PUBLIC

Infineon Technologies AG

Chip Card and Security

Evaluation Documentation

Security Target Lite

M9900 A21

Version	**1.1**
Date	**2012-07-31**
Author	**Jürgen Noller**

REVISION HISTORY

1.1	2012-07-31 Finale Version

TABLE OF CONTENTS

1 SECURITY TARGET INTRODUCTION (ASE_INT) 5

1.1 SECURITY TARGET AND TARGET OF EVALUATION REFERENCE 5
1.2 TARGET OF EVALUATION OVERVIEW 7

2 TARGET OF EVALUATION DESCRIPTION 9

2.1 TOE DEFINITION 9
2.2 SCOPE OF THE TOE 12
2.2.1 Hardware of the TOE 12
2.2.2 Firmware and software of the TOE 13
2.2.3 Interfaces of the TOE 14
2.2.4 Guidance documentation 14
2.2.5 Forms of delivery 15
2.2.6 Production sites 15
2.2.7 TOE Configuration 15
2.2.8 TOE initialization with Customer Software 16

3 CONFORMANCE CLAIMS (ASE_CCL) 17

3.1 CC CONFORMANCE CLAIM 17
3.2 PP CLAIM 17
3.3 PACKAGE CLAIM 17
3.4 CONFORMANCE RATIONALE 18
3.5 APPLICATION NOTES 19

4 SECURITY PROBLEM DEFINITION (ASE_SPD) 20

4.1 THREATS 20
4.1.1 Additional Threat due to TOE specific Functionality 20
4.1.2 Assets regarding the Threats 21
4.2 ORGANIZATIONAL SECURITY POLICIES 22
4.2.1 Augmented Organizational Security Policy 22
4.3 ASSUMPTIONS 23
4.3.1 Augmented Assumptions 24

5 SECURITY OBJECTIVES (ASE_OBJ) 25

5.1 SECURITY OBJECTIVES FOR THE TOE 25
5.2 SECURITY OBJECTIVES FOR THE DEVELOPMENT AND OPERATIONAL ENVIRONMENT 26
5.2.1 Clarification of "Usage of Hardware Platform (OE.Plat-Appl)" 26
5.2.2 Clarification of "Treatment of User Data (OE.Resp-Appl)" 27
5.2.3 Clarification of "Protection during Composite product manufacturing (OE.Process-Sec-IC)" 27
5.3 SECURITY OBJECTIVES RATIONALE 27

6 EXTENDED COMPONENT DEFINITION (ASE_ECD) 29

6.1 COMPONENT "SUBSET TOE SECURITY TESTING (FPT_TST)" 29
6.2 DEFINITION OF FPT_TST.2 29
6.3 TSF SELF TEST (FPT_TST) 30
6.4 FAMILY "GENERATION OF RANDOM NUMBERS (FCS_RNG)" 30
6.5 DEFINITION OF FCS_RNG.1 31

7 SECURITY REQUIREMENTS (ASE_REQ) 32

7.1 TOE SECURITY FUNCTIONAL REQUIREMENTS 32

7.1.1 Extended Components FCS_RNG.1 and FAU_SAS.1 33
7.1.2 Subset of TOE testing 34
7.1.3 Memory access control 35
7.1.4 Support of Cipher Schemes 39
7.1.5 Data Integrity 40
7.2 TOE SECURITY ASSURANCE REQUIREMENTS 42
7.2.1 Refinements 43
7.3 SECURITY REQUIREMENTS RATIONALE 43
7.3.1 Rationale for the Security Functional Requirements 43
7.3.2 Rationale of the Assurance Requirements 48

8 TOE SUMMARY SPECIFICATION (ASE_TSS) 50

8.1 SF_DPM: DEVICE PHASE MANAGEMENT 50
8.2 SF_PS: PROTECTION AGAINST SNOOPING 50
8.3 SF_PMA: PROTECTION AGAINST MODIFYING ATTACKS 50
8.4 SF_PLA: PROTECTION AGAINST LOGICAL ATTACKS 50
8.5 SF_CS: CRYPTOGRAPHIC SUPPORT 50
8.6 ASSIGNMENT OF SECURITY FUNCTIONAL REQUIREMENTS TO TOE'S SECURITY FUNCTIONALITY 51
8.7 SECURITY REQUIREMENTS ARE INTERNALLY CONSISTENT 52

9 REFERENCES 53

9.1 LITERATURE 53

10 LIST OF ABBREVIATIONS 54

11 GLOSSARY 56

List of tables:

Table 1: Identification 6
Table 2: Options to implement user software at Infineon production premises 16
Table 3: Augmentations of the assurance level of the TOE 17
Table 4: Threats according PP [1] 20
Table 5: Additional threats due to TOE specific functions and augmentations 21
Table 6: Organizational Security Policies according PP [1] 22
Table 7: Assumption according PP [1] 23
Table 8: Objectives for the TOE according to PP [1] 25
Table 9: Additional objectives due to TOE specific functions and augmentations 26
Table 10: Security objectives for the environment according to PP [1] 26
Table 11: Security Objective Rationale 27
Table 12: Security functional requirements defined in PP [1] 32
Table 13: Augmented security functional requirements 32
Table 14: Assurance components 43
Table 15: Rational for additional SFR in the ST 44
Table 16: Dependency for cryptographic operation requirement 47
Table 17: Mapping of SFR and SF 51

1 Security Target Introduction (ASE_INT)

1.1 Security Target and Target of Evaluation Reference

The title of this document is Security Target (ST) M9900 A21 option and comprises the Infineon Technologies Smart Card IC (Security Controller) M9900 A21 with specific IC dedicated software.

The target of evaluation (TOE) M9900 A21 is described in the following. The Security Target has the revision 1.1 and is dated 2012-07-31.

The Target of Evaluation (TOE) is an Infineon smart card IC (Security Controller) M9900 A21 with specific IC dedicated software (firmware). The design step is A21.

The Security Target is based on the Protection Profile “Smartcard IC Platform Protection Profile” [1].

The Protection Profile and the Security Target are built in compliance with Common Criteria v3.1.

The ST takes into account all relevant current final interpretations.

Table 1: Identification

	Version	Date	Registration
Security Target	1.1	2012-07-31	M9900 A21
Target of Evaluation	A21		M9900 with Firmware Identifier 80001140 and external Flash-memory (optional) and Guidance documentation
	Revision 2.0 ID021310 Rev. 1.8 Edition July 31, 2012 Rev.1.0	2012-03-26 12. February 2010 2012-05-24 May 10, 2012 2012-07-31 2012-05-09	SLE97 Hardware Reference Manual ARMv7-M Architecture Reference Manual, ARM DDI 0403D ID021310, ARM Limited SLE 97 Programmer´s Reference User´s Manual SLE97 / SLC14 Family Production and Personalization User´s Manual M9900 Security Guidelines User´s Manual M9900 Errata Sheet
	1.0	2007-06-15	Security IC Platform Protection Profile PP0035
Common Criteria	3.1 Revision 3	2009-July	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model CCMB-2009-07-001 Part 2: Security functional requirements CCMB-2009-07-002 Part 3: Security Assurance Components CCMB-2009-07-003

A customer can identify the TOE and its configuration (for details see chapter 2.2.7) using the Non-ISO ATR. The TOE answers the Non-ISO-ATR with a Generic Chip Identification Mode (GCIM). This GCIM outputs the chip identification data, as defined in the SLE97 Family – Hardware Reference Manual [7]. The identification data and configuration details are described in the confidential Security Target [16] and in the SLE97 Programmer´s Reference User´s Manual [11].

1.2 Target of Evaluation overview

The TOE comprises the Infineon Technologies AG security controller M9900 with specific IC dedicated software.

The TOE is a member of the Infineon Technologies AG security controller family SLE97 meeting high requirements in terms of performance and security. The SLE97 family has been developed with a modular concept and different memory configurations, sets of peripherals and interfaces as well as different security features to satisfy market requirements. A summary product description is given in this Security Target (ST).

The TOE offer all functions that are both required and useful in security systems, and integrated peripherals that are typically needed in chipcard applications, such as information security, identification, access control, GSM and UMTS projects, electronic banking, digital signature and multi-application cards, ID cards, transportation and e-purse applications.

The TOE implements a dedicated security 32-bit RISC CPU designed on the basis of the ARMv7_M architecture designed in 90 nm CMOS technology. The integrated peripheral combine enhanced performance and optimized power consumption for a minimized die size to make the SLE97 controllers ideal for chipcard applications. The TOE offer a wide range of peripherals, including a UART (using the ISO interface), four timers, two watchdogs, a CRC module, a true RNG (TRNG), coprocessors for symmetric (e.g. DES, AES) and asymmetric (e.g. RSA, EC) cryptographic algorithms. Additionally a range of communication interfaces, such as GPIO, I2C, SWP, USB, SSC/SPI and a Mifare-compatible Interface are offered to provide maximum flexibility in terms of simultaneously communication ability.

The TOE provides a real 32-bit CPU-architecture and is compatible to the ARMv7-M instruction set architecture. The major components of the core system are the 32-bit CPU as a variant of the ARM Secure Core SC300, the Cache system, the Memory Protection Unit and the Memory Encryption/Decryption Unit. The TOE implements a full 32-bit addressing with up to 4 GByte linear addressable memory space, a simple scalable memory management concept and a scalable stack size. The flexible memory concept is built on the non volatile memory, respectively SOLID FLASH™[1]. For the SOLID FLASH™ the Unified Channel Programming (UCP) memory technology is used. Additionally an optional external Flash-memory connected via the SPI interface is available.

The TOE provides the low-level firmware components Boot System (BOS) and Resource Management System (RMS) and the high-level firmware Flash Loader (FL) and Mifare-compatible software. The RMS firmware providing some functionality via an API to the Smartcard Embedded Software contains for example SOLID FLASH™ service routines and functionality for the tearing save write into the SOLID FLASH™. The BOS firmware is used for test purposes during start-up and the FL allows downloading of user software to the NVM during the manufacturing process. The BOS is implemented in a separated Test-ROM being part of the TOE. The Mifare-compatible software includes support for the Mifare-compatible card as well as support to ease the implementation of the reader functionality.

The two cryptographic co-processors serve the need of modern cryptography: The symmetric co-processor (SCP) combines both AES and Triple-DES with dual-key or triple-key hardware acceleration. The Asymmetric Crypto Co-processor, called Crypto2304T in the following, supports RSA-2048 bit (4096-bit with CRT) and Elliptic Curve (EC) cryptography with high performance.

A True Random Number Generator (TRNG) specially designed for smart card applications is implemented. The TRNG fulfils the requirements from the functionality class PTG2 of the AIS31 and produces genuine random numbers which then can be used internally or by the user software.

To fulfill the high security standards for smartcards today and also in the future, this TOE utilizes an integral security concept comprising countermeasure mechanisms specially designed against

[1] SOLID FLASH™ is an Infineon Trade Mark and stands for Flash EEPROM technology.

possible attack scenarios. The TOE provide a robust set of sensors for the purpose of monitoring proper chip operating conditions and detecting fault attack scenarios. The sensors are complemented with digital error detection mechanisms such as parities, error detection codes and instruction stream signatures. Probing and forcing attacks will be counteracted by the I2-Shield approach, implemented by an Infineon-specific shielding combined with secure wiring of security critical signals, partly masking of security critical signals and by encryption of all memories inside the chip (RAM, ROM, NVM). A decentralized alarm propagation and system deactivation principle is implemented, further decreasing the risk of manipulating and tampering. Additionally, an online check of the security mechanisms is available by using the User Mode Security Life Control (UMSLC). Side-channel attacks (e.g. Timing Attack, SPA, DPA, EMA) are typically defeated using a combination of hardware and software mechanisms, for this the TOE provides several supporting features e.g. trash register writes and instruction interrupt prevention. The Instruction Stream Signature Checking (ISS) is a powerful countermeasure against fault attacks that try to manipulate the execution sequence of the instruction stream. All executed instructions are hashed in the CPUs signature register and the hardware automatically checks the fitting of the values.

In this security target the TOE 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 and the security policy are defined, as well as the security requirements. These security requirements are built up of the security functional requirements as part of the security policy and the security assurance requirements. These are the steps during the evaluation and certification showing that the TOE meets the targeted requirements. In addition, the functionality of the TOE matching the requirements is described.

The assets, threats, security objectives and the security functional requirements are defined in this Security Target and in [1] and are referenced here. These requirements build up a minimal standard common for all Smartcards.

The security 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].

2 Target of Evaluation Description

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 [1] as it belongs to the specific TOE.

2.1 TOE Definition

The TOE consists of smart card ICs (Security Controllers) meeting high requirements in terms of performance and security. They are manufactured by Infineon Technologies AG in a 90 nm CMOS-technology (L90). This TOE is intended to be used in smart cards for particularly security-relevant applications and for its previous use as developing platform for smart card operating systems according to the lifecycle model from [1]

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 consists of a core system, memories, co-processors, security peripherals, control logic and peripherals. The major components of the core system are the 32-bit CPU (Central Processing Unit), the MPU (Memory Protection Unit), the MED (Memory Encryption/Decryption Unit), the Nested Vectored Interrupt Controller (NVIC), the Instruction Stream Signature Checking (ISS) and the Cache system. The TOE contains the co-processors for RSA/EC (Crypto2304T) and DES/AES (SCP) processing, a CRC module and the peripherals random number generator, four timers and two watchdog timers and several external interface services. All data of the memory block is encrypted, RAM and ROM are equipped with an error detection code (EDC) and the SOLID FLASH™ is equipped in addition with an error correction code (ECC).
The memories are connected to the Core with the AXI™ Memory Bus and the peripherals are connected with the APB™ Peripheral Bus.

The Analog Modules (ANA) serve for operation within the specified range and manage the alarms. A set of sensors (temperature sensor, backside light detector, glitch sensor) is used to detect excessive deviations from the specified operational range and serve for robustness of the TOE and the UMSLC function can be used to test the alarm lines.

The CPU is compatible with the instruction set of the ARMv7_M architecture. Despite its compatibility the CPU implementation is entirely proprietary and not standard.

The CPU accesses the memory via the integrated Memory Encryption and Decryption unit (MED). The memory model of the TOE provides two distinct, independent levels. Additionally up to eight regions can be defined with different access rights controlled by the Memory Protection Unit (MPU). Errors in RAM and ROM are automatically detected (EDC, Error Detection Code), in terms of the SOLID FLASH™ errors are detected and 1-Bit-errors are also corrected (ECC, Error Correction Code).

The controller of this TOE store both code and data in a linear 4-GByte memory space, allowing direct access without the need to swap memory segments in and out of memory using a memory protection unit.
Additionally an optional external Flash-memory (EXF) connected via the SSC/GPIO interfaces is available. The data stored in the external Flash-memory are not protected as the external Flash-memory is not part of the security functional requirements (SFR) of the TOE and not in the scope of the evaluation.

The CACHE is a high-speed memory-buffer located between the CPU and the (external) main memories holding a copy of some of the memory contents to enable access, which is considerably faster than retrieving the information from the main memory. In addition to its fast access speed,

the CACHE also consumes less power than the main memories. The CACHE is equipped with a integrity check to verify the contents of the cache memories.

A True Random Number Generator (TRNG) specially designed for smart card applications is implemented. The TRNG fulfils the requirements from the functionality class PTG2 of the AIS31 and produces genuine random numbers which then can be used internally or by the user software.

The implemented sleep mode logic (clock stop mode per ISO/IEC 7816-3) is used to reduce the overall power consumption. The timers 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 controller and the terminal interface to be operated independently.

The Clock Unit (CLKU) supplies the clocks for all components of the TOE. It generates the system clock and an approximately 1MHz clock for the timers. The 1MHz clock is derived from an internal oscillator, while the system clock may either be based on the internal oscillator clock (internal clock mode) or on an external clock (external clock mode). Additionally a sleep mode is available. When operating in the internal clock mode the system frequency can be configured by the user software combined with the current limitation functionality. In the external clock mode the clock is derived from the external clock and a parameter with the range of 1 to 8. The system frequency may be 1 up to 8 times the externally applied frequency but is of course limited to the maximum system frequency and can be combined with the current limitation function.

Two co-processors for cryptographic operations are implemented on the TOE. The Crypto2304T for calculation of asymmetric algorithms like RSA and Elliptic Curve (EC) and the Symmetric Cryptographic Processor (SCP) for dual-key or triple-key triple-DES and AES calculations. These co-processors are especially designed for smart card applications with respect to the security and power consumption. The SCP module computes the complete DES algorithm within a few clock cycles and is especially designed to counter attacks like DPA, EMA and DFA. The Crypto2304T module provides basic functions for the implementation of RSA and EC cryptographic libraries.

Note that this TOE can come with both crypto co-processors accessible, or with a blocked SCP or with a blocked Crypto2304T, or with both crypto co-processors blocked. The blocking depends on the customer demands prior to the production of the hardware. No accessibility of the deselected cryptographic co-processors is without impact on any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use the cryptographic co-processors.

The cyclic redundancy check (CRC) module is a 16-bit checksum generator, which shall not be used for security-critical data. The TOE includes two timer modules each with two 16-bit general purpose timers. The timer module can be used also as watchdog timer to monitor system operation for possible timeouts and to check the correct order of operation.

A Interface Management module, located in the System Module (SYS), provides the TOE with the possibility to maintain two or more data interfaces simultaneously. The TOE is provided with, dependent on the configuration, different peripherals and interfaces as the Universal Serial Bus (USB), the SWP Slave Peripheral (SWP), the Synchronous Serial Communication (SSC), which provides the serial Peripheral Interface (SPI), the GPIO module (GPIO), the Inter-Integrated Cirquit Module (I2C) and the Standard ISO Interface (PAD) to satisfy the different market requirements.

The BOS (Boot Software) and the RMS (Resource Management System) compose the TOE firmware stored in the ROM and the patches hereof in the SOLID FLASH™. All mandatory functions for start-up and internal testing (BOS) are protected by a dedicated hardware firewall. Additionally two levels are provided, the privileged level and the user level, both are protected by a hardwired Memory Protection Unit (MPU) setting. The RMS is accessible in privileged level only. The FL (Flash Loader) and the Mifare-compatible software compose the TOE software stored in the SOLID FLASH™. The FL allows downloading of user software to the NVM during the manufacturing process and can be completely deactivated. The Mifare-compatible software includes support for the Mifare-compatible card as well as support to ease the implementation of the reader functionality.

The user software can be implemented in various options depending on the user's choice and described in chapter 1.1. Thereby the user software can be implemented the NVM or coming without user software. In the latter case, the user downloads his entire software on his own using the Flash Loader software.

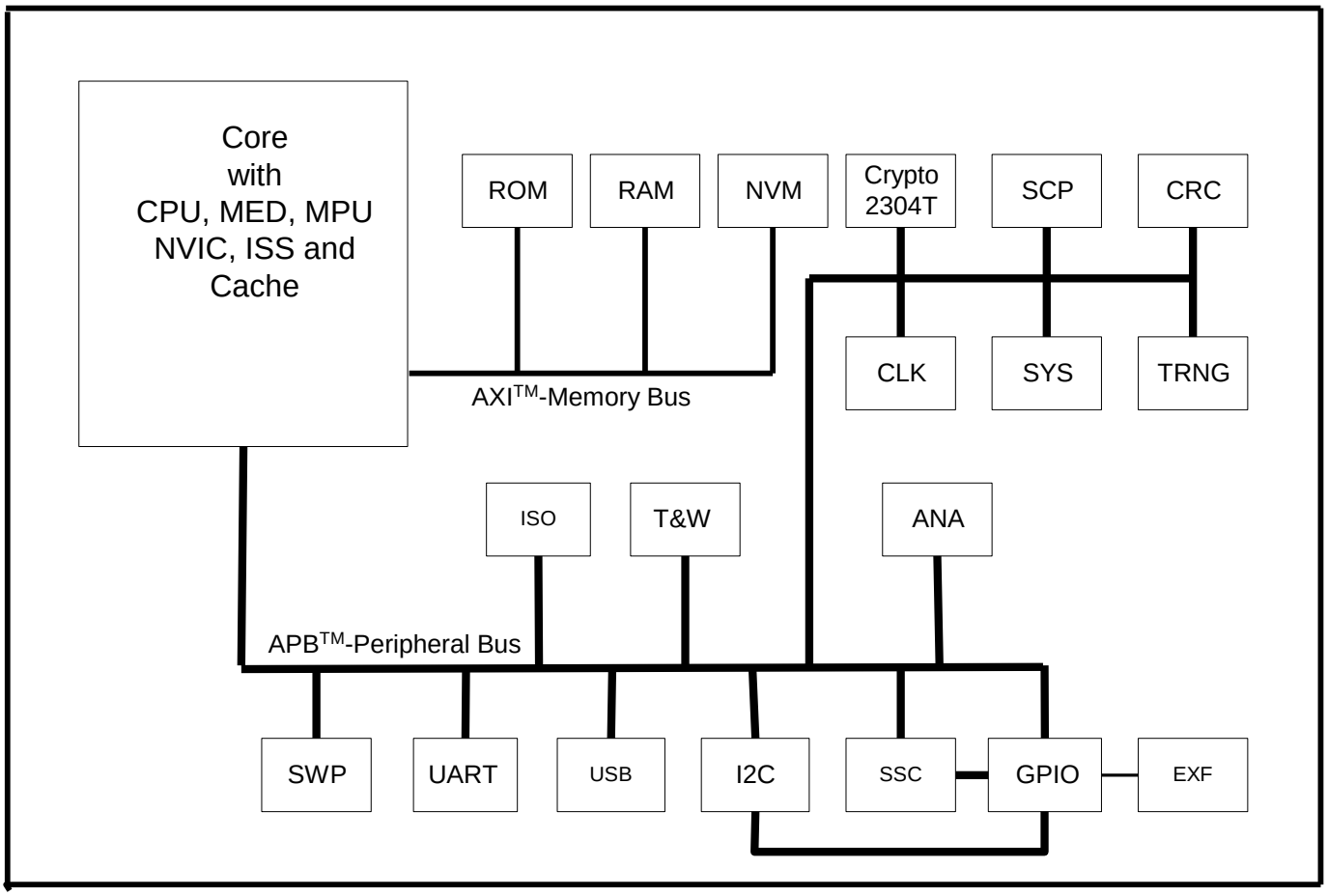
The TOE uses also Special Function Registers SFR. These SFR registers are used for general purposes and chip configuration. These registers are located in the SOLID FLASH™ as configuration area page.

An intelligent shielding algorithm finishes the upper layers above security critical signals and wires, finally providing the so called "I2-shield".

The TOE with its integrated security features meets the requirements of all smart card applications such as information integrity, access control, mobile telephone and identification, 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 improved performance, optimized power consumption, at minimal chip size while implementing high security.

Figure 1: Block diagram of the TOE



Core	Core System	ROM	Read Only Memory
NVM	SOLID FLASH™ memory	RAM	Random Access Memory
CLK	Clock Unit	SYS	System Module
Crypto	Crypto2304T	SCP	Symmetric Crypto Processor
CRC	Cyclic Redundancy Check	TRNG	True Random Number Generator
T&W	Timer and Watchdog	UART	UART

I2C	Inter Integrated Chip	GPIO	General Purpose IO
SSC	Synchronous Serial Communication	SWP	Single Wire Protocol
USB	Universal Serial Bus	ANA	Analog Units
ISO	Standard Interface	ISO	Standard ISO Interface
EXF	External Flash-memory (optional)		

2.2 Scope of the TOE

The TOE comprises three parts:

- Hardware of the smart card security controller
- Associated firmware and software
- Documents.

The hardware configuration options and configuration methods are described in section 1.1.
The second part of this TOE includes the associated firmware and software required for operation. The TOE can be delivered in various configurations, achieved by means of blocking and depending on the customer order.

The documents as described in section 2.2.4 and listed in Table 1, are supplied as user guidance. All product derivates of this TOE, including all configuration possibilities differentiated by the GCIM data and the configuration information output, are manufactured by Infineon Technologies AG. In the following descriptions, the term “manufacturer” stands short for Infineon Technologies AG, the manufacturer of the TOE. The Smartcard Embedded Software respectively user software is not part of the TOE. New configurations can occur at any time depending on the user blocking or by different configurations applied by the manufacturer. In any case the user is able to clearly identify the TOE hardware, its configuration and proof the validity of the certificate independently, meaning without involving the manufacturer. The various blocking options, as well as the means used for the blocking, are done during the manufacturing process or at user premises. Entirely all means of blocking and the, for the blocking involved firmware respectively software parts, used at Infineon Technologies AG and/or the user premises, are subject of the evaluation. All resulting configurations of a TOE derivative are subject of the certificate. All resulting configurations are either at the predefined limits or within the predefined configuration ranges.

2.2.1 Hardware of the TOE

The hardware part of the TOE (see Figure 1) as defined in [1] is comprised of:

Core System

32-bit CPU implementation of ARM Secure Core SC300 based on ARMv7-M Instruction set architecture including the Instruction Stream Signature Checking (ISS)

CACHE for code and data buffering

Memory Encryption/Decryption Unit (MED) and Error Detection Unit

Memory Protection Unit (MPU)

Nested Vectored Interrupt Controller (NVIC)

Memories

Read-Only Memory (ROM, for internal firmware)

Random Access Memory (RAM)

SOLID FLASH™ memory (NVM)

External Flash-memory (EXF, optional)

Note that the TOE has implemented a SOLID FLASH™ memory module. Parts of this memory module are configured to work as an EEPROM.

Peripherals

Universal Asynchronous Receiver/Transmitter (UART)

Single-Wire Protocol (SWP) with Mifare-compatible interface

Inter Integrated Circuite (I2C) interface

General Purpose Input Output (GPIO)

Synchronous Serial Communication (SSC) which provides the Serial Peripheral Interface (SPI)

Universal Serial Bus (USB) interface

Standard ISO Interface (PAD)

True Random Number Generator (TRNG)

Timers and Watchdog including a checkpoint register (T&W)

System Module (SYS)

Clock Unit (CLK)

Coprocessors

Crypto2304T co-processor for asymmetric algorithms like RSA and EC (Crypto, optional)

Symmetric Crypto co-processor for 3DES and AES Standards (SCP, optional)

Checksum module (CRC)

Analog Module (ANA)

Glitch Sensor

Temperature Sensor

Backside Light Detector

User Mode Security Life Control (UMSLC)

Buses

AXI™ Memory Bus

APB™ Peripheral Bus

2.2.2 Firmware and software of the TOE

The entire firmware and software of the TOE consists of different parts:

One part comprises the RMS routines for SOLID FLASH™ programming and security functions test (Resource Management System, IC Dedicated Support Software in PP [1]). The RMS routines are stored from Infineon Technologies AG in the ROM.

The second part is the BOS, consisting of test and initialization routines (Boot System, IC Dedicated Test Software in PP [1]). The BOS routines are stored in the especially protected test ROM and are not accessible for the user software.

The third part is the Flash Loader, a piece of software located in the ROM and allowing downloading the user software or parts of it to the SOLID FLASH™ memory. After completion of the download the Flash Loader can be permanently deactivated by the user.

The fourth part is the Mifare-compatible Interface routines called via RMS routines if the Mifare-compatible interface option is active. Note that the Mifare-compatible Interface portion is always

present but deactivated in case of the non-Mifare compatible Interface derivates. Thus the user interface is identically in both cases and subsequently the Mifare-compatible Interface routines can be called in each of the derivates. In case Mifare-compatible Interface routines are called in derivates without Mifare-compatible Interface a dedicated error code is returned and in case of the Mifare-compatible Interface derivate the according function is performed.

2.2.3 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:
  - The five ISO 7816 pads consist particularly of the contacted RES, I/O, CLK lines and supply lines VCC and GND. The contact based communication is according to ISO 7816/ETSI/EMV.
    The I2C communication can be driven via the ISO 7816 pads. In this case no other communication using the ISO 7816 pads is possible.
  - The GPIO interface consists of 4 pads which can be individually configured and combined in various ways.
  - Also the I2C and the SSC/SPI communication can be exclusively driven via the GPIO pads. In this case no other communication using the GPIO pads is possible.
  - The USB interface is build out of two dedicated pads for data communication and two pads used from the ISO 7816 interface supplying power and ground.
  - The SWP interface is build out of one pad to support the SWP slave functionality.
- The data-oriented I/O interface to the TOE is formed by the I/O pad.
- 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 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 BOS test routine call, i.e. entry to test mode (OS-TM entry).

2.2.4 Guidance documentation

The guidance documentation consists

- SLE97 Hardware Reference Manual
- ARMv7-M Architecture Reference Manual, ARM Limited , ARM DDI 0403D ID021310, 12. February 2010
- SLE97 / SLC14 Family Production and Personalization User´s Manual
- SLE 97 Programmer´s Reference User´s Manual
- M9900 Security Guidelines User´s Manual
- M9900 Errata Sheet

Finally the certification report may contain an overview of the recommendations to the software developer regarding the secure use of the TOE. These recommendations are also included in the ordinary documentation.

2.2.5 Forms of delivery

The TOE can be delivered in form of bare dies, in form of plain wafers, in form of complete modules (wire bond module M4.x, provided as single chip wire bond or as stacked wire bond), or in one of the following an IC cases: MFC5.8 (FCOS), PG-VQFN-8-1, PG-VQFN-32-13 (SMD). The form of delivery does not affect the TOE security and it can be delivered in any form, as long as the processes applied and sites involved have been subject of the appropriate audit.

The delivery can therefore be at the end of phase 3 or at the end of phase 4 which can also include pre-personalization steps according to PP [1]. 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 identical.

The delivery to the software developer (phase 2 ➔ phase 1) contains the development package and is delivered in form of documentation as described above, data carriers containing the tools and emulators as development and debugging tool.
Part of the software delivery could also be the Flash Loader program, provided by Infineon Technologies, running on the TOE and receiving via the UART interface the transmitted information of the user software to be loaded into the SOLID FLASH™ memory. The download is only possible after successful authentication. The user software can also be downloaded in an encrypted way. In addition, the user can permanently block further use of the Flash Loader. Whether the Flash Loader program is present or not depends on the procurement order.

2.2.6 Production sites

The TOE may be handled in different production sites but the silicon of this TOE is produced in Dresden, Germany only, as listed below. To distinguish the different production sites of various products in the field, the site is coded into the Chip Ident Mode data. The exact coding of the chip identification data is described in [7], section Generic Chip Identification Mode.

The delivery measures are described in the ALC_DVS aspect.

2.2.7 TOE Configuration

This TOE is represented by various configurations called products, which are all derived from the equal hardware design M9900. The same mask is used to produce different products of the TOE. The first metal mask (called the M1 mask) contains the specific information to identify the TOE.

The M9900 product offers different configuration options, which a customer can choose. The mechanism to choose a configuration can be done by the following methods:

1. by product selection or dialog-based in Tools,
2. via Bill-per-Use (BpU) and Flash Loader (FL),

The degree of freedom for configuring the TOE is predefined by Infineon Technologies AG. The list of predefined TOE configurations is given in the Hardware Reference Manual [7], section 18.

All these possible TOE configurations equal and/or within the specified ranges are covered by the certificate.

Beside fix TOE configurations, which can be ordered as usual, this TOE implements optionally the so called Bill-Per-Use (BPU) ability. This solution enables the customer to tailor the product on his own to the required configuration by blocking parts of the chip on demand into the final configuration at his own premises, without further delivery or involving support by Infineon Technology AG. Customers, who are intended to use this feature receiving the TOE in a predefined configuration including the Flash Loader software, enhanced with the BPU blocking software. The blocking information is part of a chip configuration area and can be modified by customers using specific APDUs. Once a final blocking is done, further modifications are disabled.

The BPU software part is only present on the products which have been ordered with the BPU option. In all other cases this software is not present on the product.

2.2.8 TOE initialization with Customer Software

Beside the various TOE configurations further possibilities of how the user inputs his software on the TOE are in place. This provides a maximum of flexibility and for this an overview is given in the following table:

Table 2: Options to implement user software at Infineon production premises

1.	The user or/and a subcontractor downloads the software into the SOLID FLASH™ memory on his own. Infineon Technologies AG has not received user software and there are no user data in the ROM.	The Flash Loader can be activated or reactivated by the user or subcontractor to download his software in the SOLID FLASH™ memory.
2	The user provides software for the download into the SOLID FLASH memory to Infineon Technologies AG. The software is downloaded to the SOLID FLASH™ memory during chip production. There are no user data in the ROM.	The Flash Loader is deactivated.
3	The user provides software for the download into the SOLID FLASH™ memory to Infineon Technologies AG. The software is downloaded to the SOLID FLASH™ memory during chip production. There are no user data in the ROM	The Flash Loader is blocked afterwards but can be activated or reactivated by the user or subcontractor to download his software in the SOLID FLASH™ memory. Precondition is that the user has provided an own reactivation procedure in software prior chip production to Infineon Technologies AG.

The Generic Chip Identification Mode (GCIM) data of the TOE allows a unique identification of each TOE and provides several detailed production information. The Chip Identification Mode data is accessible by a non-ISO reset or can be read directly from the configuration area located at the NVM by the user operating system. The SLE97 Family - Hardware Reference Manual [7] gives a detailed description of the GCIM data.

3 Conformance Claims (ASE_CCL)

3.1 CC Conformance Claim

This Security Target (ST) and the TOE claim conformance to Common Criteria version v3.1 part 1 [2], part 2 [3] and part 3 [4].

Conformance of this ST is claimed for:
Common Criteria part 2 extended and Common Criteria part 3 conformant.

3.2 PP Claim

This Security Target is in **strict conformance** to the
Security IC Platform Protection Profile [1].

The Security IC Platform Protection Profile is registered and certified by the Bundesamt für Sicherheit in der Informationstechnik[2] (BSI) under the reference BSI-PP-0035, Version 1.0, dated 15.06.2007.

The security assurance requirements of the TOE are according to the Security IC Platform Protection Profile [1]. They are all drawn from Part 3 of the Common Criteria version v3.1.

The augmentations of the PP [1] are listed below.

Table 3: Augmentations of the assurance level of the TOE

Assurance Class	Assurance components	Description
Life-cycle support	**ALC_DVS.2**	Sufficiency of security measures
Vulnerability assessment	**AVA_VAN.5**	Advanced methodical vulnerability analysis

3.3 Package Claim

This Security Target does not claim conformance to a package of the PP [1].

The assurance level for the TOE is EAL5 augmented with the components ALC_DVS.2 and AVA_VAN.5.

[2] Bundesamt für Sicherheit in der Informationstechnik (BSI) is the German Federal Office for Information Security

3.4 Conformance Rationale

This security target claims strict conformance only to one PP, the PP [1].

The Target of Evaluation (TOE) is a typical security IC as defined in PP chapter 1.2.2 comprising:

- the circuitry of the IC (hardware including the physical memories),
- configuration data, initialisation data related to the IC Dedicated Software and the behaviour of the security functionality
- the IC Dedicated Software with the parts
- the IC Dedicated Test Software,
- the IC Dedicated Support Software.

The TOE is designed, produced and/or generated by the TOE Manufacturer.

Security Problem Definition:

Following the PP [1], the security problem definition is enhanced by adding an additional threat, an organization security policy and an augmented assumption. Including these add-ons, the security problem definition of this security target is consistent with the statement of the security problem definition in the PP [1], as the security target claimed strict conformance to the PP [1].

Conformance Rationale:

The augmented organizational security policy P.Add-Functions, coming from the additional security functionality of the cryptographic libraries, the augmented assumption A.Key-Function, related to the usage of key-depending function, and the threat memory access violation T.Mem-Access, due to specific TOE memory access control functionality, have been added. These add-ons have no impact on the conformance statements regarding CC [2] and PP [1], with following rational:

- The security target remains conformant to CC [2], claim 482 as the possibility to introduce additional restrictions is given.
- The security target fulfils the strict conformance claim of the PP [1] due to the application notes 5, 6 and 7 which apply here. By those notes the addition of further security functions and security services are covered, even without deriving particular security functionality from a threat but from a policy.

Due to additional security functionality, one coming from the cryptographic libraries - O.Add-Functions, and due to the memory access control - O.Mem-Access, additional security objectives have been introduced. These add-ons have no impact on the conformance statements regarding CC [2] and PP [1], with following rational:

- The security target remains conformant to CC [2], claim 482 as the possibility to introduce additional restrictions is given.
- The security target fulfils the strict conformance of the PP [1] due to the application note 9 applying here. This note allows the definition of high-level security goals due to further functions or services provided to the Security IC Embedded Software.

Therefore, the security objectives of this security target are consistent with the statement of the security objectives in the PP [1], as the security target claimed strict conformance to the PP [1].

All security functional requirements defined in the PP [1] are included and completely defined in this ST. The security functional requirements listed in the following are all taken from Common Criteria part 2 [3] and additionally included and completely defined in this ST:

- FDP_ACC.1 “Subset access control”
- FDP_ACF.1 “Security attribute based access control”
- FMT_MSA.1 “Management of security attributes”
- FMT_MSA.3 “Static attribute initialisation”
- 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
- FDP_SDI.2 “Stored data integrity monitoring and action

The security functional requirement

- FPT_TST.2 “Subset TOE security testing“(Requirement from [3])
- FCS_RNG.1 “Generation of Random Numbers”

is included and completely defined in this ST, section 6.

All assignments and selections of the security functional requirements are done in the PP [1] and in this security target in section 7.2.

The Assurance Requirements of the TOE obtain the Evaluation Assurance Level 5 augmented with the assurance components ALC_DVS.2 and AVA_VAN.5 for the TOE.

3.5 Application Notes

The functional requirement FCS_RNG.1 is a refinement of the FCS_RNG.1 defined in the Protection Profile [1] according to “Anwendungshinweise und Interpretationen zum Schema (AIS)” [15].

4 Security Problem Definition (ASE_SPD)

The content of the PP [1] applies to this chapter completely.

4.1 Threats

The threats are directed against the assets and/or the security functions of the TOE. For example, certain attacks are only one step towards a disclosure of assets while others may directly lead to a compromise of the application security. 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 PP [1] section 3.2.

The threats to security are defined and described in PP [1] section 3.2.

Table 4: Threats according PP [1]

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

4.1.1 Additional Threat due to TOE specific Functionality

The additional functionality of introducing sophisticated privilege levels and access control allows the secure separation between the operation system(s) and applications, the secure downloading of applications after personalization and enables multitasking by separating memory areas and performing access controls between different applications. Due to this additional functionality “area based memory access control” a new threat is introduced.

The Smartcard Embedded Software is responsible for its User Data according to the assumption “Treatment of User Data (A.Resp-Appl)”. However, the Smartcard Embedded Software may comprise different parts, for instance an operating system and one or more applications. In this case, such parts may accidentally or deliberately access data (including code) of other parts, which may result in a security violation.

The TOE shall avert the threat “Memory Access Violation (T.Mem-Access)” as specified below.

T.Mem-Access Memory Access Violation

Parts of the Smartcard Embedded Software may cause security violations by accidentally or deliberately accessing restricted data (which may include code) or privilege levels. Any restrictions are defined by the security policy of the specific application context and must be implemented by the Smartcard Embedded Software.

Table 5: Additional threats due to TOE specific functions and augmentations

T.Mem-Access	Memory Access Violation

For details see PP [1] section 3.2.

4.1.2 Assets regarding the Threats

The primary assets concern the User Data which includes the user data as well as program code (Security IC Embedded Software) stored and in operation and the provided security services. These assets have to be protected while being executed and or processed and on the other hand, when the TOE is not in operation.

This leads to four primary assets with its related security concerns:

- SC1 Integrity of User Data and of the Security IC Embedded Software (while being executed/processed and while being stored in the TOE's memories),
- SC2 Confidentiality of User Data and of the Security IC Embedded Software (while being processed and while being stored in the TOE's memories)
- SC3 Correct operation of the security services provided by the TOE for the Security IC Embedded Software.
- SC4 Continuous availability of random numbers

SC4 is an additional security service provided by this TOE which is the availability of random numbers. These random numbers are generated either by a true random number or a deterministic random number generator or by both, when a true random number is used as seed for the deterministic random number generator. Note that the generation of random numbers is a requirement of the PP [1].

To be able to protect the listed assets the TOE shall protect its security functionality as well. Therefore critical information about the TOE shall be protected. Critical information includes:

- logical design data, physical design data, IC Dedicated Software, and configuration data
- Initialisation Data and Pre-personalisation Data, specific development aids, test and characterisation related data, material for software development support, and reticles.

The information and material produced and/or processed by the TOE Manufacturer in the TOE development and production environment (Phases 2 up to TOE Delivery) can be grouped as follows:

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

as long as they are generated, stored, or processed by the TOE Manufacturer.

For details see PP [1] section 3.1.

4.2 Organizational Security Policies

The TOE has to be protected during the first phases of their lifecycle (phases 2 up to TOE delivery which can be after phase 3 or phase 4). Later on each variant of the TOE has to protect itself. The organisational security policy covers this aspect.

P.Process-TOE Protection during TOE Development and Production

An accurate identification must be established for the TOE. This requires that each instantiation of the TOE carries this unique identification.

The organisational security policies are defined and described in PP [1] section 3.3. Due to the augmentations of PP [1] an additional policy is introduced and described in the next chapter.

