PUBLIC

Common Criteria

Information Technology

Security Evaluation

Project Choctaw

Security Target Lite of S3CC924/S3CC928 16-bit RISC Microcontroller For Smart Cards

Version 1.2

30th March 2009

SAMSUNG ELECTRONICS

REVISION HISTORY

UPDATES:

Version	Date	Modification
1.0	20th August 2008	Creation
1.1	27th October 2008	BSI comments
1.2	30th March 2009	Chip version update

WRITERS:

Written by	Title
Bryant Kyungsuk Yi	Senior Engineer

CONTENTS

1 INTRODUCTION

2 This introductory chapter contains the following sections:

1.1 Security Target Identification

1.2 Security Target Overview

1.3 Common Criteria conformance & Evaluation Assurance Level

1.1 Security Target Identification

3 The Security Target version is 1.1 and dated 30th March 2009

4 The Security Target is based on the Smartcard IC Platform Protection Profile BSI-PP-0002 version 1.0, July 2001.

5 The Protection Profile and the Security Target are built on *Common Criteria version 2.3*.

- Title: Security Target of S3CC924/S3CC928 16-Bit RISC Microcontroller for Smart Cards
- Target of Evaluation: S3CC924/S3CC928 revision 3
- Provided by: Samsung Electronics Co., Ltd.
- Common Criteria version : *ISO/IEC 15408-2005(E) (CC V2.3) part 1 to 3*

1.2 Security Target Overview

6 The Target of Evaluation (TOE), the S3CC924/S3CC928 microcontroller is a smartcard integrated circuit which is composed of a processing unit, security components and contact based I/O ports, hardware circuit for testing purpose during the manufacturing process and volatile and non-volatile memories (hardware). The TOE also includes any IC Designer/Manufacturer proprietary IC Dedicated Software as long as it physically exists in the smartcard integrated circuit after being delivered by the IC Manufacturer. Such software (also known as IC firmware) is used for testing purpose during the manufacturing process but also provides additional services to facilitate the usage of the hardware and/or to provide additional services, including an *AIS20* compliant random number generation library. All other software is called Smartcard Embedded Software and is not part of the TOE.

7 The TOE are listed in title are identical in hardware and only its EEPROM memory size is different. EEPROM size can be selected by hardware circuit before wafer testing in TEST mode. Therefore unused EEPROM area of S3CC924 is blocked and protected by SF2: Access control (invalid address access).

1.3 CC Conformance & Evaluation Assurance Level

8 This security target conforms to *Common Criteria* version 2.3 (ISO15408) part 2 extended, part 3 conformant and conforms to the *Smartcard IC Platform Protection Profile BSI-PP-0002* version 1.0, July 2001. The assurance level is EAL4 augmented with components ADV_IMP2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4. The minimum strength of the TOE security functions is Strength of Functions High (“SOF high”).

2 TOE DESCRIPTION

9 This chapter 2 contains the following sections:

2.1 Product Description

2.2 TOE Definition

2.3 TOE Features

2.4 Interface of the TOE

2.5 TOE intended usage

2.1 Product Description

10 The Target of Evaluation (TOE), the S3CC924/S3CC928 microcontroller is a smartcard integrated circuit which is composed of a processing unit, security components and contact based I/O ports, hardware circuit for testing purpose during the manufacturing process and volatile and non-volatile memories (hardware). The TOE also includes any IC Designer/Manufacturer proprietary IC Dedicated Software as long as it physically exists in the smartcard integrated circuit after being delivered by the IC Manufacturer. Such software (also known as IC firmware) is used for testing purpose during the manufacturing process but also provides additional services to facilitate the usage of the hardware and/or to provide additional services, including an *AIS20* compliant random number generation library. All other software is called Smartcard Embedded Software and is not part of the TOE.

11 The S3CC924/S3CC928 single-chip CMOS micro-controller is designed and packaged specifically for "Smart Card" applications.

12 The CalmRISC16 CPU architecture of the S3CC924/S3CC928 microcontroller follows the Harvard style, that is, it has separate program memory and data memory. Both instruction and data can be fetched simultaneously without causing a stall, using separate paths for memory access.

13 The main security features of the S3CC924/S3CC928 integrated circuit are:

- Security sensors or detectors including High and Low Temperature detectors, High and Low Frequency detectors, High and Low Supply Voltage detectors, Supply Voltage Glitch detectors, Light detector and the Passivation Removal Detector
- An Active Shield against physical intrusive attacks
- Dedicated tamper-resistant design based on synthesizable glue logic and secure topology
- Dedicated hardware mechanisms against side-channel attacks such as Internal Variable Clock, Random Waits Generator, Random Current Generator, RAM and EEPROM encryption mechanisms
- Secure DES Symmetric Cryptography support
- A non-deterministic Random Number Generator
- The IC Dedicated Software includes:
  - A Deterministic Random Number Generator (DRNG) for AIS20-compliant Random Number Generation

14 The main hardware blocks of the S3CC924/S3CC928 Integrated Circuit are described in Figure 1 below:

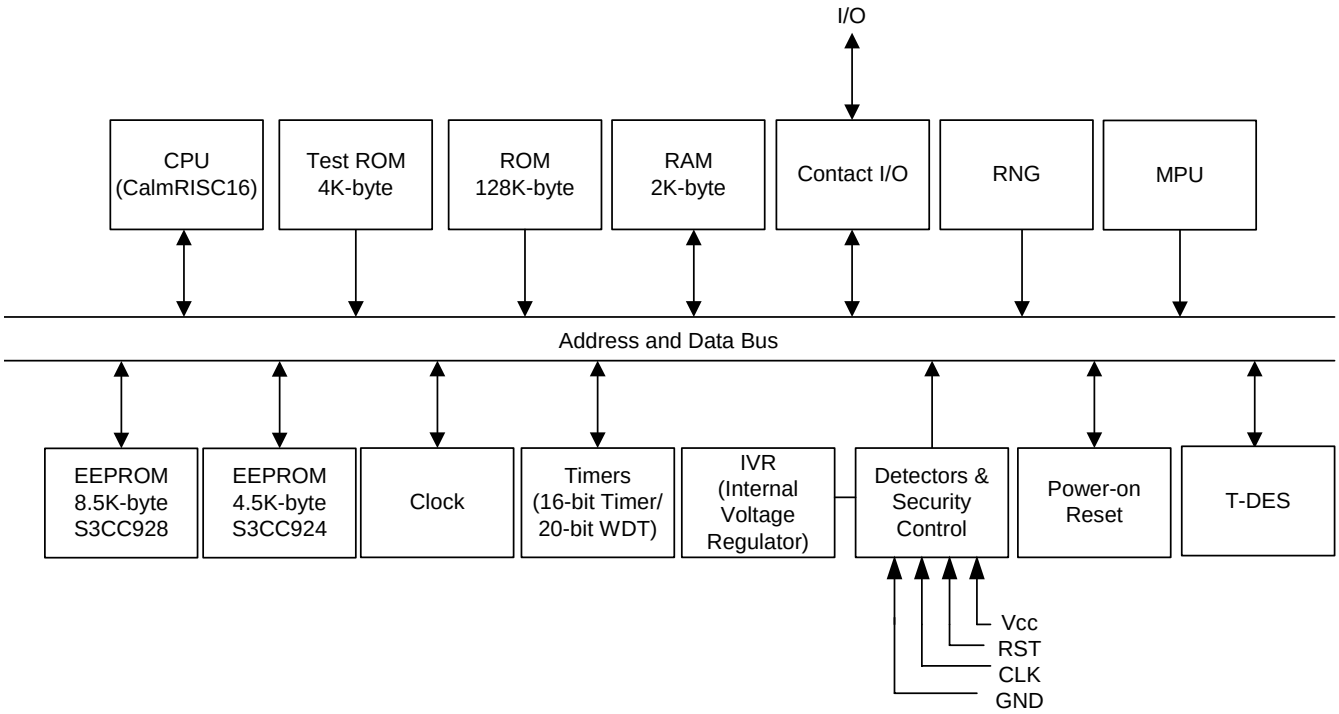

Figure1. S3CC924/S3CC928 Block Diagram

15 Note that only the Triple DES algorithm belongs to the TOE, not the Single DES.

2.2 TOE Definition

16 The TOE consists of the following Hardware and Software:

2.2.1 TOE Hardware

- 4.5K bytes EEPROM (S3CC924)/8.5K bytes EEPROM (S3CC928)
- 2K bytes RAM/128K User ROM/4K Test ROM
- 16-bit Central Processing Unit (CPU)
- Internal Voltage Regulator (IVR)
- Detectors & Security Logic
- A non-deterministic random number generator (RNG)
- Memory Protection Unit (MPU)
- Triple DES cryptographic coprocessor with 112 or 168 bits key size
- Hardware UART for contact
- Address & data buses
- Internal Clock
- Timers

2.2.2 TOE Software

17 The TOE software comprises the following components:

- Test ROM code that is used for testing the chip during production
- A Deterministic Random Number Generator (DRNG) that fulfills the requirements of *AIS 20*, Class K3, Strength of Function High.

18 The TOE configuration is summarized in table 1 below:

Item Type	Item	Version	Form of delivery
Hardware	S3CC924/S3CC928 16-Bit RISC Microcontroller for Smart Card	3	Wafer
Software	Test ROM Code	1.0	Included in S3CC924/S3CC928 Test ROM
Software	DRNG	2.0	Software Library
Document	Hardware User's manual	3.0	Softcopy
Document	Security Application Note	1.6	Softcopy

Table 1. TOE Configuration

2.3 TOE Features

CPU
- 16-bit CalmRISC16 core

Memory
- 128K-byte Program Memory (ROM)
- 4K- byte Test ROM
- 4.5K-byte Data/Program Memory (EEPROM) – S3CC924
- 8.5K-byte Data/Program Memory (EEPROM) – S3CC928
- 2K-byte Data Memory (RAM)

EEPROM Write Operations
- 1 to 128-byte erase/write operation
- 1.5msec erase/write time for each operation
- Min. 500,000 write/erase cycles
- Data retention for min. 10 years
- 128-bytes Read-only Area
- 128-bytes non erasable EEPROM (OTP)

Triple DES
- Built-in hardware Triple DES accelerator
- Circuit for resistance against SPA and DPA attacks

Abnormal Condition Detectors
- Abnormal Voltage/Frequency/Light/Temperature detectors
- Power glitch detector
- Inner insulation removal detector
- Active shield removal detector

Interrupts
- Two interrupt sources and vectors (FIQ,IRQ)
- Source for FIQ: Invalid memory access
- Sources for IRQ:
  - SIO Falling edge
  - 16-bit Timer
  - Watchdog Timer
  - Contact UART Tx/Rx
  - Software Interrupts

Serial I/O Interface
- UART for handling serial I/O interface in accordance with the ISO 7816 communication protocols

Reset and Power Down Mode

- Power-on reset and external reset
- Stop mode

16-Bit Random Number Generator

- One 16-bit RNG with non-deterministic internal oscillator
- Start/Stop control

Memory Encryption and BUS Scrambling

- Static bus scrambling
- Automatic RAM encryption
- EEPROM scrambling with User-defined value

Timers

- 16-Bit Timer with 8 Bit prescaler
- 20-bit Watchdog Timer

Clock Sources

- External clock: 1 MHz–5 MHz
- Internal clock: 2MHz–18MHz (non-divided)

Operating Voltage Range

- 1.62 V - 5.5 V

Operating Temperature

- - 25°C to 85°C

Package

- Wafer
- 8-pin COB (compliant with ISO 7816)

2.4 Interfaces of the TOE

- The physical interface of the TOE with the external environment is the entire surface of the IC
- The electrical interface of the TOE with the external environment is made of the chip's pads including the Vdd, RESETB, XCLK, GND, IO1, IO2 and FUSE.
- The data interface of the TOE is made of the Contact I/O pads.
- The software interface of the TOE with the hardware consists of Special Function Registers (SFR) and CPU instructions.

