MF2DL(H)x0, MF2ID(H)10, NT4H2x21Gf and NT4H2x21Tf

Security Target Lite

Rev. 1.0 – 2018-12-31 **Evaluation documentation**

Final **PUBLIC**

<Certid>

Document Information

Info	Content
Keywords	Common Criteria, Security Target Lite, MF2DL(H)x0, MF2ID(H)10, NT4H2x21Gf, NT4H2x21Tf
Abstract	Evaluation of the MF2DL(H)x0, MF2ID(H)10, NT4H2x21Gf and NT4H2x21Tf product, developed and provided by NXP Semiconductors, Business Unit Security & Connectivity, according to the Common Criteria for Information Technology Evaluation Version 3.1 at EAL4

Rev	Date	Description
1.0	31-December-2018	Initial version of this Security Target Lite based on Security Target Revision 1.9

1 ST Introduction

1.1 ST Reference

MF2DL(H)x0, MF2ID(H)10, NT4H2x21Gf and NT4H2x21Tf Security Target Lite, Revision 1.0, NXP Semiconductors, Date 2018-12-31.

1.2 TOE Reference

MF2DL(H)x0, MF2ID(H)10, NT4H2x21Gf and NT4H2x21Tf, Version 01.1

1.3 TOE Overview

1.3.1 Introduction

NXP has developed the TOE to be used with Proximity Coupling Devices (PCDs, also called "terminals") according to ISO14443 Type A [10][12][13][11]. The communication protocol complies to ISO 14443 part 3 [13] and 4 [11]. The TOE is primarily designed for secure contactless transport applications, loyalty programs, access management, closed loop payment, account based services and secure NFC applications. It fully complies with the requirements for fast and highly secure data transmission and interoperability with existing infrastructure.

The TOE provides resistance against attack of an attacker with an enhanced-basic attack potential. This is achieved by a combination of different security features that provide a base-line protection against information leakage via side-channels, fault injections and physical attacks. Furthermore, the TOE protects the different operating modes of the Security IC to avoid ab-use by an attacker. Protected by these security features the TOE implements the following main security services:

- secure mutual authentication to support authentication of authorized users and the TOE
- secure channel establishment and secure messaging to support confidential and integrity protected data transfer
- secure dynamic messaging to allow secure export of user data in unauthenticated state on MIFARE IDentity and NTAG42x DNA (Tf) variants of the TOE
- supporting non-traceability of the TOE by providing the option to use random IDs during contactless protocol establishment
- enhanced secure transaction management provided by the MIFARE DESFire Light and MIFARE IDentity variants of the TOE
- additional functionality to check the status of a tamper evident tag provided by the NTAG42x DNA Tf variant of the TOE

These security functionalities aim at enabling card issuers to use the product for various use-cases as outlined in the following.

The TOE is a Security IC comprising a hardware platform and a fixed software package. The software is stored in ROM and provides an operating system which implements a set of functions used to manage various kinds of data files stored in the non-volatile EEPROM memory. The operating system provides access control if required by the configuration. The operating system is designed as platform, which supports command sets for four different applications forming four different product variants, in detail:

- **MIFARE DESFire Light**: the MF2DL(H)x0 variant of the TOE (short: MF2DL) is intended for limited-use transport tickets (value and account based), event ticketing (e.g. cinema, game or concert) or access control badges and also loyalty cards. The card reader command set is to be compatible with (a subset of) the MIFARE DESFire EV2 command set.
- **MIFARE IDentity**: the MF2ID(H)10 variant of the TOE (short: MF2ID) is intended for account-based services e.g. account based ticketing in transport application or event management. The card reader command set is to be compatible with (a subset of) the MIFARE DESFire EV2 command set
- **NTAG42x DNA**: the NT4H2x21Gf variant of the TOE (short: NTAG42x) is intended as NFC Forum Type 4 Tag. It might generate Secure Unique NFC Message in each tap for direct access to web services. A subset of the supported card reader command set is to be compatible with the NFC Forum Type 4 Tag standard.
- **NTAG42x DNA Tf**: the NT4H2x21Tf variant of the TOE (short: NTAG42xTf) is identical to NTAG42x DNA, but supports additionally the "tag tamper feature", which allows the user to control when a tamper evidence mechanism has been triggered. This feature supports use cases, where product integrity needs to be verified e.g. seals for high-value liquids.

Remark 1. The reader of this Security Target must be aware, that the references to the different variants of the TOE might vary throughout the document. Depending on the context, one of the available names (as introduced above) might be used. For example, the MIFARE DESFire Light variant of the TOE might be referenced either by the full name (MIFARE DESFire Light), the short name (MF2DL) or the technical name (MF2DL(H)x0). Same holds for other variants of the TOE, where in particular NTAG42x DNA and NTAG42x DNA Tf might be referred to as NTAG42x DNA (Tf) respectively NTAG42x(Tf) when addressing both variants with one identifier.

The concrete product variant is instantiated by NXP during production by properly configuring the operating system platform and the provisioning of a dedicated file system layout. The security features of the platform enforce that once configured to one of above listed products the product variant cannot be further changed.

The customer can optionally provide pre-defined content for the file system via Order Entry Form (OEF) to support customer specific use cases, which is integrated into the TOE by NXP during controlled production process.

The file system is under full control of the access rule management provided by the operating system, which enforces the isolation of the NXP proprietary configuration data, files and keys. In addition, the operating system platform allows for enabling and disabling various configuration options using dedicated command during normal operation. The default settings for these configuration options can also be chosen by the customer for proper setting during production by NXP. In case sufficient security anchors (i.e. customer specific keys) are properly set during production by NXP the customer can safely finalize the pre-personalization and personalization relying on the protection features of the TOE already. In any case the customer must adhere to the guidance requirements for finishing the personalization process.

As a consequence, each variant of the TOE is identified precisely by the version of the underlying hardware and software operating system augmented with the identification of the one of the four main application variants (MIFARE DESFire Light, MIFARE IDentity, NTAG42x DNA and NTAG42x DNA Tf) used for production. The TOE does not provide any code loading or application management functionality after production. The only exception is a feature of the MIFARE DESFire Light variant, which allows renaming the DF in the file system. However, this management feature does not impact the security and in particular the access protection of the file system.

The TOE includes also IC Dedicated Software for test purposes during production. This functionality is permanently blocked once the TOE is configured in user operating mode. The micro-controller comprises a 16-bit processing unit, volatile and non-volatile memories, cryptographic co-processor, security components and one communication interface.

The TOE includes a guidance document and a datasheet for each of the four TOE variants. The different (package) types are described in detail in Section 1.4.1.1.

1.3.2 TOE Type

The TOE is a Security IC comprising a hardware platform, a fixed software package implemented in ROM and a set of data files stored in EEPROM. The TOE is delivered in different formats as described in section 1.4.1.1. For each variant of the product, the documentation consists of:

- The Product Data Sheet providing the functional specification as well as the available interfaces of the variant of the TOE, and
- The Guidance and Operational Manual providing guidelines for secure usage and operation of the security functionality of the variant of the TOE.

All relevant documents are listed in table 1.1, thus being components of the TOE.

1.3.3 Required non-TOE Hardware/Software/Firmware

The TOE requires an ISO 14443 [10, 12, 13, 11] compliant card terminal to be provided with power and to receive adequate commands.

1.4 TOE Description

1.4.1 Physical Scope of TOE

Type	Name	Release	Date	Form of Delivery
Hardware	Analog	Version A1	15.03.2018	Sawn wafer or modules
Hardware	Digital	Version A1	15.03.2018	Sawn wafer or modules
Software	Firmware / OS	Version A1	15.03.2018	ROM on chip
Filesystem	Application Data	Version A1	15.03.2018	EEPROM on chip
Documents	according to tables 1.2, 1.3, 1.4 and 1.5	-	-	Electronic Documents

Tab. 1.1: Components of the TOE

The following TOE components are relevant for the MIFARE DESFire Light variant of the TOE only:

Type	Name	Release	Date	Form of Delivery
Document	MF2DL(H)x0 - MIFARE DESFire Light contactless application IC, Product Data Sheet	430712	05.11.2018	Electronic Document
Document	MF2DL(H)x0 - Information on Guidance and Operation, Guidance and Operation Manual	447910	23.10.2018	Electronic Document

Tab. 1.2: Dedicated components of the MIFARE DESFire Light variant of the TOE

The following TOE components are relevant for the MIFARE IDentity variant of the TOE only:

Type	Name	Release	Date	Form of Delivery
Document	MF2ID(H)10 - MIFARE IDentity - Smart Credential for Account Based Services, Product Data Sheet	465612	05.11.2018	Electronic Document
Document	MF2ID(H)10 - Information on Guidance and Operation, Guidance and Operation Manual	448010	23.10.2018	Electronic Document