Table 6: Organizational Security Policies according PP [1]

P.Process-TOE	Protection during TOE Development and Production

4.2.1 Augmented Organizational Security Policy

Due to the augmentations of the PP [1] an additional policy is introduced.

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:

- Advanced Encryption Standard (AES)
- Triple Data Encryption Standard (3DES)

Note 1:
This TOE can come with both crypto co-processors accessible, or with a blocked SCP or with a blocked Crypto2304T, or with both crypto co-processors blocked. The blocking depends on the customer demands prior to the production of the hardware. In case the SCP is blocked, no AES and 3DES computation supported by hardware is possible. No accessibility of the deselected cryptographic co-processors is without impact on any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use the cryptographic co-processors.

End of note.

4.3 Assumptions

The TOE assumptions on the operational environment are defined and described in PP [1] section 3.4.

The assumptions concern the phases where the TOE has left the chip manufacturer.

A.Process-Sec-IC Protection during Packaging, Finishing and Personalization

It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end-consumer 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 Security IC 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 Security IC Embedded Software as documented in the certification report.

A.Resp-Appl Treatment of User Data

All User Data are owned by Security IC Embedded Software. Therefore, it must be assumed that security relevant User Data (especially cryptographic keys) are treated by the Security IC Embedded Software as defined for its specific application context.

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

Table 7: Assumption according PP [1]

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

4.3.1 Augmented Assumptions

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

For details see PP [1] section 3.4.

5 Security objectives (ASE_OBJ)

This section shows the subjects and objects where are relevant to the TOE.
A short overview is given in the following.

The user has the following standard high-level security goals related to the assets:

- SG1 maintain the integrity of User Data and of the Security IC Embedded Software
- SG2 maintain the confidentiality of User Data and of the Security IC Embedded Software
- SG3 maintain the correct operation of the security services provided by the TOE for the Security IC Embedded Software
- SG4 provision of random numbers.

5.1 Security objectives for the TOE

The security objectives of the TOE are defined and described in PP [1] section 4.1.

Table 8: Objectives for the TOE according to PP [1]

O.Phys-Manipulation	Protection against Physical Manipulation
O.Phys-Probing	Protection against Physical Probing
O.Malfunction	Protection against Malfunction
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 provides “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:

- Advanced Encryption Standard (AES)
- Triple Data Encryption Standard (3DES)

Note 2:
This TOE can come with both crypto co-processors accessible, or with a blocked SCP or with a blocked Crypto2304T, or with both crypto co-processors blocked. The blocking depends on the customer demands prior to the production of the hardware. In case the SCP is blocked, no AES and 3DES computation supported by hardware is possible. No accessibility of the deselected cryptographic co-processors is without impact on any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use the cryptographic co-processors.

End of note.

The TOE shall provide “Area based Memory Access Control (O.Mem-Access)” as specified below.

O.Mem-Access	Area based Memory Access Control The TOE must provide the Smartcard Embedded Software with the capability to define restricted access memory areas. The TOE must then enforce the partitioning of such memory areas so that access of software to memory areas and privilege levels is controlled as required, for example, in a multi-application environment.

Table 9: Additional objectives due to TOE specific functions and augmentations

O.Add-Functions	Additional specific security functionality
O.Mem-Access	Area based Memory Access Control

5.2 Security Objectives for the development and operational Environment

The security objectives for the security IC embedded software development environment and the operational environment is defined in PP [1] section 4.2 and 4.3. The table below lists the security objectives.

Table 10: Security objectives for the environment according to PP [1]

Phase 1	OE.Plat-Appl	Usage of Hardware Platform
	OE.Resp-Appl	Treatment of User Data
Phase 5 – 6 optional Phase 4	OE.Process-Sec-IC	Protection during composite product manufacturing

5.2.1 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)“.

The objectives of the environment regarding the memory, software and firmware protection and the SFR and peripheral-access-rights-handling have to be clarified. For the separation of different applications the Smartcard Embedded Software (Operating System) may implement a memory management scheme based upon security functions of the TOE.

5.2.2 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 memory, software and firmware protection and the SFR and peripheral access rights handling these objectives 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.

5.2.3 Clarification of "Protection during Composite product manufacturing (OE.Process-Sec-IC)"

The protection during packaging, finishing and personalization includes also the personalization process (Flash Loader software) and the personalization data (TOE software components) during Phase 4, Phase 5 and Phase 6.

5.3 Security Objectives Rationale

The security objectives rationale of the TOE are defined and described in PP [1] section 4.4. For organizational security policy P.Add-Functions, OE.Plat-Appl and OE.Resp-Appl the rationale is given in the following description.

Table 11: Security Objective Rationale

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

The justification related to the security objective "Additional Specific Security Functionality (O.Add-Functions)" is as follows: Since O.Add-Functions requires the TOE to implement exactly the same specific security functionality as required by P.Add-Functions; the organisational security policy is covered by the objective.

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 PP [1] 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 the PP [1] 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.

Compared to the PP [1] an enhancement regarding memory area protection has been established. The clear definition of privilege levels for operated software establishes the clear separation of different restricted memory areas for running the firmware, downloading and/or running the operating system and to establish a clear separation between different applications. Nevertheless, it is also possible to define a shared memory section where separated applications may exchange defined data. The privilege levels clearly define by using a hierarchical model the access right from one level to the other. These measures ensure that the threat T.Mem-Access is clearly covered by the security objective O.Mem-Access.

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.

6 Extended Component Definition (ASE_ECD)

There are four extended components defined and described for the TOE:

- the family **FCS_RNG** at the class FCS Cryptographic Support
- the family **FMT_LIM** at the class FMT Security Management
- the family **FAU_SAS** at the class FAU Security Audit
- the component **FPT_TST.2** at the class FPT Protection of the TSF

The extended components FMT_LIM and FAU_SAS are defined and described in PP [1] section 5. The components FPT_TST.2 and FCS_RNG are defined in the following sections.

6.1 Component “Subset TOE security testing (FPT_TST)”

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 or is done automatically and continuously.

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 verification of the integrity of TSF data and of the stored TSF executable code which might violate the security policy. Therefore, the functional component **”Subset TOE security testing (FPT_TST.2)”** of the family TSF self test has been newly created. This component allows that particular parts of the security mechanisms and functions provided by the TOE are tested.

6.2 Definition of FPT_TST.2

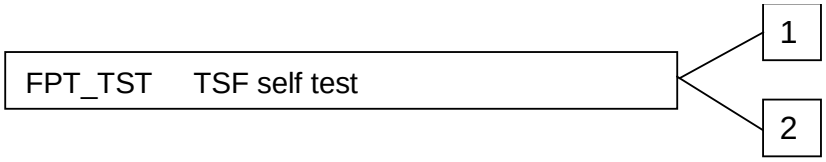
The functional component “Subset TOE security testing (FPT_TST.2)” has been newly created (Common Criteria Part 2 extended). This component allows that particular parts of the security mechanisms and functions provided by the TOE can be tested after TOE Delivery or are tested automatically and continuously during normal operation transparent for the user. 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 functional component “Subset TOE testing (FPT_TST.2)” is specified as follows (Common Criteria Part 2 extended).

6.3 TSF self test (FPT_TST)

Family Behavior The Family Behavior is defined in [3] section 15.14 (442, 443).

Component leveling



FPT_TST.1: The component FPT_TST.1 is defined in [3] section 15.14 (444, 445, 446).

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 authorized user, or when other conditions are met. It also provides the ability to verify the integrity of TSF data and executable code.

Management: FPT_TST.2

The following actions could be considered for the management functions in FMT:

- management of the conditions under which subset TSF self testing occurs, such as during initial start-up, regular interval or under specified conditions
- management of the time of the interval appropriate.

Audit: FPT_TST.2

There are no auditable events foreseen.

FPT_TST.2 Subset TOE testing

Hierarchical to: No other components.

Dependencies: No dependencies

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 authorized 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].

6.4 Family “Generation of Random Numbers (FCS_RNG)”

The family “Generation of Random Numbers (FCS_RNG.1)” has to be newly created according the new version of the “Anwendungshinweise und Interpretationen zum Schema (AIS)” [15]. This security functional component is used instead of the functional component FCS_RNG.1 defined in the protection profile [1].

The family “Generation of Random Numbers (FCS_RNG.1)” is specified as follows (Common Criteria Part 2 extended).

6.5 Definition of FCS_RNG.1

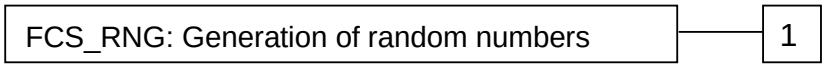
This section describes the functional requirements for the generation of random numbers, which may be used as secrets for cryptographic purposes or authentication. The IT security functional requirements for the TOE are defined in an additional family (FCS_RNG) of the Class FCS (Cryptographic support).

FCS_RNG Generation of random numbers

Family Behaviour

This family defines quality requirements for the generation of random numbers that are intended to be used for cryptographic purposes.

Component levelling:



FCS_RNG.1: Generation of random numbers, requires that the random number generator implements defined security capabilities and that the random numbers meet a defined quality metric.

Management: FCS_RNG.1

There are no management activities foreseen.

Audit: FCS_RNG.1

There are no actions defined to be auditable.

FCS_RNG.1 Random number generation

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RNG.1.1: The TSF shall provide a [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*] random number generator that implements: [assignment: *list of security capabilities*].

FCS_RNG.1.2: The TSF shall provide random numbers that meet [assignment: *a defined quality metric*].

Application Note 1: The functional requirement FCS_RNG.1 is a refinement of the FCS_RNG.1 defined in the Protection Profile [1] according to “Anwendungshinweise und Interpretationen zum Schema (AIS)” [15].

7 Security Requirements (ASE_REQ)

For this section the PP [1] section 6 can be applied completely.

7.1 TOE Security Functional Requirements

The security functional requirements (SFR) for the TOE are defined and described in the PP [1] section 6.1 and in the following description.

The Table 12 provides an overview of the functional security requirements of the TOE, defined in the in PP [1] section 6.1. In the last column it is marked if the requirement is refined. The refinements are also valid for this ST.

Table 12: Security functional requirements defined in PP [1]

Security Functional Requirement		Refined in PP [1]
FRU_FLT.2	“Limited fault tolerance“	Yes
FPT_FLS.1	“Failure with preservation of secure state”	Yes
FMT_LIM.1	“Limited capabilities”	No
FMT_LIM.2	“Limited availability”	No
FAU_SAS.1	“Audit storage”	No
FPT_PHP.3	“Resistance to physical attack”	Yes
FDP_ITT.1	“Basic internal transfer protection”	Yes
FPT_ITT.1	“Basic internal TSF data transfer protection	Yes
FDP_IFC.1	“Subset information flow control”	No

The Table 13 provides an overview about the augmented security functional requirements, which are added additional to the TOE and defined in this ST. All requirements are taken from Common Criteria Part 2 [3], with the exception of the requirement FPT_TST.2 and FCS_RNG.1, which are defined in this ST completely.

Table 13: 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.1	“Management of security attributes”
FMT_MSA.3	“Static attribute initialisation”
FMT_SMF.1	“Specification of Management functions”
FCS_COP.1	“Cryptographic support”

Security Functional Requirement	
FDP_SDI.1	“Stored data integrity monitoring
FDP_SDI.2	“Stored data integrity monitoring and action”
FCS_RNG.1	“Quality metric for random numbers”

All assignments and selections of the security functional requirements of the TOE are done in PP [1] and in the following description.

The above marked extended components FMT_LIM.1 and FMT_LIM.2 are introduced in PP [1] to define the IT security functional requirements of the TOE as an additional family (FMT_LIM) of the Class FMT (Security Management). This family describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF.

The additional component FAU.SAS is introduced to define the security functional requirements of the TOE of the Class FAU (Security Audit). This family describes the functional requirements for the storage of audit data and is described in the next chapter.

The requirement FPT_TST.2 is the subset of TOE testing and originated in [3]. This requirement is given as the correct operation of the security functions is essential. The TOE provides mechanisms to cover this requirement by the smartcard embedded software and/or by the TOE itself.

7.1.1 Extended Components FCS_RNG.1 and FAU_SAS.1

7.1.1.1 FCS_RNG

To define the IT security functional requirements of the TOE an additional family (FCS_RNG) of the Class FCS (cryptographic support) is defined here. This family describes the functional requirements for random number generation used for cryptographic purposes.

FCS_RNG.1 Random Number Generation

Hierarchical to: No other components

Dependencies: No dependencies

FCS_RNG.1 Random numbers generation Class PTG.2 according to [6]

FCS_RNG.1.1 The TSF shall provide a *physical* random number generator that implements:

PTG.2.1 *A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.*

PTG.2.2 *If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source.*

PTG.2.3 *The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.*

PTG.2.4	*The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.*
PTG.2.5	*The online test procedure checks the quality of the raw random number sequence. It is triggered continuously. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.*

FCS_RNG.1.2 The TSF shall provide *numbers in the format 8- or 16-bit* that meet

PTG.2.6	*Test procedure A, as defined in [6] does not distinguish the internal random numbers from output sequences of an ideal RNG.*
PTG.2.7	*The average Shannon entropy per internal random bit exceeds 0.997.*

Application Note 2*:* The functional requirement FCS_RNG.1 is a refinement of the FCS_RNG.1 defined in the Protection Profile [1] according to “Anwendungshinweise und Interpretationen zum Schema (AIS)” [15].

7.1.1.2 FAU_SAS

To define the security functional requirements of the TOE an additional family (FAU_SAS) of the Class FAU (Security Audit) is defined here. This family describes the functional requirements for the storage of audit data. It has a more general approach than FAU_GEN, because it does not necessarily require the data to be generated by the TOE itself and because it does not give specific details of the content of the audit records.

The TOE shall meet the requirement “Audit storage (FAU_SAS.1)” as specified below (Common Criteria Part 2 extended).

FAU_SAS.1	Audit Storage
Hierarchical to:	No dependencies
Dependencies:	No dependencies.
FAU_SAS.1.1	The TSF shall provide the test process *before TOE Delivery* with the capability to store *the Initialization Data and/or Pre-personalization Data and/or supplements of the Security IC Embedded Software* in the *not changeable configuration page area and non-volatile memory.*

7.1.2 Subset of TOE testing

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.

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.
Dependencies:	No dependencies

FPT_TST.2.1 The TSF shall run a suite of self tests *at the request of the authorized user* to demonstrate the correct operation of the *alarm lines and/or the environmental sensor mechanisms:*

- *CORE – CPU related alarms*
- *Symmetric Cryptographic Processor*
- *Temperature alarm*
- *AXI – Memory Bus*
- *NVM_MISS – NVM illegal addressing alarm*
- *Memory - Error Detection Code alarm*
- *FSE – Internal Frequency Sensor alarm*
- *Light sensitive and Backside light detection alarm*
- *WDT - Watch Dog Timer related alarms*
- *SW – Software triggered alarm*
- *Glitch sensor alarm*
- *Reset source for clearing alarm bits*
- *Test controller*

7.1.3 Memory access control

Usage of multiple applications in one Smartcard often requires code and data separation in order to prevent that one application can access code and/or data of another application. For this reason the TOE provides Area based Memory Access Control. The underlying Memory Protection Unit (MPU) is documented in section 4 of the [7].

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 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 and execute accesses of software running at the privilege levels as defined below. Any access is controlled, regardless whether the access is on code or data or a jump on any other privilege level outside the current one.

The memory model provides two distinct, independent levels separated from each other. These levels are referred to as the privileged level and the user level. In the user level up to eight regions can be defined with different access rights. The access rights are controlled by the MPU related to the following rules:

- the privilege level has access to the user level
- the user level have no access to the privilege level
- the user level have no access to other user levels in the case that no overlapping exist
- overlapping user levels, have access to other user levels with ascending region priority
- access permissions

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.
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1	The TSF shall enforce the *Memory Access Control Policy* on *all subjects (software running at the defined and assigned levels), all objects (data including code stored in memories) and all the operations defined in the Memory Access Control Policy, i.e. levels*.

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.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1	The TSF shall enforce the *Memory Access Control Policy* to objects based on the following: *Subject*: - *software running at privilege level required to securely operate the chip. This includes also privilege level running interrupt routines.*

- *software running at the user level containing the user software*

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 of the relevant memory range before, during or after 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 authorize 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*.

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.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the *Memory Access Control Policy* to provide *well defined*[3] 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*[4], to specify alternative initial values to override the default values when an object or information is created.

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.

[3] The static definition of the access rules is documented in [7]

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

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
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 the software running on the levels.*

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
Dependencies:	No dependencies
FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions*: access the configuration registers of the MPU*.

7.1.4 Support of Cipher Schemes

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

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; dependencies are discussed in Section 7.3.1.1.

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

- Advanced Encryption Standard (AES)
- Triple Data Encryption Standard (3DES)

Preface regarding Security Level related to Cryptography:

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

The cryptographic functionality 2-key Triple-DES provided by the TOE achieves a security level of maximum 80 Bits (in general context).

Triple-DES Operation

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

FCS_COP.1/DES	Cryptographic operation
Hierarchical to:	No other components.
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 management] FCS_CKM.4 Cryptographic key destruction
FCS_COP.1.1/DES	The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *Triple Data Encryption Standard (3DES)* in *Electronic Codebook Mode (ECB) and in the Cipher Block Chaining Mode (CBC)* and with cryptographic key sizes *of 2 x 56 bit or 3 x 56 bit,* that meet the following *standards*: *National Institute of Standards and Technology (NIST), Technology Administration, U.S. Department of Data Encryption Standard (DES), NIST Special Publication 800-67, Version 1.1* *and* *NIST Special Publication 800-38A, Edition 2001*

Note 3:
This TOE can come with both crypto co-processors accessible, or with a blocked SCP or with a

blocked Crypto2304T, or with both crypto co-processors blocked. The blocking depends on the customer demands prior to the production of the hardware. In case the SCP is blocked, no AES and 3DES computation supported by hardware is possible. No accessibility of the deselected cryptographic co-processors is without impact on any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use the cryptographic co-processors. End of note.

AES Operation

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

FCS_COP.1/AES	Cryptographic operation
Hierarchical to:	No other components.
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
FCS_COP.1.1/AES	The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *Advanced Encryption Standard (AES)* in *Electronic Codebook Mode (ECB) and in the Cipher Block Chaining Mode (CBC)* and cryptographic key sizes of *128 bit or 192 bit or 256 bit* that meet the following standards: *U.S. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL),* *Advanced Encryption Standard (AES), FIPS PUB 197* *and* *NIST Special Publication 800-38A, Edition 2001*

Note 4:
This TOE can come with both crypto co-processors accessible, or with a blocked SCP or with a blocked Crypto2304T, or with both crypto co-processors blocked. The blocking depends on the customer demands prior to the production of the hardware. In case the SCP is blocked, no AES and 3DES computation supported by hardware is possible. No accessibility of the deselected cryptographic co-processors is without impact on any other security policy of the TOE; it is exactly equivalent to the situation where the user decides just not to use the cryptographic co-processors.

End of note.

7.1.5 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
Dependencies:	No dependencies

FDP_SDI.1.1	The TSF shall monitor user data stored in containers controlled by the TSF for *inconsistencies between stored data and corresponding EDC* on all objects, based on the following attributes: *EDC value for RAM and ROM and ECC value for the SOLID FLASH™ and verification of stored data in the SOLID FLASH™*

The TOE shall meet the requirement “Stored data integrity monitoring and action (FDP_SDI.2)” as specified below:

FDP_SDI.2	Stored data integrity monitoring and action
Hierarchical to:	FDP_SDI.1 stored data integrity monitoring
Dependencies:	No dependencies
FDP_SDI.2.1	The TSF shall monitor user data stored in containers controlled by the TSF for *data integrity and one- and/or more-bit-errors* on all objects, based on the following attributes: *corresponding EDC value for RAM and ROM and error correction ECC for the SOLID FLASH™.*
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall *correct 1 bit errors in the SOLID FLASH™ automatically and inform the user about more bit errors.*

7.2 TOE Security Assurance Requirements

The evaluation assurance level is EAL5 augmented with ALC_DVS.2 and AVA_VAN.5. In the following table, the security assurance requirements are given. The augmentation of the assurance components compared to the Protection Profile [1] is expressed with bold letters.

Aspect	Acronym	Description	Refinement
Development	ADV_ARC.1	Security Architecture Description	in PP [1]
	ADV_FSP.5	**Complete semiformal functional specification with additional error information**	in ST
	ADV_IMP.1	Implementation representation of the TSF	in PP [1]
	ADV_INT.2	**Well-structured internals**	
	ADV_TDS.4	**Semi-formal modular design**	
Guidance Documents	AGD_OPE.1	Operational user guidance	in PP [1]
	AGD_PRE.1	Preparative procedures	in PP [1]
Life-Cycle Support	ALC_CMC.4	Production support, acceptance procedures and automation	in PP [1]
	ALC_CMS.5	**Development tools CM coverage**	in ST
	ALC_DEL.1	Delivery procedures	in PP [1]
	ALC_DVS.2	Identification of security measures	in PP [1]
	ALC_LCD.1	Developer defined life-cycle model	
	ALC_TAT.2	**Compliance with implementation standards**	in ST
Security Target Evaluation	ASE_CCL.1	Conformance claims	
	ASE_ECD.1	Extended components definition	
	ASE_INT.1	ST introduction	
	ASE_OBJ.2	Security objectives	
	ASE_REQ.2	Derived security requirements	
	ASE_SPD.1	Security problem definition	
	ASE_TSS.1	TOE summary specification	
Tests	ATE_COV.2	Analysis of coverage	in PP [1]
	ATE_DPT.3	**Testing: modular design**	in ST
	ATE_FUN.1	Functional testing	
	ATE_IND.2	Independent testing - sample	
Vulnerability Assessment	AVA_VAN.5	Advanced methodical vulnerability testing	in PP [1]

Table 14: Assurance components

7.2.1 Refinements

Some refinements are taken unchanged from the PP [1]. In some cases a clarification is necessary. In Table 16 an overview is given where the refinement is done.
Two refinements from the PP [1] have to be discussed here in the Security Target, as the assurance level is increased.

Life cycle support (ALC_CMS, ALC_TAT)

The refinement from the PP [1] can be applied even at the chosen assurance level EAL 5 augmented with ALC_CMS.5 and ALC_TAT.2. The assurance package ALC_CMS.4 is extended to ALC_CMS.5 with aspects regarding the configuration control system for the TOE. The assurance package ALC_TAT.1 is extended to ALC_TAT.2 with aspects regarding the implementation standards for the TOE. The refinements are not touched.

Functional Specification (ADV_FSP)

The refinement from the PP [1] can be applied even at the chosen assurance level EAL 5 augmented with ADV_FSP.5. The assurance package ADV_FSP.4 is extended to ADV_FSP.5 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 PP [1].

Tests (ATE_DPT.3)

The refinement from the PP [1] can be applied even at the chosen assurance level EAL 5 augmented with ATE_DPT.3. The assurance package ATE_DPT.2 is augmented to ATE_DPT.3 relating to the requirements of the assurance level EAL 5. The refinement is not touched.

7.3 Security Requirements Rationale

7.3.1 Rationale for the Security Functional Requirements

The security functional requirements rationale of the TOE are defined and described in PP [1] section 6.3 for the following security functional requirements: FDP_ITT.1, FDP_IFC.1, FPT_ITT.1, FPT_PHP.3, FPT_FLS.1, FRU_FLT.2, FMT_LIM.1, FMT_LIM.2, FCS_RNG.1 and FAU_SAS.1.

The security functional requirements FPT_TST.2, FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FCS_COP.1, FDP_SDI.1 and FDP_SDI.2 are defined in the following description:

Table 15: Rational for additional SFR in the ST

Objective	TOE Security Functional Requirements
O.Add-Functions	- FCS_COP.1/DES „Cryptographic operation“ - FCS_COP.1/AES „Cryptographic operation“
O.Phys-Manipulation	- FPT_TST.2 „ Subset TOE security testing “
O.Mem-Access	- 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”
O.Malfunction	- FDP_SDI.1 „Stored data integrity monitoring“ - FDP_SDI.2 „Stored data integrity monitoring and action“

The table above gives an overview, how the security functional requirements are combined to meet the security objectives. The detailed justification is given in the following:

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.

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 specific 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,

All these requirements have to be fulfilled to support OE.Resp-Appl for FCS_COP.1/DES (3DES algorithm) and for FCS_COP.1/AES (AES algorithm).

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.

The usage of cryptographic algorithms requires the use of appropriate keys. Otherwise these cryptographic functions do not provide security. The keys have to be unique with a very high probability, and must have a certain cryptographic strength etc. In case of a key import into the TOE (which is usually after TOE delivery) it has to be ensured that quality and confidentiality are maintained. Keys for 3DES and AES are provided by the environment..

In this ST the objectives for the environment OE.Plat-Appl and OE.Resp-Appl have been clarified. The Smartcard Embedded Software defines the use of the cryptographic functions FCS_COP.1 provided by the TOE. The requirements for the environment FDP_ITC.1, FDP_ITC.2, FCS_CKM.1 and FCS_CKM.4 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.

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 verification of the integrity of TSF data and stored TSF executable code which might violate the security policy.

The tested security enforcing functions are SF_DPM Device Phase Management, SF_CS Cryptographic Support and SF_PMA Protection against modifying attacks.

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.

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 as required by O.Mem-Access. The related TOE security functional requirements FDP_ACC.1, FDP_ACF.1, FMT_MSA.3, FMT_MSA.1 and FMT_SMF.1 cover this security objective. The implementation of these functional requirements is represented by the dedicated privilege level concept.

The justification of the security objective and the additional requirements show that they do not contradict to the rationale already given in the Protection Profile for the assumptions, policy and threats defined there. Moreover, these additional security functional requirements cover the requirements by [3] user data protection of chapter 11 which are not refined by the PP [1].

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. The TOE only provides the tool to implement the policy defined in the context of the application.

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 an Error Detection (EDC) algorithm which detects integrity errors of the data stored in RAM, ROM and SOLID FLASH™ (in the SOLID FLASH™ more bit errors are detected). By this the malfunction of the TOE using corrupt data is prevented. Therefore FDP_SDI.1 is suitable to meet the security objective.

The security functional requirement “Stored data integrity monitoring and action (FDP_SDI.2)” requires the implementation of an integrity observation and correction which is implemented by the Error Detection (EDC) and Error Correction (ECC) measures. The EDC is present in RAM and ROM of the TOE while the ECC is realized in the SOLID FLASH™. These measures detect and inform about one and more bit errors. In case of the SOLID FLASH 1 bit errors of the data are corrected automatically. By the ECC mechanisms it is prevented that the TOE uses corrupt data. Therefore FDP_SDI.2 is suitable to meet the security objective.

The CC part 2 defines the component FIA_SOS.2, which is similar to FCS_RNG.1, as follows:

FIA_SOS.2 TSF Generation of secrets

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.2.1 The TSF shall provide a mechanism to generate secrets that meet [assignment:*a defined quality metric*].
FIA_SOS.2.2 The TSF shall be able to enforce the use of TSF generated secrets for [assignment: *list of TSF functions*].

The CC part 2, annex G.3 [3], states: “This family defines requirements for mechanisms that enforce defined quality metrics on provided secrets, and generate secrets to satisfy the defined metric“. Even the operation in the element FIA_SOS.2.2 allows listing the TSF functions using the generated secrets. Because all applications discussed in annex G.3 are related to authentication, the component FIA_SOS.2 is also intended for authentication purposes while the term “secret” is not limited to authentication data (cf. CC part 2, paragraphs 39-42).
Paragraph 685 in the CC part 2 [3] recommends use of the component FCS_CKM.1 to address random number generation. However, this may hide the nature of the secrets used for key generation and does not allow describing random number generation for other cryptographic methods (e.g., challenges, padding), authentication (e.g., password seeds), or other purposes (e.g., blinding as a countermeasure against side channel attacks).
The component FCS_RNG addresses general RNG, the use of which includes but is not limited to cryptographic mechanisms. FCS_RNG allows to specify requirements for the generation of random numbers including necessary information for the intended use. These details describe the quality of the generated data where other security services rely on. Thus by using FCS_RNG a ST or PP author is able to express a coherent set of SFRs that include or use the generation of random numbers as a security service.

7.3.1.1 Dependencies of Security Functional Requirements

The dependence of security functional requirements are defined and described in PP [1] section 6.3.2 for the following security functional requirements: FDP_ITT.1, FDP_IFC.1, FPT_ITT.1, FPT_PHP.3, FPT_FLS.1, FRU_FLT.2, FMT_LIM.1, FMT_LIM.2, FCS_RNG.1 and FAU_SAS.1.

The dependence of security functional requirements for the security functional requirements FPT_TST.2, FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FCS_COP.1, FDP_SDI.1 and FDP_SDI.2 are defined in the following description.

Table 16: Dependency for cryptographic operation requirement

Security Functional Requirement	Dependencies	Fulfilled by security requirements
FCS_COP.1/DES	FCS_CKM.1	Yes, see comment 3
	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) FCS_CKM.4	Yes, see comment 3
FCS_COP.1/AES	FCS_CKM.1	Yes, see comment 3
	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) FCS_CKM.4	Yes, see comment 3
FPT_TST.2	None	See comment 1
FDP_ACC.1	FDP_ACF.1	Yes
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Yes Yes
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes Not required, see comment 2
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes See comment 2 Yes
FMT_SMF.1	None	N/A
FDP_SDI.1	None	N/A
FDP_SDI.2	None	N/A

Comment 1:
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. Therefore, the former dependency to FPT_AMT.1 is fulfilled without further and by that dispensable. CC in the Revision 3 considered this and dropped this dependency. The requirement FPT_TST.2 is satisfied.
End of comment.

Comment 2:
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.
End of comment.

Comment 3:
The security functional requirement “Cryptographic operation (FCS_COP.1)” met by the 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]
- FCS_CKM.1 Cryptographic key generation

- FCS_CKM.4 Cryptographic key destruction.

These requirements all address the appropriate management of cryptographic keys used by the specified cryptographic function and are not part of the PP [1]. 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.
For the security functional requirement FCS_COP.1/DES and FCS_COP.1/AES the respective dependencies FCS_CKM.1, FCS_CKM.4 and FDP_ITC.1 or FDP_ITC.2 have to be fulfilled by the environment. That mean, that the environment shall meet the requirements FCS_CKM.1 and FCS_CKM.4 as defined in [3], section 10.1 and shall meet the requirements FDP_ITC.1 or FDP_ITC.2 as defined in [3], section 11.7.
End of comment.

7.3.2 Rationale of the Assurance Requirements

The chosen assurance level EAL5 and the augmentation with the requirements ALC_DVS.2 and AVA_VAN.5 were chosen in order to meet the assurance expectations explained in the following paragraphs. In Table 14 the different assurance levels are shown as well as the augmentations. The augmentations are in compliance with the Protection Profile.

An assurance level EAL5 with the augmentations ALC_DVS.2 and AVA_VAN.5 are required for this type of TOE since it is intended to defend against **highly sophisticated attacks** without protective environment. This evaluation assurance package was selected to permit a developer to gain maximum assurance from positive security engineering based on good commercial practices. In order to provide a meaningful level of assurance that the TOE provides an adequate level of defence against such attacks, the evaluators should have access to all information regarding the TOE including the TSF internals, the low level design and source code including the testing of the modular design. Additionally the mandatory technical document “Application of Attack Potential to Smartcards” [10] shall be taken as a basis for the vulnerability analysis of the TOE.

ALC_DVS.2 Sufficiency of security measures

Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE.

In the particular case of a Security IC the TOE is developed and produced within a complex and distributed industrial process which must especially be protected. Details about the implementation, (e.g. from design, test and development tools as well as Initialization Data) may make such attacks easier. Therefore, in the case of a Security IC, maintaining the confidentiality of the design is very important.

This assurance component is a higher hierarchical component to EAL5 (which only requires ALC_DVS.1). ALC_DVS.2 has no dependencies.

AVA_VAN.5 Advanced methodical vulnerability analysis

Due to the intended use of the TOE, it must be shown to be highly resistant to penetration attacks. This assurance requirement is achieved by the AVA_VAN.5 component.

Independent vulnerability analysis is based on highly detailed technical information. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing high attack potential.

AVA_VAN.5 has dependencies to ADV_ARC.1 “Security architecture description”, ADV_FSP.2 “Security enforcing functional specification”, ADV_TDS.3 “Basic modular design”, ADV_IMP.1 “Implementation representation of the TSF”, AGD_OPE.1 “Operational user guidance”, and AGD_PRE.1 “Preparative procedures”.

All these dependencies are satisfied by EAL5.

It has to be assumed that attackers with high attack potential try to attack Security ICs like smart cards used for digital signature applications or payment systems. Therefore, specifically AVA_VAN.5 was chosen in order to assure that even these attackers cannot successfully attack the TOE.

8 TOE Summary Specification (ASE_TSS)

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

The TOE is equipped with following Security Features to meet the security functional requirements:

SF_DPM	Device Phase Management
SF_PS	Protection against Snooping
SF_PMA	Protection against Modification Attacks
SF_PLA	Protection against Logical Attacks
SF_CS	Cryptographic Support

The following description of the Security Features is a complete representation of the TSF.

8.1 SF_DPM: Device Phase Management

The life cycle of the TOE is split up into several phases. Different operation modes help to protect the TOE during each phase of its lifecycle.

8.2 SF_PS: Protection against Snooping

The TOE uses various means to protect from snooping of memories and busses and prevents single stepping.

8.3 SF_PMA: Protection against Modifying Attacks

This TOE implements protection against modifying attacks of memories, alarm lines and sensors.

8.4 SF_PLA: Protection against Logical Attacks

The memory model of the TOE provides two distinct, independent levels and the possibility to define up to eight memory regions with different access rights enforced by the Management Protection Unit (MPU).

8.5 SF_CS: Cryptographic Support

The TOE is equipped with an asymmetric and a symmetric hardware accelerator to support several symmetric and asymmetric cryptographic operations. Additionally the TOE is equipped with a True Random Number Generator for the generation of random numbers.

8.6 Assignment of Security Functional Requirements to TOE's Security Functionality

The justification and overview of the mapping between security functional requirements (SFR) and the TOE's security functionality (SF) is given in sections the sections above. The results are shown in Table 17. The security functional requirements are addressed by at least one relating security feature.

The various functional requirements are often covered manifold. As described above the requirements ensure that the TOE is checked for correct operating conditions and if a not correctable failure occurs that a stored secure state is achieved, accompanied by data integrity monitoring and actions to maintain the integrity although failures occurred. An overview is given in following table:

Table 17: Mapping of SFR and SF

Security Functional Requirement	SF_DPM	SF_PS	SF_PMA	SF_PLA	SF_CS
FAU_SAS.1	X				
FMT_LIM.1	X				
FMT_LIM.2	X				
FDP_ACC.1	X			X	
FDP_ACF.1	X			X	
FPT_PHP.3		X	X		X
FDP_ITT.1	X	X	X		X
FDP_SDI.1			X		
FDP_SDI.2			X		
FDP_IFC.1		X	X		
FMT_MSA.1	X			X	
FMT_MSA.3	X			X	
FMT_SMF.1	X			X	
FRU_FLT.2			X		
FPT_ITT.1	X	X	X		X
FPT_TST.2			X		X
FPT_FLS.1		X	X	X	X
FCS_RNG.1					X
FCS_COP.1/DES					X
FCS_COP.1/AES					X

8.7 Security Requirements are internally Consistent

For this chapter the PP [1] section 6.3.4 can be applied completely.

In addition to the discussion in section 6.3 of PP [1] 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.

As disturbing, manipulating during or forcing the results of the test checking the security functions after TOE delivery, this security functional requirement FPT_TST.2 has to be protected. An attacker could aim to switch off or disturb certain sensors or filters and preserve the detection of his manipulation by blocking the correct operation of FPT_TST.2. 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 security functional requirement FPT_TST.2. Therefore, the related security functional requirements support the secure implementation and operation of FPT_TST.2.

The requirement FPT_TST.2 allows testing of some security mechanisms by the Smartcard Embedded Software after delivery. In addition, the TOE provides an automated continuous user transparent testing of certain functions.

The implemented level concept represents the area based memory access protection enforced by the MPU. As an attacker could attempt to manipulate the privilege level definition as defined and present in the TOE, the functional requirement FDP_ACC.1 and the related other requirements have to be protected themselves. 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.2.1 allows detection of integrity errors of data stored in memory. FDP_SDI.2.2 in addition allows correction of one bit errors or taking further action. Both meet the security objective O.Malfunction. The requirements FRU_FLT.2, FPT_FLS.1, and FDP_ACC.1 which also meet this objective are independent from FDP_SDI.2 since they deal with the observation of the correct operation of the TOE and not with the memory content directly.

9 References

9.1 Literature

[1] Security IC Platform Protection Profile, Version 1.0, 15.06.2007, BSI-PP-0035

[2] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model; Version 3.1 Revision 3 July 2009, CCMB-2009-07-001

[3] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements; Version 3.1 Revision 3 July 2009, CCMB-2009-07-002

[4] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements; Version 3.1 Revision 3 July 2009, CCMB-2009-07-003

[5] ARMv7-M Architecture Reference Manual, ARM DDI 0403D ID021310, 12. February 2010, ARM Limited

[6] A proposal for: Functionality classes for random number generators, Version 2.0, 18. September 2011

[7] SLE97 Hardware Reference Manual, Infineon Technologies AG

[10] Joint Interpretation Library, Application of Attack Potential to Smartcards, Version 2.7, February 2009

[11] SLE97 Programmer's Reference User's Manual, Infineon Technologies AG

[12] M9900 Errata Sheet, Infineon Technologies AG

[15] Anwendungshinweise und Interpretationen zum Schema (AIS), AIS31, Version 2.1, 2011-12-02, Bundesamt für Sicherheit in der Informationstechnik

[23] M9900 Security Guidelines User´s Manual

.

Note that the versions of these documents will be defined at the end of the evaluation and listed in the certification report.

10 List of Abbreviations

AES	Advanced Encryption Standard
AIS31	“Anwendungshinweise und Interpretationen zu ITSEC und CC Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren”
APB™	Advanced Peripheral Bus
API	Application Programming Interface
AXI™	Advanced eXtensible Interface Bus Protocol
BOS	Boot System
CC	Common Criteria
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
Crypto2304T	Asymmetric Cryptographic Processor
CRT	Chinese Reminder Theorem
DPA	Differential Power Analysis
DFA	Differential Failure Analysis
EC	Elliptic Curve
ECC	Error Correction Code
EDC	Error Detection Code
EDU	Error Detection Unit
GCIM	Generic Chip Identification Mode (BOS-CIM)
EEPROM	Electrically Erasable and Programmable Read Only Memory
EMA	Electro magnetic analysis
HW	Hardware
IC	Integrated Circuit
ID	Identification
IMM	Interface Management Module
I/O	Input/Output
MED	Memory Encryption and Decryption
MPU	Memory Protection Unit
O	Object
OS	Operating system
RAM	Random Access Memory
RMS	Resource Management System
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rives-Shamir-Adleman Algorithm

SCP	Symmetric Cryptographic Processor
SF	Security Feature
SFR	Special Function Register, as well as Security Functional Requirement The specific meaning is given in the context
Solid Flash™	Electrically Erasable and Programmable Read Only Memory (EEPROM)
SPA	Simple power analysis
SW	Software
T	Threat
TM	Test Mode (BOS)
TOE	Target of Evaluation
TRNG	True Random Number Generator
TSF	TOE Security Functionality
UART	Universal Asynchronous Receiver/Transmitter
UM	User Mode (BOS)
UMSLC	User Mode Security Life Control
3DES	Triple DES Encryption Standard

11 Glossary

Boot System	Part of the firmware with routines for controlling the operating state and testing the TOE hardware
Central Processing Unit	Logic circuitry for digital information processing
Chip	Integrated Circuit]
Chip Identification Mode data	Data stored in the Solid Flash™ 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 BOS version number
Chip Identification Mode	Operational status phase of the TOE, in which actions for identifying the individual chip by transmitting the Chip Identification Mode data take place
Controller	IC with integrated memory, CPU and peripheral devices
Crypto2304T	Cryptographic coprocessor for asymmetric cryptographic operations (RSA, Elliptic Curves)
Cyclic Redundancy Check	Process for calculating checksums for error detection
Electrically Erasable and Programmable Read Only Memory (Solid Flash™)	Non-volatile memory permitting electrical read and write operations
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
Memory Encryption and Decryption	Method of encoding/decoding data transfer between CPU and memory
Memory	Hardware part containing digital information (binary data)
Microprocessor	CPU with peripherals
Object	Physical or non-physical part of a system which contains information and is acted upon by subjects
Operating System	Software which implements the basic TOE actions necessary for operation
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 Solid Flash™ programming routines, AIS31 testbench etc.
Security Mechanism	Logic or algorithm which implements a specific security function in hardware or software
SCP	Symmetric cryptographic coprocessor for symmetric cryptographic operations (3DES, AES).
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
Smart Card	Plastic card in credit card format with built-in chip
Software	Information (non-physical part of the system) which is required to implement functionality in conjunction with the hardware (program code)
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
Threat	Action or event that might prejudice security
User	Person in contact with a TOE who makes use of its operational capability
User Mode	Operational status phase of the TOE in which actions intended for the user takes place