NXP Secure Smart Card Controller MF3F60x1 with IC Dedicated Support Software

Security Target Lite

Rev. 1.6 — 4 February 2010	Evaluation Documentation
BSI-DSZ-CC-0587	PUBLIC

Document information

Info	Content
Keywords	Security Target Lite, MF3F60x1 with IC Ded. Supp. SW, MF3F60
Abstract	Evaluation of the NXP Secure Smart Card Controller MF3F60x1 with IC Dedicated Support Software developed and provided by NXP Semiconductors according to the Common Criteria for Information Technology Evaluation (CC) at Level EAL4 augmented

Revision history			
Rev	**Date**	**Description**	**Remarks**
1.6	4-February 2010	Derived from full Security Target MF3F60x1	

Latest version is: Rev. 1.6 (4 February 2010)

Contact information

For additional information, please visit: http://www.nxp.com

For sales office addresses, please send an email to: salesaddresses@nxp.com

1. ST Introduction

This chapter is divided into the following sections: “ST Reference”, “TOE Reference”, “TOE Overview” and “TOE Description”.

1.1 ST Reference

NXP Secure Smart Card Controller MF3F60x1 with IC Dedicated Support Software Security Target Lite, Rev. 1.6, NXP Semiconductors, 4 February 2010.

1.2 TOE Reference

NXP Secure Smart Card Controller MF3F60x1 with IC Dedicated Support Software

1.3 TOE Overview

1.3.1 Usage and Major Security Features of the TOE

The TOE comprises the microcontroller chip MF3F60x1 (named hardware platform in the following) and IC Dedicated Test Software as well as IC Dedicated Support Software. The IC Dedicated Test Software is used for test purposes (referred to as Test Operating System, active only during wafer test). The IC Dedicated Test Software is stored in the Test-ROM. The IC Dedicated Support Software dissolves into:

- a Boot ROM Software executed during each starting up and used to initialize and configuring the TOE which is also stored in the Test-ROM,
- a software library called “Hardware Abstraction Library” (further referred to as HAL) which is delivered as binary Library and linked to the customer operating system and,
- a software library called “Low Level Library” (further referred to as LLL) which is also delivered as binary Library and linked to the customer operating system.

The hardware platform comprises an 8-bit central processing unit, volatile and non-volatile memories accessible via a memory control unit, a cryptographic co-processor, security components and a contactless communication interface.

The TOE also includes a Guidance Document which contains guide lines on how to securely use the microcontroller chip and the IC Dedicated Support Software by the Security IC Embedded Software.

The security measures of the MF3F60x1 with IC Ded. Supp. SW are designed to act as an integral part of the complete security system in order to strengthen the TOE as a whole. A number of security measures are completely implemented in and controlled by hardware. Further security measures are implemented in the hardware and require configuration or control by the IC Dedicated Support Software.

The non-volatile EEPROM can be used as data memory only. It contains high reliability cells which guarantee data integrity. This is ideal for applications requiring non-volatile data storage. Security features protect data in the on-chip ROM, EEPROM and RAM.

Hence the TOE maintains

- the integrity and the confidentiality of code and data stored in the memories of it,
- the different TOE modes with the related capabilities for configuration and memory access and
- the integrity, the correct operation and the confidentiality of security services (security features and associated functionality) provided by the TOE.

The security services are ensured by the construction of the TOE and the security features it provides. The "NXP Secure Smart Card Controller MF3F60x1 with IC Dedicated Support Software" (TOE) is a security IC with IC Dedicated Support Software mainly providing:

- functions to calculate the Data Encryption Standard (Triple-DES) with two keys,
- a random number generator,
- access control to memories and hardware resources,
- cyclic redundancy check calculation (CRC),
- a contact-less interface supporting ISO/IEC 18092 [12].

In addition several security features independently implemented in hardware or controlled by the IC Dedicated Software will be provided to ensure proper operation as well as integrity and confidentiality of stored data. This includes memory encryption and sensors to allow operation only under specified operating conditions.

1.3.2 TOE Type

The Target of Evaluation (TOE) is the NXP Secure Smart Card Controller MF3F60x1 with IC Dedicated Support Software. The TOE includes the hardware platform, IC Dedicated Test Software, IC Dedicated Support Software (partly as library) and the User Guidance.

The TOE is delivered

- as MOA4 modules, or
- laser diced wafers, on film frame carrier.

1.3.3 Required Non-TOE Hardware/Software/Firmware

None

1.4 TOE Description

1.4.1 Physical Scope of TOE

The Target of Evaluation (TOE) comprises the hardware platform depicted in Fig 1 as block diagram. The hardware platform named MF3F60x1 is manufactured in an advanced CMOS process. The TOE includes IC Dedicated Test Software and IC Dedicated Support Software. The IC Dedicated Support Software comprises the Boot ROM Software as part of the hardware platform and the HAL and LLL as precompiled binary libraries. All other software is called Security IC Embedded Software and is not part of the TOE.

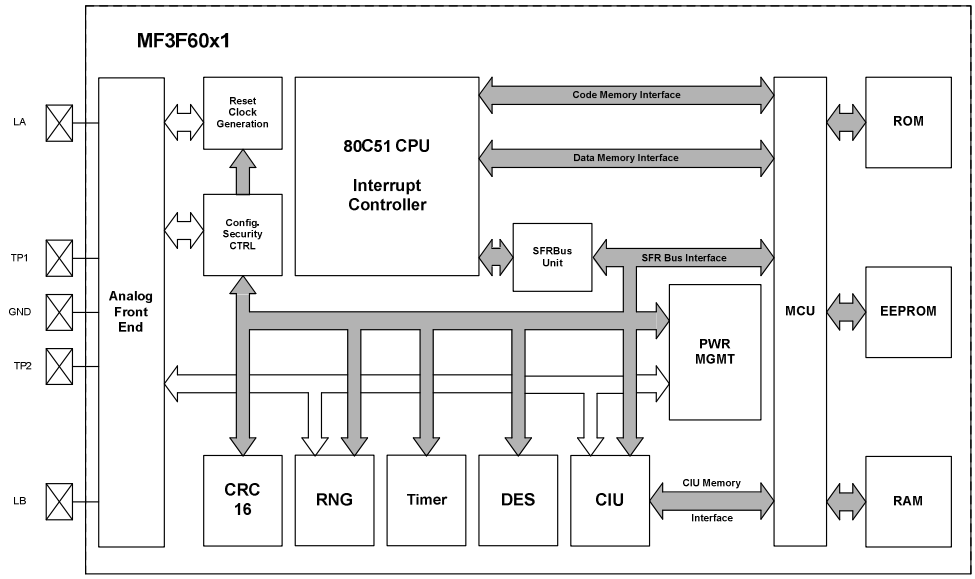

Fig 1. Block Diagram of the MF3F60x1 with IC Ded. Supp. SW

The following table lists the TOE components.

TOE Components

Table 1. Components of the TOE

Type	Name	Release	Date	Form of delivery
Hardware	MF3F60x1	V0A	t506A.gds2 18.3.2009	Wafer, modules and package (dice include reference t506A)
Software	Test ROM Software (the *IC Dedicated Test Software*)	V1.1	23.6.2009	Test ROM on chip (MF3F60_TestOS.hex)
Software	Boot ROM Software (part of the *IC Dedicated Support Software*)	V1.1	23.6.2009	Test ROM on chip (MF3F60_TestOS.hex)
Library	Hardware Abstraction Library (part of the *IC Dedicated Support Software*)	V1.1	6.9.2009	Software Library (libphHalWyv.lib)
Library	Low Level Library (part of the *IC Dedicated Support Software*)	V1.1	6.9.2009	Software Library (WyvernLLL.lib)
Document	MF3F60x1, Secured contactless smartcard controller, Objective data sheet [8]			Electronic document
Document	MF3F60x1, Guidance, Delivery and Operation Manual [9]			Electronic document

1.4.1.1 Hardware Configuration

The hardware platform contains the following blocks:

- **80C51** compatible **CPU** core plus **7** source interrupt controller
- Memory comprises **64 kB ROM**, **1.25 kB RAM** and **6 kB EEPROM**
- Reset sequencer and system clock generation
- Power management unit
- Configuration and security control
- 16 bit general purpose **CRC**
- 16 bit general purpose timer
- 2 Key triple **DES** crypto processor
- **ISO/IEC 18092** interface unit (passive target for **212**/**424 kBps**)
- True random number generator

The MF3F60x1 with IC Ded. Supp. SW does not have any major configuration options.

1.4.1.2 IC Dedicated Support Software

The IC Dedicated Support Software comprises three parts. The Boot ROM Software is part of the Test-ROM. The Hardware Abstraction Library and the Low Level Library are delivered in the form of two precompiled binary libraries and two C header files containing all type definitions and function prototypes. These must be linked to the Security IC Embedded Software during the software generation process.

The Hardware Abstraction Library (HAL) provides a set of types and functions which can be dissolved into the following groups:

- Initialization, self testing and sanity check
- Cryptographic functions
- CRC calculation functions
- NVM control functions
- Communication control functions
- Random number generation functions

The Low Level Library (LLL) provides speed improved versions of the ANSI C functions

- Memcpy
- Memset

Furthermore it provides a speed and security improved version of the ANSI C function

- Memcmp

at the cost of giving up the ANSI C compliance for the return values.

Note that the IC Dedicated Test Software is not listed here because it is disabled before TOE delivery and does not provide security functionality during the usage phase.

1.4.1.3 Evaluated Chip and Package Types

Different package types are supported for the TOE. Each package type has a different commercial type name. The commercial type name for the TOE has the following format:

- MF3F60*x*1*tpp*/*vvrrff*

The commercial type name is composed by the notation MF3F60 which identifies the product family and the chip type plus other characters which are described in Table 2.