Tab. 1.3: Dedicated components of the MIFARE IDentity variant of the TOE

The following TOE components are relevant for the NTAG42x DNA variant of the TOE only:

Type	Name	Release	Date	Form of Delivery
Document	NT4H2421Gx - NTAG 424 DNA - Secure NFC T4T compliant IC, Product Data Sheet	465411	13.11.2018	Electronic Document
Document	NT4H2621Gx - NTAG 426 DNA - Secure NFC T4T compliant IC, Product Data Sheet	510310	13.11.2018	Electronic Document
Document	NT4H2x21Gf - Information on Guidance and Operation, Guidance and Operation Manual	448111	14.11.2018	Electronic Document

Tab. 1.4: Dedicated components of the NTAG42x DNA variant of the TOE

The following TOE components are relevant for the NTAG42x DNA Tf variant of the TOE only:

Type	Name	Release	Date	Form of Delivery
Document	NT4H2421Tx - NTAG 424 DNA TT - Secure NFC T4T compliant IC with Tag Tamper feature, Product Data Sheet	465511	13.11.2018	Electronic Document
Document	NT4H2621Tx - NTAG 426 DNA TT - Secure NFC T4T compliant IC with Tag Tamper feature, Product Data Sheet	510410	13.11.2018	Electronic Document
Document	NT4H2x21Tf - Information on Guidance and Operation, Guidance and Operation Manual	448211	14.11.2018	Electronic Document

Tab. 1.5: Dedicated components of the NTAG42x DNA Tf variant of the TOE

1.4.1.1 Evaluated Chip and Package Types

A number of package types are supported for the TOE. Each package type has a different commercial type name. Find below the overview for the four variants:

- A commercial type name for the MIFARE DESFire Light variant has the following general format: MF2DL*cyeffdpp*/*vvkk*

Type	*c*	*y*	*e*	*ff*	*d*	*pp*	/	*vv*	*kk*
MF2DL	H	0	0	01	D	A4	/	01	01
...	...	...	...	...	...	...	/	...	...

Tab. 1.6: Supported Types for MIFARE DESFire Light variant

Identifier	Description	Valid Values	Digits	Assignment	Meaning
c	input capacitance	alphanumeric	0 – 1	”	17 pF
				H	50 pF

Identifier	Description	Valid Values	Digits	Assignment	Meaning
y	memory size	numeric	1	0 1 2	No optional standard data file Optional (256 byte) standard data file Optional (512 byte) standard data file
e	evolution	numeric	1	0	the first evolution of MIFARE DESFire Light
ff	FAB produced	numeric	2	01	SSMC
d	operating temperature range	alphabetic	1	D	$-25 < t_{\text{operating}} < 70$
pp	package type	alphanumeric	2	Ux A4 A8	according to table 1.14 MOA4 module MOA8 module
vv	Product Revision	hexadecimal	2	01	Revision 1
kk	Fabkey Identifier	hexadecimal	2	” 01, ..., FF	Default Personalisation Content Dedicated Personalisation Content

Tab. 1.7: Variable Definitions for Commercial Type Names of MIFARE DESFire Light

- A commercial type name for the MIFARE IDentity variant has the following general format: MF2ID*cyeffdpp*/*vvkk*

Type	*c*	*y*	*e*	*ff*	*d*	*pp*	*/*	*vv*	*kk*
MF2ID	H	1	0	01	D	UD	/	01	
...	...	...	...	...	...	...	/	...	...

Tab. 1.8: Supported Types for MIFARE IDentity variant

Identifier	Description	Valid Values	Digits	Assignment	Meaning
c	input capacitance	alphanumeric	0 – 1	” H	17 pF 50 pF
y	memory size	numeric	1	1	Standard MIFARE IDentity file system
e	evolution	numeric	1	0	the first evolution of MIFARE IDentity
ff	FAB produced	numeric	2	01	SSMC
d	operating temperature range	alphabetic	1	D	$-25 < t_{\text{operating}} < 70$
pp	package type	alphanumeric	2	Ux A4 A8	according to table 1.14 MOA4 module MOA8 module
vv	Product Revision	hexadecimal	2	01	Revision 1
kk	Fabkey Identifier	hexadecimal	2	” 01, ..., FF	Default Personalisation Content Dedicated Personalisation Content

Tab. 1.9: Variable Definitions for Commercial Type Names of MIFARE IDentity

- A commercial type name for the NTAG42x DNA variant has the following general format: NT4*cxe*G*fdpp*/*vvkk*

Type	*c*	*x*	*e*	*Gf*	*d*	*pp*	*/*	*vv*	*kk*
NT4	H2	4	21	G0	D	A8	/	01	FF
...	...	...	...	...	...	...	/	...	...

Tab. 1.10: Supported Types for NTAG42x DNA variant

Identifier	Description	Valid Values	Digits	Assignment	Meaning
c	input capacitance	alphanumeric	2	H2	50 pF
x	memory size	numeric	1	4	NDEF file of 256 byte
				6	NDEF file of 768 byte
e	evolution	numeric	2	21	the first evolution of NTAG42x DNA
Gf	NTAG configuration	numeric	2	G0	Default
				GS	Service Type
				GC	Customized Type
d	operating temperature range	alphabetic	1	D	$-25 < t_{\text{operating}} < 70$
pp	package type	alphanumeric	2	Ux	according to table 1.14
				A8	MOA8 module
vv	Product Revision	hexadecimal	2	01	Revision 1
kk	Fabkey Identifier	hexadecimal	2	”	Default Personalisation Content
				01, ..., FF	Dedicated Personalisation Content

Tab. 1.11: Variable Definitions for Commercial Type Names of NTAG42x DNA

- A commercial type name for the NTAG42x DNA Tf variant has the following general format: NT4*cxe*T*fdpp*/*vvkk*

Type	*c*	*x*	*e*	*Tf*	*d*	*pp*	*/*	*vv*	*kk*
NT4	H2	4	21	TT	D	UX	/	01	FF
...	...	...	...	...	...	...	/	...	...

Tab. 1.12: Supported Types for NTAG42x DNA Tf variant

Identifier	Description	Valid Values	Digits	Assignment	Meaning
c	input capacitance	alphanumeric	2	H2	50 pF
x	memory size	numeric	1	4	NDEF file of 256 byte
				6	NDEF file of 768 byte
e	evolution	numeric	2	21	the first evolution of NTAG42x DNA Tf
Tf	NTAG configuration	numeric	2	TT	Default
				TS	Service Type

Identifier	Description	Valid Values	Digits	Assignment	Meaning
				TC	Customized Type
d	operating temperature range	alphabetic	1	D	$-25 < t_{\text{operating}} < 70$
pp	package type	alphanumeric	2	Ux	according to table 1.14
vv	Product Revision	hexadecimal	2	01	Revision 1
kk	Fabkey Identifier	hexadecimal	2	” 01, ..., FF	Default Personalisation Content Dedicated Personalisation Content

Tab. 1.13: Variable Definitions for Commercial Type Names of NTAG42x DNA Tf

Wafer Type Assignment	Description
UD	sawn wafer on UV foil 120 μm bumped
UF	sawn wafer on UV foil 75 μm bumped

Tab. 1.14: Supported Types in tems of Sawn Wafer

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 above are subject of this evaluation. 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 TOE contains a general-purpose low-power CPU that supports a 32-/16-bit instruction set optimized for smartcard applications. The on-chip hardware components are controlled by the TO FW Software via Special Function Registers. These registers are correlated to the activities of the CPU, the memory management unit, interrupt control, communication, EEPROM, timers, the AES co-processor and other HW blocks. The communication with the TOE is performed through the contactless interface.

The device includes ROM (64 kByte), RAM (1.25 kByte) and EEPROM (2 kByte) memory. The ROM is split in ROM constants, Test code and User code. The AES co-processor supports AES and LRP operations with a key length of 128 bits. The random number generator provides true random numbers, which are used, beside other purposes, to seed pseudo random number generator used for less or non-security critical operations.

1.4.2.2 Software Description

The IC Dedicated Test software in the Test code of the TOE is used by the TOE Manufacturer to test the functionality of the chip and to guarantee high production fault coverage. The test functionality is disabled before the operational use of the TOE. The IC Dedicated Test Software includes test routine for all HW blocks including memories, support of the RAM code execution during the test, test commands and access control to ensure that

security relevant test operations cannot be executed illegally once the TOE is configured in the user operating mode.

