Security Target
BSI-DSZ-CC-0166

Version 1.2

July 10th, 2001

Evaluation of the Philips P8WE6017V11 Secure 8-bit Smart Card Controller

Developed and provided by

Philips Semiconductors, Business Line Identification

According to the
Common Criteria for Information Technology
Evaluation (CC) at Level EAL5 augmented

by

Philips Semiconductors Hamburg
Unternehmensbereich der Philips GmbH
Stresemannallee 101
22505 Hamburg

Document Information

Document History

Version	Date	Changes	Remarks
Version 1.2	10.07.2001	Public version	

Latest version is: Version 1.2 (July 10th, 2001)

Document Invariants

Name	Value (to be edited)	Test Output (to copy)
File name and length	Automatically	st-phil6017-1_2.doc (1625600 Byte)
Latest version	Version 1.2	Version 1.2
Date of this version	July 10th, 2001	July 10th, 2001
Classification	Confidential	Confidential
TOE name (long)	Philips P8WE6017V1I Secure 8-bit Smart Card Controller	Philips P8WE6017V1I Secure 8-bit Smart Card Controller
TOE name (short)	P8WE6017V1I	P8WE6017V1I
Developer (long)	Philips Semiconductors, Business Line Identification	Philips Semiconductors, Business Line Identification
Developer (short)	Philips	Philips
Sponsor (long)	Philips Semiconductors, Business Line Identification	Philips Semiconductors, Business Line Identification
Sponsor (short)	Philips	Philips
Certification ID	BSI-DSZ-CC-0166	BSI-DSZ-CC-0166
Evaluation facility	Prüfstelle debis IT security services	Prüfstelle debis IT security services
list of authors	Hans-Gerd Albertsen	Hans-Gerd Albertsen
certific. body (short)	BSI	BSI
certific. body (long)	Bundesamt für Sicherheit in der Informationstechnik	Bundesamt für Sicherheit in der Informationstechnik

Table of Contents

1 ST Introduction 6
1.1 ST Identification 6
1.2 ST Overview 6
1.3 CC Conformance 7
2 TOE Description 9
2.1 TOE Definition 9
2.1.1 Hardware Description 11
2.1.2 Software Description 12
2.1.3 Documentation 12
2.1.4 Interface of the TOE 12
2.2 Smartcard Product Life Cycle 13
2.3 TOE Environment 14
2.3.1 TOE Development Environment 14
2.3.2 TOE Production Environment 14
2.3.3 TOE User Environment 15
2.4 TOE Logical Phases 15
2.5 TOE Intended Usage 15
2.6 General IT features of the TOE 16
2.7 Further Definitions and Explanations 17
3 TOE Security Environment 19
3.1 Description of Assets 19
3.2 Assumptions 21
3.3 Threats 22
3.4 Organisational Security Policies 27
4 Security Objectives 29
4.1 Security Objectives for the TOE 29
4.2 Security Objectives for Environment 32

5 IT Security Requirements 35
5.1 TOE Security Requirements 35
5.1.1 TOE Functional Requirements 35
5.1.2 TOE Assurance Requirements 45
5.1.3 Refinements of the TOE Assurance Requirements 46
5.2 Security Requirements for the Environment 59
5.2.1 Security Requirements for the IT-Environment 59
5.2.2 Security Requirements for the Non-IT-Environment 59
6 TOE Summary Specification 61
6.1 TOE Security Functions 61
6.2 Assurance measures 64
7 PP Claims 66
8 Rationale 66
8.1 Security Objectives Rationale 66
8.2 Security Requirements Rationale 68
8.2.1 Rationale for the security functional requirements 68
8.2.2 Dependencies of security functional requirements 74
8.2.3 Rationale for the Assurance Requirements and the Strength of Function Level 76
8.2.4 Security Requirements are Mutually Supportive and Internally Consistent 76
8.3 TOE Summary Specification Rationale 76
8.4 PP Claims Rationale 76
9 Annexes 78
9.1 Development and Production Process (life-cycle) 78
9.1.1 Life-Cycle Description 78
9.1.2 Scope of the Common Criteria Assurance Requirements 81
9.1.3 Description of Assets of the Integrated Circuits Designer/Manufacturer 82

9.2 Security Aspects of the Smartcard Embedded Software 83

9.2.1 Further Information regarding A.Resp-Appl 83

9.2.2 Examples of Specific Functional Requirements for the Smartcard Embedded Software 84

9.3 Examples of Attack Scenarios 85

9.4 Definition of the Family FCS_RND 88

9.5 Definition of the Family FMT_LIM 88

9.6 Definition of the Family FAU_SAS 90

9.7 Glossary and Vocabulary 91

9.8 List of Abbreviations 93

9.9 Further Documents 94

1 ST Introduction

The chapter *ST Introduction* is divided into the following sections:

ST Identification

ST Overview

CC Conformance

1.1 ST Identification

This Security Target (st-phil6017-1_1.doc, Version 1.2, July 10th, 2001) refers to the "Philips P8WE6017V1I Secure 8-bit Smart Card Controller" (TOE) for a Common Criteria evaluation.

1.2 ST Overview

The TOE is the hardware of the microcontroller chip P8WE6017V1I produced by Philips and the test software located in the Test-ROM of the microcontroller. The TOE includes the documentation of the P8WE6017V1I, which consists of a Data Sheet and an additional Guidance Document. The documentation contains a description of the architecture, the secure configuration of the chip by the user and the instruction set.

The P8WE6017V1I supports the usage for a wide range of security applications within the information technology. The TOE is embedded in a micro-module or another sealed package. The micro-modules are embedded into a credit card sized plastic card.

The E2PROM makes the TOE ideal for application requiring non-volatile data storage, including smart cards and portable data banks. Security functions protect data in the on-chip ROM, E2PROM and RAM. In particular when being used in the banking and finance market or in electronic commerce applications the smart card must provide security. Hence the TOE shall

- maintain the integrity and the confidentiality of data stored in non-volatile memory using the TOE and
- maintain the integrity, operation and to some extend the confidentiality of security functions (security mechanisms and associated functions) provided by the TOE.

This is ensured by the construction of the TOE and by security functions provided by the TOE. Usually the smart card is assigned to a single individual only but may store and process secrets of the system too. So, the TOE must meet security requirements to be applied to security modules.

The "Philips P8WE6017V1I Secure 8-bit Smart Card Controller" (TOE) mainly provides a hardware platform for a smart card with

- functions to calculate the Data Encryption Algorithm (DEA) resistant to Differential Power Analysis (DPA) attacks, Differential Fault Analysis (DFA) attacks, Simple Power Analysis (SPA) and Timing attacks,

- a random number generator and
- mode control regarding a test mode and a user mode.

In addition several security features independently implemented in hardware or controlled by software will be provided to ensure proper operations as well as integrity and confidentiality of stored data. This includes for example measures for memory protection and sensors to allow operations only under specified conditions.

Regarding the life cycle of the smartcard the development and the production phase of the IC with its dedicated software as described for the Target of Evaluation (TOE) is part of the evaluation. This is based on

- the description of the security environment of the TOE including the assets to be protected and the threats to be countered by the TOE and by the operational environment during the development, production and user phases,
- the description of the security objectives for the TOE and for its environment in terms of integrity and confidentiality of application data and programs, protection of the TOE and associated documentation during the development and production phases and
- the specification of the security requirements which includes the TOE security functional requirements and the TOE security assurance requirements.

1.3 CC Conformance

The Evaluation is based upon:

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 2.1; August 1999 and ISO 15408-1:1999

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 2.1; August 1999 and ISO 15408-2:1999

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 2.1; August 1999 and ISO 15408-3:1999

For the evaluation the following methodology will be used

[4] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part 2: Evaluation Methodology; Version 1.0; August 1999

The chosen level of assurance is

EAL 5 augmented. The minimum strength level for the TOE security functions is SOF-high (Strength of Functions High).

This security Target claims the following CC conformances:

Part 2 extended, Part 3 augmented.

The Security Target doesn't claim formal conformance to a Protection Profile.

However, this Security Target is written using a draft version of a Protection Profile "Smartcard IC Platform Protection Profile" under development by the following Integrated Circuits manufacturers:

- Atmel,
- Hitachi Europe,
- Infineon Technologies, and
- Philips Semiconductors.

The level of evaluation and the functionality of the TOE are chosen in order to allow the confirmation that the TOE is suitable for use within devices compliant with the German Digital Signature Law.

2 TOE Description

The chapter *TOE Description* is divided into the following sections:

TOE Definition

Smartcard Product Life Cycle

TOE Environment

TOE Logical Phases

TOE Intended Usage

General IT features of the TOE

Further Definitions and Explanations

2.1 TOE Definition

The Target of Evaluation (TOE) is a *smartcard integrated circuit* which is composed of a processing unit, security components, I/O ports and volatile and non-volatile memories (*hardware*). The TOE also includes IC Designer/Manufacturer proprietary IC Dedicated Software. This software (also known as IC firmware) is used for testing purposes during production only and does not provide additional services. All other software is called Smartcard Embedded Software and is not part of the TOE.

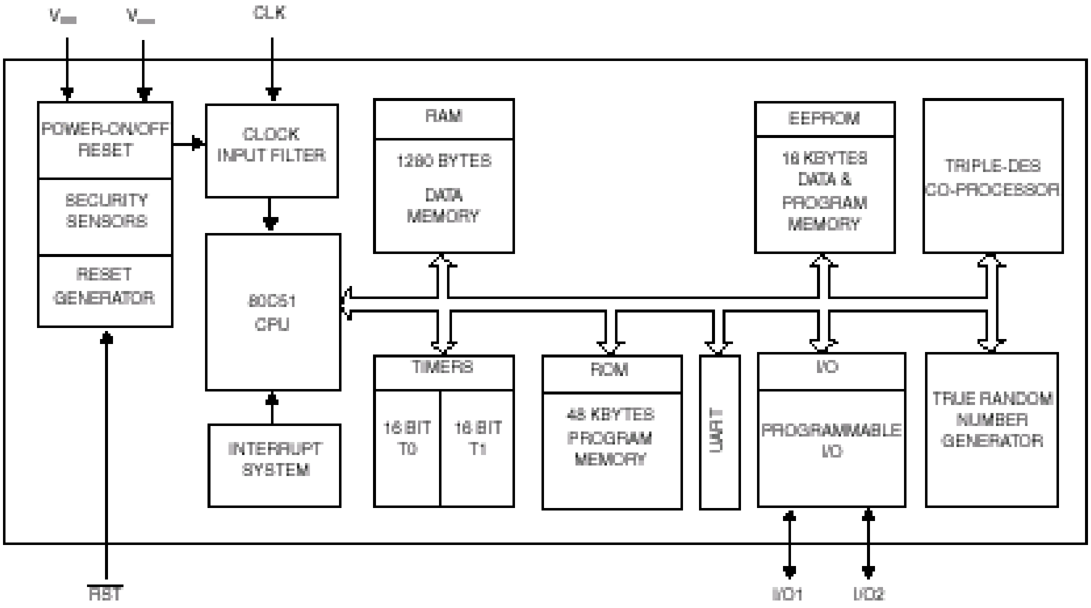


Fig 1: Overview diagram P8WE6017V1I

The TOE named P8WE6017V1I is a single chip secured 8-Bit microcontroller with firmware, manufactured in an advanced CMOS process by Philips. The device is developed for most high-end safeguarded applications, and is designed for embedding into chip cards according to ISO 7816. Each security measure is designed to act as an integral part of the complete system in order to strengthen the design as a whole. The security measures can be divided into hardware controlled security measures that do not allow for software guided exceptions and security measures that shall be controlled by software. In addition the die is embedded into a module which in turn is embedded into a smart card. Note that Philips delivers wafers. Module production and module embedding (card production) takes place at the Card Manufacturer.
The module and card embedding of the TOE provide external security mechanisms because they make it harder for an attacker to access parts of the TOE for physical manipulation.

The following table lists the TOE components.

Type	Name	Release	Date	form of delivery
Hardware	Philips P8WE6017V1I Secure 8-bit Smart Card Controller	V1I	13.07.2000	chip
Software	Test ROM Software *(the IC dedicated software)*	xk033a	19.07.2000	test-ROM on the chip
Document	Guidance, Delivery and Operation Manual	1.0	02.04.2001	printed document
Document	Data Sheet	3.1	26.01.2001	printed document

Table 1: Components of the TOE

The CPU of the P8WE6017V1I is a derivation of the 80C51 family and has the same instruction set. Figure 1 shown above gives an overview to the components of the microcontroller.

The device includes ROM, RAM and EEPROM memory. The EEPROM can be accessed as data memory as well as program memory. The Triple-DES co-processor supplies single DES and Triple-DES operations. Only Triple-DES will be used in this evaluation. The random generator provides true random numbers without pseudo random calculation.

The on-chip hardware is software controlled via Special Function Registers. These registers are correlated to the activities of the CPU, Interrupt, I/O, EEPROM, Timers, and UART. The communication with the P8WE6017V1I can be performed through a serial interface I/O according to ISO standard 7816-3. Two 16-bit timers and five vectorized interrupts provide further functionality for I/O, timers and EEPROM.

The P8WE6017V1I operates with a single 3V or 5V nominal power supply at a nominal maximum external clock frequency of 8 MHz. The controller provides an internal clock to perform security algorithms. The instruction set contains 255 different instructions, there the instruction has a length of one byte which can be followed by parameters of one or two additional bytes. The controller provides two power saving modes with reduced activity: the IDLE Mode and the SLEEP Mode, which includes the CLOCK STOP Mode.

The P8WE6017V1I chip will be implemented in a credit card sized plastic card (micro-module embedded into the plastic card) or another sealed package. The chip provides a hardware computing platform to run smart card applications executed by a smart card operating system. Smart card applications will be used to store secret data and calculate cryptographic functions. The secret data shall be used as input for the calculation of authentication data, the calculation of signatures and the encryption of data and keys.

The smart card operating system stored in the Customer-ROM and the application stored in the Customer-ROM and/or in the EEPROM are not a part of the TOE. The code in the Test-ROM of the TOE is used by the manufacturer of the smart card to check the chip function. This test code is disabled before the operational use of the smart card.

The smart card applications use the security functions of the operating system based on the security features of the TOE. Mostly independent of the smart card operation system, the TOE provides a symmetric block cipher algorithm and a random number generator to perform cryptographic operations in a secure way. The block cipher algorithm may be used as a cryptographic primitive for encryption/decryption of user data and for authentication of user data and entities. The random number generator may be used by the software of the TOE environment for the generation of cryptographic parameters on the smart card and especially of keys. These strong keys should be used when the cryptographic primitives of the TOE are invoked by the software of the environment.

The TOE protects the secret data stored in and operated by the TOE against physical tampering. Within the composition of this TOE, the operating system, and the smart card application the security functionality is only partly provided by the TOE and causes dependencies between the TOE security functions and the functions provided by the operating system or the smart card application on top.

2.1.1 Hardware Description

The microcontroller chip includes the following components as depicted in Figure 2 above:

CPU 80C51 with:

memory consisting of:

256 + 1024 Bytes RAM,

48 KBytes ROM,

16 KBytes EEPROM,

Triple-DES Co-processor,

Interrupt module,

Random generator,

Two 16-bit Timers,

Power module with security sensors and security logic,

I/O-Interface,

UART.