Table 2. Variable Definitions for Commercial Type Names

Variable	Definition
x1	Factory, the silicon is being produced (*x*=0: product produced in SSMC).
t	Operating temperature range (*t*=E: -25 < $t_{operating}$ < +85°C).
pp	Package type (*pp*=UG: 150µm lacer diced; *pp*=UD: 120µm lacer diced; *pp*=A4: MOA4 module on reel).
vv	HW-version (*vv*=0A: HW-Version 0Ah).
rr	SW-version (*rr*=01: SW-Version 01h)
ff	Customer specified personalization option, NVM content only (*ff*=01: personalization option 01h; *ff*=02: personalization option 02h).

Since *x, t, vv* and *rr* only provide 1 option the format is restricted to:

- MF3F6001E*pp*/0A01*ff*

For example, the commercial type name MF3F6001EA4/0A0101 denotes an MF3F60x1 in a MOA4 package, manufactured in SSMC, with HW-version 0Ah, SW-version 01h and personalization option 01h.

The package type does not influence the security functionality of the TOE.

The following package types are supported in this Security Target.

Table 3. Supported package types

Type	*x*1	*t*	*pp*	*vv*	*rr*	*ff*	Description
MF3F60	01	E	UG	0A	01	01	8 inch wafer (laser diced; 150 µm thickness, on film frame carrier; electronic fail die marking according to SECSII format), 6K EEPROM, HW version: 0Ah; ROM version: 01h; Personalization option 01h
MF3F60	01	E	UG	0A	01	02	8 inch wafer (laser diced; 150 µm thickness, on film frame carrier; electronic fail die marking according to SECSII format), 6K EEPROM, HW version: 0Ah; ROM version: 01h; Personalization option 02h

Type	*x*1	*t*	*pp*	*vv*	*rr*	*ff*	Description
MF3F60	01	E	A4	0A	01	01	plastic leadless module carrier package; 35 mm wide tape, 6K EEPROM, HW version: 0Ah; ROM version: 01h; Personalization option 01h
MF3F60	01	E	A4	0A	01	02	plastic leadless module carrier package; 35 mm wide tape, 6K EEPROM, HW version: 0Ah; ROM version: 01h; Personalization option 02h
MF3F60	01	E	UD	0A	01	01	8 inch wafer (laser diced; 120 µm thickness, on film frame carrier; electronic fail die marking according to SECSII format), 6K EEPROM, HW version: 0Ah; ROM version: 01h; Personalization option 01h
MF3F60	01	E	UD	0A	01	02	8 inch wafer (laser diced; 120 µm thickness, on film frame carrier; electronic fail die marking according to SECSII format), 6K EEPROM, HW version: 0Ah; ROM version: 01h; Personalization option 02h

For all package types listed above, the security during development, production and assembly is ensured (refer to section 1.4.3).

As already described above, the complete resulting commercial type name is dependent on the Security IC Embedded Software (customer software). In consequence this means that a full commercial product name that fits in the variable forms described in Table 3 determines that the hardware is an evaluated product, however this gives no conclusion on the software and if the software does use the proper hardware configuration as described in subsection 1.4.2.1.

1.4.2 Logical Scope of TOE

1.4.2.1 Hardware Description

The CPU of the MF3F60x1 with IC Ded. Supp. SW has an 8-bit architecture with an instruction set that is based on the 8051 family instruction set. It distinguishes between two different TOE modes:

- **System Mode**
- **User Mode**

The System Mode is the hardware default mode when the device is powered. It has extended access rights to memories and configurations. It is not available for the Security IC Embedded Software developer. The System Mode is reserved for the execution of the Boot ROM Software. The Security IC Embedded Software as well as the HAL are executed in User Mode (refer to the beginning of section 1.4.1).

The Security IC Embedded Software is always executed in User Mode. The User Mode provides only limited access to the SFR and the memories and is not allowed to alter the memory configuration (sizes and access rights). The only option to access security functionality in the User Mode is via the Hardware Abstraction Library (HAL).

The TOE comprises a life cycle related status coding in order to determine the TOE mode selection at the end of the boot sequence. After TOE delivery the status coding enforces a TOE mode change from System Mode to User Mode at the end of each boot sequence.

The Triple-DES co-processor supports single DES and Triple-DES operations. Only Triple-DES in 2-key operation will be considered in this evaluation.

The TOE´s random number generator provides true random numbers without pseudo random calculation.

1.4.2.2 Software Description

The customers will receive a library they have to use for executing any security relevant operation of the TOE (like 3-DES, random number generator, clock configuration, etc). The customers have to include this hardware abstraction library in their software which is stored in the User-ROM.

The smart card operating system and the application are developed by the customers and are called Security IC Embedded Software in the following. The Security IC Embedded Software is stored in the User-ROM and is not part of the TOE.

The IC Dedicated Test Software (Test ROM Software) in the Test-ROM of the TOE is used by the TOE Manufacturer of the smart card to test the functionality of the hardware platform. The test functionality is disabled before the operational use of the Security IC by switching fuses of the hardware platform which prevent that the Boot ROM Software starts the IC Dedicated Test Software. The IC Dedicated Test Software is developed by NXP and embedded in the Test-ROM. The IC Dedicated Test Software includes the test operating system, test routines for the various blocks of the hardware platform, control flags for the configuration of the hardware platform and security features to ensure that test operations cannot be executed illegally after phase 3.

The IC Dedicated Support Software comprises two parts:

- The Boot ROM Software is executed after each reset of the TOE, i.e. every time when the TOE starts. It sets up the TOE and does some basic configuration of the hardware. This software is stored in the Test-ROM and
- The libraries consisting of two parts that are linked to the IC Embedded Software and stored in the User-ROM. This software is delivered as binary library:
  - The Hardware Abstraction Library as described above. Note that the HAL is a software library that has to be linked to the Security IC Embedded Software.
  - The Low Level Library as described above. Note that the LLL is a software library that has to be linked to the Security IC Embedded Software.

1.4.2.3 Documentation

The HAL interface specification describes all functions accessible through the hardware abstraction library and is documented chapter 9 of the MF3F60x1, Secured contactless smartcard controller, Objective data sheet, [8]. The MF3F60x1, Guidance, Delivery and Operation Manual, [9] describes the HAL as well as the Low Level Library (LLL) procedures and their proper usage. The provided documentation is part of the TOE and shall be used by the software developer to develop the Security IC Embedded Software.

1.4.3 Security during Development and Production

Regarding the life cycle of the TOE (refer to the “Security IC Platform Protection Profile”, [6] section 7.1), the development and the production phase of the IC with its dedicated software is part of the evaluation.

Referring to the description in the PP, the TOE is delivered at the end of phase 3 or of phase 4 (cf. section 1.2.4 in [6]).

Regarding the Application Note 3 of [6] the TOE supports the authentic delivery using the FabKey feature (refer to Section 4 in [9]).

During the design and the layout process only people involved in the specific development project for the dedicated hardware platform and IC Dedicated Software have access to the source code and other sensitive data. Different people are responsible for the design data and for customer related data. The security measures installed within NXP ensure a secure computer system and provide appropriate equipment for the different development tasks.

The verified layout data is provided by the developers of NXP Semiconductors, Business Line Identification, MST AFC directly to the wafer fab. The wafer fab generates and forwards the layout data related to the different photo masks to the manufacturer of the photo masks. The photo masks are generated off-site and verified against the design data of the development before the usage. Accountability and traceability are ensured among the wafer fab and the photo mask 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 mask set independent of the customer. After that step the wafers are completed by merging the Boot ROM Software and Test ROM Software with the customer specific mask which together forms the final ROM mask to be processed. Afterwards the remaining fixed masks are processed. 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 a test centre of NXP. Delivery processes between the involved sites provide accountability and traceability of the produced wafers. NXP embeds the dice into smart card modules or other packages based on customer demand. Information about non-functional dice is stored on magnetic/optical media enclosed with the delivery or the non-functional items are physically marked.

The Hardware Abstraction Library (HAL) and the Low Level Library (LLL) which are part of the IC Dedicated Support Software are developed by NXP and sent to the customer in the form of precomiled libraries which the customer has to link to the Security IC Embedded Software. Traceability of the library versions and the environment under which the precompiled libraries have been generated, are guaranteed by NXP´s version management system. The libraries are delivered to the customer via a secure channel. The authenticity of the binary files is guaranteed by generating a hash value over the data which is communicated separately to the customer. These procedures are documented in the User Guidance Manual, [9]. It is at the responsibility of the customer to check whether the hash values match.

1.4.4 TOE Intended Usage

The final product as a combination of the hardware platform and the compiled Security IC Embedded Software comprising the Hardware Abstraction Library, the Low Level Library, and the operating system and application are used by the end-user (phase 7). The method of use of the product in this phase depends on the application. The TOE is intended to be used in an insecure environment that does not protect against threats.

The device is developed for most high-end safeguarded applications, and is designed for embedding into contact-less smart cards according to ISO 18092, [12]. Usually the smart card is assigned to a single individual only although the smart card may be expected to be used for multiple applications. So the TOE must meet security requirements to be applied to security modules. Secret data stored on the smart card shall be used as input for the calculation of authentication data, the calculation of signatures and the encryption of data and keys.

The TOE user environment is the environment from TOE Delivery to phase 7. At the phases up to 6, the TOE user environment must be a controlled environment.

In the end-user environment (phase 7) Security ICs are used in a wide range of applications to assure authorized 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.

Note 1. The life cycle phases after TOE Delivery (phase 3 or 4) up to phase 7 of the Security IC Product life cycle are not part of the TOE construction process in the sense of this Security Target. Information about those phases is only included to describe how the TOE is used after its construction. Nevertheless the security features of the hardware platform that are independent of the Security IC Embedded Software are active at TOE Delivery and cannot be disabled in the phases afterwards.

