MF1P(H)x1y1

MIFARE Plus EV1 – Security Target Lite

Rev. 1.3 – 2016-09-27
Final

Evaluation documentation
PUBLIC

Document Information

Info	Content
Keywords	Security Target Lite, NXP Secure Smart Card Controller MF1P(H)x1y1 with IC Dedicated Support Software
Abstract	Evaluation of the MF1P(H)x1y1 developed and provided by NXP Semiconductors, Business Unit Identification, according to the Common Criteria for Information Technology Evaluation Version 3.1 at EAL5 augmented

Rev	Date	Description
1.0	01-March-2016	Initial Version of this Security Target Lite
1.1	25-March-2016	Update based on ITSEF review
1.2	31-March-2016	Update of TOE Reference and References of Components of the TOE
1.3	27-September-2016	Another Update of TOE Reference and References of Components of the TOE

1 ST Introduction

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

1.1 ST Reference

MF1P(H)x1y1 Security Target, 1.3, NXP Semiconductors, 2016-09-27.

1.2 TOE Reference

NXP Secure Smart Card Controller MF1P(H)x1y1, Version 1.3

1.3 TOE Overview

1.3.1 Introduction

NXP has developed the MF1P(H)x1y1 to be used with Proximity Coupling Devices (PCDs) according to ISO14443 Type A [16]. The communication protocol complies to part ISO 14443-3 [17] and 14443-4 [15]. The MF1P(H)x1y1 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 is a smart card comprising a hardware platform and a fixed software package. The software package is stored in non-volatile memory and provides an operating system with a set of functions, used to manage the various kinds of data files stored in the non-volatile EEPROM memory.

The TOE also includes IC Dedicated Software to support its start-up and for test purposes after production. The Smart Card Controller hardware comprises an 16-bit processing unit, volatile and non-volatile memories, cryptographic co-processors, security components and one 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 MF1P(H)x1y1 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.

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

1.3.2 TOE Type

The TOE is a Smart Card comprising a hardware platform and a fixed software package. 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 [14, 16, 17, 15] card terminal to be provided with power and to receive adequate commands.

1.4 TOE Description

1.4.1 Physical Scope of TOE

The Target of Evaluation (TOE) is the smart card integrated circuit named MF1P(H)x1y1 in combination with a fixed software package, the IC Dedicated Software. The TOE is manufactured in an advanced CMOS process. The TOE includes IC Designer/Manufacturer proprietary IC Dedicated Test Software and IC Dedicated Support Software, according to the terminology used in [13]. Note that the MIFARE Plus Software is part of the IC Dedicated Support Software.

Table 1.1 lists the TOE components.

Type	Name	Release	Date	Form of Delivery
Hardware	MF1P(H)x1y1 Hardware	VA	11.06.2015	Wafer, modules and package
Software	Test ROM Software (the IC Dedicated Test Software)	1.0	18.06.2015	SM ROM on chip
Software	IC Dedicated Boot Software (part of the IC Dedicated Support Software)	1.0	18.06.2015	SM ROM on chip
Software	HAL ROM Software (part of the IC Dedicated Support Software)	1.0	18.06.2015	SM ROM on chip
Software	MIFARE Plus Software (part of the IC Dedicated Support Software)	1.0	26.02.2016	SM ROM on chip
Document	MF1P(H)x1y1 - MIFARE Plus EV1, Product Data Sheet [8]	322630	2016-08-01	Electronic Document
Document	MF1P(H)x1y1 PDC - MIFARE Plus EV1 Post Delivery Configuration, Product Data Sheet Addendum [9]	332712	2016-02-17	Electronic Document
Document	MF1P(H)x1y1 - User Guidance Manual, Guidance Documentation [7]	333511	2016-03-30	Electronic Document

Tab. 1.1: Components of the TOE

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 four different packages and three different memory configurations.

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

- MF1P*cxeyfdpp*/*svw*

Type	*c*	*x*	*e*	*y*	*f*	*d*	*pp*	*/*	*s*	*v*	*w*
MF1P	H	4	1	0	1	D	UD	/	0	1	0
...	...	...	...	...	...	...	...	/	...	...	...

Tab. 1.2: Supported Types

Table 1.2 illustrates the commercial type names that are subject of the evaluation.

Identifier	Description	Valid Values	Digits	Assignment	Meaning
c	input capacitance	alphabetic	1-2	 H	17pF 70pF
x	memory size	numeric	1	1 2 4	1KB EEPROM 2KB EEPROM 4KB EEPROM
e	evolution	numeric	1	1	the second evolution of MIFARE Plus
y	UID length	numeric	1	0 2 3	7 byte UID 4 byte NUID (UID0=0x*F according to ISO 14443-3 [17] ONUID
f	FAB produced	numeric	1	1	Universal
d	operating temperature range	alphabetic	1	D	$-30 < t_{\text{operating}} < 70$
pp	package type	alphabetic	2	UD UF A4 A6	$120\mu m$ sawn wafer $75\mu m$ sawn wafer MOA4 module on reel MOB6 module on reel
s	Fabkey Identifier	alphanumeric	1	0 1..9, A..Z	Default EEPROM configuration Dedicated customer specific EEPROM configuration
v	Product Version	alphanumeric	1	1	Version 1
w	Customized UID Range (for UID=XFh)	alphanumeric	1		Default

Identifier	Description	Valid Values	Digits	Assignment	Meaning
				Full Range	Denotes a dedicated, customer specific range defined in the XFh UID range

Tab. 1.3: Variable Definitions for Commercial Type Names

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

- MF1P*cx*1*y*1D*pp*/s1w

For example, the commercial type name ”MF1P2131DUD/01” denotes a MF1P(H)x1y1 supplied in wafer delivery form, with 2KB EEPROM, 4 byte ONUID, Product Version 1. The commercial type name ”MF1P4101DA4/01” denotes a MF1P(H)x1y1 supplied in MOA4 modules on a reel, with 4KB EEPROM, 7 byte UID, Product Version 1.

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 ”MF1P(H)x1y1” 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 TOE

1.4.2.1 Hardware Description

The CPU of the MF1P(H)x1y1 has an 16-bit architecture. The on-chip hardware components are controlled by the MIFARE Plus 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 MF1P(H)x1y1 can be performed through the contact-less interface.

The device includes ROM (48 kByte), RAM (1kByte), EEPROM (10 kByte) and FLASH (64kByte) memory. The ROM is split in Application-ROM, HAL-ROM and Test-ROM. The EEPROM size can logically be configured as denoted in table 1.3.

The AES co-processor supports AES operations with a key length of 128 bits. The random number generator provides true random numbers which are used to seed pseudo random number generator.

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 (compared to section 1.4.4).

The TOE also contains IC Dedicated Support Software. The Boot ROM Software which is stored in the Test-ROM is part of the IC Dedicated Support Software. This software is executed after each reset of the TOE, meaning every time when the TOE starts. It sets up the TOE and does some basic configuration.

The MIFARE Plus Software is also part of the IC Dedicated Support Software and provides the main functionality of the TOE in the usage phase. The MF1P(H)x1y1 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 (including so called Values which are Blocks in a specific format representing a number).
- Authentication on Sector level with fine-grained access conditions Blocks.
- Message authentication to support replay attack protection.
- Data encryption for confidentiality of the contact-less communication.
- Unique serial number for each device (UID) with optional random ID.
- The TOE supports MIFARE Plus EV0

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.

MIFARE Plus Software offers three different SecurityLevels. The higher the SecurityLevel, the more secure the MIFARE Plus Software is intended to be. In addition, each Sector is associated its corresponding SectorSecurityLevel, where the SecurityLevel equals the SectorSecurityLevel of the Sector with the lowest SectorSecurityLevel at any time. As a consequence, the TOE supports multiple SectorSecurityLevel but only one designated SecurityLevel at one time.

Note that in the remainder of the document the terms SL0, SL1 and SL3 are used equivalent to the terms SecurityLevel 0, SecurityLevel 1 and SecurityLevel 3, in order to make referencing easier.

For SL1 and SL3 the SecurityLevel for the TOE as a whole, as well as the SectorSecurityLevels for dedicated Sectors can be switched to a higher level. A migration, both at TOE or at Sector level, is only possible to a higher level and not to a lower one. In case dedicated sectors have been migrated to higher SectorSecurityLevels, the overall TOE behaviour must remain by default according to the lowest SectorSecurityLevel among all Sectors of the TOE. If the TOE is in SL0, this must always hold for the whole TOE, which means that all Sectors are in SectorSecurityLevel 0.

The TOE is delivered as ”L1 card”, indicating that SL0, SL1 and SL3 are available.

The main features of each SecurityLevel are listed below:

Security level 0: The TOE does not provide any functionality besides initialization. The TOE is initialized in plaintext, especially keys for the further levels can be brought in. A TOE in SL0 is not usable for other purposes. After all mandatory keys and security attributes have been stored in the TOE, it can be switched to SL1.

Security level 1: The CardUser can access the Blocks in the TOE after an authentication procedure. The communication with the terminal is protected, however the authentication and the protected communication in this SecurityLevel are not evaluated security services of the TOE. The functionality provided by SL1 (beside one expection stated in the subsequent Note) does not implement any Security Functional Requirement and is therefore not in the scope of the evaluation. The TOE can be switched to SL3, dedicated Sectors can be switched to SectorSecurityLevel 3. Both actions require preceding authentication using the AES algorithm with the appropriate key.

Note: The only functionality provided by SL1 that is within the scope of the evulation, is the switch of the SecurityLevel from 1 to 3.

Security level 3: The CardUser can access the data and Value Blocks in the TOE via an adequate card terminal after an authentication procedure based on the AES algorithm. The communication with the card terminal can be protected with secure messaging. The authentication and the secure messaging are security services of the TOE. The TOE cannot be switched to a different SecurityLevel. In SL3, the TOE offers two

secure messaging modes: EV0 Secure Messaging and EV1 Secure Messaging (see section 8.10.3 of [8]).

Note: All functionality provided by SecurityLevel 3 is within the scope of the evaluation.

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

1.4.2.3 Documentation

The Functional Specification [8] 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 [7] 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 with Augmentation Packages [13], 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 MF1P(H)x1y1 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 [13], 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. Therefore the TOE evaluation perimeter comprising the development and production environment of the TOE, consists of life cycle phases 2 - 4 (according to the Security IC Platform Protection Profile with Augmentation Packages [13], section 1.2.4).