2.5 TOE Intended Usage

19 The TOE is dedicated to applications such as:

- Banking and finance applications for credit or debit cards, electronic purse (stored value cards) and electronic commerce.
- Network based transaction processing such a mobile phones (GSM SIM cards), pay TV (subscriber and pay-per-view cards), communication highways (Internet access and transaction processing).
- Transport and ticketing applications (access control cards).
- Governmental cards (ID cards, health cards, driving licenses).
- Multimedia applications and Digital Right Management protection.

3 TOE SECURITY ENVIRONMENT

20 This chapter 3 contains the following sections:

3.1 Definition of Assets

3.2 Assumptions

3.3 Threats

3.4 Organizational Security Policies

3.1 Definition of Assets

21 The primary assets to be protected are

- User's Data stored in the TOE memories (confidentiality and integrity)
- Smartcard Embedded Software for (confidentiality and integrity)
- Correct operation of the TOE (integrity)

22 Other primary assets are

- Random numbers generated by the TOE (confidentiality and integrity)

23 Other secondary assets are

- logical design data,
- physical design data,
- IC Dedicated Software, Initialization Data, Pre-personalization Data, TSF data
- specific development aids,
- test and characterization related data,
- material for software development support, and
- photomasks and products in any form

3.2 Assumptions

24 The following assumptions apply in this Security Target.

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

It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end-user to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).

A.Plat-Appl Usage of Hardware Platform

The Smartcard Embedded Software is designed so that the requirements from the following documents are met:

(i) S3CC924/S3CC928 User's manual

(ii) S3CC924/S3CC928 Security application Note

(iii) TOE application notes, and

(iv) Results from TOE evaluation reports relevant for the Smartcard Embedded Software.

A.Resp-Appl Treatment of User Data

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

25 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 e xecuted are part of the Smartcard Embedded Software. In contrast to this the threats T.Leak-Inherent and T.Leak-Forced address (i) the cryptographic routines which are part of the TOE and (ii) the processing of User Data including cryptographic keys.

3.3 Threats

26 According to the *Protection Profile BSI-PP-0002*, section 3.3 there are the following high-level security concerns:

SC1 Manipulation of User Data and of the Smartcard Embedded Software (while being executed/processed and while being stored in the TOE's memories)

SC2 Disclosure of User Data and of the Smartcard Embedded Software (while being processed and while being stored in the TOE's memories).

SC3 Deficiency of random numbers.

3.3.1 Standard Threats (referring to SC1 and SC2)

27 The TOE shall avert the threat "Inherent Information Leakage (T.Leak-Inherent)" as specified below.

T.Leak-Inherent Inherent Information Leakage

An attacker may exploit information which is leaked from the TOE during usage of the Smartcard in order to disclose confidential data (User Data or TSF data).

No direct contact with the Smartcard internals is required here. Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. One example is the Differential Power Analysis (DPA).

28 The TOE shall avert the threat "Physical Probing (T.Phys-Probing)" as specified below.

T.Phys-Probing Physical Probing

An attacker may perform physical probing of the TOE in order (i) to disclose User Data, (ii) to disclose/reconstruct the Smartcard Embedded Software or (iii) to disclose other critical operational information especially TSF data.

Physical probing requires direct interaction with the Smartcard Integrated Circuit internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of User Data may also be a pre-requisite.

29 The TOE shall avert the threat "Malfunction due to Environmental Stress (T.Malfunction)" as specified below.

T.Malfunction Malfunction due to Environmental Stress

An attacker may cause a malfunction of TSF or of the Smartcard Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functions of the TOE or (ii) deactivate or modify security functions of the Smartcard Embedded Software. This may be achieved by operating the Smartcard outside the normal operating conditions. To exploit this an attacker needs information about the functional operation.

30 The TOE shall avert the threat "Physical Manipulation (T.Phys-Manipulation)" as specified below.

T.Phys-Manipulation Physical Manipulation

An attacker may physically modify the Smartcard in order to (i) modify security features or functions of the TOE, (ii) modify security functions of the Smartcard Embedded Software or (iii) to modify User Data.

The modification may be achieved through techniques com-monly employed in IC failure analysis and IC reverse engineering efforts. The modification may result in the deactivation of a security function. Before that hardware security mechanisms and layout characteristics need to be

identified. Determination of software design including treatment of User Data may also be a pre-requisite. Changes of circuitry or data can be permanent or temporary.

In contrast to malfunctions (refer to T.Malfunction) the attacker requires to gather significant knowledge about the TOE's internal construction.

31 The TOE shall avert the threat "Forced Information Leakage (T.Leak-Forced)" as specified below:

T.Leak-Forced Forced Information Leakage

An attacker may exploit information which is leaked from the TOE during usage of the Smartcard in order to disclose confidential data (User Data or TSF data) even if the information leakage is not inherent but caused by the attacker.

This threat pertains to attacks where methods described in "Malfunction due to Environmental Stress" (refer to T.Malfunction) and/or "Physical Manipulation" (refer to T.Phys-Manipulation) are used to cause leakage

from signals which normally do not contain significant information about secrets.

32 The TOE shall avert the threat "Abuse of Functionality (T.Abuse-Func)" as specified below.

T.Abuse-Func Abuse of Functionality

An attacker may use functions of the TOE which may not used after TOE Delivery in order to (i) disclose or manipulate User Data, (ii) to manipulate (explore, bypass, deactivate change) security features or functions of the TOE or of the Smartcard Embedded Software or (iii) to enable an attack.

3.3.2 Threats related to Specific Functionality (referring to SC3)

33 The TOE shall avert the threat "Deficiency of Random Numbers (T.RND)" as specified below.

T.RND Deficiency of Random Numbers

An attacker may predict or obtain information about random numbers generated by the TOE for instance because of a lack of entropy of the random numbers provided.

An attacker may gather information about the produced random numbers which might be a problem because they may be used for instance to generate cryptographic keys.

Here the attacker is expected to take advantage of statistical properties of the random numbers generated by the TOE without specific knowledge about the TOE's generator. Malfunctions or premature ageing are also considered which may assist in getting information about random numbers.

3.3.3 Threats related to additional TOE Specific Functionality

34 The TOE shall avert the additional 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). Any restrictions are defined by the security policy of the specific application context and must be implemented by the Smartcard Embedded Software.

3.4 Organizational Security Policies

35 The IC Developer / Manufacturer must apply the policy "Protection during TOE Development and Production (P.Process-TOE)" as specified below.

P.Process-TOE Protection during TOE Development and Production

The TOE Manufacturer must ensure that the development and production of the Smartcard Integrated Circuit (Phase 2 up to TOE Delivery, refer to Section 2.1) is secure so that no information is unintentionally made available for the operational phase of the TOE. For example, the confidentiality and integrity of design information and test data shall be guaranteed; access to samples, development tools and other material shall be restricted to authorized persons only; scrap will be destroyed etc. This not only pertains to the TOE but also to all information and material exchanged with the developer of the Smartcard Embedded Software and therefore especially to the Smartcard Embedded Software itself. This includes the delivery (exchange) procedures for Phase 1 and the Phases after TOE Delivery as far as they can be controlled by the TOE Manufacturer.

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

36 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.

37 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:

- Triple Data Encryption Standard (3DES)

4 SECURITY OBJECTIVES

38 This chapter Security Objectives contains the following sections:

4.1 Security Objectives for the TOE

4.2 Security Objectives for Environment

4.1 Security objectives for the TOE

39 According to the Protection Profile[BSI-PP-0002] there are the following standard high-level security goals:

SG1	maintain the integrity of User Data and of the Smartcard Embedded Software (when being executed/processed and when being stored in the TOE's memories)
SG2	maintain the confidentiality of User Data and of the Smartcard Embedded Software (when being processed and when being stored in the TOE's memories).
SG3	provide random numbers.

40 These standard high-level security goals are refined below by defining security objectives as required by the *Common Criteria*. Note that the integrity of the TOE is a mean to reach these objectives.

4.1.1 Standard Security Objectives (referring to SG1 and SG2)

41 The TOE shall provide "Protection against Inherent Information Leakage (O.Leak-Inherent)" as specified below.

O.Leak-Inherent — Protection against Inherent Information Leakage

The TOE must provide protection against disclosure of confidential data (User Data or TSF data) stored and/or processed in the Smartcard IC

- by measurement and analysis of the shape and amplitude of signals (for example on the power, clock, or I/O lines) and
- by measurement and analysis of the time between events found by measuring signals (for instance on the power, clock, or I/O lines).

This objective pertains to measurements with subsequent complex signal processing whereas O.Phys-Probing is about direct measurements on elements on the chip surface. Details correspond to an analysis of attack scenarios which is not given here.

42 The TOE shall provide "Protection against Physical Probing (O.Phys-Probing)" as specified below.

O.Phys-Probing — Protection against Physical Probing

The TOE must provide protection against disclosure of User Data, against the disclosure/reconstruction of the Smartcard Embedded Software or against the disclosure of other critical operational information. This includes protection against

- measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or
- measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis)

with a prior

- reverse-engineering to understand the design and its properties and functions.

The TOE must be designed and fabricated so that it requires a high combination of complex equipment, knowledge, skill, and time to be able to derive detailed design information or other information which could be used to compromise security through such a physical attack.

