# Security Target Lite
## BSI-DSZ-CC-0177

**Version 1.6**

**August 19th, 2002**

# Evaluation of the Philips P8WE5033V0F Secure 8-bit Smart Card Controller

**Developed and provided by**

**Philips Semiconductors, Business Unit Identification**

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

**by**

**Philips Semiconductors GmbH**
**Stresemannallee 101**
**22505 Hamburg**

## Document Information

### Document History

| *Version* | *Date* | *Changes* | *Remarks* |
|---|---|---|---|
| 1.6 | August 19th, 2002 | | ST-lite, derived from ST V1.5 |

Latest version is: Version 1.6 (August 19th, 2002)

### Document Invariants

| *Name* | *Value (to be edited)* | *Test Output (to copy)* |
|---|---|---|
| File name and length | Automatically | st-lite_5033V0F_v1_6.doc (308224 Byte) |
| Latest version | Version 1.6 | Version 1.6 |
| Date of this version | August 19th, 2002 | August 19th, 2002 |
| Classification | Security Document – Strictly Confidential | Security Document – Strictly Confidential |
| TOE name (long) | Philips P8WE5033V0F Secure 8-bit Smart Card Controller | Philips P8WE5033V0F Secure 8-bit Smart Card Controller |
| TOE name (short) | P8WE5033V0F | P8WE5033V0F |
| Developer (long) | Philips Semiconductors, Business Unit Identification | Philips Semiconductors, Business Unit Identification |
| Developer (short) | Philips | Philips |
| Sponsor (long) | Philips Semiconductors, Business Unit Identification | Philips Semiconductors, Business Unit Identification |
| Sponsor (short) | Philips | Philips |
| Certification ID | BSI-DSZ-CC-0177 | BSI-DSZ-CC-0177 |
| Evaluation facility | Prüfstelle IT-Sicherheit<br>T-Systems ISS GmbH | Prüfstelle IT-Sicherheit<br>T-Systems ISS GmbH |
| list of authors | Hans-Gerd Albertsen | Hans-Gerd Albertsen |
| certific. body (long) | Bundesamt für Sicherheit in der Informationstechnik | Bundesamt für Sicherheit in der Informationstechnik |
| certific. body (short) | BSI | BSI |

**Table of Contents**

1 ST Introduction 5
1.1 ST Identification 5
1.2 ST Overview 5
1.2.1 Introduction 5
1.2.2 Life-Cycle 6
1.2.3 Specific Issues of Smartcard Hardware and the Common Criteria 7
1.3 CC Conformance and Evaluation Assurance Level 7
2 TOE Description 8
2.1 TOE Definition 8
2.1.1 Hardware Description 9
2.1.2 Software Description 10
2.1.3 Documentation 10
2.1.4 Interface of the TOE 10
2.1.5 Life Cycle and Delivery of the TOE 11
2.1.6 TOE Intended Usage 11
2.1.7 TOE User Environment 12
2.1.8 General IT features of the TOE 13
2.2 Further Definitions and Explanations 13
3 TOE Security Environment 14
3.1 Description of Assets 14
3.2 Assumptions 14
3.3 Threats 15
3.4 Organisational Security Policies 15
4 Security Objectives 17
4.1 Security Objectives for the TOE 17
4.2 Security Objectives for the Environment 18
5 IT Security Requirements 20
5.1 TOE Security Requirements 20
5.1.1 TOE Security Functional Requirements 20

5.1.2 TOE Security Assurance Requirements 23
5.1.3 Refinements of the TOE Security Assurance Requirements 24
5.2 Security Requirements for the Environment 25
5.2.1 Security Requirements for the IT-Environment 26
5.2.2 Security Requirements for the Non-IT-Environment 26
6 TOE Summary Specification 28
6.1 TOE Security Functions 28
6.2 Assurance measures 30
7 PP Claims 33
8 Rationale 34
8.1 Security Objectives Rationale 34
8.2 Security Requirements Rationale 35
8.2.1 Rationale for the security functional requirements 35
8.2.2 Dependencies of security functional requirements 36
8.2.3 Rationale for the Assurance Requirements and the Strength of Function Level 37
8.2.4 Security Requirements are Mutually Supportive and Internally Consistent 37
8.3 TOE Summary Specification Rationale 37
8.3.1 Rationale for TOE security functions 37
8.3.2 Rationale for assurance measures 38
8.4 PP Claims Rationale 38
9 Annexes 40
9.1 Further Information contained in the PP 40
9.2 Glossary and Vocabulary 40
9.3 List of Abbreviations 42
9.4 Bibliography 43
9.4.1 Evaluation Documents 43
9.4.2 Developer Documents 44
9.4.3 Other Documents 44

# 1 ST Introduction

This chapter is divided into the following sections: “ST Identification”, “ST Overview” and “CC Conformance and Evaluation Assurance Level”.

## 1.1 ST Identification

This Security Target (st-lite_5033V0F_v1_6.doc, Version 1.6, August 19th, 2002) refers to the "Philips P8WE5033V0F Secure 8-bit Smart Card Controller" (TOE) provided by Philips Semiconductors, Business Unit Identification for a Common Criteria evaluation.

## 1.2 ST Overview

### 1.2.1 Introduction

The TOE is the hardware of the microcontroller chip P8WE5033V0F composed of a processing unit, security components, I/O ports, cryptographic co-processors and volatile and non-volatile memories produced by Philips. The P8WE5033V0F includes IC Dedicated Software for test purposes stored in the Test-ROM of the microcontroller. The TOE includes the documentation, 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 application software and the instruction set.

The security features of the P8WE5033V0F are mostly independent from the application software and support 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 non-volatile EEPROM makes the TOE ideal for applications requiring non-volatile data storage, including smart cards and portable data banks. Security functions protect data in the on-chip ROM, EEPROM 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 the memory of the TOE and
- maintain the integrity, the correct operation and the confidentiality of security functions (security mechanisms and associated functions) provided by the TOE.

This is ensured by the construction of the TOE and the 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 P8WE5033V0F Secure 8-bit Smart Card Controller" (TOE) mainly provides a hardware platform for a smart card with

- functions to calculate the Data Encryption Algorithm (Triple-DES) with two keys,
- support for large integer arithmetic (multiplication, addition and logical operations) with up to a length of 8192 bits,
- a random number generator and
- mode control regarding a test mode and an user mode.