Regarding the Application Note 2 of [13], the TOE provides additional functionality which is not covered in the Security IC Platform Protection Profile with Augmentation Packages [13]. The additional functionality is due to the MIFARE Plus Software that is part of the IC Dedicated Support Software and 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 MIFARE Plus Software. SL0 is intended for personalisation in Phase 6. The SL1 and SL3 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 [14, 16, 17, 15]. 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 dataand 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.

Remark 1. 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 [8].

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 including Values
- Secure configuration in the field
- Encryption of communication
- Random ID to exacerbate tracing of end-users

2 Conformance Claims

2.1 CC Conformance Claim

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

- Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model - Version 3.1 CCMB-2012-09-001, Revision 4, September 2012, [2]
- Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components, Version 3.1 CCMB-2012-09-002, Revision 4, September 2012, [3]
- Common Criteria for Information Technology Security Evaluation, Part 3 – Security Assurance Components, Version 3.1 CCMB-2012-09-003, Revision 4, September 2012, [4]

For the evaluation the following methodology will be used:

- Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, Version 3.1 CCMB-2012-09-004, Revision 4, September 2012, [5]

This Security Target claims to be CC Part 2 extended and CC Part 3 conformant. The extended Security Functional Requirements are defined in chapter 6.

2.2 Package Claim

This Security Target claims conformance to the assurance package **EAL5 augmented**. The augmentations to EAL5 are ALC_DVS.2 and AVA_VAN.5. In addition, this Security Target is augmented using the components ASE_TSS.2 and ALC_FLR.1.

Note: The Protection Profile Security IC Platform Protection Profile with Augmentation Packages [13], to which this Security Target claims conformance (refer to section 2.3), requires assurance level EAL4 augmented. The changes, which are needed for EAL5, are described in the relevant sections of this Security Target.

2.3 PP Claim

This Security Target claims strict conformance to the Security IC Platform Protection Profile with Augmentation Packages [13]. Thus, the concepts are used in the same sense. For the definition of terms refer to [13]. This chapter does not need any supplement in the Security Target.

Note that the Security IC Platform Protection Profile with Augmentation Packages [13] defines (optional) ”Augmentation Packages”, which are not applied in this Security Target.

2.4 Conformance Claim Rationale

According to section 2.3 this Security Target claims strict conformance to the Security IC Platform Protection Profile with Augmentation Packages [13]. Note that the term Protection Profile will be used in the remainder of the document to make referencing easier.

The TOE type defined in section 1.3.2 of this Security Target is a smart Card controller with IC Dedicated Support Software. This is consistent with the TOE definition for a Security IC in section 1.2.2 of [13].

The sections within this document where security problem definitions, objectives and security requirements are defined, clearly state which of these items are taken from the Protection Profile and which are added in this ST. Therefore the content of the Protection Profile is not repeated in this Security Target. Moreover, all additionally stated items in this Security Target do not contradict the items included from the Protection Profile (see the respective sections in this document). The operations done for the SFRs taken from the Protection Profile are also clearly indicated.

The evaluation assurance level claimed for this TOE (EAL5 augmented) is shown in section 6.2.1 to include respectively exceed the requirements claimed by the PP (EAL4 augmented).

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

3 Security Problem Definition

Since this Security Target claims strict conformance to the Protection Profile, the Assets, Threats, Assumptions, and Organizational Security Policies are taken from the Protection Profile. In the following only the extensions of the different sections are detailed. The elements of the Security Problem Definition that are not extended in the Security Target, are not repeated in this Security Target. They are cited here for completeness.

3.1 Description of Assets

All assets, which are related to the high-level concerns defined in section 3.1 of the Protection Profile, are related to standard functionality and are applied in this Security Target. The high-level concerns are cited here completely:

- Integrity and confidentiality of User Data stored and in operation,
- Integrity and confidentiality of the Security IC Embedded Software, stored and in operation,
- Correct operation of the Security Services provided by the TOE for the Security IC Embedded Software,
- Deficiency of random numbers.

To be able to protect the assets based on this concerns, 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, Security IC Embedded Software and configuration data.
- Initialization Data and Pre-personalization Data, specific development aids, test and characterization related data, material for software development support, and photo masks.

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

3.2 Threats

All threats defined in section 3.2 of the Protection Profile are valid for this Security Target. These threats are listed in table 3.1. In addition the threat T.Masquerade_TOE is applicable for this TOE as stated below.

T.Masquerade_TOE **Masquerade the TOE**
An attacker may threaten the property being a genuine TOE by producing a chip which is not a genuine TOE but wrongly identifying itself as genuine TOE sample.

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
T.Masquerade_TOE	Masquerade the TOE

Tab. 3.1: Threats defined in the Security IC Protection Profile

Considering the Application Note 4 in the Protection Profile, the following additional threats are defined in this Security Target.

Name	Title
T.Data-Modification	Unauthorised Data Modification
T.Impersonate	Impersonating authorised users during authentication
T.Cloning	Cloning

Tab. 3.2: Additional Threats defined in this ST

T.Data-Modification **Unauthorised Data Modification**
Application data and code 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 Organizational Security Policies

All security policies defined in section 3.3 of the Protection Profile are valid for this Security Target. These security policies are listed in Table 3.3.

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

Tab. 3.3: Policies defined in the Security IC Protection Profile

In compliance with Application Note 5 in the Protection Profile, this Security Target defines additional security policies as detailed in the following.

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

The IC Developer / Manufacturer therefore applies the policies Confidentiality during communication, Integrity during communication and Un-traceability of end-users as specified below.

Name	Title
P.Encryption	Confidentiality during communication
P.MAC	Integrity during communication
P.No-Trace	Un-traceability of end-users

Tab. 3.4: Additional Policies defined in this ST

P.Encryption **Confidentiality during communication**
The TOE shall provide the possibility to protect selected data elements from eavesdropping during contact-less communication.

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.

3.4 Assumptions

All assumptions defined in section 3.4 of the Protection Profile are valid for this Security Target. These assumptions are listed in Table 3.5.

Name	Title
A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation
A.Resp-Appl	Treatment of user data of the Composite TOE

Tab. 3.5: Assumptions defined in the Security IC Protection Profile

In compliance with Application Notes 6 and 7 in the Protection Profile, this Security Target defines two additional assumptions as follows:

A.Secure_Values **Usage of secure values**
Only confidential and cryptographically strong keys shall be used to set up the authentication. These values are generated outside the TOE and they are downloaded to the TOE.

A.Terminal_Support **Terminal support to ensure integrity, confidentiality and use of random numbers**
The terminal verifies information sent by the TOE in order to ensure integrity and confidentiality of the communication. Furthermore the terminal shall provide random numbers according to AIS20 (see [18]) or AIS31 (see [19]) for the authentication.

These assumptions are summarized in Table 3.6.

Name	Title
A.Secure_Values	Usage of secure values
A.Terminal_Support	Terminal support to ensure integrity, confidentiality and use of random numbers

Tab. 3.6: Additional Assumptions defined in this ST

4 Security Objectives

4.1 Security Objectives for the TOE

All security objectives for the TOE, which are defined in section 4.1 of the Protection Profile, are applied to this Security Target and listed in table 4.1.

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

Tab. 4.1: Security Objectives of the TOE (PP)

Regarding the Application Notes 8 and 9 in the Protection Profile, additional security objectives that are based on additional functionality provided by the TOE, are defined and listed in table 4.2.

Name	Title
O.Access-Control	Access Control
O.Authentication	Authentication
O.Type-Consistency	Data type consistency
O.No-Trace	Preventing Traceability
O.Encryption	Confidential Communication
O.MAC	Integrity-Protected Communication

Tab. 4.2: Security Objectives of the TOE (ST)

These additional security objectives are specified as follows.

O.Access-Control **Access Control**

The TOE must provide an access control mechanism for application code and data stored by it. The access control mechanism shall apply to all operations for application elements and to reading and modifying security attributes. 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.Encryption **Confidential Communication**

The TOE must be able to protect the communication by encryption. This shall be implemented by security attributes that enforce encrypted communication for the respective data elements.

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.Type-Consistency **Data type consistency**

The TOE must provide a consistent handling of the different supported data types. This comprises over- and underflow checking for Values and for Block sizes.

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.

4.2 Security Objectives for the Security IC Embedded Software development Environment

All security objectives for the Security IC Embedded Software development Environment, which are defined in section 4.2 of the Protection Profile, are applied to this Security Target and listed in table 4.3.

Name	Title
OE.Resp-Appl	Treatment of User Data

Tab. 4.3: Security Objectives of the DVE (PP)

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

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

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

4.3 Security Objectives for the Operational Environment

In addition to the security objective for the operational environment as required by CC Part 1 [2], all security objectives for the operational environment, which are defined in section 4.3 of the Protection Profile, are applied to this Security Target and listed in table 4.4.

Name	Title
OE.Process-Sec-IC	Protection during composite product manufacturing

Tab. 4.4: Security Objectives of the OPE (PP)

In addition, the following additional security objectives for the operational environment are defined in this Security Target and listed in table 4.5.

Name	Title
OE.Secure_Values	Generation of secure values
OE.Terminal_Support	Terminal support to ensure integrity and confidentiality

Tab. 4.5: Security Objectives of the OPE (ST)

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

OE.Secure_Values **Generation of secure values**
The environment shall generate confidential and cryptographically strong 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 up to Phase 7.

The TOE provides specific functionality to verify the success of the application download process. Therefore, OE.Terminal_Support is defined to allow triggering the verification process.

OE.Terminal_Support **Terminal support to ensure integrity and confidentiality**
The terminal shall verify information sent by the TOE in order to ensure integrity and confidentiality 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. Furthermore the terminal shall provide random numbers according to AIS20 (see [18]) or AIS31 (see [19]) for the authentication.

4.4 Security Objectives Rationale

Section 4.4 in the Protection Profile provides a rationale how the threats, organisational security policies and assumptions are addressed by the security objectives defined in the Protection Profile. Table 4.6 summarizes this.

Security Problem Definition	Security Objective	Notes
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	
P.Process-TOE	O.Identification	Phases 2–3
A.Process-Sec-IC	OE.Process-Sec-IC	Phases 4–6
A.Resp-Appl	OE.Resp-Appl	Phase 1
T.Masquerade_TOE	OE.Process-Sec-IC	

Tab. 4.6: Security Objectives vs. Security Problem Definition (PP)

Table 4.7 summarizes how threats, organisational security policies and assumptions are addressed by the security objectives with respect to those items defined in the Security Target. All these items are in line with those in the Protection Profile.

