necessary access is therefore allowed)* [6] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

The TOE shall meet the requirement “Management of security attributes (FMT_MSA.1)” as specified below:

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the *Memory Access Control Policy* to restrict the ability to *change default, modify or delete* the security attributes *permission control information* to *running at interrupt level (system mode)*.

Dependencies: [FDP_ACC.1 Subset access control or

FDP_IFC.1 Subset information flow control]

FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

The TOE shall meet the requirement “Specification of management functions (FMT_SMF.1)” as specified below:

FMT_SMF.1 Specification of management functions

Hierarchical to: No other components

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions*: access the configuration registers of the MMU*.

Dependencies: No dependencies

[5] The static definition of the access rules is documented in [DataBook] section 5

[6] The Smartcard Embedded Software is intended to set the memory access control policy

5.1.1.3 Support of cipher schemas

FCS_COP.1 Cryptographic operation requires a cryptographic operation to be performed in accordance with a specified algorithm and with a cryptographic key of specified sizes. The specified algorithm and cryptographic key sizes can be based on an assigned standard. The dependencies will be discussed in Section 8.2.

The following additional specific security functionality is implemented in the TOE:

- *Triple Data Encryption Standard (3DES),*
- *Rivest-Shamir-Adleman (RSA),*

Triple-DES Operation

The DES Operation of the TOE shall meet the requirement “Cryptographic operation (FCS_COP.1)” as specified below.

FCS_COP.1	Cryptographic operation
Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *Triple Data Encryption Standard (3DES)* and cryptographic key sizes *of 112 bit* that meet the following *standards*: *U.S. Department of Commerce / National Bureau of Standards Data Encryption Standard (DES), FIPS PUB 46-3, 1999 October 25, keying option 2*
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes

Rivest-Shamir-Adleman (RSA) operation

The Modular Arithmetic Operation of the TOE shall meet the requirement “Cryptographic operation (FCS_COP.1)” as specified below.

FCS_COP.1	Cryptographic operation
Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *Rivest-Shamir-Adleman (RSA)* and cryptographic key sizes *1024 - 2048 bits* that meet the following *standards* *ISO/IEC 9796-1, Annex A, sections A.4 and A.5, and Annex C*.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

Rivest-Shamir-Adleman (RSA) key generation

The key generation for the RSA shall meet the requirement “Cryptographic key generation (FCS_CKM.1)”

FCS_CKM.1	Cryptographic key generation
Hierarchical to:	No other components.
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *specified in [ETSI] and [ALGO]* and specified cryptographic key sizes *1024 - 2048 bits* that meet the following *standards*. *ISO/IEC 9796-1, Annex A, sections A.4 and A.5, and Annex C*.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes

5.1.1.4 Data Integrity

The TOE shall meet the requirement “Stored data integrity monitoring (FDP_SDI.1)” as specified below:

FDP_SDI.1	Stored data integrity monitoring
Hierarchical to:	No other components
FDP_SDI.1.1	The TSF shall monitor user data stored within the TSC for *inconsistencies between stored data and corresponding CRC checksum* on all objects, based on the following attributes: *CRC checksum value*.
Dependencies:	No dependencies

5.1.2 TOE security assurance requirements

The evaluation assurance level is EAL 5 augmented. In Table 11 the security assurance requirements are given. The increase of the assurance components compared to the Smartcard IC Platform Protection Profile is expressed with bold letters. The augmentation of the assurance components to level EAL5 is given in bold letters.

Table 11: Assurance components

Aspect	Acronym	Description	Refinement
Configuration management	ACM_AUT.1	Partial CM automation	
	ACM_CAP.4	Generation support and acceptance procedures	in PP
	ACM_SCP.3	**Development tools CM coverage**	**in ST**
Delivery and operation	ADO_DEL.2	Detection of modification	in PP
	ADO_IGS.1	Installation, generation, and start-up procedures	in PP
Development	**ADV_FSP.3**	**Semiformal functional specification**	**in ST**
	ADV_HLD.3	**Semiformal high-level design**	
	ADV_IMP.2	Implementation of the TSF	
	ADV_INT.1	**Modularity**	
	ADV_LLD.1	Descriptive low-level design	
	ADV_RCR.2	**Semiformal correspondence demonstration**	
	ADV_SPM.3	**Formal TOE security policy model**	
Guidance documents	AGD_ADM.1	Administrator guidance	in PP
	AGD_USR.1	User guidance	in PP
Life cycle support	*ALC_DVS.2*	*Sufficiency of security measures*	*in PP*
	ALC_LCD.2	**Standardised life-cycle model**	
	ALC_TAT.2	**Compliance with implementation standards**	
Tests	ATE_COV.2	Analysis of coverage	in PP
	ATE_DPT.2	**Testing: low-level design**	
	ATE_FUN.1	Functional testing	
	ATE_IND.2	Independent testing – sample	
Vulnerability assessment	**AVA_CCA.1**	**Covert channel analysis**	
	AVA_MSU.3	*Validation of analysis*	
	AVA_SOF.1	Strength of TOE security function evaluation	
	AVA_VLA.4	*Highly resistant*	

5.1.3 Refinements

Some refinements are taken unchanged from the Smartcard IC Platform Protection Profile. In some cases a clarification is necessary. In Table 11 an overview is given where the refinement is done. Two refinements from the Smartcard IC Platform Protection Profile have to be discussed here in the Security Target, as the assurance level is increased.

Configuration Management Scope (ACM_SCP)

The refinement from the Smartcard IC Platform Protection Profile can be applied even at the chosen assurance level EAL 5 augmented with ACM_SCP.3. The assurance package ACM_SCP.2 is extended to ACM_SCP.3 with aspects regarding the development tools. The refinement is not touched.

Refinement for CM scope (ACM_SCP)

The “TOE implementation representation” within the scope of the CM shall include at least:

- logical design data,
- physical design data,
- IC Dedicated Software,
- Smartcard Embedded Software,
- final physical design data necessary to produce the photo masks, and
- photo masks.