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

### 1.2.2 Life-Cycle

Regarding the life cycle of the smartcard (refer to the “Smartcard IC Platform Protection Profile”, [5] section 8.1), 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.

Referring to the description in the PP [5], the TOE is delivered at the end of phase 3 in form of wafers as described in section 2.1. Regarding the Application Note 1 of [5] the TOE supports the authentic delivery using the Fabkey feature (see section 18.4 in the Data Sheet, P8WE5033 Secure 8-bit Smart Card Controller as well as section 2.4 in the Guidance, Delivery and Operation Manual of the P8WE5033V0F).

#### Security during Development and Production

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 patterns generated by Philips Semiconductors, Business Unit Identification. Different people are responsible for the design data and for customer related data. The security measures installed within Philips ensure a secure computer system and provide appropriate storage equipment for the different development tasks.

The verified layout data for the wafer fab is provided by the developer of the chip. The wafer fab provides the layout data of the different photomasks to the manufacturer of the photomasks. The photomasks are generated off-site and 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 includes 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. The computer tracking ensures the control of the complete process including the storage of the semi-finished wafers.

The test process of every die is performed by Philips. Delivery processes 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 customer.

### 1.2.3 Specific Issues of Smartcard Hardware and the Common Criteria

Regarding the Application Note 2 of [5] the TOE provides additional functionality which is not covered in the "Smartcard IC Platform Protection Profile". This additional functionality is added using the policy "P.Add-Func" (see section 3.4 of this Security Target).

## 1.3 CC Conformance and Evaluation Assurance Level

The evaluation is based upon

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 2.1, August 1999, [1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 2.1, August 1999, [2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 2.1, August 1999, [3]

For the evaluation the following methodology will be used:

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

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 conformant, EAL 5 augmented
- Conformance to the Protection Profile "Smartcard IC Platform Protection Profile", [5]

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.

Note: The "Smartcard IC Platform Protection Profile", [5] requires the assurance level EAL4 augmented. Regarding the Application Note 3 of [5] the changes which are needed for EAL5 are described in the different relevant sections of this Security Target.

# 2 TOE Description

This chapter is divided into the following sections: “TOE Definition” and “Further Definitions and Explanations”. TOE Definition has the sub-sections “Hardware Description”, “Software Description”, “Documentation”, “Interface of the TOE”, “Life Cycle and Delivery of the TOE”, “TOE Intended Usage”, “TOE User Environment” as well as “General IT features of the TOE”.

## 2.1 TOE Definition

The Target of Evaluation (TOE) is the smartcard integrated circuit depicted in figure 1 as block diagram. The TOE named P8WE5033V0F is manufactured in an advanced CMOS process. The TOE includes IC Designer/Manufacturer proprietary IC Dedicated Software in an 8kByte part of the ROM. 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.

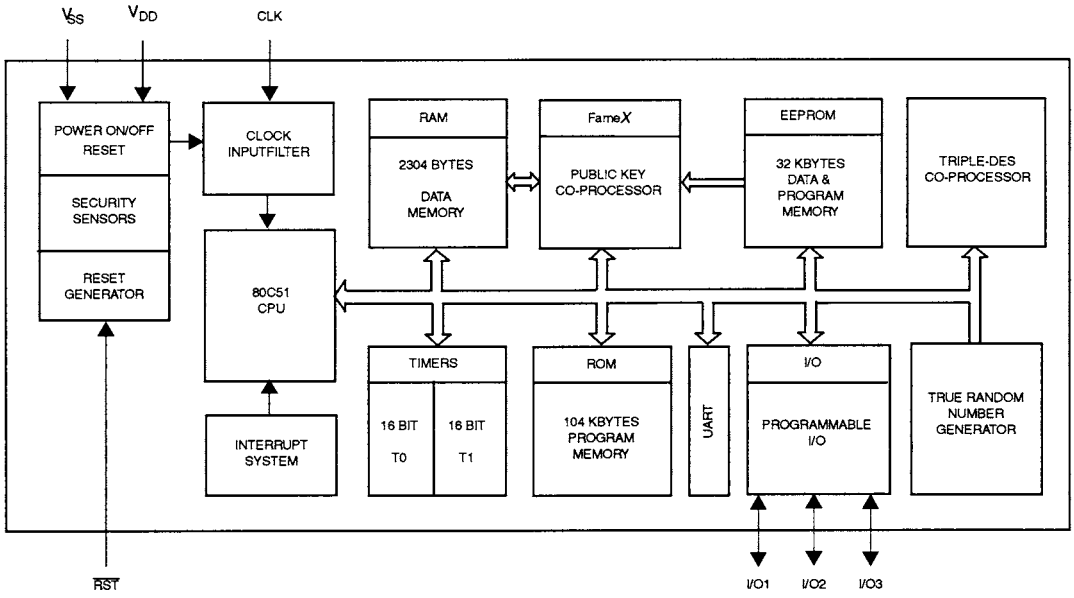


*Figure 1 Block Diagram of the P8WE5033V0F*

The device is developed for most high-end safeguarded applications, and is designed for embedding into chip cards according to ISO 7816 [12]. 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. 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.

The TOE is delivered in two different versions. The version P8WE5033V0G is an improved version of the P8WE5033V0F. This improvement releases a minor restriction to a software developer as stated in the user guidance manual for the P8WE5033V0F. Since both versions P8WE5033V0F as well as P8WE5033V0G comprise the same functionality and provide the same security features, both are addressed as "TOE" (Target of Evaluation) or named explicitly as "P8WE5033V0F".

The following table lists the TOE components.

| Type | Name | Release | Date | Form of delivery |
|---|---|---|---|---|
| Hardware | Philips P8WE5033V0F Secure 8-bit Smart Card Controller | V0F | 2001-10-16 (GDS2 File) | wafer (dice include reference C012F) |
| Software | Test ROM Software (the *IC dedicated software*) | yl038 | 2001-04-19 | Test ROM on the chip |
| Document | Guidance, Delivery and Operation Manual for V0F | | | printed document |
| Document | Data Sheet, P8WE5033 Secure 8-bit Smart Card Controller | 3.2 | 2002 July 05 | printed document |

*Table 1: Components of the TOE*

Note that the first character of the die reference for the P8WE5033V0F depends on the production site of the wafer.