Note 2. The Security IC Embedded Software has to use the HAL and LLL for security functionality provided by the hardware platform.

1.4.5 Interface of the TOE

The electrical interfaces of the TOE are the pads (called LA and LB) for the antenna of the contactless interface unit. There are additional test pads which are exclusively accessible during the production testing before the delivery.

The software interface (including access to the special function registers as well as to the memories) of the TOE depends on the TOE mode:

- Upon every start-up the Boot ROM Software is executed in System Mode. This software initializes and configures the TOE. This comprises the selection of IC Dedicated Test Software (before TOE delivery) and of Security IC Embedded Software (after TOE delivery). The software does not provide any interface. The Boot ROM Software is stored in the Test-ROM.
- Before TOE delivery the logical interface is defined by the IC Dedicated Test Software. This IC Dedicated Test Software is executed in System Mode and comprises the test operating system used for production testing. IC Dedicated Test Software is stored in the Test-ROM.
- After TOE Delivery the logical interface is defined by the Security IC Embedded Software. The Security IC Embedded Software is executed in User Mode. The Security IC Embedded Software is stored in the User-ROM.

Note 3. Note that the logical interface provided by the TOE for the Security IC Embedded Software is the set of instructions defined in the HAL, the configurable bits in the Special Function Registers in User Mode, the address

map of the CPU including memories and the instruction set of the CPU. This interface of the hardware platform is not an external interface of a composite product including the TOE.

The chip surface can be seen as an interface of the TOE, too. This interface is taken into account regarding environmental stress e.g. like temperature and in the case of an attack where the attacker tries to manipulate the chip surface or the chip.

Note 4. An external energy and timing supply as well as a data interface are necessary for the operation of the TOE. Beyond the physical behavior the interface is defined by the application environment.

2. Conformance Claims

This chapter is divided into the following sections: “CC Conformance Claim", "Package Claim", "PP Claim", and "Conformance Claim Rationale”.

2.1 CC Conformance Claim

This Security Target claims to be conformant to the Common Criteria version 3.1:

- Common Criteria for Information Technology Security Evaluation, Part 1 - Introduction and general model - Version 3.1 CCMB-2006-09-001, Revision 1, September 2006, [1]
- Common Criteria for Information Technology Security Evaluation, Part 2 - Security functional requirements, Version 3.1 CCMB-2007-09-002, Revision 2, September 2007, [2]
- Common Criteria for Information Technology Security Evaluation, Part 3 - Security Assurance Requirements, Version 3.1 CCMB-2007-09-003, Revision 2, September 2007, [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 3.1 CCMB-2007-09-004, Revision 2, September 2007, [4]

This Security Target claims to be CC Part 2 extended and CC Part 3 conformant. The extended Security Functional Requirements are defined in chapter 5.

2.2 Package Claim

Furthermore, this Security Target claims conformance to the assurance package **EAL 4 augmented**. The augmentations to EAL4 are ALC_DVS.2, ASE_TSS.2 and AVA_VAN.5. The augmentations ALC_DVS.2 and AVA_VAN.5 are taken from the Protection Profile.

2.3 PP Claim

This Security Target claims conformance to the Protection Profile “Security IC Platform Protection Profile”, [6].

Since the Security Target claims conformance to the PP “Security IC Platform Protection Profile”, the concepts are used in the same sense. For the definition of terms refer to the Protection Profile [6]. This chapter does not need any supplement in the Security Target.

Regarding the Application Note 4 of [6] the TOE provides additional functionality which is not covered in the “Security IC Platform Protection Profile”. This additional functionality is added using the policy “P.Add-Components” (see section 3.3 of this Security Target).

2.4 Conformance Claim Rationale

According to section 2.3 this Security Target claims conformance to the Protection Profile “Security IC Platform Protection Profile, registered and certified by Bundesamt fuer Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0035, Rev 1.0, 15 June 2007” [6].

The TOE type defined in section 1.3.2 of this Security Target is a smart card controller with IC Dedicated Support Software. This is consistent with the TOE definition for a Security IC in section 1.2.2 of [6].

The sections within this document where security problem definitions, 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 the content of the Protection Profile is not repeated in this Security Target. Moreover, all additionally stated items in this Security Target do not contradict 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 evaluation assurance level claimed for this TOE is shown in section 6.2 to include respectively exceed the requirements claimed by the PP (EAL4+).

These considerations show that the Security Target correctly claims conformance to the “Security IC Platform Protection Profile”, [6].

3. Security Problem Definition

This Security Target claims conformance to the “Security IC Platform Protection Profile”, [6]. The Assets, Threats, Assumptions, and Organizational Security Policies are taken from the Protection Profile. In the following only the extensions of the different sections are detailed. The elements of the Security Problem Definition that are not extended in the Security Target. They are cited here for completeness.

This chapter is divided into the following sections: “Description of Assets", "Threats", "Organizational Security Policies", and "Assumptions".

3.1 Description of Assets

Since this Security Target claims conformance to the PP “Security IC Platform Protection Profile”, [6], the assets defined in section 3.1 of the Protection Profile are applied and cited here completely:

The assets related to standard functionality are:

- The User Data
- The Security IC Embedded Software, stored and in operation
- The security services provided by the TOE for the Security IC Embedded Software

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

- Logical design data, physical design data, IC Dedicated Software, the hardware abstraction library, the low level library and configuration data
- Initialization Data and Pre-personalization Data, specific development aids, test and characterization related data, material for software development support, and photo masks.

Note that the keys for the cryptographic co-processors are seen as User Data.

3.2 Threats

Since this Security Target claims conformance to the PP “Security IC Platform Protection Profile”, [6], the threats defined in section 3.2 of the Protection Profile are valid for this Security Target. The following table lists the threats defined by the PP:

Table 4. Threats defined by the Protection Profile

Name	Title
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

Name	Title
T.Abuse-Func	Abuse of Functionality
T.RND	Deficiency of Random Numbers

Considering the Application Note 5 of [6] there are no additional threats defined in this Security Target.

3.3 Organizational Security Policies

Since this Security Target claims conformance to the PP “Security IC Platform Protection Profile” [6], the policy P.Process-TOE “Protection during TOE Development and Production” of the Protection Profile is applied here also.

Regarding the Application Note 6 of [6] there is one additional policy defined in this Security Target as detailed in the following:

The TOE provides specific security functionality which can be used by the Security IC 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 smart card application, against which threats the Security IC Embedded Software will use the specific security functionality.

The IC Developer / Manufacturer therefore applies the policy “Additional Specific Security Components (P.Add-Components)” as specified below.

P.Add-Components — Additional Specific Security Components

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

- Triple DES encryption and decryption
- Area based Memory Access Control
- Special Function Register Access Control.

3.4 Assumptions

Since this Security Target claims conformance to the PP “Security IC Platform Protection Profile” [6], the assumptions defined in section 3.4 of the Protection Profile are valid for this Security Target. The following table lists the assumptions of the Protection Profile.

Table 5. Assumptions defined in the Protection Profile

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

The following additional assumptions are added in this Security Target according to the Application Notes 7 and 8 of [6].

The developer of the Security IC Embedded Software must support the “Identification of the TOE” after delivery in phase 3 or phase 4 by the developer.

A.Check-Init	Check of initialization data by the Security IC Embedded Software The Security IC Embedded Software must provide a function to check initialization data. The data is defined by the customer and injected by the TOE Manufacturer into the non-volatile memory to provide the possibility for TOE identification and for traceability.

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

A.Key-Function	Usage of Key-dependent Functions Key-dependent functions (if any) shall be implemented in the Security IC Embedded Software in a way that they are not susceptible to leakage attacks (as described under T.Leak-Inherent and T.Leak-Forced). Note that here the routines which may compromise keys when being executed are part of the Security IC Embedded Software. In contrast to this the threats T.Leak-Inherent and T.Leak-Forced address (i) the cryptographic routines which are part of the TOE and (ii) the processing of User Data including cryptographic keys.

4. Security Objectives

This chapter contains the following sections: "Security Objectives for the TOE", "Security Objectives for the Security IC Embedded Software development Environment" "Security Objectives for the Operational Environment", and "Security Objectives Rationale".

4.1 Security Objectives for the TOE

The TOE shall provide the following security objectives, taken from the Protection Profile “Security IC Platform Protection Profile”, [6]:

Table 6. Security objectives defined in the PP

Name	Title
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

Regarding the Application Notes 9 and 10 of [6] the following additional security objectives are defined based on additional functionality provided by the TOE as specified below.

O.HW_DES3 Triple DES Functionality

The TOE shall provide the cryptographic functionality to calculate a Triple DES encryption and decryption in standard or CBC mode. The TOE supports directly the calculation of Triple DES with two keys.

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.

O.MEM_ACCESS Area based Memory Access Control

The TOE shall provide separation between (a) the Test-ROM and (b) the User-ROM. The separation shall comprise software execution and data access.

O.SFR_ACCESS Special Function Register Access Control

The TOE shall provide access control to the Special Function Registers. The access control restricts access to hardware components of the TOE based on the TOE mode.

4.2 Security Objectives for the Security IC Embedded Software development Environment

In addition to the security objectives for the operational environment as required by CC Part 1 [1] the Protection Profile [6] defines security objectives for the Security IC Embedded Software development environment which are listed below.

Table 7. Security objectives for the Security IC Embedded Software development environment, taken from the PP

Security objective	Description	Applies to phase...
OE.Plat-Appl	Usage of Hardware Platform	Phase 1
OE.Resp-Appl	Treatment of User Data	Phase 1

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

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

If the random number generator is used for leakage countermeasures, cryptographic operations (e.g. key generation) or cryptographic protocols (e.g. challenge response) these random numbers must be tested appropriately.

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

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

This means that keys are treated as confidential as soon as they are generated. The keys must be unique with a very high probability, as well as cryptographically strong. If keys are imported into the TOE and/or derived from other keys, quality and confidentiality must be maintained. This implies that appropriate key management has to be realized in the environment.

4.3 Security Objectives for the Operational Environment

According to the Protection Profile [6] the following security objective for the operational environment is specified:

Table 8. Security objectives for the operational environment, taken from the PP

Security objective	Description	Applies to phase...

Security objective	Description	Applies to phase...
OE.Process-Sec-IC	Protection during composite product manufacturing	TOE delivery up to the end of phase 6

Check of initialization data

The TOE provides specific functionality that requires the TOE Manufacturer to implement measures for the unique identification of the TOE. Therefore, OE.Check-Init is defined to allow a TOE specific implementation (refer also to A.Check-Init).

OE.Check-Init — Check of initialization data by the Security IC Embedded Software

To ensure the receipt of the correct TOE, the Security IC Embedded Software shall check a sufficient part of the pre-personalization data. This shall include at least the FabKey Data that is agreed between the customer and the TOE Manufacturer.

4.4 Security Objectives Rationale

Section 4.4 of the Protection Profile provides a rationale how the assumptions, threats, and organizational security policies are addressed by the objectives that are specified in the PP “Security IC Platform Protection Profile”, [6]. The following Table 9 reproduces the table in section 4.4 of [6].

Table 9. Security Objectives versus Assumptions, Threats or Policies

Assumption, Threat or OSP	Security Objective	Notes
A.Plat-Appl	OE.Plat-Appl	Phase 1
A.Resp-Appl	OE.Resp-Appl	Phase 1
P.Process-TOE	O.Identification	Phase 2 – 3
A.Process-Sec--IC	OE.Process-Sec-IC	Phase 4 – 6
T.Leak-Inherent	O.Leak-Inherent	
T.Phys-Probing	O.Phys-Probing	
T.Malfunction	O.Malfunction	
T.Phys-Manipulation	O.Phys-Manipulation	
T.Leak-Forced	O.Leak-Forced	
T.Abuse-Func	O.Abuse-Func	
T.RND	O.RND	

The following Table 10 provides the justification for the additional security objectives. They are in line with the security objectives of the Protection Profile and supplement these according to the additional assumptions and organizational security policy.

Table 10. Additional Security Objectives versus Assumptions or Policies

Assumption/Policy	Security Objective	Note
P.Add-Components	O.HW_DES3 O.MEM_ACCESS O.SFR_ACCESS	
A.Key-Function	OE.Plat-Appl OE.Resp-Appl	Phase 1
A.Check-Init	OE.Check-Init	Phase 1 and Phase 4 - 6

The justification related to the policy “Additional Specific Security Components (P.Add-Components)” is as follows:

The justification related to the security objectives O.HW_DES3, O.MEM_ACCESS and O.SFR_ACCESS is as follows: Since these objectives require the TOE to implement exactly the same specific security functionality as required by P.Add-Components, the organizational security policy is covered by the objectives.

Nevertheless the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced define how to implement the specific security functionality required by P.Add-Components. These security objectives are also valid for the additional specific security functionality since they must avert the related threats also for the components added related to the policy.

The justification related to the assumption A.Key-Function is as follows:

- Compared to [6] a clarification has been made for the security objective “Usage of Hardware Platform (OE.Plat-Appl)”: If required, the Security IC Embedded Software shall use the cryptographic service of the TOE and its interface as specified. In addition, the Security IC Embedded Software (i) must implement operations on keys (if any) in such a manner that they do not disclose information about confidential data and (ii) must ensure that different applications (if any) are sufficiently separated. This addition ensures that the assumption A.Key-Function is still covered by the objective OE.Plat-Appl although additional functions are being supported according to P.Add-Components.
- Compared to [6] a clarification has been made for the security objective “Treatment of User Data (OE.Resp-Appl)”: By definition cipher or plain text data and cryptographic keys are User Data. So, the Security IC Embedded Software will protect such data if required and use keys and functions appropriately in order to ensure the strength of cryptographic operation. Quality and confidentiality must be maintained for keys that are imported and/or derived from other keys. This implies that appropriate key management has to be implemented in the environment. These measures make sure that the assumption A.Key-Function is still covered by the security objective OE.Resp-Appl although additional functions are being supported according to P.Add-Components.

The justification related to the assumption "Check of initialization data by the Security IC Embedded Software (A.Check-Init)" is as follows:

Since OE.Check-Init requires the Security IC Embedded Software developer to implement a function assumed in A.Check-Init, 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.

5. Extended Components Definition

This Security Target does not define extended components.

Note that the PP “Security IC Platform Protection Profile”, [6] defines extended security functional requirements in chapter 5, which are included in this Security Target.

6. Security Requirements

This section consists of the subsections “Security Functional Requirements”, “Security Assurance Requirements” and “Security Requirements Rationale”.

6.1 Security Functional Requirements

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

6.1.1 SFRs of the Protection Profile

Table 11 below shows all SFRs which are specified in the Protection Profile “Security IC Platform Protection Profile”, [6] (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.

Table 11. SFRs taken from the PP

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
FMT_LIM.1	Limited capabilities	PP, Section 5.2
FMT_LIM.2	Limited availability	PP, Section 5.2
FAU_SAS.1	Audit storage	PP, Section 5.3
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_RNG.1	Random number generation	PP, Section 5.1

All assignment and selection operations of the SFR listed in the table above are performed except the operations completed below:

For the SFR FAU_SAS.1 the PP [6] leaves the assignment operation open for the non-volatile memory type in which initialization data, pre-personalization data and/or other supplements for the Security IC Embedded Software are stored. This assignment operation is filled in by the following statement. Note that the assignment operations for the list of subjects and the list of audit information have already been filled in by the PP [6].

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_SAS.1.1	The TSF shall provide *the test process before TOE Delivery* [1] with the capability to store *the Initialization Data and/or Pre-personalization Data* [2] in the *EEPROM* [3].

For FCS_RNG.1.1 the PP [6] partially fills in the assignment for the security capabilities of the RNG by requiring a total failure test of the random source and adds an assignment operation for additional security capabilities of the RNG.

In addition, for FCS_RNG.1.2 the PP [6] partially fills in the assignment operation for the defined quality metric for the random numbers by replacing it by a selection and assignment operation.

For the above operations the original operations defined in chapter 5 of the PP [6] have been replaced by the open operations in the statement of the security requirements in chapter 6 of [6] for better readability. Note that the selection operation for the RNG type has already been filled in by the PP.

FCS_RNG.1	Random number generation
Hierarchical to:	No other components.
	FCS_RNG.1.1The TSF shall provide a *physical*[4] random number generator that implements *total failure test of the random source and an online test when random numbers are requested by the Security IC Embedded Software*[5].
FCS_RNG.1.2	The TSF shall provide random numbers that meet *independent bits with Shannon entropy of 7.976 bits per octet*[6].
Dependencies:	No dependencies.
Note:	Application Note 20 in [6] requires that the Security Target specifies for the security capabilities in FCS_RNG.1.1 how the results of the total failure test of the random source are provided to the Security IC Embedded Software. When the random number generator is called via the HAL a hardware test is included. The results of the internal test sequence are provided to the Security IC Embedded Software as a pass or fail criterion by means of a return value.

1 [assignment: *list of subjects*]

2 [assignment: *list of audit information*]

3 [assignment: *type of persistent memory*]

4 [selection: *physical, non-physical true, deterministic, hybrid*]

5 [assignment: *list of additional security capabilities*]

6 [selection: *independent bits with Shannon entropy of 7.976 bits per octet, Min-entropy of 7.95 bit per octet, [assignment: other comparable quality metric]*]

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.

The value "7.976" is assigned due to the requirements of "AIS31", [5].

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

Considering the Application Note 12 of [6] in the following subsection the additional functions for cryptographic support and access control are defined. These SFRs are not required in the Protection Profile.

As required by the Application Note 14 of [6] the secure state is described in section 7.2.1 in the rationale for SF.OPC.

Regarding the Application Note 15 of [6] 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).

As required by the Application Note 18 of [6] the automatic response of the TOE is described in section 7.2.1 in the rationale for SF.PHY.

6.1.2 Additional SFRs regarding cryptographic functionality

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

FCS_COP.1	**Cryptographic operation**
Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform *encryption and decryption*[7] in accordance with a specified cryptographic algorithm *Triple Data Encryption Algorithm (TDEA) in standard or CBC mode* [8] and a cryptographic key size *of 112 bits*[9] that meet the following *standard*[10]: *FIPS PUB 46-3 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION DATA ENCRYPTION STANDARD (DES) Reaffirmed 1999 October 25, keying option 2.*

[7] [assignment: list of cryptographic operations]

[8] [assignment: cryptographic algorithm]

[9] [assignment: cryptographic key sizes]

[10] [assignment: list of standards]

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

6.1.3 Additional SFRs regarding access control

Access Control Policy

The hardware shall provide different TOE modes to the IC Dedicated Software and the Security IC Embedded Software. The TOE shall separate IC Dedicated Software and Security IC Embedded Software from each other by partitioning of memory. The selection between IC Dedicated Software and Security IC Embedded Software as well as the configuration of the hardware shall be performed in respective dedicated TOE modes.

The Security Function Policy (SFP) **Access Control Policy** uses the following definitions:

The subjects are

- The **Security IC Embedded Software** i.e. data in the memories of the TOE executed as instructions by the CPU. Note that the HAL and LLL (which are part of IC Dedicated Support Software) are executed in the same context as the Security IC Embedded Software because they are libraries linked to the Security IC Embedded Software.
- The "**Test ROM Software**" as IC Dedicated Test Software
- The "**Boot ROM Software**" as part of the IC Dedicated Support Software

The objects are

- the **memories** consisting of
  - ROM which is partitioned into Test-ROM and User-ROM,
  - EEPROM which is partitioned into the Security Row with FabKey Area and the remaining User-EEPROM,
  - RAM which is not partitioned.
- the **Special Function Registers** consisting of
  - Special Function Registers to configure the TOE. These Special Function Registers allow configuring the behavior of the hardware platform.
  - Special Function Registers related to testing. These Special Function Registers are reserved for testing purposes.
  - Special Function Registers related to hardware components and general CPU functionality. The Special Function Registers related to hardware components are used to utilize hardware components like the co-processors or the interrupt system. The Special Function Registers related to general CPU functionality comprise e.g. the accumulator, stack pointer and data pointers.

The memory operations are

- **read** data from the memory,
- **write** data into the memory and

- **execute** data in the memory.

Note that execution of data in the EEPROM memory is possible only in System Mode. The TOE guarantees that execution of data in EEPROM memory cannot be performed in User Mode, which is the Security IC Embedded Software's operating mode.

The Special Function Register operations are

- **read** data from a Special Function Register and
- **write** data into a Special Function Register.

The security attributes are

- **TOE mode**: There are two different TOE modes. The TOE always starts in System Mode and switches to User Mode at the end of a successful boot sequence.
- **Configuration values for memory partition**: These configuration values are stored in the Security Row.

In the following the term "code running" combined with a TOE mode (e.g. "code running in System Mode") will be used to name subjects.

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

FDP_ACC.1[MEM]	**Subset access control**
Hierarchical to:	No other components.
FDP_ACC.1.1	The TSF shall enforce the *Access Control Policy* [11] on *all code running on the TOE, all memories and all memory operations* [12].
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.1[SFR]	**Subset access control**
Hierarchical to:	No other components.
FDP_ACC.1.1	The TSF shall enforce the *Access Control Policy* [13] on *all code running on the TOE, all Special Function Registers, and all Special Function Register operations* [14].
Dependencies:	FDP_ACF.1 Security attribute based access control
Application Note:	The Access Control Policy shall be enforced by implementing hardware access control to each Special Function Register. For every access the TOE mode is used to determine if the access shall be granted or denied. A denied read access returns "0" instead of the actual value, a denied write access will be treated as a security violation and will subsequently

[11] [assignment: access control SFP]

[12] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

[13] [assignment: access control SFP]

[14] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

lead to a system reset. The read and/or write access to a Special Function Register may be not allowed depending on the function of the register or on the TOE mode to enforce the access control policy or ensure a secure operation. In addition, if a Special Function Register is not implemented, a read access will return “0”, and a write access to its address will be treated as a security violation and therefore force a system reset.

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

FDP_ACF.1[MEM]	**Security attribute based access control**
Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the *Access Control Policy* [15] to objects based on the following: *all subjects and objects and the attribute TOE mode* [16].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *Code executed in the System Mode* • *has read and execute access to all code/data in the ROM,* • *has read and write access to all data in the RAM,* • *has read, write and execute access to all code/data in the whole EEPROM* *Code executed in the User Mode* • *has read and execute access to code/data in the User-ROM,* • *has read and write access to all data in the User-EEPROM,* • *has read and write access to all data in the RAM.*[17]
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *Code running in User Mode has read access to the FabKey Area and portions of the Security Row.*[18]
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the *rules: none* [19].

[15] [assignment: access control SFP]

[16] [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]

[17] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]

[18] [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects]

[19] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

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

FDP_ACF.1[SFR] **Security attribute based access control**

Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the *Access Control Policy* [20] to objects based on the following: *all subjects and objects and the attribute TOE mode* [21].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: • *The code executed in System Mode is allowed to access all Special Function Register groups.* • *The code executed in the User Mode is allowed to access Special Function Registers related to hardware components and general CPU functionality* [22].
FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *none* [23]
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the rules: *The Special Function Registers DKEY, RPT0, RPT1, EPT0 and EPT1 are not readable. The Special Function Register RNR is read-only* [24]
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization

Implications of the Access Control Policy

The Access Control Policy has some implications, that can be drawn from the policy and that are essential parts of the TOE security services and features.

- Code executed in the System Mode is quite powerful and used to configure and test the TOE.
- Code executed in the User Mode cannot administrate the configuration of the TOE, because it has no access to the related Special Function Registers.

The TOE shall meet the requirement “Static attribute initialization (FMT_MSA.3)” as specified below.

FMT_MSA.3[MEM] **Static attribute initialization**

Hierarchical to:	No other components.

[20] [assignment: access control SFP]

[21] [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]

[22] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]

[23] [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects]

[24] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

FMT_MSA.3.1	The TSF shall enforce the *Access Control Policy* [25] to provide *restrictive* [26] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow *no subject* [27] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Application Note:	The TOE does not provide objects or information that can be created, since it provides access to memory areas. The definition of objects that are stored in the TOE's memory is subject to the Security IC Embedded Software.

FMT_MSA.3[SFR]	**Static attribute initialization**
Hierarchical to:	No other components.
FMT_MSA.3.1	The TSF shall enforce the *Access Control Policy* [28] to provide *restrictive* [29] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow *no subject* [30] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Application Note:	The TOE does not provide objects or information that can be created, since no further security attributes can be derived (i.e. the set of Special Function Registers that contain security attributes is fixed). The definition of objects that are stored in the TOE's memory is subject to the Security IC Embedded Software.

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

FMT_MSA.1[MEM]	**Management of security attributes**
Hierarchical to:	No other components.
FMT_MSA.1.1	The TSF shall enforce the *Access Control Policy* [31] to restrict the ability to *modify* [32] the security attributes *configuration*

[25] [assignment: access control SFP, information flow control SFP]
[26] [selection, choose one of: restrictive, permissive, [assignment: other property]]
[27] [assignment: the authorized identified roles]
[28] [assignment: access control SFP, information flow control SFP]
[29] [selection, choose one of: restrictive, permissive, [assignment: other property]]
[30] [assignment: the authorized identified roles]
[31] [assignment: access control SFP(s), information flow control SFP(s)]

values for memory partition [33] to *code executed in the System Mode* [34].

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

FMT_MSA.1[SFR] **Management of security attributes**

Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the *Access Control Policy* [35] to restrict the ability to *modify* [36] the security attributes *TOE mode* [37] to *none* [38].

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

The TOE shall meet the requirement "Specification of Management Functions (FMT_SMF.1)" as specified below.

FMT_SMF.1 **Specification of Management Functions**

Hierarchical to: No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:

Change of the TOE mode with a special LCALL address. [39]

Dependencies: No dependencies

Application Note: The iteration of FMT_MSA.1 with the dependency to FMT_SMF.1 may imply a separation of the Specification of Management Functions. However, iteration of FMT_SMF.1 is not needed because all management functions rely on the same features implemented in the hardware.

6.2 Security Assurance Requirements

Table 12 below lists all security assurance components that are valid for this Security Target. With one exception these security assurance components are required by EAL4 (see section 2.2) or by the Protection Profile. The exception is the component

[32] [selection: change_default, query, modify, delete, [assignment: other operations]]
[33] [assignment: list of security attributes]
[34] [assignment: the authorized identified roles]
[35] [assignment: access control SFP(s), information flow control SFP(s)]
[36] [selection: change_default, query, modify, delete, [assignment: other operations]]
[37] [assignment: list of security attributes]
[38] [assignment: the authorized identified roles]
[39] [assignment: list of management functions to be provided by the TSF]

ASE_TSS.2 which is chosen as an augmentation in this ST to give architectural information on the security functionality of the TOE.

Considering the Application Note 21 of [6] the column “Required by” shows the differences in the requirements of security assurance components between the PP and the Security Target. The entry “EAL4 / PP” denotes that an SAR is required by both EAL4 and the requirement of the PP, “EAL4” means that this requirement is due to EAL4 and beyond the requirement of the PP, and “PP” identifies this component as a requirement of the PP which is beyond EAL4. The augmentation ASE_TSS.2 chosen in this security target is denoted by "ST". The refinements of the PP “Security IC Platform Protection Profile”, [6] that must be adapted for EAL4 are described in section 6.2.1.

Table 12. Security Assurance Requirements

SAR	Title	Required by
ADV_ARC.1	Security architecture description	EAL4 / PP
ADV_FSP.4	Complete functional specification	EAL4 / PP
ADV_IMP.1	Implementation representation of the TSF	EAL4 / PP
ADV_TDS.3	Basic modular design	EAL4 / PP
AGD_OPE.1	Operational user guidance	EAL4 / PP
AGD_PRE.1	Preparative procedures	EAL4 / PP
ALC_CMC.4	Production support, acceptance procedures and automation	EAL4 / PP
ALC_CMS.4	Problem tracking CM coverage	EAL4 / PP
ALC_DEL.1	Delivery procedures	EAL4 / PP
ALC_DVS.2	Sufficiency of security measures	PP
ALC_LCD.1	Developer defined life-cycle model	EAL4 / PP
ALC_TAT.1	Well defined development tools	EAL4 / PP
ASE_CCL.1	Conformance claims	EAL4 / PP
ASE_ECD.1	Extended components definition	EAL4 / PP
ASE_INT.1	ST introduction	EAL4 / PP
ASE_OBJ.2	Security objectives	EAL4 / PP
ASE_REQ.2	Derived security requirements	EAL4 / PP
ASE_SPD.1	Security problem definition	EAL4 / PP
ASE_TSS.2	TOE summary specification with architectural design summary	ST
ATE_COV.2	Analysis of coverage	EAL4 / PP
ATE_DPT.2	Testing: security enforcing modules	EAL4 / PP
ATE_FUN.1	Functional testing	EAL4 / PP

SAR	Title	Required by
ATE_IND.2	Independent testing - sample	EAL4 / PP
AVA_VAN.5	Advanced methodical vulnerability analysis	PP

6.2.1 Refinements of the Security Assurance Requirements

The ST claims conformance to the Protection Profile “Security IC Platform Protection Profile”, [6] and therefore it has to be conform to the refinements of the TOE security assurance requirements (see Application Note 22 of the PP). [40]

6.3 Security Requirements Rationale

6.3.1 Rationale for the security functional requirements

Section 6.3.1 of the PP “Security IC Platform Protection Profile”, [6] provides a rationale for the mapping between security functional requirements and security objectives defined in the Protection Profile. The mapping is reproduced in the following table.

Table 13. Security Requirements versus Security Objectives

Objective	TOE Security Functional Requirements
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”
O.Phys-Probing	FPT_PHP.3 “Resistance to physical attack”
O.Malfunction	FRU_FLT.2 “Limited fault tolerance FPT_FLS.1 “Failure with preservation of secure state”
O.Phys-Manipulation	FPT_PHP.3 “Resistance to physical attack”
O.Leak-Forced	All requirements listed for O.Leak-Inherent FDP_ITT.1, FPT_ITT.1, FDP_IFC.1 plus those listed for O.Malfunction and O.Phys-Manipulation FRU_FLT.2, FPT_FLS.1, FPT_PHP.3
O.Abuse-Func	FMT_LIM.1 “Limited capabilities” FMT_LIM.2 “Limited availability” plus those for O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation, O.Leak-Forced FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_PHP.3, FRU_FLT.2, FPT_FLS.1
O.Identification	FAU_SAS.1 “Audit storage”
O.RND	FCS_RNG.1 “Quality metric for random numbers” plus those for O.Leak-Inherent, O.Phys-Probing, O.Malfunction,

40 According to the Application Note 30 in [6], the ST should indicate the version of the Mandatory Technical Document “Application of Attack Potential to Smartcards”, [7] used for the vulnerability analysis in AVA_VAN.5. The current version is given in the bibliography.

Objective	TOE Security Functional Requirements
	O.Phys-Manipulation, O.Leak-Forced FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_PHP.3, FRU_FLT.2, FPT_FLS.1
OE.Plat-Appl	not applicable
OE.Resp-Appl	not applicable
OE.Process-Sec-IC	not applicable

The Security Target additionally defines the SFRs for the TOE that are listed in Table 14. In addition Security Requirements for the Environment are defined. The following table gives an overview, how the requirements are combined to meet the security objectives.

Table 14. Mapping of security objectives and requirements

Objective	TOE Security Functional Requirement
O.HW_DES3	FCS_COP.1
O.MEM_ACCESS	FDP_ACC.1[MEM] FDP_ACF.1[MEM] FMT_MSA.3[MEM] FMT_MSA.1[MEM] FMT_SMF.1
O.SFR_ACCESS	FDP_ACC.1[SFR] FDP_ACF.1[SFR] FMT_MSA.3[SFR] FMT_MSA.1[SFR] FMT_SMF.1
OE.Check-Init	not applicable

The justification related to the security objective “Triple DES Functionality” (O.HW_DES3) is as follows:

O.HW_DES3 requires the TOE to support Triple DES encryption and decryption in standard or CBC mode. Exactly this is the requirement of FCS_COP.1. Therefore FCS_COP.1 is suitable to meet O.HW_DES3.

The justification related to the security objective “Area based Memory Access Control (O.MEM_ACCESS)” is as follows:

The security functional requirement “Subset access control (FDP_ACC.1[MEM])” with the related Security Function Policy (SFP) “Access Control Policy” exactly require to implement a memory partition as demanded by O.MEM_ACCESS. Therefore, FDP_ACC.1[MEM] with its SFP is suitable to meet the security objective.

The security functional requirement “Security attribute based access control (FDP_ACF.1[MEM])” with the related Security Function Policy (SFP) “Access Control Policy” defines the rules to implement the memory partition as demanded by O.MEM_ACCESS. Therefore, FDP_ACF.1[MEM] with its SFP is suitable to meet the security objective.

The security functional requirement “Static attribute initialization (FMT_MSA.3[MEM])” requires that the TOE provide default values for the security attributes. Since the TOE is a hardware platform these default values are generated by the reset procedure for the related Special Function Register. They are needed by the TOE to provide a default configuration after reset. Therefore this requirement (as dependency from FDP_ACF.1) is suitable to meet the security objective.

The security functional requirement “Management of security attributes (FMT_MSA.1)[MEM]” requires that the ability to update the security attributes is restricted to privileged subject(s). These management functions ensure that the required access control can be realized using the functions provided by the TOE.

Finally, the security functional requirement “Specification of Management Functions (FMT_SMF.1)” is used for the specification of the management functions to be provided by the TOE as demanded by O.MEM_ACCESS. Therefore, FMT_SMF.1 is suitable to meet the security objective.

The justification related to the security objective “Special Function Register Access Control (O.SFR_ACCESS)” is as follows:

The security functional requirement “Subset access control (FDP_ACC.1[SFR])” with the related Security Function Policy (SFP) “Access Control Policy” require to implement access control for Special Function Register as demanded by O.SFR_ACCESS. Therefore, FDP_ACC.1[SFR] with its SFP is suitable to meet the security objective.

The access to Special Function Register is related to the TOE mode. The Special Function Register required to use hardware components like e.g. the co-processor or the Random Number Generator can be accessed in the System Mode as specified by the Security Function Policy (SFP) “Access Control Policy”. In the User Mode only Special Function Register required to run the CPU are accessible by default. In addition, specific Special Function Registers related to hardware components can be made accessible for the User Mode.

The security functional requirement “Security attribute based access control (FDP_ACF.1[SFR])” with the related Security Function Policy “Access Control Policy” exactly require certain security attributes to implement the access control to Special Function Register as demanded by O.SFR_ACCESS. Therefore, FDP_ACF.1[SFR] with its SFP is suitable to meet the security objective.

The security functional requirement “Static attribute initialization (FMT_MSA.3[SFR])” requires that the TOE provides default values for the Special Function Register (values as well as access control). The default values are needed to ensure a defined setup for the operation of the TOE. Therefore this requirement (as dependency from FDP_ACF.1) is suitable to meet the security objective.

The security functional requirement “Management of security attributes (FMT_MSA.1[SFR])” is realized in a way that – besides the definition of access rights to Special Function Registers related to hardware components in User Mode - no management of the security attributes is possible because the attributes are implemented in the hardware and cannot be changed.

Finally, the security functional requirement “Specification of Management Functions (FMT_SMF.1)” is used for the specification of the management functions to be provided

by the TOE as demanded by O.SFR_ACCESS. Therefore, FMT_SMF.1 is suitable to meet the security objective.

Note that the iteration of FDP_ACF.1 and FDP_ACC.1 with the respective dependencies are needed to separate the different types of objects because they have different security attributes.

6.3.2 Dependencies of security functional requirements

The dependencies listed in the Protection Profile [6] are independent of the additional dependencies listed in the table below. The dependencies of the Protection Profile are fulfilled or appropriately addressed within the Protection Profile.

The following discussion demonstrates how the dependencies defined by Part 2 of the Common Criteria for the requirements specified in sections 6.1.2 and 6.1.3 are satisfied.

The dependencies defined in the Common Criteria are listed in the table below:

Table 15. Dependencies of security functional requirements

Security Functional Requirement	Dependencies	Fulfilled by security requirements in this ST
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1 FCS_CKM.4	See discussion below
FDP_ACC.1[MEM]	FDP_ACF.1	Yes, by FDP_ACF.1[MEM]
FDP_ACC.1[SFR]	FDP_ACF.1	Yes, by FDP_ACF.1[SFR]
FDP_ACF.1[MEM]	FDP_ACC.1 FMT_MSA.3	Yes, by FDP_ACC.1[MEM] Yes
FDP_ACF.1[SFR]	FDP_ACC.1 FMT_MSA.3	Yes, by FDP_ACC.1[SFR] Yes
FMT_MSA.3[MEM]	FMT_MSA.1 FMT_SMR.1	Yes, by FMT_MSA.1[MEM] See discussion below
FMT_MSA.3[SFR]	FMT_MSA.1 FMT_SMR.1	Yes, by FMT_MSA.1[SFR] See discussion below
FMT_MSA.1[MEM]	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes, by FDP_ACC.1[MEM] See discussion below Yes
FMT_MSA.1[SFR]	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes, by FDP_ACC.1[SFR] See discussion below Yes

The developer of the Security IC Embedded Software must ensure that the additional security functional requirement FCS_COP.1 is used as specified and that the User Data processed by the related security functionality is protected as defined for the application context.

The dependent requirements of FCS_COP.1 completely address the appropriate management of cryptographic keys used by the specified cryptographic function and the management of access control rights as specified for the memory access control function. All requirements concerning these management functions shall be fulfilled by the environment (Security IC Embedded Software).

The functional requirements [FDP_ITC.1, or FDP_ITC.2 or FCS_CKM.1] and FCS_CKM.4 are not included in this Security Target since the TOE only provides a pure engine for encryption and decryption without additional features for the handling of cryptographic keys. Therefore the Security IC Embedded Software must fulfill these requirements related to the needs of the realized application.

The dependency FMT_SMR.1 introduced by the two components FMT_MSA.1 and FMT_MSA.3 must be fulfilled by the Security IC Embedded Software. The definition and maintenance of the roles that act on behalf of the functions provided by the hardware must be subject of the Security IC Embedded Software.

6.3.3 Rationale for the Assurance Requirements

The selection of assurance components is based on the underlying Protection Profile [6]. The Security Target uses the same augmentations as the PP including the same assurance level, the only exception is ASE_TSS.2. This component is chosen as an augmentation in this ST to give architectural information on the security functionality of the TOE. ASE_TSS.2 is hierarchical to ASE_TSS.1 which is part of all EAL defined by Common Criteria. Since also its dependencies (ASE_INT.1, ASE_REQ.1 and ADV_ARC.1) are fulfilled by the assurance requirements claimed by this ST it is considered as consistent augmentation.

The rationale for the augmentations is the same as in the PP. The assurance level EAL4 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 4. Therefore, these components add additional assurance to EAL 4, but the mutual support of the requirements is still guaranteed.

As stated in the Protection Profile, section 6.3.3, 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_VAN.5 was chosen by the PP in order to assure that even these attackers cannot successfully attack the TOE.

6.3.4 Security Requirements are 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 show that the security functional and assurance requirements support each other and that there are no inconsistencies between these groups.

The security functional requirements required to meet the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced also protect the cryptographic algorithms and the memory separation function as well as the access control to Special Function Register implemented according to the security

functional requirement FCS_COP.1 and FDP_ACC.1[MEM], FDP_ACC.1[SFR] with reference to the Access Control Policies defined in FDP_ACF.1[MEM] and FDP_ACF.1[SFR]. Therefore, these security functional requirements support the secure implementation and operation of FCS_COP.1 and both iterations of FDP_ACC.1 with FDP_ACF.1, respectively, as well as the dependent security functional requirements.

A smart card platform requires Security IC Embedded Software to build a secure product. Thereby the Security IC Embedded Software must support the security features of the hardware and implement a sufficient management of the security features implemented in the hardware. The realization of the Security Functional Requirements within the TOE provides a good balance between flexible configuration and restrictions to ensure a secure behavior of the TOE.

7. TOE Summary Specification

This chapter is divided into the sections “Portions of the TOE Security Functionality” and “TOE Summary Specification Rationale”.

7.1 Portions of the TOE Security Functionality

The TOE Security Functionality (TSF) directly corresponds to the TOE security functional requirements defined in section 6.

The following portions of security functionality are applicable to the phases 4 to 7.

Note 5. Parts of the security functionality are configured at the end of phase 3 and the whole security functionality is already active during the delivery from phase 3 to phase 4.

The TOE comprises additional features that are not listed as security functionality in the following. They do not provide a complete portion of the security functionality by themselves but they can be used to support a portion of the security functionality implemented by the Security IC Embedded Software, e.g. the CRC calculation for the control of data integrity.

The TOE Security Functionality (TSF) described in the following is split into Security Services und Security Feature.

7.1.1 Security Services

SS.RNG: Random Number Generator

The random number generator is accessible via the hardware abstraction library and produces random numbers with an arbitrary length. The TOE implements the SS.RNG by means of a physical hardware random number generator working stable within the limits guaranteed by SF.OPC (operational conditions).

The security service provided by the TOE comprises a total failure test and an online test. If an error occurs, an error return code is provided by the HAL.

According to AIS31, [5] the random number generator claims the fulfillment of the requirements of functionality class P2. This means that the random number generator is suitable for generation of signature key pairs, generation of session keys for symmetric encryption mechanisms, random padding bits, zero-knowledge proofs and generation of seeds for DRNGs.

SS.HW_DES: Triple-DES Co-processor

The TOE provides the Triple Data Encryption Algorithm (TDEA) in standard or CBC mode according to the Data Encryption Standard (DES). SS.HW_DES 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 [11]. The key management for the 2-key (112 bit) Triple DES algorithm shall be provided by the Security IC Embedded Software. For encryption and decryption the Hardware Abstraction Library provides dedicated functions that must be used by the Security IC Embedded Software.

Note that the TOE does also allow Single-DES, but this shall not be used in the evaluated product.

7.1.2 Security Features

SF.OPC: Control of Operating Conditions

The function SF.OPC ensures the correct operation of the TOE (functions offered by the micro-controller including the standard CPU as well as the Triple-DES co-processor, the memories, registers, I/O interfaces and the other system peripherals) during the execution of the IC Dedicated Support Software and Security IC Embedded Software. This includes all specific security features of the TOE which are able to provide an active response.

The TOE ensures its correct operation and prevents any malfunction using the following features: filtering of power supply and clock sources as well as monitoring of power supply, the frequency of the clocks and the temperature of the chip by means of sensors. There are multiple sensors implemented to monitor the supply voltage during the contact-less operation. Light sensors are distributed over the chip surface and used to detect light attacks. The thresholds allowed for these parameters are defined within the range where the TOE ensures its correct operation.

For performance reasons, the CPU is not directly connected to the ROM memory module but to a code fetch cache instead. The code fetch cache is equipped with special consistency checks for cached addresses as well as for the cached data.

The DES co-processor of the TOE is equipped with special circuitry to detect single fault injection attacks. A detected single fault injection attack will be treated as a security violation and will therefore trigger a system reset.

The SFR access control comprises a fault detection that also leads to a reset of the device if an operation was performed which is not permitted within the executed TOE mode.

If one of the monitored parameters is out of the specified range, the TOE will execute a system reset which consequently aborts the actual running Security IC Embedded Software. A reset is forced by the sensors for voltage, suspension time, temperature, light and sensor integrity (plausibility of the various sensor´s activity). In addition, violations of SFR and memory access rights will also trigger a system reset.

If the TOE is reset, all components of the TOE are initialized with their reset values. In addition, the TOE provides a reset cause indicator to the Security IC Embedded Software which is available after each system reset and as long as the TOE is powered.

If the inverse error correction of the EEPROM is enabled (refer to section 2.6 of [9]) the probability to detect fault injection errors increases, compared to the double read mode and other implemented EEPROM attack counter measures, and the error correction logic will force a reset if an error is detected.

The HAL provides write and erase operations for the EEPROM that include the control of specific operating conditions and the verification of the written data. The result of the operation is provided to the Security IC Embedded Software as a return code.

In the User Mode the TOE enables the sensors automatically when operated. Furthermore the TOE prevents the Security IC Embedded Software from disabling the sensors.

SF.PHY: Protection against Physical Manipulation

The feature SF.PHY protects the TOE against manipulation of (i) the hardware, (ii) the IC Dedicated Software in the ROM, (iii) the Security IC Embedded Software in the ROM and (iv) the application data in the EEPROM and RAM including the configuration data in the security row. It also protects all data stored in the memories including User Data and TSF data against disclosure by physical probing when stored or while being processed by the TOE.

The protection of the TOE comprises different features within the design and construction which make reverse-engineering and tamper attacks difficult. These features comprise dedicated shielding techniques and specific encryption features for the memory blocks. SF.PHY supports the efficiency of other portions of the security functionality.

SF.PHY also supports the integrity of the memories by implementing parity control for the ROM and the RAM as well as redundancy with error correction for the EEPROM.

SF.LOG: Logical Protection

SF.LOG implements measures to limit or eliminate the information that might be contained in the shape and amplitude of signals or in the time between events found by measuring such signals. This comprises the power consumption and signals on the other pads that are not intended by the terminal or the Security IC Embedded Software. Thereby SF.LOG prevents the disclosure of User Data or TSF data stored and/or processed in the security IC through the measurement of the power consumption or emanation and subsequent complex signal processing. The protection of the TOE comprises different features within the design that support the other portions of security functionality.

The Triple-DES co-processor includes special features to prevent SPA/DPA analysis of shape and amplitude of the power consumption and ensures that the calculation time is independent from any key and plain/cipher text.

Additional features that can be configured by the Security IC Embedded Software, comprise CPU and DES clock configurations that can be used to prevent the possibility to synchronize the internal operation with the external field clock or to synchronize with the characteristics of the power consumption that can be used as trigger signal to support other attacks.

Specific features as described for SF.PHY (e.g. the encryption features) and for SF.OPC (e.g. the filter feature) support the logical protection.

SF.COMP: Protection of Mode Control

SF.COMP provides a control of the TOE modes (System Mode and User Mode). This includes the protection of electronic fuses.

The control of the TOE modes prevent the abuse of test functions after TOE delivery. Additionally it also ensures that features used during the boot sequence to configure the TOE can not be abused. Hardware circuitry and the Boot ROM Software determine whether the test functionality is available or not. If it is available, the TOE starts the IC

Dedicated Test Software in the System Mode. Otherwise, the TOE switches to the User Mode and starts execution of the Security IC Embedded Software.

SF.COMP ensured that it is only possible to switch from System Mode to User Mode, which is performed by a LCALL to a specific address. The switch to the IC Dedicated Test Software is prevented after TOE delivery because specific electronic fuses guarantee that the IC Dedicated Test Software cannot be selected. The System Mode is the more privileged TOE mode, the User Mode is the less privileged TOE mode. Only Boot ROM Software and IC Dedicated Test Software are executed in System Mode. For the Security IC Embedded Software, only the User Mode is available.

The protection of the electronic fuses especially ensures that configuration options with regard to the security functionality cannot be changed, abused or influenced in any way in User Mode. SF.COMP ensures that activation or deactivation of security features cannot be influenced by the Security IC Embedded Software.

The TSF controls access to the Fabkey and Security Row. The top-most 128 Bytes of the EEPROM memory are accessible at reserved addresses within the logical memory map. The available EEPROM memory space for the Security IC Embedded Software is reduced by this area. SF.COMP further limits the read-only access (provided by SF.MEM_ACC) to certain bytes within the Fabkey and Security Row in User Mode.

SF.COMP limits the capabilities of the test functions and provides test personnel during phase 3 with the capability to store the identification and/or pre-personalization data in the EEPROM.

SF.MEM_ACC: Memory Access Control

SF.MEM_ACC controls access of any subject (program code comprising processor instructions) to the memories of the TOE. The access control is implemented by a partition of the memories: The ROM is split into two parts. In User Mode the CPU has access to only one part of the memory that comprises the Security IC Embedded Software. In the System Mode access to both parts is allowed in order to test the memory block, but execution of the Security IC Embedded Software in System Mode is not possible.

The EEPROM is split into the User-EEPROM and the Security Row with the FabKey Area. SF.MEM_ACC ensures that the Security Row as well as the Fab Key Area can only be read in User Mode whereas System Mode has full access to the EEPROM.

The memory partition of ROM and EEPROM is fixed and cannot be changed in User Mode. The size of each partition is determined by the design of the TOE.

In addition, SF.MEM_ACC permanently checks whether the selected addresses are within the boundaries of the physically implemented memory ranges. Access to outside the boundary of the physically implemented memory ranges forces a reset. Also, SF.MEM_ACC permanently checks for the consistency of addresses and data for the ROM cache and for RAM read/write accesses.

SF.SFR_ACC: Special Function Register Access Control

SF.SFR_ACC implements the access control to the Special Function Registers as specified in the Access Control Policy and the Security Functional Requirements FDP_ACC.1[SFR] and FDP_ACF.1[SFR].

Based on the function of the register and on the TOE mode, the read and/or write access for a specific Special Function Register is allowed or not allowed. SF.SFR_ACC will ignore any read operation on the Special Function Registers that are not allowed or not implemented. Ignore in this case means that the read access always provides a fixed return value.

If the CPU tries to write to Special Function Registers that are not implemented at all or that have no write permission in the currently active TOE mode, SF.SFR_ACC forces a system reset.

The combination of SF.SFR_ACC and SF.COMP ensures that the access rights of the System Mode are not available in the User Mode.

7.2 TOE Summary Specification Rationale

7.2.1 Rationale for the portions of the TOE security functionality

The following table provides a mapping of portions of the TSF to SFR.

Table 16. Mapping of Security Functional Requirements and the portions of the TOE Security Functionality

	SS.RNG	SS.HW_DES	SF.OPC	SF.PHY	SF.LOG	SF.COMP	SF.MEM_ACC	SF.SFR_ACC
FAU_SAS.1				X		X		
FCS_RNG.1	X			X				
FDP_IFC.1				X	X			
FDP_ITT.1				X	X			
FMT_LIM.1				X		X		
FMT_LIM.2				X		X		
FPT_FLS.1			X	X				
FPT_ITT.1				X	X			
FPT_PHP.3				X				
FRU_FLT.2			X	X				
FCS_COP.1		X		X				
FDP_ACC.1[MEM]				X			X	
FDP_ACC.1[SFR]				X				X
FDP_ACF.1[MEM]				X			X	
FDP_ACF.1[SFR]				X				X

	SS.RNG	SS.HW_DES	SF.OPC	SF.PHY	SF.LOG	SF.COMP	SF.MEM_ACC	SF.SFR_ACC
FMT_MSA.1[MEM]				X			X	
FMT_MSA.1[SFR]				X				X
FMT_MSA.3[MEM]				X			X	
FMT_MSA.3[SFR]				X				X
FMT_SMF.1				X			X	X

The "X" means that the specific portion of the TOE security functionality realizes or supports the functionality required by the respective Security Functional Requirement.

8. Annexes

8.1 Further Information contained in the PP

The Annex of the Protection Profile ([6], chapter 7) provides further information. Section 7.1 of the PP describes the development and production process of security ICs, containing a detailed life-cycle description and a description of the assets of the Integrated Circuits Designer/Manufacturer. Section 7.2 is concerned with security aspects of the Security IC Embedded Software (further information regarding A.Resp-Appl and examples of specific Functional Requirements for the Security IC Embedded Software). Section 7.3 gives examples of Attack Scenarios.

8.2 Glossary and Vocabulary

Note: To ease understanding of the used terms the glossary of the Protection Profile [6] is included here.

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 [6], Figure 2 in section 1.2.3 and section 7.1.1). The Card Manufacturer has the following roles (i) the Smartcard Product Manufacturer (Phase 5) and (ii) the Personalizer (Phase 6). If the TOE is delivered after Phase 3 in form of wafers or laser diced wafers (dice) he has the role of the IC Packaging Manufacturer (Phase 4) in addition.
TOE Mode	Mode in which the CPU operates. The TOE supports two TOE modes, the System Mode and the User Mode.
FabKey Area	A memory area of 64 bytes in the EEPROM that contains data that is programmed during testing by the IC Manufacturer. The amount of data and the type of information can be selected by the customer. The FabKey Area is part of the Security Row.
Integrated Circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions.
IC Dedicated Software	IC proprietary software embedded in an 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 Support Software	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.
IC Dedicated Test Software	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.
Initialization 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).
Memory	The memory comprises the RAM, the ROM, and the EEPROM of the TOE.
Pre-personalization 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.
Security Row	Top-most 128 bytes of the EEPROM memory reserved for configuration purposes as well as dedicated memory area for the Security IC Embedded Software to store life-cycle information about the TOE.
Security IC Embedded Software	Software embedded in a security IC and not being developed by the IC Designer. The Security IC Embedded Software is designed in Phase 1 and embedded into the security 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 Security IC Embedded Software can be considered as being application dependent whereas the IC Dedicated Software is definitely not.
Special Function Registers	Registers used to access and configure the functions for the communication with an external interface device, the cryptographic co-processor for Triple-DES, the random numbers generator and chip configuration.
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.
System Mode	TOE mode for configuration of the TOE during start-up and for executing the IC Dedicated Test Software. The access to the IC Dedicated Test Software is permanently and irreversible disabled after production

	testing. In System Mode specific Special Function Registers are accessible for test purposes.
TOE Delivery	The period when the TOE is delivered which is (refer to [6], Figure 2 in section 1.2.3) either (i) after Phase 3 (or before Phase 4) if the TOE is delivered in form of wafers or laser diced 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 (for example configuration data). Note that the TOE is the security IC. Initialization 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 Security IC Embedded Software. Therefore, the "user" or "customer" of the TOE (as used in the Common Criteria assurance class AGD: guidance) is the Security IC Embedded Software. Guidance is given for the Security IC Embedded Software Developer. On the other hand the final product (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 Security IC Embedded Software in the application context. User data comprise all data in the final security IC except the TSF data.
User Mode	The User Mode is a limited mode in which the Security IC Embedded Software is executed.

8.3 List of Abbreviations

CC	Common Criteria Version 3.1.
CIU	Contact-less Interface Unit
CPU	Central Processing Unit
DEA	Data Encryption Algorithm.
DES	Data Encryption Standard.
DRNG	Deterministic Random Number Generator
EAL	Evaluation Assurance Level
HAL	Hardware Abstraction Library
LLL	Low Level Library
IC	Integrated circuit.
IT	Information Technology.
NDA	Non Disclosure Agreement.
NFC	Near Field Communication
NVM	Non Volatile Memory (EEPROM)
PP	Protection Profile.
SAR	Security Assurance Requirement.
SFR	as abbreviation of the CC term: Security Functional Requirement, as abbreviation of the technical term of the IC hardware: Special Function Register[41]
SSMC	Systems on Silicon Manufacturing Co. Pte. Ltd
ST	Security Target.
TOE	Target of Evaluation.
TRNG	True Random Number Generator
TSF	TOE Security functionality.
TSFI	TSF Interface.

[41] This security target does not use SFR as abbreviation for Special Function Register in the explanatory text to avoid confusion. However, the abbreviation is used in objective or security functionality identifiers and to distinguish iterations.

8.4 Bibliography

8.4.1 Evaluation Documents

[1] Common Criteria for Information Technology Security Evaluation, Part 1 - Introduction and general model - Version 3.1 CCMB-2006-09-001, Revision 1, September 2006

[2] Common Criteria for Information Technology Security Evaluation, Part 2 - Security functional requirements, Version 3.1 CCMB-2007-09-002, Revision 2, September 2007

[3] Common Criteria for Information Technology Security Evaluation, Part 3 - Security Assurance Requirements, Version 3.1 CCMB-2007-09-003, Revision 2, September 2007

[4] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part 2 - Evaluation Methodology, Version 3.1 CCMB-2007-09-004, Revision 2, September 2007

[5] Functionality classes and evaluation methodology for true (physical) random number generators, Bundesamt fuer Sicherheit in der Informationstechnik (BSI), Version 3.1, 25 September 2001

[6] Security IC Platform Protection Profile, registered and certified by Bundesamt fuer Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0035, Rev 1.0, 15 June 2007

[7] Application of Attack Potential to Smartcards, Version 2.5, Revision 1, April 2008, CCDB-2008-04-001

8.4.2 Developer Documents

[8] MF3F60x1, Secured contactless smartcard controller, Objective data sheet

[9] MF3F60x1, Guidance, Delivery and Operation Manual

[10] MF3F60x1, Order Entry Form, NXP Semiconductors, Business Line Identification

8.4.3 Other Documents

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

[12] ISO/IEC 18092: Information technology - Telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol (NFCIP-1), First Edition, 2004

9. Legal information

9.1 Definitions

Draft — The document is a draft version only. The content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included herein and shall have no liability for the consequences of use of such information.

9.2 Disclaimers

General — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in medical, military, aircraft, space or life support equipment, nor in applications where failure or malfunction of a NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors accepts no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is for the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from national authorities.

9.3 Licenses

ICs with DPA Countermeasures functionality

NXP ICs containing functionality implementing countermeasures to Differential Power Analysis and Simple Power Analysis are produced and sold under applicable license from Cryptography Research, Inc.

9.4 Trademarks

Notice: All referenced brands, product names, service names and trademarks are property of their respective owners.

MIFARE — is a trademark of NXP B.V.

.

10. Contents

For more information, please visit: http://www.nxp.com
For sales office addresses, email to: sales.addresses@www.nxp.com

Date of release: 4 February 2010