Functional Specification (ADV_FSP)

The refinement from the Smartcard IC Platform Protection Profile can be applied even at the chosen assurance level EAL 5 augmented with ADV_FSP.3. The assurance package ADV_FSP.2 is extended to ADV_FSP.3 with aspects regarding the descriptive level. The level is increased from informal to semi formal with informal description. The refinement is not touched from this measure.

For details of the refinement see Smartcard IC Platform Protection Profile.

5.2 Security requirements for the Environment

5.2.1 Security requirements for the IT Environment

5.2.1.1 Security requirements for the IT Environment resulting from FCS_COP.1

The security functional requirement “Cryptographic operation (FCS_COP.1)” met by TOE has the following dependencies

- [FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation],
- FCS_CKM.4 Cryptographic key destruction,
- FMT_MSA.2 Secure security attributes.

These requirements all address the appropriate management of cryptographic keys used by the specified cryptographic function and are not part of the Smartcard IC Platform Protection Profile. Most requirements concerning key management shall be fulfilled by the environment since the Smartcard Embedded Software is designed for a specific application context and uses the cryptographic functions provided by the TOE.

In the following the dependencies are discussed separately for the 3DES and the RSA algorithm.

3DES

The environment shall meet the requirement “Import of user data without security attributes FDP_ITC.1)” as specified below.

FDP_ITC.1 Import of user data without security attributes

Hierarchical to: No other components.

FDP_ITC.1.1 The TSF shall enforce the *Access Control Policy or Information Flow Control Policy* when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: Data *Access Control Policy or Information Flow Control Policy.*

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FMT_MSA.3 Static attribute initialisation

or

The environment shall meet the requirement “Import of user data with security attributes FDP_ITC.2)” as specified below.

FDP_ITC.2 Import of user data without security attributes

Hierarchical to: No other components.

FDP_ITC.2.1 The TSF shall enforce the *Access Control Policies or Information Flow Control Policies* when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.2.2 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.3 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.4 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: *Access Control Policy or Information Flow Control Policy.*

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]

FPT_TDC.1 Inter-TSF basic TSF data consistency

or

The environment shall meet the requirement “Cryptographic key generation (FCS_CKM.1)” as specified below.

FCS_CKM.1 Cryptographic key generation (3DES)

Hierarchical to: No other components.

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *3DES* and specified cryptographic key sizes *112 bit* that meet the following: *U.S. Department of Commerce / National Bureau of Standards Data Encryption Standard (DES), FIPS PUB 46-3, 1999 October 25, keying option 2*.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

Remark: Cryptographic keys for the 3DES algorithm have to be generated in the environment and imported into the TOE.

The environment shall meet the requirement “Cryptographic key destruction (FCS_CKM.4)” as specified below.

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *change key and change key with certificate verification that* meets the following: ISO/IEC 7816.

Dependencies: [FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation]

FMT_MSA.2 Secure security attributes

The environment shall meet the requirement “Secure security attributes (FMT_MSA.2)” as specified below.

FMT_MSA.2 Secure security attributes

Hierarchical to: No other components.

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

Dependencies: ADV_SPM.1 Informal TOE security policy model

[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]

FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

RSA

The environment shall meet the requirement “Import of user data without security attributes FDP_ITC.1)” as specified below.

FDP_ITC.1 Import of user data without security attributes

Hierarchical to: No other components.

FDP_ITC.1.1 The TSF shall enforce the *Access Control Policy or Information Flow Control Policy* when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: Data *Access Control Policy or Information Flow Control Policy.*

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FMT_MSA.3 Static attribute initialisation

or

the environment shall meet the requirement “Import of user data with security attributes FDP_ITC.2)” as specified below.

FDP_ITC.2 Import of user data without security attributes

Hierarchical to: No other components.

FDP_ITC.2.1 The TSF shall enforce the *Access Control Policies or Information Flow Control Policies* when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.2.2 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.3 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.4 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: *Access Control Policy or Information Flow Control Policy.*

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]

FPT_TDC.1 Inter-TSF basic TSF data consistency

or

the environment shall meet the requirement “Cryptographic key generation (FCS_CKM.1)” as specified below.

FCS_CKM.1 Cryptographic key generation (RSA)

Hierarchical to: No other components.

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *specified in [ETSI] and [ALGO]* and specified cryptographic key sizes *1024 - 2048 bits* that meet the following *standards*.

ISO/IEC 9796-1, Annex A, sections A.4 and A.5, and Annex C.

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

Remark: Cryptographic keys for the RSA algorithm can either be generated in the TOE or in the environment. If they are generated in the environment they have to be imported into the TOE.

The environment shall meet the requirement “Cryptographic key destruction (FCS_CKM.4)” as specified below.

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *change key and change key with certificate verification that* meets the following: ISO/IEC 7816.

Dependencies: [FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation]

FMT_MSA.2 Secure security attributes

The environment shall meet the requirement “Secure security attributes (FMT_MSA.2)” as specified below.

FMT_MSA.2 Secure security attributes

Hierarchical to: No other components.

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

Dependencies: ADV_SPM.1 Informal TOE security policy model

[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]

FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

5.2.1.2 Security requirements for the IT Environment resulting from FCS_CKM.1

The security functional requirement “Cryptographic key generation (FCS_CKM.1)” met by TOE has the following dependencies

- [FDP_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation],
- FCS_CKM.4 Cryptographic key destruction,
- FMT_MSA.2 Secure security attributes.

FCS_COP.1 is fulfilled by the TOE. FCS_CKM.4 and FMT_MSA.2 has to be fulfilled by the environment as described above for the RSA algorithm.

5.2.2 Security Requirements for the Non-IT-Environment

In the following security requirements for the Non-IT-Environment are defined. For the development of the Smartcard Embedded Software (in Phase 1) the requirement RE.Phase-1 is valid.