### 2.1.1 Hardware Description

The CPU of the P8WE5033V0F is a derivative of the 80C51 family and has the same instruction set. The instruction set contains 255 different instructions, each instruction has a length of one byte which can be followed by parameters consisting of one or two additional bytes. The on-chip hardware is controlled by software via Special Function Registers. These registers are correlated to the activities of the CPU, Interrupt, I/O, EEPROM, Timers, UART and the two co-processors. The communication with the TOE can be performed through a serial interface I/O according to ISO standard 7816-3 [13]. Two 16-bit timers and six vectorized interrupts provide further functionality for I/O, timers, FameX and EEPROM.

The device includes ROM (96kByte User-ROM + 8kByte Test-ROM), RAM (2304 Byte) and EEPROM (32kByte) memory. The EEPROM can be accessed as data memory as well as program memory. The Triple-DES co-processor supports single DES and Triple-DES operations, but only Triple-DES will be used in this evaluation. The FameX co-processor supplies basic arithmetic functions to perform asymmetric crypto algorithms implemented by the Smartcard Embedded Software. The random number generator provides true random numbers without pseudo random calculation.

The P8WE5033V0F 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 controller provides two power saving modes with reduced activity: the IDLE Mode and the SLEEP Mode, which includes the CLOCK STOP Mode.

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.

### 2.1.2 Software Description

The smart card operating system and the application are developed by the customer and called Smartcard Embedded Software in the following. The Smartcard Embedded Software is stored in the User-ROM and/or in the EEPROM and is not a part of the TOE. The application software depends on the usage of the smartcard.

The code in the Test-ROM of the TOE is used by the TOE Manufacturer of the smart card to check the chip function. This IC Dedicated Software is disabled before the operational use of the smart card. The IC Dedicated Software (called firmware in the following) is developed by Philips and embedded in the Test-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 after phase 3.

### 2.1.3 Documentation

The Data Sheet [8] of the P8WE5033V0F 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 techniques 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 and I/O1.

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

- In the user mode 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 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.

### 2.1.5 Life Cycle and Delivery of the TOE

For the usage phase the P8WE5033V0F 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 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.

Regarding the Application Note 4 of [5] Philips will deliver the TOE at the end of phase 3 after the production test in form of wafers. Module production and embedding (card production) shall take place at the Card Manufacturer (see A.Process-Card).

Regarding the Application Note 5 of [5] Philips will deliver the TOE without IC Dedicated Support Software. The IC Dedicated Software stored in the Test-ROM is disabled before the TOE is delivered by Philips and cannot be used in the following 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.

### 2.1.6 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 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/she 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 parts: The IC manufacturer is responsible for the IC production itself. Regarding to 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 an 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.

### 2.1.7 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) Smartcard ICs 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 by the application software in the phases 4 to 7.

### 2.1.8 General IT features of the TOE

The TOE IT functionality consist of:

- tamper resistant data storage
- basic cryptographic functions (Triple-DES co-processor)
- basic arithmetic functions (FameX co-processor for the calculation of asymmetric crypto algorithms)
- physical random number generator
- data communication

## 2.2 Further Definitions and Explanations

Since the Security Target claims conformance to the PP “Smartcard IC Platform Protection Profile”, the concepts are used in the same sense. For the definition of terms refer to the Protection Profile [5]. This chapter does not need any supplement in the Security Target.

# 3 TOE Security Environment

This Security Target claims conformance to the Smartcard IC Platform Protection Profile. The Assets, Assumptions, Threats and Organisational Security Policies are completely taken from the Protection Profile. In the following only the extension of the different sections are listed. The titles of the chapters that are not extended are cited here for completeness.

## 3.1 Description of Assets

Since this Security Target claims conformance to the PP "Smartcard IC Platform Protection Profile", the assets defined in section 3.1 of the Protection Profile apply to this Security Target.

Regarding the Application Notes 6 and 7 of [5] there are no additional assets defined in this Security Target. The keys for the cryptographic co-processors are seen as User Data.

## 3.2 Assumptions

Since this Security Target claims conformance to the PP "Smartcard IC Platform Protection Profile", the assumptions defined in section 3.2 of the Protection Profile are valid for this Security Target. The following table lists the assumptions of the Protection Profile.

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

*Table 2: Assumptions defined in the Protection Profile*

Additionally, two more assumptions are defined considering the Application Notes 8 and 9 of [5] related to the specialised encryption hardware of the P8WE5033V0F.

The personaliser or the smartcard issuer together with the developer of the Smartcard Embedded Software must ensure the appropriate "Usage of Strong Keys (A.Strong-Key)" as specified below.

A.Strong-Key Usage of Strong Keys

The Smartcard Embedded Software shall use only appropriate secret keys (chosen from a large key space) as input for the cryptographic function of the TOE to ensure the strength of cryptographic operation.

The developer of the Smartcard Embedded Software must ensure the appropriate "Key-dependent Functions (A.Key-Fun)" as specified below.

A.Key-Fun Key-dependent Functions

When the Smartcard Embedded Software is just being executed no information about cryptographic keys can be gathered by analysing leakage of the Smartcard IC. The different types of leakage are described in the threat T.Leak-Inherent.

## 3.3 Threats

Since this Security Target claims conformance to the PP "Smartcard IC Platform Protection Profile", the threats defined in section 3.3 of the Protection Profile are valid for this Security Target. The following table lists the threats defined by the PP:

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

*Table 3: Threats defined by the Protection Profile*

Considering the Application Notes 10 and 11 of [5] there are no additional high-level security concerns or additional new threats defined in this Security Target.

## 3.4 Organisational Security Policies

Since this Security Target claims conformance to the PP "Smartcard IC Platform Protection Profile", the policy P.Process-TOE "Protection during TOE Development and Production" of the Protection Profile is applied here also.

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

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

P.Add-Func Additional Specific Security Functionality

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

- Triple DES encryption and decryption
- Basic support for large integer arithmetic (calculation of e.g. RSA)

Regarding the Application Note 12 of [5] there are no other additional policies defined in this Security Target.

# 4 Security Objectives

This chapter contains the following sections: Security Objectives for the TOE and Security Objectives for the Environment.

## 4.1 Security Objectives for the TOE

The TOE shall provide the following security objectives, taken from the Protection Profile Smartcard IC Platform Protection Profile:

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

*Table 4: Security objectives defined in the PP*

Regarding the Application Notes 13 and 14 of [5] the following additional security objectives are defined based on the cryptographic functionality provided by the TOE as specified below.

O.DES3 Triple DES Functionality

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

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

O.MOD_ARITH Basic support for modular arithmetic with large integer numbers

The TOE shall provide support for modular arithmetic (especially modular exponentiation) with large integer numbers to the Smartcard Embedded Software.

Note: Based on the principles of the co-processor, the confidentiality of the User Data (and especially cryptographic keys) during arithmetic operation must be ensured by the TOE together with suitable Smartcard

Embedded Software. The part provided by the TOE is supported by O.Leak-Inherent.

## 4.2 Security Objectives for the Environment

According to the Protection Profile, the following security objectives for the environment are specified:

| Security objective | Description | Applies to phase... |
|---|---|---|
| OE.Plat-Appl | Usage of Hardware Platform | Phase 1 |
| OE.Resp-Appl | Treatment of User Data | Phase 1 |
| OE.Process-TOE | Protection during TOE Development and Production | Phase 2 up to the TOE Delivery |
| OE.Process-Card | Protection during Packaging, Finishing and Personalisation | Starting with delivery by the TOE Manufacturer up to the end of phase 6 * |

*Table 5: Security objectives for the environment, taken from the PP*

Additionally, the Security Target defines three security objectives for the environment related to the specialised encryption hardware of the P8WE5033V0F (Triple-DES co-processor, FameX co-processor):

OE.Gen-Key Generation of Keys

If a key or a key pair is generated, this process must be performed in a confidential way and the keys generated must be unique with a very high probability and cryptographically strong. In addition, it must not be possible to derive the private key from a public key.

The objective is applicable to phase 1 when the Smartcard Embedded Software is developed because the internal key generation is under control of the Smartcard Embedded Software.

OE.Key-Fun Key-dependent Functions

Key-dependent functions shall be implemented in the Smartcard Embedded Software in a way that they are not susceptible to attacks where cryptographic keys are compromised for instance by analysing leakage of the Smartcard IC. The different types of leakage are described in the threat T.Leak-Inherent.

Note that here the routines which may compromise keys when being executed are part of the Smartcard Embedded Software. In contrast to this the threats T.Leak-Inherent and T.Leak-Forced address (see [5], section 3.3) the cryptographic routines being a part of the TOE.

The above objective is applicable to phases 4 to 7 when the Smartcard IC is under control of the application software.

OE.Strong-Key Usage of Strong Keys

The Smartcard Embedded Software will only use appropriate secret cryptographic keys (chosen from a sufficient key space and with sufficient entropy) as an input for the TOE's cryptographic function.

This objective is applicable to phases 4 to 7 when the Smartcard IC is under control of the application software. The objective must be supported by the Smartcard Embedded Software for the keys that are generated within the Smartcard IC as well as by the personaliser and the smartcard issuer since cryptographic keys can be loaded from the environment into the Smartcard IC.

# 5 IT Security Requirements

## 5.1 TOE Security Requirements

This section consists of the subsections "TOE Security Functional Requirements", "TOE Security Assurance Requirements" and "Refinements of the TOE Security Assurance Requirements".

### 5.1.1 TOE Security Functional Requirements

To support a better understanding of the combination Protection Profile vs. Security Target, the TOE SFRs are presented in the following two different sections.

#### 5.1.1.1 SFRs of the Protection Profile

Table 6 below shows all SFRs which are specified in the Protection Profile Smartcard IC Platform Protection Profile (in the order of definition in the PP). Some of the SFRs are CC Part 2 extended and defined in the Protection Profile. This is shown in the third column of the table.

| SFR | Title | Defined in ... |
|---|---|---|
| FRU_FLT.2 | Limited fault tolerance | CC, Part 2 |
| FPT_FLS.1 | Failure with preservation of secure state | CC, Part 2 |
| FPT_SEP.1 | TSF domain separation | CC, Part 2 |
| FMT_LIM.1 | Limited capabilities | PP, Section 8.5 |
| FMT_LIM.2 | Limited availability | PP, Section 8.5 |
| FAU_SAS.1 | Audit storage | PP, Section 8.6 |
| FPT_PHP.3 | Resistance to physical attack | CC, Part 2 |
| FDP_ITT.1 | Basic internal transfer protection | CC, Part 2 |
| FPT_ITT.1 | Basic internal TSF data transfer protection | CC, Part 2 |
| FDP_IFC.1 | Subset information flow control | CC, Part 2 |
| FCS_RND.1 | Quality metric for random numbers | PP, Section 8.4 |

*Table 6: SFRs taken from the PP*

With one exception, all assignment and selection operations are performed. The exception is the left open definition of a quality metric for the random numbers required by FCS_RND.1. This assignment operation is filled in by the following statement:

*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 an entropy of at least 7 bit in each byte* [1].

Dependencies: No dependencies.

*Note:* The entropy of the random number is measured by the Shannon-Entropy as follows:

$E = -\sum_{i=0}^{255} p_i \cdot \log_2 p_i$ , where $p_i$ is the probability that the byte $(b_7, b_6, \ldots, b_0)$ is equal to $i$ as binary number. Here term "bit" means measure of the Shannon-Entropy.

By this, all assignment/selection operations are performed. This Security Target does not perform any other/further operations than stated in the Protection Profile.

Regarding the Application Note 16 of [5] an additional generation of audit is not defined for "Limited fault tolerance" (FRU_FLT.2) and "Failure with preservation of secure state" (FPT_FLS.1).

Considering the Application Note 17 of [5] no additional requirement is defined for the TOE, since the Initialisation Data (refer to FAU_SAS.1) is protected by standard mechanisms of the TOE and will not be further processed by the TOE itself.

#### 5.1.1.2 Additional SFRs

Considering the Application Note 15 of [5] in the following paragraphs the additional cryptographic functions are defined. The CC operation *iteration* will be used with the component FCS_COP.1. To distinguish between the two, a label written in square brackets is attached to the component name. If anywhere it happens that the label is missing, the statement refers to both iterations of the component.

The following table lists the additional SFRs for cryptographic support which are taken from CC Part 2 and which are not defined in the Protection Profile.

[1] [assignment: a defined quality metric]

| SFR | Title | Defined in ... |
|---|---|---|
| FCS_COP.1[DES] | Cryptographic operation | CC, Part 2 |
| FCS_COP.1[Fame] | Cryptographic operation | CC, Part 2 |

*Table 7: Additional SFRs*

The (DES co-processor of the) TOE shall meet the requirement "Cryptographic operation (FCS_COP.1[DES])" as specified below.