Security Problem Definition	Security Objective	Notes
T.Data-Modification	O.Access-Control O.Type-Consistency OE.Terminal_Support	
T.Impersonate	O.Authentication	
T.Cloning	O.Access-Control O.Authentication	
P.Encryption	O.Encryption	
P.MAC	O.MAC	
P.No-Trace	O.Access-Control O.Authentication O.No-Trace	

Security Problem Definition	Security Objective	Notes
A.Secure_Values	OE.Secure_Values	
A.Terminal_Support	OE.Terminal_Support	

Tab. 4.7: Security Objectives vs. Security Problem Definition (ST)

The rationale for the threat T.Masquerade_TOE is given below:

Justification related to T.Masquerade_TOE:

Objective	Rationale
OE.Process-Sec-IC	The Security Objective for the Operational Environment requires that the confidentiality and integrity of the TOE is maintained. Thus the threat is covered.

The rationale for all items defined in the Security Target is given below.

Justification related to T.Data-Modification:

Objective	Rationale
O.Access-Control	This objective requires an access control mechanism that limits the ability to modify data and code elements stored by the TOE.
O.Type-Consistency	This objective ensures that data types are adhered, so that TOE data can not be modified by abusing type-specific operations.
OE.Terminal_Support	This objective requires that the terminal must support this by checking the TOE responses.

Justification related to T.Impersonate:

Objective	Rationale
O.Authentication	This objective requires that the authentication mechanism provided by the TOE shall be resistant against attack scenarios targeting the impersonation of authorized users.

Justification related to T.Cloning:

Objective	Rationale

Objective	Rationale
O.Access-Control	This objective requires that unauthorized users can not read any information that is restricted to the authorized subjects. The cryptographic keys used for the authentication are stored inside the TOE and are protected by this objective. This objective states that no keys used for authentication shall ever be output.
O.Authentication	This objective requires that users are authenticated before they can read any information that is restricted to authorized users.

Justification related to A.Secure_Values:

Objective	Rationale
OE.Secure_Values	This objective is an immediate transformation of the assumption, therefore it covers the assumption.

Justification related to A.Terminal_Support:

Objective	Rationale
OE.Terminal_Support	This objective is an immediate transformation of the assumption, therefore it covers the assumption. The TOE can only check the integrity of data received from the terminal. For data transferred to the terminal the receiver must verify the integrity of the received data. Furthermore the TOE cannot verify the entropy of the random number sent by the terminal. The terminal itself must ensure that random numbers are generated with appropriate entropy for the authentication. This is assumed by the related assumption, therefore the assumption is covered.

Justification related to P.Encryption:

Objective	Rationale
O.Encryption	This objective is an immediate transformation of the security policy, therefore it covers the Security Policy.

Justification related to P.MAC:

Objective	Rationale
O.MAC	This objective is an immediate transformation of the security policy, therefore it covers the Security Policy.

Justification related to P.No-Trace:

Objective	Rationale
O.Access-Control	This objective provides means to implement access control to data elements on the TOE in order to prevent tracing based on freely accessible data elements.
O.Authentication	This objective provides means to implement authentication on the TOE in order to prevent tracing based on freely accessible data elements.
O.No-Trace	This objective 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 unauthorized subject. This objective includes the UID.

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

5 Extended Components Definitions

This Security Target does not define extended components.

Note that the Protection Profile defines extended security functional requirements FCS_RNG.1, FMT_LIM.1, FMT_LIM.2, FAU_SAS.1 and FDP_SDC.1 in chapter 5, which are included in this Security Target.

6 Security Requirements

This chapter defines the security requirements that shall be met by the TOE. These security requirements are composed of the security functional requirements and the security assurance requirements that the TOE must meet in order to achieve its security objectives.

CC allows several operations to be performed on security requirements (on the component level); refinement, selection, assignment, and iteration are defined in section 8.1 of CC Part 1 [2]. These operations are used in the Protection Profile and in this Security Target, respectively.

The refinement operation is used to add details to requirements, and thus, further intensifies a requirement.

Refinements of security requirements are denoted in such a way that added words are in bold text.

The selection operation is used to select one or more options provided by the Protection Profile or CC in stating a requirement. Selections having been made are denoted as italic text. The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments having been made are denoted as italic text.

The iteration operation is used when a component is repeated with varying operations. It is denoted by showing brackets "[iteration indicator]" and the iteration indicator within the brackets.

For the sake of a better readability, the iteration operation may also be applied to some single components (being not repeated) in order to indicate belonging of such SFRs to same functional cluster. In such a case, the iteration operation is applied to only one single component.

Whenever an element in the Protection Profile contains an operation that is left uncompleted, the Security Target has to complete that operation.

6.1 Security Functional Requirements

All Security Functional Requirements (SFRs) of the TOE are presented in the following sections to support a better understanding of the combination of the Protection Profile and this Security Target.

6.1.1 SFRs of the Protection Profile

Table 6.1 shows all SFRs which are specified in the Protection Profile.

Name	Title
FAU_SAS.1[HW]	Audit Storage
FCS_RNG.1[HW]	Random Number Generation (Class PTG.2)
FCS_RNG.1[DET]	Random Number Generation (Deterministic)
FDP_ITT.1[HW]	Basic Internal Transfer Protection
FDP_IFC.1	Subset Information Flow Control
FDP_SDC.1[HW]	Stored data confidentiality
FDP_SDI.2[HW]	Stored data integrity monitoring and action

Name	Title
FMT_LIM.1[HW]	Limited Capabilities
FMT_LIM.2[HW]	Limited Availability
FPT_FLS.1	Failure with Preservation of Secure State
FPT_ITT.1[HW]	Basic Internal TSF Data Transfer Protection
FPT_PHP.3	Resistance to Physical Attack
FRU_FLT.2	Limited Fault Tolerance

Tab. 6.1: Security Functional Requirements defined in the Security IC Protection Profile

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

For the SFR FAU_SAS.1[HW] the Protection Profile leaves the assignment operation open for the non volatile memory type in which initialization data, pre-personalization data and/or other supplements of 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 Protection Profile.

FAU_SAS.1[HW]	**Audit Storage**
Hierarchical-To	No other components.
Dependencies	No dependencies.
FAU_SAS.1.1[HW]	The TSF shall provide *the test process before TOE Delivery* with the capability to store *the Initialisation Data and/or Pre-personalisation Data and/or supplements of the Security IC Embedded Software* in the *NVM*.

For FCS_RNG.1.1 the Protection Profile 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 Protection Profile partially fills in the assignment operation for the defined quality metric for the random numbers by replacing it by a selection and assignment operation.

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

FCS_RNG.1[HW]	**Random Number Generation (Class PTG.2)**
Hierarchical-To	No other components.

Dependencies	No dependencies.
FCS_RNG.1.1[HW]	The TSF shall provide a *physical* random number generator that implements:

(PTG.2.1) A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.

(PTG.2.2) If a total failure of the entropy source occurs while the RNG is being operated, the RNG *prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source.*

(PTG.2.3) The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.

(PTG.2.4) The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.

(PTG.2.5) The online test procedure checks the quality of the raw random number sequence. It is triggered *at regular intervals or continuously*. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.

FCS_RNG.1.2[HW]	The TSF shall provide *octets of bits* that meet:

(PTG.2.6) Test procedure A [1] does not distinguish the internal random numbers from output sequences of an ideal RNG.

(PTG.2.7) The average Shannon entropy per internal random bit exceeds 0.997.

Note: The definition of the Security Functional Requirement FCS_RNG.1 has been taken from [1].

Note: The functional requirement FCS_RNG.1[HW] is a refinement of FCS_RNG.1 defined in PP [13] according to [1].

Note: Application Note 20 in [13] requires that the Security Target specifies for the security capabilities in FCS_RNG.1.1[HW] how the results of the total failure test of the random source are provided to the MIFARE Plus Software. The results of the internal test sequence are provided to the MIFARE Plus Software as a pass or fail criterion. The entropy of the random number is measured by the Shannon-Entropy as follows: $E = -\sum_{i=0}^{255} p_i \cdot \log_2 p_i$ where p_i is the probability that the byte $(b_7, b_6, \ldots, b_0)$ is equal to i as binary number. Here the term "bit" means measure of the Shannon-Entropy. The value "7.976" is assigned due to the requirements of "AIS31", [19].

In addition to FCS_RNG.1[HW] the TOE provides a deterministic random number generator:

FCS_RNG.1[DET]	**Random Number Generation (Deterministic)**
Hierarchical-To	No other components.

[1] Note: according par.295 in [19] the assignment may be empty.

Dependencies	No dependencies.
FCS_RNG.1.1[DET]	The TSF shall provide a *deterministic* random number generator that implements:
	(DRG.3.1) *If initialized with a random seed using a PTRNG of class PTG.2 (as defined in [19]) as random source, the internal state of the RNG shall have at least 230 bits (TDES) resp. 254 bits (AES) of entropy.*
	(DRG.3.2) *The RNG provides forward secrecy (as defined in [19]).*
	(DRG.3.3) *The RNG provides backward secrecy even if the current internal state is known (as defined in [19]).*
FCS_RNG.1.2[DET]	The TSF shall provide random numbers that meet:
	(DRG.3.4) *The RNG, initialized with a random seed using a PTRNG of class PTG.2 (as defined in [19]) as random source, generates output for which in AES mode* 2^{48} *and in 3DES mode* 2^{35} *strings of bit length 128 are mutually different with probability at least* $1 - 2^{-24}$ *in AES mode and* $1 - 2^{-17}$ *in 3DES mode.*
	(DRG.3.5) *Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A* [2] *(as defined in [19]).*

Note: The CryptoLib Software provides the Security IC Embedded Software with seperate functionality to initialise the deterministic random number generator (which includes the chi-square test) and to generate pseudo-random data. It is the responsibility of the user to initialise the DRNG before generating random data. If it is tried to request pseudo-random numbers without having seeded the DRNG a security reset is triggered.

Note: Only if the chi-square test succeeds the hardware random number generator seeds the deterministic random number generator implemented as part of the CryptoLib Software.