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

The developers shall design and implement the Smartcard Embedded Software in such way that it meets the requirements from the following documents: (i) hardware data sheet for the TOE, (ii) TOE application notes, and (iii) findings of the TOE evaluation reports relevant for the Smartcard Embedded Software.

The developers shall implement the Smartcard Embedded Software in a way that it protects security relevant User Data (especially cryptographic keys) as required by the security needs of the specific application context.

The responsible parties for the Phases 4-6 are required to support the security of the TOE by appropriate measures:

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

The Card Manufacturer (after TOE Delivery up to the end of Phase 6) shall use adequate security measures 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).

The Smartcard Embedded Software shall meet the requirements “Cipher Schemas (RE.Cipher)” as specified below.

RE.Cipher Cipher Schemas

The developers of Smartcard Embedded Software must not implement routines in a way which may compromise keys when the routines are executed as part of the Smartcard Embedded Software. Performing functions which access cryptographic keys could allow an attacker to misuse these functions to gather information about the key which is used in the computation of the function.

Keys must be kept confidential as soon as they are generated. The keys must be unique with a very high probability, as well as cryptographically strong. For example, it must be ensured that it is not possible to derive the private key from a public key if asymmetric algorithms are used. If keys are imported into the TOE and/or derived from other keys, quality and confidentiality must be maintained. This implies that an appropriate key management has to be realised in the environment.

6 TOE summary specification

The product overview is given in section 2.1. In the following the security functionality is described and the relation to the security functional requirements is shown.

The TOE is equipped with 9 security enforcing functions to meet the security functional requirements. The functions are:

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

The following description of the security enforcing functions is a complete representation of the TSF.

6.1 SEF1: Operating state checking

Correct function of both products is only given when operated in the specified range of the environmental operating parameters. To prevent an attack exploiting those circumstances it is necessary to detect if the specified range is left.

All operating signals are filtered to prevent malfunction. The FRU_FLT.2 “Limited fault tolerance” requirement is satisfied.

In addition the operating state is monitored with sensors for the operating voltage, clock signal frequency, and temperature and electro magnetic radiation. The TOE falls into the defined secure state in case of a specified range violation[7]. The defined secure state causes the chip internal reset process. The FPT_FLS.1 “Failure with preservation of secure state“-requirement is satisfied.

In order to prevent accidental bit faults during production in the ROM, over the data stored in ROM a CRC-Checksum is calculated. The FDP_SDI.1 “Stored data integrity monitoring” is satisfied.

The covered security functional requirements are FRU_FLT.2, FPT_FLS.1 and FDP_SDI.1. The SEF1 does not use probabilistic or permutational effects. Since the ROM CRC functionality is not accessible via an external interface no direct attacks are possible. Therefore this function is not included in the SOF claim.

6.2 SEF2: Phase management with test mode lock-out

The life cycle of the TOE is split-up in several phases. Chip development and production (phase 2, 3, 4) and final use (phase 4-7) is a rough split-up from TOE point of view. These phases are implemented in both TOE products as test mode (phase 2, 3, 4) and user mode (phase 1, 4-7). In addition a chip identification mode exists which is active in all phases.

[7] The operating state checking SEF1 can only work when the TOE is running and can not prevent reverse engineering.

During start-up of the TOE the decision for the user mode or the test mode is taken dependent on several phase identifiers (phase management). If test mode is the active phase the TOE requests authentication before any action (test mode lock-out). FMT_LIM.1 and FMT_LIM.2 are satisfied.

If the chip identification mode is requested the chip identification data (O.Identification) stored in a non modifiable EEPROM area is reported. FAU_SAS.1 “Audit storage” is satisfied.

The phase management is used to provide the separation between the security enforcing functions and the user software. The FPT_SEP.1 “TSF domain separation“ is satisfied.

The covered security functional requirements are FMT_LIM.1, FMT_LIM.2, FPT_SEP.1 and FAU_SAS.1. The test mode lock-out uses probabilistic or permutational effects and has to be included in the AVA_SOF analysis with SOF *high*.

6.3 SEF3: Protection against snooping

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

There are topological design measures for disguise, such as the use of the top metal layer with active signals for protecting critical data. The entire design is kept in a non standard way to prevent attacks using standard analysis methods. A Smartcard dedicated CPU with a non public bus protocol is used which makes analysis complicated.

The covered security functional requirement is FPT_PHP.3 “Resistance to physical attack“ as these measures make it difficult to do the physical analysis necessary before manipulation. The protection against snooping uses probabilistic or permutational effects and has to be included in the AVA_SOF analysis with SOF *high*.

6.4 SEF4: Data encryption and data disguising

The readout of data can be controlled with the use of encryption. An attacker can not use the data obtained by espionage due to their encryption.

The memory contents of both TOE products are encrypted on chip to protect against data analysis on stored data as well as on internally transmitted data. To prevent interpretation of leaked processed or transferred information randomness is inserted in the information. In addition important parts of the CPU and the complete DES component are especially designed to counter leakage attacks like DPA or EMA. The current consumption is independent of the processed data. In order to counter fault attacks in the RSA-calculation redundant calculations are performed.

The information leakage is kept low with special design measures. An interpretation of leaked data is not possible as all the data is encrypted. The covered security functional requirements are FDP_ITT.1 “Basic internal transfer protection“ and FPT_ITT.1 “Basic internal TSF data transfer protection“. The encryption covers the data processing policy and FDP_IFC.1 “Subset information flow control“. The SEF4 uses probabilistic or permutational effects and has to be included in the AVA_SOF analysis with SOF *high*.

6.5 SEF5: Random number generation

Random data is essential for cryptography as well as for physical security mechanisms. Both TOE products are equipped with a true random generator based on physical probabilistic controlled effects. The random data can be used from the Smartcard Embedded Software as well as from the security enforcing functions. It should fulfil the requirements from the functionality class P2 of [AIS31]

The generated numbers are true random due to the construction principle. The covered security functional requirement is FCS_RND.1.

The SEF5 uses a special metric as defined in [AIS31]. It has to be included in the AVA_SOF analysis with SOF *high*.

6.6 SEF6: TSF self test

The TSF of both TOE products have either hardware controlled self test which can be started from the Smartcard Embedded Software by a RMS function call or can be tested directly from the Smartcard Embedded Software for the active shield. The tested security enforcing functions are SEF1, SEF5 and SEF7.

As any attempt to modify the sensor devices will be detected from the test, the covered security functional requirement is FPT_TST.2. The TSF self test does not use probabilistic or permutational effects.

6.7 SEF7: Notification of physical attack

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

The attempt to use an opened device will be detected. The covered security functional requirement is FPT_PHP.3. Especially manipulation and the usage of galvanic contacts to gain information on the chip or the data are covered of this security enforcing function. The SEF7 “Notification of physical attack” does not use probabilistic or permutational effects.

6.8 SEF8: Memory Management Unit (MMU)

The MMU of both TOE products provide the Smartcard Embedded Software the possibility to define different access rights for memory areas and components. In case of an access violation the MMU will generate a non maskable interrupt (NMI). Then a interrupt service routine (ISR) can react on the access violation.

The MMU is used to map the logical address range of 64 kByte in the 8051 architecture to the physical memory range of 1 MByte and to control access to the component’s special function registers. The MMU provides the privileged system mode (at interrupt level) and the regular application mode. Both modes own two descriptors for data access and two descriptors for code access. The descriptor table defines the physical base address and the length of the memory range in 256 byte granularity which will be used for the logical to physical address translation. Two additional registers contain the access information of the component’s SFR. Access violation is caused if the physical address is not in the range defined from the descriptor or the access to the SFR is not granted. The reaction on access violation is a non maskable interrupt (NMI).

Only system mode has access to the descriptor table. The MMU has to be enabled as the default mode after reset is a compatibility mode without access permission (transparent mode).

As the TOE provides support for separation of memory areas the covered security functional requirements are FDP_ACC.1 as access control is provided, FDP_ACF.1 as a privileged and a regular mode exists, FMT_MSA.3 is covered from the initial (transparent) mode, FMT_MSA.1 is covered from the possibility to enable the MMU and FMT_SMF.1 is covered from the access to the special function register. The SEF8 “Memory Management Unit” does not use probabilistic or permutational effects.

6.9 SEF9: Cryptographic Support

The TOE is equipped with several hardware accelerators to support the standard cryptographic operations. This security enforcing function is introduced to include the cryptographic operation in the scope of the evaluation as the cryptographic function itself is not used from the TOE security policy. On the other hand these functions are of special interest for the use of the hardware as

platform for the software. The components are a hardware DES encryption unit and a combination of software and hardware unit to support RSA cryptography and RSA key generation. The key for the cryptographic 3DES operations are provided from the Smartcard Embedded Software (environment).

As defined cryptographic operations are provided by the TOE, the covered security functional requirement is FCS_COP.1 and FCS_CKM.1 in case of the RSA key generation. The SEF9 does use probabilistic or permutational effects, but cryptographic algorithms are excluded from the SOF assessment.

6.10 Mapping of Security Functional Requirements

The justification of the mapping between Security Functional Requirements and the Security Enforcing Functions is given in sections 6.1-6.9. The results are shown in Table 12. The security functional requirements are addressed by one relating security enforcing function except the security functional requirement FPT_PHP.3. The security functional requirement FPT_PHP.3 is covered from the SEF3 for the aspect of making the reverse engineering harder even if the TOE is out of operation and from SEF7 for the aspect of detecting the attempt to modify the TOE when the chip is running. The SEF3 and the SEF7 are mutually supportive to cover FPT_PHP.3.

Table 12: Mapping of SFR and SEF

	SEF 1	SEF 2	SEF 3	SEF 4	SEF 5	SEF 6	SEF 7	SEF 8	SEF 9
FAU_SAS.1		X							
FCS_RND.1					X				
FDP_IFC.1				X					
FDP_ITT.1				X					
FMT_LIM.1		X							
FMT_LIM.2		X							
FPT_FLS.1	X								
FPT_ITT.1				X					
FPT_PHP.3			X				X		
FPT_SEP.1		X							
FRU_FLT.2	X								
FPT_TST.2						X			
FDP_ACC.1								X	
FDP_ACF.1								X	
FMT_SMF.1								X	
FMT_MSA.3								X	
FMT_MSA.1								X	
FCS_COP.1									X
FCS_CKM.1									X
FDP_SDI.1	X								

6.11 Assurance Measures

In Table 13 the TOE specific assurance measures are listed. These measures fulfil the requirements from Table 11.

This Security Target is the first document in the course of an evaluation. The exact references (version numbers and date) of the documents are not final during the evaluation of the security target. To avoid an update of the security target at the end of the evaluation the exact references are listed in the configuration list (ACM_SCP.3) of the evaluation.

Table 13: Assurance measures

Assurance measure class	Acronym components	Document
Security Target	ASE	Security Target
Configuration management	ACM_AUT.1	Development Production (Dev_Prod)
	ACM_CAP.4	
	ACM_SCP.3	Configuration management scope (ACM_SCP)
Delivery and operation	ADO_DEL.2	Development Production (Dev_Prod)
	ADO_IGS.1	
Development	ADV_FSP.3	Functional Specification (ADV_FSP.3)
	ADV_HLD.3	High Level Design (ADV_HLD.3)
	ADV_IMP.2	Implementation (ADV_IMP.2)
	ADV_INT.1	TSF Internals (ADV_INT.1)
	ADV_LLD.1	Low Level Design (ADV_LLD.1)
	ADV_RCR.2	Representation Correspondence (ADV_RCR.2)
	ADV_SPM.3	LKW model
Guidance documents	AGD_ADM.1	Documentation (AGD)
	AGD_USR.1	
Life cycle support	ALC_DVS.2	Development Production (Dev_Prod)
	ALC_LCD.2	
	ALC_TAT.2	
Tests	ATE_COV.2	Test Documentation (ATE)
	ATE_DPT.2	
	ATE_FUN.1	
	ATE_IND.2	
Vulnerability assessment	AVA_CCA.1	Vulnerability Assessment (AVA)
	AVA_MSU.3	
	AVA_SOF.1	
	AVA_VLA.4	

7 PP claims

7.1 PP reference

This security target is conformant to the Smartcard IC Platform Protection Profile.

7.2 PP tailoring

The assignments and selections foreseen in the Smartcard IC Platform Protection Profile are done here.

7.2.1 FCS_RND

The random numbers are generated from SEF5. The quality level of the random numbers is defined as functionality class P2 with SOF-high of [AIS31].

FCS_RND.1	Quality metric for random numbers
FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet *functionality class P2 with SOF-high of [AIS31].*

Additional requirements are taken from the augmentation paper to the Smartcard IC Platform Protection Profile. The requirements FDP_ITC.1, FCS_CKM.1 and FCS_CKM.4 which include open assignments and selections are requirements for the IT environment. All necessary assignments and selections are described in chapter 5.2.1.

7.3 PP additions

Additional objectives and security functional requirements are explicitly mentioned in this security target.

- Key-Function in section 3.2,
- P.Add-Functions in section 3.4.1,
- Add-Functions in section 4.1,
- OE.Plat-Appl and OE.Resp-Appl in section 4.2.
- FPT_TST.2, FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FCS_COP.1, FCS_CKM.1, and FDP_SDI.1 in section 5.1.1,
- FDP_ITC.1, FDP_ITC.2, FCS_CKM.1, and FCS_CKM.4 in section 5.2.1,
- RE.Cipher in section 5.2.2.

8 Rational

The rational from the Smartcard IC Platform Protection Profile is used here and it is not changed. The augmentations are designed to be compliant to the rational of the Smartcard IC Platform Protection Profile. The necessary extensions to the Smartcard IC Platform Protection Profile rational are given in the following.

8.1 Security Objectives Rationale

Table 14: Security Objective Rational

Assumption, Threat or Organisational Security Policy	Security Objective
P.Add-Functions	O.Add-Functions
A.Key-Function	OE.Plat-Appl OE.Resp-Appl

The justification related to the security objective “Additional Specific Security Functionality (O.Add-Functions)” is as follows: The organisational security policy is covered by the objective above, since O.Add-Functions requires the TOE to implement exactly the same specific security functionality as required by P.Add-functions.

Nevertheless the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced define how to implement the specific security functionality required by P.Add-Functions. (Note that these objectives support that the specific security functionality is provided in a secure way as expected from P.Add-Functions.) Especially O.Leak-Inherent and O.Leak-Forced refer to the protection of confidential data (User Data or TSF data) in general. User Data are also processed by the specific security functionality required by P.Add-Functions.

Compared to Smartcard IC Platform Protection Profile a clarification has been made for the security objective “Usage of Hardware Platform (OE.Plat-Appl)”: If required the Smartcard Embedded Software shall use these cryptographic services of the TOE and their interface as specified. In addition, the Smartcard Embedded Software must implement functions which perform operations on keys (if any) in such a manner that they do not disclose information about confidential data. The non disclosure due to leakage A.Key-Function attacks is included in this objective OE.Plat-Appl. This addition ensures that the assumption A.Plat-Appl is still covered by the objective OE.Plat-Appl although additional functions are being supported according to O.Add-Functions.

Compared to Smartcard IC Platform Protection Profile a clarification has been made for the security objective “Treatment of User Data (OE.Resp-Appl)”: By definition cipher or plain text data and cryptographic keys are User Data. So, the Smartcard Embedded Software will protect such data if required and use keys and functions appropriately in order to ensure the strength of cryptographic operation. Quality and confidentiality must be maintained for keys that are imported and/or derived from other keys. This implies that appropriate key management has to be realised in the environment. That is expressed by the assumption A.Key—Function which is covered from OE.Resp–Appl. These measures make sure that the assumption A.Resp-Appl is still covered by the security objective OE.Resp-Appl although additional functions are being supported according to P.Add-Functions.

The justification of the additional policy and the additional assumption show that they do not contradict to the rationale already given in the Protection Profile for the assumptions, policy and threats defined there.

8.2 Security Requirements Rationale

8.2.1 Rationale for the security functional requirements

Cryptographic operation (FCS_COP.1)

Table 15: Rational for cryptographic operation requirement

Objective	TOE Security Functional Requirements	Security Requirements for the environment
O.Add-Functions	- FCS_COP.1 „Cryptographic operation“ - FCS_CKM.1 „Cryptographic key generation“	RE.Phase-1 “Design and Implementation of the Smartcard Embedded Software” with RE.Cipher
OE.Plat-Appl		RE.Phase.1 RE.Cipher
OE.Resp-Appl		RE.Phase.1 RE.Cipher FDP_ITC.1 or FDP_ITC.2 (for 3DES and RSA) FCS_CKM.1 (for 3DES and optional for RSA) FCS_CKM.4 (for 3DES and RSA) FMT_MSA.2 (for 3DES and RSA)

The justification related to the security objective “Additional Specific Security Functionality (O.Add-Functions)” is as follows:

The security functional requirement(s) “Cryptographic operation (FCS_COP.1)” exactly requires those functions to be implemented which are demanded by O.Add-Functions. FCS_CKM.1 supports the generation of RSA keys needed for this cryptographic operations. Therefore, FCS_COP.1 and FCS_CKM.1 are suitable to meet the security objective.