*FCS_COP.1[DES] Cryptographic operation*

FCS_COP.1.1 The TSF shall perform *encryption and decryption* [2] in accordance with a specified cryptographic algorithm *Triple Data Encryption Algorithm (TDEA)* [3] and cryptographic key sizes *of 112 bit* [4] that meet the following *list of standards* [5]:

*FIPS PUB 46-3 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION DATA ENCRYPTION STANDARD (DES) Reaffirmed 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.

The (FameX co-processor of the) TOE shall meet the requirement "Cryptographic operation (FCS_COP.1[Fame])" as specified below.

*FCS_COP.1[Fame] Cryptographic operation*

FCS_COP.1.1 The TSF shall perform *operations to support raising to a power modulo an integer* [6] in accordance with a specified cryptographic algorithm *Rivest-Shamir-Adleman (RSA)* [7] and cryptographic key sizes *of at least 1024 bit* [8] that meet the following *list of standards* [9]:

*PKCS #1: RSA Cryptography Specifications, Version 2.0. RSA Laboratories, September 1998*

---

2 [assignment: list of cryptographic operations]

3 [assignment: cryptographic algorithm]

4 [assignment: cryptographic key sizes]

5 [assignment: list of standards]

6 [assignment: list of cryptographic operations]

7 [assignment: cryptographic algorithm]

8 [assignment: cryptographic key sizes]

9 [assignment: list of standards]

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.

Note that the mathematical function "exponentiation to a defined basis modulo an integer" may be used in different cryptographic algorithms, e.g. RSA, DSA, SHA-1 and elliptic curve. The padding algorithms are not performed by the function.

#### 5.1.1.3 SOF claim for TOE security functional requirements

Since the assurance level is augmented with AVA_VLA.4 the required level for the Strength of Function (SOF) of the above listed security functional requirements (refer to Table 6 and Table 7) is “SOF-high”. Note that the cryptographic algorithms are not assessed as part of the evaluation (refer to chapter 1 of [1]).

### 5.1.2 TOE Security Assurance Requirements

Table 8 below lists all security assurance components that are valid for this Security Target. These security assurance components are required by EAL5 (see section 1.3) or by the Protection Profile.

Considering the Application Note 18 of [5] the column “Required by” shows the differences in the requirements of security assurance components between the PP and the Security Target. The entry “EAL5 / PP” denotes that an SAR is required by both EAL5 and the requirement of the PP, “EAL5” means that this requirement is due to EAL5 and beyond the requirement of the PP, and “PP” identifies this component as a requirement of the PP which is beyond EAL5. The Security Target does not include additional augmentations. The refinements of the PP “Smartcard IC Platform Protection Profile” that must be adapted for EAL5 are described in section 5.1.3.

| *SAR* | *Title* | *Required by* |
|---|---|---|
| ACM_AUT.1 | Partial CM automation | EAL5 / PP |
| ACM_CAP.4 | Generation support and acceptance procedures | EAL5 / PP |
| ACM_SCP.3 | Development tools CM coverage | EAL5 |
| ADO_DEL.2 | Detection of modification | EAL5 / PP |
| ADO_IGS.1 | Installation, generation, and start-up procedures | EAL5 / PP |
| ADV_FSP.3 | Semiformal functional specification | EAL5 |
| ADV_HLD.3 | Semiformal high-level design | EAL5 |
| ADV_IMP.2 | Implementation of the TSF | EAL5 / PP |
| ADV_INT.1 | Modularity | EAL5 |
| ADV_LLD.1 | Descriptive low-level design | EAL5 / PP |
| ADV_RCR.2 | Semiformal correspondence demonstration | EAL5 |

| *SAR* | *Title* | *Required by* |
|---|---|---|
| ADV_SPM.3 | Formal TOE security policy model | EAL5 |
| AGD_ADM.1 | Administrator guidance | EAL5 / PP |
| AGD_USR.1 | User guidance | EAL5 / PP |
| ALC_DVS.2 | Sufficiency of security measures | PP |
| ALC_LCD.2 | Standardised life-cycle model | EAL5 |
| ALC_TAT.2 | Compliance with implementation standards | EAL5 |
| ATE_COV.2 | Analysis of coverage | EAL5 / PP |
| ATE_DPT.2 | Testing: low-level design | EAL5 |
| ATE_FUN.1 | Functional testing | EAL5 / PP |
| ATE_IND.2 | Independent testing – sample | EAL5 / PP |
| AVA_CCA.1 | Covert channel analysis | EAL5 |
| AVA_MSU.3 | Analysis and testing for insecure states | PP |
| AVA_SOF.1 | Strength of TOE security function evaluation | EAL5 |
| AVA_VLA.4 | Highly resistant | PP |

*Table 8: Security Assurance Requirements EAL5 and PP augmentations*

### 5.1.3 Refinements of the TOE Security Assurance Requirements

The ST claims conformance to the Protection Profile "Smartcard IC Platform Protection Profile", and therefore it has to be conform to the refinements of the TOE security assurance requirements (see Application Note 19 of the PP). Because the refinements in the PP are defined for the security assurance components of EAL4, some refinements have to be applied to assurance components of the higher level EAL5 stated in the Security Target.

Table 9 lists the influences of the refinements of the PP on the ST. Most of the refined security assurance components have the same level in both documents (Protection Profile and Security Target). Note that section 5.1.3.10 "Additional Guidance regarding Vulnerability Analysis (AVA_VLA) and Strength of Functions (AVA_SOF)" also applies to this Security Target and the two assurance components, although it is not a refinement. The following two subsections apply the refinements to ACM_SCP.3 and ADV_FSP.3 which are different between the PP and the ST.

| Refined in PP | Influence on ST |
|---|---|
| ACM_CAP.4 | Same as in ST, refinement valid without change |
| ACM_SCP.2 | ACM_SCP.3, refinements have to be applied |
| ADO_DEL.2 | Same as in ST, refinement valid without change |

| Refined in PP | Influence on ST |
|---|---|
| ADO_IGS.1 | Same as in ST, refinement valid without change |
| ADV_FSP.2 | ADV_FSP.3, refinements have to be applied |
| AGD_ADM.1 | Same as in ST, refinement valid without change |
| AGD_USR.1 | Same as in ST, refinement valid without change |
| ALC_DVS.2 | Same as in ST, refinement valid without change |
| ATE_COV.2 | Same as in ST, refinement valid without change |

*Table 9: Security Assurance Requirements, overview of differences of refinements*

#### 5.1.3.1 Refinements regarding CM scope (ACM_SCP)

This Security Target requires a higher evaluation level for the CC family ACM_SCP, namely ACM_SCP.3 instead of ACM_SCP.2. The refinement of the PP regarding ACM_SCP.2 is a clarification of the configuration item "TOE implementation representation". Since in ACM_SCP.3, the content and presentation of evidence element ACM_SCP.3.1C only adds a further configuration item to the list of items to be tracked by the CM system, the refinement can be applied without changes.

The refinement of the configuration item "TOE implementation representation" of ACM_SCP.2 can be found in section 5.1.3.3 of the Protection Profile [5] and is not cited here.

#### 5.1.3.2 Refinements regarding functional specification (ADV_FSP)

This Security Target requires a higher evaluation level for the CC family ADV_FSP, namely ADV_FSP.3 instead of ADV_FSP.2. The refinement of the PP regarding ADV_FSP.2 is concerned with the description of the TSF and its external interfaces, the purpose and method of use of all external TSF interfaces, the complete representation of the TSF and the accuracy and completeness of the TOE SFR instantiations. The refinement is not a change in the wording of the action elements, but a more detailed definition of the above items.

Since the higher level ADV_FSP.3 requires a Functional Specification in a "semiformal style, supported by informal, explanatory text where appropriate" (ADV_FSP.3.1C) the changes only affect the style of description, the refinements can be applied without changes and are valid for ADV_FSP.3.

The refinement of the original component ADV_FSP.2 can be found in section 5.1.3.5 of the Protection Profile [5] and is not cited here.

## 5.2 Security Requirements for the Environment

This chapter consists of the sections Security Requirements for the IT-Environment and Security Requirements for the Non-IT-Environment

### 5.2.1 Security Requirements for the IT-Environment

There are no Security Requirements for the IT-Environment defined in the PP "Smartcard IC Platform Protection Profile". This Security Target does not define Security Requirements for the IT-Environment, too.

### 5.2.2 Security Requirements for the Non-IT-Environment

Since this ST claims conformance to the PP "Smartcard IC Platform Protection Profile", the following security requirements for the Non-IT-Environment are taken from the PP:

- RE.Phase-1
- RE.Process-Card

The Security Target specifies the following additional security requirements for the Non-IT-Environment.

The Smartcard Embedded Software shall meet the requirements "Key-dependent Functions (RE.Key-Fun)" and "Usage of Strong Keys (RE.Strong-Key)" as specified below.

RE.Key-Fun Key-dependent Functions

The developers of Smartcard Embedded Software must not implement routines in a way which may compromise keys when the routines are executed as part of the Smartcard Embedded Software.

Performing functions which access cryptographic keys could allow an attacker to misuse these functions to gather information about the key which is used in the computation of the function.

RE.Strong-Key Usage of Strong Keys

The developers must design the Smartcard Embedded Software in a way that it will use only appropriate cryptographic keys as input of the TOE's cryptographic function as required in FCS_COP.1.

This may be ensured by generating cryptographic keys with the support of the random number generator provided by the TOE (see FCS_RND.1).

However there are other possibilities to work with strong keys, i. e. securely loading them from outside of the smart card, by derivation from Masterkeys or by other key exchange protocols. In this case the personaliser or the smartcard issuer must ensure that the Masterkeys meet the requirements for strong keys.

In addition this requirement implies that an appropriate key management has to be realised in the environment.

| | |
|---|---|
| RE.Gen-Key | Generation of Keys<br><br>The developer must ensure that keys or key pairs are treated confidential when they are generated by the Smartcard Embedded Software running on the TOE. The generation procedure must ensure that the keys are unique with a very high probability and cryptographically strong. In addition, it must be ensured that it is not possible to derive the private key from a public key. |

# 6 TOE Summary Specification

This chapter is divided in the sections TOE Security Functions and Assurance measures.

## 6.1 TOE Security Functions

The TOE Security Functions (TSF) 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 from 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).

The TOE provides random numbers according to the functionality class P2 as defined in [6] with a strength of function (consistently with other claims) SOF-high.

Note: The application software shall observe a minimum of 4800 internal clocks between reading two random numbers.

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 [10]. 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 bytes of the plain text and F.DEA calculates 8 bytes cipher text. The calculation output is read by the application software. For decryption the application software also provides 8 bytes of cipher text and F.DEA calculates 8 bytes plain text. The calculation output 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.

F.FAME: The TOE provides basic support for large integer modular arithmetic. The arithmetic functions can be used to accelerate asymmetric crypto algorithms, e.g.

RSA. The Smartcard Embedded Software must select the appropriate functions of the co-processor and provide the operands for the arithmetic functions.

Note that the TOE does not calculate e.g. the RSA algorithm itself in a single operation. In fact, it provides functions for modular multiplication, modular addition and bit operations, and is therefore not limited to RSA. The functions can be used by the application software, maybe in form of a special crypto library. This software is not part of the evaluation.

The TSF provides specific implementation features to reduce leakage of confidential user and TSF data. These features must be supplemented by measures of the Smartcard Embedded Software, since F.FAME only provides support for modular arithmetic and not for a single/specific algorithm.

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.

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 software disables the sensors.

Beside these sensors the security function comprises an additional sensor to check the high voltage for the write process to the EEPROM during every write sequence. The result of this sensor must be read from a Special Function Register and does not force an automatic event (e.g. reset).

F.PHY: The function F.PHY protects the TOE against manipulation of (i) the hardware, (ii) the IC Dedicated Test Software in the ROM, (iii) the Smartcard Embedded Software in the ROM and the EEPROM, (iv) the application data in the EEPROM and RAM, (v) the configuration data in the security row and (vi) the mode-switch. It also protects secret user data against disclosure when stored in EEPROM and RAM or while being processed by the TOE.

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.

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 TSF F.COMP has two aspects:

- Access control: In the Test Mode the TOE (i) allows to execute the IC Dedicated Test Software and (ii) prevents to execute the Smartcard

Embedded Software. In the User Mode the TOE (i) allows to execute the Smartcard Embedded Software and (ii) prevents to execute the IC Dedicated Test Software.

- Mode switch: The initial TOE mode is the Test Mode. The TOE allows to change the mode-switch only one time from the Test Mode into 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 enforces 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.