43 The TOE shall provide "Protection against Malfunctions (O.Malfunction)" as specified below.

O.Malfunction Protection against Malfunctions

The TOE must ensure its correct operation.

The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation has not been proven or tested. This is to prevent errors. The environmental conditions may include voltage, clock frequency, temperature, or external energy fields.

Remark: A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the objective O.Phys-Manipulation) provided that detailed knowledge about the TOE´s internal construction is required and the attack is performed in a controlled manner.

44 The TOE shall provide "Protection against Physical Manipulation (O.Phys-Manipulation)" as specified below.

O.Phys-Manipulation Protection against Physical Manipulation

The TOE must provide protection against manipulation of the TOE (including its software and TSF data), the Smartcard Embedded Software and the User Data. This includes protection against

- reverse-engineering (understanding the design and its properties and functions),
- manipulation of the hardware and any data, as well as
- controlled manipulation of memory contents (User Data).

The TOE must be designed and fabricated so that it requires a high combination of complex equipment, knowledge, skill, and time to be able to derive detailed design information or other information which could be used to compromise security through such a physical attack.

45 The TOE shall provide "Protection against Forced Information Leakage (O.Leak-Forced)" as specified below:

O.Leak-Forced Protection against Forced Information Leakage

The Smartcard must be protected against disclosure of confidential data (User Data or TSF data) processed in the Card (using methods as described under O.Leak-Inherent) even if the information leakage is not inherent but caused by the attacker

- by forcing a malfunction (refer to "Protection against Malfunction due to Environmental Stress (O.Malfunction)" and/or\
- by a physical manipulation (refer to "Protection against

Physical Manipulation (O.Phys-Manipulation)". If this is not the case, signals which normally do not contain significant information about secrets could become an information channel for a leakage attack.

46 The TOE shall provide "Protection against Abuse of Functionality (O.Abuse-Func)" as specified below.

O.Abuse-Func Protection against Abuse of Functionality

The TOE must prevent that functions of the TOE which may not be used after TOE Delivery can be abused in order (i) to disclose critical User Data, (ii) to manipulate critical User Data of the Smartcard Embedded Software, (iii) to manipulate Soft-coded Smartcard Embedded Software or (iv) bypass, deactivate, change or explore security features or functions of the TOE. Details depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

47 The TOE shall provide "TOE Identification (O.Identification)" as specified below:

O.Identification TOE Identification

The TOE must provide means to store Initialisation Data and Pre-personalisation Data in its non-volatile memory. The Initialisation Data (or parts of them) are used for TOE identification.

4.1.2 Security Objectives related to Specific Functionality (referring to SG3)

48 The TOE shall provide "Random Numbers (O.RND)" as specified below.

O.RND Random Numbers

The TOE will ensure the cryptographic quality of random number generation. For instance random numbers shall not be predictable and shall have sufficient entropy.

The TOE will ensure that no information about the produced random numbers is available to an attacker since they might be used for instance to generate cryptographic keys.

4.1.3 Security Objectives for Added Function

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

O.Add-Functions Additional Specific Security Functionality

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

- Triple Data Encryption Standard (3DES)

50 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 is controlled as required, for example, in a multi-application environment.

4.2 Security objectives for the Environment

4.2.1 Phase 1

51 The Smartcard Embedded Software shall provide "Usage of Hardware Platform (OE.Plat-Appl)" as specified below.

OE.Plat-Appl Usage of Hardware Platform

To ensure that the TOE is used in a secure manner the Smartcard Embedded Software shall be designed so that the requirements from the following documents are met:

(i) S3CC924/S3CC928 User's manual

(ii) S3CC924/S3CC928 Security Application Note

(iii) TOE application notes, and

(iv) Results from the TOE evaluation reports relevant for the Smartcard Embedded Software.

52 The Smartcard Embedded Software shall provide "Treatment of User Data (OE.Resp-Appl)" as specified below.

OE.Resp-Appl Treatment of User Data

Security relevant User Data (especially cryptographic keys) are treated by the Smartcard Embedded Software as required by the security needs of the specific application context.

For example the Smartcard Embedded Software will not disclose security relevant user data to unauthorised users or processes when communicating with a terminal.

4.2.2 Phase 2 up to TOE Delivery

53 The TOE Manufacturer shall ensure the "Protection during TOE Development and Production (OE.Process-TOE)" as specified below.

OE.Process-TOE	Protection during TOE Development and Production The TOE Manufacturer must ensure that the development and production of the Smartcard Integrated Circuit (Phases 2 and 3 up to TOE Delivery, refer to Section 2.1) is secure so that no information is unintentionally made available for the operational phase of the TOE. For example, the confidentiality and integrity of design information and test data must be guaranteed, access to samples, development tools and other material must be restricted to authorised persons only, scrap must be destroyed. This not only pertains to the TOE but also to all information and material exchanged with the developer of the Smartcard Embedded Software and therefore especially to the Smartcard Embedded Software itself. This includes the delivery (exchange) procedures for Phase 1 and the Phases after TOE Delivery as far as they can be controlled by the TOE Manufacturer. An accurate identification must be established for the TOE. This requires that each instantiation of the TOE carries this unique identification. In order to make this practical, electronic identification shall be possible.

4.2.3 TOE Delivery up to the end of Phase 6

54 Appropriate "Protection during Packaging, Finishing and Personalisation (OE.Process-Card)" must be ensured after TOE Delivery up to the end of Phases 6, as well as during the delivery to Phase 7 as specified below.

OE.Process-Card	Protection during Packaging, Finishing and Personalisation Security procedures shall be used after TOE Delivery up to delivery to the end-user to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthoriseduse). This means that Phases after TOE Delivery up to the end of Phase 6 (refer to Section 2.1) must be protected appropriately.

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

55 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)".

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

57 For the separation of different applications the Smartcard Embedded Software may implement a memory management scheme based upon security mechanisms of the TOE as required by the security policy defined for the specific application context.

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

58 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.

59 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.

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

61 The treatment of User Data is still required when a multi-application operating system is implemented as part of the Smartcard Embedded Software on the TOE. In this case the multi-application operating system should not disclose security relevant user data of one application to another application when it is processed or stored on the TOE.

5 IT SECURITY REQUIREMENTS

62 This chapter 5 IT Security Requirements contains the following sections:

5.1 TOE Security Requirements

5.2 Security Requirements for the Environment

5.1 TOE security requirements

5.1.1 TOE security functional requirements

63 In order to define the Security Functional Requirements the Part 2 of the Common Criteria was used. However, some Security Functional Requirements have been newly created and are not taken from Part 2 of the Common Criteria. Therefore, this Security Target is characterized by "Part 2 extended".

5.1.1.1 Malfunctions

64 The TOE shall meet the requirement "Limited fault tolerance (FRU_FLT.2)" as specified below.

FRU_FLT.2	Limited fault tolerance
Hierarchical to:	FRU_FLT.1
FRU_FLT.2.1	The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: *exposure to operating conditions which are not detected according to the requirement Failure with preservation of secure state (FPT_FLS.1) .*
Dependencies:	FPT_FLS.1 Failure with preservation of secure state
Refinement:	The term "failure" above means "circumstances". The TOE prevents failures for the "circumstances" defined above.

65 The TOE shall meet the requirement "Failure with preservation of secure state (FPT_FLS.1)" as specified below.

FPT_FLS.1	Failure with preservation of secure state
Hierarchical to:	No other components.
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: exposure to operating *conditions which may not be tolerated according to the requirement Limited fault tolerance (FRU_FLT.2) and where therefore a malfunction could occur.*
Dependencies:	ADV_SPM.1 informal TOE security policy model
Refinement:	The term "failure" above also covers "circumstances". The TOE prevents failures for the "circumstances" defined above.

66 The TOE shall meet the requirement "TSF domain separation" state (FPT_SEP.1)" as specified below.

FPT_SEP.1	TSF domain separation
Hierarchical to:	No other components.
FPT_SEP.1.1	The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.
FPT_SEP.1.2	The TSF shall enforce separation between the security domains of subjects in the TSC.
Dependencies:	No dependencies.
Refinement:	Those parts of the TOE, which support the security functional requirements "Limited fault tolerance (FRU_FLT.2)" and "Failure with preservation of secure state (FPT_FLS.1)" shall be protected from interference of the Smartcard Embedded Software.

5.1.1.2 Abuse of Functionality

67 The TOE shall meet the requirement "Limited capabilities (FMT_LIM.1)" as specified below (Common Criteria Part 2 extended).

FMT_LIM.1	Limited capabilities
Hierarchical to:	No other components.
FMT_LIM.1.1	The TSF shall be designed in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced: *Deploying Test Features after TOE Delivery does not allow User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks.*
Dependencies:	FMT_LIM.2 Limited availability.

68 The TOE shall meet the requirement "Limited availability (FMT_LIM.2)" as specified below (Common Criteria Part 2 extended).

FMT_LIM.2	Limited availability
Hierarchical to:	No other components.
FMT_LIM.2.1	The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced: *Deploying Test Features after TOE Delivery does not allow User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks.*
Dependencies:	FMT_LIM.1 Limited capabilities.

69 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 other components.
FAU_SAS.1.1	The TSF shall provide test personnel before TOE Delivery with the capability to store the Initialisation Data and/or Prepersonalisation *Data and/or supplements of the Smartcard Embedded Software* [8] in the audit records.
Dependencies:	No dependencies.

5.1.1.3 Physical Manipulation and Probing

70 The TOE shall meet the requirement "Resistance to physical attack (FPT_PHP.3)" as specified below.

FPT_PHP.3	Resistance to physical attack
Hierarchical to:	No other components.
FPT_PHP.3.1	The TSF shall resist *physical manipulation and physical probing* [10] to the *TSF* [11] by responding automatically such that the TSP is not violated.
Dependencies:	No dependencies.
Refinement:	The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, "automatic response" means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

5.1.1.4 Leakage

71 The TOE shall meet the requirement "Basic internal transfer protection (FDP_ITT.1)" as specified below.

FDP_ITT.1	Basic internal transfer protection
Hierarchical to:	No other components.
FDP_ITT.1.1	The TSF shall enforce the *Data Processing Policy* to prevent the *disclosure* of user data when it is transmitted between physically-separated parts of the TOE.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
Refinement:	The different memories, the CPU and other functional units of the TOE (e.g. a cryptographic co-processor) are seen as physically-separated parts of the TOE.