Nevertheless, the developer of the Smartcard Embedded Software must ensure that the additional functions are used as specified and that the User Data processed by these functions are protected as defined for the application context. These issues are addressed by the requirement RE.Phase-1 and more specific by the security functional requirements:

- [FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation],
- FCS_CKM.4 Cryptographic key destruction,
- FMT_MSA.2 Secure security attributes.

All these requirements have to be fulfilled to support OE.Resp-Appl for the 3DES algorithm. For the RSA algorithm FCS_CKM.1 is optional, since it is fulfilled by the TOE. Nevertheless the user can generate keys externally additionally.

The security functional requirements required to meet the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced define how to implement the specific security functionality. However, key-dependent functions could be implemented in the

Smartcard Embedded Software. In this case RE.Cipher requires that these functions ensure that confidential data (User Data) can not be disclosed while they are just being processed by the Smartcard Embedded Software. Therefore, with respect to the Smartcard Embedded Software the issues addressed by the objectives just mentioned are addressed by the requirement RE.Cipher.

The usage of cryptographic algorithms requires the use of appropriate keys. Otherwise they do not provide security. The requirement RE.Cipher addresses these specific issues since cryptographic keys and other data are provided by the Smartcard Embedded Software. RE.Cipher requires that keys must be kept confidential. They must be unique with a very high probability, cryptographically strong etc. In case of key importing into the TOE (usually after TOE Delivery), it has to be ensured that quality and confidentiality are maintained. Keys for 3DES are provided by the environment. Keys for RSA can be provided either by the TOE or the environment. Therefore, with respect to the environment the issues addressed (i) by the objectives just mentioned and (ii) implicitly by O.Add-Functions are addressed by the requirement RE.Cipher.

In this ST the objectives for the environment OE.Plat-Appl and OE.Resp-Appl have been clarified. The requirement for the environment Re.Cipher has been introduced to cover the objectives OE.Plat-Appl and OE.Resp-Appl (in addition to O.Add-Functions). The Smartcard Embedded Software defines the use of the cryptographic functions FCS_COP.1 provided by the TOE. RE.Phase-1, which is assigned to OE.Resp-Appl in the Smartcard IC Platform Protection Profile, requires the Smartcard Embedded Software Developer to design and implement the software that it protects security relevant User Data (especially cryptographic keys). The requirements for the environment FDP_ITC.1, FDP_ITC.2 FCS_CKM.1, FCS_CKM.4, and FMT_MSA.2 support an appropriate key management. These security requirements are suitable to meet OE.Resp-Appl.

The justification of the security objective and the additional requirements (both for the TOE and its environment) show that they do not contradict to the rationale already given in the Protection Profile for the assumptions, policy and threats defined there.

Subset TOE security testing (FPT_TST.2)

Table 16: Rational for subset TOE security testing requirement

Objective	TOE Security Functional Requirements	Security Requirements for the environment
O.Phys-Manipulation	- FPT_TST.2 „ Subset TOE security testing “	

The security functional component Subset TOE security testing (FPT_TST.2) has been newly created (Common Criteria Part 2 extended). This component allows that particular parts of the security mechanisms and functions provided by the TOE can be tested after TOE Delivery. This security functional component is used instead of the functional component FPT_TST.1 from Common Criteria Part 2. For the user it is important to know which security functions or mechanisms can be tested. The functional component FPT_TST.1 does not mandate to explicitly specify the security functions being tested. In addition, FPT_TST.1 requires the verification of the integrity of TSF data and stored TSF executable code which might violate the security policy.

The tested security enforcing function is SEF1, SEF5 and SEF7.

The security functional requirement FPT_TST.2 will detect attempts to conduce a physical manipulation on the monitoring functions of the TOE. The objective of FPT_TST.2 is O.Phys-Manipulation. The physical manipulation will be tried to overcome security enforcing functions.

Memory Access Control Policy

Table 17: Rational for Memory Access Control Policy requirement

Objective	TOE Security Functional Requirements	Security Requirements for the environment
O.Add-Functions	- FDP_ACC.1 “Subset access control” - FDP_ACF.1 “Security attribute based access control” - FMT_MSA.3 “Static attribute initialisation” - FMT_MSA.1 “Management of security attributes” - FMT_SMF.1 “Specification of Management Functions”	RE.Phase-1 “Design and Implementation of the Smartcard Embedded Software”

The justification related to the security objective “Additional Specific Security Functionality (O.Add-Functions)” is as follows:

The security functional requirement “Subset access control (FDP_ACC.1)” with the related Security Function Policy (SFP) “Memory Access Control Policy” exactly require the implementation of an area based memory access control, which is a requirement from O.Add-Functions. Therefore, FDP_ACC.1 with its SFP is suitable to meet the security objective.

Nevertheless, the developer of the Smartcard Embedded Software must ensure that the additional functions are used as specified and that the User Data processed by these functions are protected as defined for the application context. These issues are addressed by the requirement RE.Phase-1. The TOE only provides the tool to implement the policy defined in the context of the application.

Integrity check (FDP_SDI.1)

Table 18: Rational for integrity check requirement

Objective	TOE Security Functional Requirements	Security Requirements for the environment
O.Malfunction	- FDP_SDI.1 „Stored data integrity monitoring “	

The justification related to the security objective “Protection against Malfunction due to Environmental Stress (O.Malfunction)” is as follows:

The security functional requirement “Stored data integrity monitoring (FDP_SDI.1)” requires the implementation of a CRC checksum algorithm which detects integrity errors of the data stored in the memory. By this malfunction of the TOE by using corrupt data is prevented. Therefore FDP_SDI.1 is suitable to meet the security objective.

8.2.2 Dependencies of security functional requirements

Table 19: Dependency for cryptographic operation requirement

Security Functional Requirement	Dependencies	Fulfilled by security requirements
FCS_COP.1 (3DES)	FCS_CKM.1	Yes (by the environment)
	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) FCS_CKM.4 FMT_MSA.2	Yes (by the environment)
FCS_COP.1 (RSA)	FCS_CKM.1	Yes (additionally it can be fulfilled by the environment)
	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) FCS_CKM.4 FMT_MSA.2	Yes (by the environment)
FCS_CKM.1	FCS_COP.1 (or FCS_CKM.2)	Yes
	FCS_CKM.4 FMT_MSA.2	Yes (by the environment)

The dependencies FCS_CKM.1 (for 3DES), FDP_ITC.1 or FDP_ITC.2, FCS_CKM.4 and FMT_MSA.2 must be covered from the environment (the smartcard embedded software) and are addressed additionally by the requirement RE.Cipher. The dependency FCS_CKM.1 (for RSA) has to be fulfilled by the TOE. In addition the environment can fulfil it.

Table 20: Dependency for subset TOE security testing requirement

Security Functional Requirement	Dependencies	Fulfilled by security requirements
FPT_TST.2	FPT_AMT.1	See discussion below

The following discussion demonstrates how the dependencies defined by Part 2 of the Common Criteria for the requirement FPT_TST.2 are satisfied. The dependency defined in the Common Criteria is Abstract machine testing (FPT_AMT.1).

Part 2 of the Common Criteria explains that „the term »underlying abstract machine« typically refers to the hardware components upon which the TSF has been implemented. However, the phrase can also be used to refer to an underlying, previously evaluated hardware and software combination behaving as a virtual machine upon which the TSF relies.“

The TOE is already a platform representing the lowest level in a Smartcard. There is no lower or »underlying abstract machine« used by the TOE which can be tested. There is no need to perform testing according to FPT_AMT.1 and the dependency in the requirement FPT_TST.2 is therefore considered to be satisfied.

Table 21: Dependency for Memory Access Control Policy requirement

Security Functional Requirement	Dependencies	Fulfilled by security requirements
FDP_ACC.1	FDP_ACF.1	Yes
FDP_ACF.1	FDP_ACC.1	Yes
	FMT_MSA.3	Yes
FMT_MSA.3	FMT_MSA.1	Yes
	FMT_SMR.1	See discussion below
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	Yes
	FMT_SMR.1	See discussion below
	FMT_SMF.1	Yes

The dependency FMT_SMR.1 introduced by the two components FMT_MSA.1 and FMT_MSA.3 is considered to be satisfied because the access control specified for the intended TOE is not role-based but enforced for each subject. Therefore, there is no need to identify roles in form of a security functional requirement FMT_SMR.1.

Table 22: Dependency for integrity check requirement

Security Functional Requirement	Dependencies	Fulfilled by security requirements
FDP_SDI.1	none	N/A

FDP_SDI.1 has no dependency which has to be satisfied.

8.2.3 Rationale for the Assurance Requirements and the Strength of Function Level

The chosen assurance level EAL 5 augmented determines the assurance requirements. In Table 11 the different assurance levels are shown as well as the augmentations. The augmentations are not changed compared to the Protection Profile

The assurance level EAL5 and the augmentation with the requirements ALC_DVS.2, AVA_MSU.3, and AVA_VLA.4 were chosen in order to meet assurance expectations. An assurance level of EAL5 is required for this type of TOE since it is intended to defend against highly sophisticated attacks without a protected environment. This evaluation assurance level was selected since it provides even formal evidence on the conducted vulnerability assessment. In order to provide a meaningful level of assurance that the TOE provides an adequate level of defence against such attacks, the evaluators have access to all information regarding the TOE including the low level design and source code.

The rational for the strength of function level from the Smartcard IC Platform Protection Profile is used as the level is not changed.

8.3 Security Requirements are Mutually Supportive and Internally Consistent

In addition to the discussion in section 7.3 of the Smartcard IC Platform Protection Profile the security functional requirement FCS_COP.1 is introduced. The security functional requirements required to meet the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced also protect the cryptographic algorithms implemented according

to the security functional requirement FCS_COP.1. Therefore, these security functional requirements support the secure implementation and operation of FCS_COP.1.

The security functional requirements required to meet the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced also protect the self-test functions implemented according to the security functional requirement FPT_TST.2. Therefore, these security functional requirements support the secure implementation and operation of FPT_TST.2.

The requirement FPT_TST.2 allows testing of some security mechanisms including the correct operation of the sensors after delivery. These tests can be executed by the Smartcard Embedded Software. This is not in contradiction to the requirement FPT_SEP.1 (see refinement in [PP]: sensors should be protected from interference of the Smartcard Embedded Software) since the Smartcard Embedded Software only executes the test. The test is implemented in the TOE and there is no possibility to influence the sensors itself.

The security functional requirements required to meet the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced also protect the area based memory access control function implemented according to the security functional requirement described in the security functional requirement FDP_ACC.1 with reference to the Memory Access Control Policy and details given in FDP_ACF.1. Therefore, those security functional requirements support the secure implementation and operation of FDP_ACF.1 with its dependent security functional requirements.

The requirement FDP_SDI.1 allows the detection of integrity errors of data stored in memory and meets the security objective O.Malfunction. The requirements FRU_FLT.2, FPT_FLS.1, and FPT_SEP.1 which also meet this objective are independent from FDP_SDI.1 since they deal with the sensors monitoring the operating state and not the memory content directly.

9 References

9.1 Documents and User Guidance

Table 23: User guidance

[Status]	Status report, List of all available user guidance including application notes	
[DataBook]	Data Book, SLE66CxxxP	

Versions of these documents will be defined at the end of the evaluation and listed in the certification report

9.2 Literature

Table 24: Table of Criteria

[ProtectionProfile]	Smartcard IC Platform Protection Profile	BSI-PP-0002; Version 1.0, July 2001
[AIS31]	Functionality classes and evaluation methodology for physical random number generators	AIS31, Version1, 25.9.2001
[CC]	Common Criteria for Information Technology Security Evaluation	Version 2.1, August 1999
[ALGO]	*Bundesanzeiger Nr. 59*, *Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signatur-verordnung (Übersicht über geeignete Algorithmen),* Regulierungsbehörde für Telekommunikation und Post	30 März 2005
[ETSI]	*Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms*	ETSI TS 102 176-1 V1.2.1 (2005-07)

9.3 List of abbreviations

API	Application Programming Interface
CC	Common Criteria
CI	Chip Identification Mode (STS-CI)
CIM	Chip Identification Mode (STS-CI), same as CI
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
DPA	Differential Power Analysis
DFA	Differential Failure Analysis
EEPROM	Electrically Erasable and Programmable Read Only Memory
EMA	Electro magnetic analysis

HW	Hardware
IC	Integrated Circuit
ID	Identification
I/O	Input/Output
IRAM	Internal Random Access Memory
ITSEC	Information Technology Security Evaluation Criteria
M	Mechanism
MED	Memory Encryption and Decryption
MMU	Memory Management Unit
MOVC	MOVe Code
O	Object
OS	Operating system
PCD	Proximity Coupling Device
PICC	Proximity Integrated Chip Card
PLL	Phase Locked Loop
PROM	Programmable Read Only Memory
RAM	Random Access Memory
RMS	Resource Management System
RNG	Random Number Generator
ROM	Read Only Memory
S	Subject
SF	Security function
SFR	Special Function Register, as well as Security Functional Requirement The specific meaning is given in the context
SPA	Simple power analysis
STS	Self Test Software
SW	Software
SO	Security objective
T	Threat
TM	Test Mode (STS)
TOE	Target of Evaluation
UM	User Mode (STS)
UMC	Production site in Taiwan
XRAM	eXtended Random Access Memory

9.4 Glossary

Application Program/Data	Software which implements the actual TOE functionality provided for the user or the data required for that purpose
Threat	Action or event that might prejudice security

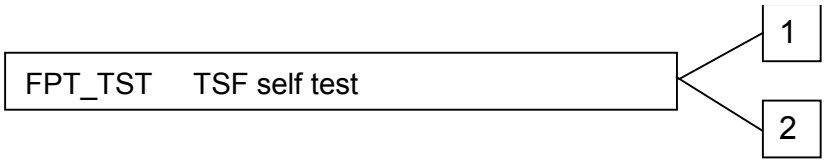
Operating System	Software which implements the basic TOE actions necessary for operation
Central Processing Unit	Logic circuitry for digital information processing
Chip → Integrated Circuit	Chip Identification Data Data stored in the EEPROM containing the chip type, lot number (including the production site), die position on wafer and production week and data stored in the ROM containing the STS version number
Chip Identification Mode	Operational status phase of the TOE, in which actions for identifying the individual chip by transmitting the Chip Identification Data take place
Smart Card	Plastic card in credit card format with built-in chip
Controller	IC with integrated memory, CPU and peripheral devices
Cyclic Redundancy Check	Process for calculating checksums for error detection
Electrically Erasable and Programmable Read Only Memory (EEPROM)	Nonvolatile memory permitting electrical read and write operations
End User	Person in contact with a TOE who makes use of its operational capability
Firmware	Part of the software implemented as hardware
Hardware	Physically present part of a functional system (item)
Integrated Circuit	Component comprising several electronic circuits implemented in a highly miniaturized device using semiconductor technology
Internal Random Access Memory	RAM integrated in the CPU
Mechanism	Logic or algorithm which implements a specific security function in hardware or software
Memory Encryption and Decryption	Method of encoding/decoding data transfer between CPU and memory
Microcontroller → Controller	Microprocessor → CPU
Move Code	Instruction in the CPU's instruction set for transferring program memory contents to an internal register
Object	Physical or non-physical part of a system which contains information and is acted upon by subjects
Programmable Read Only Memory	Non-volatile memory which can be written once and then only permits read operations
Random Access Memory	Volatile memory which permits write and read operations
Random Number Generator	Hardware part for generating random numbers
Read Only Memory	Non-volatile memory which permits read operations only
Resource Management System	Part of the firmware containing EEPROM programming routines
Self Test Software	Part of the firmware with routines for controlling the operating state and testing the TOE hardware

Security Function	Part(s) of the TOE used to implement part(s) of the security objectives
Security Target	Description of the intended state for countering threats
Software	Information (non-physical part of the system) which is required to implement functionality in conjunction with the hardware (program)
Memory	Hardware part containing digital information (binary data)
Subject	Entity, generally in the form of a person, who performs actions
Target of Evaluation	Product or system which is being subjected to an evaluation
Test Mode	Operational status phase of the TOE in which actions to test the TOE hardware take place
User Mode	Operational status phase of the TOE in which actions intended for the user takes place

10 Definition of the Security Functional Component FPT_TST.2

The following additions are made to „TSF self test (FPT_TST)“ in Common Criteria:

Component levelling



FPT_TST.1 TSF testing provides the ability to test TSFs correct operation. These tests may be performed at start-up, periodically, at the request of the authorised user, or when other conditions are met. It also provides the ability to verify the integrity of TSF data and executable code.

FPT_TST.2 Subset TOE security testing, provides the ability to test the correct operation of particular security functions or mechanisms. These tests may be performed at start-up, periodically, at the request of the authorised user, or when other conditions are met. It also provides the ability to verify the integrity of TSF data and executable code.

The security functional component family “Subset TOE testing (FPT_TST.2)” is specified as follows.

FPT_TST.2	Subset TOE testing
Hierarchical to:	No other components.
FPT_TST.2.1	The TSF shall run a suite of self tests [selection: during initial start-up, periodically during normal operation, at the request of the authorised user, and/or at the conditions [assignment: conditions under which self test should occur] to demonstrate the correct operation of [assignment: functions and/or mechanisms].
Dependencies:	FPT_AMT.1 Abstract machine testing