### SOF claim

According to the CEM [4] 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 leakage attacks 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 section 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(s) containing or referring the relevant information* | *Input evidence according to CC Part 3, which is contained or referred to in the document(s)* | *Input for assurance families (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 |
| Correspondence Demonstration, Design Report | low level design | ADV_LLD |
| | architectural description | ADV_INT |
| | correspondence analysis between high-level design and low-level design | ADV_RCR |
| | correspondence analysis between low-level design and implementation representation | ADV_RCR |
| Implementation representation, Source Code | implementation representation | ADV_IMP |
| Quality Management Manual and Security Management Manual | configuration management documentation | ACM |
| | development tools documentation | ALC |
| | development security documentation | |
| | life cycle definition documentation | |
| | parts of the delivery documentation | ADO |

| *Document(s) containing or referring the relevant information* | *Input evidence according to CC Part 3, which is contained or referred to in the document(s)* | *Input for assurance families (according to developer actions in CC Part 3)* |
|---|---|---|
| Guidance, Delivery and Operation Manual, Data Sheet | administrator guidance | AGD_ADM, AVA_MSU |
| | secure installation, generation, and start-up procedures | ADO_IGS |
| | 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 10: List of documents describing the measures regarding the assurance requirements*

# 7 PP Claims

This Security Target claims conformance to the following Protection Profile:

Smartcard IC Platform Protection Profile, Version 1.0, July 2001; registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0002-2001, [5]

The short term for this Protection Profile used in this document is “Smartcard IC Platform Protection Profile”.

# 8 Rationale

This chapter contains the following sections: Security Objectives Rationale, Security Requirements Rationale, TOE Summary Specification Rationale and PP Claims Rationale.

## 8.1 Security Objectives Rationale

Section 7.1 of the Protection Profile provides a rationale of the security objectives that are subject of the PP "Smartcard IC Platform Protection Profile". Table 1 in section 7.1 of [5] lists the objectives.

The justification provided in the Protection Profile is completely valid for this Security Target. The additional security objective are in line with the security objectives of the Protection Profile and supplement these according to the additional functionality.

| Assumption/Policy | Security Objective | Note |
|---|---|---|
| P.Add-Func | O.DES3<br>O.MOD_ARITH | |
| A.Strong-Key | OE.Gen-Key<br>OE.Strong-Key | (Phase 1) or (Phases 4 to 6) |
| A.Key-Fun | OE.Key-Fun | (Phase 1) |

*Table 11: Additional Security Objectives versus Assumptions or Policies*

The justification related to the policy "Additional Specific Security Functionality (P.Add-Func)" is as follows:

Since the objectives O.DES3 and O.MOD_ARITH defines the functionality required by P.Add-Func, this policy is covered by the two objectives.

The justification related to the assumption "Usage of Strong Keys (A.Strong-Key)" is as follows:

OE.Gen-Key requires the software developer to implement the functions for the generation of keys in a way that they ensure the confidentiality and strongness of the key. In addition OE.Strong-Key requires the software developer to use only appropriate keys as input for the cryptographic functions. OE.Strong-Key shall be applied for keys generated using external equipment and loaded from outside into the Smartcard IC as well as for keys generated by the TOE inside the Smartcard IC. Therefore the assumption is covered by the objectives.

The justification related to the assumption "Key-dependent Functions (A.Key-Fun)" is as follows:

Since OE.Key-Fun requires the developer of the Smartcard Embedded Software to implement functions which perform operations on keys in such a manner that they do not disclose information on the key when being executed, the assumption is covered by the objective.

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

## 8.2 Security Requirements Rationale

### 8.2.1 Rationale for the security functional requirements

Section 7.2 of the PP "Smartcard IC Platform Protection Profile" provides a rationale for the security functional requirements defined in this Protection Profile.

The Security Target additionally defines two SFRs for the TOE and three Security Requirements for the Environment. The following table gives an overview, how the requirements are combined to meet the security objectives.

| Objective | TOE Security Functional Requirement | Security Requirements for the environment |
|---|---|---|
| O.DES3 | FCS_COP.1[DES] | |
| O.MOD_ARITH | FCS_COP.1[Fame] | |
| OE.Key-Fun | | RE.Key-Fun |
| OE.Strong-Key | | RE.Strong-Key |
| OE.Gen-Key | | RE.Gen-Key |

*Table 12: Mapping of Security Objectives and Requirements*

The justification related to the security objective "Triple DES Functionality" (O.DES3) is as follows:

O.DES3 requires the TOE to support Triple DES encryption and decryption. Exactly this is the requirement of FCS_COP.1[DES]. Therefore FCS_COP.1[DES] is suitable to meet O.DES3.

The justification related to the security objective "Basic support for modular arithmetic with large integer numbers" (O.MOD_ARITH) is as follows:

O.MOD_ARITH requires the TOE to support the calculation of asymmetric cryptographic functions providing modular arithmetic operations. Exactly this is the requirement of FCS_COP.1[Fame]. Therefore FCS_COP.1[Fame] is suitable to meet O.MOD_ARITH.

The justification related to the security objective "Generation of Keys" (OE.Gen-Key) is as follows:

The requirements for the generation of keys that are defined for the developer by RE.Gen-Key are suitable for to meet the objective OE.Gen-Key.

The justification related to the security objective “Key-dependent Functions” (OE.Key-Fun) is as follows:

RE.Key-Fun requires the Smartcard Embedded Software developer to design and implement the software in a way, which is suitable to meet OE.Key-Fun.

The justification related to the security objective “Usage of Strong Keys” (OE.Strong-Key) is as follows:

RE.Strong-Key addresses the usage of keys generated inside the Smartcard IC as well as keys downloaded into the Smartcard IC. The requirement for the usage of appropriate cryptographic keys for the cryptographic functions is suitable to meet OE.Strong-Key.

### 8.2.2 Dependencies of security functional requirements

The following discussion demonstrates how the dependencies defined by Part 2 of the Common Criteria for the requirement FCS_COP.1 (both iterations) are satisfied.

The dependencies defined in the Common Criteria are

- [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.

The dependency requirements completely address the appropriate management of cryptographic keys used by the specified cryptographic function. All requirements concerning key management shall be fulfilled by the environment (Smartcard Embedded Software in this case) according to the requirements RE.Resp-Appl and RE.Strong-Key.

It was decided not to include the functional requirements [FDP_ITC.1 or FCS_CKM.1], FCS_CKM.4 and FMT_MSA.2 explicitly as security functional requirements for the environment because this would mean a restriction for the realisation of the Smartcard Embedded Software that is not justifiable. The possibility was seen that special smart card applications may be designed that are able to resolve the dependencies without use of all the explicit functional requirements (for example by moving some of the functional responsibilities to organisational measures outside of the smart card). So the more abstract requirements RE.Resp-Appl, RE.Strong-Key and RE.Gen-Key were chosen to give the developers of the Smartcard Embedded Software the freedom to choose how to fulfil them.

The same argument holds for further indirect dependencies of FCS_COP.1.1 according to [2] (FDP_ACC.1, FDP_IFC.1, FDP_ACF.1, FDP_IFF.1, FMT_MSA.3, FCS_CKM.2, FMT_MSA.1, FMT_SMR.1, FIA_UID.1 and ADV_SPM.1).

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

The selection of assurance components is based on the underlying Protection Profile [5]. The Security Target uses the same augmentations as the PP, but chooses a higher assurance level. The level EAL5 is chosen in order to meet assurance expectations of digital signature applications and electronic payment systems. Additionally, the requirement of the PP to choose at least EAL4 is fulfilled.

The rationale for the augmentations is the same as in the PP. The assurance level EAL5 is an elaborated pre-defined level of the CC, part 3 [3]. 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.

As stated in the Protection Profile, section 7.2.3, 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 by the PP 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.

Note that for the augmentation to EAL5 the document “ Smartcard Integrated Circuit Platform Augmentations” as supposed by Application Note 21 was not considered because at the time of writing the document has not reached a final state.

### 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

### 8.3.1 Rationale for TOE security functions

Note: The rational is present here in a tabular form. The remainder of this chapter (8.3.1) was not intended to be published.

| | F.RNG | F.DEA | F.FAME | F.OPC | F.PHY | F.COMP |
|---|---|---|---|---|---|---|
| FCS_RND.1 | X | | | | X | |
| FCS_COP.1[DES] | | X | | | X | |
| FCS_COP.1[Fame] | | | X | | X | |
| FDP_ITT.1 | | X | X | | X | |
| FPT_ITT.1 | | X | X | | X | |
| FDP_IFC.1 | | X | X | | X | |
| FPT_PHP.3 | | | | | X | |
| FRU_FLT.2 | | | | X | X | |
| FPT_FLS.1 | | | | X | X | |
| FPT_SEP.1 | | | | X | X | X |
| FMT_LIM.1 | | | | | X | X |
| FMT_LIM.2 | | | | | X | X |
| FAU_SAS.1 | | | | | X | X |

*Table 13: Mapping of Security Functional Requirements and the TOE Security Functions*

The "X" means that the TOE Security Function realises or supports the functionality required by the respective Security Functional Requirement.

### 8.3.2 Rationale for assurance measures

Note: This chapter (8.3.2) was not intended to be published.

## 8.4 PP Claims Rationale

According to chapter 7 this Security Target claims conformance to the Protection Profile “Smartcard IC Platform Protection Profile, Version 1.0, July 2001; registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0002-2001” [5].

The sections of this document where threats, objectives and security requirements are defined, clearly state which of these items are taken from the Protection Profile and which are added in this ST. Therefore this is not repeated here. Moreover all additional stated items in this ST do not contradict to the items included from the PP (see the respective sections in this document). The operations done for the SFRs taken from the PP are also clearly indicated.

The assurance level claimed for this target (EAL5+) is shown in section 5.1.2 to include resp. exceed the requirements claimed by the PP (EAL4+).

These considerations show that the Security Target correctly claims conformance to the Smartcard IC Platform Protection Profile.

# 9 Annexes

## 9.1 Further Information contained in the PP

The Annex of the Protection Profile ([5], chapter 9) provides further information. Section 8.1 of the PP describes the development and production process of smartcards, containing a detailed life-cycle description and a description of the assets of the Integrated Circuits Designer/Manufacturer. Section 8.2 is concerned with security aspects of the Smartcard Embedded Software (further information regarding A.Resp-Appl and examples of specific Functional Requirements for the Smartcard Embedded Software). Section 8.3 gives examples of Attack Scenarios.

## 9.2 Glossary and Vocabulary

Note: To ease understanding of the used terms the Glossary of the Protection Profile [5] is reproduced here. Readers familiar with the Protection Profile may skip this subsection.

| | |
|---|---|
| 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 [5], Figure 4 on page 17 and Section 8.1.1).<br><br>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 the Protection Profile [5]) 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.<br><br>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 [5], Figure 4 on page 17) 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 (as defined in Section 2.1) and its development and production environment are fulfilled (refer to [5], Figure 4 on page 17).<br><br>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 (for example configuration data). Note that the TOE is the Smartcard IC.<br><br>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.<br><br>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. |

## 9.3 List of Abbreviations

DEA Data Encryption Algorithm.

| | |
|---|---|
| DES | Data Encryption Standard. |
| 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. |
| SAR | Security Assurance Requirement. |
| SFR | Security Functional Requirement. |
| SF | Security function. |
| SIM | Subscriber Identity Module. |
| 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. |
| UART | Universal Asynchronous Receiver and Transmitter. |

## 9.4 Bibliography

### 9.4.1 Evaluation Documents

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

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

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

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

[5] Smartcard IC Platform Protection Profile, Version 1.0, July 2001; registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0002-2001

[6] Anwendungshinweise und Interpretationen zum Schema, AIS31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 1, 25.09.2001, Bundesamt für Sicherheit in der Informationstechnik

### 9.4.2 Developer Documents

[7] Security Target for the P8WE5033V0F, BSI-DSZ-CC-0177, Version 1.5, Philips Semiconductors, 19.08.2002

[8] Data Sheet, P8WE5033 Secure 8-bit Smart Card Controller, Product Specification, Philips Semiconductors, Revision 3.2, Document Number: 047632, 2002 July 05

[9] Guidance, Delivery and Operation Manual of the P8WE5033V0F, Secure 8-bit Smart Card Controller

### 9.4.3 Other Documents

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

[11] PKCS #1: RSA Cryptography Specifications, Version 2.0. RSA Laboratories, September 1998

[12] ISO/IEC 7816-2:1996 Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 2: Dimensions and location of contacts

[13] ISO/IEC 7816-3:1997 Information technology – Identification cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocols