MIFARE Plus MF1SPLUSx0y1

Security Target Lite

Rev. 1.2 — 14 May 2010	Evaluation Documentation
BSI-DSZ-CC-0620	PUBLIC

Document information	
Info	**Content**
Keywords	Security Target Lite, MF1SPLUSx0y1
Abstract	Evaluation of the NXP MIFARE Plus MF1SPLUSx0y1 Secure Smart Card Controller developed and provided by NXP Semiconductors, Business Line Identification according to the Common Criteria for Information Technology Evaluation (CC) at level EAL4 augmented

Revision history			
Rev	**Date**	**Description**	**Remarks**
1.1	23 July 2009	Derived from full Security Target MF1SPLUSx0y1	
1.2	14 May 2010	Hardware update reflected; Type identifier v changed form SW-Version to Product Version.	

Latest version is: Rev. 1.2 (14 May 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

MIFARE Plus MF1SPLUSx0y1 Security Target Lite, Rev. 1.2, NXP Semiconductors, 14 May 2010

1.2 TOE reference

The term “NXP MIFARE Plus MF1SPLUSx0y1” is used as short reference for the TOE. The references of all evaluated versions are provided in section 1.4.1.1.

1.3 TOE Overview

1.3.1 Introduction

The TOE is a smart card comprising a hardware platform and a fixed software package (Security IC Embedded Software and IC Dedicated Software). The software package provides an operating system with a set of functions used to manage the data stored in the non-volatile EEPROM memory.

NXP has developed the NXP MIFARE Plus MF1SPLUSx0y1 to be used with Proximity Coupling Devices (PCDs) according to ISO14443 Type A. The communication protocol complies to part ISO 14443-3 and 14443-4. The MF1SPLUSx0y1 is primarily designed for secure contact-less transport applications and related loyalty programs as well as access management systems. It fully complies with the requirements for fast and highly secure data transmission, flexible data storage and interoperability with existing infrastructures.

The TOE includes IC Dedicated Test Software for test purposes after production. The Smart Card Controller hardware comprises an 8-bit processing unit, volatile and non-volatile memories, a cryptographic co-processor, security components and a contact-less communication interface.

The TOE includes a Functional Specification and a Guidance Document. This documentation contains a description of the hardware and software interface, the secure configuration and usage of the product by the terminal designer.

The security measures of the MF1SPLUSx0y1 are designed to act as an integral part of the combination of hardware platform and software package in order to strengthen the product as a whole. Several security measures are completely implemented in and controlled by the hardware. Other security measures are controlled by the combination of hardware and software.

1.3.2 TOE Type

The TOE is a Smart Card comprising a hardware platform and a fixed software package (Security IC Embedded Software and IC Dedicated Software). The guidance consists of two documents that are also part of the TOE.

1.3.3 Required non-TOE hardware/software/firmware

The TOE requires an ISO 14443 card terminal to be provided with power and to receive adequate commands.

1.4 TOE Description

1.4.1 Physical scope of the TOE

The Target of Evaluation (TOE) is the smart card integrated circuit named MF1SPLUSx0y1 together with its Security IC Embedded Software. It is manufactured in an advanced CMOS process. The TOE includes IC Designer/Manufacturer proprietary IC Dedicated Test Software and IC Dedicated Support Software. The MIFARE Plus Embedded Software is called Security IC Embedded Software according to the terminology used in [7]. Note that this Security IC Embedded Software is part of the TOE.

The following table lists the TOE components.

Table 1. Components of the TOE

Type	Name	Release	Date	Form of delivery
Hardware	NXP MIFARE Plus MF1SPLUSx0y1 Master	t507C	t507C.gds2 (21.07.2009)	Wafer or modules (dice include reference t507C)
Hardware	NXP MIFARE Plus MF1SPLUSx0y1 Via	002	romt0byf002.eco (08.05.2009)	Wafer or modules (dice include reference 002 on via)
Software	Test ROM Software (the *IC Dedicated Test Software*)	1.13	24.03.2009	ROM on the chip *(DF8_TestOS_YAM1_PROD.hex)*
Software	Boot ROM Software (the *IC Dedicated Support Software*)	1.13	24.03.2009	ROM on the chip *(DF8_TestOS_YAM1_PROD.hex)*
Software	MIFARE Plus Embedded Software *(the Security IC Embedded Software)*	1.20	06.05.2009	ROM on the chip *(MFP_PROD.hex)*
Document	Data Sheet, MF1SPLUSx0y1 [9]			Electronic document
Document	Guidance, Delivery and Operation Manual, MF1SPLUSx0y1 [10]			Electronic document

1.4.1.1 Evaluated package types

A number of package types are supported for the TOE. Each package type has a different commercial type name. The TOE will be available in two different packages and two different memory configurations.

A commercial type name for the TOE has the following general format:

- MF1SPLUS*xeyfdpp/lv*

Table 2 illustrates the commercial type names that are subject of the evaluation. All package types are manufactured in SSMC.

Table 2. Supported package types and memory configurations

Type	*x*	*e*	*y*	*f*	*d*	*pp*	/	*l*	*v*	Description
MF1SPLUS	6	0	2	1	D	UD	/	0	3	2K EEPROM, 4 byte UID; UID0=xF according to ISO 14443-3, 120µm sawn wafer, L1 card, Product Version 3
MF1SPLUS	6	0	1	1	D	UD	/	0	3	2K EEPROM, 4 byte UID, 120µm sawn wafer, L1 card, Product Version 3
MF1SPLUS	6	0	0	1	D	UD	/	0	3	2K EEPROM, 7 byte UID, 120µm sawn wafer, L1 card, Product Version 3
MF1SPLUS	6	0	2	1	D	A4	/	0	3	2K EEPROM, 4 byte UID; UID0=xF according to ISO 14443-3, MOA4 module on reel, L1 card, Product Version 3
MF1SPLUS	6	0	1	1	D	A4	/	0	3	2K EEPROM, 4 byte UID, MOA4 module on reel, L1 card, Product Version 3
MF1SPLUS	6	0	0	1	D	A4	/	0	3	2K EEPROM, 7 byte UID, MOA4 module on reel, L1 card, Product Version 3
MF1SPLUS	8	0	2	1	D	UD	/	0	3	4K EEPROM, 4 byte UID; UID0=xF according to ISO 14443-3, 120µm sawn wafer, L1 card, Product Version 3
MF1SPLUS	8	0	1	1	D	UD	/	0	3	4K EEPROM, 4 byte UID, 120µm sawn wafer, L1 card, Product Version 3
MF1SPLUS	8	0	0	1	D	UD	/	0	3	4K EEPROM, 7 byte UID, 120µm sawn wafer, L1 card, Product Version 3
MF1SPLUS	8	0	2	1	D	A4	/	0	3	4K EEPROM, 4 byte UID; UID0=xF according to ISO 14443-3, MOA4 module on reel, L1 card, Product Version 3
MF1SPLUS	8	0	1	1	D	A4	/	0	3	4K EEPROM, 4 byte UID, MOA4 module on reel, L1 card, Product Version 3
MF1SPLUS	8	0	0	1	D	A4	/	0	3	4K EEPROM, 7 byte UID, MOA4 module on reel, L1 card, Product Version 3

The commercial type name is different depending on

- the memory size (*x*=6: 2K EEPROM, *x*=8: 4K EEPROM),
- the evolution (*e*=0: the very first evolution of MIFARE Plus),
- the UID length (*y*=0: 7 byte UID, *y*=1: 4 byte UID, *y*=2: 4 byte UID; UID0=xF according to ISO 14443-3),
- the FAB produced (*f*=1: product produced in SSMC),
- the operating temperature range for the product (*d*=D: -20 < $t_{operating}$ < 70),
- the package type (*pp*=UD: 120µm sawn wafer, *pp*=A4: MOA4 module on reel),
- the Security Level when switching from Security Level 0 (*l*=0: L1 card),

and

- the Product Version (*v*=3: Product Version 3).

Since *e*, *f*, *d*, *l* and *v* only provide 1 option the format is restricted to:

- MF1SPLUS*x*0*y*1D*pp*/03

For example, the commercial type name “MF1SPLUS6011DUD/03” denotes a MIFARE Plus supplied in wafer form, with 2K EEPROM, 4 byte UID, manufactured in SSMC and supporting security levels 0, 1 and 3, Product Version 3. The commercial type name “MF1SPLUS8001DA4/03” denotes a MIFARE Plus supplied in modules on a reel, with 4K EEPROM, 7 byte UID, manufactured in SSMC and supporting security levels 0, 1 and 3, Product Version 3.

The package type does not influence the security functionality of the TOE. For all package types listed above the security during development and production is ensured (refer to section 1.4.3).

All commercial types listed in the table above are subject of this evaluation. However the identifier “MF1SPLUSx0y1” will be used in the remainder of the document to make referencing easier. Unless described explicitly all information given in the remainder of the ST applies to all commercial types.

1.4.2 Logical Scope of the TOE

1.4.2.1 Hardware Description

The CPU of the MF1SPLUSx0y1 has an 8-bit architecture with an instruction set that is based on the 8051-family instruction set. The on-chip hardware components are controlled by the Security IC Embedded Software via Special Function Registers. These registers are correlated to the activities of the CPU, the memory management unit, interrupt control, contact-less communication, EEPROM, timers and the AES co-processor. The communication with the MF1SPLUSx0y1 can be performed through the contact-less interface.

The device includes ROM (32 kByte), RAM (512 Byte) and EEPROM (8 kByte) memory. The ROM is split in Application-ROM and Test-ROM.

The AES co-processor supports AES operations with a key length of 128 bits. The random number generator provides true random numbers without pseudo random calculation.

1.4.2.2 Software Description

The IC Dedicated Test Software (Test ROM Software) in the Test-ROM of the TOE is used by the TOE Manufacturer to test the functionality of the chip. The test functionality is disabled before the operational use of the smart card. The IC Dedicated Test Software includes the test operating system, test routines for the various blocks of the circuitry, control flags for the status of the EEPROM security row and shutdown functions to ensure that security relevant test operations cannot be executed illegally after phase 3 of the TOE life cycle (cf. section 1.4.4).

The TOE also contains IC Dedicated Support Software which is also stored in the Test-ROM. The IC Dedicated Support Software consists of the Boot ROM Software. This 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.

The Security IC Embedded Software provides the main functionality of the TOE in the usage phase. The MF1SPLUSx0y1 is primarily designed for secure contact-less transport applications and related loyalty programs as well as access management systems. It fully complies with the requirements for fast and highly secure data

transmission, flexible data storage and interoperability with existing infrastructures. Its functionality consists of:

- A data storage system that contains blocks grouped in sectors which can store data.
- Authentication on sector level with fine-grained access conditions blocks.
- Message authentication to support replay attack protection.
- Unique serial number for each device (UID) with optional random ID.

The TOE features enable it to be used for a variety of applications:

- Electronic fare collection
- Stored value card systems
- Access management systems
- Loyalty

If privacy is an issue, the TOE can be configured not to disclose privacy-related information to unauthorised users.

The card is in one (of in total four) security levels. The TOE is delivered as “L1 card”, indicating that security levels 0, 1 and 3 are available. The main features of each security level are listed below:

Security level 0: The card does not provide any functionality besides initialization. The card is initialized in plaintext, especially keys for the further levels can be brought in. A card in security level 0 is not usable for other purposes. After all mandatory keys and security attributes have been stored in the card it can be switched to security level 1.

Security level 1: The card user can access the blocks in the card after an authentication procedure. The communication with the terminal is protected, however the authentication and the protected communication in this security level are not evaluated security services of the TOE. It can be switched to security level 3 if an authentication using the AES algorithm with the necessary key is performed.

Security level 2: This security level is not supported by the TOE.

Security level 3: The card user can access the data blocks in the card via an adequate card terminal after an authentication procedure based on the AES algorithm. The communication with the card terminal can be protected by using a message authentication code (MAC). The authentication and the MAC are security services of the TOE. The TOE cannot be switched to a different security level.

In all security levels the TOE does additionally support the so-called originality function which allows verifying the authenticity of the TOE.

There is also a card state called “TERMINATION”. In response to detected attacks on the TOE it can switch to the “TERMINATION” state. This state is irreversible and does not allow any access to the card data.

1.4.2.3 Documentation

The Functional Specification [9] is also part of the TOE. It contains a functional description of the communication protocols and the commands implemented by the TOE. The provided documentation can be used by a customer to construct applications using the TOE. In addition there is a dedicated guidance manual [10] focused on security aspects.

1.4.3 Security during Development and Production

During the design and the layout process of the IC and the development of the software only people involved in the specific development project have access to sensitive 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 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. The accountability and the traceability is ensured among the wafer fab and the photo mask provider.

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 based on customer demand. Information about non-functional items is stored on magnetic/optical media enclosed with the delivery, available for download or the non-functional items are physically marked.

In summary the TOE can be delivered in two different forms:

- Dice on wafers
- Smart card modules on a module reel

The different (package) types are described in detail in section 1.4.1.1.

1.4.4 Life Cycle and Delivery of the TOE

The life-cycle phases are according to the Security IC Platform Protection Profile [7], section 1.2.4:

- Phase 1: IC Embedded Software Development
- Phase 2: IC Development
- Phase 3: IC Manufacturing
- Phase 4: IC Packaging
- Phase 5: Composite Product Integration
- Phase 6: Personalisation
- Phase 7: Operational Usage

For the usage phase the MF1SPLUSx0y1 chip will be embedded in a credit card sized plastic card (micro-module embedded into the plastic card) or another sealed package.

The module and card embedding of the TOE provide external security mechanisms because they make it harder for an attacker to access parts of the TOE for physical manipulation.

Regarding the Application Note 1 of [7] NXP will deliver the TOE at the end of phase 3 in form of wafers or at the end of phase 4 in packaged form.

Regarding the Application Note 2 of [7] the TOE provides additional functionality which is not covered in the “Security IC Platform Protection Profile”. The additional functionality is due to the Security IC Embedded Software that is included in this evaluation.

The TOE is able to control two different logical phases. After production of the chip every start-up will lead to the Test Mode and the execution of the IC Dedicated Test Software. At the end of the production test the access to the IC Dedicated Test Software is disabled. With disabled test software every start-up of the chip will lead to the User Mode with the CPU executing the Security IC Embedded Software.

The security level 0 is intended for personalisation in phase 6. The security levels 1 to 3 are intended for the phase 7.

1.4.5 TOE Intended Usage

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. Regarding to phase 7, the TOE is used by the end-user. The method of use of the product in this phase depends on the application. The TOE is intended to be used in an unsecured environment that does not avoid a threat.

The device is developed for high-end safeguarded applications, and is designed for embedding into contact-less smart cards according to ISO 14443 [12]. Usually the smart card is assigned to a single individual only and the smart card may be used for multiple applications in a multi-provider environment. Therefore the TOE may store and process secrets of several systems that must be protected from each other. The secret data shall be used as input for the calculation of authentication data and the encryption of data for communication.

In the end-user environment (phase 7) Smart card ICs are used in a wide range of applications to assure authorised conditional access. Examples of such are transportation or access management. 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.

The system integrators such as the terminal software developer may use samples of the TOE during the development phases for their testing purposes. These samples do not differ from the TOE, they do not have any additional functionality used for testing.

Note: The phases from TOE Delivery to phase 7 of the smart card life cycle are not part of the TOE construction process in the sense of this Security Target. Information about those phases is just included to describe how the TOE is used after its construction. Nevertheless the security features of the TOE cannot be disabled in these phases.

1.4.6 Interface of the TOE

The electrical interface of the TOE consists of the pads to connect the RF antenna. The functional interface is defined by the commands implemented by the TOE and described in [9].

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

1.4.7 General IT features of the TOE

The TOE IT functionality consists of:

- Tamper resistant data storage
- Control of operation conditions to provide correct operation in the specified range
- Data communication via contact-less interface
- Strong authentication mechanism to prevent unauthorised use
- Access management to separate different sectors
- Data blocks for data storage
- Secure configuration in the field
- Random ID to exacerbate tracing of end-users

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 Common Criteria version 3.1:

- Common Criteria, Part 1: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 1, September 2006, CCMB-2006-09-001, [1]
- Common Criteria, Part 2: Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements, Version 3.1, Revision 2, September 2007, CCMB-2007-09-002, [2]
- Common Criteria, Part 3: Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, Version 3.1, Revision 2, September 2007, CCMB-2007-09-003, [3]

For the evaluation the following methodology will be used:

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 2, September 2007, CCIMB-2007-09-004, [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 **EAL4 augmented**. The augmentations to EAL4 are ALC_DVS.2 and AVA_VAN.5. In addition the Security Target is augmented using the component ASE_TSS.2 which is chosen to include architectural information on the security functionality of the TOE.

2.3 PP Claim

This Security Target claims conformance to the following Protection Profile:

Security IC Platform Protection Profile, Version 1.0, 15.06.2007, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0035, [7].

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

2.4 Conformance Claim rationale

According to section 2.3 this Security Target claims conformance to the Protection Profile “Security IC Platform Protection Profile” [7].

The TOE type defined in section 1.3.2 of this Security Target is a Smart Card comprising a hardware platform and a fixed software package, together with guidance documentation. This is consistent with the TOE definition for a Security IC in

section 1.2.2 of [7], since the Security IC is a part of the Smart Card comprising a hardware platform and a fixed software package.

The sections of this document where security problem definition, objectives and security requirements are defined clearly state which of these items are taken from the Protection Profile and which are added in this ST. Therefore this is not repeated here. Moreover, all additional stated items in this ST do not contradict 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 target (EAL4+) 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”, [7].

3. Security Problem Definition

This Security Target claims conformance to the Security IC Platform Protection Profile, [7]. The Assets, Assumptions, Threats and Organisational Security Policies are completely taken from the Protection Profile. In the following only the extension of the different sections are described in detail and the items taken from the Protection Profile are cited for completeness.

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

3.1 Description of Assets

Since this Security Target claims conformance to the PP “Security IC Platform Protection Profile”, [7], the assets defined in section 3.1 of the Protection Profile are cited here for completeness.

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, and configuration data,
- Initialisation data and pre-personalisation data, specific development aids, test and characterisation related data, material for software development support, and photomasks.

3.2 Threats

Since this Security Target claims conformance to the PP “Security IC Platform Protection Profile” [7], 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 3. 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
T.Abuse-Func	Abuse of Functionality
T.RND	Deficiency of Random Numbers

Considering the Application Note 5 of [7] the following additional threats are defined in this Security Target:

T.Data-Modification — Unauthorised data modification

User data stored by the TOE may be modified by unauthorised subjects. This threat applies to the processing of modification commands received by the TOE, it is not concerned with verification of authenticity.

T.Impersonate — Impersonating authorised users during authentication

An unauthorised subject may try to impersonate an authorised subject during the authentication sequence, e.g. by a man-in-the middle or replay attack.

T.Cloning — Cloning

All data stored on the TOE (including keys) may be read out in order to create a duplicate.

3.3 Organisational Security Policies

Since this Security Target claims conformance to the PP “Security IC Platform Protection Profile” [7], the Organisational Security Policies of the Protection Profile are applied here also.

Table 4. Organisational Security Policies defined by the Protection Profile

Name	Title
P.Process-TOE	Protection during TOE Development and Production

Regarding the Application Note 6 of [7] the following additional policies are defined in this Security Target:

P.MAC — Integrity during communication

The TOE shall provide the possibility to protect the contact-less communication from modification or injections. This includes especially the possibility to detect replay or man-in-the-middle attacks within a session.

P.No-Trace — Un-traceability of end-users

The TOE shall provide the ability that authorised subjects can prevent that end-user of TOE may be traced by unauthorised subjects without consent. Tracing of end-users may happen by performing a contact-less communication with the TOE when the end-user is not aware of it. Typically this involves retrieving the UID or any freely accessible data element.

The following policies are part of this Security Target because the TOE implements Security IC Embedded Software that addresses the assumptions A.Plat-Appl and A.Resp-Appl made in [7].[1]

P.Plat-Appl — Usage of hardware platform

The Security IC Embedded Software uses the TOE hardware platform according to the assumption A.Plat-Appl defined in [7].

P.Resp-Appl — Treatment of user data

The Security IC Embedded Software treats user data according to the assumption A.Resp-Appl defined in [7].

3.4 Assumptions

Since this Security Target claims conformance to the PP "Security IC Platform Protection Profile" [7], the assumptions defined in section 3.4 of the Protection Profile are valid for this Security Target. Note that the assumptions A.Plat-Appl and A.Resp-Appl are missing in the following table because they were re-assigned to organisational security policies (see section 3.3).

Table 5. Assumptions defined in the Protection Profile

Name	Title
A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation

The following assumptions are made in addition in this Security Target:

A.Secure_Values — Usage of secure values

Only confidential and secure keys shall be used to set up the authentication and access rights. These values are generated outside the TOE and they are downloaded to the TOE.

A.Terminal_Support — Terminal support to ensure integrity

The terminal verifies information sent by the TOE in order to ensure integrity of the communication.

Regarding the Application Notes 7 and 8 of [7] this Security Target defines two additional assumptions regarding specific security functionality.

[1] The Common Criteria do not explicitly allow re-assigning of Assumptions from a PP to OSPs in a ST, but they also do not explicitly forbid those re-assignments. Since it is allowed to re-assign objectives for the environment to objectives for the TOE (see [1], Annex D.2) theses operations are considered valid for this ST.

4. Security Objectives

This chapter contains the following sections: “Security Objectives for the TOE”, “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 [7]:

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 [7] the following additional security objectives are defined based on additional functionality provided by the TOE as specified below.

O.Access-Control — Access Control

The TOE must provide an access control mechanism for data stored by it. The access control mechanism shall apply to all operations for data elements and to reading and modifying security attributes as well as authentication data. The cryptographic keys used for authentication shall never be output.

O.Authentication — Authentication

The TOE must provide an authentication mechanism in order to be able to authenticate authorised users. The authentication mechanism shall be resistant against replay and man-in-the-middle attacks.

O.MAC — Integrity-protected Communication

The TOE must be able to protect the communication by adding a MAC. This shall be mandatory for commands that modify data on the TOE and optional on read commands. In addition a security attribute shall be available to mandate MAC on read commands, too. Usage of the protected

communication shall also support the detection of injected and bogus commands within the communication session before the protected data transfer.

O.No-Trace — Preventing Traceability

The TOE must be able to prevent that the TOE end-user can be traced. This shall be done by providing an option that disables the transfer of privacy-related information that is suitable for tracing an end-user by an unauthorised subject.

Note that the following two objectives are identical to the objectives OE.Plat-Appl and OE.Resp-Appl defined in section 4.2, “Security Objectives for the Security IC Embedded Software development Environment”, in [7].[2]

O.Plat-Appl — Usage of hardware platform

To ensure that the TOE is used in a secure manner the Security IC Embedded Software shall be designed so that the requirements from the following documents are met: (i) hardware data sheet for the TOE, (ii) TOE application notes, and (iii) findings of the TOE evaluation reports relevant for the Security IC Embedded Software.

O.Resp-Appl — Treatment of user data

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

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

4.2 Security Objectives for the Operational Environment

According to the Protection Profile [7], the following security objectives for the environment are specified:

Table 7. Security objectives for the environment, taken from the PP

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

Note that the security objectives for the environment OE.Plat-Appl and OE.Resp-Appl are missing in Table 7 because they were re-assigned to security objectives for the TOE (see section 4.1).

The following additional security objectives for the environment are defined in this Security Target:

[2] CC Part 1 ([1], Annex D.2) permits explicitly, that the ST-author “*may specify that certain objectives for the operational environment in the PP are security objectives for the TOE in the ST. This is called re-assigning a security objective.*”

OE.Secure_Values	Generation of secure values The environment shall generate confidential and secure keys for authentication purpose. These values are generated outside the TOE and they are downloaded to the TOE during the personalisation or usage in phase 5 to 7
OE.Terminal_Support	Terminal support to ensure integrity The terminal shall verify information sent by the TOE in order to ensure integrity of the communication. This involves checking of MAC values, verification of redundancy information according to the cryptographic protocol and secure closing of the communication session.

4.3 Security Objectives Rationale

Section 4.4 of the Protection Profile provides a rationale how the assumptions, threats, and organisational security policies are addressed by the objectives that are subject of the PP “Security IC Platform Protection Profile”. The following table reproduces the table in section 4.4 of [7].

Table 8. Security Objectives versus Assumptions, Threats or Policies

Assumption, Threat or OSP	Security Objective	Note
A.Plat-Appl	*OE.Plat-Appl*	*(Phase 1)* *Covered by P.Plat-Appl respectively O.Plat-Appl in the ST*
A.Resp-Appl	*OE.Resp-Appl*	*(Phase 1)* *Covered by P.Resp-Appl respectively O.Resp-Appl in the ST*
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 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 threats and organisational security policies.

Table 9. Additional Security Objectives versus Threats or Policies

Threat/Policy	Security Objective	Note
A.Secure_Values	OE.Secure_Values	(Phase 5 – 6)
A.Terminal_Support	OE.Terminal_Support	(Phase 7)
T.Data-Modification	O.Access-Control OE.Terminal_Support	
T.Impersonate	O.Authentication	
T.Cloning	O.Access-Control O.Authentication	
P.MAC	O.MAC OE.Terminal_Support	
P.No-Trace	O.No-Trace O.Access-Control O.Authentication	
P.Plat-Appl	O.Plat-Appl	Covers OE.Plat-Appl of the PP.
P.Resp-Appl	O.Resp-Appl	Covers OE.Resp-Appl of the PP.

The justification related to the assumption “Generation of secure values (A.Secure_Values)” is as follows:

Since OE.Secure_Values requires using secure values for the configuration of the authentication and access control as assumed in A.Secure_Values, the assumption is covered by the objective.

The justification related to the assumption “Terminal support to ensure integrity (A.Terminal_Support)” is as follows:

The objective OE.Terminal_Support is an immediate transformation of the assumption A.Terminal_Support, therefore it covers the assumption.

The justification related to the threat “Unauthorised data modification (T.Data-Modification)” is as follows:

According to threat T.Data-Modification the TOE shall avoid that user data stored by the TOE may be modified by unauthorised subjects. The objective O.Access-Control requires an access control mechanism that limits the ability to modify data elements stored by the TOE. The terminal must provide support by checking the TOE responses, which is required by OE.Terminal_Support. Therefore T.Data-Modification is covered by these two objectives.

The justification related to the threat “Impersonating authorised users during authentication (T.Impersonate)” is as follows:

The threat is related to the fact that an unauthorised subject may try to impersonate an authorised subject during authentication, e.g. by a man-in-the middle or replay attack.

The goal of O.Authentication is that an authentication mechanism is implemented in the TOE that prevents these attacks. Therefore the threat is covered by O.Authentication.

The justification related to the threat “Cloning (T.Cloning)” is as follows:

The concern of T.Cloning is that all data stored on the TOE (including keys) may be read out in order to create a duplicate. The objectives O.Authentication together with O.Access-Control require that unauthorised users cannot read any information that is restricted to the authorised subjects. The cryptographic keys used for the authentication are stored inside the TOE protected by O.Access-Control. This objective states that the TOE shall never output any keys used for authentication. Therefore the two objectives cover T.Cloning.

The justification related to the policy “Integrity during communication (P.MAC)” is as follows:

The policy P.MAC requires the TOE to provide the possibility to protect the contactless communication from modification or injections. This includes especially the possibility to detect replay or man-in-the-middle attacks within a session. O.MAC requires that a security attribute for the card contains an option that the communication must be MACed. In order to ensure the security the terminal must support the TOE by checking the MAC in the TOE responses, which is goal of the objective OE.Terminal_Support. Therefore both objectives cover the policy.

The justification related to the policy “Un-traceability of end-users (P.No-Trace)” is as follows:

The policy requires that the TOE has the ability to prevent tracing of end-users. Tracing can be performed with the UID or with any freely accessible data element stored by the TOE. The objective O.No-Trace requires that the TOE shall provide an option to prevent the transfer of any information that is suitable for tracing an end-user by an unauthorised subject, which includes the UID. The objectives O.Authentication and O.Access-Control provide means to authorise subjects and to implement access control to data elements in a way that unauthorised subjects can read any element usable for tracing. Therefore the policy is covered by the three objectives.

The justification related to the policy “Usage of hardware platform (P.Plat-Appl)” is as follows:

The policy states that the Security IC Embedded Software uses the TOE hardware according to the respective PP assumption. O.Plat-Appl has the same objective as OE.Plat-Appl defined in the PP. Since O.Plat-Appl has the same objective as OE.Plat-Appl, OE.Plat-Appl is based on the PP assumption A.Plat-Appl and in the ST the decision was made to cover the assumption by a policy, the objective covers the policy.

The justification related to the policy “Treatment of user data (P.Resp-Appl)” is as follows:

In analogy to P.Plat-Appl, the policy P.Resp-Appl is covered in the same way by the objective O.Resp-Appl.

The justification of the additional threats and policies 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”, [7] 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 10 below shows all SFRs which are specified in the Protection Profile Security IC Platform Protection Profile [7] (in alphabetical order). 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 10. SFRs taken from the PP

SFR	Title	Defined in ...
FAU_SAS.1	Audit storage	PP, Section 5.3
FCS_RNG.1	Quality metric for random numbers	PP, Section 5.1
FDP_IFC.1	Subset information flow control	CC, Part 2
FDP_ITT.1	Basic internal transfer protection	CC, Part 2
FMT_LIM.1	Limited capabilities	PP, Section 5.2
FMT_LIM.2	Limited availability	PP, Section 5.2
FPT_FLS.1	Failure with preservation of secure state	CC, Part 2
FPT_ITT.1	Basic internal TSF data transfer protection	CC, Part 2
FPT_PHP.3	Resistance to physical attack	CC, Part 2
FRU_FLT.2	Limited fault tolerance	CC, Part 2

The protection profile does not fill in all operations of the components, the remaining operations are filled in the following.

For the SFR FAU_SAS.1 the PP [7] leaves the assignment operation open for the non-volatile memory type in which initialisation data, pre-personalisation 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 [7].

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* [3] with the capability to store *the Initialisation Data and/or Pre-personalisation Data and/or supplements of the Security IC Embedded Software* [4] in the *EEPROM* [5].

For FCS_RNG.1.1 the PP [7] 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 [7] 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 operations of FCS_RNG.1 the original operations defined in chapter 5 of the PP [7] have been replaced by the open operations of the partially filled in operations in the statement of the security requirements in chapter 6 of [7] 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.1.1	The TSF shall provide a *physical* [6] random number generator that implements *total failure test of the random source* [7].
FCS_RNG.1.2	The TSF shall provide random numbers that meet *independent bits with Shannon entropy of 7.976 bits per octet* [8].
Dependencies:	No dependencies.
Note:	Application Note 20 in [7] 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. The TOE features a hardware test which is called by the Security IC Embedded Software. 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 special function register.

6.1.2 Additional SFRs regarding access control

Access Control Policy

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

[3] [assignment: *list of subjects*]

[4] [assignment: *list of audit information*]

[5] [assignment: *type of persistent memory*]

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

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

[8] [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 following roles are supported:

- The **Personaliser** who can personalise the TOE.
- The **Card Administrator** who can change security attributes which do not require being changed in the field.
- The **Card Manager** who can change security attributes which may require being changed in the field.
- The **Card Security Level Manager** who can switch the card to security level 3.
- The **Card User** who can perform operations with blocks.
- The **Originality Key User** who can authenticate himself to prove the authenticity of the Card.

Note that multiple subjects may have the same role, e.g. for every sector there are two Card Users (identified by the respective “Key A” and “Key B” for this sector). The assigned rights to the Card Users can be different, which allows having more or less powerful Card Users. There are also more than one Originality Key Users.

Any other subject belongs to the role **Anybody** which is not modelled explicitly in the policy because no access rights are granted to this role. This role includes the card holder (i.e. end-user) and any other subject e.g. an attacker.

The objects are

- **blocks** that are grouped in **sectors**. Each sector consists of either 4 or 16 blocks. One block of each sector contains the access conditions and is called **sector trailer**.

The operations that can be performed with the objects and security attributes are

- **read** data from a block,
- **write** data to a block and
- **read** or **modify** the security attributes.

The security attributes are

- the **Field Configuration Block**,
- the **sector trailer** for a sector and
- the **security level** of the TOE.

Note that subjects are authorised by cryptographic keys. These keys are considered as authentication data and not as security attributes. The TOE stores a dedicated cryptographic key for every subject. The key of the Card Administrator is called “Card Master Key” and the key for the Card Manager is called “Card Configuration Key”. The Card Security Level Manager key is called “Level 3 Switch Key”. The keys of the Card Users are called “AES Sector Keys”. Since there are two keys for every sector the keys are called “AES Sector Key A” and “AES Sector Key B” or in short “Key A” and “Key B”. The keys of the Originality Key User are called “Originality Keys”.

The TOE shall meet the requirements “Security roles (FMT_SMR.1)” as specified below.

FMT_SMR.1	**Security roles**
Hierarchical to:	No other components.

FMT_SMR.1.1	The TSF shall maintain the roles *Personaliser, Card Administrator, Card Manager, Card Security Level Manager, Card User and Originality Key User* [9].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification

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

FDP_ACC.1	**Subset access control**
Hierarchical to:	No other components.
FDP_ACC.1.1	The TSF shall enforce the *Access Control Policy* [10] on *all subjects, objects, operations and attributes defined by the Access Control Policy* [11].
Dependencies:	FDP_ACF.1 Security attribute based access control

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

FDP_ACF.1	**Security attribute based access control**
Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the *Access Control Policy* [12] to objects based on the following: *all subjects, objects and attributes* [13].
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 Personaliser can change all blocks.* • *For every sector the Card User can read or write a data block based on the access control settings in the respective sector trailer.* [14]
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none* [15]
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the *rules:*

[9] [assignment: the authorised identified roles]

[10] [assignment: access control SFP]

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

[12] [assignment: access control SFP]

[13] [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]

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

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

- *The block 0 (first block of the first sector) can not be modified.* [16]

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

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

FMT_MSA.3 **Static attribute initialisation**

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the *Access Control Policy* [17] to provide *permissive* [18] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow *no subject* [19] 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

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

FMT_MSA.1 **Management of security attributes**

Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the *Access Control Policy* [20] to restrict the ability to *modify* [21] the security attributes *Field Configuration Block, security level and sector trailers* [22] to *the Card Manager, Card Administrator,Card Security Level Manager and Card User, respectively* [23].

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.

16 [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]
17 [assignment: access control SFP, information flow control SFP]
18 [selection, choose one of: restrictive, permissive, [assignment: other property]]
19 [assignment: the authorised identified roles]
20 [assignment: access control SFP(s), information flow control SFP(s)]
21 [selection: change_default, query, modify, delete, [assignment: other operations]]
22 [assignment: list of security attributes]
23 [assignment: the authorised identified roles]

FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: *Authenticate a user,* *Invalidating the current authentication state based on the functions: Issuing a request for authentication, Occurrence of any error during the execution of a command, Reset, Switching the security level of the TOE, DESELECT according to ISO 14443-3, explicit authentication reset;* *Finishing the personalisation phase by explicit request of the Personaliser,* *Changing a security attribute.* [24]
Dependencies:	No dependencies

The TOE shall meet the requirement “Import of user data with security attributes (FDP_ITC.2)” as specified below.

FDP_ITC.2	**Import of user data with security attributes**
Hierarchical to:	No other components.
FDP_ITC.2.1	The TSF shall enforce the *Access Control Policy* [25] when importing user data, controlled under the SFP, from outside of the TSC.
FDP_ITC.2.2	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.
FDP_ITC.2.4	The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.
FDP_ITC.2.5	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: *no additional rules* [26].
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency

The TOE shall meet the requirement “Inter-TSF basic TSF data consistency (FPT_TDC.1)” as specified below.

[24] [assignment: list of management functions to be provided by the TSF]

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

[26] [assignment: additional importation control rules]

FPT_TDC.1	**Inter-TSF basic TSF data consistency**
Hierarchical to:	No other components.
FPT_TDC.1.1	The TSF shall provide the capability to consistently interpret *data blocks* [27] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2	The TSF shall use *the rules: data blocks can always be modified by the write operation. Sector trailers must have a specific format* [28] when interpreting the TSF data from another trusted IT product.
Dependencies:	No dependencies.
Application Note:	The TOE does not interpret the *contents* of the data, e.g. it cannot determine if data stored in a specific block is an identification number that adheres to a specific format. For sector trailers the TOE enforces a specific format.

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 functions.

- The TOE end-user does normally not belong to the group of authorised users (Card Administrator, Card Manager, Card Security Level Manager, Card User, Originality Key User), but is regarded as 'Anybody' by the TOE. This means that the TOE cannot determine if it is used by its intended end-user (in other words: it cannot determine if the current card holder is the owner of the card).
- The Personaliser is very powerful, although the role is limited to Security Level 0. The Personaliser can write all blocks and therefore change all data and the sector trailers.
- Switching of the security level is an integral part of the TOE security. The TOE is switched from security level 0 to security level 1 or 3 (refer to section 1.4.2.2) at the end of the personalisation phase. The security level can be increased by the Card Security Level Manager afterwards.

6.1.3 Additional SFRs regarding confidentiality, integrity and authentication

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* [29] in accordance with a specified cryptographic algorithm *Advanced*

[27] [assignment: list of TSF data types]

[28] [assignment: list of interpretation rules to be applied by the TSF]

[29] [assignment: list of cryptographic operations]

Encryption Standard (AES) [30] and cryptographic key sizes *of 128 bit* [31] that meet the following *list of standards* [32]:

FIPS PUB 197 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, ADVANCED ENCRYPTION STANDARD (AES), National Institute of Standards and Technology, 2001 November 26.

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.

The TOE shall meet the requirement “User identification before any action (FIA_UID.2)” as specified below.

FIA_UID.2	**User identification before any action**
Hierarchical to:	FIA_UID.1
FIA_UID.2.1	The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	No dependencies.
Application Note:	Identification of a user is performed upon an authentication request based on the key block number. For example, if an authentication request for key number 0x9000 is issued after selecting the Card, the user is identified as the Card Administrator.

The TOE shall meet the requirement “User authentication before any action (FIA_UAU.2)” as specified below.

FIA_UAU.2	**User authentication before any action**
Hierarchical to:	FIA_UAU.1
FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	FIA_UID.1 Timing of identification

The TOE shall meet the requirement “Multiple authentication mechanisms (FIA_UAU.5)” as specified below.

FIA_UAU.5	**Multiple authentication mechanisms**
Hierarchical to:	No other components.

[30] [assignment: cryptographic algorithm]
[31] [assignment: cryptographic key sizes]
[32] [assignment: list of standards]

FIA_UAU.5.1	The TSF shall provide *'none' and cryptographic authentication* [33] to support user authentication.
FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the *following rules:* • *The 'none' authentication is performed with anyone who communicates with the TOE in security level 0. The 'none' authentication implicitly and solely authenticates the Personaliser subject.* • *The cryptographic authentication is used in security level 0 to authenticate the Originality Key User.* • *The cryptographic authentication is used in security level 1 to authenticate the Originality Key User and the Card Security Level Manager.* • *The cryptographic authentication is used in security level 3 to authenticate the Originality Key User, Card Administrator, Card Manager and the Card User* [34].
Dependencies:	No dependencies.

The TOE shall meet the requirement "Management of TSF data (FMT_MTD.1)" as specified below.

FMT_MTD.1	**Management of TSF data**
Hierarchical to:	No other components.
FMT_MTD.1.1	The TSF shall restrict the ability to *modify* [35] the *security attributes and authentication data* [36] to *the Personaliser, Card Administrator, Card Manager, Card Security Level Manager and Card User* [37].
Refinement:	The detailed management abilities are: • The Personaliser can change all security attributes as well as all keys except the keys of the Originality Key User. • The Card Administrator can change the Level 3 Switch Key and the Card Master Key. • The Card Manager can change the Field Configuration Block and the Card Configuration Key. • The Card Security Level Manager can switch the security level of the TOE to security level 3. • The Card User may change the AES Sector Keys and the sector trailer if the access conditions in the corresponding sector trailer grants him this right.

[33] [assignment: list of multiple authentication mechanisms]
[34] [assignment: rules describing how the multiple authentication mechanisms provide authentication]
[35] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
[36] [assignment: list of TSF data]
[37] [assignment: the authorised identified roles]

Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

The TOE shall meet the requirement “Trusted path (FTP_TRP.1)” as specified below.

FTP_TRP.1	**Trusted path**
Hierarchical to	No other components.
FTP_TRP.1.1	The TSF shall provide a communication path between itself and *remote* [38] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *modification* [39].
FTP_TRP.1.2	The TSF shall permit *remote users* [40] to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for *authentication requests, data integrity verification for data transfers*[41].
Dependencies:	No dependencies.

The TOE shall meet the requirement “Cryptographic key destruction (FCS_CKM.4)” as specified below.

FCS_CKM.4	**Cryptographic key destruction**
Hierarchical to:	No other components.
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *overwriting of memory* [42] that meets the following: *none* [43].
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]

6.1.4 Additional SFRs regarding the robustness

The TOE shall meet the requirement “Replay detection (FPT_RPL.1)” as specified below.

FPT_RPL.1	**Replay detection**
Hierarchical to:	No other components.
FPT_RPL.1.1	The TSF shall detect replay for the following entities: *authentication requests, data integrity verification for data transfers*[44].

[38] [selection: remote, local]
[39] [selection: modification, disclosure, [assignment: other types of integrity or confidentiality violation]]
[40] [selection: the TSF, local users, remote users]
[41] [selection: initial user authentication,[assignment: other services for which trusted path is required]]
[42] [assignment: cryptographic key destruction method]
[43] [assignment: list of standards]

FPT_RPL.1.2	The TSF shall perform *rejection of the request* [45] when replay is detected.
Dependencies:	No dependencies.

The TOE shall meet the requirement “Unlinkability (FPR_UNL.1)” as specified below.

FPR_UNL.1	**Unlinkability**
Hierarchical to:	No other components.
FPR_UNL.1.1	The TSF shall ensure that *unauthorised subjects other than the card holder* [46] are unable to determine whether *any operation of the TOE* [47] *were caused by the same user* [48].
Dependencies:	No dependencies.

6.2 Security Assurance Requirements

Table 11 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 ASE_TSS.2 which is chosen as an augmentation in this ST to give architectural information on the security functionality of the TOE.

The column “Note” 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 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”, [7] that must be adapted for EAL4 are described in section 6.2.1.

Table 11. Security Assurance Requirements according to PP

SAR	Title	Note
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

[44] [assignment: list of identified entities]
[45] [assignment: list of specific actions]
[46] [assignment: set of users and/or subjects]
[47] [assignment: list of operations]
[48] [selection: were caused by the same user, are related as follows[assignment: list of relations]]

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

6.2.1 Refinements of the TOE Security Assurance Requirements

The ST claims conformance to the Protection Profile “Security IC Platform Protection Profile”, and therefore it has to be conform to the refinements of the TOE security assurance requirements made by the PP. Refinements are defined in [7] for the Security Assurance Requirements ALC_DEL.1, ALC_DVS.2, ALC_CMS.4, ALC_CMC.4, ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ATE_COV.2, AGD_OPE.1, AGD_PRE.1 and AVA_VAN.5. With regard to Application Note 22 of the PP the ST does not claim conformance to affected hierarchically higher assurance requirements.

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” 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 12. Security Requirements versus Security Objectives

Objective	TOE Security Functional Requirements
O.Leak-Inherent	FDP_ITT.1 “Basic internal transfer protection”

Objective	TOE Security Functional Requirements
	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, 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	Cf. O.Plat-Appl in Table 13
OE.Resp-Appl	Cf. O.Resp-Appl in Table 13
OE.Process-Sec-IC	Not applicable

The Security Target additionally defines the SFRs for the TOE that are listed in Table 13. The following table gives an overview, how the requirements are combined to meet the security objectives.

Table 13. Mapping of security objectives and requirements

Objective	TOE Security Functional Requirement
O.Access-Control	FMT_SMR.1 FDP_ACC.1 FDP_ACF.1 FMT_MSA.3 FMT_MSA.1 FMT_SMF.1 FDP_ITC.2 FPT_TDC.1 FCS_CKM.4

Objective	TOE Security Functional Requirement
	FMT_MTD.1
O.Authentification	FCS_COP.1 FIA_UID.2 FIA_UAU.2 FIA_UAU.5 FTP_TRP.1 FPT_RPL.1
O.MAC	FCS_COP.1 FTP_TRP.1 FPT_RPL.1
O.No-Trace	FPR_UNL.1
O.Plat-Appl	all SFR from the PP
O.Resp-Appl	all SFR defined additionally in the ST

The justification related to the security objective “Access Control” (O.Access-Control) is as follows:

The SFR FMT_SMR.1 defines the roles of the Access Control Policy. The SFR FDP_ACC.1 and FDP_ACF.1 define the rules and FMT_MSA.3 and FMT_MSA.1 the attributes that the access control is based on. FMT_MTD.1 provides the rules for the management of the authentication data. The management functions are defined by FMT_SMF.1. Since the TOE stores data on behalf of the authorised subjects import of user data with security attributes is defined by FDP_ITC.2. The SFR FPT_TDC.1 requires the TOE to consistently interpret data blocks (sector trailers). The TOE will honour the respective file formats and boundaries. Since cryptographic keys are used for authentication (refer to O.Authentication), these keys have to be removed if they are no longer needed for the access control. This is required by FCS_CKM.4. These nine SFR together provide an access control mechanism as required by the objective O.Access-Control.

The justification related to the security objective “Authentication” (O.Authentication) is as follows:

The SFR FCS_COP.1 requires that the TOE provides the basic cryptographic algorithm that can be used to perform the authentication. The SFR FIA_UID.2, FIA_UAU.2 and FIA_UAU.5 together define that users must be identified and authenticated before any action. FTP_TRP.1 requires a trusted communication path between the TOE and remote users, FTP_TRP.1.3 especially requires “authentication requests”. Together with FPT_RPL.1 which requires a replay detection for these authentication requests the six SFR fulfil the objective O.Authentication.

The justification related to the security objective “Integrity-protected Communication” (O.MAC) is as follows:

The SFR FCS_COP.1 requires that the TOE provides the basic cryptographic algorithms that can be used to compute a MAC which can protect the integrity of the communication. FTP_TRP.1 requires a trusted communication path between the TOE

and remote users, FTP_TRP.1.3 especially requires “data integrity verification for data transfers on request of the file owner”. Together with FPT_RPL.1 which requires a replay detection for these data transfers the three SFR fulfil the objective O.MAC.

The justification related to the security objective “Preventing Traceability” (O.No-Trace) is as follows:

The SFR FPR_UNL.1 requires that unauthorised subjects other than the card holder are unable to determine whether any operation of the TOE was caused by the same user. This meets the objective O.No-Trace.

The justification related to the security objective “Usage of hardware platform” (O.Plat-Appl) is as follows:

The objective was transferred from an environment objective in the PP to a TOE objective in this ST. Its goal is to ensure that the hardware platform is used in a secure manner, which is based on the insight that hardware and software have to supplement each other in order to build a secure whole. The ST claims conformance to the PP and the PP SFR do cover the PP TOE objectives. The PP uses the environment objective OE.Plat-Appl to ensure appropriate software support for its SFR, but since the TOE does now consist of hardware and software the PP SFR do also apply to the Security IC Embedded Software and thereby all PP SFR fulfil the objective O.Plat-Appl. In other words: The software support required by the hardware-focused PP is now included in this combined hardware-software TOE and both hardware and software fulfil the PP SFR.

The justification related to the security objective “Treatment of user data” (O.Resp-Appl) is as follows:

The objective was transferred from an environment objective in the PP to a TOE objective in this ST. The objective is that “security relevant User Data (especially cryptographic keys) are treated by the Security IC Embedded Software as required by the security needs of the specific application context.” The application context is defined by the security environment described in this ST. The additional SFR defined in this ST do address the additional TOE objectives of the ST based on the ST security environment, therefore O.Resp-Appl is fulfilled by the additional ST SFR.

6.3.2 Dependencies of security functional requirements

The dependencies listed in the Protection Profile [7] are independent form the additional dependencies listed in the table below. The dependencies of the Protection Profile are fulfilled within the Protection Profile and at least one dependency is considered to be satisfied.

The following discussion demonstrates how the dependencies defined by Part 2 of the Common Criteria for the requirements specified in sections 6.1.3 and 6.1.4 are satisfied.

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

Table 14. Dependencies of security functional requirements

Security Functional Requirement	Dependencies	Fulfilled by security requirements in this ST
FMT_SMR.1	FIA_UID.1	Yes (by FIA_UID.2)

Security Functional Requirement	Dependencies	Fulfilled by security requirements in this ST
FDP_ACC.1	FDP_ACF.1	Yes
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Yes Yes
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes Yes
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes (both) Yes Yes
FMT_SMF.1	No dependencies	
FDP_ITC.2	FDP_ACC.1 or FDP_IFC.1 FTP_ITC.1 or FTP_TRP.1 FPT_TDC.1	Yes (both) Yes (by FTP_TRP.1) Yes
FPT_TDC.1	No dependencies	
FCS_COP.1	FDP_ITC.1, or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	Yes (FDP_ITC.2) Yes
FIA_UID.2	No dependencies	
FIA_UAU.2	FIA_UID.1	Yes (by FIA_UID.2)
FIA_UAU.5	No dependencies	
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	Yes Yes
FTP_TRP.1	No dependencies	
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Yes (FDP_ITC.2)
FPT_RPL.1	No dependencies	
FPR_UNL.1	No dependencies	

As shown in the table above all dependencies are satisfied.

6.3.3 Rationale for the Assurance Requirements

The selection of assurance components is based on the underlying Protection Profile [7]. 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 algorithm and the access control function used to implement the Access Control Policy. The security objectives defined in the PP can be seen as “low-level protection” objectives, while the additional security objectives defined in this ST are “high-level protection” objectives. For example, O.MAC states that the integrity of the communication can be protected by adding a MAC. While this ensures the rather high-level goal that the communication is protected, this overall goal is ensured with the help of the PP objective that prevent attacks on the key and the cryptographic implementation like probing or fault injection attacks.

7. TOE Summary Specification

This chapter is divided in the sections “Portions of the TOE Security Function” 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 chapter 6.

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

Note: Parts of the security functionality are configured at the end of phase 3 and all security functionalities are already active during the delivery from phase 3 to phase 4.

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

7.1.1 Security Services

SS.AUTH: Authentication

The TOE provides an authentication mechanism to separate authorised subjects from unauthorised subjects. The authentication of subjects is performed by a cryptographic challenge-response. The TOE supports the cryptographic algorithm 128-bit AES; according to FIPS PUB 197 [11]. A hardware random number generator according to AIS31, functionality class P2, is used to protect the authentication against attacks like replay.

SS.AUTH identifies the user to be authenticated by the key block number indicated in the authentication request. In security level 0 the TOE identifies and authenticates the Personaliser by default, in addition the Originality Key User can be identified with an explicit authentication request. In the other security levels SS.AUTH by default and before any authentication request identifies and authenticates the role Anybody. The roles Card Administrator, Card Manager, Card Security Level Manager, Card User and Originality Key User are authenticated during the authentication request by the knowledge of the respective cryptographic key.

The authentication state is remembered by SS.AUTH and the authentication needs not to be performed again as long as none of the following events occur: Occurrence of any error during the processing of a command, Reset, Switching the security level of the TOE, DESELECT according to ISO 14443-3, explicit authentication reset. These events will reset the authentication state to the default (Anybody). Of course a new authentication (possibly by another user) will invalidate the old authentication state, too. The authentication state will be invalidated as soon as the authentication request is received.

SS.ACC_CTRL: Access Control

SS.ACC_CTRL provides an access control mechanism to the objects and security attributes that are part of the Access Control Policy. The access control mechanism assigns Card Users to 2 different groups of operations on blocks. The operations are “read” and “write”. There are several sets of predefined access conditions which may be assigned to each sector. These sets can also contain the access condition “never” for

one group of operations. Card Users can also modify the sector trailer or the AES sector keys, if the access conditions allow this.

The Originality Key User is not allowed to perform any action on objects, but with a successful authentication he can prove the authenticity of the Card.

The Card Administrator can change the Level 3 Switch Key and the Card Master Key.

The Card Manager can modify the Field Configuration Block, which are attributes that may have to be changed in the field. He is also allowed to change the Card Configuration Key.

The Card Security Level Manager can switch the security level of the card to level 3 by authenticating with the corresponding key.

The Access Control Policy an therefore SS.ACC_CTRL has to take care that all sectors are initialized with permissive default values in the sector trailer, this means the contained access conditions shall allow the Card User to access all blocks.

Finally SS.ACC_CTRL ensures the type consistency of the blocks stored by the TOE. Furthermore size limitations of blocks are obeyed.

SS.MAC: Message Authentication Code

SS.MAC adds data to the communication stream that enables both the TOE and the terminal to detect integrity violations, replay attacks or man-in-the-middle attacks.

The detection mechanism covers all frames exchanged between the terminal and the card up to the current frame. Therefore SS.MAC can detect any injected/modified frame in the communication before the transfer of the frame. Depending on the selected mode it can also detect what frame was injected/modified.

SS.NO_TRACE: Preventing traceability

SS.NO_TRACE provides an option to use a random ID during the ISO14443 anti-collision sequence. If this option is set, the TOE does not send its UID, but generates a new random ID number during every power-on sequence. By this the card cannot be traced any more by simply retrieving its UID. Setting this option is restricted to the Card Manager since it belongs to the Field Configuration Block.

Note that SS.NO_TRACE protects the card specific data that can be read by unauthorised subjects. Card specific information suitable to identify single end-users can still be read out only by the authorised subjects according to the Access Control Policy implemented by SS.ACC_CTRL.

By using SS.NO_TRACE it can be ensured that no unauthorised subject can gain information about the end-user that allows to identify the end-user. As a consequence this does not allow tracing of the end-user, e.g. by setting up a terminal controlled by an attacker. However, SS.NO_TRACE can not prevent that an individual can be traced by observing authorised terminals, either by environmental means like optical observation or technical means like eavesdropping plaintext communication.

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 AES co-processor, the memories, registers, I/O interface and the other system peripherals) during the execution of the IC Dedicated Support Software and the 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 sub-functions: filtering of power supply and clock input as well as monitoring of power supply, the frequency of the clock and the temperature of the chip by means of sensors. 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. Specific functional units of the TOE are equipped with special circuitry to detect a number of single fault injection attacks. The TOE software has additional means to detect integrity violations.

If one of the monitored parameters is out of the specified range, the TOE will enter a secure state. The TOE distinguishes two severity levels of out-of-range conditions and limits the total accepted number of the more severe level. If this maximum is exceeded the TOE disables itself and switches to the TERMINATION state.

The Security IC Embedded Software cannot disable the filters and sensors. In addition the filters and sensors are implemented mostly independent of the other hardware components.

SF.PHY: Protection against Physical Manipulation

The function 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 the EEPROM, (iv) the application data in the EEPROM and RAM including the configuration data in the security row. It also protects User Data or 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 more difficult. These features comprise dedicated shielding techniques for different components and specific encryption and integrity features for the memory blocks. The security feature SF.PHY supports the efficiency of other TSF parts.

SF.LOG: Logical Protection

The function 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 this security function prevents the disclosure of User Data or TSF data stored and/or processed in the smart card IC through the measurement of the power consumption and subsequent complex signal processing. The protection of the TOE comprises different features within the design that support the other security functions.

The cryptographic co-processor includes special features to prevent analysis of shape and amplitude of the power consumption and ensure that the calculation time is independent from any key and plain/cipher text. Additional features comprise the internal clock that is used to prevent the possibility to synchronise the internal operation with the

external clock or to synchronise with the characteristics of the power consumption that can be used as trigger signal to support leakage attacks.

Software measures are implemented to counter timing attacks for security relevant decisions and for the support of the hardware components.

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

SF.COMP: Protection of Mode Control

The function SF.COMP provides a control of the TOE mode for (i) Test Mode and (ii) User Mode. This includes the protection of electronic fuses stored in a protected memory area, the so-called “Security Row”.

The control of the TOE mode according to Test Mode and User Mode prevents the abuse of test functions after TOE delivery. Additionally it also ensures that features used at boot time to configure the TOE cannot be abused. Hardware circuitry determines whether the Test Mode is available or not. If it is available, the TOE starts the IC Dedicated Test Software in the Test Mode. Otherwise, the TOE switches to the User Mode and starts execution of the Security IC Embedded Software. Therefore, once the TOE has left the test phase and every time the TOE is started up the Security IC Embedded Software is executed.

The protection of electronic fuses ensures the secure storage of configuration- and calibration data stored in the Test Mode. The protection of electronic fuses especially ensures that configuration options cannot be changed, abused or influenced in any way. SF.COMP ensures that activation or deactivation of security features cannot be influenced by the Security IC Embedded Software so that the TSF maintain a security domain for its own execution that protects it from interference and tampering.

SF.COMP also provides the possibility to store initialisation data in the so-called "System Settings" area and the block 0 (first block of the first sector). The configuration of the EEPROM memory size is stored in this area. It is also used to store a unique identification for each die and other manufacturing data.

SF.COMP limits the capabilities of the test functions and provides test personnel during phase 3 with the capability to store the initialization data in the EEPROM. The security function SF.COMP maintains the security domain for its own execution that protects it from interference and tampering by untrusted subjects. It also enforces the separation between the security domains of subjects regarding the IC Dedicated Software and the Security IC Embedded Software.

7.2 TOE Summary Specification Rationale

7.2.1 Rationale for TOE security functionality

The following table provides a mapping of SS and SF to SFR. The mapping is described in detail in the text following the table (only in the full version of the Security Target).

Table 15. Mapping of Security Functional Requirements and the TOE Security Functions

	SS.AUTH	SS.ACC_CTRL	SS.MAC	SS.NO_TRACE	SF.OPC	SF.PHY	SF.LOG	SF.COMP
FAU_SAS.1								X
FCS_RNG.1	X							
FDP_IFC.1							X	
FDP_ITT.1							X	
FMT_LIM.1								X
FMT_LIM.2								X
FPT_FLS.1					X			
FPT_ITT.1							X	
FPT_PHP.3						X		
FRU_FLT.2					X			
FMT_SMR.1	X	X						
FDP_ACC.1		X						
FDP_ACF.1		X	X					
FMT_MSA.1		X						
FMT_MSA.3		X						
FMT_SMF.1	X	X						
FDP_ITC.2		X						
FPT_TDC.1		X						
FCS_COP.1	X		X					
FIA_UID.2	X							
FIA_UAU.2	X							
FIA_UAU.5	X							
FMT_MTD.1		X						
FTP_TRP.1	X		X					
FCS_CKM.4		X						
FPT_RPL.1	X		X					
FPR_UNL.1				X				

The "X" means that the TOE Security Function realises 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 ([7], chapter 7) provides further information. Section 7.1 of the PP describes the development and production process of smart cards, 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 [7] 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 [7], Figure 2 in section 1.2.3 and section 7.1.1). The Card Manufacturer has the following roles (i) the Composite Product Manufacturer (Phase 5) and (ii) the Personaliser (Phase 6). If the TOE is delivered after Phase 3 in form of wafers or sawn wafers (dice) he has the role of the IC Packaging Manufacturer (Phase 4) in addition.
Integrated Circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions.
IC Dedicated Software	IC proprietary software embedded in a smart card 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	That part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Support Software might be restricted to certain phases.
IC Dedicated Test Software	That part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter
Initialisation Data	Initialisation Data defined by the TOE Manufacturer to identify the TOE and to keep track of the Security IC's production and further life-cycle phases are considered

	as belonging to the TSF data. These data are for instance used for traceability and for TOE identification (identification data).
Integrated Circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions.
Memory	The memory comprises the RAM, ROM and the EEPROM of the TOE.
MIFARE	Contact-less smart card interface standard, complying with ISO14443A.
Security IC	(as used in the Protection Profile) Composition of the TOE, the Security IC Embedded Software, User Data and the package (the Security IC carrier).
Security IC Embedded Software	Software embedded in a Security IC and normally 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 Security IC product life-cycle. In this evaluation the TOE consist of an IC *and* Security IC Embedded Software.
Security row	First 64 bytes of the EEPROM memory reserved for configuration purposes and to store life-cycle information about the TOE.
Special Function Registers	Registers used to access and configure the functions for the communication with an external interface device, the cryptographic co-processors or other functional blocks.
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.
Test Mode	CPU mode for configuration of the TOE executing the IC Dedicated Test Software. The Test Mode is permanently and irreversible disabled after production testing.
TOE Delivery	The period when the TOE is delivered which is (refer to [7], 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 sawn wafers (dice) or (ii) after Phase 4 (or before Phase 5) if the TOE is delivered in form of packaged products.
TOE Manufacturer	The TOE Manufacturer must ensure that all requirements for the TOE and its development and

	production environment are fulfilled (refer to [7], Figure 2 in section 1.2.3). 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. This includes information about the TOE's configuration, if any is coded in non-volatile non-programmable memories (ROM), in specific circuitry, in non-volatile programmable memories (for instance EEPROM) or a combination thereof.
User Data	All data managed by the Security IC Embedded Software in the application context. User data comprise all data in the final Smartcard IC except the TSF data.
Virtual Card	Mechanism to implement multiple applications (or cards) in one physical object.

8.3 List of Abbreviations

AES	Advanced Encryption Standard.
CC	Common Criteria (Version 3.1 in this ST).
CIU	Contact-less Interface Unit
CPU	Central Processing Unit
EAL	Evaluation Assurance Level.
IC	Integrated circuit.
IT	Information Technology.
MAC	Message Authentication Code.
PP	Protection Profile.
SAR	Security Assurance Requirement.
SFP	Security Function Policy.
SFR	Security Functional Requirement.
SL	Security Level
SOF	Strength of function.
ST	Security Target.
TOE	Target of Evaluation.

TRNG	True Random Number Generator
TSC	TSF Scope of Control.
TSF	TOE Security functions.
TSFI	TSF Interface.
TSP	TOE Security Policy.
VC	Virtual Card

8.4 Bibliography

8.4.1 Evaluation Documents

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

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

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

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 2, September 2007, CCIMB-2007-09-004

[5] Anwendungshinweise und Interpretationen zum Schema, AIS31: Funktionalitäts-klassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 1, 25.09.2001, Bundesamt für Sicherheit in der Informationstechnik

[6] Anwendungshinweise und Interpretationen zum Schema, AIS32: Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema, Version 1, 02.07.2001, Bundesamt für Sicherheit in der Informationstechnik

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

[8] CC Supporting Document, Application of Attack Potential to Smartcards, Version 2.5, Revision 1, CCDB-2008-04-001, April 2008

8.4.2 Developer Documents

[9] Data Sheet, MF1SPLUSx0y1, Mainstream contactless smart card IC for fast and easy solution development, NXP Semiconductors

[10] Guidance, Delivery and Operation Manual, MF1SPLUSx0y1, NXP Semiconductors,

8.4.3 Other Documents

[11] FIPS PUB 197 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, ADVANCED ENCRYPTION STANDARD (AES), National Institute of Standards and Technology, 2001 November 26

[12] ISO/IEC 14443-1:2000 Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 1: Physical characteristics

[13] ISO/IEC 14443-2:2001 Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 2: Radio frequency power and signal interface

[14] ISO/IEC 14443-3:2001 Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 3: Initialization and anticollision

[15] ISO/IEC 14443-4:2001 Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 4: Transmission protocol

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 Patents

Notice is herewith given that the subject device uses one or more of the following patents and that each of these patents may have corresponding patents in other jurisdictions.

<Patent ID> — owned by <Company name>

9.5 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.

MIFARE Plus — 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: 14 May 2010