The TOE also contains IC Dedicated Support Software. The Boot ROM software is part of the IC Dedicated Support Software. The Boot SW is executed after each reset of the TOE, i.e. every time when the TOE starts. It sets up the TOE and does initial configuration. IC Dedicated Support Software further contains code for anti-tear protection, HAL library, CRC, memory management unit as well as control of crypto co-processor and RNG.

The Operating System (OS) Software is also part of the TOE. It includes a generic application OS and four different applications. Only one of the applications is available during usage. OS Software provides the main functionality of the TOE in the usage phase. The TOE is primarily designed for secure contactless transport applications and related loyalty programs as well as access control systems. It fully complies with the requirements for fast and secure data transmission and interoperability with existing infrastructure. Its functionality consists of:

- Static file system with one active application.
- Support for different file types like value files, data record files and Transaction MAC file (for MIFARE DESFire Light and MIFARE IDentity variants of the TOE).
- Mutual three pass authentication
- Authentication on application level with fine-grained access conditions for files.
- Data encryption on the communication path.
- Message Authentication Codes (MAC) for replay attack protection.
- Transaction system with rollback that ensures consistency for complex transactions.
- Unique serial number for each device (UID) with optional random UID.
- Transaction MAC feature to prevent fraudulent merchant attacks.
- Originality functionality that allows verifying the authenticity of the TOE.
- AES based Leakage Resilient Primitive (LRP) crypto functionality with higher SCA resistance.
- Secure Dynamic Messaging functionality, resulting in a Secure Unique NFC Message (SUN) for NTAG42x(Tf) variants of the TOE, that allows confidential and integrity protected data exchange, without requiring a preceding authentication
- Tag-tamper detection,
- The TOE supports a MIFARE DESFire EV2 backward compatible authentication with 128 bit AES.

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

- Electronic fare collection
- Stored value card systems

- Access control systems
- Loyalty
- Tag-tamper detection

If privacy is an issue, the TOE can be configured not to disclose any information to unauthorized users by randomizing the UID used for communication establishment and protecting the device specific internal UID. However, the privacy protection needs to be supported by proper application settings. In particular, this requires avoiding the exposure of other card specific pieces of information that allows for tracing the card. In case that a specific customer use-case requires the free exposure of such information the TOE still guarantees the protection of the internal UID but the user needs to be aware that the non-traceability objective is then no longer achieved. For further details on this aspect, refer to the guidance documentation.

1.4.2.3 Documentation

Refer to Section 1.4.1 for the documentation, which forms part of the TOE delivery.

1.4.3 Security during Development and Production

During the design, 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 developers of NXP Semiconductors, Business Unit Security & Connectivity provide the verified layout data 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 die into specific modules (as stated in section 1.4.1.1), 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:

- Diced dies on wafers
- 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 standard life-cycle for Security IC products as detailed in the Protection Profile (see section 2.4 for details), 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 6a (Optional): Finalization of the personalization
- Phase 7: Operational Usage

During TOE packaging TOE will be embedded either in a plastic inlay (plastic layer containing printed or wired antenna) for direct antenna connection or in one of the supported package types (MOA4 or MOA8). 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 the Protection Profile, NXP will deliver the TOE at the end of Phase 6 in delivery form listed in Section 1.4.1.1. Therefore, the TOE evaluation perimeter comprising the development and production environment of the TOE, consists of life-cycle phases 1 - 6. The TOE is fully integrated composite product is comprised of the underlying security IC HW combined with the embedded software developed by NXP. Therefore, the Phase 5 is fully under control of NXP and does not involve data exchange with other parties.

The developer also provides a commercial option to configure the TOE on behalf of the customer in order to personalize before the usage. Alternatively, the customer can also finalize the partially personalized TOE after delivery. In case that all required security anchors (key material) are already installed during personalization by NXP, the customer can finalize the personalization of the file system content relying on the operational security features of the TOE.

The TOE Software is embedded in the TOE during the TOE evaluation perimeter (life-cycle phases 1 - 6) and the TOE does not allow the modification of installation of any piece of IC Embedded Software after TOE delivery. Moreover, the TOE is being locked to the user operating mode before TOE delivery at the end of Phase 6.

The TOE is able to control different logical phases. After production of the chip every start-up will lead to the initial operating mode. In the initial operating mode the production test shall be performed and the TOE is trimmed and initialized. The selection of the required variant is part of the initialization. At the end of the production test, the access to the test and initialization software is disabled. Subsequent start-ups of the chip will always enter the user operating mode with the CPU executing the TOE operating system software. The TOE will stay in the user operating mode until the end of its life-time. In exceptional cases, which impact the integrity of the TOE in a non-recoverable way (typically if the TOE configuration is corrupted or TOE faces physical damage) the TOE switches into the mute or freeze operating mode. In those modes the TOE is effectively unusable.

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. The only exception is that customer specific keys can be installed using trust provisioning services in Phase 6. In this case the customer can finalize the personalization in the subsequent personalization finalization Phase 6a already relying on the TOE provided operational security services. 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 security relevant applications that require protection against enhanced-basic attack potential. In case that additional resistance against a high-attack potential is required, the MIFARE product portfolio also offers stronger alternatives (like MIFARE DESFire EV2). The product is designed for embedding into contactless integrated circuit cards according to ISO 14443 [10][12][13][11]. Usually the TOE is assigned to a single individual only and can be used for a single application only. The secret data shall be used as input for the calculation of authentication data, encryption and integrity protection of data for communication.

In the end-user environment (Phase 7) Security ICs are used in a wide range of applications to assure authorized conditional access. Examples of such are 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 attempts 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 2. The phases from TOE Delivery to Phase 7 of the Security IC 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. The security features of the TOE cannot be disabled in these

phases.

1.4.6 Interface of the TOE

The pads to connect the RF antenna form the electrical interface of the TOE.

The functional interface is defined by the commands implemented by the TOE and described in datasheets listed in Table 1 within Section 1.4.1.

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.

2 Conformance Claims

2.1 CC Conformance Claim

This Security Target claims to be conformant to the Common Criteria version 3.1, Revision 5:

- Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model - Version 3.1 CCMB-2017-04-001, Revision 5, April 2017, [2]
- Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components, Version 3.1 CCMB-2017-04-002, Revision 5, April 2017, [3]
- Common Criteria for Information Technology Security Evaluation, Part 3 – Security Assurance Components, Version 3.1 CCMB-2017-04-003, Revision 5, April 2017, [4]

For the evaluation the following methodology will be used:

- Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, Version 3.1 CCMB-2017-04-004, Revision 5, April 2017, [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 level **EAL4**, which in particular includes the resistance against an **enhanced-basic attack potential** (as implied by the inclusion of AVA_VAN.3).

2.3 PP Claim

This Security Target does not claim conformance to any Protection Profile.

2.4 Conformance Claim Rationale

Even though this Security Target does not claim conformance to any Protection Profile, the general modelling approach of the security problem definition and the structure of the security functional requirements have been taken from the Security IC Platform Protection Profile with Augmentation Packages [9]. Whenever referring to 'Protection Profile', the reader of this Security Target must be aware about section 2.3 and the current section.

The TOE is a similar product-type (embedded software running on a security IC intended to be embedded in one of the different package types stated in section 1.4.1.1). The primary difference is in the claimed attack resistance level, which is justified by the value of the assets protected by the TOE. A second difference is that the Protection Profile formulates the security objectives for the security IC form the perspective of a generic platform protecting

arbitrary kinds of embedded software implementations. In contrast, the TOE is evaluated as a combination of a hardware platform together with the an Operating System (OS) functionality.

Therefore, the following modifications and precisions for the TOE use-case have been made: The assumption A.Resp-Appl and the related objective for the TOE environment OE.Resp-Appl have not been taken from the Protection Profile because they formulate assumptions on the behaviour of the embedded-software, which is for the platform part of the TOE and not of the environment of the TOE.

3 Security Problem Definition

Although this Security Target does not claim conformance to any Protection Profile, the general modelling approach of the security problem definition and the structure of the security functional requirements have been taken over from the Protection Profile. The only deviation is explained in section 2.4. In the following paragraphs 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 only.

3.1 Description of Assets

The 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 in the following:

- Integrity and confidentiality of User Data stored and in operation. More concretely, the user-data comprises the data and key material contained in files in the file system, customer configurable configuration options, as well as NXP configuration data and other administrative information that ensures proper operation of the operating system.
- Integrity and confidentiality of UID depending on configuration
- Integrity 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 these 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.

Observe that the protection requirements for the assets are defined by the assumed enhanced-basic attack potential and as such can be often lower than for products aiming at resisting against an attacker with a high attack potential. Also note that all assets valid for this TOE are considered when specifying the threats defined in the subsequent section.

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 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 Security Target

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

T.Impersonate **Impersonating authorised users during authentication**
An unauthorised subject may try to impersonate an authorised subject during the authentication sequence, e.g. by a man-in-the middle or replay attack in order to affect user data stored by the TOE.

T.Cloning **Cloning**
User and TSF data stored on the TOE (including keys) may be read out by an unauthorised subject in order to create a duplicate.

3.3 Organizational Security Policies

All security policies defined in Section 3.3 of the Protection Profile are taken over to 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 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 hardware and underlying firmware supplies security functionality which is further used by the operating system 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 specific application, against which threats the TOE Software will use the specific security functionality.

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

Name	Title
P.Encryption	Confidentiality during communication
P.MAC	Integrity during communication
P.Transaction	Transaction mechanism
P.No-Trace	Un-traceability of end-users
P.Tag-Tamper	Tag tamper detection

Tab. 3.4: Additional Policies defined in this Security Target

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

P.MAC **Integrity during communication**
The TOE shall provide the possibility to protect the contactless communication from modification or injections. This includes especially the possibility to detect replay or man-in-the-middle attacks within a session.

P.Transaction **Transaction mechanism**

The TOE shall provide the possibility to combine a number of data modification operations in one transaction, so that either all operations or no operation at all is performed.

Remark 3. This policy is only relevant for MIFARE DESFire Light and MIFARE IDentity variants of the TOE.

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 contactless 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.

Remark 4. This policy is only relevant for MIFARE DESFire Light and MIFARE IDentity variants of the TOE.

P.Tag-Tamper **Tag tamper detection**
The TOE shall provide the possibility to detect and permanently record tampering status on the tag tamper wire.

Remark 5. This policy is only relevant for the NTAG42xTf variant of the TOE.

3.4 Assumptions

One of the assumptions defined in Section 3.4 of the Protection Profile is taken over to this Security Target. These assumptions are listed in Table 3.5. Section 2.2 clarifies the omitted assumptions with their reasoning.

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

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 secure 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 [14]) or AIS31 (see [15]) 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 Security Target

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 taken from the Protection Profile

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.Encryption	Confidential Communication
O.MAC	Integrity-protected Communication
O.Type_Consistency	Data type consistency
O.Transaction	Transaction mechanism
O.No-Trace	Preventing Traceability
O.Tag-Tamper	Tag tamper detection

Tab. 4.2: Security Objectives of the TOE defined in this Security Target

These additional security objectives are specified as follows.

O.Access-Control **Access Control**

The TOE must provide an access control mechanism for data stored by it. The access control mechanism shall apply to read, modify, create and delete operations for data elements and to reading and modifying security attributes as well as authentication data. It shall be possible to

limit the right to perform a specific operation to a specific user. The security attributes (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 implemented by security attributes that enforce integrity protected communication for the respective data elements. 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, for data file sizes and record handling.

O.Transaction **Transaction mechanism**
The TOE must be able to provide a transaction mechanism that allows to update multiple data elements either all in common or none of them.

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 any information that is suitable for tracing an end-user by an unauthorised subject.

O.Tag-Tamper **Tag tamper detection**
The TOE must be able to detect and permanently record tampering status on the tag tamper wire.

4.2 Security Objectives for the 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 4.3.

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

Tab. 4.3: Security Objectives of the Operational Environment taken from the Protection Profile

In addition, the following additional security objectives for the operational environment are defined in this Security Target and listed in table 4.4.

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

Tab. 4.4: Security Objectives of the Operational Environment defined in this Security Target

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 to 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, confidentiality and use of random numbers**
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 [14]) or AIS31 (see [15]) for the authentication.

4.3 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 4.5 summarizes this.

Security Problem Definition	Security Objective	Notes
T.Leak-Inherent	O.Leak-Inherent	

Security Problem Definition	Security Objective	Notes
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
T.Masquerade_TOE	OE.Process-Sec-IC	

Tab. 4.5: Security Objectives vs. Security Problem Definition (Protection Profile)

Table 4.6 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.Transaction	O.Transaction	
P.No-Trace	O.Access-Control O.Authentication O.No-Trace	
P.Tag-Tamper	O.Tag-Tamper	
A.Secure_Values	OE.Secure_Values	
A.Terminal_Support	OE.Terminal_Support	

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

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
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.Transaction:

Objective	Rationale
O.Transaction	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.

Objective	Rationale
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.

Justification related to P.Tag-Tamper:

Objective	Rationale
O.Tag-Tamper	This objective is an immediate transformation of the security policy, therefore it covers the Security policy.

5 Extended Components Definitions

To define the Secure Dynamic Messaging property of the TOE, which is available in some configurations, an additional component FDP_ETC.3 of the family FDP_ETC (export from the TOE) of the class FDP (user data protection) is defined. This component describes the functional requirements for Secure Dynamic Messaging capability of the TOE.

As defined in CC Part 2 [3], FDP class addresses user data protection. FDP_ETC family defines functions for TSF-mediated exporting of user data from the TOE such that its security attributes and protection either can be explicitly preserved or can be ignored once it has been exported. Export of user data in unauthenticated state (FDP_ETC.3) addresses a similar concern but does not require a TOE enforcement of an access control SFP(s) and/or information flow control SFP(s) as already defined components of the FDP_ETC family. Therefore the extended component FDP_ETC.3 is defined.

This Security Target also re-uses the extended security functional requirements

- FCS_RNG.1,
- FMT_LIM.1,
- FMT_LIM.2,
- FAU_SAS.1,
- and FDP_SDC.1

from Chapter 5 of the Protection Profile.

5.1 Export of user data in unauthenticated state (FDP_ETC.3)

Class and family behaviour are already defined in CC Part 2 [3].

Component leveling:

Fig. 5.1: Component Levelling of Extended Component FDP_ETC

FDP_ETC	Export from the TOE
Management:	FDP_ETC.3 There are no management activities foreseen.
Audit:	FDP_ETC.3 There are no actions defined to be auditable.
FDP_ETC.3	**Export of user data in unauthenticated state**
Hierarchical to:	No other components.
Dependencies	No dependencies.
FDP_ETC.3.1	**The TSF shall export the following pieces of user data [assignment: pieces of user data] with the following user data's associated security attributes [assignment: list of security attributes].**
FDP_ETC.3.2	**The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.**
FDP_ETC.3.3	**The TSF shall enforce the following rules when user data is exported from the TOE: [assignment: additional exportation control rules].**

The extended component is defined to capture the SDM feature provided by the TOE, which allows for the encrypted and authenticated extraction of user data without the need of establishing a trusted channel beforehand. Due to this specific property, the existing data export SFRs FDP_ETC.1 and FDP_ETC.2 did not apply well.

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

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)
FDP_ITT.1[HW]	Basic Internal Transfer Protection
FDP_IFC.1	Subset Information Flow Control

Name	Title
FDP_SDC.1[HW]	Stored data confidentiality
FDP_SDI.2[HW]	Stored data integrity monitoring and action
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 FAU_SAS.1[HW] the Protection Profile leaves the assignment operation open for the persistent memory type in which initialization data, pre-personalization data and/or other supplements for the Security IC Embedded Software are stored. This assignment operation is filled in by the following statement. Note that the assignment operations for the list of subjects and the list of audit information have already been filled in by the 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* in the *EEPROM*.

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, generates the internal random numbers with a post-processing algorithm of class DRG.2 as long as its internal state entropy guarantees the claimed output entropy*.

(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 *applied on the following internal event: each time random numbers are drawn from the RNG*. 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 the Protection Profile according to [1].

Note: Application Note 20 in the Protection Profile 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 TOE Software. The results of the internal test sequence are provided to the TOE 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”, [15].

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 EEPROM*.

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 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*.

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 following definitions:
The subjects are

Subject	**AppMgr**	**Application Manager**
Info	The AppMgr is the subject that owns or has access to the AppMasterKey. Note that the TOE supports only a single Application.	

Subject	**AppUser**	**Application User**
Info	The AppUser is the subject that owns or has access to an AppKey. Note that the TOE supports multiple AppUser within the Application and the assigned rights to the AppUser can be different, which allows to have more or less powerful AppUser. There are 5 different AppKeys.	

Subject	**OrigKeyUser**	**Originality Key User**
Info	The OrigKeyUser is the subject that owns or has acces to an PICCOriginalityKeys. The OrigKeyUser can authenticate with the TOE to prove the authenticity of the Security IC.	

Subject	Anybody	Anybody
Info	Any subject that does not belong to one of the roles AppMgr, AppUser or OrigKeyUser, 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 AppMgr, AppUser, OrigKeyUser 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.	

The objects are

Object	Application	Application
Info	The card can store one Application at a time. An Application can store a number of Files.	
Operation	Select	Select an Application.

Object	File	File
Info	An Application can store a number of File of different types.	
Info	Note that the TOE has a static file system. File.Create and File.Delete is only supported for TransactionMAC files and relevant for the variants MIFARE DESFire Light and MIFARE IDentity. File.Rename is only relevant for the variant MIFARE DESFire Light.	
Operation	Create	Create a TransactionMAC File.
Operation	Delete	Delete a TransactionMAC File.
Operation	Freeze	Freeze attributes of File.
Operation	Read	Read operations accessing the content of a File.
Operation	Write	Write operations accessing the content of a File
Operation	ReadWrite	ReadWrite operations accessing the content of a File
Operation	Change	Change operation to change the attribute File.AccessRights
Operation	Rename	Rename operation to change the name of a File.
Attribute	AccessRights	Generic access rights for File.

Object	PICCOriginalityKeys	PICC Originality Keys
Info	Keys to check the originality of the card. They are not changeable.	

Object	AppMasterKey	Application Master Key
Info	Application Master Key	
Operation	Change	Change the AppMasterKey

Object	AppKey	Application Key
Info	Application Key. Note that there are five Application Keys.	
Operation	Change	Change the AppKey.

Object	AppTransactionMACKey	Application Transaction MAC Key
Info	Application Transaction MAC Key	
Info	Application Transaction MAC Key. Note that to change the Transaction MAC key, AppTransactionMACKey.Delete and AppTransactionMACKey.Create have to be applied. Note that this is only relevant for the variants MIFARE DESFire Light and MIFARE IDentity.	
Operation	Create	Create the AppTransactionMACKey.
Operation	Delete	Delete the AppTransactionMACKey.

Note that subjects are authorized by cryptographic keys. These keys are considered as authentication data and not as security attributes of the subjects. There is one Application available at a time. The Application has an AppMasterKey and 5 AppKeys used for operations on Files. Keys are persistent and stored in EEPROM.

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

FMT_SMR.1[DF]	**Security Roles**
Hierarchical-To	No other components.
Dependencies	FIA_UID.1 Timing of identification
FMT_SMR.1.1[DF]	The TSF shall maintain the roles *AppMgr, AppUser, OrigKeyUser and Anybody*.
FMT_SMR.1.2[DF]	The TSF shall be able to associate users with roles.

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

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

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

FDP_ACF.1[DF]	**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[DF]	The TSF shall enforce the *TOE Access Control Policy* to objects based on the following: *all subjects, objects and attributes*.
FDP_ACF.1.2[DF]	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
MFP_ACP_ACF1_21	*The AppMgr is allowed to perform File.Create and File.Delete.*
MFP_ACP_ACF1_22	*The AppMgr is allowed to perform File.Rename.*
FDP_ACF.1.3[DF]	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules:
MFP_ACP_ACF1_31	*The AppUser is allowed to perform File.Read or File.Write or File.ReadWrite or File.Change on File if the File.AccessRights grant these rights.*
MFP_ACP_ACF1_32	*Anybody is allowed to perform File.Read or File.Write or File.ReadWrite or File.Change if the File.AccessRights grant these rights.*
FDP_ACF.1.4[DF]	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 File.Read or File.Write or File.ReadWrite or File.Change if theFile.AccessRights do not grant this right.*
MFP_ACP_ACF1_42	*OrigKeyUser is not allowed to perform any operation on objects.*
MFP_ACP_ACF1_43	*No one but Nobody is allowed to perform any operation on PICCOriginalityKeys.*

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

FMT_MSA.3[DF]	**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[DF]	The TSF shall enforce the *TOE Access Control Policy* to provide *permissive* default values for security attributes that are used to enforce the Security Function Policy (SFP).
FMT_MSA.3.2[DF]	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.
Application Note:	The file system is fully instantiated (partially upon customer requests) during the initialization of the product. Therefore, the TOE Access Control Policy does not allow the creation and consequently the manipulation of the default values in operational mode.

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

FMT_MSA.1[DF]	**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[DF]	The TSF shall enforce the *TOE Access Control Policy* to restrict the ability to *modify and change* the security attributes *File.AccessRights* to *the AppUser*.

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

FMT_MTD.1[DF]	**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[DF]	The TSF shall restrict the ability to *perform AppMasterKey.Change* to *AppUser*.
Refinement:	The detailed management abilities are:

MFP_ACP_MTD1_11 *The AppMgr is allowed to perform AppMasterKey.Change.*

MFP_ACP_MTD1_12 *The AppMgr is allowed to perform AppKey.Change.*

MFP_ACP_MTD1_13 *The AppMgr is allowed to perform AppTransactionMACKey.Create and AppTransactionMACKey.Delete.*

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

FMT_SMF.1[DF]	**Specification of Management Functions**
Hierarchical-To	No other components.
Dependencies	No dependencies.
FMT_SMF.1.1[DF]	The TSF shall be capable of performing the following security management functions: • *Authenticate a user,* • *Invalidating the current authentication state based on the functions: Selecting and reselecting an application or the card, Changing the key corresponding to the current authentication, Occurence of any error during the execution of a command, Starting a new authentication and Reset,* • *Changing a security attribute,* • *Performing File.Create or File.Delete*

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

FDP_ITC.2[DF]	**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[DF]	The TSF shall enforce the *TOE Access Control Policy* when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.2.2[DF]	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3[DF]	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[DF]	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[DF]	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 TOE Access Control Policy

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

- The TOE end-user does normally not belong to the group of authorised users (AppMgr and AppUser), but 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).
- AppMgr has to authenticate with the AppMasterKey to change the AppMasterKey and AppKeys.
- Furthermore, the AppMgr has the right to perform File.Create and File.Delete within his Application scope

6.1.3 Additional SFRs regrading confidentiality, authentication and integrity

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

FCS_COP.1[DF-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[DF-AES]	The TSF shall perform *encryption and decryption and cipher based MAC 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) [7] and*
- *NIST Special Publication 800-38B (CMAC mode) [8]*

Application Note: The standard AES implementation is provided primarily for backward compatibility purposes. For ensuring the required resistance level the guidance requirements need to be strictly followed when using the standard AES. The product also provides a security enhanced AES variant (c.f. FCS_COP.1[DF-AESLRP]. It is possible to configure the product in a way that the use of the enhanced primitive is always enforced.

The TOE shall meet the requirements "Cryptographic Operation (AESLRP) (FCS_COP.1[DF-AESLRP])" as specified below.

FCS_COP.1[DF-AESLRP]	**Cryptographic Operation (AESLRP)**
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[DF-AESLRP]	The TSF shall perform *encryption and decryption and cipher based MAC for authentication and communication* in accordance with the specified cryptographic algorithm *Leakage Resilient Primitive LRP in one of the following modes of operation: Leakage Resilient Indexed Codebook (LRICB), CMAC* and a cryptographic key size *of 128 bits* that meet the following *standards*: • *Leakage Resilient Primitive, [16]*

Application Note: Leakage Resilient Primitive is a proprietary cryptographic algorithm, which based on the standard block cipher AES128. It is implemented as software on top of the AES co-processor with substantially reduced side channel resistance requirements.

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

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

Application Note: Identification of a user is performed upon an authentication request based on the currently selected context and the key number. For example, if an authentication request for key number 0 is issued after selecting a specific Application, the user is identified as the AppMgr of the respective Application. Before any authentication request is issued the user is identified as Anybody.

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

FIA_UAU.2[DF]	**User Authentication before any Action**
Hierarchical-To	FIA_UAU.1 Timing of authentication
Dependencies	FIA_UID.1 Timing of identification
FIA_UAU.2.1[DF]	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[DF])" as specified below.

FIA_UAU.5[DF]	**Multiple Authentication Mechanisms**
Hierarchical-To	No other components.
Dependencies	No dependencies.
FIA_UAU.5.1[DF]	The TSF shall provide *'none' and cryptographic authentication* to support user authentication.
FIA_UAU.5.2[DF]	The TSF shall authenticate any user's claimed identity according to the *following rules*: • *The 'none' authentication is performed with anyone who communicates with the TOE without issuing an explicit authentication request. The 'none' authentication implicitly and solely authorizes the subject Anybody.* • *The cryptographic authentication is used to authorise the AppMgr and AppUser.*
Refinement:	For the applied cryptographic operation please refer to FCS_COP.1[DF-AES] and FCS_COP.1[DF-AESLRP]

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

FTP_TRP.1[DF]	**Trusted Path**
Hierarchical-To	No other components.
Dependencies	No dependencies.
FTP_TRP.1.1[DF]	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[DF]	The TSF shall permit *remote users* to initiate communication via the trusted path.
FTP_TRP.1.3[DF]	The TSF shall require the use of the trusted path for *authentication requests with AES or AESLRP, confidentiality and/or integrity verification for data transfers protected with AES or AESLRP based on a setting in the file attributes*.

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

FCS_CKM.4[DF]	**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[DF]	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[DF])” as specified below.

FPT_TDC.1[DF]	**Inter-TSF Basic TSF Data Consistency**
Hierarchical-To	No other components.
Dependencies	No dependencies.
FPT_TDC.1.1[DF]	The TSF shall provide the capability to consistently interpret *data files and values* when shared between the TSF and another trusted IT product.
FPT_TDC.1.2[DF]	The TSF shall use *the rules: data files or values can only be modified by their dedicated type-specific operations honouring the type-specific boundaries* when interpreting the TSF data from another trusted IT product.

6.1.4 Additional SFRs regrading the robustness

The TOE shall meet the requirements ”Basic rollback (FDP_ROL.1[DF])” as specified below.

FDP_ROL.1[DF]	**Basic rollback**
Hierarchical-To	No other components.
Dependencies	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_ROL.1.1[DF]	The TSF shall enforce Access Control Policy to permit the rollback of *the operations that modify the value or data file objects* on *the backup files*.
FDP_ROL.1.2[DF]	The TSF shall permit operations to be rolled back within *the scope of the current transaction, which is defined by the following limitative events: chip reset, select command, deselect command, explicit commit, explicit abort, command failure*.
Application Note:	Only relevant for the variants MIFARE DESFire Light and MIFARE IDentity.

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

FPT_RPL.1[DF]	**Replay detection**
Hierarchical-To	No other components.
Dependencies	No dependencies.
FPT_RPL.1.1[DF]	The TSF shall detect replay for the following entities: *authentication requests with AES or AESLRP, confidentiality and/or data integrity verification for data transfers protected with AES or AESLRP and based on a setting in the file attributes*.
FPT_RPL.1.2[DF]	The TSF shall perform *rejection of the request* when replay is detected.

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

FPR_UNL.1[DF]	**Unlinkability**
Hierarchical-To	No other components.
Dependencies	No dependencies.
FPR_UNL.1.1[DF]	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*.

6.1.5 Additional SFRs regarding Secure Dynamic Messaging Feature

The TOE shall meet the requirements ”Export of user data in unauthenticated state (FDP_ETC.3[DF])” as specified below.

FDP_ETC.3[DF]	**Export of user data in unauthenticated state**
Hierarchical-To	No other components.
Dependencies	No dependencies.
FDP_ETC.3.1[DF]	The TSF shall export the following pieces of user data *a configurable subset of file data* with the following user data’s associated security attributes: *confidentiality, authenticity and replay protection for the configurable subset of the file data*.
FDP_ETC.3.2[DF]	The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.
FDP_ETC.3.3[DF]	The TSF shall enforce the following rules when user data is exported from the TOE: *Plain export of file data in case that SDM is not activated for the file*.

6.1.6 Additional SFRs regarding Tag Tampering Feature

The TOE shall meet the requirements ”Protected audit trail storage (FAU_STG.1[DF])” as specified below.

FAU_STG.1[DF]	**Protected audit trail storage**
Hierarchical-To	No other components.
Dependencies	FAU_GEN.1 Audit data generation
FAU_STG.1.1[DF]	The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG.1.2[DF]	The TSF shall be able to *prevent* unauthorised modifications to the stored audit records in the audit trail.

The TOE shall meet the requirements ”Guarantees of audit data availability (FAU_STG.2[DF])” as specified below.

FAU_STG.2[DF]	**Guarantees of audit data availability**
Hierarchical-To	FAU_STG.1 Protected audit trail storage
Dependencies	FAU_GEN.1 Audit data generation
FAU_STG.2.1[DF]	The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG.2.2[DF]	The TSF shall be able to *prevent* unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.2.3[DF] The TSF shall ensure that *permanent 1-byte status TTPermStatus* will be maintained when the following conditions occur: \emphg{failure and attack}.

6.2 Security Assurance Requirements

Table 6.13 below lists all security assurance components that are valid for this Security Target. These security assurance components are required by EAL4 (according to section 2.2)

Name	Title
ADV_ARC.1	Security architecture description
ADV_FSP.4	Complete functional specification
ADV_IMP.1	Implementation representation of the TSF
ADV_TDS.3	Basic modular design
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.4	Production support, acceptance procedures and automation
ALC_CMS.4	Problem tracking CM coverage
ALC_DEL.1	Delivery procedures
ALC_DVS.1	Identification of security measures
ALC_LCD.1	Developer defined life-cycle model
ALC_TAT.1	Well-defined development tools
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.1	TOE summary specification
ATE_COV.2	Analysis of coverage
ATE_DPT.1	Testing: basic design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing - sample
AVA_VAN.3	Focused vulnerability analysis

Tab. 6.13: Security Assurance Requirements of the TOE

6.3 Security Requirements Rationale

6.3.1 Rationale for the Security Functional Requirements

The following tables show the mappings from security functional requirements to the security objectives of the TOE, coming from the Protection Profile (table 6.14) and the Security Target (table 6.15) respectively. Detailed mapping justifications are given in the following text.

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

Tab. 6.14: Security Functional Requirements vs. Security Objectives (Protection Profile)

SO	SFR
O.Access-Control	FCS_CKM.4[DF] FDP_ACC.1[DF] FDP_ACF.1[DF] FDP_ITC.2[DF] FMT_MSA.1[DF] FMT_MSA.3[DF] FMT_MTD.1[DF] FMT_SMF.1[DF] FMT_SMR.1[DF]
O.Authentication	FCS_COP.1[DF-AES] FIA_UID.2[DF] FIA_UAU.2[DF] FIA_UAU.5[DF] FMT_SMF.1[DF] FPT_RPL.1[DF] FTP_TRP.1[DF] FCS_COP.1[DF-AESLRP]
O.Encryption	FCS_CKM.4[DF] FCS_COP.1[DF-AES] FTP_TRP.1[DF] FDP_ETC.3[DF] FCS_COP.1[DF-AESLRP]
O.MAC	FCS_CKM.4[DF] FCS_COP.1[DF-AES] FPT_RPL.1[DF] FTP_TRP.1[DF] FDP_ETC.3[DF] FCS_COP.1[DF-AESLRP]
O.Type_Consistency	FPT_TDC.1[DF]
O.Transaction	FDP_ROL.1[DF]
O.No-Trace	FPR_UNL.1[DF]
O.Tag-Tamper	FAU_STG.1[DF] FAU_STG.2[DF]

Tab. 6.15: Security Functional Requirements vs. Security Objectives (Security Target)

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

The SFR FMT_SMR.1[DF] defines the roles of the Access Control Policy. The SFRs FDP_ACC.1[DF] and FDP_ACF.1[DF] define the rules and FMT_MSA.3[DF] and FMT_MSA.1[DF] the attributes that the access control is based on. FMT_MTD.1[DF] provides the rules for the management of the authentication data. The manage-

ment functions are defined by FMT_SMF.1[DF]. Since the TOE stores data on behalf of the authorised subjects import of user data with security attributes is defined by FDP_ITC.2[DF]. 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 (i.e. deletion of the TransactionMAC files, invalidation of the old keys in case of a key change, invalidation of session keys). This is required by FCS_CKM.4[DF]. These nine SFR together provide an access control mechanism as required by the objective O.Access-Control.

Justification related to "Authentication (O.Authentication)"

The two SFRs FCS_COP.1[DF-AES] and FCS_COP.1[DF-AESLRP] require that the TOE provides the basic cryptographic algorithms that can be used to perform the authentication. The SFRs FIA_UID.2[DF], FIA_UAU.2[DF] and FIA_UAU.5[DF] together define that users must be identified and authenticated before any action. The "none" authentication of FIA_UAU.5[DF] also ensures that a specific subject is identified and authenticated before an explicit authentication request is sent to the TOE. FMT_SMF.1[DF] defines security management functions the TSF shall be capable to perform. FTP_TRP.1[DF] requires a trusted communication path between the TOE and remote users, FTP_TRP.1.3[DF] especially requires "authentication requests". Together with FPT_RPL.1[DF] which requires a replay detection for these authentication requests the eight SFR fulfil the objective O.Authentication.

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

The two SFRs FCS_COP.1[DF-AES] and FCS_COP.1[DF-AESLRP] require that the TOE provides the basic cryptographic algorithms that can be used to protect the communication by encryption. FTP_TRP.1[DF] requires a trusted communication path between the TOE and remote users, FTP_TRP.1.3[DF] especially requires "confidentiality and/or data integrity verification for data transfers protected with AES and based on a setting in the file attributes". FCS_CKM.4[DF] requires that cryptographic keys used for encryption have to be removed after usage.

The MIFARE IDentity and NTAG42x DNA (Tf) variants of the TOE also provides Secure Dynamic Messaging service which allows encrypted and MACed data read without being in the authenticated state. FDP_ETC.3[DF] requires user data export in unauthenticated state hence models the requirements to reach O.Encryption. These five SFR fulfil the objective O.Encryption.

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

The two SFRs FCS_COP.1[DF-AES] and FCS_COP.1[DF-AESLRP] require 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[DF] requires a trusted communication path between the TOE and remote users, FTP_TRP.1.3[DF] especially requires "confidentiality and/or data integrity verification for data transfers on request of the file owner". FCS_CKM.4[DF] requires that cryptographic keys used for MAC operations have to be removed after usage. Also FPT_RPL.1[DF] requires a replay detection for these data transfers. MIFARE IDentity and NTAG42x DNA (Tf) variants of the TOE also provides Secure Dynamic Messaging service which allows encrypted and MACed data read without being in the authenticated state. FDP_ETC.3[DF] requires user data export in unauthenticated state hence models the requirements to reach O.MAC.

Justification related to "Data type consistency (O.Type_Consistency)"

The SFR FPT_TDC.1[DF] requires the TOE to consistently interpret data files and values. 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 "Transaction mechanism (O.Transaction)"

The SFR FDP_ROL.1[DF] requires the possibility to rollback a set of modifying operations on backup files in total. The set of operations is defined by the scope of the transaction, which is itself limited by some boundary events. This fulfils the objective O.Transaction.

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

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

Justification related to "Tag tamper detection (O.Tag-Tamper)"

The two SFRs FAU_STG.1[DF] and FAU_STG.2[DF] require the TOE to prevent unauthorised deletion and modifications to the stored tag tamper status. They also require the TOE to maintain the permanent 1-byte status TTPermStatus in case of failure or attack. This meets the objective O.Tag-Tamper.

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
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 below
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

SFR	Dependencies	Fulfilled by Security Requirements in the ST
FRU_FLT.2	FPT_FLS.1 Failure with preservation of secure state.	Yes

Tab. 6.16: Dependencies of Security Functional Requirements (PP)

SFR	Dependencies	Fulfilled by Security Requirements in the ST
FCS_CKM.4[DF]	[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[DF].
FCS_COP.1[DF-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[DF]. Yes, by FCS_CKM.4[DF].
FCS_COP.1[DF-AESLRP]	[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[DF]. Yes, by FCS_CKM.4[DF].
FAU_STG.1[DF]	FAU_GEN.1 Audit data generation	See discussion below
FAU_STG.2[DF]	FAU_GEN.1 Audit data generation	See discussion below
FDP_ACC.1[DF]	FDP_ACF.1 Security attribute based access control.	Yes, by FDP_ACF.1[DF].
FDP_ACF.1[DF]	FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization	Yes, by FDP_ACC.1[DF]. Yes, by FMT_MSA.3[DF].
FDP_ETC.3[DF]	No dependencies.	No dependency

SFR	Dependencies	Fulfilled by Security Requirements in the ST
FDP_ITC.2[DF]	[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[DF]. Yes, by FTP_TRP.1[DF]. Yes, by FPT_TDC.1[DF].
FDP_ROL.1[DF]	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	Yes, by FDP_ACC.1[DF].
FIA_UID.2[DF]	No dependencies.	No dependency
FIA_UAU.2[DF]	FIA_UID.1 Timing of identification	Yes, by FIA_UID.2[DF].
FIA_UAU.5[DF]	No dependencies.	No dependency
FMT_MSA.1[DF]	[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[DF]. Yes, by FMT_SMR.1[DF]. Yes, by FMT_SMF.1[DF].
FMT_MSA.3[DF]	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	Yes, by FMT_MSA.1[DF]. Yes, by FMT_SMR.1[DF].
FMT_MTD.1[DF]	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	Yes, by FMT_SMR.1[DF]. Yes, by FMT_SMF.1[DF].
FMT_SMF.1[DF]	No dependencies.	No dependency
FMT_SMR.1[DF]	FIA_UID.1 Timing of identification	Yes, by FIA_UID.2[DF].
FPR_UNL.1[DF]	No dependencies.	No dependency
FPT_RPL.1[DF]	No dependencies.	No dependency
FPT_TDC.1[DF]	No dependencies.	No dependency
FTP_TRP.1[DF]	No dependencies.	No dependency

Tab. 6.17: Dependencies of Security Functional Requirements (Security Target)

Part 2 of the Common Criteria defines the dependency of FDP_IFC.1 (information flow control policy statement) on FDP_IFF.1 (Simple security attributes). The specification of FDP_IFF.1 would not capture the nature of the security functional requirement nor add any detail. As stated in the Data Processing Policy referred to in FDP_IFC.1 there are no attributes necessary. The security functional requirement for the TOE is sufficiently described using FDP_ITT.1 and its Data Processing Policy (FDP_IFC.1).

Part 2 of the Common Criteria defines the dependency of FAU_STG.1 (Protected audit trail storage) and FAU_STG.2 (Guarantees of audit data availability) on FAU_GEN.1 (Audit data generation). The specification of FAU_GEN.1 focusses on the list of data that shall be recorded in each audit record together with its time stamp. However, in the perspective of the TOE, FAU_STG.1 and FAU_STG.2 aim at just storing the status of the tag tamper wire in the binary format. In contrast, FAU_GEN.1, specified way more detailed logging information like time stamps than required for the target use-case. Therefore, FAU_GEN.1 is not added.

6.3.3 Rationale for the Assurance Requirements

The selection of assurance components is based on the chosen evaluation assurance level. The level EAL4 is chosen in order to meet assurance expectations of access control applications and automatic fare collection systems. The assurance level EAL4 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. There is not any augmentation to the chosen assurance level.

6.3.4 Security Requirements are Internally Consistent

The discussion of security functional requirements and assurance components in the preceding sections has shown that mutual support and consistency are given for both groups of requirements. The arguments given for the fact that the assurance components are adequate for the functionality of the TOE also show that the security functional and assurance requirements support each other and that there are no inconsistencies between these groups.

The security functional requirements required to meet the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced also protect the cryptographic algorithms and the access control function used to implement the Access Control Policy. The security objectives defined in the PP0084 can be seen as "low-level protection" objectives, while the additional security objectives defined in this Security Target are "high-level protection" objectives. For example O.Encryption states that the communication can be protected by encryption. While this ensures the rather high-level goal that the communication cannot be eavesdropped, the overall goal that the communication is confidential is ensured with the help of the Protection Profile objective that prevent attacks on the key and the cryptographic implementation like side channel or fault injection attacks.

7 TOE Summary Specification

7.1 TOE Security Functionality

7.1.1 Security Services

SS.AUTH **Authentication**

The TOE provides an authentication mechanism to separate authorized subjects from unauthorized subjects. The authentication of subjects is performed by a cryptographic challenge response. The TOE supports the cryptographic algorithms 128-bit AES and 128-bit AESLRP; for AES according to FIPS PUB 197 [6] and for AESLRP according to AESLRP Whitepaper [16]. The authentication mechanisms are implemented using the cryptographic coprocessors and the hardware random number generator provided by the hardware platform. The authentication mechanisms are protected against attacks like e.g. replay.

The TOE enforces the use of the enhanced AESLRP authentication always for authentications with the PICCOriginalityKeys. For other keys, it depends on the TOE configuration: after AESLRP is activated the AES algorithm cannot be used anymore, therefore the TOE is bound to authentications and secure messaging (i.e. the configuration also applies for subsequent SS.ENCRYPTION and SS.MAC) with AESLRP algorithm.

SS.AUTH identifies the user to be authenticated by the currently selected context (card or specific application, chosen by a "select" command) and the key number indicated in the authentication request. By default and before any authentication request SS.AUTH identifies and authenticates the role Anybody. The roles AppMgr, AppUser, and OrigKeyUser 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: issue of a "select" command, occurrence of any error during the processing of a command, change of the key that was used for authentication and reset (any cause, either internal or external reset). These events will reset the authentication state to the default (Anybody)

SS.ACC_CTRL **Access Control**

SS.ACC_CTRL provides an access control mechanism to the Objects and Security Attributes that are part of the TOE Access Control Policy. The access control mechanism assigns subjects - AppUser- to different groups of operations on Files. The operations are File.Read, File.Write, File.ReadWrite, File.Change and File.Rename. One subject can be assigned to each group of File operations. The special subjects Anybody and Nobody can also be assigned. File.Rename operation can be performed only once on Files in MIFARE DESFire Light variant by AppMgr. For Files, the operations furthermore are File.Create and File.Delete. These operations can be assigned to the AppMgr and only relevant for the Transaction MAC Files. The assignment is

stored in the Application attributes. For the Application there are no operation defined except select, since only one Application is available at the delivery time and another application cannot be created or the current one cannot be deleted.

SS.ACC_CTRL also controls access to the Security Attributes and the authentication data. The Application attributes, AppKeys and AppMasterKeys can be changed by the AppMgr. For Files the attributes can be changed by the subject that has the File.AccessRights to perform the operation File.Change.

The OrigKeyUser is not allowed to perform any operation on objects, but with a successful authentication he can prove the authenticity of the Security IC.

Finally, SS.ACC_CTRL ensures the type consistency of the File types stored by the TOE. It ensures that values cannot over- or underflow. Furthermore, size limitations of Files are obeyed by SS.ACC_CTRL.

SS.ENCRYPTION **Encryption**

The TSF SS.ENCRYPTION provides a mechanism to protect the communication against eavesdropping. In order to do this the communication can be encrypted. The encryption is requested by the file owner (i.e. the subject that has the right to ”change attribute” for a file) by setting an option in the file attributes.

The encryption algorithm is the same as the one used during authentication for the session and supports the AES and AESLRP algorithms.

Note that the TSF SS.ENCRYPTION is active after authentication performed with SS.AUTH. SS.ENCRYPTION also adds data to the communication stream that enables the terminal to detect integrity violations, replay attacks or man-in-the-middle attacks.

If an encrypted communication is requested, SS.ENCRYPTION also verifies the data sent by the terminal and returns an error code if integrity violations, replay attacks or man-in-the-middle attacks is detected. The detection mechanism covers all frames exchanged between the terminal and the card up to the current encrypted frame. Therefore SS.ENCRYPTION can detect any injected/modified frame in the communication before the transfer of the encrypted frame.

SS.MAC **Message Authentication Code**

The TSF SS.MAC provides a mechanism for integrity protection, replay attack protection and protection against man-in-the-middle attacks on the communication path. The integrity protection is requested by the File owner (i.e. the subject that has the right to perform File.Change for a File) by setting an option in the attribute File.AccessRights.

SS.MAC adds data to the communication stream that enables both the TOE and the terminal to detect integrity violations, replay attacks or man-in-the-middle attacks using the cryptographic algorithm 128-bit AES CMAC [8]

or AESLRP CMAC [16].

If an integrity protected communication is requested, SS.MAC verifies the data sent by the terminal and returns an error code if such an attack is detected. The detection mechanism covers all frames exchanged between the terminal and the TOE up to the current integrity protected frame. Therefore SS.MAC can detect any injected/modified frame in the communication before the transfer of the integrity protected frame.

SS.TRANSACTION **Transaction**

The transaction mechanism implemented by SS.TRANSACTION ensures that either all or none of the (modifying) commands within a transaction are performed. The transaction mechanism is active for backup data files, values, cyclic record files and transaction MAC files. It is not active for standard data files. All file types with the exception of ”standard data files” are called ”backup files” in the following.

Remark 6. The SS.TRANSACTION service is only supported by the MIFARE DESFire Light and MIFARE IDentity variants.

SS.TRANSACTION is always active for the respective file types. This means that for every modifying operation with a backup file an explicit commit request must be issued in order to let the modifications take effect.

Several reasons will abort a transaction: These are the explicit abort request, chip reset, a "select" command, a deselect command, a create or delete transaction MAC file command, any failure of a command, or certain configuration changes like enabling LRP.

SS.TRANSACTION_MAC **Transaction Message Authentication Code**

SS.TRANSACTION_MAC ensures that a MAC is calculated over a commited transaction with the dedicated AppTransactionMACKey, wich exists per Application. Note that a commited transaction consists of a sequence of operations on the TOE.

This is done by creating a so called "TransactionMAC file" and defining a AppTransactionMACKey.

SS.TRANSACTION_MAC provides a service to AppUsers and AppMgr. SS.TRANSACTION_MAC helps AppUsers to prove the authenticity of committed transactions on the TOE towards the AppMgr or a backend. The transaction MAC, calculated by SS.TRANSACTION_MAC, also involves a Transaction MAC Counter maintained by the TOE, which helps the AppMgr to detect replay by the AppUser.

Remark 7. The SS.TRANSACTION_MAC service accessible in the MIFARE DESFire Light and MIFARE IDentity variants.

SS.NO_TRACE **Preventing Traceability**

SS.NO_TRACE provides an option to use a random ID during the ISO14443 anti-collision sequence [13]. 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.

Card specific information suitable to identify single end-users comprises the UID, and files readable by Anybody depending on the file configuration. The UID can be read out only by the AppMgr and AppUser if the option for the random UID is set. Setting this option is restricted to the AppMgr.

Remark 8. Note that SS.NO_TRACE protects the card specific data. In order to prevent traceability at all the authorised subjects have to make use of the access control mechanism implemented by SS.ACC_CTRL.

By using SS.NO_TRACE and SS.ACC_CTRL it can be ensured that no unauthorised subject can gain information about the end-user that allows for identifying the end-user. As a consequence this does not allow for tracing the end-user, e.g. by setting up a terminal controlled by an attacker.

SS.TAG-TAMPER **Tag Tamper Detection**

SS.TAG-TAMPER provides a mechanism for detection and permanent storage of the status of the tag tamper wire. The recorded status byte cannot be changed or deleted. The status byte can be read via NXP proprietary command, as well as via standard ISO7816-4 commands by a reader capable of reading NFC Forum Type 4 tag.

Remark 9. This security service is only available for NTAG42xTf

7.1.2 Security Features

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. Thereby SF.LOG prevents the disclosure of User Data or TSF data stored and/or processed in the security IC through the measurement of the power consumption or emanation and subsequent complex signal processing. The protection of the TOE comprises different features within the design that support the other portions of security functionality. The protection level aims at providing resistance against an attack with an enhanced-basic attack potential.

SF.COMP **Protection of Mode Control**

SF.COMP provides a control of the TOE modes. This includes the protection and storing of NXP configuration data.

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 AES co-processor, the memories, registers, I/O interfaces and the other system peripherals) during the execution of the IC Embedded Software. This includes all specific security features of the TOE which are able to provide an active response.

The TOE ensures its correct operation and prevents any malfunction 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.

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. 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 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 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 configuration as stored in NV memory. Depending in the kind of integrity violation the TOE may also enter a permanent irreversible secure state from which it is not possible to recover. 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.

Mounting physical attacks require usually a significant amount of attacker expertise and costly equipment. Furthermore, very often physical attacks alone do not lead to a direct exposure of assets, because the attacker needs to additionally bypass other supportive mechanisms. Therefore, sophisticated attacks including physical attack techniques are difficult to mount for an attack with an enhanced-basic attack potential.
As a consequence, the TOE implements a restricted set of features to protect itself against the effects of these attacks. In detail:

- Layout Protection: a set of security mechanisms to hamper reverse engineering of the IC and physical probing such as specific synthesis, layout techniques and shielding
- Memory Integrity Protection: Integrity protection on EEPROM by error correction codes.
- Start-up Integrity Protection: Set of security mechanisms that detect integrity errors during start-up
- Redundant Encoding: Set of security mechanisms that ensure that security critical flags and the according checks are kept with a redundancy.
- Address Scrambling: Set of security mechanisms that ensure that physical addresses are scrambled before writing data to the RAM or EEPROM memory.
- Code.- & Datapath Key Management: Set of security mechanisms that ensure that keys used for the secure data path are derived correctly and securely

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-2017-04-001, Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components, Version 3.1 CCMB-2017-04-002, Revision 5, April 2017.

[4] Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components, Version 3.1 CCMB-2017-04-003, Revision 5, April 2017.

[5] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1 CCMB-2017-04-004, Revision 5, April 2017.

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

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

[8] 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.

[9] 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.

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

[11] ISO/IEC 14443-4:2008 Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 4: Transmission protocol, 07 2008.

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

[13] ISO/IEC 14443-3:2011 Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 3: Initialization and anticollision, 04 2011.

[14] 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.

[15] 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.

[16] Martin Feldhofer Bruce Murray Marcel Medwed, Ventzislav Nikov and Mario Lamberger. Leakage resilient primitive, v1.1 external, May 16th, 2017.

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: 2018-12-31

Document identifier: <Certid>