For FDP_SDC.1.1 the Protection Profile leaves the assignment operation open for the memory area in which the TSF ensures the confidentiality of information of user data while being stored in that memory area. The assignment operation is filled with the following statement.

FDP_SDC.1[HW]	**Stored data confidentiality**
Hierarchical-To	No other components.
Dependencies	No dependencies.
FDP_SDC.1.1[HW]	The TSF shall ensure the confidentiality of the information of the user data while it is stored in the *RAM and Non Volatile Memory*.

For FDP_SDI.2.1 the Protection Profile leaves the assignment operations open on the type of integrity errors of user data and the attributes the user data is based on. For FDP_SDI.2.2 the Protection Profile leaves the

[2] Note: according par.295 in [19] the assignment may be empty.

assignment operation open on the type of action that shall be taken upon registration of integrity errors. The assignment operations are filled with the following statements.

FDP_SDI.2[HW]	**Stored data integrity monitoring and action**
Hierarchical-To	FDP_SDI.1 Stored data integrity monitoring
Dependencies	No dependencies.
FDP_SDI.2.1[HW]	The TSF shall monitor user data stored in containers controlled by the TSF for *modification, deletion, repetition or loss of data* on all objects, based on the following attributes: *integrity check information associated with the data stored in memories*.
FDP_SDI.2.2[HW]	Upon detection of a data integrity error, the TSF shall *trigger a Security Reset*.

By this, all assignment/selection operations are performed. This Security Target does not perform any other/further operations for the Security Functional Requirements defined in the Protection Profile. Considering the Application Note 12 in the Protection Profile in the following subsection the additional functions, such as for cryptographic support, authentication and access control are defined. These SFRs are not required in the Protection Profile. As required by the Application Note 14 in the Protection Profile the secure state is described in section 7.2.1 in [10] . Regarding the Application Note 15 in the Protection Profile an additional generation of audit is not defined for ”Limited Fault Tolerance (FRU_FLT.2)”. As required by the Application Note 19 in the Protection Profile the automatic response of the TOE is described in section 7.2.1 in [10].

6.1.2 Additional SFRs regarding Access Control

6.1.2.1 Access Control Policy

The Security Function Policy (SFP) **Access Control Policy** uses the subsequent definitions including the subjects defined as follows:

Subject	**Personaliser**	**Personaliser**
Info	The Personaliser is the subject that owns or has access to all cryptographic keys in order to provide them to the TOE. Note that all actions performed by the Personaliser are restricted to SL0 and that those actions do not require an active authentication.	

Subject	**CardAdmin**	**Card Administrator**
Info	The CardAdmin is the subject that owns or has access to the CardMasterKey.	

Subject	**CardManager**	**Card Manager**
Info	The CardManager is the subject that owns or has access to the CardConfigurationKey.	

Subject	SecurityLevelManager	Card Security Level Manager
Info	The SecurityLevelManager is the subject that owns or has access to the Level3SwitchKey.	

Subject	SectorSecurityLevelManager	Sector Security Level Manager
Info	The SectorSecurityLevelManager is the subject that owns or has access to the Level3SectorSwitchKey and one or more AESSectorKeys.	

Subject	CardUser	Card User
Info	The CardUser is the subject that owns or has access to one or more AESSectorKeys. Note that the CardUser does not necessarily need to know both AESSectorKeys.KeyA and AESSectorKeys.KeyB of a particular Sector.	

Subject	OriginalityKeyUser	Originality Key User
Info	The OriginalityKeyUser is the subject that owns or has access to one or more OriginalityKeys.	

Subject	TransMACConfManager	Transaction MAC Configuration Manager
Info	The TransMACConfManager is the subject that owns or has access to one or more TransMACConfKeys.	

Subject	Anybody	Anybody
Info	Any subject that does not belong to one of the roles Personaliser, CardAdmin, CardManager, SecurityLevelManager, SectorSecurityLevelManager, CardUser, OriginalityKeyUser or TransMACConfManager, belongs to the role Anybody. This role includes the card holder (also referred to as end-user), and any other subject like an attacker for instance. The subjects belonging to Anybody do not possess any key and therefore are not able to perform any operation that is restricted to one of the roles which are explicitely excluded from the role Anybody.	

Subject	Nobody	Nobody
Info	Any subject that does not belong to one of the roles Personaliser, CardAdmin, CardManager, SecurityLevelManager, SectorSecurityLevelManager, CardUser, OriginalityKeyUser, TransMACConfManager or Anybody, belongs to the role Nobody. Due to the definition of Anybody, the set of all subjects belonging to the role Nobody is the empty set.	

Note that multiple subjects may have the same role, e.g. for every Sector there are two CardUser (identified by the respective AESSectorKeys.KeyA and AESSectorKeys.KeyB for this Sector). The assigned rights to the CardUsers can be different, which allows having more or less powerful CardUser. There are also more than one OriginalityKeyUser and SecurityLevelManager.

The objects are defined as follows:

Object	Block	Block
Info	Data is organized in Blocks of 16 bytes, which are accessed as elementary data units. Several instances of a Block are grouped into Sectors.	
Operation	Read	Read data from a Block.
Operation	Write	Write data to a Block.

Object	Sector	Sector
Info	Each Sector consists of 4 or 16 Blocks.	

Object	SectorTrailer	Sector Trailer
Info	The security attribute SectorTrailer is a specific Block that contains the access conditions for the corresponding Sector.	
Operation	Read	Read the security attribute SectorTrailer.
Operation	Modify	Modify the security attribute SectorTrailer.

Object	Value	Value
Info	One specific type of data stored in a Block is called Value.	
Operation	Increase	Increase a Value.
Operation	Decrease	Decrease a Value.
Operation	Transfer	Transfer a Value.
Operation	Restore	Restore a Value.

Object	MFPConfigurationBlock	MFP Configuration Block
Info	The security attribute MFPConfigurationBlock.	
Operation	Modify	Modify the security attribute MFPConfigurationBlock.

Object	FieldConfigurationBlock	Field Configuration Block
Info	The security attribute FieldConfigurationBlock.	

Object	FieldConfigurationBlock	Field Configuration Block
Operation	Modify	Modify the security attribute FieldConfigurationBlock.

Object	SectorSecurityLevel	Sector Security Level
Info	The sector security level of a designated Sector of the TOE.	
Operation	Switch	Switch the SectorSecurityLevel.

Object	SecurityLevel	Card Security Level
Info	The security attribute SecurityLevel of the TOE.	
Operation	Switch	Switch the SecurityLevel.

Object	CardMasterKey	Card Master Key
Info	The key to manage keys and parameters for items of the TOE that do not require being changed in the field.	
Operation	Change	Change the CardMasterKey.

Object	CardConfigurationKey	Card Configuration Key
Info	The key to manage keys and parameters for items of the TOE that may require being changed in the field.	
Operation	Change	Change the CardConfigurationKey.

Object	Level3SwitchKey	Level 3 Switch Key
Info	Key to change SecurityLevel from SL1 to SL3.	
Operation	Change	Change the Level3SwitchKey.

Object	Level3SectorSwitchKey	Level 3 Sector Switch Key
Info	Key to switch dedicated Sectors from SectorSecurityLevel 1 to SectorSecurityLevel 3.	
Operation	Change	Change the Level3SectorSwitchKey.

Object	TransMACKey	Transaction MAC Key
Info	Key to derive session keys that are used in the actual Transaction MAC computation. Note that there exists of four of these keys in total.	
Operation	Change	Change the TransMACKey.

Object	TransMACConfKey	Transaction MAC Configuration Key
Info	Each TransMACKey is assigned a TransMACConfKey. An active authentication with the TransMACConfKey is required to enable the Transaction MAC feature for one or more dedicated Blocks.	
Operation	Change	Change the TransMACConfKey.

Object	TransMACConfBlock	Transaction MAC Configuration Block
Info	Each TransMACKey is related with several TransMACConfBlocks.	
Operation	Write	Write data to TransMACConfBlock.

Object	AESSectorKeys	AES Sector Keys
Info	The keys to manage access to Sectors. Since there are two keys for every Sector the keys are called AESSectorKeys.KeyA and AESSectorKeys.KeyB.	
Operation	Change	Change the AESSectorKeys.
Attribute	KeyA	AES Sector key AESSectorKeys.KeyA.
Attribute	KeyB	AES Sector key AESSectorKeys.KeyB.

Object	OriginalityKey	Originality Key
Info	The key to check the originality of the TOE.	
Operation	Change	Change the OriginalityKey.

Note that subjects are authorised by cryptographic keys by appyling an authentication procedure. These keys are considered as authentication data and not as security attributes of the subjects.

The TOE shall meet the requirements ”Security Roles (FMT_SMR.1[MFP])” as specified below.

FMT_SMR.1[MFP]	**Security Roles**
Hierarchical-To	No other components.
Dependencies	FIA_UID.1 Timing of identification
FMT_SMR.1.1[MFP]	The TSF shall maintain the roles *Personaliser*, *CardAdmin*, *CardManager*, *SecurityLevelManager*, *SectorSecurityLevelManager*, *CardUser*, *OriginalityKeyUser*, *TransMACConfManager*, *Anybody* and *Nobody*.
FMT_SMR.1.2[MFP]	The TSF shall be able to associate users with roles.

The TOE shall meet the requirements ”Subset Access Control (FDP_ACC.1[MFP])” as specified below.

FDP_ACC.1[MFP]	**Subset Access Control**
Hierarchical-To	No other components.
Dependencies	FDP_ACF.1 Security attribute based access control.

FDP_ACC.1.1[MFP] The TSF shall enforce the *Access Control Policy* on *all subjects, objects, operations and attributes defined by the MFP Access Control Policy*.

The TOE shall meet the requirements "Security Attribute Based Access Control (FDP_ACF.1[MFP])" as specified below.