Philips will deliver the TOE at the end of phase 3 after the production test in form of wafers.

2.1.2 Software Description

The TOE includes IC dedicated software (called firmware in the following) developed by Philips and embedded in the Test-ROM. The smart card embedded software (called application software in the following; not being part of the TOE) is stored in the Customer-ROM area (User-ROM). The firmware includes the Test Operating System, test routines for the various blocks of the circuitry, control flags for the status of the EEPROM's security area and shutdown functions to ensure that security relevant test operations cannot be executed illegally. The application software depends on the usage of the smartcard and does normally include an Operating System and an application.

2.1.3 Documentation

The Data Sheet of the P8WE6017V1I is also part of the TOE. It contains a functional description needed to develop software, guidelines for the use of security features and the instruction set of the TOE. Additional application notes describe aspects of the program interface and the use of programming measures to improve the security. The provided documentation can be used by the application software developer to develop the smartcard embedded software.

2.1.4 Interface of the TOE

In the user mode the electrical interface of the TOE are the pads to connect the lines power supply, reset input, clock input, ground, Input1/Output1.

The software interface of the TOE depends on the operation mode of the TOE:

- In the user mode (use after delivery of the TOE at the end of phase 3) the software interface is the set of instructions, the bits in the special function registers that are related to the user mode and described in the data sheet as well as the address map of the CPU including memories.

  Note: The interface of the TOE after phase 3 is based on the embedded software developed by the application software developer.

- In the test mode (use before delivery of the TOE after production in phase 3) the interface is the set of test functions based on the test operating system in the Test-ROM and provided at the electrical interface.

The chip surface can be seen as an interface of the TOE, too. This is in the case of an attack where the attacker manipulates the chip surface.

2.2 Smartcard Product Life Cycle

According to the life cycle description in chapter 9.1.1 the TOE's life cycle is decomposed into 7 phases which can be summarised as follows:

Phase 1:	Smartcard embedded software development
Phase 2:	IC Development
Phase 3:	IC manufacturing and testing
Phase 4:	IC packing and testing
Phase 5:	Smartcard product and finishing process
Phase 6:	Smartcard personalisation
Phase 7:	Smartcard end usage

Details of the Life Cycle description are given in chapter 9.1.1.

The scope of those assurance components referring the product's life-cycle is limited to Phases 2 and 3. These phases are under the control of the TOE manufacturer. All procedures within these phases are covered by the evaluation. This includes the interfaces to the other phases where information and material is being exchanged with the partners of the developer/manufacturer of the TOE.

Philips will deliver the TOE at the end of phase 3 after the production test in form of wafers. The IC Packaging (phase 4) and the following phases are under control of the customer of Philips. Nevertheless, the chip is totally dealt in an appropriate packaging when being used in the field at phase 7.

2.3 TOE Environment

2.3.1 TOE Development Environment

The development of the TOE includes the development of the hardware and of the software in the Test-ROM. The following steps are relevant for the development:

Concept and specification of the microcontroller,

HW-Design including the design of the circuit and the layout,

Development of the firmware,

Handling of customer specific data (ROM-code) as well as

Preparation of documentation for the customer (software developer).

During the design and the layout process only people involved in the specific development project for an IC have access to sensitive data. The trustworthiness of used components is ensured with simulation and verification tools that use test pattern generated by Philips Semiconductors, Business Line Identification. Different people are responsible for the design data and for customer related data. The security measures installed within Philips Semiconductors, Business Line Identification ensure a secure computer system and provide appropriate storage equipment for the different development tasks.

The verified layout data is provided from the development to the wafer fab.

2.3.2 TOE Production Environment

The wafer fab provides the layout data of the different photomasks to the manufacturer of the photomasks. The photomasks are generated off-site. The photomasks are verified against the design data of the development before the usage. The accountability and the traceability is ensured among the wafer fab and the photomask provider.

The production of the wafers may be split into two different steps regarding the production flow. In the first step the wafers are produced with the fixed masks independent of the customer. After that step the wafers are completed with the customer specific masks and the remaining masks. Between the two steps the wafers can be stored in a wafer stock. The computer tracking ensures the control of the complete process including the storage of the semi-finished wafers.

The test process of the wafers is performed within another site of Philips. The delivery process between the involved Philips sites provide accountability and traceability of the produced wafers. Non-functional ICs are marked on the wafer but will be delivered on the wafer to the packaging process.

2.3.3 TOE User Environment

The TOE user environment is the environment of phases 4 to 7. At phases 4, 5 and 6, the TOE user environment must be a controlled environment.

In the End-user environment (phase 7) smartcards are used in a wide range of applications to assure authorised conditional access. Examples of such are Pay-TV, Banking Cards, Portable communication SIM cards, Health cards, Transportation cards.

The end-user environment therefore covers a wide spectrum of very different functions, thus making it difficult to avoid and monitor any abuse of the TOE.

Phases 4 to 7 of the smart card life cycle are not part of the TOE construction process in the sense of this Security Target. Information about those phases are just included to describe how the TOE is used after its construction. Nevertheless the security features of the smartcard IC hardware that are independent of the software are active from the end of phase 3 and cannot be disabled thought the application software in the phases 4 to 7.

2.4 TOE Logical Phases

The TOE is able to control two different logical phases. After production the chip is in the test mode that means under the control of the test software. At the end of the production test the chip will be switched into the user mode so that the chip is under the control of the application software.

2.5 TOE Intended Usage

Regarding to phase 7, the combination of the smartcard hardware and the application software is used by the end-user. The method of use of the product in this phase depends on the application. During the other phases of the product construction and the product usage there are several administrator- and user-functions.

Phase 1: The smartcard embedded software developer develops software for the smartcard, including a smartcard operating system and/or application specific software parts. By using the software interface of the TOE (in user mode) as defined in section 2.1.4 he is the user of the smartcard hardware with the hardware features.

Phase 2: The IC designer is responsible for the design of the chip that is developed within this phase. In parallel the IC designer develops the IC dedicated software for the production test of the chip that is included in the Test-ROM. Therefore the IC designer takes the role of the administrator during this phase.

Phase 3: The function of the administrator is split into two: The IC manufacturer is responsible for the IC production itself. Regarding the production test after the manufacturing process the test engineer is the administrator.

Note: The definition of the user roles regarding the TOE for the phases 4 to 7 is provided here as additional information and is not in the scope of the evaluation. However the operation manuals address some of the user roles defined for phase 1 and the following phases.

Phase 4: the IC packaging manufacturer (administrator),
the smartcard embedded software developer (user),
the system integrators such as the terminal software developer (user).

Phase 5: the smartcard product manufacturer (administrator),
the smartcard embedded software developer (user),
the system integrators such as the terminal software developer (user).

Phase 6: the personaliser (administrator),
the smartcard issuer (administrator),
the smartcard embedded software developer (user),
the system integrators such as the terminal software developer (user).

Phase 7: the smartcard issuer (administrator),
the smartcard end-user (user),
the smartcard embedded software developer (user),
the system integrators such as the terminal software developer (user).

The smartcard embedded software developer and the system integrators such as the terminal software developer are listed in Phases 4-7 because they may use samples of the TOE in these phases for their testing purposes. It is not intended that they are able to change the behaviour of the smartcard in another way than a user.

The IC manufacturer and the smartcard product manufacturer may receive ICs from different phases for analysis purpose, if problems should occur during the smartcard usage.

2.6 General IT features of the TOE

The TOE IT functionality consist of:

- tamper resistant data storage
- basic cryptographic functions (DES co-processor)
- physical random number generator
- data communication

2.7 Further Definitions and Explanations

The Smartcard Embedded Software is normally stored in non-volatile non-programmable memories (ROM). But some parts of it (called supplements for the Smartcard Embedded Software, refer to section 9.1) may also be stored in non-volatile programmable memories (for instance E2PROM). All data managed by the Smartcard Embedded Software is called User Data. In addition, Pre-personalisation Data (refer to section 9.1) belongs to the User Data.

Therefore, not included in the TOE, but part of the smartcard (refer to below) there is

- the Smartcard Embedded Software comprising
  - Hard-coded Smartcard Embedded Software (normally stored in ROM)
  - Soft-coded Smartcard Embedded Software (normally stored in E^{2}PROM) and
  - User Data (especially personalisation data and other data generated and used by the Smartcard Embedded Software)

  The Smartcard Embedded Software is not designed and the User Data are not generated by the TOE Manufacturer.

The “Smartcard” comprises

- the TOE,
- the Smartcard Embedded Software,
- User Data (including Pre-personalisation Data), and
- its package (the smartcard carrier).

  Note that it is assumed here that the chip is packed. However, the way it is packaged is not specified here.

Further terms are explained in the Glossary and Vocabulary (refer to section 9.7).

The following explanations help to understand the focus of the threats and objectives defined below. For example, certain attacks are only one step towards a disclosure of assets, others may directly lead to a compromise of the application security.

- Manipulation of data (which may comprise any data, including code, stored in or processed by the smartcard integrated circuit) means that an attacker is able to alter a meaningful block of data. This should be considered for the threats T.Malfunction, T.Phys-Manipulation and T.Abuse-Func.
- Manipulation of the TOE means that an attacker is able to deliberately deactivate or otherwise change the behaviour of a specific function in a manner which enables exploitation. This should be considered for the threat T.Malfunction, T.Phys-Manipulation and T.Abuse-Func.

- Disclosure of data (which may comprise any data, including code, stored in or processed by the smartcard integrated circuit) means that an attacker is realistically[1] able to determine a meaningful block of data. This should be considered for the threats T.Leak-Inherent, T.Phys-Probing, T.Leak-Forced and T.Abuse-Func.

[1] taking into account the assumed attack potential (and for instance the probability of errors)

3 TOE Security Environment

This chapter *TOE* Security *Environment* contains the following sections:

Description of Assets

Assumptions

Threats

Organisational Security Policies

3.1 Description of Assets

Assets regarding the Threats

The primary assets (related to standard functionality) to be protected are

- the User Data.

Especially the User Data can be subject to manipulation and disclosure while being stored or processed by the TOE. However, also

- the Smartcard Embedded Software

needs to be protected to prevent manipulation and disclosure.

It is also essential that the TOE (including its Random Number Generator) guarantees

- its correct operation.

In particular this means that the Smartcard Embedded Software is correctly being executed which includes the correct operation of the TOE's functions.

Additional assets (secondary ones) are critical information about the TOE which include

- logical design data, physical design data, IC Dedicated Software, and TSF Data.

In addition,

- Initialisation Data and Pre-personalisation Data, specific development aids, test and characterisation related data, material for software development support, and photomasks

will also contain information about the TOE. Such information and the ability to perform manipulations assist in threatening the above primary assets.

Note that there are many ways to manipulate or disclose the User Data. (i) An attacker may manipulate the Smartcard Embedded Software or the TOE. (ii) An attacker may cause malfunctions of the TOE or abuse Test Features provided by the TOE. Such attacks usually require design information of the TOE to be obtained. Therefore, the design information is a secondary asset. They pertain to all information about (i) the circuitry of the IC (hardware including the physical memories), (ii) the IC Dedicated Software with the part IC Dedicated Test Software and (iii) the TSF data.

Other primary assets (related to specific functionality) are

- the random numbers generated by the TOE [2],
- the keys used for encryption and decryption of the User data.

Assets regarding the Organisational Security Policy P.Process-TOE

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

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

as long as they are generated, stored, or processed by the TOE Manufacturer. Explanations can be found in section 9.1.3.

Assets regarding the Assumption A.Process-Card

The information and material produced and/or processed by the Smartcard Embedded Software Developer in Phase 1 and by the Card Manufacturer can be grouped as follows:

- the Smart Card Embedded Software including specifications, implementation and related documentation,
- pre-personalisation and personalisation data including specifications of formats and memory areas, test related data,

[2] Note that random numbers are to be protected in terms of confidentiality for instance against the threat of leakage because they might be used to generate cryptographic keys.

- the User Data and related documentation, and
- material for software development support

as long as they are not under the control of the TOE Manufacturer.

3.2 Assumptions

The intended usage of the TOE is twofold, depending on the Life Cycle Phase: (i) The Smartcard Embedded Software developer uses it as a platform for the smartcard software being developed. The Card Manufacturer (and the end-user) uses it as a part of the Smartcard. The Smartcard is used in a terminal which supplies the card (with power and clock) and (at least) mediates the communication with the Smartcard Embedded Software.

Before being delivered to the end-user the TOE is packaged. Many attacks require the TOE to be removed from the carrier. Though this extra step adds difficulties for the attacker no specific assumptions are made here regarding the package.

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

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).

This means that the Phases after TOE Delivery (refer to sections 2.2 and 9.1) are assumed to be protected appropriately.

The developer of the Smartcard Embedded Software must ensure the appropriate “Usage of Hardware Platform (A.Plat-Appl)” while developing this software in Phase 1 as specified below.

A.Plat-Appl Usage of Hardware Platform

The Smartcard Embedded Software is designed so that the requirements from the following documents are met: (i) TOE guidance documents (refer to the Common Criteria assurance class AGD) such as the hardware data sheet, and the hardware application notes, and (ii) findings of the TOE evaluation reports relevant for the Smartcard Embedded Software.

Note that particular requirements for the Smartcard Embedded Software are often not clear before considering a specific attack scenario during vulnerability analysis of the smartcard integrated circuit (AVA_VLA). Therefore, such results from the TOE evaluation (as contained in the Evaluation Technical Report (ETR)) must be given to the developer of the Smartcard Embedded Software in an appropriate and authorised form and be taken into account during the evaluation of the software. This may also hold for additional tests being required for the combination of hardware and software. The TOE evaluation must be completed before evaluation of the Smartcard Embedded Software can be completed. The TOE evaluation can be conducted before and independent from the evaluation of the Smartcard Embedded Software.

The developer of the Smartcard Embedded Software must ensure the appropriate "Treatment of User Data (A.Resp-Appl)" while developing this software in Phase 1 as specified below.

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.

3.3 Threats

The cloning of the functional behaviour of the Smartcard on its ISO command interface is the highest level security concern in the application context.

The cloning of that functional behaviour requires to (i) develop a functional equivalent of the Smartcard Embedded Software, (ii) disclose, interpret and employ the secret User Data stored in the TOE, and (iii) develop and build a functional equivalent of the smartcard using the input from the previous steps.

The smartcard integrated circuit is a platform for the Smartcard Embedded Software which ensures that especially the critical User Data are stored and processed in a secure way (refer to below). The Smartcard Embedded Software must also ensure that critical User Data are treated as required in the application context (refer to section 3.2). In addition, the personalisation process supported by the Smartcard Embedded Software (and perhaps by the smartcard integrated circuit in addition) must be secure (refer to section 3.2). This last step is beyond the scope of this Security Target. As a result the threat "cloning of the functional behaviour of the smartcard on its ISO command interface" is averted by the combination of measures which split into those being evaluated according to this Security Target and those being subject to the evaluation of the Smartcard Embedded Software or the Smartcard and the corresponding personalisation process. Therefore, functional cloning is indirectly covered by the security concerns and threats described below.

According to this Security Target there are the following standard 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) and

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

Though the Smartcard Embedded Software (normally stored in the ROM) will in many cases not contain secret data or algorithms, it must be protected from being disclosed, since for instance knowledge of specific implementation details may assist an attacker. In many cases critical User Data will be stored in the E^2PROM.

These high-level security concerns are refined below by defining threats as required by the Common Criteria. Note that manipulation of the TOE is only a means to threaten User Data or the Smartcard Embedded Software and is not a success for the attacker in itself.

According to this Security Target there are the following high-level security concerns related to specific functionality:

SC3 deficiency of random numbers.

These high-level security concerns being related to specific functionality are refined below by defining threats as required by the Common Criteria.

The Smartcard Embedded Software must contribute to averting the threats: At least it must not undermine the security provided by the TOE. For detail refer to the assumptions regarding the Smartcard Embedded Software specified in section 3.2.

The above security concerns are derived from considering the end-usage phase (Phase 7) since

- Phase 1 and the Phases from TOE Delivery up to the end of Phase 6 are covered by assumptions and
- the development and production environment starting with Phase 2 up to TOE Delivery are covered by an organisational security policy.

The TOE's countermeasures are designed to avert the threats described below. Nevertheless, they may be effective in earlier phases (Phases 4 to 6).

The TOE is exposed to different types of influences or interactions with its outer world. Some of them may result from using the TOE only but others may also indicate an attack. The different types of influences or interactions are visualised in Figure 2.

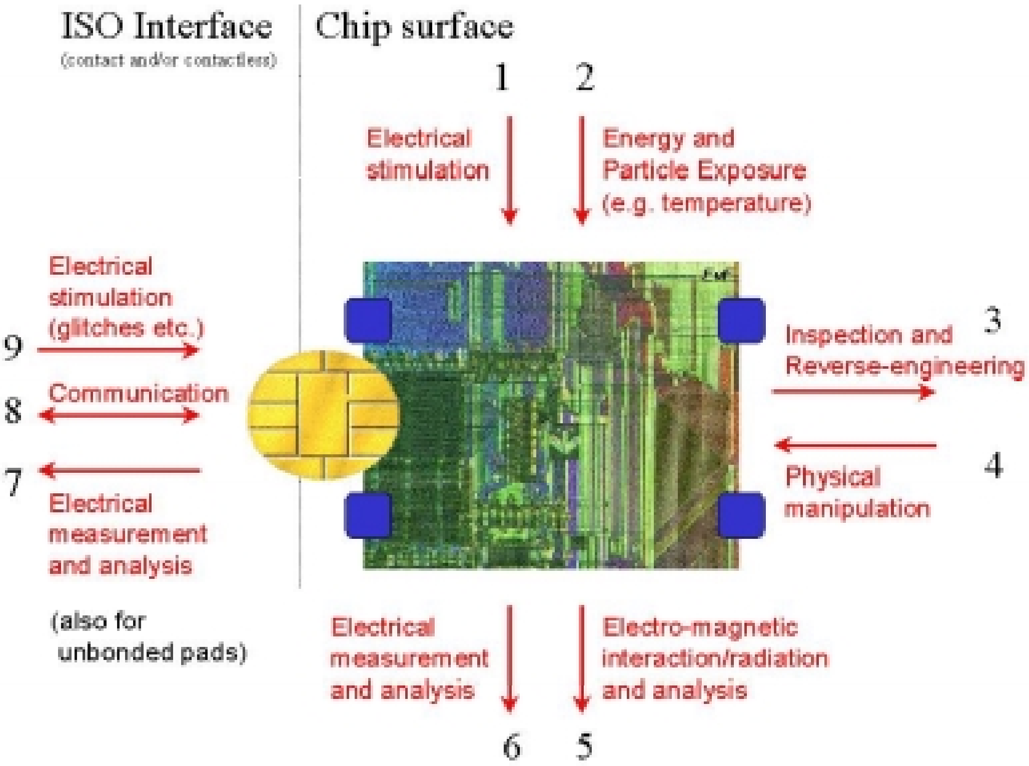

ISO Interface
(contact and/or contactless)
Chip surface
1
2
Electrical stimulation
Energy and Particle Exposure (e.g. temperature)
9
Electrical stimulation (glitches etc.)
8
Communication
7
Electrical measurement and analysis
(also for unbonded pads)
3
Inspection and Reverse-engineering
4
Physical manipulation
Electrical measurement and analysis
Electro-magnetic interaction/radiation and analysis
6
5

Figure 2: Attack Model for the TOE

An interaction with the TOE can be done through the ISO interfaces (Number 7 – 9 in Figure 2) which are realised using contacts and/or a contactless interface. Influences or interactions with the TOE also occurs through the chip surface (Number 1 – 6 in Figure 2). In Number 1 and 6 galvanic contacts are used. In Number 2 and 5 the influence (arrow directed to the chip) or the measurement (arrow starts from the chip) does not require a contact. Number 3 and 4 refer to specific situations where the TOE and its functional behaviour is not only influenced but definite changes are made by applying mechanical, chemical and other methods (such as 1, 2). Many attacks require a prior inspection and some reverse-engineering (Number 3).

Examples for specific attacks are given in section 9.3.

Standard Threats (referring to SC1 and SC2)

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). This leakage may be interpreted as a covert channel transmission but is more closely related to measurement of operating parameters, which may be derived either from direct (contact) measurements (Numbers 6 and 7 in Figure 2) or measurement of emanations (Number 5 in Figure 2) and can then be related to the specific operation being performed.

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 (Numbers 5 and 6 in Figure 2). 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 (Number 3 in Figure 2). Determination of software design including treatment of User Data may also be a pre-requisite.

This pertains to “measurements” using galvanic contacts or any type of charge interaction whereas manipulations are considered under the threat “Physical Manipulation (T.Phys-Manipulation)”. The threats “Inherent Information Leakage (T.Leak-Inherent)” and “Forced Information Leakage (T.Leak-Forced)“ may use physical probing but require complex signal processing in addition.

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 (Numbers 1, 2 and 9 in Figure 2).

To exploit this an attacker needs information about the functional operation.

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 commonly employed in IC failure analysis (Numbers 1, 2 and 4 in Figure 2) and IC reverse engineering efforts (Number 3 in Figure 2). 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 here (Number 3 in Figure 2).

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 (Numbers 5, 6, 7 and 8 in Figure 2) which normally do not contain significant information about secrets.

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 be used after TOE Delivery in order 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.

Threats related to Specific Functionality (referring to SC3)

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

T.RND Deficiency of Random Numbers

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.

Threats to be Averted by the TOE's Environment

There are no threats directed to the TOE's environment only. The target of the above threats is the Smartcard comprising the (i) TOE, (ii) the Smartcard Embedded Software and (iii) the smartcard carrier. The Smartcard Embedded Software must contribute to avert the threats: At least it must not undermine the security provided by the TOE. For detail refer to the assumptions regarding the Smartcard Embedded Software specified in section 3.2.

3.4 Organisational Security Policies

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 2.2) is secure. 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 authorised 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.

The TOE provides additional security functionality (a hardware Triple-DEA implementation), which can be used by the Smartcard Embedded Software. This security functionality is not based primarily on a threat identified in this Security Target, because it has to be decided in the context of the smartcard application, against which threats the Smartcard Embedded Software will use the DEA functionality. Therefore the necessity of this functionality is not derived from a threat identified in this Security Target, but the Security Target requires that the TOE provides this additional security functionality according to the following policy:

P.Add-Func Additional Security Functionality

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

Triple DES encryption and decryption

4 Security Objectives

This chapter Security Objectives contains the following sections:

Security Objectives for the TOE

Security Objectives for Environment

4.1 Security Objectives for the TOE

The product supports 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) as well as

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).

Though the Smartcard Embedded Software (normally stored in the ROM) will in many cases not contain secret data or algorithms, it must be protected from being disclosed, since for instance knowledge of specific implementation details may assist an attacker. In many cases critical User Data will be stored in the E2PROM.

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 means to reach these objectives.

The product supports the following high-level security goals related to specific functionality:

SG3 provide random numbers.

Standard Security Objectives (referring to SG1 and SG2)

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.

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.

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 that it is operated 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.

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.

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.

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.

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.

Security Objectives related to Specific Functionality (referring to SG3)

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 a 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.

The TOE shall provide cryptographic functionality (O.DES3)” as specified below.

O.DES3 Triple DES Functionality

The TOE will provide the cryptographic functionality of Triple DES encryption and decryption to the Smartcard Embedded Software.

Note: The TOE will ensure the confidentiality of the User Data (and especially cryptographic keys) during Triple DES operation. This is supported by O.Leak-Inherent.

4.2 Security Objectives for Environment

Phase 1

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

OE.Plat-Appl Usage of Hardware Platform

The Smartcard Embedded Software shall be designed so that the requirements from the following documents are met: (i) hardware data sheet for the TOE, (ii) TOE application notes, and (iii) findings of the TOE evaluation reports relevant for the Smartcard Embedded Software.

The 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.

Phase 2 up to TOE Delivery

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 2.2) is secure. 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.

TOE Delivery up to the end of Phase 6

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 unauthorised use).

This means that Phases after TOE Delivery up to the end of Phase 6 (refer to section 3.1) must be protected appropriately.

5 IT Security Requirements

This chapter IT Security Requirements contains the following sections:

TOE Security Requirements (5.1)
TOE Functional Requirements (5.1.1)
TOE Assurance Requirements (5.1.2)
Refinements of the TOE Assurance Requirements (5.1.3)
Security Requirements for the Environment (5.2)

Note that section 5.1.3 is not mandatory according to the Common Criteria. The Refinements of the TOE Assurance Requirements take into account the peculiarities of the smartcard development and production process (card's life-cycle).

5.1 TOE Security Requirements

5.1.1 TOE Functional Requirements

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

The Security Functional Requirements are shown in the following table. These security functional components are listed and explained below.

Security Functional Requirement	Note
FRU_FLT.2 Limited fault tolerance	
FPT_FLS.1 Failure with preservation of secure state	
FPT_SEP.1 TSF domain separation	
FPT_PHP.3 Resistance to physical attack	

Security Functional Requirement	Note
FDP_ITT.1 Basic internal transfer protection	Used in the sense of counter measures against DPA/SPA and Timing attacks, refer to the Data Processing Policy
FDP_IFC.1 Subset information flow control	Used in the sense of counter measures against DPA/SPA and Timing attacks, refer to the Data Processing Policy
FPT_ITT.1 Basic internal TSF data transfer protection	Used in the sense of counter measures against DPA/SPA and Timing attacks, refer to the Data Processing Policy
FAU_SAS.1 Audit storage	
FMT_LIM.1 Limited capabilities	Used in the sense of counter measures against the abuse of test functions
FMT_LIM.2 Limited availability	Used in the sense of counter measures against the abuse of test functions
FCS_RND.1 Quality metric for random numbers	
FCS_COP.1 Cryptographic operation	

Table 2: Security Functional Requirements

Malfunctions

There are different ranges of operating conditions such as supply voltage, external frequency and temperature. The TOE can be operated within the limits visualised as the inner dotted rounded rectangle in Figure 3 and must operate correctly there. The limits have been reduced to ensure correct operation. This is visualised by the outer dotted rounded rectangle in the figure.

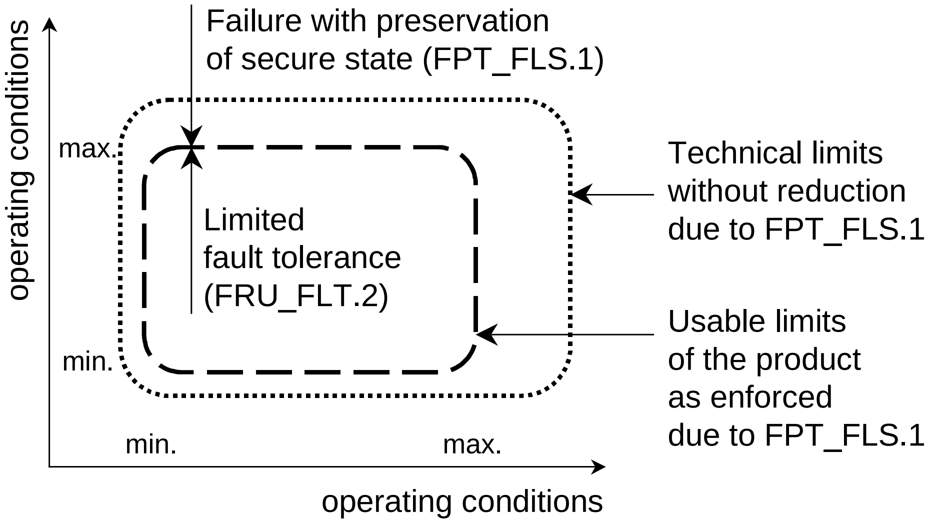

operating conditions
Failure with preservation of secure state (FPT_FLS.1)
max.
min.
Limited fault tolerance (FRU_FLT.2)
Technical limits without reduction due to FPT_FLS.1
Usable limits of the product as enforced due to FPT_FLS.1
min.
max.
operating conditions

Figure 3: Paradigm regarding Operating Conditions

Figure 3 must not be understood as being two-dimensional and defining static limits only. Reality is multi-dimensional and includes a variety of timing aspects. Note that the limit of the operating conditions visualised by the inner dashed rounded rectangle in Figure 3 is not necessarily exactly reflected by the limits identified in the TOE's data sheet. Instead this limit marks the boundary between the "tolerance reaction" of the TOE and the "active reaction" of sensors (and perhaps other circuitry).

The security functional component Limited fault tolerance (FRU_FLT.2) has been selected in order to address the robustness within some limit (as shown by the inner dashed rectangle in Figure 3) before active reaction takes place. Note that the TOE does not (in most cases) actually detect faults or failures and then correct them in order to guarantee further operation of all the TOE's capabilities. This is the way software would implement Limited fault tolerance (FRU_FLT.2). Instead the TOE will achieve exactly the same by eliminating the cause for possible faults (by means of filtering for instance) and by being resistant against influences (robustness). In the case of the TOE the "reaction to a failure" is replaced by the "reaction to operating conditions" which could cause a malfunction without the reaction of the TOE's countermeasure.

If the TOE is exposed to other operating conditions this may not be tolerated. Then the TOE must detect that and "preserve a secure state" (use of detectors and cause a reset for instance). The security functional component Failure with preservation of secure state (FPT_FLS.1) has been selected to ensure that. The way the secure state is reached depends on the implementation. Note that the TOE can monitor both external operating conditions and other internal conditions and then react appropriately. Exposure to specific "out of range" external operating conditions (environmental stress) may actually cause failure conditions internally which can be detected by FPT_FLS.1. Referring to external operating conditions the TOE is expected to respond if conditions are detected which may cause a failure. Examples for implementations of the security functional requirement Failure with preservation of secure state (FPT_FLS.1) are a voltage detector (external condition) and a circuitry which detects accesses to address areas which are not used (internal condition).

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. The security functional component TSF Domain Separation (FPT_SEP.1) has been selected to ensure that.

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)* [3].
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.

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* [4].
Dependencies:	ADV_SPM.1 Informal TOE security policy model
Refinement:	The term “failure” above also covers “circumstances”. Then the TOE prevents failures for the “circumstances” defined above.

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

FPT_SEP.1	TSF domain separation

[3] [assignment: list of type of failures]

[4] [assignment: list of types of failures in the TSF]

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.

Abuse of Functionality

During testing at the end of Phase 3 before TOE Delivery, the TOE shall be able to store some data (for instance about the production history or identification data of the individual die or other data to be used after delivery). Therefore, the security functional component Audit storage (FAU_SAS.1) has been added. The security functional component FAU_SAS.1 has been newly created (refer to section 9.6) and is used instead of FAU_GEN.1 which is too comprehensive to be applicable in this context.

The requirement FAU_SAS.1 shall be regarded as covering the injection of Initialisation Data and/or Pre-personalisation Data and of supplements of the Smartcard Embedded Software as described in section 9.1.1. After TOE Delivery the identification data (injected as part of the Initialisation Data) and the Pre-personalisation Data are available to the Smartcard Embedded Software. These data are protected by the TOE as all other User Data. It’s up to the Smartcard Embedded Software to use these data stored and provided by the TOE.

The TOE shall prevent functions (provided by the IC Dedicated Test Software or by hardware features) from being abused after TOE Delivery in order to compromise the TOE’s security. (All such functions are called “Test Features” below.) This includes but is not limited to: disclose or manipulate User Data and bypass, deactivate, change or explore security features or functions of the TOE. Details depend on the capabilities of the Test Features provided by the IC Dedicated Test Software and/or the hardware.

This can be achieved (i) by limiting the capabilities of these Test Features after Phase 3, (ii) by limiting the availability of these Test Features after Phase 3 or (iii) by a combination of both. The security functional components Limited capabilities (FMT_LIM.1) and Limited availability (FMT_LIM.2) have been newly created (refer to section 9.5) to address this.

Examples of the technical mechanism used in the TOE are user authentication (“passwords”), non-availability (for instance through removal or disabling by “fusing”) or a combination of both. A detailed technical specification would unnecessarily disclose details and is beyond the scope of a Protection Profile or Security Target.

The TOE is tested after production in Phase 3 (refer to section 9.1.1) using means provided by the IC Dedicated Software and/or specific hardware. Testing is evaluated according to the requirements of the Common Criteria assurance class ATE. The IC Dedicated Software is considered as being a test tool delivered as part of the TOE and used before TOE Delivery only. It does not provide functions in later phases of the card's life-cycle. Therefore, no security functional requirement is mandatory according to this Protection Profile regarding testing.

The implementation of the Test Features must be analysed to ascertain the existence and exploitability of vulnerabilities. This is subject to the Vulnerability Assessment (AVA). All necessary information about the Test Features (including the IC Dedicated Software) must be provided for Vulnerability Assessment (AVA). For further information of how to handle the Test Features refer to Section 5.1.3.

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.*[5]

Dependencies: FMT_LIM.2 Limited availability.

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.*[6]

[5] [assignment: Limited capability and availability policy]

[6] [assignment: Limited capability and availability policy]

Dependencies: FMT_LIM.1 Limited capabilities.

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* [7] with the capability to store *the Initialisation Data and/or Pre-personalisation Data and/or supplements of the Smartcard Embedded Software* [8] in the audit records.

Dependencies: No dependencies.

Physical Manipulation and Probing

The TOE can be subject to “tampering” which here pertains to (i) manipulation of the chip hardware and its security features with (ii) prior reverse-engineering to understanding the design and its properties and functions), (iii) determination of critical data through measuring using galvanic contacts, (iv) determination of critical data not using galvanic contacts and (v) calculated manipulation of memory contents. Refer to section 2.7 for further explanations.

The TOE is not always powered and therefore not able to detect, react or notify that it has been subject to tampering. Nevertheless, its design characteristics make reverse-engineering and manipulations etc. more difficult. This is regarded as being an “automatic response” to tampering. Therefore, the security functional component Resistance to physical attack (FPT_PHP.3) has been selected. The TOE may also provide features to actively respond to a possible tampering attack which is also covered by FPT_PHP.3.

The TOE may also leave it up to the Smartcard Embedded Software to react when a possible tampering has been detected. Comprehensive guidance (refer to Common Criteria assurance class AGD) will be given for the developer of the Smartcard Embedded Software in this case. Taking the assumption “Usage of Hardware Platform (A.Plat-Appl)” into consideration this case shall therefore also be covered by FPT_PHP.3.9

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

[7] [assignment: authorised users]

[8] [assignment: list of audit information]

[9] This must be evaluated for the final smartcard product.

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.

Leakage

When the Smartcard processes User Data and/or TSF Data, information about these data may be leaked by signals which can be measured externally (especially the ISO contacts of the Smartcard). An attacker may also cause malfunctions or perform manipulations of the TOE in order to cause the TOE to leak information. The analysis of those measurement data can lead to the disclosure of User Data and other critical data. Examples are given in Section 9.3.

The security functional requirements "Basic internal transfer protection (FDP_ITT.1)", "Basic internal TSF data transfer protection (FPT_ITT.1)" and "Subset information flow control (FDP_IFC.1)" have been selected to ensure that the TOE must resist leakage attacks (both for User Data and TSF data). These security functional requirements address inherent leakage. With respect to forced leakage they have to be considered in combination with the security functional requirements "Limited fault tolerance (FRU_FLT.2)" and "Failure with preservation of secure state (FPT_FLS.1)" on the one hand and "Resistance to physical attack (FPT_PHP.3)" on the other.

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*[12] to prevent the *disclosure*[13] of user data when it is transmitted between physically-separated parts of the TOE.

[10] [assignment: physical tampering scenarios]

[11] [assignment: list of TSF devices/elements]

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.

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*[14] 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.

The following Security Function Policy (SFP) Data Processing Policy is defined for the requirement "information flow control (FDP_ITT.1)":

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

FDP_IFC.1.1 The TSF shall enforce the *Data Processing Policy*[15] on *all confidential data when they are processed or transferred by the TOE or by the Smartcard Embedded Software*[16].

Dependencies: FDP_IFF.1 Simple security attributes

[12] [assignment: access control SFP(s) and/or information flow control SFP(s)]

[13] [selection: disclosure, modification, loss of use]

[14] [selection: disclosure, modification]

[15] [assignment: information flow control SFP]

[16] [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP]

Data Processing Policy User Data and TSF data shall not be available/ obtainable on external interfaces of the TOE except when the Smartcard Embedded Software decides to communicate the User Data via such an external interface. The protection shall be applied to confidential data only but without the distinction of attributes controlled by the Smartcard Embedded Software.

Random Numbers

The TOE generates random numbers. To define the IT security functional requirements of the TOE an additional family (FCS_RND) of the Class FCS (cryptographic support) is defined in chapter 9.4. This class FCS_RND Generation of random numbers describes the functional requirements for random number generation used for cryptographic purposes. For details on tests refer to the refinement of the assurance component of the family ATE_FUN in section 5.1.3.

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 requirement to provide 8 bit random numbers with an entropy of at least 7 bit in each byte* [17].

Dependencies: No dependencies.

Cryptographic Support

The TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below.

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform *encryption and decryption* [18] in accordance with a specified cryptographic algorithm *Triple Data Encryption Algorithm (TDEA)* [19] and cryptographic key sizes *of 112 bit* [20] that meet the following *list of standards* [21]:

[17] [assignment: a defined quality metric]

[18] [assignment: list of crypto-graphic operations]

[19] [assignment: cryptographic algorithm]

[20] [assignment: cryptographic key sizes]

[21] [assignment: list of 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 FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes.

5.1.2 TOE Assurance Requirements

The Security Target contains refinements for the evaluation of the TOE and its development and operating environment those taken from the

Evaluation Assurance Level 5 (EAL5)
and augmented by taking the following components:
ADV_LLD.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4.

The assurance requirements are:
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.2)
TSF internals (Component ADV_INT.1)
Implementation Representation (Component ADV_IMP.2)
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)

The minimum strength of security functions for the TOE is SOF-high (Strength of Functions High).

5.1.3 Refinements of the TOE Assurance Requirements

The following refinements shall support the comparability of evaluations according to this Security Target. Other standards as those issued for a specific certification scheme may not be replaced.

Refinements regarding Delivery (ADO_DEL)

Refinements regarding Development Security (ALC_DVS)

Refinement regarding CM scope (ACM_SCP)

Refinement regarding CM capabilities (ACM_CAP)

Refinements regarding Functional Specification (ADV_FSP)

Refinement regarding Test Coverage (ATE_COV)

Refinement regarding Installation, Generation and Start-up (ADO_IGS)

Refinement regarding User Guidance (AGD_ADM)

Refinement regarding Administrator Guidance (AGD_ADM)

5.1.3.1 Refinements regarding Delivery (ADO_DEL)

Introduction

The Common Criteria assurance component of the family ADO_DEL (delivery) refer to the delivery of (i) the TOE or parts of it (ii) to the user or user's site. The Common Criteria assurance component ADO_DEL.2 requires procedures and technical measures to detect modifications.

In the particular case of a Smartcard Integrated Circuit more "material and information" than the TOE itself (which by definition includes the necessary guidance) is exchanged with "users".

Therefore, considering the definition of the Common Criteria the following refinement is made regarding the items “TOE” and “to the user or user’s site”:

The following text reflects the requirements of the selected component ADO_DEL.2:

Developer action elements:

ADO_DEL.2.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.2.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.2.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user’s site.

ADO_DEL.2.2C The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer’s master copy and the version received at the user site.

ADO_DEL.2.3C The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user’s site.

Evaluator action elements:

ADO_DEL.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Refinement

For delivery “to the user” or “the user’s site”, all the external interfaces of the TOE Manufacturer have to be taken into account. These are:

- the interface with the Smartcard Embedded Software Developer (Phase 1) where information about the smartcard integrated circuit, development software and/or tools for software development, IC pre-personalisation requirements, the Smartcard Embedded Software and possible information about mask options are exchanged and
- the interface with the Phase after TOE Delivery (Phase 4 or 5) where pre-personalisation data, information about tests, and the product in form of wafers, sawn wafers (dice) or modules are exchanged.

All assets identified in sections 3.1 and additionally described in 9.1.3 (if being exchanged) have to be taken into account in order to avoid any tampering with the actual version or substitution of a false version (including unauthorised modification or replacement) as specified in the Common Criteria.

5.1.3.2 Refinements regarding Development Security (ALC_DVS)

Introduction

The Common Criteria assurance component of the family ALC_DVS refer (i) to "development environment", (ii) to the "TOE" or "TOE design and implementation". The component ALC_DVS.2 requires additional evidence for the sufficiency of the security measures.

In the particular case of a Smartcard Integrated Circuit the TOE is developed and produced within a complex industrial process which must especially be protected. Therefore, considering the definition of the Common Criteria the following refinement is made regarding the items "development environment", "TOE" or "TOE design and implementation" and the confirmation of the application of the security measures:

The following text reflects the requirements of the selected component ALC_DVS.2:

Developer action elements:

ALC_DVS.2.1D The developer shall produce development security documentation.

Content and presentation of evidence elements:

ALC_DVS.2.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.2.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

ALC_DVS.2.3C The evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

Evaluator action elements:

ALC_DVS.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.2.2E The evaluator shall confirm that the security measures are being applied.

Refinement

The "development environment" as referred to in the Common Criteria covers both, the development (Phase 2) and the production (at least Phase 3) of the TOE. The scope of the requirement of "Development Security (ALC_DVS)" pertains to the Phase 2 up to TOE Delivery. These phases are under the control of the TOE Manufacturer.

The IC Designer or IC Manufacturer is responsible to guarantee confidentiality and authenticity on the interface within Phase 3 where the necessary part of the smartcard IC database is delivered to the IC Mask Manufacturer and the IC photomasks are received by the IC manufacturer.

Mask manufacturing is covered by this Protection Profile and considered under the Common Criteria assurance component of the family ALC_DVS (development security) since the manufacturer of the TOE can not delegate any responsibility here. The certification body has to decide on a case by case decision how to handle this if the mask manufacturing is outsourced.

"TOE design and implementation" must be understood as comprising all material and information related to the development and production of the TOE. Therefore, all assets identified in section 3.1 and 9.1.3 (referred to as information and material in the following paragraphs) have to be taken into account in order to ensure confidentiality and integrity (including unauthorised disclosure, unauthorised modification or replacement and theft) as specified in the Common Criteria.

The evaluator action includes assessment of all sites being involved in the development and production of the product. Sometimes standard cells (such as standard gates, standard memories) are used for the TOE as well as in other products. The corresponding items are produced and/or processed (also) in other sites where not all requirements may be applicable for practical reasons. For those assets, the certification body has to decide on a case by case decision how to handle these assets within a specific evaluation.

Whenever material and information is given to external partners (such as the developer of the Smartcard Embedded Software) the latter must be obliged by an Non Disclosure Agreement to treat the material and information as it is required for the TOE Manufacturer.

Guidance

Additionally, the following guidance is given, in order to fulfil the requirements of the Common Criteria assurance family ALC_DVS. There are restrictions resulting from the nature of the material and information. But in addition there are general requirements for the organisation of an industrial complex like a semiconductor manufacturer.

All sensitive information and material shall be forwarded on a need-to-know basis. To guarantee the confidentiality of information each department must have a clear interface to other departments or partners. It must be ensured that the material and information being exchanged is limited to what is absolutely needed by the other partner to do the work he is responsible for.

Roles and responsibilities of departments and teams shall be well-defined. This includes the content and the extent of the work to be done. Responsibilities and competence of individuals (including managers) shall be defined. All departments should consider that they contribute to develop and produce a security product.

Defined procedures must be adhered to - and their significance has to be understood by the personnel. The process procedures shall especially define requirement for secure communication and distribution of data, documents and material between the different development and production departments and to external companies and their departments the chip manufacturer works with. Confidentiality and integrity of data have to be preserved during the whole developing and manufacturing cycle.

The hardware design department shall provide sufficient information to the department developing the IC Dedicated Software regarding inherent hardware security mechanisms in order to allow the latter to appropriately use the hardware. On the other hand this information shall be limited as far as possible.

All sensitive information and material must be stored in a secure way to ensure confidentiality and to avert unauthorised access. Appropriate measures for physical protection include but are not limited to admittance control, airlock, fences, camera supervision, locked doors and windows, safes, locked cupboards, alarm systems, burglary proof buildings. Appropriate measures to protect data files include but are not limited to logon procedures, access control, encryption, firewall systems, isolation of computers and local networks, audit and accountability.

Appropriate procedures and means for the disposal and destruction of wafers, dies and chips failed during the performed tests have to be provided in co-ordination with the requirements for traceability (refer to the sub-section “Refinement regarding ‘Configuration Management (ACM)’”).

Whenever material and information is given to external partners (such as the developer of the Smartcard Embedded Software) the latter must be obliged by an Non Disclosure Agreement to treat the material and information as it is required for the TOE Manufacturer.

5.1.3.3 Refinement regarding CM scope (ACM_SCP)

Introduction
The Common Criteria assurance component of the family ACM_SCP (CM scope) refers to the tracking of specific configuration items within the developers configuration management system.

In the particular case of a Smartcard Integrated Circuit it is helpful to clarify the scope of the configuration item “TOE implementation representation”:

The following text reflects the requirements of the selected component ACM_SCP.2:

Developer action elements:
ACM_SCP.2.1D The developer shall provide CM documentation.

Content and presentation of evidence elements:
ACM_SCP.2.1C The CM documentation shall show that the CM system, as a minimum, tracks the following: the <u>TOE implementation representation</u>, design documentation, test documentation, user documentation, administrator documentation, and CM documentation, and security flaws.

ACM_SCP.2.2C The CM documentation shall describe how configuration items are tracked by the CM system.

Evaluator action elements:
ACM_SCP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Refinement
The "TOE implementation representation" within the scope of the CM shall include at least:

- logical design data,
- physical design data,
- IC Dedicated Software,
- Smartcard Embedded Software,
- final physical design data necessary to produce the photomasks,
- photomasks and products in any form.

5.1.3.4 Refinement regarding CM capabilities (ACM_CAP)

Introduction
The Common Criteria assurance component of the family ACM_CAP (CM capabilities) refers to the capabilities of a CM system. The component ACM_CAP.4 refers to "configuration items" and "configuration list" and uses the term "TOE" in addition.

In the particular case of a Smartcard Integrated Circuit the scope of "configuration items" and the meaning of "TOE" in this context need to be clarified:

The following text reflects the requirements of the selected component ACM_CAP.4:

Developer action elements:
ACM_CAP.4.1D The developer shall provide a reference for the TOE.

ACM_CAP.4.2D The developer shall use a CM system.

ACM_CAP.4.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:
ACM_CAP.4.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.4.2C The TOE shall be labelled with its reference.

ACM_CAP.4.3C The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.

ACM_CAP.4.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.4.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.4.6C The CM system shall uniquely identify all configuration items.

ACM_CAP.4.7C The CM plan shall describe how the CM system is used.

ACM_CAP.4.8C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.4.9C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.4.10C The CM system shall provide measures such that only authorised changes are made to the configuration items.

ACM_CAP.4.11C The CM system shall support the generation of the TOE.

ACM_CAP.4.12C The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

Evaluator action elements:
ACM_CAP.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Refinement
“configuration items” comprise all items defined and refined under ACM_SCP (see above) to be tracked under CM.

The item “Smartcard Embedded Software” is only relevant for the configuration list as far as the TOE manufacturer can control it since the Smartcard Embedded Software is developed by another company and not part of the TOE though delivered together with it.

If specific requirements are not applicable for standard cells (such as standard gates, standard memories) being also used in other products, the certification body has to decide on a case by case decision how to handle them within the evaluation.

The term “TOE” shall be read as comprising all results built on the basis of the data sources. The results are

- final physical design data necessary to produce the photomasks,
- photomasks and products,

Photomasks and products must be uniquely traceable to the above “configuration items”.

A production control system has to be applied to guarantee the traceability and completeness of different production charges or lots. The number of wafers, dies and chips must be tracked by this system. Appropriate administration procedures have to be provided for managing wafers, dies or complete chips, which are being removed from the production-process in order to verify and to control predefined quality standards and production parameters. It has to be controlled that these wafers or dies are returned to the same production stage from which they are taken; otherwise they have to be destroyed.

5.1.3.5 Refinements regarding Functional Specification (ADV_FSP)

Introduction
The Common Criteria assurance component of the family ADV_FSP (functional specification) refer to the user-visible interface and behaviour of the TSF. It is an instantiation of the TOE security functional requirements. The functional specification has to show that all the TOE security functional requirements are addressed. It is a basis for the Test Coverage Analysis.

In the particular case of a Smartcard Integrated Circuit specific design measures, which are non-functional in nature, provide security and additionally, a test tool is delivered to the user as a part of the TOE. Therefore, refinements are provided.

The following text reflects the requirements of the selected component ADV_FSP.2:

Developer action elements:
ADV_FSP.2.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:
ADV_FSP.2.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.2.2C The functional specification shall be internally consistent.

ADV_FSP.2.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.

ADV_FSP.2.4C The functional specification shall completely represent the TSF.

ADV_FSP.2.5C The functional specification shall include rationale that the TSF is completely represented.

Evaluator action elements:
ADV_FSP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

Refinement

The Functional Specification is expected also to specify the operating conditions of the TOE. These conditions include but are not limited to the frequency of the clock, the power supply, and the temperature.

The Functional Specification is expected to refer to measures against physical attacks in a more general way only, but detailed enough to be able to support Test Coverage Analysis also for those measures where inspection of the layout is of relevance.

Although the IC Dedicated Test Software is a part of the TOE, the test functions of the IC Dedicated Test Software are not described in the Functional Specification because the IC Dedicated Test Software is considered as a test tool delivered with the TOE but not providing security functions for the operational phase of the TOE.

All functions and mechanisms which control access to the functions provided by the IC Dedicated Test Software (refer to the security functional requirement Limited availability (FMT_LIM.2)) must at least be referred to within the Functional Specification. Details can be given in the document for “Installation, Generation and Start-up (ADO_IGS)”, refer to Section 5.1.3.7. In addition, all these functions and mechanisms must subsequently be refined according to all relevant requirements of the Common Criteria assurance class ADV because these functions and mechanisms are active after TOE Delivery and need to be part of the assurance aspects Tests (class ATE) and Vulnerability Assessment (class AVA). Therefore, all necessary information must be provided to allow tests and vulnerability assessment.

5.1.3.6 Refinement regarding Test Coverage (ATE_COV)

Introduction

The Common Criteria assurance component of the family ATE_COV (test coverage) “addresses the extent to which the TSF is tested, and whether or not the testing is sufficiently extensive to demonstrate that the TSF operates as specified.”

The following text reflects the requirements of the selected component ATE_COV.2:

Developer action elements:

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

Content and presentation of evidence elements:

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

Evaluator action elements:
ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Refinement
The TOE must be tested under different operating conditions (at least) within the specified ranges. These conditions include but are not limited to the frequency of the clock, the power supply, and the temperature. This means that "Limited fault tolerance (FRU_FLT.2)" must be proven for all TSF (including the TOE's random number generator, refer to the functional requirement FCS_RND.1). The tests must also cover functions which may be affected by "ageing" (such as E^2PROM writing).

The existence and effectiveness of measures against physical attacks (as specified by the functional requirement FPT_PHP.3) can not be tested in a straightforward way. Instead the TOE Manufacturer shall provide evidence that the TOE actually has the particular physical characteristics (especially layout design principles). This can be done by checking the layout (implementation or actual integrated circuit) in an appropriate way. The required evidence pertains to the existence of measures against physical attacks (unless being obvious) but will cover only a subset of the characteristics against physical attacks.

The IC Dedicated Test Software is seen as a "test tool" being delivered as part of the TOE. However, the Test Features do not provide security functions and are not used after TOE Delivery. Therefore, Test Features need not to be covered by the Test Coverage Analysis but all functions and mechanisms which control access to the functions provided by the IC Dedicated Test Software must be part of the Test Coverage Analysis.

5.1.3.7 Refinement regarding Installation, Generation and Start-up (ADO_IGS)

Introduction
The life-cycle model to be described under the Common Criteria assurance component of the family ALC_LCD refers to organisational and procedural controls such as design methods, review procedures, project management controls, change control procedures, test methods and acceptance procedures. TOE configuration and administration is subject to the Common Criteria assurance component of the families ADO_IGS and AGD_ADM.

The requirements of the Common Criteria assurance family ADO_IGS "call for a secure transition from the TOE's implementation representation being under configuration control to its initial operation in the user environment." "The requirements in this assurance family are presented separately from those in the AGD_ADM family, due to the infrequent, possibly one-time use of the installation, generation and start-up procedures.“

Though the TOE is not delivered and then configured, its configuration needs to be addressed as a specific aspect since these procedures may affect the overall security. Therefore, the terms "installation" and "generation" need to be refined:

The following text reflects the requirements of the selected component ADO_IGS.1:

Developer action elements:
ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:
ADO_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

Evaluator action elements:
ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

Refinement
The TOE may be configured after production before the Smartcard is delivered to the end-user (this would be addressed by security functional requirement Limited availability (FMT_LIM.2)). In this case, these configuration aspects have to be considered. Differences between the TOE before first use (normally done during wafer test) and Phase 7 must be summarised. Guidance to change that behaviour must exist. Regarding technical details, the documentation provided by the developer can refer to documents provided for the Common Criteria class ADV.

Note that most of the security functions will already be effective before TOE Delivery. However, guidance to determine the behaviour of Security Functions, to disable, to enable or to modify the behaviour of Security Functions must be given as follows:

- If configuration of a Security Function of the TOE done before TOE Delivery (that means by the TOE Manufacturer) the corresponding guidance is given under the assurance component of the family ADO_IGS. Note that this document is an internal document of the TOE Manufacturer and not delivered to their customers.
- If administration of a Security Function of the TOE is done after TOE Delivery (that means by the Card Manufacturer) the corresponding guidance must be in the Administrator Guidance (refer to the Common Criteria assurance component of the family AGD_ADM) as it shall describe how to administer the TOE in a secure manner. This guidance document is delivered by the TOE Manufacturer.

Guidance documents must not contain security relevant details which are not absolutely necessary for the administration actually to be done.

5.1.3.8 Refinement regarding User Guidance (AGD_ADM)

Introduction
The Common Criteria assurance components of the families AGD_USR (user guidance) and AGD_ADM (administrator guidance) "describe all relevant aspects for the secure application of the TOE." The terms "user" and "administrator" are used.

In the case of a Smartcard Integrated Circuit the meaning of the terms "user" and "administrator" are not obvious. Therefore, the following refinements are given regarding guidance.

User guidance refers to material that is intended to be used by non-administrative human users of the TOE, and by others (e.g. programmers) using the TOE's external interfaces. User guidance describes the security functions provided by the TSF and provides instructions and guidelines, including warnings, for its secure use.

The following text reflects specific requirements of the selected component AGD_USR.1:

Developer action elements:
AGD_USR.1.1D The developer shall provide <u>user</u> guidance.

Content and presentation of evidence elements:
AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative <u>users of the TOE</u>.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

Refinement
The TOE serves as a platform for the Smartcard Embedded Software. Therefore, the "user" of the TOE (as used in the Common Criteria assurance class AGD: guidance) is the Smartcard Embedded Software.

- User Guidance (refer to the Common Criteria assurance component of the family AGD_USR) must be given to the developer of the Smartcard Embedded Software to ensure that the Smartcard Embedded Software properly uses the TOE.

On the other hand the Smartcard (with the TOE as a major element) is used in a terminal where communication is performed through the ISO interface provided by the TOE. Therefore, another "user" of the TOE is the terminal (with its software).

- User Guidance (refer to the Common Criteria assurance component of the family AGD_USR) must be given to the developer of the terminal. However, this is only little information about the physical characteristics of the device, the ISO interface and perhaps standard protocols (such as T=1 if implemented in the TOE). Other information could be needed if the TOE provides other services in the end-user phase (Phase 7, refer to section 9.1) which may be augmented to this Protection Profile.

The User Guidance documents should provide only the information which is necessary for using the TOE. Depending on the recipient of that guidance documentation User and Administrator Guidance can be given in the same document.

After production the TOE is tested where communication is performed by directly contacting the pads that mostly become part of the ISO interface during packaging. Here no guidance document according to Common Criteria class AGD is required (provided that the tests are performed by the TOE Manufacturer). Note that test procedures are described under the Common Criteria assurance component of the family ATE_FUN.

5.1.3.9 Refinement regarding Administrator Guidance (AGD_ADM)

Introduction
Administrator guidance refers to written material that is intended to be used by those persons responsible for configuring, maintaining, and administering the TOE in a correct manner for maximum security.

The following text reflects specific requirements of the selected component AGD_ADM.1:

Developer action elements:
AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:
AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

Refinement
If the TOE provides security functions which can or need to be administrated (i) by the Smartcard Embedded Software or (ii) using services of the TOE after TOE Delivery (refer to section 2.2) an Administrator Guidance must be given in addition.

Most of the security functions will already be effective before TOE Delivery. However, guidance to determine the behaviour of Security Functions, to disable, to enable or to modify the behaviour of Security Functions must be given if administration of a Security Function is done after TOE Delivery (that means by the Card Manufacturer). This guidance document is delivered by the TOE Manufacturer.

Guidance documents must not contain security relevant details which are not absolutely necessary for the administration actually to be done. Depending on the recipient of that guidance documentation User and Administrator Guidance can be given in the same document.

5.1.3.10Additional Guidance regarding Vulnerability Analysis (AVA_VLA)" and Strength of Functions (AVA_SOF)

When rating attack potential according to the Common Methodology for Information Technology Security Evaluation [4] for the assurance aspects Vulnerability Analysis and Strength of Functions, as expertise of an attacker it is distinguished between "expert", "proficient" and "laymen". With respect to the knowledge of the TOE it is distinguished between "no information about the TOE", "public information concerning the TOE", and "sensitive information about the TOE". The information gained from a user guide is given as an example for public information concerning the TOE. This is not applicable here since the protection of such information is demanded according to this Protection Profile (refer to refinement regarding "Development Security (ALC_DVS)").

During the Vulnerability Analysis it must be assessed that the functions provided by the IC Dedicated Test Software can not be abused after TOE Delivery (refer to the security functional requirements FMT_LIM.1 and FMT_LIM.2). All necessary information must be provided to allow that assessment.

5.2 Security Requirements for the Environment

5.2.1 Security Requirements for the IT-Environment

The security objectives for the environment will be ensured by Non-IT security requirements only (refer to the next subsection, section 5.2.2, and the rationale, section 8.2.1).

5.2.2 Security Requirements for the Non-IT-Environment

In the following security requirements for the Non-IT-Environment are defined for the development of the Smartcard Embedded Software (in Phase 1) and the Smartcard Packaging, Finishing and Personalisation (Phases after TOE Delivery up to Phase 7).

The Smartcard Embedded Software is developed in Phase 1 and must support the security functionality of the TOE. This Protection Profile does not directly define obligatory security functional requirements for the Smartcard Embedded Software itself, because this might restrict the implementation possibilities for the developer. Instead the following general requirement for the design and implementation of the software is stated.

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

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

The developers shall implement the Smartcard Embedded Software in a way that it protects security relevant User Data (especially cryptographic keys) as required by the security needs of the specific application context.[22]

The requirement RE.Phase-1 also addresses the fact that the Smartcard Embedded Software may need to support the security functions of the TOE. Examples for such security functional requirements for the Smartcard Embedded Software are given in section 9.2.2.

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).

[22] In particular, the Smartcard Embedded Software shall not disclose secret User Data to unauthorised users or processes as defined for the application context. Similarly the Smartcard Embedded Software shall not allow unauthorised users or processes to use or modify security relevant User Data.

6 TOE Summary Specification

The chapter is divided into the following sections:

TOE Security Functions

Assurance measures

6.1 TOE Security Functions

The IT security functions directly correspond to the TOE security functional requirements defined in chapter 5.1.1.

The following security functions are applicable to the phases 4 to 7

Note: Some of the security functions are configured at the end of phase 3 and all security functions are already active during the delivery form phase 3 to phase 4.

F.RNG: The random number generator continuously produces random numbers with a length of one byte. Each byte will at least contain a 7 bit entropy. The TOE implements the F.RNG by means of a physical hardware random number generator working stable within the limits guaranteed by F.OPC (operational conditions).

This Security Function fulfils the security functional component FCS_RND.1.

F.DEA: The TOE provides the Triple Data Encryption Algorithm (TDEA) according to the Data Encryption Standard (DES). F.DEA is a modular basic cryptographic function which provides the TDEA algorithm as defined by FIPS PUB 46 by means of a hardware co-processor and supports the 2-key Triple DEA algorithm according to keying option 2 in FIPS PUB 46-3. The two 56 bit keys (112 bit) for the 2-key Triple DES algorithm shall be provided by the application software. For encryption the application software provides 8 byte of the plain text and F.DEA calculates 8 byte cipher text. The output of calculation is read by the application software. For decryption the application software also provides 8 byte of cipher text and F.DEA calculates 8 byte plain text. The output of calculation is read by application software.

The TSF provides specific implementation features to reduce leakage of confidential user and TSF data to ensure that attackers are unable to observe the keys and plain text by measuring the external behaviour during the Triple-DES-operation. This includes:

Differential Power Analysis,

Differential Fault Analysis,

Simple Power Analysis and

Timing Attacks.

This Security Function fulfils the security functional component FCS_COP.1 and in part the SFRs FDP_ITT.1, FPT_ITT.1 and FDP_IFC.1

F.OPC: The function F.OPC has the following sub-functions: A function that filters power supply and clock input and a function that monitors the power supply, the frequency of the clock and the temperature of the chip by means of sensors. The ranges allowed for these parameters are defined for:

low frequency of clock input and

high frequency of clock input and

low voltage power supply and

high voltage power supply and

low temperature and

high temperature and

high voltage for the write process to the EEPROM.

If one of these parameters is out of the specified range a reset of the actual running program and a CPU reset will be initiated. Before TOE delivery the mode-switch is set to user mode. In user mode the TOE enables the sensors automatically when operated. Furthermore it prevents that the application program disables the sensors.

This Security Function fulfils the security functional component FRU_FLT.2, FPT_FLS.1 and in part FPT_SEP.1.

F.PHY: The function F.PHY protects the TOE against manipulation of (i) the hardware, (ii) the test software in the ROM, (iii) the application software in the ROM and the E2PROM, (iv) the application data in the E2PROM and RAM, (v) the configuration data in the security row and (vi) the mode-switch. It also protects secret user data against the disclosure when stored in E2PROM and RAM or while being processed by the TOE (thereby also supporting FDP_ITT.1, FPT_ITT.1 and FDP_IFC.1).

The protection of the TOE comprises different features of the construction which makes a tamper attack more difficult. By this the security function F.PHY also supports in general the secure implementation of all Security Functional Requirements defined in chapter 5.1.1.

This Security Function fulfils the security functional component FPT_PHP.3 and in part the SFRs FDP_ITT.1, FPT_ITT.1 and FDP_IFC.1 (and supports all other SFRs).

F.COMP: The function F.COMP provides access control by means of TOE modes of operation selected by a mode-switch: (i) Test Mode and (ii) User Mode. The F.COMP contains 3 sub-functions:

Identification: In the Test Mode the TOE identifies the administrator. In the User Mode the TOE identifies the user.

Access control: In the Test Mode the TOE (i) allows to execute the test software and (ii) prevents to execute the application software. In the User Mode the TOE (i) allows to execute the application software and (ii) prevents to execute the test software.

Mode switch: The initial TOE mode is the Test Mode. The TOE allows to change the mode-switch from the Test mode into the User Mode. If the mode-switch is changed the TOE will remain in an endless loop waiting for a reset to start a program in the User mode. The TOE prevents to change the mode-switch from the User mode into the Test Mode.

Further the security function F.COMP maintains the security domain for its own execution that protects it from interference and tampering by untrusted subjects both in the Test Mode and in the User Mode. It also enforce the separation between the security domains of subjects within each mode.

The function F.COMP also provides test personnel during Phase 3 with the capability to store the identification and/or pre-personalisation data and/or supplements of the Smartcard Embedded Software in the EEPROM.

This Security Function fulfils the security functional component FMT_LIM.1, FMT_LIM.2 and FAU_SAS.1 and in part FPT_SEP.1.

Explicit SOF claim

According to the CEM a Security Target shall identify all mechanisms which can be assessed according to the assurance requirement AVA_SOF.1.

The following mechanisms contributing to these functions were identified, which can be analysed for their permutational or probabilistic properties:

1. The output of the Random Number Generator F.RNG can be analysed with probabilistic methods.
2. The quality of the mechanism contributing to the DPA resistance of F.DEA can be analysed using probabilistic methods on power consumption of the TOE.

Therefore an explicit SOF claim of “high” is made for these mechanisms.
Note, that the cryptographic algorithm of F.DEA can also be analysed with permutational or probabilistic methods but that this is not in the scope of CC evaluations.

6.2 Assurance measures

Appropriate assurance measures will be employed to satisfy the security assurance requirements defined in chapter 5.1.2. The developer will provide documents containing the measures and further information needed to examine conformance of the measures to the assurance requirements. The following table gives a mapping between the assurance requirements and the documents containing the information needed for the respective requirement either directly or referring to further documents containing this information.

Document containing or referring the relevant information	Input evidence according to CC Part 3, which is contained or referred to in the document	Input for assurance component(s) (according to developer actions in CC Part 3)
Functional Specification, Data Sheet	semiformal functional specification	ADV_FSP
	correspondence analysis between the TOE summary specification and the functional specification	ADV_RCR
Formal Model	TSP model (formal)	ADV_SPM
High Level design, Design Report	high-level design (semiformal)	ADV_HLD
	correspondence analysis between functional specification and high-level design	ADV_RCR
Low Level Design, Design Report	low level design	ADV_LLD
	architectural description	ADV_INT
	correspondence analysis between functional specification and high-level design	ADV_RCR
	correspondence analysis between high-level design and implementation representation	ADV_RCR
Implementation representation, Source Code	implementation representation	ADV_IMP
Configuration Management and Life Cycle documentation, and additional documents referenced in this document	configuration management documentation	ACM
	development tools documentation	ALC
	development security documentation	
	life cycle definition documentation	
	parts of the delivery documentation	ADO
Guidance, Delivery and Operation, Data Sheet	administrator guidance	AGD_ADM, AVA_MSU
	secure installation, generation, and start-up procedures	ADO_IGS

Document containing or referring the relevant information	Input evidence according to CC Part 3, which is contained or referred to in the document	Input for assurance component(s) (according to developer actions in CC Part 3)
	user guidance	AGD_USR, AVA_MSU
	parts of the delivery documentation	ADO_DEL
Vulnerability Assessment	vulnerability assessment	AVA
	covert channel analysis	
	strength of function claims analysis	
Test Documentation Roadmap, Verification Test, Characterisation Report, Electrical Test Specification	test documentation	ATE
	test coverage analysis	
	depth of testing analysis	

Table 3: List of documents describing the measures regarding the assurance requirements

7 PP Claims

This Security Target doesn't claim formal conformance to a protection profile.

However, this Security Target is written using a draft version of a Protection Profile "Smartcard IC Platform Protection Profile" under development by the following Integrated Circuits manufacturers:

- Atmel,
- Hitachi Europe,
- Infineon Technologies, and
- Philips Semiconductors.

8 Rationale

The chapter *Rationale* is divided into the following sections:

Security Objectives Rationale
Security Requirements Rationale
TOE Summary Specification Rationale
PP Claims Rationale

8.1 Security Objectives Rationale

Table 4 below gives an overview, how the assumptions, threats, and organisational security policies are addressed by the objectives. The text following after the table justifies this in detail.

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	(Phase 4 – 6)
P.Add-Func	O.DES3	
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	

Table 4: Security Objectives versus Assumptions, Threats or Policies

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

> 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.

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

> 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.

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

> OE.Process-TOE requires the TOE manufacturer to implement those measures assumed in P.Process-TOE. Therefore, the assumption 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 assumption is covered by OE.Process-Card and O.Identification.

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

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

The justification related to the organisational security policy “ Additional Security Functionality (P.Add-Func)” is as follows:

> O.DES3 states that the TOE shall implement Triple DES encryption and decryption. This is exactly what is required by P.Add-Func. Therefore this security policy is covered by the objective.

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:

> For all threats the corresponding objectives (refer to Table 4) are stated in a way, which directly corresponds to the description of the threat (refer to Section 3.3). It is clear from the description of each objective (refer to Section 4.1), 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 removed, if the objective holds.

8.2 Security Requirements Rationale

8.2.1 Rationale for the security functional requirements

Table 5 below gives an overview, how the security functional requirements are combined to meet the security objectives. The detailed justification follows after the table.

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 to physical attack”	RE.Phase-1 “Design and Implementation of the Smartcard Embedded Software”

Objective	TOE Security Functional Requirements	Security Requirements for the environment
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 plus those listed for O.Malfunction and O.Phys-Manipulation	RE.Phase-1 "Design and Implementation of the Smartcard Embedded Software"
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	
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	RE.Phase-1 "Design and Implementation of the Smartcard Embedded Software" (e. g. by implementing FPT_AMT.1 "Abstract machine testing")

Objective	TOE Security Functional Requirements	Security Requirements for the environment
O.DES3	FCS_COP.1 “Cryptographic operation” plus those for O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation, O.Leak-Forced	RE.Phase-1 “Design and Implementation of the Smartcard Embedded Software” (e. g. by implementing appropriate key management)
OE.Plat-Appl		RE.Phase-1 “Design and Implementation of the Smartcard Embedded Software”
OE.Resp-Appl		RE.Phase-1 “Design and Implementation of the Smartcard Embedded Software”
OE.Process-TOE	FAU_SAS.1 “Audit storage”	Several Assurance Components[23]
OE.Process-Card		RE.Process-Card, possibly supported by RE.Phase-1

Table 5: Security Requirements versus Security Objectives

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

> 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 between separate 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.
>
> 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.

[23] Delivery (ADO_DEL); Installation, generation, and start-up (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)

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

> 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.
> It is possible that the TOE needs additional support by the Smartcard Embedded Software (e. g. to send data over certain busses 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.

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

> 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 by 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 works normally 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 constellation for O.Malfunction, which is not covered.

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

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

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

> 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 he 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.

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

This objective states that abuse of functions (especially provided by the IC Dedicated Test Software, e. g. 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.

Other security functional requirements which prevent attackers from circumventing the functions implementing these two security functional requirements (e. g. by manipulating the hardware) also support the objective (the relevant objectives are listed in Table 5).

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: The reason to prefer security functional requirements from Part 2 of the Common Criteria wherever possible is, that the potential customer shall be able to compare the properties of different products because similar security functional requirements are used. However, any selection from Part 2 of the Common Criteria would make 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.

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

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.

It was chosen to define FAU_SAS.1 explicitly (not using a given SFR from Part 2 of the Common Criteria) for the following reason: The SFR 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 (e. g. data and time). The possibility to use test functions in order to store security relevant 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.

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

FCS_RND.1 requires the TOE to provide random numbers of good quality. Other security functional requirements, which prevent physical manipulation of the TOE (see the corresponding objectives listed in the table) support this objective because they prevent attackers from manipulating or otherwise affecting the RNG.

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.

Depending on the functionality of specific TOEs the Smartcard Embedded Software will have to support the objective by providing runtime-tests which check that the RNG is still active. Together, these requirements allow the TOE to provide cryptographically good random numbers.

It was chosen to define FCS_RND.1 explicitly, because Part 2 of the Common Criteria do 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.)

The justification related to the objective “Cryptographic operation” (O.DES3)” is as follows:

FCS_COP.1 requires the TOE to implement Triple DEA. Other security functional requirements, which prevent physical manipulation of the TOE (see the corresponding objectives listed in the table) support this objective because they prevent attackers from manipulating or otherwise affecting the Triple-DEA implementation.

Note that the TOE must also prevent the unauthorised disclosure of secret user data processed by the DEA hardware. Other security functional requirements which prevent inherent leakage attacks, probing and forced leakage attacks ensure this.

The Smartcard Embedded Software will have to support the objective by providing appropriate key management. Together, these requirements allow the TOE to provide a secure Triple DEA implementation.

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

> 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.

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

> 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.

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

> The objective OE.Process-TOE has mainly to be fulfilled by organisational and other measures, which the IC designer and manufacturer has to implement in Phases 2 and 3. 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 Identification data is provided according to FAU_SAS.1. Together these security requirements are suitable to meet the objective.

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

> RE.Process-Card requires the responsible parties for Phases 4-6 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 e. g. by using appropriate authentication mechanisms for personalisation functions. Therefore, RE.Phase-1 may support RE.Process-Card in fulfilling the objective.

8.2.2 Dependencies of security functional requirements

Table 6 below lists the security functional requirements defined in this Security Target, their dependencies and whether they are satisfied by other security requirements defined in this Security Target. The text following the table discusses the remaining cases.

Security Functional Requirement	Dependencies	Fulfilled by security requirements in this ST
FRU_FLT.2	FPT_FLS.1	Yes
FPT_FLS.1	ADV_SPM.1	Yes (Part of EAL 5)
FPT_SEP.1	None	No dependency
FMT_LIM.1	FMT_LIM.2	Yes

Security Functional Requirement	Dependencies	Fulfilled by security requirements in this ST
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)
FPT_ITT.1	None	No dependency
FDP_IFC.1	FDP_IFF.1	See discussion below
FCS_RND.1	None	No dependency
FCS_COP.1	FDP_ITC.1 or FCS_CKM.1; FCS_CKM.4; FMT_MSA.2	See discussion below

Table 6: Dependencies of the Security Functional Requirements

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.

FCS_COP.1 requires a number of dependencies, all of which are related to key management. Since the Triple-DEA-functionality is provided to the application software and the cryptographic keys are parameters supplied by the application software, these dependencies have to be fulfilled by functionality of the application software. A comprehensive discussion, how this can be achieved is already given in section 5.2.2. Therefore the dependency is considered satisfied.

As Table 6 shows, all other dependencies are fulfilled by security requirements defined in this Security Target.

The discussion in section 8.2.1 has shown, how the security functional requirements support each other in meeting the security objectives of this Security Target. In particular the security functional requirements providing resistance of the hardware against manipulations (e. g. FPT_PHP.3) support all other more specific security functional requirements (e. g. FCS_RND.1) because they prevent an attacker from disabling or circumventing the latter. Together with the discussion of the dependencies above this shows that the security functional requirements build a mutually supportive whole.

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

The assurance level EAL 5 and the augmentation with the requirements ADV_LLD.2, ALC_DVS.2, AVA_MSU.3, and AVA_VLA.4 were chosen in order to meet assurance expectations of digital signature applications and electronic payment systems.

It has to be assumed that attackers with high attack potential try to attack smart cards used for digital signature applications or payment systems. Therefore specifically AVA_VLA.4 was chosen in order to assure that even these attackers cannot successfully attack the TOE. For the same reason the Strength of Function level “high” is required.

The assurance components in an EAL level are chosen in a way that they build a mutually supportive and complete set of components. The requirements chosen for augmentation do not add any dependencies, which are not already fulfilled for the corresponding requirements contained in EAL 5. Therefore, these components add additional assurance to EAL 5, but the mutual support of the requirements is still guaranteed.

The following argument shows that the assurance requirements chosen for this Security Target are also applicable to and appropriate for the explicitly defined SFRs. All explicitly defined SFRs are defined in close analogy to the SFRs included in the CC Part 2: FCS_RND.1 provides cryptographic functionality comparable to FCS_COP.1. FAU_SAS.1 is a more general version of FAU_GEN.1 while FMT_LIM.1 and FMT_LIM.2 describe a specific situation but are comparable with requirements regarding access control and information flow security in CC Part 2. Therefore these SFRs can be examined with the same assurance methods as the Part 2 SFRs.

8.2.4 Security Requirements are Mutually Supportive and Internally Consistent

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.

8.3 TOE Summary Specification Rationale

Note: This chapter (8.3) was not intended to be published

8.4 PP Claims Rationale

This Target doesn’t claim formal conformance to a PP.

However, this Security Target is written using a draft version of a Protection Profile “Smartcard IC Platform Protection Profile“ under development by the following Integrated Circuits manufacturers:

- Atmel,
- Hitachi Europe,
- Infineon Technologies, and
- Philips Semiconductors.

9 Annexes

9.1 Development and Production Process (life-cycle)

9.1.1 Life-Cycle Description

The smartcard product life-cycle is visualised in Figure 4.

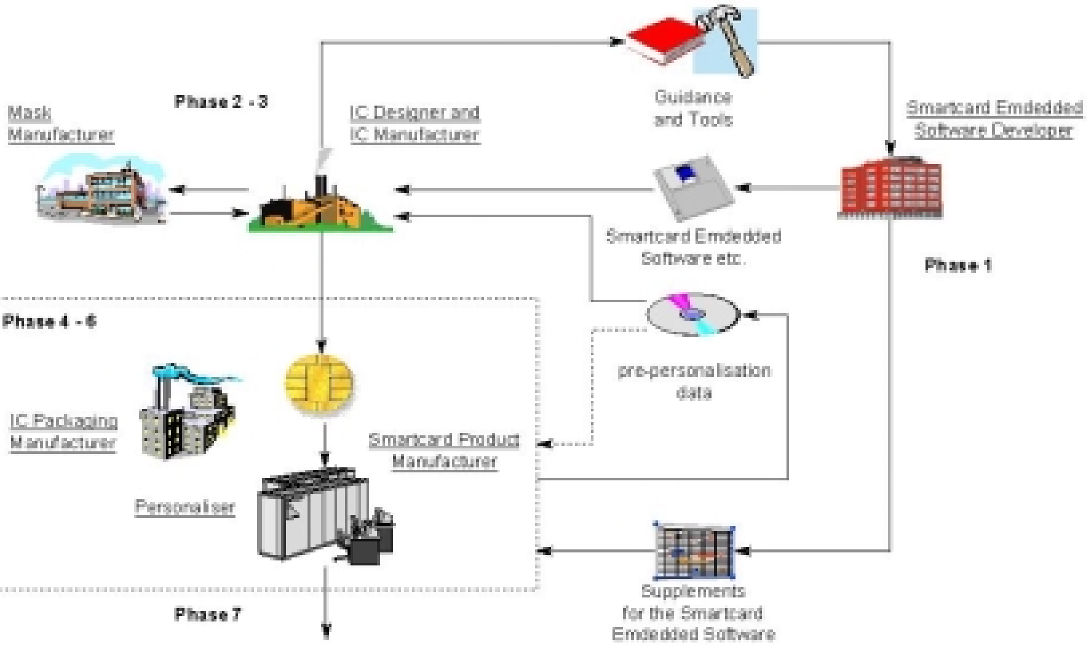

Phase 2 - 3
Mask Manufacturer
IC Designer and IC Manufacturer
Guidance and Tools
Smartcard Emdedded Software Developer
Smartcard Emdedded Software etc.
Phase 1
Phase 4 - 6
pre-personalisation data
IC Packaging Manufacturer
Smartcard Product Manufacturer
Personaliser
Phase 7
Supplements for the Smartcard Emdedded Software

Figure 4: Smartcard Life-Cycle

The smartcard product life-cycle is decomposed into seven phases where the following authorities are involved:

Phase 1	Smartcard Embedded Software Development	The Smartcard Embedded Software Developer is in charge of • the smartcard embedded software development and • the specification of IC pre-personalisation requirements, though the actual data for IC pre-personalisation come from Phase 6 (or Phase 4 or 5).

Phase 2	IC Development	The IC Designer • designs the IC,

		• develops IC Dedicated Software, • provides information, software or tools to the Smartcard Embedded Software Developer, and • receives the smartcard embedded software from the developer, through trusted delivery and verification procedures. From the IC design, IC Dedicated Software and Smartcard Embedded Software, the IC Designer • constructs the smartcard IC database, necessary for the IC photomask fabrication.
Phase 3	IC Manufacturing and Testing	The IC Manufacturer is responsible for • producing the IC through three main steps: IC manufacturing, IC testing, and IC pre-personalisation. The IC Mask Manufacturer • generates the masks for the IC manufacturing based upon an output from the smartcard IC database.
Phase 4	IC Packaging and Testing	The IC Packaging Manufacturer is responsible for • the IC packaging and testing.
Phase 5	Smartcard Product Finishing Process	The Smartcard Product Manufacturer is responsible for • the smartcard product finishing process and testing.
Phase 6	Smartcard Personalisation	The Personaliser is responsible for • the smartcard personalisation and final tests. Other smartcard embedded software may be loaded onto the chip at the personalisation process,
Phase 7	Smartcard End-usage	The Smartcard Issuer is responsible for • the smartcard product delivery to the smartcard end-user, and the end of life process.

The relation between the semiconductor industry (TOE Manufacturer, refer to Section 2.1, in particular comprising the roles IC Designer / IC Manufacturer and IC Mask Manufacturer) and the other parties being involved in the Smartcard development and production (especially the Smartcard Embedded Software Developer) are visualised in Figure 5.

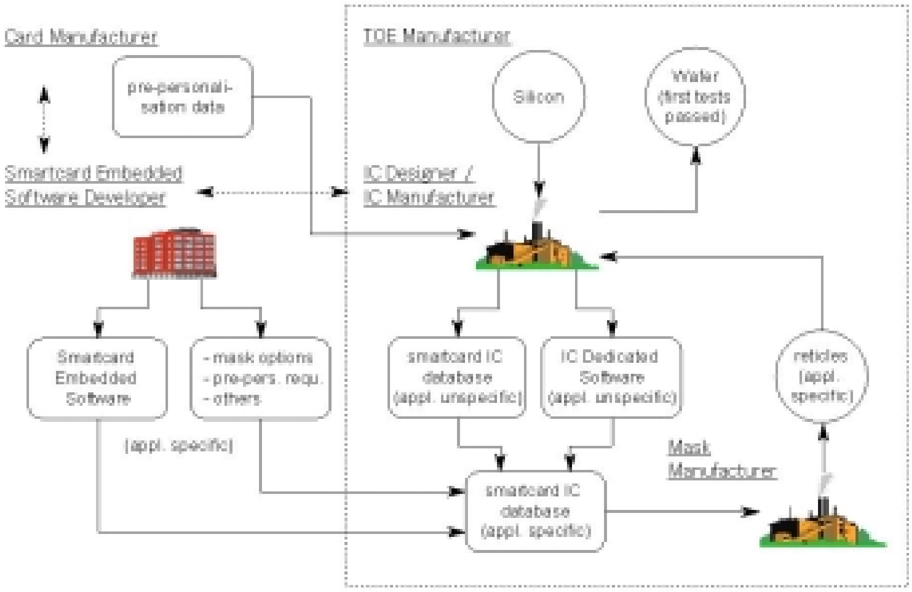

Card Manufacturer
pre-personali-sation data
Smartcard Embedded Software Developer
TOE Manufacturer
Silicon
Wafer (first tests passed)
IC Designer / IC Manufacturer
Smartcard Embedded Software
- mask options
- pre-pers. requ.
- others
(appl. specific)
smartcard IC database (appl. unspecific)
IC Dedicated Software (appl. unspecific)
reticles (appl. specific)
Mask Manufacturer
smartcard IC database (appl. specific)

Figure 5: Development and Wafer Production including Testing

The development process of the TOE starts with a process qualification. In parallel the concept of the integrated circuit and the corresponding logical design is developed. The design uses standard library elements (circuitry and layout) which could be used for other (non security) integrated circuits but may include full custom elements specially designed for the TOE as well. Some cells have parameters: For instance the concrete layout of a ROM cell is determined by its contents which in turn is determined by the software or the data to be stored within.

All these "cells" not only differ in their logical or physical behaviour but also in their structure size which may range from very few elements such as simple gates up to physical units or sub-circuitry which may represent whole independent logical processing units. The physical "cells" (physical layout information is used) are placed on the chip area and then connected by wires (routing). Information about the physical layout of "cells", about their position, about the shape of connecting wires and other process information define the physical layout of the chip.

These development steps are very complex. Only the development of the logical design might be similar to standard software development. However, technological constraints (such as timing) make this process more complicated and require for instance simulations which take technological and layout information into account. So, logical and physical design are developed in close relation.

The development of the information which defines the physical layout of an integrated circuit is a very complex matter. The masks or reticles required for wafer production are basically produced based upon this information. However, a bunch of technology related parameters (possible even some depending on the wafer foundry) are taken into account in addition.

The masks or reticles are used to realise the integrated circuitry on/in a substrate. This again comprises tens of process steps each effecting the final result. Not only layout principles but process information is proprietary to IC Designers / IC Manufacturers. The evaluator will not be able to comprehend the details of wafer processing. Each single chip (die or dice) is being tested after production.

The development and production is based upon a well established process of the manufacturer of the TOE. The processes are continuously developed and improved mainly in order to increase yield and reliability.

During integrated circuit development and production many information and material is produced as summarised in section 9.1.3. The evaluator must concentrate on the most important assets and exactly assess their storage and handling. It is not sufficient to assess a company as a whole, arguing that personnel is trustworthy and exchange of information and material with external partners is properly controlled.

9.1.2 Scope of the Common Criteria Assurance Requirements

The Common Criteria depict the product's life-cycle by defining appropriate assurance components. The scope of those assurance components referring the product's life-cycle is limited to Phases 2 and 3. These phases are under the control of the Integrated Circuits manufacturer. All procedures within these phases are covered by the Security Target. This includes the interfaces to the other phases where information and material is being exchanged with the partners of the Integrated Circuits manufacturer.

The TOE shall provide its security functions in Phase 7 where (normally) no control can be applied to the smartcard. Though most of the security functions will already be effective in Phases 4-6. Differences must be summarised under the assurance component of the family ADO_IGS. Guidance to change that behaviour must exist.

The interfaces to be considered in the assurance component of the family ADO_DEL (delivery) are:

- the interface with the Smartcard Embedded Software Developer (Phase 1) where
- information about the smartcard integrated circuit (data sheets etc.) and development software and/or tools are delivered by the Integrated Circuits manufacturer,
- the IC pre-personalisation requirements are received by the Integrated Circuits manufacturer, and
- the Smartcard Embedded Software and possible information about mask options etc. is received by the Integrated Circuits manufacturer,
- the interface with Phases 4 through 7 where
- pre-personalisation data are received by the Integrated Circuits manufacturer,
- information about tests is delivered by the Integrated Circuits manufacturer, and

- the product is delivered by the Integrated Circuits manufacturer in form of wafers, sawn wafers (dice) or modules.

The last step originally pertains to the requirements for secure delivery to be described in family ADO_DEL.

The IC Designer or IC Manufacturer is responsible to guarantee confidentiality and authenticity on

- the interface within Phase 3 where
- the necessary part of the smartcard IC database is delivered to the IC Mask Manufacturer and
- the IC photomasks are received by the Integrated Circuits manufacturer.

This is considered under the Common Criteria assurance component of the family ALC_DVS (development security) since the IC Designer or IC Manufacturer can not delegate any responsibility.

9.1.3 Description of Assets of the Integrated Circuits Designer/Manufacturer

The assets of the manufacturer of the TOE to be protected during development and production of the TOE were already identified. Further explanatory text is given here.

The logical design data are those used to design the schematics of the chip (schematics or HDL sources and design documents). With the logical design data the functionality of the chip can be understood. The logical design data can be regarded as being independent from the actual implementation (layout) though they contain the timing characteristics of some functional units (circuitry blocks).

The physical design data comprises all topographic information (three dimensional) about parts of the chip or the whole chip. Topographic information is the absolute or relative position, form, thickness, length and size of any structures realised on the chip surface. These structures are pads, connecting wires, isolation layers, vias, and implants.

The IC Dedicated Software, Smartcard Embedded Software, Initialisation Data and Pre-personalisation Data comprises the source code including the related documents and the corresponding binaries as well as other data to be injected into the TOE before TOE Delivery.

The specific development aids comprise all tools especially developed to produce the product. One important example is the “ROM translator” which produces the physical memory content from the software binaries.

The test and characterisation related data comprise all information, which is used for testing including test results (pre-layout, post layout and product) and the characterisation of the final chip.

The material for software development support comprises all information and material given to the Smartcard Embedded Software Developer to support the development of the Smartcard Embedded Software.

The photomasks and products comprises the photomasks or reticles (usable and scrap) and chips (usable and scrap) in different forms.

The requirements of the Common Criteria assurance family ALC_DVS apply to all the above items. This includes assessment of all sites being involved in the development and production of the product. Exceptions must be agreed with the certification body.

9.2 Security Aspects of the Smartcard Embedded Software

9.2.1 Further Information regarding A.Resp-Appl

When defining the Protection Profile or Security Target for the evaluation of the Smartcard Embedded Software appropriate threats must be defined which depend on the application context. These security needs are condensed in the assumption A.Resp-Appl (refer to section 3.2) of this Protection Profile which is very general since the application context is not known and the evaluation of the Smartcard Embedded Software is not covered by this Protection Profile. Refer to the requirement RE.Phase-1 (Section 5.2.2) in addition.

Note that this Security Target only specifies (and further refers to) the assumptions A.Plat-Appl and A.Resp-Appl for the usage of the TOE. All other assumption on the development of the Smartcard Embedded Software are only given for the sake of information and are examples which must be selected and refined in the application context. The evaluation of the smartcard integrated circuit according to this Security Target is conducted independent from the application context and evaluation results must be available before the evaluation of the Smartcard Embedded Software can be completed.

The next level of security aspects for the Smartcard Embedded Software (TOE security environment) are expected to cover the following:

Secure Communications (A.Sec-Com)

The Smartcard Embedded Software must support secure communication protocols and procedures between the smartcard and a terminal or a remote host as required by the application context. This prevents

- unauthorised usage of functions and/or data by intercepting data on the I/O-lines,
- disclosure or undetected manipulation of data exchanged via the I/O-lines.
- replay of exchanged data through the I/O-lines

which would cause for instance financial loss or at least affect the reputation of the system. Details must be specified in the application context.

Logical Protection (A.Log-Prot)

The Smartcard Embedded Software must prevent logical compromise through attacks on its logical operation visible on the external I/O interface. This includes protection against

- release of information though the analysis of responses to repetitive challenges[24],
- causing faults by stimulating the card and interrupting its operation, and
- disclosure of data by measuring and analysis as described in O.Leak.

Details must be specified in the application context.

Further concrete requirements for the Smartcard Embedded Software may include but is not limited to (i) Data Authenticity (A.Data-Auth), (ii) User Authentication (A.User-Auth), (iii) Stored Data Confidentiality (A.Data-Conf), (iv) Accountability (A.Account), (v) Access Control (A.Acc-Control), (vi) Administration (A.Admin), (vii) Audit and Accountability (A.Audit). The concrete requirements are to be defined in the Protection Profile / Security Target for the Smartcard Embedded Software.

9.2.2 Examples of Specific Functional Requirements for the Smartcard Embedded Software

The following two Security Functional Requirements are typical examples of functionality to be provided by the Smartcard Embedded Software in order to support the security provided by the TOE.

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

FDP_SDI.1	Stored data integrity monitoring
Hierarchical to:	No other components.
FDP_SDI.1.1	The TSF shall monitor user data stored within the TSC for *integrity errors after writing and before usage (and if necessary after processing)*[25] on all objects, based on the following attributes: *data are considered as being critical*[26].

[24] This objective could also work through the detection of such attacks and the initiation of corrective actions to counter such attempts.

[25] [assignment: integrity errors]

[26] [assignment: user data attributes]

Dependencies: No dependencies.

Refinement: The wording "and if necessary after processing" refers to situations where errors occurred during a calculation[27] (though the TOE provides FRU_FLT.2 and FPT_FLS.1). In this case it might be necessary that the Smartcard Embedded Software supports the overall security for instance by redundant calculations and verification after that.

Example 2: The Smartcard Embedded Software shall meet the requirement "Abstract machine testing (FPT_AMT.1)" as specified below.

FPT_AMT.1 Abstract machine testing

Hierarchical to: No other components.

FPT_AMT.1.1 The TSF shall run a suite of tests *at initial start-up or before use of the random number generator if being used by the Smartcard Embedded Software* [28] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

Dependencies: No dependencies.

9.3 Examples of Attack Scenarios

In this section background information is given to better understand the threats defined in section 3.3. The different types of influences on or interactions with the Smartcard were already visualised in Figure 2. The contents of this section shall not be considered as being complete nor as a comprehensive guidance for the evaluation.

A standard tool used for electrical measurement (and application of voltage and injection of current) is the needle probe workstation. Often appropriate contact areas must be prepared before using the methods described above (refer to the threat T.Phys-Manipulation). The actual measurement is done using standard tools such as voltmeters, oscilloscopes and signal analysers.

[27] for instance due to exposure to specific "radiation"

[28] [selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]]

In addition, there are indirect methods for measurements not requiring a direct (metallic) contact. Examples are voltage contrast imaging and electron probe microscopy. These methods are also referred to as physical probing since the Smartcard must be prepared before using the methods described above (refer to the threat T.Phys-Manipulation).

The interface for the attack is (the smartcard carrier and then) the surface of the integrated circuit.

The application of appropriate combinations of such methods in order to reveal information (via a non-standard interface) are addressed by the threat T.Phys-Probing.

Malfunctions of the TOE may cause some of its TSF to fail to be effective. Often more critical, security functions (or mechanisms) of the Smartcard Embedded Software may fail to be effective. This can be utilised by an attacker. The most straightforward way to cause malfunctions are irregular operating conditions in amplitude, shape, timing, occurrence etc. on the ISO interface (for instance such as glitches). Malfunctions can be due to errors or premature ageing.

The attacker stimulates the ISO interface (power supply, the external clock, reset and/or I/O). The attacker may also consider other types of influences on the Smartcard or directly onto the surface of the integrated circuit. In the latter case it might be required to manipulate the Smartcard (refer to the threat T.Phys-Manipulation). In addition, the attacker needs to observe the behaviour of the Smartcard and immediately take advantage of a possible malfunction. This requires to have additional equipment such as a terminal and communication software, but may include other things depending on the application to be attacked.

The application of appropriate combinations of such methods in order to manipulate the Smartcard Embedded Software (or the IC Dedicated Test Software) while being executed (via a standard interface) are addressed by the threat T.Malfunction.

Specific sorts of malfunctions are a means to reveal information about cryptographic keys or other critical data. Such methods are addressed by the threat T.Leak-Forced.

Standard tools used for the manipulation of circuitry are the Focused Ion Beam (FIB) and the laser cutter. The contents of programmable memories (such as E^{2}PROM) may be modified for instance by manipulation of circuitry, by exposing cells to charged particle beams, by using electromagnetic waves or by electrical probing (application of voltage and injection of current).

Manipulations require prior extensive reverse-engineering. The methods being applied are for instance optical inspection, voltage contrast imaging, image processing and pattern matching. In order to analyse circuitry the chip hardware must be removed from its carrier and then de-layered using appropriate methods (wet etching, plasma etching, grinding).

The interface for the attack is (the smartcard carrier and then) the surface of the integrated circuit.

The application of appropriate combinations of such methods in order to perform manipulations are addressed by the threat T.Phys-Manipulation.

When the Smartcard processes User Data and other critical data information about these data may be contained in signals which can be measured on the ISO contacts of the Smartcard using standard tools such as voltmeters, oscilloscopes and signal analysers. The Smartcard may also produce emanation which can be received using an antenna and analysed. For the analysis of the measured data specific tools (software) are required.

> The interface for the attack is the ISO interface (contacts of the Smartcard) but other interfaces may also be used.
> The application of appropriate combinations of such methods in order to reveal information (without affecting the TOE's operation or the TOE itself) are addressed by the threat T.Leak-Inherent. Public known attack scenarios are for instance the Simple Power Analysis (SPA) and the Differential Power Analysis (DPA).
> An attacker may also apply methods in order to cause the TOE to leak information. For instance the attacker must in addition cause faults. The interface for the attack can be more complex in this case. The ISO interface (contacts of the Smartcard), the Smartcard itself and/or the surface of the integrated circuit may be used to cause faults (refer to the threat T.Malfunction for more detail). Physical manipulations may also be done (refer to the threat T.Phys-Manipulation).
> The application of appropriate combinations of such methods in order to reveal information (by affecting the TOE's operation or manipulating the TOE itself) are addressed by the threat T.Leak-Forced not being related to attacks on cryptographic algorithms only. Public known attack scenarios are for instance the Differential Fault Analysis (DFA) and the Bellcore type of attacks.
> The evaluation of the TOE will in many cases not lead to final results for smartcard products built using the TOE. Tests must be repeated with the actual Smartcard Embedded Software.

Test Features (including other non-application related function) implemented in the TOE might be abused in order to disclose or manipulate User Data and bypass, deactivate, change or explore security features or functions of the TOE. Details depend on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

> If the IC Dedicated Test Software offers commands via the ISO I/O interface an attacker needs to communicate with the Smartcard using a terminal and the communication software. If other interfaces are used and/or if the usage of such commands is protected, it can be necessary to manipulate the TOE (refer to the threat T.Phys-Manipulation for more detail) and/or to circumvent authentication mechanisms. An attacker may also reveal information by physical probing (refer to the threat T.Phys-Probing) or analysing data (refer to the threats T.Leak-Inherent and T.Leak-Forced). If the TOE provides a command interface it can be subject to manipulations as described under the threat T.Malfunction and the software must not be susceptible to invalid inputs and other types of logical attacks being specific for software. Details depend on the way the Test Features are provided and protected by the TOE which is not specified here.
> The application of appropriate combinations of methods in order to reveal information or perform manipulations are addressed by the threat T.Abuse-Func.

9.4 Definition of the Family FCS_RND

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

FCS_RND Generation of random numbers

Family behaviour

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

Component levelling:

FCS_RND Generation of random numbers
1

FCS_RND.1 Generation of random numbers requires that random numbers meet a defined quality metric.

Management: FCS_RND.1

There are no management activities foreseen.

Audit: FCS_RND.1

There are no actions defined to be auditable.

FCS_RND.1 Quality metric for random numbers

Hierarchical to: No other components.

FCS_RND.1.1 The TSF shall provide a mechanism to generate random numbers that meet [assignment: a defined quality metric].

Dependencies: No dependencies.

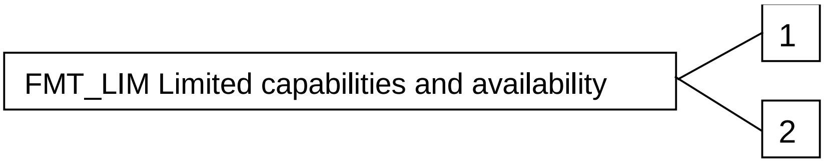
9.5 Definition of the Family FMT_LIM

To define the IT security functional requirements of the TOE an additional family (FMT_LIM) of the Class FMT (Security Management) is defined here. This family describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE (refer to Section 5.1.1) show that no other class is appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

The family “Limited capabilities and availability (FMT_LIM)” is specified as follows.

FMT_LIM Limited capabilities and availability
Family behaviour
This family defines requirements that limits the capabilities and availability of functions in a combined manner. Note that FDP_ACF restricts the access to functions whereas the Limited capability of this family requires the functions themselves to be designed in a specific manner.

Component levelling:



FMT_LIM.1 Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.

FMT_LIM.2 Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE’s life-cycle.

Management: FMT_LIM.1, FMT_LIM.2

There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2

There are no actions defined to be auditable.

The TOE Functional Requirement “Limited capabilities (FMT_LIM.1)” is specified as follows.

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 [assignment: Limited capability and availability policy].

Dependencies: FMT_LIM.2 Limited availability.

The TOE Functional Requirement “Limited availability (FMT_LIM.2)” is specified as follows.

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 [assignment: Limited capability and availability policy].

Dependencies: FMT_LIM.1 Limited capabilities.

Application note: The functional requirements FMT_LIM.1 and FMT_LIM.2 assume that there are two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the policy. This also allows that

(i) the TSF is provided without restrictions in the product in its user environment but its capabilities are so limited that the policy is enforced

or conversely

(ii) the TSF is designed with high functionality but is removed or disabled in the product in its user environment.

The combination of both requirements shall enforce the policy.

9.6 Definition of the Family FAU_SAS

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

The family “Audit data storage (FAU_SAS)” is specified as follows.

FAU_SAS Audit data storage
Family behaviour
This family defines functional requirements for the storage of audit data.
Component levelling

FAU_SAS Audit data storage
1

FAU_SAS.1 Requires the TOE to provide the possibility to store audit data.

Management: FAU_SAS.1

There are no management activities foreseen.

Audit: FAU_SAS.1

There are no actions defined to be auditable.

FAU_SAS.1	Audit storage
Hierarchical to:	No other components.
FAU_SAS.1.1	The TSF shall provide [assignment: authorised users] with the capability to store [assignment: list of audit information] in the audit records.
Dependencies:	No dependencies.

9.7 Glossary and Vocabulary

Administrator — (in the sense of the Common Criteria) The TOE may provide security functions which can or need to be administrated (i) by the Smartcard Embedded Software or
(ii) using services of the TOE after delivery to Phases 4-6. Then a privileged user (in the sense of the Common Criteria, refer to definition below) becomes an administrator.

Card Manufacturer — The customer of the TOE Manufacturer who receives the TOE during TOE Delivery. The Card Manufacturer includes all roles after TOE Delivery up to Phase 7 (refer to section 9.1.1).
The Card Manufacturer has the following roles (i) the Smartcard Product Manufacturer (Phase 5) and (ii) the Personaliser (Phase 6). If the TOE is delivered after Phase 3 in form of wafers or sawn wafers (dice) he has the role of the IC Packaging Manufacturer (Phase 4) in addition.

Integrated Circuit (IC) — Electronic component(s) designed to perform processing and/or memory functions.

IC Dedicated Software — IC proprietary software embedded in a smartcard IC (also known as IC firmware) and developed by the IC Developer. Such software is required for testing purpose (IC Dedicated Test Software) but may provide additional services to facilitate usage of the hardware and/or to provide additional services (IC Dedicated Support Software).

IC Dedicated Test Software — That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.

IC Dedicated Support Software — That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.

Initialisation Data
Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 3). These data are for instance used for traceability and for TOE identification (identification data).

Pre-personalisation Data
Any data supplied by the Card Manufacturer that is injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 3). These data are for instance used for traceability and/or to secure shipment between phases.

Smartcard
(as used in this Protection Profile) Composition of the TOE, the Smartcard Embedded Software, User Data and the package (the smartcard carrier).

Smartcard Embedded Software
Software embedded in a smartcard IC and not being developed by the IC Designer. The Smartcard Embedded Software is designed in Phase 1 and embedded into the Smartcard IC in Phase 3 or in later phases of the smartcard product life-cycle.
Some part of that software may actually implement a smartcard application others may provide standard services. Nevertheless, this distinction doesn’t matter here so that the Smartcard Embedded Software can be considered as being application dependent whereas the IC Dedicated Software is definitely not.

Test Features
All features and functions (implemented by the IC Dedicated Test Software and/or hardware) which are designed to be used before TOE Delivery only and delivered as part of the TOE.

TOE Delivery
The period when the TOE is delivered which is (refer to section 9.1.1) either (i) after Phase 3 (or before Phase 4) if the TOE is delivered in form of wafers or sawn wafers (dice) or (ii) after Phase 4 (or before Phase 5) if the TOE is delivered in form of modules.

TOE Manufacturer
The TOE Manufacturer must ensure that all requirements for the TOE and its development and production environment are fulfilled.
The TOE Manufacturer has the following roles: (i) IC Developer (Phase 2) and (ii) IC Manufacturer (Phase 3). If the TOE is delivered after Phase 4 in form of modules, he has the role of the (iii) IC Packaging Manufacturer (Phase 4) in addition.

TSF data
Data created by and for the TOE, that might affect the operation of the TOE [1] (for example configuration data). Note that the TOE is the Smartcard IC.

Initialisation Data defined by the Integrated Circuits manufacturer to identify the TOE and to keep track of the product's production and further life-cycle phases are also considered as belonging to the TSF data.

User — (in the sense of the Common Criteria) The TOE serves as a platform for the Smartcard Embedded Software. Therefore, the "user" of the TOE (as used in the Common Criteria assurance class AGD: guidance) is the Smartcard Embedded Software. Guidance is given for the Smartcard Embedded Software Developer.
On the other hand the Smartcard (with the TOE as a major element) is used in a terminal where communication is performed through the ISO interface provided by the TOE. Therefore, another "user" of the TOE is the terminal (with its software).

User Data — All data managed by the Smartcard Embedded Software in the application context. User data comprise all data in the final Smartcard IC except the TSF data.

9.8 List of Abbreviations

CC	Common Criteria Version 2.0 or Version 2.1. Note that the Version 2.1 (ISO 15408) is technically identical with Version 2.0 of the Common Criteria.
EAL	Evaluation Assurance Level.
IC	Integrated circuit.
IT	Information Technology.
NDA	Non Disclosure Agreement
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

9.9 Further Documents

[5] Data Encryption Standard (DES), FIBS PUB 46, US NBS, 1977, Washington,

[6] FIPS PUB 46-3 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION DATA ENCRYPTION STANDARD (DES) Reaffirmed 1999 October 25

[7] Smartcard Integrated Circuit Platform Augmentations, Version 0.81, December 6, 2000