72 The TOE shall meet the requirement "Basic internal TSF data transfer protection (FPT_ITT.1)" as specified below.

FPT_ITT.1	Basic internal TSF data transfer protection
Hierarchical to:	No other components.
FPT_ITT.1.1	The TSF shall protect TSF data from *disclosure* when it is transmitted between separate parts of the TOE.
Dependencies:	No dependencies.
Refinement:	The different memories, the CPU and other functional units of the TOE (e.g. a cryptographic co-processor) are seen as separated parts of the TOE. This requirement is equivalent to FDP_ITT.1 above but refers to TSF data instead of User Data. Therefore, it should be understood as to refer to the same *Data Processing Policy* defined under FDP_IFC.1 below.

73 The TOE shall meet the requirement " Subset information flow control (FDP_IFC.1)"as specified below:

FDP_IFC.1	Subset information flow control
Hierarchical to:	No other components.
FDP_IFC.1.1	The TSF shall enforce the Data Processing Policy on *all confidential data when they are processed or transferred by the TOE or by the Smartcard Embedded Software*.
Dependencies:	FDP_IFF.1 Simple security attributes
Data Processing Policy	User Data and TSF data shall not be accessible from the TOE except when the Smartcard Embedded Software decides to communicate the User Data via an external interface. The protection shall be applied to confidential data only but without the distinction of attributes controlled by the Smartcard Embedded Software.

5.1.1.5 Random Numbers

74 The TOE shall meet the requirement "Quality metric for random numbers (FCS_RND.1)" as specified below (Common Criteria Part 2 extended).

FCS_RND.1	Quality metric for random numbers
FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet the *AIS20 version 1, Functional Classes and Evaluation Methodology for Deterministic Random Number Generators,* 2 December 1999, Class K3 Strength of Function High requirements.
Dependencies:	No dependencies.

5.1.1.6 Memory access control

75 Usage of multiple applications in one Smartcard often requires separating code and data in order to prevent that one application can access code and/or data of another application. To support this the TOE provides Area based Memory Access Control.

76 The security service being provided is described in the Security Function Policy (SFP) **Memory Access Control Policy**. The security functional requirement **"Subset access control (FDP_ACC.1)"** requires that this policy is in place and defines the scope were it applies. The security functional requirement **"Security attribute based access control (FDP_ACF.1)"** defines addresses security attribute usage and characteristics of policies. It describes the rules for the function that implements the Security Function Policy (SFP) as identified in FDP_ACC.1. The decision whether an access is permitted or not is taken based upon attributes allocated to the software. The user 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.

77 The security functional requirement **"Static attribute initialization (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).

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

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

Memory Access Control Policy

The TOE shall control *read, write, delete, execute accesses of software running at between two different modes (privilege and user mode)* on *data including code stored in memory areas.*

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

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

FDP_ACC.1	Subset access control
Hierarchical to:	No other components.
FDP_ACC.1.1	The TSF shall enforce the *Memory Access Control Policy* on *all subjects (software with privilege mode and user mode), all objects (data including code stored in memories) and all the operations defined in the Memory Access Control Policy.* Subjects are software codes in Privilege and User mode. Object are data stored in ROM, RAM and EEPROM memories.
Dependencies:	FDP_ACF.1 Security attribute based access control

81 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

The attributes are all the operations related to the data stored in memories, which are the *read, write, delete* and *execute* operations.

Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the Memory Access Control Policy to objects based on the *memory area where the software is executed from and/or the memory area where* the *access is performed to and/or the operation to be performed.*

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

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

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

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

82 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.

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

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

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

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

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

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

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

FMT_SMF.1	Specification of management functions
Hierarchical to:	No other components
FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions*: access the control registers of the address filter*.
Dependencies:	No dependencies

5.1.1.7 Cryptographic Support

85 FCS_COP.1n 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.

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

- Triple Data Encryption Standard (3DES) with 112bit or 168bit key size,

5.1.1.7.1 Triple-DES Operation

87 The Triple DES (3DES) operation of the TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below.

FCS_COP.1	Cryptographic operation
Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *Triple Data Encryption Standard (3DES)* with 112bit or 168bit key size that meet the following standards: *U.S. Department of Commerce / National Bureau of Standards, Data Encryption Standard (DES), FIPS PUB 46-3, 1999 October 25, keying option 2*
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes

5.1.1.7.2 Summary of Security Functional Requirements

Security Functional Requirements
Limited fault tolerance (FRU_FLT.2)
Failure with preservation of secure state (FPT_FLS.1)
TSF Domain Separation (FPT_SEP.1)
Audit storage (FAU_SAS.1[1])
Limited capabilities(FMT_LIM.1[1])
Limited availability (FMT_LIM.2[1])
Resistance to physical attack (FPT_PHP.3)
Basic internal transfer protection (FDP_ITT.1)
Basic internal TSF data transfer protection (FPT_ITT.1)
Subset information flow control (FDP_IFC.1)
Quality metric for random numbers (FCS_RND.1[1])

Table 2. Security Functional Requirements defined in Smart Card IC Protection Profile

Note [1]: Security Functional Requirement coming from *Protection Profile BSI-PP-0002 version 1.0*, not from *Common Criteria version 2.3 Part 2*

Security Functional Requirements
Subset access control (FDP_ACC.1)
Security attribute based access control (FDP_ACF.1)
Static attribute initialization (FMT_MSA.3)
Management of security attributes (FMT_MSA.1)
Specification of management functions (FMT_SMF.1)
Cryptographic operation (FCS_COP.1)

Table 3. Augmented Security Functional Requirements

5.1.2 TOE Assurance Requirements

88 The Security Target to be developed based upon this Protection Profile will be evaluated according to

Security Target evaluation (Class ASE)

89 The TOE Assurance Requirements for the evaluation of the TOE and its development and operating environment are those taken from the

Evaluation Assurance Level 5 (EAL5)

and augmented by the following components

ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4.

90 corresponding to level "EAL5+".

91 All refinements from *Protection Profile BSI-PP-0002 version 1.0* for the assurance requirements (ACM_CAP.4, ADO_DEL.2, ADO_IGS.1, AGD_ADM.1, AGD_USR.1, and ATE_COV.2) have to be taken into consideration.

Development activities (Class ADV)
Functional Specification (Component ADV_FSP.3)
Security Policy Modelling (Component ADV_SPM.3)
High-Level Design (Component ADV_HLD.3)
Low-Level Design (Component ADV_LLD.1)
Implementation Representation (Component ADV_IMP.2)
TSF internals (Component ADV_INT.1)
Representation Correspondence (Component ADV_RCR.2)

Tests activities (Class ATE)
Coverage (Component ATE_COV.2)
Depth (Component ATE_DPT.2)
Functional Tests (Component ATE_FUN.1)
Independent Testing (Component ATE_IND.2)

Delivery and operation activities (Class ADO)
Delivery (Component ADO_DEL.2)
Installation, generation, and start-up (Component ADO_IGS.1)

Guidance documents activities (Class AGD)
Administrator Guidance (Component AGD_ADM.1)
User guidance (Component AGD_USR.1)

Configuration management activities (Class ACM)
CM automation (Component ACM_AUT.1)
CM Capabilities (Component ACM_CAP.4)
CM Scope (Component ACM_SCP.3)

Life cycle support activities (Class ALC)
Development Security (Component ALC_DVS.2)
Life Cycle Definition (Component ALC_LCD.2)
Tools and Techniques (Component ALC_TAT.2)

Vulnerability assessment activities (Class AVA)
Covert Channel Analysis (Component AVA_CCA.1)
Misuse (Component AVA_MSU.3)
Strength of TOE Security Functions (Component AVA_SOF.1)
Vulnerability Analysis (Component AVA_VLA.4)

5.2 Security Requirements for the Environment

5.2.1 Security Requirements for the IT-Environment

92 The security functional requirement "Cryptographic operation (FCS_COP.1)" met by TOE has the following dependencies:

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

93 These requirements all address the appropriate management of cryptographic keys used by the specified cryptographic function. All 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.

5.2.1.1 Triple DES

94 The environment shall meet the requirement "Import of user data without security attributes (FDP_ITC.1)" or "Import of user data with security attributes (FDP_ITC.2)" or "Cryptographic key generation (FCS_CKM.1)" as specified below.

FDP_ITC.1	Import of user data without security attributes
Hierarchical to:	No other components.
FDP_ITC.1.1	The TSF shall enforce *the Access Control Policy or Information Flow Control Policy* when importing user data, controlled under the SFP, from outside of the TSC.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.
FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: *Access Control Policy or Information Flow Control Policy* .
Dependencies:	[FDP_ITC.2 Import of user data with security attributes, or FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation
FDP_ITC.2	Import of user data with security attributes
Hierarchical to:	No other components.
FDP_ITC.2.1	The TSF shall enforce the *Access Control Policy or Information Flow Control Policy* when importing user data, controlled under the SFP, from outside of the TSC.
FDP_ITC.2.2	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4	The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.
FDP_ITC.2.5	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: *Access Control Policy or Information Flow Control Policy*
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency
FCS_CKM.1	Cryptographic keys generation

Hierarchical to: No other components.

FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *Triple DES* (*3DES*) and specified cryptographic key sizes 112 bit or 168 bit that meet the following: *U.S. Department of Commerce / National Bureau of Standards Data Encryption Standard (DES), FIPS PUB 46-3, 1999 October 25, keying option 2.*
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction FMT_MSA.2 Secure security attributes

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

FCS_CKM.4	Cryptographic key destruction
Hierarchical to:	No other components.
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *change key and change key with certificate verification* that meets the following: *ISO/IEC 7816.*
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation] FMT_MSA.2 Secure security attributes

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

FMT_MSA.2	Secure security attributes
Hierarchical to:	No other components.
FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for security attributes.
Dependencies:	ADV_SPM.1 Informal TOE security policy model [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]

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

5.2.2 Security Requirements for the Non-IT-Environment

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

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

The developers shall design and implement the Smartcard Embedded Software in such way that it meets the requirements from the following documents:

(i) S3CC924/S3CC928 user's manual,
(ii) Security application note,
(iii) TOE-application notes and
(iv) findings of the TOE evaluation reports relevant for the Smartcard Embedded Software.

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

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

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

The Card Manufacturer (after TOE Delivery up to the end of Phase 6) shall use adequate security measures to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).

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

RE.Cipher Cipher Schemas

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

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

6 TOE SUMMARY SPECIFICATION

100 This chapter 6 TOE Summary Specification contains the following sections:

6.1 List of Security Functions

6.2 Relationship between security functions and functional requirements

6.3 Assurances Measures

6.1 List of Security Functions

SF1: Environmental Security violation recording and reaction

1) **Detectors**

101 These functions records in register the events notified by the detectors (refer to list below). The software configures the reaction in case of detection:

- The TOE is immediately reset when an event is detected.
- Or, a special function register bit is set.

List of detectors:

- Abnormal frequency Detector
- Abnormal voltage Detector
- Abnormal temperature Detector
- Light Detector
- Inner insulation removal Detector
- Active shield removal Detector
- Power Glitch Detector

2) Filters

102 These filters are used for preventing noise, glitches and extremely high frequency in the external reset or clock pad from causing undefined or unpredictable behavior of the chip.

- High Frequency Filter.
- Reset Noise Filter:

103 Security Function 1 covers the following Security Functional Requirements:

104 FPT_FLS.1: Failure with preservation of secure state. The detection thresholds of SF1 detectors are inside the operating range of the TOE. Therefore abnormal events/failures are detected before the secure state is compromised. This allows to take User's defined appropriate actions by software or to immediately RESET the TOE.

105 FRU_FLT.2: Limited fault tolerance. All operating signals (Clock, RESET and supply voltage) are filtered/regulated in order to prevent malfunction.

106 FPT_SEP.1: TSF domain separation. SF1 filters and detectors are implemented by the hardware. The filtering and detection cannot be affected or bypassed by Smartcard Embedded Software. The reaction to the detection can be configured by the software. The influence on security and the way how to configure it is described in details in the S3CC924/S3CC928 *User's Manual*. Therefore, FPT_SEP.1 is implemented by SF1.

107 FPT_PHP.3: Resistance to physical attacks. This requirement is achieved by security feature as the Active shield must be removed and bypassed in order to perform physical intrusive attacks

SF2: Access Control

1) **Security registers access control**

108 This security function manages access to the security control registers through access control security attributes.

109 The USER mode has another function, which is write-enable bit for security related registers. If user does not enable this bit in 128cycles after the reset, user cannot write security control registers any more.

2) Invalid address access

110 This function detects invalid address access occurrence. In case of an invalid address access is detected, an FIQ is evoked. The memory access rights are defined and configured trough the control register MASCON and an address filter.

111 The address filter provides the Embedded Software the ability to define access rights for data and program memory areas. In case of an illegal memory access, a non-maskable interrupt (FIQ) is generated, allow to take dedicated and appropriate actions.

3) Access rights for the code executed in EEPROM

112 This security function manages the code execution in EEPROM, through access control security attributes. If an invalid access is detected, then a FIQ occurs.

113 Security Function 2 covers the following Security Functional Requirements:

114 FDP_ACC.1: Subset access control. The address filter allows defining different memory areas with different access rights.

115 FDP_ACF.1: Security attributes based access control. This is covered by the Privilege and User modes of the TOE.

116 FMT_MSA.3: Static attribute initialization. All Special Function Registers have DEFAULT values after Power on Reset.

117 FMT_MSA.1: Management of security attributes. This is achieved with an address filter feature.

118 FMT_SMF.1: Specification of management functions. This is achieved via access to Special Function Registers.

119 FPT_SEP.1: TSF domain separation. Security domains are maintained since accesses to the access-prohibited area are trapped by this access control function. Therefore, FPT_SEP.1 is implemented by this SF.

SF3: Non-reversibility of TEST and NORMAL modes

The NORMAL mode of the TOE consists of PRIVILEGE mode and USER mode (cf. chapter 2.3 of this document).

1) Non-reversibility of TEST mode and NORMAL mode

120 This function disables the TEST mode and enables the NORMAL mode of the TOE. This function ensures the non-reversibility of the NORMAL mode. This function is used once during the manufacturing process.

2) **TEST mode communication protocol and data commands**

121 This function is the proprietary protocol used to operate the chip in TEST mode. This function enforces the identification and authentication of the TEST administrator during the test phase of the manufacturing process. The Strength of this function (SOF) is: High

3) Functional Tests

122 During the manufacturing process, the operation of the TOE and the embedded software checksum are verified. This security function ensures the correct operation of the TOE security functions and the integrity of the embedded software.

4) Identification

123 During the TEST mode of manufacturing process, traceability data are written in the non-volatile memory of the TOE. Once the TOE is switched from TEST to NORMAL mode, those traceability data are READ ONLY and cannot be modified anymore. This enables to identify and track the TOE during the rest of its life.

124 Security Function 3 covers the following Security Functional Requirements:

125 FAU_SAS.1: Audit Storage. This is fulfilled by the traceability/identification data written once and for all during the TEST mode of the manufacturing process.

126 FMT_LIM.1: Limited capabilities. TEST mode can be accessed only by the TEST administrator by supplying an authentication password through a proprietary protocol.

127 FMT_LIM.2: Limited availability. TEST mode can be accessed only by the TEST administrator by supplying an authentication password through a proprietary protocol.

SF4: Hardware countermeasures for unobservability

This Security Function is ensured by the combination of the following security features.

1) **Static Address/Data scrambling for bus and memory**

128 This function protects memory and address/data bus from probing attacks.

2) **Memory encryption**

129 This security function protects the memory contents of the TOE from data analysis on the stored data as well as on internally transmitted data. The algorithms used for encryption are proprietary. The ROM encryption is static key while the RAM and the EEPROM encryption is dynamic key. RAM encryption is performed automatically while EEPROM encryption is defined and managed by the embedded software.

3) Synthesizable processor core

130 The Central Processing Unit (CPU) of the TOE is synthesizable with glue logic, which makes reverse engineering and signal identification more difficult. Most sensitive hardware components such as buses are also hidden and implemented in deepest layers.

4) De-synchronization and signal-to-noise ratio reduction mechanisms

131 The TOE operations can be made asynchronous by using the Internal Variable Clock and the Random Wait Generator security features. They make a full range of intrusive (e.g. probing attacks) and non intrusive attacks (e.g. side-channel attacks) more complex and difficult.

132 Security Function 4 covers the following Security Functional Requirements:

133 FPT_PHP.3: Resistance to physical attacks. This requirement is achieved by bypassed in order to perform physical intrusive attacks and by security features 1) and 3) that makes the reverse-engineering of the TOE layout unpractical.

134 FDP_IFC.1: Subset information flow control. This requirement is covered by security feature 2).

135 FDP_ITT.1: Basic internal transfer protection. This requirement is achieved by the combination of the TOE security features 1) to 4) as it is unpractical to get access to internal signals and interpret them.

136 FPT_ITT.1: Basic internal TSF data transfer protection. This requirement is achieved by the combination of the TOE features 1) to 4) as it is unpractical to get access to internal signals and interpret them.

SF5: Cryptography

1) Triple Data Encryption Standard Engine

137 This function is used for encrypting and decrypting data using the Triple DES symmetric algorithm with 112bit or 168bit key size.

2) Random Number Generator

138 This function is used for generating random numbers for security process in smart card applications and provides a mechanism to generate random numbers. It includes two functions:

- A random SEED Generation algorithm that generates a truly random number
- A Digital Random Number Generator (DRNG) algorithm compliant with *AIS 20* class K3 SOF High requirements.

139 Security Function 5 covers the following Security Functional Requirements:

140 FCS_RND.1: Quality metric for random number. This requirement is ensured by the design of the random number generation algorithm that follows the requirements and the metric of the *AIS20* Class K3 SOF High standard.

141 FCS_COP.1: Cryptographic operation. This requirement is provided by the TOE.

6.2 Relationship between security functions and functional requirements

142 The following table shows that the set of Security Functions covers all Functional Requirements:

SF \ SR	FAU_SAS.1	FDP_IFC.1	FDP_ITT.1	FMT_LIM.1	FMT_LIM.2	FPT_FLS.1	FPT_PHP.3	FPT_ITT.1	FPT_SEP.1	FRU_FLT.2	FDP_ACC.1	FDP_ACF.1	FMT_MSA.3	FMT_MSA.1	FMT_SMF.1	FCS_RND.1	FCS_COP.1 (3DES)
SF1						✔	✔		✔	✔							
SF2									✔		✔	✔	✔	✔	✔		
SF3	✔			✔	✔												
SF4		✔	✔				✔	✔									
SF5																✔	✔

Table 4. Relationship between security function and functional requirement

6.3 Assurance Measures

Assurance Class	Assurance Family	Assurance Component	Assurance measure (document reference)
Security Target	ASE		Security Target
ACM: Configuration Management	ACM_AUT	**1**	Configuration Management Documentation (Class ACM)
	ACM_CAP	**4**	
	ACM_SCP	**2**	
ADO: Delivery and Operation	ADO_DEL	**2**	Delivery Procedures Documentation (Class ADO)
	ADO_IGS	**1**	Installation, generation and start-up Procedures (Class ADO)
ADV: Development	ADV_FSP	**1**	Functional Specification (Class ADV)
	ADV_HLD	**1**	High Level Design (Class ADV)
	ADV_LLD	**1**	Low Level Design (Class ADV)
	ADV_IMP	**2**	Implementation (Class ADV)
	ADV_RCR	**1**	All representation correspondence analyses are included in the relevant TOE representation documentation (FSP, HLD, LLD, IMP)
	ADV_SPM	**1**	Security Policy Model (Class ADV)
AGD: Guidance Documents	AGD_ADM	**1**	Guidance Documentation (Class AGD)
	AGD_USR	**1**	
ALC: Life Cycle Support	ALC_DVS	**2**	Development Security Procedures (Class ALC)
	ALC_LCD	**1**	Life Cycle Definition Documentation (Class ALC)
	ALC_TAT	**1**	Development Tool Documentation (Class ALC)
ATE: Tests	ATE_COV	**2**	Test Coverage Analysis (Class ATE)
	ATE_DPT	**1**	Test Depth Analysis (Class ATE) is described in Test Documentation (Class ATE)
	ATE_FUN	**1**	Test Documentation (Class ATE),
	AVA_MSU	**3**	Analysis of the Guidance Documentation (Class AVA)
	AVA_SOF	**1**	Strength of TOE SF Analysis (Class AVA)
	AVA_VLA	**4**	Vulnerability Analysis (Class AVA)

Table 5. Assurance measures table

7 PP CLAIMS

143 This chapter 7 PP Claims contains the following sections:

7.1 PP Reference

7.2 PP Tailoring

7.3 PP Auditions

7.1 PP reference

144 This security target conforms to the Smartcard IC Platform Protection Profile [BSI-PP-0002].

7.2 PP tailoring

145 The only tailoring made to the Smartcard IC Platform Protection Profile [BSI-PP-0002] is FCS_RND as described in section 5.1.1.5.

7.3 PP additions

146 Additional objectives and security functional requirements are explicitly mentioned in this Security Target:

147 One additional assumption A.Key-Function as described in section 3.2

148 One additional threat T.Mem-Access as described in section 3.3.3

149 One additional security policy P.Add-Functions as described in section 3.4.1,

150 Two additional security objectives O.Add-Functions and O.Mem-Access as described in section 4.1.3,

151 Additional functional requirements FDP_ACC.1, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, and FCS_COP.1, as described in section 5.1.1,

152 Additional functional requirements for the environment FDP_ITC.1, FDP_ITC.2, FCS_CKM.1, and FCS_CKM.4 as described in section 5.2.1,

153 One additional requirement for the non-IT environment RE.Cipher as described in section 5.2.2.

8 RATIONALE

154 This chapter 8 Rational contains the following sections:

8.1 Security Objectives Rationale

8.2 Security Requirements Rationale

8.3 Security Requirements are Mutually Supportive and Internally Consistent

8.1 Security Objectives Rationale

Assumption, Threat or Organisational Security Policy	Security Objective	Note
A.Plat-Appl	OE.Plat-Appl	(Phase 1)
A.Resp-Appl	OE.Resp-Appl	(Phase 1)
P.Process-TOE	OE.Process-TOE O.Identification	(Phase 2 – 3)
A.Process-Card	OE.Process-Card	Card (Phase 4 – 6)
T.Leak-Inherent	O.Leak- Inherent	
T.Phys_Probing	O.Phys-Probing	
T.Malfunction	O.Malfunction	
T.Phys-Manipulation	O.Phys-Manipulation	
T.Leak-Forced	O.Leak-Forced	
T.Abuse-Func	O.Abuse-Func	
T.RND	O.RND	
T.Mem-Access	O.Mem-Access	
P.Add-Functions	O.Add-Functions	
A.Key-Function	OE.Plat-Appl OE.Resp-Appl	

Table 6. Security Objectives versus Assumptions, Threats or Policies

155 The justification related to the assumption “Usage of Hardware Platform (A.Plat-Appl)” is as follows:

156 Since OE.Plat-Appl requires the Smartcard Embedded Software developer to implement those measures assumed in A.Plat-Appl, the assumption is covered by the objective.

157 The justification related to the assumption “Treatment of User Data (A.Resp-Appl)” is as follows:

158 Since OE.Resp-Appl requires the developer of the Smartcard Embedded Software to implement measures as assumed in A.Resp-Appl, the assumption is covered by the objective.

159 The justification related to the organisational security policy “Protection during TOE Development and Production (P.Process-TOE)” is as follows:

160 OE.Process-TOE requires the TOE Manufacturer to implement those measures assumed in P.Process-TOE. Therefore, the organisational security policy is covered by this objective, as far as organisational measures are concerned. The only issue not completely covered by these measures is the fact that the TOE has to support the possibility of unique identification. This is the content of

O.Identification. Therefore, the organisational security policy is covered by OE.Process-Card and O.Identification.

161 The justification related to the assumption “Protection during Packaging, Finishing and Personalisation (A.Process-Card)” is as follows:

162 Since OE.Process-Card requires the Card Manufacturer to implement those measures assumed in A.Process-Card, the assumption is covered by this objective.

163 The justification related to the threats “Inherent Information Leakage (T.Leak-Inherent)”, “Physical Probing (T.Phys-Probing)”, “Malfunction due to Environmental Stress (T.Malfunction)”, “Physical Manipulation (T.Phys-Manipulation)”, “Forced Information Leakage (T.Leak-Forced)“, “Abuse of Functionality (T.Abuse-Func)” and “Deficiency of Random Numbers (T.RND)” is as follows:

164 For all threats the corresponding objectives are stated in a way, which directly corresponds to the description of the threat. It is clear from the description of each objective , that the corresponding threat is removed if the objective is valid. More specifically, in every case the ability to use the attack method successfully is countered, if the objective holds. The justification related to the threat “Memory Access Violation (T.Mem-Access)” is as follows:

165 According to O.Mem-Access the TOE must enforce the partitioning of memory areas so that access of software to memory areas is controlled. Any restrictions are to be defined by the Smartcard Embedded Software. Thereby security violations caused by accidental or deliberate access to restricted data (which may include code) can be prevented (refer to T.Mem-Access). The threat T.Mem-Access is therefore removed if the objective is met.

166 The clarification of “Usage of Hardware Platform (OE.Plat-Appl)” makes clear that it is up to the Smartcard Embedded Software to implement the memory management scheme by appropriately administrating the TSF. This is also expressed both in T.Mem-Access and O.Mem-Access. The TOE shall provide access control functions as a means to be used by the Smartcard Embedded Software. This is further emphasised by the clarification of “Treatment of User Data (OE.Resp-Appl)” which reminds that the Smartcard Embedded Software must not undermine the restrictions it defines. Therefore, the clarifications contribute to the coverage of the threat T.Mem-Access.

167 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.

168 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.

169 Compared to Smartcard IC Platform Protection Profilea 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.

170 Compared to Smartcard IC Platform Protection Profilea 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.

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

8.2 Security Requirements Rationale

8.2.1 Rationale for the security functional requirements

Objective	TOE Security Functional Requirements	Security Requirements for the environment
O.Leak-Inherent	• FDP_ITT.1 "Basic internal transfer protection" • FPT_ITT.1 "Basic internal TSF data transfer protection" • FDP_IFC.1"Subset information flow control"	RE.Phase-1 "Design and Implementation of the Smartcard Embedded Software"
O.Phys-Probing	• FPT_PHP.3 "Resistance physical attack"	RE.Phase-1 "Design and Implementation of the Smartcard Embedded Software"
O.Malfunction	• FRU_FLT.2 "Limited fault tolerance • FPT_FLS.1 "Failure with preservation of secure state" • FPT_SEP.1 "TSF domain separation"	
O.Phys-Manipulation	• FPT_PHP.3 "Resistance to physical attack"	RE.Phase-1 "Design and Implementation of the Smartcard Embedded Software" (e. g. by implementing FDP_SDI.1 Stored data integrity monitoring)
O.Leak-Forced	All requirements listed for O.Leak-Inherent • FDP_ITT.1, FPT_ITT.1, FDP_IFC.1 plus those listed for O.Malfunction and O.Phys-Manipulation • FRU_FLT.2, FPT_FLS.1, FPT_SEP.1,FPT_PHP.3	RE.Phase-1 "Design and Implementation of the Smartcard Embedded Software"

Objective	TOE Security Functional Requirements	Security Requirements for the environment
O.Abuse-Func	• FMT_LIM.1 "Limited capabilities" • FMT_LIM.2 "Limited availability" plus those for O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation, O.Leak-Forced • FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_PHP.3, FRU_FLT.2, FPT_FLS.1, FPT_SEP.1	
O.Identification	- FAU_SAS.1 "Audit storage"	
O.RND	• FCS_RND.1 "Quality metric for random numbers" plus those for O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-manipulation, O.Leak-Forced • FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_PHP.3, FRU_FLT.2, FPT_FLS.1,FPT_SEP.1	RE.Phase-1 "Design and Implementation of the Smartcard Embedded Software" (e. g. by implementing FPT_AMT.1 "Abstract machine testing")
OE.Process-TOE	• FAU_SAS.1 "Audit storage"	Assurance Components: Delivery (ADO_DEL); Installation, generation, and startup (ADO_IGS) (using Administrator Guidance (AGD_ADM), User guidance (AGD_USR)); CM automation (ACM_AUT); CM Capabilities (ACM_CAP); CM Scope (ACM_SCP); Development Security (ALC_DVS); Life Cycle Definition (ALC_LCD); Tools and Techniques (ALC_TAT)
OE.Process-Card		RE.Process-Card possibly supported by RE.Phase-1

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

Table 7. Security Objectives versus Assumptions, Threats or Policies

172 The justification related to the security objective “Protection against Inherent Information Leakage (O.Leak-Inherent)” is as follows:

173 The refinements of the security functional requirements FPT_ITT.1 and FDP_ITT.1 together with the policy statement in FDP_IFC.1 explicitly require the prevention of disclosure of secret data (TSF data as well as User Data) when transmitted betweenseparate parts of the TOE or while being processed. This includes that attackers cannot reveal such data by measurements of emanations, power consumption or other behaviour of the TOE while data are transmitted between or processed by TOE parts.

174 Of course this has also to be supported by the Smartcard Embedded Software. For example timing attacks were possible if the processing time of algorithms implemented in the software would depend on the content of secret variables. The requirement RE.Phase-1 makes sure that this is avoided.

175 The justification related to the security objective “Protection against Physical Probing (O.Phys-Probing)” is as follows:

176 The scenario of physical probing as described for this objective is explicitly included in the assignment chosen for the physical tampering scenarios in FPT_PHP.3. Therefore, it is clear that this security functional requirement supports the objective.

177 It is possible that the TOE needs additional support by the Smartcard Embedded Software (e. g. to send data over certain buses only with appropriate precautions). If necessary this support is provided according to RE.Phase-1. Together with this FPT_PHP.3 is suitable to meet the objective.

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

179 The definition of this objective shows that it covers a situation, where malfunction of the TOE might be caused by the operating conditions of the TOE (while direct manipulation of the TOE is covered O.Phys-Manipulation). There are two possibilities in this situation: Either the operating conditions are inside of the tolerated range or at least one of them is outside of this range. The second case is covered by FPT_FLS.1, because it states that a secure state is preserved in this case. The first case is covered by FRU_FLT.2 because it states that the TOE operates correctly under normal (tolerated) conditions. To support this, FPT_SEP.1 the functions implementing FRU_FLT.2 and FPT_FLS.1 must work independently so that their operation can not affected by the Smartcard Embedded Software (refer to the refinement). Therefore, there is no possible instance of conditions under O.Malfunction, which is not covered.

180 The justification related to the security objective “Protection against Physical Manipulation (O.Phys-Manipulation)” is as follows:

181 The scenario of physical manipulation as described for this objective is explicitly included in the assignment chosen for the physical tampering scenarios in FPT_PHP.3. Therefore, it is clear that this security functional requirement supports the objective.

182 It is possible that the TOE needs additional support by the Embedded Software (for instance by implementing FDP_SDI.1 to check data integrity with the help of appropriate checksums, refer to Section 8.2.2). This support is provided according to RE.Phase-1. Together with this FPT_PHP.3 is suitable to meet the objective.

183 The justification related to the security objective “Protection against Forced Information Leakage (O.Leak-Forced)“ is as follows:

184 This objective is directed against attacks, where an attacker wants to force an information leakage, which would not occur under normal conditions. In order to achieve this the attacker has to combine a first attack step, which modifies the behaviour of the TOE (either by exposing it to extreme operating conditions or by directly manipulating it) with a second attack step measuring and analysing some output produced by the TOE. The first step is prevented by the same measures which support O.Malfunction and O.Phys-Manipulation, respectively. The requirements covering O.Leak-Inherent also support O.Leak-Forced because they prevent the attacker from being successful if he tries the second step directly.

185 The justification related to the security objective “Protection against Abuse of Functionality (O.Abuse-Func)” is as follows:

186 This objective states that abuse of functions (especially provided by the IC Dedicated Test Software, for instance in order to read secret data) must not be possible in Phase 7 of the life-cycle. There are two possibilities to achieve this: (i) They cannot be used by an attacker (i. e. its availability is limited) or (ii) using them would not be of relevant use for an attacker (i. e. its capabilities are limited) since the functions are designed in a specific way. The first possibility is specified by FMT_LIM.2 and the second one by FMT_LIM.1. Since these requirements are combined to support the policy, which is suitable to fulfil O.Abuse-Func, both security functional requirements together are suitable to meet the objective.

187 Other security functional requirements which prevent attackers from circumventing the functions implementing these two security functional requirements (for instance by manipulating the hardware) also support the objective.

188 It was chosen to define FMT_LIM.1 and FMT_LIM.2 explicitly (not using Part 2 of the Common Criteria) for the following reason: Though taking components from the Common Criteria catalogue makes it easier to recognise functions, any selection from Part 2 of the Common Criteria would have made it harder for the reader to understand the special situation meant here. As a consequence, the statement of explicit security functional requirements was chosen to provide more clarity.

189 The justification related to the security objective “TOE Identification (O.Identification)“ is as follows:

190 Obviously the operations for FAU_SAS.1 are chosen in a way that they require the TOE to provide the functionality needed for O.Identification. The Initialisation Data (or parts of them) are used for TOE identification.

191 It was chosen to define FAU_SAS.1 explicitly (not using a given security functional requirement from Part 2 of the Common Criteria) for the following reason: The security functional requirement FAU_GEN.1 in Part 2 of the CC requires the TOE to generate the audit data and gives details on the content of the audit records (for instance data and time). The possibility to use the functions in order to store securityrelevant data which are generated outside of the TOE, is not covered by the family FAU_GEN or by other families in Part 2. Moreover, the TOE cannot add time information to the records, because it has no real time clock. Therefore, the new family FAU_SAS was defined for this situation.

192 The justification related to the security objective “Random Numbers (O.RND)” is as follows:

193 FCS_RND.1 requires the TOE to provide random numbers of good quality.

194 Other security functional requirements, which prevent physical manipulation and malfunction of the TOE (see the corresponding objectives listed in the table) support this objective because they prevent attackers from manipulating or otherwise affecting the random number generator.

195 Random numbers are often used by the Smartcard Embedded Software to generate cryptographic keys for internal use. Therefore, the TOE must prevent the unauthorised disclosure of random numbers. Other security functional requirements which prevent inherent leakage attacks, probing and forced leakage attacks ensure the confidentiality of the random numbers provided by the TOE.

196 Depending on the functionality of specific TOEs the Smartcard Embedded Software will have to support the objective by providing runtime-tests of the random number generator .Together, these requirements allow the TOE to provide cryptographically good random numbers and to ensure that no information about the produced random numbers is available to an attacker.

197 It was chosen to define FCS_RND.1 explicitly, because Part 2 of the Common Criteria does not contain generic security functional requirements for Random Number generation. (Note that there are security functional requirements in Part 2 of the Common Criteria, which refer to random numbers. However, they define requirements only for the authentication context, which is only one of the possible applications of random numbers.)

198 The justification related to the security objective “Usage of Hardware Platform (OE.Plat-Appl)” is as follows:

199 RE.Phase-1 requires the Smartcard Embedded Software developer to design and implement the software in a way, which is suitable to meet OE.Plat-Appl.

200 The justification related to the security objective “Treatment of User Data (OE.Resp-Appl)” is as follows:

201 RE.Phase-1 requires the developer of the Smartcard Embedded Software to design and implement the software in a way, which is suitable to meet OE.Resp-Appl.

202 The justification related to the security objective “Protection during TOE Development and Production (OE.Process-TOE)” is as follows:

203 The objective OE.Process-TOE has mainly to be fulfilled by organisational and other measures, which the TOE Manufacturer has to implement. These measures are a subset of those measures, which are examined during the evaluation of the assurance requirements of the classes ACM, AGD, ALC and ADO. The technical capability of the TOE to store Initialisation Data and/or Pre-personalisation Data is provided according to FAU_SAS.1. Together these security requirements are suitable to meet the objective.

204 The justification related to the security objective “Protection during Packaging, Finishing and Personalisation (OE.Process-Card)” is as follows:

205 RE.Process-Card requires the Card Manufacturer to use adequate measures to fulfil OE.Process-Card. Depending on the security needs of the application, the Smartcard Embedded Software may have to

support this for instance by using appropriate authentication mechanisms for personalisation functions. Therefore, RE.Phase-1 may support RE.Process-Card in fulfilling the objective in addition.

206 The justification related to the security objective "Area based Memory Access Control (O.Mem-Access)" is as follows:

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

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

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

210 The security functional requirement(s) "Cryptographic operation (FCS_COP.1)" exactly requires those functions to be implemented which are demanded by O.Add-Functions. Therefore, FCS_COP.1 is suitable to meet the security objective.

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

212 [FDP_ITC.1 Import of user data without security attributes or
FDP_ITC.2 Import of user data with security attributes or
FCS_CKM.1 Cryptographic key generation],
FCS_CKM.4 Cryptographic key destruction,
FMT_MSA.2 Secure security attributes.
to be met by the environment.

213 All these requirements have to be fulfilled to support OE.Resp-Appl for the 3DES algorithms.

214 The security functional requirements required to meet the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced define how to implement the specific security functionality. However, key-dependent functions could be implemented in the Smartcard Embedded Software. In this case RE.Cipher requires that these functions ensure that confidential data (User Data) can not be disclosed while they are just being processed by the Smartcard Embedded Software. Therefore, with respect to the Smartcard Embedded Software the issues addressed by the objectives just mentioned are addressed by the requirement RE.Cipher.

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

216 All these requirements have to be fulfilled to support OE.Resp-Appl for the 3DES algorithms.

217 In this ST the objectives for the environment OE.Plat-Appl and OE.Resp-Appl have been clarified. The requirement for the environment Re.Cipher has been introduced to cover the objectives OE.Plat-Appl and OE.Resp-Appl (in addition to O.Add-Functions). The Smartcard Embedded Software defines the use of the cryptographic functions FCS_COP.1 provided by the TOE. RE.Phase-1, which is assigned to OE. Resp-Appl in the Smartcard IC Platform Protection Profile, requires the Smartcard Embedded Software Developer to design and implement the software that it protects security relevant User Data

(especially cryptographic keys). The requirements for the environment FDP_ITC.1, FDP_ITC.2, FCS_CKM.1, FCS_CKM.4, and FMT_MSA.2 support an appropriate key management. These security requirements are suitable to meet OE.Resp-Appl.

218 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.

8.2.2 Dependencies of security functional requirements

Security Functional Requirement	Dependencies	Fulfilled by security requirements
FRU_FLT.2	FPT_FLS.1	Yes
FPT_FLS.1	ADV_SPM.1	Yes (Part of EAL4)
FPT_SEP.1	None	No dependency
FMT_LIM.1	FMT_LIM.2	Yes
FMT_LIM.2	FMT_LIM.1	Yes
FAU_SAS.1	None	No dependency
FPT_PHP.3	None	No dependency
FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1	Yes
FDP_IFC.1	FDP_IFF.1	See discussion below
FPT_ITT.1	None	No dependency
FCS_RND.1	None	No dependency
FCS_COP.1 (3DES)	FCS_CKM.1	Yes (by the environment)
	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) FCS_CKM.4 FMT_MSA.2	Yes (by the environment)
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 See discussion below
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes See discussion below Yes
FMT_SMF.1	None	No dependency

Table 8. Dependencies of the Security Functional Requirements

219 Part 2 of the Common Criteria defines the dependency of FDP_IFC.1 (information flow control policy statement) on FDP_IFF.1 (Simple security attributes). The specification of FDP_IFF.1 would not capture the nature of the security functional requirement nor add any detail. As stated in the *Data Processing Policy* referred to in FDP_IFC.1 there are no attributes necessary. The security functional requirement for the TOE is sufficiently described using FDP_ITT.1 and its *Data Processing Policy* (FDP_IFC.1). Therefore the dependency is considered satisfied.

220 As Table 8 shows, all other dependencies are fulfilled by security requirements defined in this Protection Profile. The dependencies FCS_CKM.1, FCS_CKM.4 (optional) and FMT_MSA.2 (optional) must be covered from the environment (the smartcard embedded software).

221 Concerning the requirement FPT_FLS.1 (Failure with preservation of secure state) the TSF shall preserve a secure state when the following types of failures occur: exposure to operating conditions which may not be tolerated according to the requirement FRU_FLT.2 (Limited fault tolerance) and where therefore a malfunction could occur. Here the term "failure" above also covers "circumstances". The TOE prevents failures for the "circumstances" defined above. In this context the detection thresholds of detectors are inside the operating range of the TOE. Therefore abnormal events/failures are detected before the secure state is compromised. This allows to take user defined appropriate actions by software or to immediately RESET the TOE (also cf. FPT_FLS.1 related information in the TSP model).

222 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.

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

223 The assurance level EAL4 and the augmentation with the requirements ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, and AVA_VLA.4 were chosen in order to meet assurance expectations explained in the following paragraphs.

224 An assurance level of EAL4 is required for this type of TOE since it is intended to defend against highly sophisticated attacks without a protected environment. This evaluation assurance level was selected since it provides even formal evidence on the conducted vulnerability assessment. In order to provide a meaningful level of assurance that the TOE provides an adequate level of defense against such attacks, the evaluators have access to all information regarding the TOE including the low level design and source code.

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

ADV_IMP.2 Sufficiency of security measures

226 This assurance component is a higher hierarchical component to EAL 4 (which only requires ADV_IMP.1). It is important for a smartcard IC that the evaluation includes the implementation representation of the entire TSF and determines whether the functional requirements in the Security Target are addressed by the representation of the TSF. IC dedicated software source code and IC hardware drawings are examples of TSF implementation representation.

227 The implementation representation is used to express the notion of the least abstract representation of the TSF, specifically the one that is used to create the TSF itself without further design refinement.

228 ADV_IMP.2 has dependencies with ADV_LLD.1 "Descriptive Low-Level design", ADV_RCR.1 "Informal correspondence demonstration", ALC_TAT.1 "Well defined development tools". These assurance components are included in EAL4, then these dependencies are satisfied.

ALC_DVS.2 Sufficiency of security measures

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

230 In the particular case of a Smartcard Integrated Circuit 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 Smartcard Integrated Circuit, maintaining the confidentiality of the design is very important.

231 This assurance component is a higher hierarchical component to EAL4 (which only requires ALC_DVS.1). ALC_DVS.2 has no dependencies.

AVA_MSU.3 Analysis and testing for insecure states

232 The user guidance must be correct and sufficient to ensure that the TOE can be used in a secure way and that vulnerabilities are not introduced.

233 This component is included to ensure that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect. In this component, an analysis of the guidance documentation provided by the developer is validated and confirmed through testing by the evaluator to provide additional assurance.

234 This assurance component is a higher hierarchical component to EAL4 (which only requires AVA_MSU.2).

235 AVA_MSU.3 has dependencies with ADO_IGS.1 “Installation, generation, and start-up procedures“, ADV_FSP.1 “Informal functional specification”, AGD_ADM.1 “Administrator guidance” and AGD_USR.1 “User guidance”. The dependencies are satisfied in EAL4.

AVA_VLA.4 Highly resistant

236 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_VLA.4 component.

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

238 AVA_VLA.4 has dependencies with ADV_FSP.1 “Informal functional specification”, ADV_HLD.2 “Security enforcing high-level design”, ADV_LLD.1 “Descriptive low-level design”, ADV_IMP.1 “Subset of the implementation of the TSF”, AGD_ADM.1 “Administrator Guidance”, AGD_USR.1 “User Guidance”.

239 All these dependencies are satisfied by EAL4.

8.3 Security Requirements are Mutually Supportive and Internally Consistent

240 The discussion of security functional requirements and assurance components in the preceding sections has shown that mutual support and consistency are given for both groups of requirements. The arguments given for the fact that the assurance components are adequate for the functionality of the TOE also shows that the security functional requirements and assurance requirements support each other and that there are no inconsistencies between these groups.

241 The security functional requirement FPT_PHP.3 makes it harder to manipulate User Data and TSF Data. This protects the primary assets identified in Section 3.1 and other security features or functions which use these data.

242 Though a manipulation of the TOE (refer to FPT_PHP.3) is not of great value for an attacker in itself, it can be an important step in order to threaten the primary assets identified in Section 3.1. Therefore, the security functional requirement FPT_PHP.3 is not only required to meet the security objective O.Phys-Manipulation. Instead it protects other security features or functions of both the TOE and the Smartcard Embedded Software from being bypassed, deactivated or changed. In particular this may pertain to the security features or functions being specified using FDP_ITT.1, FPT_ITT.1, FPT_FLS.1, FMT_LIM.2, FCS_RND.1, and those implemented in the Smartcard Embedded Software.

243 A malfunction of TSF (refer to FRU_FLT.2 and FPT_FLS.1) can be an important step in order to threaten the primary assets identified in Section 3.1. Therefore, the security functional requirements FRU_FLT.2 and FPT_FLS.1 are not only required to meet the security objective O.Malfunction. Instead they protect other security features or functions of both the TOE and the Smartcard Embedded Software from being bypassed, deactivated or changed. In particular this pertains to the security features or functions being specified using FDP_ITT.1, FPT_ITT.1, FMT_LIM.1, FMT_LIM.2, FCS_RND.1, and those implemented in the Smartcard Embedded Software.

244 In a forced leakage attack the methods described in "Malfunction due to Environmental Stress" (refer to T.Malfunction) and/or "Physical Manipulation" (refer to T.Phys-Manipulation) are used to cause leakage from signals which normally do not contain significant information about secrets. Therefore, in order to avert the disclosure of primary assets identified in Section 3.1 it is important that the security functional requirements averting leakage (FDP_ITT.1, FPT_ITT.1) and those against malfunction (FRU_FLT.2 and FPT_FLS.1) and physical manipulation (FPT_PHP.3) are effective and bind well. The security features and functions against malfunction ensure correct operation of other security functions (refer to above) and help to avert forced leakage themselves in other attack scenarios. The security features and functions against physical manipulation make it harder to manipulate the other security functions (refer to above).

245 Physical probing (refer to FPT_PHP.3) shall directly avert the disclosure of primary assets identified in Section 3.1. In addition, physical probing can be an important step in other attack scenarios if the corresponding security features or functions use secret data. For instance the security functional requirement FMT_LIM.2 may use passwords. Therefore, the security functional requirement FPT_PHP.3 (against probing) help to protect other security features or functions including those being implemented in the Smartcard Embedded Software. Details depend on the implementation.

246 Leakage (refer to FDP_ITT.1, FPT_ITT.1) shall directly avert the disclosure of primary assets identified in Section 3.1. In addition, inherent leakage and forced leakage (refer to above) can be an important step in other attack scenarios if the corresponding security features or functions use secret data. For instance the security functional requirement FMT_LIM.2 may use passwords. Therefore, the security functional requirements FDP_ITT.1 and FPT_ITT.1 help to protect other security features or functions implemented in the Smartcard Embedded Software (FDP_ITT.1) or provided by the TOE (FPT_ITT.1). Details depend on the implementation.

247 According to the assumption Usage of Hardware Platform (A.Plat-Appl) the Smartcard Embedded Software will correctly use the functions provided by the TOE. Hereby the User Data are treated as required to meet the requirements defined for the specific application context (refer to Treatment of User Data (A.Resp-Appl)). However, the TOE may implement additional functions. This can be a risk if their interface can not completely be controlled by the Smartcard Embedded Software. Therefore, the security functional requirements FMT_LIM.1 and FMT_LIM.2 are very important. They ensure that appropriate control is applied to the interface of these functions (limited availability) and that these functions, if being usable, provide limited capabilities only.

248 The combination of the security functional requirements FMT_LIM.1 and FMT_LIM.2 ensures that (especially after TOE Delivery) these additional functions can not be abused by an attacker to (i) disclose or manipulate User Data, (ii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or of the Smartcard Embedded Software or (iii) to enable an attack. Hereby the binding between these two security functional requirements is very important:

249 The security functional requirement Limited Capabilities (FMT_LIM.1) must close gaps which could be left by the control being applied to the function's interface (Limited Availability (FMT_LIM.2)). Note that the security feature or function which limits the availability can be bypassed, deactivated or changed by physical manipulation or a malfunction caused by an attacker. Therefore, if Limited Availability (FMT_LIM.2) is vulnerable, it is important to limit the capabilities of the functions in order to limit the possible benefit for an attacker.

250 The security functional requirement Limited Availability (FMT_LIM.2) must close gaps which could result from the fact that the function's kernel in principle would allow to perform attacks. The TOE must limit the availability of functions which potentially provide the capability to disclose or manipulate User Data, to manipulate security features or functions of the TOE or of the Smartcard Embedded Software or to enable an attack. Therefore, if an attacker could benefit from using such functions, it is important to limit their availability so that an attacker is not able to use them.

251 No perfect solution to limit the capabilities (FMT_LIM.1) is required if the limited availability (FMT_LIM.2) alone can prevent the abuse of functions. No perfect solution to limit the availability (FMT_LIM.2) is required if the limited capabilities (FMT_LIM.1) alone can prevent the abuse of functions. Therefore, it is correct that both requirements are defined in a way that they together provide sufficient security.

252 It is important to avert malfunctions of TSF and of security functions implemented in the Smartcard Embedded Software (refer to above). There are two security functional requirements which ensure that malfunctions can not be caused by exposing the TOE to environmental stress. First it must be ensured that the TOE operates correctly within some limits (Limited fault tolerance (FRU_FLT.2)). Second the TOE must prevent its operation outside these limits (Failure with preservation of secure state (FPT_FLS.1)). Both security functional requirements together prevent malfunctions. The two functional requirements must define the “limits”. Otherwise there could be some range of operating conditions which is not covered so that malfunctions may occur. Consequently, the security functional requirements Limited fault tolerance (FRU_FLT.2) and Failure with preservation of secure state (FPT_FLS.1) are defined in a way that they together provide sufficient security.

253 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.

254 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.

9 ANNEX

Glossary

Application Software (AS)

Is the part of ES in charge of the Application of the Smart Card IC.

Basic Software (BS)

Is the part of ES in charge of the generic functions of the Smart Card IC such as Operating System, general routines and Interpreters.

DAC

Discretionary Access Control

Dedicated Software (DS)

Is defined as the part of ES provided to test the component and/or to manage specific functions of the component.

Embedded Software (ES)

Is defined as the software embedded in the Smart Card Integrated Circuit. The ES may be in any part of the non-volatile memories of the Smart Card IC.

Embedded software developer

Institution (or its agent) responsible for the Smart Card embedded software development and the specification of pre-personalization requirements.

Initialization

Is the process to write specific information in the NVM during IC manufacturing and testing (phase 3) as well as to execute security protection procedures by the IC manufacturer. The information could contain protection codes or cryptographic keys.

Initialization Data

Specific information written during manufacturing or testing of the TOE

Integrated Circuit (IC)

Electronic component(s) designed to perform processing and/or memory functions.

IC designer

Institution (or its agent) responsible for the IC development.

IC manufacturer

Institution (or its agent) responsible for the IC manufacturing, testing, and pre-personalization.

IC packaging manufacturer

Institution (or its agent) responsible for the IC packaging and testing.

Personaliser

Institution (or its agent) responsible for the Smart Card personalization and final testing.

Personalization data

Specific information in the NVM during personalization phase

RBAC

Role-Based Access Control

Security Information

Secret data, initialization data or control parameters for protection system)

Smart Card

A credit sized plastic card, which has a non-volatile memory and a processing unit embedded within it.

Smart Card Issuer

Institution (or its agent) responsible for the Smart Card product delivery to the Smart Card end-user.

Smart Card product manufacturer

Institution (or its agent) responsible for the Smart Card product finishing process and testing.

Smart Card Application Software (AS)

is the part of ES dedicated to the applications

Abbreviations

CC

Common Criteria

EAL

Evaluation Assurance Level

IT

Information Technology

PP

Protection Profile

SF

Security Function

SOF

Strength of Function

ST

Security Target

TOE

Target of Evaluation

TSC

TSF Scope of Control

TSF

TOE Security Functions

TSFI

TSF Interface

TSP

TOE Security Policy

Literature

[ALGO] *Federal Gazette No 58, Notification in accordance with the Electronic Signatures Act and the Electronic Signatures Ordinance (overview of suitable algorithms), Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway, 2006-01-02*

[ETSI] *Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms,* ETSI TS 102 176-1 V1.2.1 (2005-07)