FDP_ACF.1[MFP]	**Security Attribute Based Access Control**
Hierarchical-To	No other components.
Dependencies	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization
FDP_ACF.1.1[MFP]	The TSF shall enforce the *MFP Access Control Policy* to objects based on the following: *all subjects, objects and attributes*.
FDP_ACF.1.2[MFP]	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
	MFP_ACP_ACF1_21 *In SL0 the Personaliser is allowed to perform Block.Write on all Blocks except Block 0.*
	MFP_ACP_ACF1_22 *In SL3 the CardUser is allowed to perform Block.Read and Block.Write for every Sector, if the access conditions in the corresponding SectorTrailer grants him this right.*
	MFP_ACP_ACF1_23 *In SL3 the CardUser is allowed to perform Value.Increase, Value.Decrease, Value.Transfer and Value.Restore for every Sector, if the access conditions in the corresponding SectorTrailer grants him this right.*
FDP_ACF.1.3[MFP]	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *none.*.
FDP_ACF.1.4[MFP]	The TSF shall explicitly deny access of subjects to objects based on the following additional rules:
	MFP_ACP_ACF1_41 *No one but Nobody is allowed to perform Block.Write on Block 0 (first Block of the first Sector).*
	MFP_ACP_ACF1_42 *The OriginalityKeyUser is not allowed to perform any operation on objects.*

The TOE shall meet the requirements "Static Attribute Initialization (FMT_MSA.3[MFP])" as specified below.

FMT_MSA.3[MFP]	**Static Attribute Initialization**
Hierarchical-To	No other components.
Dependencies	FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles
FMT_MSA.3.1[MFP]	The TSF shall enforce the *MFP Access Control Policy* to provide *permissive* default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2[MFP]	The TSF shall allow *no one but Nobody* to specify alternative initial values to override the default values when an object or information is created.

The TOE shall meet the requirements "Management of Security Attributes (FMT_MSA.1[MFP])" as specified below.

FMT_MSA.1[MFP]	**Management of Security Attributes**
Hierarchical-To	No other components.
Dependencies	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions
FMT_MSA.1.1[MFP]	The TSF shall enforce the *MFP Access Control Policy* to restrict the ability to *modify* the security attributes *MFPConfigurationBlock*, *FieldConfigurationBlock*, *SectorTrailer* and *SecurityLevel* to the *Personaliser*, *CardManager*, *CardAdmin*, *SecurityLevelManager* and *CardUser*, *respectively*.

Refinement: The detailed management abilities are:

MFP_ACP_MSA1_11 *In SL0 the Personaliser is allowed to perform MFPConfigurationBlock.Modify.*

MFP_ACP_MSA1_12 *In SL0 the Personaliser is allowed to perform FieldConfigurationBlock.Modify.*

MFP_ACP_MSA1_13 *In SL0 the Personaliser is allowed to perform SectorTrailer.Modify.*

MFP_ACP_MSA1_14 *In SL0 the Personaliser is allowed to perform SecurityLevel.Switch to switch the SecurityLevel to SL1 or SL3.*

MFP_ACP_MSA1_15 *The CardAdmin is allowed to perform MFPConfigurationBlock.Modify.*

MFP_ACP_MSA1_16 *The CardManager is allowed to perform FieldConfigurationBlock.Modify.*

MFP_ACP_MSA1_17 *In SL1 the SecurityLevelManager is allowed to perform SecurityLevel.Switch to switch the SecurityLevel to SL3.*

MFP_ACP_MSA1_18 *The CardUser is allowed to perform SectorTrailer.Read and SectorTrailer.Modify if the access conditions in the corresponding SectorTrailer grant him these rights.*

The TOE shall meet the requirements ”Management of TSF Data (FMT_MTD.1[MFP])” as specified below.

FMT_MTD.1[MFP]	**Management of TSF Data**
Hierarchical-To	No other components.
Dependencies	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1[MFP]	The TSF shall restrict the ability to *modify* the *authentication data* to *the Personaliser, CardAdmin, CardManager, SecurityLevelManager and CardUser.*

Refinement: The detailed management abilities are:

MFP_ACP_MTD1_11 *No one but Nobody is allowed to perform OriginalityKey.Change.*

MFP_ACP_MTD1_12 *The Personaliser is allowed to perform CardMasterKey.Change.*

MFP_ACP_MTD1_13 *The Personaliser is allowed to perform CardConfigurationKey.Change.*

MFP_ACP_MTD1_14 *The Personaliser is allowed to perform Level3SwitchKey.Change.*

MFP_ACP_MTD1_15 *The Personaliser is allowed to perform AESSectorKeys.Change.*

MFP_ACP_MTD1_16	*The CardAdmin is allowed to perform CardMasterKey.Change.*
MFP_ACP_MTD1_17	*The CardAdmin is allowed to perform Level3SwitchKey.Change.*
MFP_ACP_MTD1_18	*The CardAdmin is allowed to perform Level3SectorSwitchKey.Change.*
MFP_ACP_MTD1_19	*The CardAdmin is allowed to perform TransMACConfKey.Change.*
MFP_ACP_MTD1_1A	*The CardManager is allowed to perform CardConfigurationKey.Change.*
MFP_ACP_MTD1_1B	*The CardUser is allowed to perform AESSectorKeys.Change if the access conditions in the corresponding SectorTrailer grant him this right.*
MFP_ACP_MTD1_1C	*The TransMACConfManager is allowed to perform TransMACKey.Change.*

The TOE shall meet the requirements ”Specification of Management Functions (FMT_SMF.1[MFP])” as specified below.

FMT_SMF.1[MFP]	**Specification of Management Functions**
Hierarchical-To	No other components.
Dependencies	No dependencies.
FMT_SMF.1.1[MFP]	The TSF shall be capable of performing the following 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 SecurityLevel of the TOE or the SectorSecurityLevel of dedicated Sectors, DESELECT according to ISO 14443-3 [17], explicit authentication reset;* • *Finishing the personalisation phase by explicit request of the Personaliser,* • *Changing a security attribute,* • *Selection and Deselection of the Virtual Card.*

The TOE shall meet the requirements ”Import of user data with security attributes (FDP_ITC.2[MFP])” as specified below.

FDP_ITC.2[MFP]	**Import of user data with security attributes**
Hierarchical-To	No other components.
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
FDP_ITC.2.1[MFP]	The TSF shall enforce the *MFP Access Control Policy* when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.2.2[MFP]	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3[MFP]	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[MFP]	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[MFP]	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: *no additional rules*.

6.1.2.2 Implications of the Access Control Policy

The MFP 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 usually does not belong to the group of authorised users (consisting of CardAdmin, CardManager, SecurityLevelManager, SectorSecurityLevelManager, CardUser and OriginalityKeyUser), 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 SL0. The Personaliser is allowed to perform Block.Write on all Blocks and therefore change all data, all the keys (except the OriginalityKeys), and all SectorTrailers, MFPConfigurationBlocks and FieldConfigurationBlocks.
- Switching of the SecurityLevel is an integral part of the TOE security. The TOE is switched from SL0 to SL1 or SL3 (refer to section 1.4.2.2) at the end of the personalisation phase. Afterwards the SecurityLevel of the TOE can be increased by the SecurityLevelManager, the SectorSecurityLevels of dedicated Sectors of the TOE can be increased by the SectorSecurityLevelManager.

6.1.3 Additional SFRs regarding Confidentiality, Authenticity and Integrity

The TOE shall meet the requirements ”Cryptographic Operation (AES) (FCS_COP.1[MFP-AES])” as specified below.

FCS_COP.1[MFP-AES]	**Cryptographic Operation (AES)**
Hierarchical-To	No other components.
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.
FCS_COP.1.1[MFP-AES]	The TSF shall perform *encryption, decryption and cipher-based MAC used by the MIFARE Plus Software for authentication and communication* in accordance with the specified cryptographic algorithm *Advanced Encryption Standard AES in one of the following modes of operation: CBC, CMAC* and a cryptographic key size *of 128 bits* that meet the following *standards*: • *FIPS Publication 197, Advanced Encryption Standard (AES),* • *NIST Special Publication 800- 38A, 2001 (CBC mode) [11] and* • *NIST Special Publication 800-38B (CMAC mode) [12]*

.

Refinement: For the MIFARE Plus EV0 secure messaging the TOE uses the cryptographic algorithm for CBC according to NIST Special Publication 800-38A (CBC mode) [11] with the following modification: MIFARE Plus Software does not use an unpredictable IV instead it uses a constructed IV which is partially predictable.

The TOE shall meet the requirements "User identification before any Action (FIA_UID.2[MFP])" as specified below.

FIA_UID.2[MFP]	**User identification before any Action**
Hierarchical-To	FIA_UID.1
Dependencies	No dependencies.
FIA_UID.2.1[MFP]	The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

The TOE shall meet the requirements "User Authentication before any Action (FIA_UAU.2[MFP])" as specified below.

FIA_UAU.2[MFP]	**User Authentication before any Action**
Hierarchical-To	FIA_UAU.1
Dependencies	FIA_UID.1 Timing of identification
FIA_UAU.2.1[MFP]	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

The TOE shall meet the requirements "Multiple Authentication Mechanisms (FIA_UAU.5[MFP])" as specified below.

FIA_UAU.5[MFP]	**Multiple Authentication Mechanisms**
Hierarchical-To	No other components.
Dependencies	No dependencies.
FIA_UAU.5.1[MFP]	The TSF shall provide *'none' and cryptographic authentication* to support user authentication.
FIA_UAU.5.2[MFP]	The TSF shall authenticate any user's claimed identity according to the *following rules*:

MFP_ACP_UAU5_21 The 'none' authentication is performed with anyone who communicates with the TOE in SL0. The 'none' authentication implicitly and solely authenticates the Personaliser.

MFP_ACP_UAU5_22 The cryptographic authentication is used in SL0 to authenticate the OriginalityKeyUser.

MFP_ACP_UAU5_23 The cryptographic authentication is used in SL1 to authenticate the OriginalityKeyUser, the CardAdmin, the CardManager, the SecurityLevelManager, the SectorSecurityLevelManager and the CardUser.

MFP_ACP_UAU5_24 The cryptographic authentication is used in SL3 to authenticate the OriginalityKeyUser, the CardAdmin, the CardManager, and the CardUser.

The TOE shall meet the requirements "Trusted Path (FTP_TRP.1[MFP])" as specified below.

FTP_TRP.1[MFP]	**Trusted Path**
Hierarchical-To	No other components.
Dependencies	No dependencies.
FTP_TRP.1.1[MFP]	The TSF shall provide a communication path between itself and *remote* 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 and disclosure or only modification*.
FTP_TRP.1.2[MFP]	The TSF shall permit *remote users* to initiate communication via the trusted path.
FTP_TRP.1.3[MFP]	The TSF shall require the use of the trusted path for *authentication requests, confidentiality and/or integrity verification for data transfers based on the settings in the MFPConfigurationBlock and the SectorTrailers.*

The TOE shall meet the requirements ”Cryptographic Key Destruction (FCS_CKM.4[MFP])” as specified below.

FCS_CKM.4[MFP]	**Cryptographic Key Destruction**
Hierarchical-To	No other components.
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.4.1[MFP]	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *overwriting* that meets the following: *none.*

The TOE shall meet the requirements ”Inter-TSF Basic TSF Data Consistency (FPT_TDC.1[MFP])” as specified below.

FPT_TDC.1[MFP]	**Inter-TSF Basic TSF Data Consistency**
Hierarchical-To	No other components.
Dependencies	No dependencies.
FPT_TDC.1.1[MFP]	The TSF shall provide the capability to consistently interpret *data Blocks* when shared between the TSF and another trusted IT product.
FPT_TDC.1.2[MFP]	The TSF shall use *the rules: data Blocks can always be modified by the Block.Write operation. If a data Block is in the data Value format it can be modified by all dedicated Value-specific operations honouring the Value-specific boundaries. SectorTrailers must have a specific format* when interpreting the TSF data from another trusted IT product.
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. Instead the TOE distinguishes different types of Blocks and ensures that type-specific boundaries cannot be violated, e.g Values do not overflow. For SectorTrailers the TOE enforces a specific format.

6.1.4 Additional SFRs regarding Robustness

The TOE shall meet the requirements ”Replay detection (FPT_RPL.1[MFP])” as specified below.

FPT_RPL.1[MFP] **Replay detection**

Hierarchical-To	No other components.
Dependencies	No dependencies.
FPT_RPL.1.1[MFP]	The TSF shall detect replay for the following entities: *authentication requests, confidentiality and/or integrity verification for data transfers based on the settings in the MFPConfigurationBlock and the SectorTrailers.*
FPT_RPL.1.2[MFP]	The TSF shall perform *rejection of the request* when replay is detected.

The TOE shall meet the requirements "Unlinkability (FPR_UNL.1[MFP])" as specified below.

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

6.2 Security Assurance Requirements

Table 6.29 below lists all security assurance components that are valid for this Security Target. With two exceptions these security assurance components are required by EAL5 (see section 2.3) or by the Protection Profile. The exceptions are the components ASE_TSS.2 and ALC_FLR.1 which are chosen as an augmentation in this Security Target. ASE_TSS.2 is chosen to give architectural information on the security functionality of the TOE. ALC_FLR.1 is chosen to give assurance that the TOE will be maintained and supported in the future.

The refinements of the Protection Profile that must be adapted for EAL5 are described in section 6.2.1.

Name	Title
ADV_ARC.1	Security architecture description
ADV_FSP.5	Complete semi-formal functional specification with additional error information
ADV_IMP.1	Implementation representation of the TSF
ADV_INT.2	Well-structured internals
ADV_TDS.4	Semiformal modular design
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.4	Production support, acceptance procedures and automation
ALC_CMS.5	Development tools CM coverage
ALC_DEL.1	Delivery procedures
ALC_DVS.2	Sufficiency of security measures
ALC_FLR.1	Basic flaw remediation

Name	Title
ALC_LCD.1	Developer defined life-cycle model
ALC_TAT.2	Compliance with implementation standards
ASE_INT.1	ST introduction
ASE_CCL.1	Conformance claims
ASE_SPD.1	Security problem definition
ASE_OBJ.2	Security objectives
ASE_ECD.1	Extended components definition
ASE_REQ.2	Derived security requirements
ASE_TSS.2	TOE summary specification with architectural design summary
ATE_COV.2	Analysis of coverage
ATE_DPT.3	Testing: modular design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing - sample
AVA_VAN.5	Advanced methodical vulnerability analysis

Tab. 6.29: Security Assurance Requirements

6.2.1 Refinements of the TOE Security Assurance Requirements

In compliance to Application Note 23 in the Protection Profile, this Security Target has to conform to all refinements of the security assurance requirements in the Protection Profile. Because the refinements in the Protection Profile are defined for the security assurance components of EAL4 (augmented by ALC_DVS.2 and AVA_VAN.5), some refinements have to be applied to assurance components of the higher level EAL5 stated in the Security Target.

Table 6.30 lists the influences of the refinements of the Protection Profile on the Security Target. Most of the refined security assurance components have the same level in both documents (Protection Profile and Security Target). The following two subsections apply the refinements to ALC_CMS.5 and ADV_FSP.5, which are different between the Protection Profile and the Security Target.

SAR in PP[13]	Effect on the Security Target
ALC_DEL.1	Same as in PP, refinement valid without change
ALC_DVS.2	Same as in PP, refinement valid without change
ALC_CMS.4	ALC_CMS.5, refinements valid without change
ALC_CMC.4	Same as in PP, refinement valid without change
ADV_ARC.1	Same as in PP, refinement valid without change
ADV_FSP.4	ADV_FSP.5, refinements have to be adapted
ADV_IMP.1	Same as in PP, refinement valid without change

SAR in PP[13]	Effect on the Security Target
ATE_COV.2	Same as in PP, refinement valid without change
AGD_OPE.1	Same as in PP, refinement valid without change
AGD_PRE.1	Same as in PP, refinement valid without change
AVA_VAN.5	Same as in PP, refinement valid without change

Tab. 6.30: SARs refined in the PP [13] and their effect on this ST

6.2.1.1 Refinements regarding CM scope (ALC_CMS)

This Security Target requires a higher evaluation level for the CC family ALC_CMS, namely ALC_CMS.5 instead of ALC_CMS.4. The refinement of the Protection Profile regarding ALC_CMS.4 is a clarification of the configuration item ”TOE implementation representation”. Since in ALC_CMS.5, the content and presentation of evidence element ALC_CMS.5.1C only adds a further configuration item to the list of items to be tracked by the CM system, the refinement can be applied without changes.

The refinement of the configuration item ”TOE implementation representation” of ALC_CMS.4 can be found in section 6.2.1.3 of the Protection Profile and is not cited here.

6.2.1.2 Refinements regarding ADV_FSP

This Security Target requires a higher evaluation level for the CC family ADV_FSP, namely ADV_FSP.5 instead of ADV_FSP.4. The refinement of the Protection Profile regarding ADV_FSP.4 is concerned with the complete representation of the TSF, the purpose and method of use of all TSFI, and the accuracy and completeness of the SFR instantiations. The refinement is not a change in the wording of the action elements, but a more detailed definition of the above items.

The higher level ADV_FSP.5 requires a Functional Specification in a ”semi-formal style” (ADV_FSP.5.2C). The component ADV_FSP.5 enlarges the scope of the error messages to be described from those resulting from an invocation of a TSFI (ADV_FSP.5.6C) to also those not resulting from an invocation of a TSFI (ADV_FSP.5.7C). For the latter a rationale shall be provided (ADV_FSP.5.8C).

Since the higher level ADV_FSP.5 only affects the style of description and the scope of and rationale for error messages, the refinements can be applied without changes and are valid for ADV_FSP.5. The refinement of the original component ADV_FSP.4 can be found in section 6.2.1.6 of the Protection Profile and is not cited here.

6.3 Security Requirements Rationale

6.3.1 Rationale for the Security Functional Requirements

Section 6.3.1 in the 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.

SO	SFR
O.Leak-Inherent	FDP_ITT.1[HW] FDP_IFC.1 FPT_ITT.1[HW]
O.Phys-Probing	FDP_SDC.1[HW] FPT_PHP.3
O.Malfunction	FPT_FLS.1 FRU_FLT.2
O.Phys-Manipulation	FDP_SDI.2[HW] FPT_PHP.3
O.Leak-Forced	FDP_ITT.1[HW] FDP_IFC.1 FPT_FLS.1 FPT_ITT.1[HW] FPT_PHP.3 FRU_FLT.2
O.Abuse-Func	FDP_ITT.1[HW] FDP_IFC.1 FMT_LIM.1[HW] FMT_LIM.2[HW] FPT_FLS.1 FPT_ITT.1[HW] FPT_PHP.3 FRU_FLT.2
O.Identification	FAU_SAS.1[HW]
O.RND	FCS_RNG.1[HW] FDP_ITT.1[HW] FDP_IFC.1 FPT_FLS.1 FPT_ITT.1[HW] FPT_PHP.3 FRU_FLT.2 FCS_RNG.1[DET]

Tab. 6.31: Security Functional Requirements vs. Security Objectives (PP0084)

The Security Target additionally defines the SFRs for the TOE that are listed in Table 6.32. In addition, Security Requirements for the Environment are defined. The following table gives an overview, how the requirements are combined to meet the security objectives.

SO	SFR
O.Access-Control	FCS_CKM.4[MFP] FDP_ACC.1[MFP] FDP_ACF.1[MFP] FDP_ITC.2[MFP] FMT_MSA.1[MFP] FMT_MSA.3[MFP] FMT_MTD.1[MFP] FMT_SMF.1[MFP] FMT_SMR.1[MFP]
O.Authentication	FCS_COP.1[MFP-AES] FIA_UID.2[MFP] FIA_UAU.2[MFP] FIA_UAU.5[MFP] FMT_SMF.1[MFP] FPT_RPL.1[MFP] FTP_TRP.1[MFP]
O.Type-Consistency	FPT_TDC.1[MFP]
O.No-Trace	FPR_UNL.1[MFP]
O.Encryption	FCS_CKM.4[MFP] FCS_COP.1[MFP-AES] FTP_TRP.1[MFP]
O.MAC	FCS_CKM.4[MFP] FCS_COP.1[MFP-AES] FPT_RPL.1[MFP] FTP_TRP.1[MFP]

Tab. 6.32: Security Functional Requirements vs. Security Objectives (ST)

Justification related to ”Access Control (O.Access-Control)”

The SFR FMT_SMR.1[MFP] defines the roles of the Access Control Policy. The SFR FDP_ACC.1[MFP] and FDP_ACF.1[MFP] define the rules and FMT_MSA.3[MFP] and FMT_MSA.1[MFP] the attributes that the access control is based on. FMT_MTD.1[MFP] provides the rules for the management of the authentication data. The management functions are defined by FMT_SMF.1[MFP]. Since the TOE stores data on behalf of the authorised subjects, import of user data with security attributes is defined by FDP_ITC.2[MFP]. 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[MFP]. These nine SFR together provide an access control

mechanism as required by the objective O.Access-Control.

Justification related to "Authentication (O.Authentication)"

The SFRs FCS_COP.1[MFP-AES] requires that the TOE provides the basic cryptographic algorithm that can be used to perform the authentication. The SFRs FIA_UID.2[MFP], FIA_UAU.2[MFP] and FIA_UAU.5[MFP] together define that users must be identified and authenticated before any action. FMT_SMF.1[MFP] defines security management functions the TSF shall be capable to perform. FTP_TRP.1[MFP] requires a trusted communication path between the TOE and remote users, FTP_TRP.1.3[MFP] especially requires "authentication requests". Together with FPT_RPL.1[MFP] which requires a replay detection for these authentication requests the seven SFRs fulfill the objective O.Authentication.

Justification related to "Confidential Communication (O.Encryption)"

The SFR FCS_COP.1[MFP-AES] requires that the TOE provides the basic cryptographic algorithms that can be used to protect the communication by encryption. FTP_TRP.1[MFP] requires a trusted communication path between the TOE and remote users, FTP_TRP.1.3[MFP] especially requires a trusted path for "authentication requests, confidentiality and/or data integrity verification for data transfers based on a setting in the MFPConfigurationBlock". FCS_CKM.4[MFP] requires that cryptographic keys used for encryption have to be removed after usage. These three SFRs fulfill the objective O.Encryption.

Justification related to "Integrity-Protected Communication (O.MAC)"

The SFR FCS_COP.1[MFP-AES] 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[MFP] requires a trusted communication path between the TOE and remote users, FTP_TRP.1.3[MFP] especially requires "confidentiality and/or data integrity verification for data transfers on request of the file owner". FCS_CKM.4[MFP] requires that cryptographic keys used for MAC operations have to be removed after usage. Together with FPT_RPL.1[MFP] which requires a replay detection for these data transfers, the four SFRs fulfill the objective O.MAC.

Justification related to "Data type consistency (O.Type-Consistency)"

The SFR FPT_TDC.1[MFP] requires the TOE to consistently interpret data blocks. The TOE will honour the respective file formats and boundaries (i.e. upper and lower limits, size limitations). This meets the objective O.Type-Consistency.

Justification related to "Preventing Traceability (O.No-Trace)"

The SFR FPR_UNL.1[MFP] 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.

6.3.2 Dependencies of Security Functional Requirements

The dependencies listed in the Protection Profile are independent of 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 SFR dependencies (defined by Part 2 of the Common Criteria [3]) satisfy the requirements specified in section 6.1.

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

SFR	Dependencies	Fulfilled by Security Requirements in the ST
FAU_SAS.1[HW]	No dependencies.	No dependency
FCS_RNG.1[HW]	No dependencies.	No dependency
FCS_RNG.1[DET]	No dependencies.	No dependency
FDP_ITT.1[HW]	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	Yes
FDP_IFC.1	FDP_IFF.1 Simple security attributes	See discussion in the PP
FDP_SDC.1[HW]	No dependencies.	No dependency
FDP_SDI.2[HW]	No dependencies.	No dependency
FMT_LIM.1[HW]	FMT_LIM.2 Limited availability.	Yes
FMT_LIM.2[HW]	FMT_LIM.1 Limited capabilities.	Yes
FPT_FLS.1	No dependencies.	No dependency
FPT_ITT.1[HW]	No dependencies.	No dependency
FPT_PHP.3	No dependencies.	No dependency
FRU_FLT.2	FPT_FLS.1 Failure with preservation of secure state.	Yes

Tab. 6.33: Dependencies of Security Functional Requirements (Protection Profile [13])

SFR	Dependencies	Fulfilled by Security Requirements in the ST
FCS_CKM.4[MFP]	[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]	Yes, by FDP_ITC.2[MFP].

SFR	Dependencies	Fulfilled by Security Requirements in the ST
FCS_COP.1[MFP-AES]	[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.	Yes, by FDP_ITC.2[MFP]. Yes, by FCS_CKM.4[MFP].
FDP_ACC.1[MFP]	FDP_ACF.1 Security attribute based access control.	Yes, by FDP_ACF.1[MFP].
FDP_ACF.1[MFP]	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	Yes, by FDP_ACC.1[MFP]. Yes, by FMT_MSA.3[MFP].
FDP_ITC.2[MFP]	[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	Yes, by FDP_ACC.1[MFP]. Yes, by FTP_TRP.1[MFP]. Yes, by FPT_TDC.1[MFP].
FIA_UID.2[MFP]	No dependencies.	No dependency
FIA_UAU.2[MFP]	FIA_UID.1 Timing of identification	Yes, by FIA_UID.2[MFP].
FIA_UAU.5[MFP]	No dependencies.	No dependency
FMT_MSA.1[MFP]	[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	Yes, by FDP_ACC.1[MFP]. Yes, by FMT_SMR.1[MFP]. Yes, by FMT_SMF.1[MFP].
FMT_MSA.3[MFP]	FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles	Yes, by FMT_MSA.1[MFP]. Yes, by FMT_SMR.1[MFP].
FMT_MTD.1[MFP]	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	Yes, by FMT_SMR.1[MFP]. Yes, by FMT_SMF.1[MFP].
FMT_SMF.1[MFP]	No dependencies.	No dependency
FMT_SMR.1[MFP]	FIA_UID.1 Timing of identification	Yes, by FIA_UID.2[MFP].
FPR_UNL.1[MFP]	No dependencies.	No dependency
FPT_RPL.1[MFP]	No dependencies.	No dependency

SFR	Dependencies	Fulfilled by Security Requirements in the ST
FPT_TDC.1[MFP]	No dependencies.	No dependency
FTP_TRP.1[MFP]	No dependencies.	No dependency

Tab. 6.34: Dependencies of Security Functional Requirements (Security Target)

6.3.3 Rationale for the Assurance Requirements

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

The rationale for the augmentations is the same as in the Protection Profile. The assurance level EAL5 is an elaborated pre-defined level of the CC, part 3 [4]. 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 EAL5. Therefore, these components add additional assurance to EAL5, but the mutual support of the requirements is still guaranteed.

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.

7 TOE Summary Specification

7.1 Portions of the TOE Security Functionality

The TSF directly corresponds to the TOE security functional requirements defined in Section 6.

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

Remark 2. Parts of the security functionality are configured at the end of phase 3 and the whole security functionality is already active during the delivery from phase 3 to phase 4.

The TSF described in the following is split into Security Services and Security Features.

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 authentication is based on AES with 128 bit, according to FIPS PUB 197 [6]. A pseudo-random number generator according to AIS20, functionality class K3, is used to protect the authentication against attacks like e.g. replay.

SS.AUTH identifies the user to be authenticated by the key block number indicated in the authentication request. In SL0 the TOE identifies and authenticates the Personaliser by default, in addition the OriginalityKeyUser can be identified with an explicit authentication request. In the other SecurityLevels SS.AUTH by default and before any authentication request identifies and authenticates the role Anybody. The roles CardAdmin, CardManager, SecurityLevelManager, CardUser and OriginalityKeyUser 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, Selection and Deselection of the Virtual Card, Switching the SecurityLevel of the TOE, DESELECT according to ISO 14443-3 [17], 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 MFP Access Control Policy.

The access control mechanism assigns CardUsers to 4 different groups of operations on Blocks. The operations are "Block.Read", "Block.Write", "Value.Increase", "Value.Decrease, Value.Transfer and Value.Restore", whereby the last two groups are only applicable if the data is in the Value format. 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. CardUsers can also modify the SectorTrailer or the AESSectorKeys, if the access conditions allow this.

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

The CardAdmin can modify the MFPConfigurationBlock, which are attributes that do not have to be changed in the field. He is also allowed to change the CardMasterKey. The CardAdmin can change the Level3SwitchKey, the Level3SectorSwitchKey and the CardMasterKey itself. The CardAdmin can also change the TransMACConfKey.

The CardManager can modify the FieldConfigurationBlock, which are attributes that may have to be changed in the field. He is also allowed to change the Card CardConfigurationKey.

The SecurityLevelManager can switch the SecurityLevel of the card to a higher level by authenticating with the corresponding key. The MFP Access Control Policy and therefore SS.ACC_CTRL has to take care that all Sectors are initialized with permissive default values in the SectorTrailer, this means the contained access conditions shall allow the CardUser to access all Blocks.

Finally SS.ACC_CTRL ensures the type consistency of the Blocks stored by the TOE. It ensures that Values cannot over- or underflow. Furthermore size limitations of Blocks are obeyed.

SS.ENCRYPTION **Encryption**

SS.ENCRYPTION provides a mechanism to protect the communication against eavesdropping. In order to do this, the data sent via wireless communication must be encrypted.

The encryption algorithm is the same as the one used during authentication for the session, therefore the same cryptographic algorithm as described for SS.AUTH is supported by SS.ENCRYPTION. Note that encryption can be set optional or mandatory on a Block group basis in the SectorTrailer.

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, replace attacks or man-in-the-middle attacks.

The TOE offers multiple modes in which protection by MAC is optional or mandatory for both communication parties. Regardless of the selected mode the terminal must always provide a MAC for commands that modify

any TOE item (data or security attributes). The TOE does also provide a mode in which the MAC on its responses can be cumulated, i.e. the last response contains a MAC that covers previously sent frames without MAC.

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

SS.TRANSACTION_MAC **Transaction Message Authentication Code**

SS.TRANSACTION_MAC provides an option to furnish transactions to be committed with an additional MAC calculation. This feature can be activated with the help of one of the TransMACKeys. There exist four of these keys in total, each of them might be associated with one or more dedicated Blocks.

SS.TRANSACTION_MAC is a security service on Block Level, it is activated by assigning one of the four TransMACKeys to one or more designated Blocks. SS.TRANSACTION_MAC provides a service to CardUsers and the TransMACConfManager as it helps CardUsers to prove the authenticity of commited transactions on the TOE towards the Personaliser or CardAdmin. The transaction MAC, calculated by SS.TRANSACTION_MAC, also involves a Transaction MAC Counter maintained by the TOE, which helps the Personaliser or CardAdmin to detect replay.

SS.NO_TRACE **Preventing Traceability**

SS.NO_TRACE provides an option to use a random ID during the ISO14443 anti-collision sequence [17]. 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 CardManager since it belongs to the FieldConfigurationBlock.

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 MFP Access Control Policy implemented by SS.ACC_CTRL. In order to prevent traceability at all the authorised subjects can make use of the confidentiality protection implemented by SS.ENCRYPTION.

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**

SF.OPC ensures the correct operation of the TOE (functions offered by the micro-controller including the standard CPU as well as the unified AES/Triple-DES co-processor, the memories, registers, I/O interfaces and the other system peripherals) during the execution of the IC Dedicated Support 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 by means of three kinds of features:

Environmental Control: Set of security mechanisms that detect if the TOE runs out of the specified operation conditions. It needs to be assured that in operation mode all ambient conditions are within their specified limits. Sensors take over the role of measuring the ambient conditions and reacting in case of specification violation of one of the ambient parameters. If a sensor monitors a violation of the specified ambient conditions, a reset is triggered. Depending on the type of sensor the reset might be a security reset that decrements the error counter.

Execution Integrity Set of security mechanisms that detect if an execution of an operation has been manipulated. It needs to be assured that manipulations on operations are detected and trigger a reset that effects the error counter. Manipulating operations means the operation itself is attacked. On an abstract view this could mean that some kind of memory (e.g. register) has been attacked. On a more detailed view it can also mean that entire wires or gates are attacked. Executing integrity is achieved by means such as the following ones:

- validity checking of in- and output of security critical operations
- integrity protection of data, code and address path
- integrity protection of memories, data registers, key registers and control registers
- monitoring state machines
- integrity protection of sensor signals
- double calculations and checks

Integrity protection is achieved by various techniques, such as parity protection, redundant encoding and execution, monitoring, CRCs.

Availability Set of security mechanisms that take care that the availability of the TOEs functionality is limited if attacks occur. It needs to be assured that the detection of an attack results in secure state. This is achieved by the fact that any kind of attack or operation outside the operation conditions results in a reset where the

TOE boots in the initial configuration. Depending in the kind of reset source the reset might also have an effect on the error counter. This is especially the case for integrity violations that cannot be unintended ones.

SF.PHY **Protection against Physical Manipulation**

The feature SF.PHY protects the TOE against manipulation of

(i) the hardware,

(ii) the IC Dedicated Software in the non-volatile memory, and

(iii) the application data in the RAM and EEPROM including the configuration data stored in EEPROM.

It also protects all data stored in the memories including User Data and TSF data against disclosure by physical probing when stored or while being processed by the TOE.

The TOE ensures its correct operation and prevents any malfunction by means of several kinds of features:

- **Layout Protection:** Set of security mechanisms that hamper reverse engineering of the IC, such as layout randomization, active and passive shielding, techniques to hide shielding, multilayer interconnection, wide bus widths and dummy routing.
- **Code- & Datapath Integrity Protection:** Set of security mechanisms that ensure that manipulations on data or code stored and transmitted from respectively to the CPU are detected with high probability. This includes integrity protection of the whole code and data path including CPU internals. Integrity verification is always done before the according data is processed via e.g. an ALU operation.
- **Memory Integrity Protection:** Set of security mechanisms that ensure that manipulations on memory content are detected with high probability. This includes integrity protection of memories and registers. EEPROM are additionally equipped with error correction codes, double read technology and anti-tearing.
- **Address Path Integrity Protection:** Set of security mechanisms that ensure that manipulations on the address path are detected with high probability.
- **Startup Integrity Protection:** Set of security mechanisms that detect integrity errors during startup (e.g. with respect to configuration data).
- **Redundant Encoding:** Set of security mechanisms that ensure that security critical flags and the according checks are kept with an according level of redundancy.
- **Code Integrity Protection:** Set of security mechanisms that detect if code has been manipulated.
- **Code- & Datapath Encryption:** Set of security mechanisms that ensure that code or data processed by the CPU is stored and transmitted in encrypted form. All data transmitted over the code or datapath is encrypted with an address-dependent non-linear encryption scheme. En- and decryptions are performed in the CPU core.

- **Address Scrambling:** Set of security mechanisms that ensure that physical addresses are scrambled before writing data to the memory.
- **Code- & Datapath Key Management:** Set of security mechanisms that ensure that keys used for the secure data path are derived correctly and securely. This includes address dependent key derivation functionality with an according strength of diffusion and confusion to achieve a good avalanche effect.

Note that the TOE does also support the Proximity Check feature against relay attacks on the TOE. The proximity check feature is an optional challenge response protocol on which the round trip time is measured by the terminal.

SF.LOG	**Logical Protection** SF.LOG implements measures to limit or eliminate the information that might be contained in the shape and amplitude of signals or in the time between events found by measuring such signals. This comprises the power consumption and signals on the other pads that are not intended by the terminal or the Security IC Embedded Software. Thereby SF.LOG prevents the disclosure of User Data or TSF data stored and/or processed in the security IC through the measurement of the power consumption or emanation and subsequent complex signal processing. The protection of the TOE comprises different features within the design that support the other portions of security functionality.
SF.COMP	**Protection of Mode Control** SF.COMP provides a control of the TOE modes. This includes the protection of electronic fuses stored in a protected memory area, and the possibility to store initialisation or pre-personalisation data in the so-called FabKey Area.

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

The switch to the IC Dedicated Test Software is prevented after TOE delivery because specific electronic fuses guarantee that the IC Dedicated Test Software cannot be selected. The System Mode is the more privileged TOE mode, the User Mode is the less privileged TOE mode. The System Mode HAL Software as part of the IC Dedicated Support Software is executed in System Mode. For the MIFARE Plus Software, only the User Mode is available. The protection of the electronic fuses especially ensures that configuration options with regard to the security functionality cannot be changed, abused or influenced in any way in User Mode. SF.COMP ensures that activation or deactivation of security features cannot be influenced by the MIFARE Plus Software.

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

7.2 TOE Summary Specification Rationale

7.2.1 Rationale for assurance measures

The assurance measures defined in section 6.2 are considered to fulfil the assurance requirements of the Common Criteria, Part 3 [4] at level EAL5 augmented. Since the Protection Profile defines assurance measures that are suitable to fulfil the requirements of EAL4, all input deliverables as listed in section 6.2 shall be sufficient to fulfil the assurance requirements of the Protection Profile. The assurance measures are defined especially for the development and production of Smartcard ICs and observe also the refinements made in the Protection Profile.

As already explained in the Protection Profile, annex 7.1, the development and production process of a smartcard IC is complex. Regarding the great number of assurance measures, a detailed mapping of the assurance measures to the assurance requirements is beyond the scope of this Security Target. Nevertheless the suitability of the assurance measures is subject of different evaluation tasks. The documents "Quality Management Manual" and "Security Management Manual" describe the general benchmark of NXP.

7.2.2 Security architectural information

Since this Security Target claims the assurance requirement ASE_TSS.2, security architectural information on a very high level is supposed to be included in the TSS to inform potential customers on how the TOE protects itself against interference, logical tampering and bypassing. In the security architecture context, this covers the aspects self-protection and non-bypassability.

The self-protection and non-bypassability of the TOE is implemented by internal integrity checks of the stored data e.g. SS.ACC_CTRL, appropriate configuration of the hardware platform by enabling countermeasures controlled by the software and by countermeasures implemented in the software. SS.MAC provides protection regarding the integrity control of exchanged messages. SS.ENCRYPTION and SS.TRANSACTION_MAC provide protection against logical interference based on the control of transaction sequences.

SS.AUTH requires an authentication before specific operations are allowed. SS.AUTH authentication uses 128-bit AES cryptographic algorithm according to FIPS PUB 197 [6]. Furthermore 16 Byte random challenges are used for SS.AUTH. Any context change or error resets the authentication status to prevent the bypass of the authentication request. SS.ACC_CTRL is also implemented in a way that supports the protection against interference, logical tampering and bypass. SS.NO_TRACE contributes to the self-protection of the TOE by

protecting card specific data. Using SS.NO_TRACE and SS.ACC_CTRL ensures that traceability of end-users is prevented.

8 Bibliography

[1] A proposal for: Functionality classes for random number generators, Version 2.0, 18. September 2011.

[2] Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model - Version 3.1 CCMB-2012-09-001, Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components, Version 3.1 CCMB-2012-09-002, Revision 4, September 2012.

[4] Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components, Version 3.1 CCMB-2012-09-003, Revision 4, September 2012.

[5] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1 CCMB-2012-09-004, Revision 4, September 2012.

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

[7] MF1P(H)x1y1 - Information on Guidance and Operation, Guidance and Operation Manual, NXP Semiconductors, Document number 333511.

[8] MF1P(H)x1y1 - MIFARE Plus EV1, Product Data Sheet, NXP Semiconductors, Document number 322620.

[9] MF1P(H)x1y1 PDC - MIFARE Plus EV1 Post Delivery Configuration, Product Data Sheet Addendum, NXP Semiconductors, Document number 322712.

[10] MIFARE Plus EV1 - MF1P(H)x1y1, Security Target, NXP Semiconductors.

[11] NIST Special Publication 800-38A Recommendation for BlockCipher Modes of Operation. http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf.

[12] NIST Special Publication 800-38B Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication. http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf.

[13] Security IC Platform Protection Profile with Augmentation Packages, registered and certified by Bundesamt fuer Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014, Version 1.0, 13 January 2014.

[14] ISO/IEC 14443-1:2000 Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 1: Physical characteristics, 2008.

[15] ISO/IEC 14443-4:2001 Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 4: Transmission protocol, 2008.

[16] ISO/IEC 14443-2:2001 Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 2: Radio frequency power and signal interface, 2010.

[17] ISO/IEC 14443-3:2001 Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 3: Initialization and anticollision, 2011.

[18] Bundesamt für Sicherheit in der Informationstechnik. Anwendungshinweise und Interpretationen zum Schema, AIS20: Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Bundesamt für Sicherheit in der In formationstechnik. Version 2.0, December 2, 1999.

[19] Bundesamt für Sicherheit in der Informationstechnik. Anwendungshinweise und Interpretationen zum Schema, AIS31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Bundesamt für Sicherheit in der In formationstechnik. Version 2.0, September 18, 2011.

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

Limited warranty and liability – 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.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

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 life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an 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 at 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.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

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 competent authorities.

Evaluation products – This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer.

In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages.

Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

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.

10 Contents

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

Date of release: 2016-09-27

Document identifier: