MIFARE DESFire EV1 MF3ICD81

Security Target Lite

Rev.1.5 — 10 May 2011

Evaluation Documentation

BSI-DSZ-CC-0712

Public

Document information

Info	Content
Keywords	Security Target Lite, MF3ICD81
Abstract	Evaluation of the NXP MIFARE DESFire EV1 MF3ICD81 Secure Smart Card Controller developed and provided by NXP Semiconductors, Business Unit Identification according to the Common Criteria for Information Technology Evaluation (CC) at Level EAL4 augmented

founded by Philips

Revision history

Rev	Date	Description	Remarks
0.5	28 may 2008	Initial version	Derived from full ST V1.3.1, Chapter 8.3 changed
0.9	28 may 2008	Internally Revised Version	Revised by HGA & AHr
1.0	17 September 2008	Assumption A.Terminal_Support added (with related objective and requirement and further clarifications). Names of guidance documents changed.	Derived from (full) ST V1.5
1.1	10 October 2008	Revision History corrected	1st line of Revision History of version 1.0 deleted
1.2	09 August 2010	Update: Table 1, hardware via and software Added new commercial type, MF3ICD01	
1.3	14 February 2011	Role “Nobody” removed from FMT_SMR.1.1 Certification ID changed to 0712.	
1.4	04 March 2011	Introduction of new delivery types: MOA8 and 75µm sawn wafer; Note added to FCS_COP.1[DES].	
1.5	10 May 2011	Added hardware version t507C.	

Latest version is: Rev.1.5 (10 May 2011)

Contact information

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

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

1. ST Introduction

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

1.1 ST Identification

This Security Target (st-lite_mf3icd81.doc, Rev.1.5, 10 May 2011) refers to the "MIFARE DESFire EV1 MF3ICD81" (TOE) provided by NXP Semiconductors, Business Unit Identification for a Common Criteria evaluation.

1.2 ST Overview

1.2.1 Introduction

NXP has developed the MIFARE DESFire EV1 MF3ICD81 to be used with Proximity Coupling Devices (PCDs, also called “terminal”) according to ISO14443 Type A. The communication protocol complies to part ISO 14443-4. The MF3ICD81 is primarily designed for secure contact-less transport applications and related loyalty programs as well as access control systems. It fully complies with the requirements for fast and highly secure data transmission, flexible memory organisation and interoperability with existing infrastructure.

The TOE is a Smart Card comprising a hardware platform and a fixed software package (Smartcard Embedded Software). The software package provides an operating system with a set of functions used to manage the various kinds of data files stored in the non-volatile EEPROM memory. The operating system supports a separation between the data of different applications and provides access control if required by the configuration.

The TOE includes also IC Dedicated Software to support its start-up and for test purposes after production. The Smart Card Controller hardware comprises an 8-bit processing unit, volatile and non-volatile memories, cryptographic co-processors, security components and one communication interface.

The TOE includes a functional specification and a guidance document. This documentation contains a description of the hardware and software interface, the secure configuration and usage of the product by the terminal designer.

The security measures of the MF3ICD81 are designed to act as an integral part of the combination of hardware platform and software package in order to strengthen the product as a whole. Several security measures are completely implemented in and controlled by the hardware. Other security measures are controlled by the combination of hardware and software or software guided exceptions.

1.2.2 Life-Cycle

Regarding the life cycle of the smartcard (refer to the “Smartcard IC Platform Protection Profile”, [7] section 8.1), the development and the production phase of the IC with its Smartcard Embedded Software as described for the Target of Evaluation (TOE) is part of the evaluation.

Referring to the description in the PP [7], the TOE is delivered at the end of phase 3 or of phase 4 as described in section 2.1.

Regarding the Application Note 1 of [7] the TOE does not provide additional functions supporting the card's life-cycle beyond those specified in the PP.

Security during Development and Production

During the design and the layout process of the IC and the development of the software only people involved in the specific development project have access to sensitive data. The security measures installed within NXP ensure a secure computer system and provide appropriate equipment for the different development tasks.

The verified layout data is provided by the developers of NXP Semiconductors, Business Unit Identification directly to the wafer fab. The wafer fab generates and forwards the layout data related to the different photo masks to the manufacturer of the photo masks. The photo masks are generated off-site and verified against the design data of the development before the usage. The accountability and the traceability is ensured among the wafer fab and the photo mask provider.

The test process of every die is performed by a test centre of NXP. Delivery processes between the involved sites provide accountability and traceability of the produced wafers. NXP embeds the dice into smartcard modules based on customer demand. Information about non-functional items is stored on magnetic/optical media enclosed with the delivery, available for download or the non-functional items are physically marked.

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

- Dice on wafers
- Smart Card Modules on a module reel

The different (package) types are described in detail in section 2.2.

1.2.3 Specific Issues of Smartcard Hardware and the Common Criteria

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

1.3 CC Conformance and Evaluation Assurance Level

The evaluation is based upon

- Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 2.3, August 2005, CCMB-2005-08-001, [1]
- Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 2.3, August 2005, CCMB-2005-08-002, [2]
- Common Criteria for Information Technology Security Evaluation – Part 3: Security Assurance Requirements, Version 2.3, August 2005, CCMB-2005-08-003, [3]

For the evaluation the following methodology will be used:

- Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 2.3, August 2005, CCMB-2005-08-004, [4]

The chosen level of assurance is **EAL 4 augmented**. The minimum strength level for the TOE security functions is **SOF-high (Strength of functions high)**.

This Security Target claims the following CC conformances:

- Part 2 extended, Part 3 conformant, EAL 4 augmented
- Conformance to the Protection Profile “Smartcard IC Platform Protection Profile”, [7]

Regarding the Application Note 3 of [7] the ST does not change the augmentation as chosen in the Protection Profile. The augmentations to EAL4 defined by the Protection Profile are ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, and AVA_VLA.4.

2. TOE Description

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

2.1 TOE Definition

The Target of Evaluation (TOE) is the smartcard integrated circuit named MF3ICD81 together with its Smartcard Embedded Software. The TOE is available for two different hardware version called t504C (relating to commercial type name MF3ICD81) and t507C (relating to commercial type name MF3ICDH81). The TOE is manufactured in an advanced CMOS process. The TOE includes IC Designer/Manufacturer proprietary IC Dedicated Test Software and IC Dedicated Support Software. The DESFire EV1 Embedded Software is also called Smartcard Embedded Software, according to the terminology used in [7]. Note that this Smartcard Embedded Software is part of the TOE.

The following tables list the TOE components.

Table 1. Components of the TOE (MF3ICD81)

Type	Name	Release	Date	Form of delivery
Hardware	MIFARE DESFire EV1 MF3ICD81 Master	t504C	t504C.gds2 (26.11.2007)	Wafer or modules (dice include reference t504C)
Hardware	MIFARE DESFire EV1 MF3ICD81 Via1	005	romt0cdf005.eco (15.07.2010)	As part of wafer resp. modules (dice include reference 005 on via)
Software	Test ROM Software (the *IC Dedicated Test Software*)	t504C005	23.06.2010	ROM on the chip *(DF8_TestOS.hex)*
Software	Boot ROM Software (the *IC Dedicated Support Software*)	t504C005	23.06.2010	ROM on the chip *(DF8_TestOS.hex)*
Software	DESFire EV1 Embedded Software *(the Smartcard Embedded Software)*	t504C005	15.07.2010	ROM on the chip *(DesFire8.hex)*

Table 2. Components of the TOE (MF3ICDH81)

Type	Name	Release	Date	Form of delivery
Hardware	MIFARE DESFire EV1 MF3ICDH81 Master	t507C	t507C.gds2 (21.07.2009)	Wafer or modules (dice include reference t507C)
Hardware	MIFARE DESFire EV1 MF3ICDH81 Via1	003	romt0cyf003.eco, (19.07. 2010)	As part of wafer resp. modules

Type	Name	Release	Date	Form of delivery
				(dice include reference 003 on via)
Software	Test ROM Software (the *IC Dedicated Test Software*)	t507C003	30.06.2010	ROM on the chip *(DF8_TestOS.hex)*
Software	Boot ROM Software (the *IC Dedicated Support Software*)	t507C003	30.06.2010	ROM on the chip *(DF8_TestOS.hex)*
Software	DESFire EV1 Embedded Software *(the Smartcard Embedded Software)*	t507C003	15.07.2010	ROM on the chip *(DesFire8.hex)*

Table 3. Additional components of the TOE

Type	Name	Release	Date	Form of delivery
Document	MIFARE DESFire EV1 MF3ICD81 Functional Specification [9]			Electronic document
Document	MIFARE DESFire EV1 MF3ICD81 Guidance, Delivery and Operation Manual [10]			Electronic document

2.1.1 Hardware Description

The CPU of the MF3ICD81 has an 8-bit architecture with an instruction set that is based on the 8051 family instruction set. The on-chip hardware components are controlled by the Smartcard Embedded Software via Special Function Registers. These registers are correlated to the activities of the CPU, the memory management unit, interrupt control, contact-less communication, EEPROM, timers and the co-processors. The communication with the MF3ICD81 can be performed through the contact-less interface. The MF3ICD81 is equipped with an interrupt controller. These interrupts force the jump to specific fixed vector addresses in the ROM. Every different interrupt is controlled and guided by a specific part of the Smartcard Embedded Software.

The device includes ROM (32 kByte), RAM (512 Byte) and EEPROM (8 kByte physical – configurable for an available logical size of 0.5kB, 2kB, 4kB or 8kB) memory. The ROM is split in Application-ROM and Test-ROM.

The Triple-DES co-processor supports single DES and Triple-DES operations. Only Triple-DES will be used in this evaluation, either in 2-key or 3-key operation. The AES co-processor supports AES operations with a key length of 128 bits. The random generator provides true random numbers without pseudo random calculation.

2.1.2 Software Description

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

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

The Smartcard Embedded Software provides the main functionality of the TOE in the usage phase. The MF3ICD81 is primarily designed for secure contact-less transport applications and related loyalty programs as well as access control systems. It fully complies with the requirements for fast and highly secure data transmission, flexible memory organisation and interoperability with existing infrastructure. Its functionality consists of:

- Flexible file system that can contain up to 28 applications with up to 32 files in each application.
- Support for different file types like values or data records.
- Mutual three pass authentication, also according to ISO 7816-4.
- Authentication on application level with fine-grained access conditions for files.
- Multi-application support that allows distributed management of applications and ensures application segregation.
- Data encryption for contact-less communication with replay attack protection.
- Transaction system with rollback that ensures consistency for complex transactions.
- Unique serial number for each device (UID) with optional random UID.

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

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

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

2.1.3 Documentation

The Functional Specification [9] is also part of the TOE. It contains a functional description of the communication protocol and the commands implemented by the TOE. The provided documentation can be used by a customer to construct applications using the TOE.

The Functional Specification is supported by the Application Note “MIFARE DESFire EV1 MF3ICD81 Guidance, Delivery and Operation Manual ” [10] which gives additional guidance with regard to the secure usage of the TOE.

2.1.4 Interface of the TOE

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

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

2.1.5 Life Cycle and Delivery of the TOE

For the usage phase the MF3ICD81 chip will be implemented in a credit card sized plastic card (micro-module embedded into the plastic card) or another sealed package.

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

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

Regarding the Application Note 5 of [7] NXP will deliver the TOE with IC Dedicated Support Software and Smartcard Embedded Software, as described in this chapter.

The TOE is able to control two different logical phases. After production of the chip every start-up will lead to the Test Mode and the execution of the IC Dedicated Test Software. At the end of the production test the Test Mode is disabled. With disabled Test Mode every start-up of the chip will lead to the Application Mode with the CPU executing the DESFire EV1 Embedded Software.

2.1.6 TOE Intended Usage

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 most high-end safeguarded applications, and is designed for embedding into contact-less smart cards according to ISO 14443 [13]. Usually the smart card is assigned to a single individual only although the smartcard may be expected to be used for multiple applications in a multi-provider environment. Therefore the TOE may store and process secrets of several systems that must be protected from each other. The secret data shall be used as input for the calculation of authentication data and the encryption of data.

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.

2.1.7 TOE User Environment

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

In the end-user environment (phase 7) Smartcard ICs are used in a wide range of applications to assure authorised conditional access. Examples of such are transportation or access control. The end-user environment therefore covers a wide spectrum of very different functions, thus making it difficult to avoid and monitor any abuse of the TOE.

Note: The phases from TOE Delivery to phase 7 of the smart card life cycle are not part of the TOE construction process in the sense of this Security

Target. Information about those phases are just included to describe how the TOE is used after its construction. Nevertheless the security features of the TOE cannot be disabled in these phases.

2.1.8 General IT features of the TOE

The TOE IT functionality consists of:

- tamper resistant data storage
- control of operation conditions to provide correct operation in the specified range
- basic cryptographic functions (Triple-DES and AES co-processors) and physical random number generator as software support
- data communication via contact-less interface
- strong authentication mechanism to prevent unauthorised use
- access control to separate different applications and files
- different file types for data storage including stored values
- encryption of communication
- transaction mechanism for combining several operations in one atomic operation
- random UID to exacerbate tracing of end-users

2.2 Evaluated package types

A number of package types are supported for the TOE. Each package type has a different commercial type name. The TOE will be available in four different packages and four different memory configurations. Additionally, there are two different hardware versions, t504C (relating to MF3ICD81) and t507C (relating to MF3ICDH81) which use either 17pF or 70pF input capacitance. The operating system is the same for all different configurations. The commercial type name is formed out of the following components:

Table 4. Supported package types and memory configurations (MF3ICD81)

Type	Form	Cap	EE		Package	OS	Description
MF3…	…IC…	…D…	…81…	…01D…	…UD…	…/05	120µm sawn wafer, 8 kBytes EEPROM, 17pF cap.
			…41…				120µm sawn wafer, 4 kBytes EEPROM, 17pF cap.
			…21…				120µm sawn wafer, 2 kBytes EEPROM, 17pF cap.
			…01…				120µm sawn wafer, 0.5 kBytes EEPROM, 17pF cap.
			…81…		…UF…		75µm sawn wafer, 8 kBytes EEPROM, 17pF cap.
			…41…				75µm sawn wafer, 4 kBytes EEPROM, 17pF cap.
			…21…				75µm sawn wafer, 2 kBytes EEPROM, 17pF cap.
			…01…				75µm sawn wafer, 0.5 kBytes EEPROM, 17pF cap.
	…MO…		…81…		…A4…		MOA4 module on reel, 8 kBytes EEPROM, 17pF cap.
			…41…				MOA4 module on reel, 4 kBytes EEPROM, 17pF cap.
			…21…				MOA4 module on reel, 2 kBytes EEPROM, 17pF cap.
			…01…				MOA4 module on reel, 0.5 kBytes EEPROM, 17pF cap.
			…81…		…A8…		MOA8 module on reel, 8 kBytes EEPROM, 17pF cap.
			…41…				MOA8 module on reel, 4 kBytes EEPROM, 17pF cap.
			…21…				MOA8 module on reel, 2 kBytes EEPROM, 17pF cap.
			…01…				MOA8 module on reel, 0.5 kBytes EEPROM, 17pF cap.

Table 5. Supported package types and memory configurations (MF3ICDH81)

Type	Form	Cap	EE		Package	OS	Description
MF3…	…IC…	…DH…	…81…	…01D…	…UD…	…/05	120µm sawn wafer, 8 kBytes EEPROM, 70pF cap.
			…41…				120µm sawn wafer, 4 kBytes EEPROM, 70pF cap.
			…21…				120µm sawn wafer, 2 kBytes EEPROM, 70pF cap.
			…01…				120µm sawn wafer, 0.5 kBytes EEPROM, 70pF cap.
			…81…		…UF…		75µm sawn wafer, 8 kBytes EEPROM, 70pF cap.
			…41…				75µm sawn wafer, 4 kBytes EEPROM, 70pF cap.
			…21…				75µm sawn wafer, 2 kBytes EEPROM, 70pF cap.
			…01…				75µm sawn wafer, 0.5 kBytes EEPROM, 70pF cap.
	…MO…		…81…		…A4…		MOA4 module on reel, 8 kBytes EEPROM, 70pF cap.
			…41…				MOA4 module on reel, 4 kBytes EEPROM, 70pF cap.
			…21…				MOA4 module on reel, 2 kBytes EEPROM, 70pF cap.
			…01…				MOA4 module on reel, 0.5 kBytes EEPROM, 70pF cap.
			…81…		…A8…		MOA8 module on reel, 8 kBytes EEPROM, 70pF cap.
			…41…				MOA8 module on reel, 4 kBytes EEPROM, 70pF cap.
			…21…				MOA8 module on reel, 2 kBytes EEPROM, 70pF cap.
			…01…				MOA8 module on reel, 0.5 kBytes EEPROM, 70pF cap.

The “DH” reflects that the TOE uses the hardware version t507C. The “D” reflects that the TOE uses the hardware version t504C.

For example, the commercial type name “MF3ICDH4101DUD/05” denotes a DESFire EV1 supplied on 120µm thick wafer, with 4 K EEPROM and 70pF input capacitance. The commercial type name “MF3MOD8101DA4/05” denotes a DESFire EV1 supplied in MOA4 modules on a reel, with 8K EEPROM and 17pF input capacitance.

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 1.2.2).

All commercial types listed in the table above are subject of this evaluation. However only the identifier “MF3ICD81” will be used in the rest of the document to make referencing easier. Unless described explicitly all information given in the remainder of the ST applies to all commercial types.

2.3 Further Definitions and Explanations

Since the Security Target claims conformance to the PP “Smartcard IC Platform Protection Profile”, the concepts are used in the same sense. For the definition of terms refer to the Protection Profile [7]. This chapter does not need any supplement in the Security Target.

3. TOE Security Environment

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

3.1 Description of Assets

Since this Security Target claims conformance to the PP “Smartcard IC Platform Protection Profile” [7], the assets defined in section 3.1 of the Protection Profile are applied and the assets regarding threats are clarified in this Security Target.

The assets regarding the threats are:

- logical design data, physical design data, IC Dedicated Software,
- Initialisation Data and Pre-personalisation Data, specific development aids, test and characterisation related data, material for software development support, and photomasks
- the TOE correct operation
- the Smartcard Embedded Software
- the special functions for the communication with an external interface device, the cryptographic co-processors for Triple-DES and AES, the random number generator
- the User Data comprising
  - authentication data like keys
  - issuer data like card holder name or processing options
  - representation of monetary values, e.g. a stored value for transport applications
- the TSF Data.

Regarding the Application Notes 6 and 7 of [7] this Security Target includes Smartcard Embedded Software and therefore does contain more assets compared to [7]. These assets are described above.

3.2 Assumptions

Since this Security Target claims conformance to the PP “Smartcard IC Platform Protection Profile” [7], the assumptions defined in section 3.2 of the Protection Profile are valid for this Security Target. The following table lists the assumptions of the Protection Profile.

Table 6. Assumptions defined in the Protection Profile

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

Note that the assumptions A.Plat-Appl and A.Resp-Appl defined in the Protection Profile address the development of the Smartcard Embedded Software. In this Security Target the Smartcard Embedded Software is part of the TOE, therefore the assumptions have to be met by the TOE and are no longer addressed to the operating environment of the TOE.

A.Secure_Values — Usage of secure values

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

A.Terminal_Support — Terminal support to ensure integrity and confidentiality

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

Regarding the Application Notes 8 and 9 of [7] this Security Target defines two additional assumptions regarding specific security functionality.

3.3 Threats

Since this Security Target claims conformance to the PP “Smartcard IC Platform Protection Profile” [7], the threats defined in section 3.3 of the Protection Profile are valid for this Security Target. The following table lists the threats defined by the PP:

Table 7. Threats defined by the Protection Profile

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

Considering the Application Notes 10 and 11 of [7] the following additional threats are defined in this Security Target:

T.Data-Modification — Unauthorised data modification

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

T.Impersonate — Impersonating authorised users during authentication

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

T.Cloning

Cloning

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

3.4 Organisational Security Policies

Since this Security Target claims conformance to the PP “Smartcard IC Platform Protection Profile” [7], the policy P.Process-TOE “Protection during TOE Development and Production” of the Protection Profile is applied here also.

Regarding the Application Note 12 of [7] the following additional policies are defined in this Security Target:

P.Confidentiality

Confidentiality during communication

The TOE shall provide the possibility to protect selected data elements from eavesdropping during contact-less communication. The TOE shall also provide 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.

P.No-Trace

Un-traceability of end-users

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

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

P.Plat-Appl

Usage of hardware platform

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

P.Resp-Appl

Treatment of user data

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

4. Security Objectives

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

4.1 Security Objectives for the TOE

The TOE shall provide the following security objectives, taken from the Protection Profile Smartcard IC Platform Protection Profile [7]:

Table 8. Security objectives defined in the PP

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

Regarding the Application Notes 13 and 14 of [7] the following additional security objectives are defined based on additional functionality provided by the TOE as specified below.

O.Access-Control Access Control

The TOE must provide an access control mechanism for data stored by it. The access control mechanism shall apply to 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.Confidentiality 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 element. The TOE shall also provide the possibility to detect replay or man-in-the-middle attacks within a session. This shall be implemented by checking verification data sent by the terminal and providing verification data to the terminal.

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.

Note that the following two objectives are identical to the objectives OE.Plat-Appl and OE.Resp-Appl defined in [7].

O.Plat-Appl Usage of hardware platform

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

O.Resp-Appl Treatment of user data

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

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

4.2 Security Objectives for the Environment

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

Table 9. Security objectives for the environment, taken from the PP

Security objective	Description	Applies to phase...
OE.Plat-Appl	*Usage of Hardware Platform*	*Phase 1*

Security objective	Description	Applies to phase...
OE.Resp-Appl	*Treatment of User Data*	*Phase 1*
OE.Process-TOE	Protection during TOE Development and Production	Phase 2 up to the TOE Delivery at the end of phase 3
OE.Process-Card	Protection during Packaging, Finishing and Personalisation	Begin of phase 4 up to the end of phase 6

Note that the objective OE.Plat-Appl of the Protection Profile is replaced by O.Plat-Appl in this Security Target. In the same way OE.Resp-Appl is replaced by O.Resp-Appl.

OE.Secure_Values Generation of secure values

The environment shall generate confidential and secure keys for authentication purpose. These values are generated outside the TOE and they are downloaded to the TOE during the personalisation or usage in phase 5 to 7

OE.Terminal_Support Terminal support to ensure integrity and confidentiality

The terminal shall verify information sent by the TOE in order to ensure integrity and confidentiality of the communication. This involves checking of MAC values, verification of redundancy information according to the cryptographic protocol and secure closing of the communication session.

5. IT Security Requirements

5.1 TOE Security Requirements

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

5.1.1 TOE Security Functional Requirements

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

5.1.1.1 SFRs of the Protection Profile

Table 10 below shows all SFRs which are specified in the Protection Profile Smartcard IC Platform Protection Profile [7] (in the order of definition in the PP). Some of the SFRs are CC Part 2 extended and defined in the Protection Profile. This is shown in the third column of the table.

Table 10. SFRs taken from the PP

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

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

FCS_RND.1	**Quality metric for random numbers**
FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet *the requirement to provide an entropy of at least 7.976 bit in each byte* [1].
Dependencies:	No dependencies.

[1] [assignment: a defined quality metric]

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

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

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

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

Considering the Application Note 15 of [7] in the following paragraphs several SFRs that are not required in the Protection Profile are defined.

Regarding the Application Note 16 of [7] an additional generation of audit is not defined for “Limited fault tolerance” (FRU_FLT.2) and “Failure with preservation of secure state” (FPT_FLS.1).

Considering the Application Note 17 of [7] no additional requirement is defined for the TOE itself.

5.1.1.2 Additional SFRs regarding access control

Access Control Policy

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

The subjects are

- The **Administrator** i.e. the subject that owns or has access to the card master key.
- The **Application Manager** i.e. the subject that owns or has access to an application master key. Note that the TOE supports multiple applications and therefore multiple Application Managers, however for one application there is only one Application Manager.
- The **Application User** i.e. the subject that owns or has access to a key that allows to perform operations with application objects. Note that the TOE supports multiple Application Users within each application and the assigned rights to the Application Users can be different, which allows to have more or less powerful Application Users.
- Any other subject belongs to the role **Everybody**. This includes the card holder (i.e. end-user) and any other subject e.g. an attacker. These subjects do not possess any key and can not perform operations that are restricted to the Administrator, Application Manager and Application User.
- The term **Nobody** will be used to explicitly indicate that no rights are granted to any subject.

The objects are

- The **Card** itself.
- The card can store a number of **Applications**.
- An application can store a number of **Data Files** of different types.

- One specific type of data file are **Values**.

Note that data files and values can be grouped in *standard files* and *backup files*, with values belonging to the group of backup files. When the term “file” is used without further information then both data files and values are meant.

The operations that can be performed with the objects are

- **read** a value or data from a data file,
- **write** data to a data file,
- **increase** a value (with a limit or unlimited),
- **decrease** a value,
- **create** an application, a value or a data file,
- **delete** an application, a value or a data file and
- **modify attribute** of the card, an application, a value or a data file. Note that ‘freeze’ will be used as specific form of modification that prevents any further modify.

The security attributes are

- Attributes of the card, applications, values and data files. There is a set of attributes for the card, a set of attributes for every application and a set of attributes for every single file within an application. The term “**card attributes**” will be used for the set of attributes related to the card, the term “**application attributes**” will be used for the set of application attributes and the term “**file attributes**” will be used for the attributes of values and data files.

Note that subjects are authorised by cryptographic keys. These keys are considered as authentication data and not as security attributes. The card has a card master key. Every application has an application master key and a variable number of keys used for operations on data files or values (all these keys are called application keys). The application keys within an application are numbered.

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

FMT_SMR.1	**Security roles**
Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles *Administrator, Application Manager, Application User and Everybody*[2].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification
Note:	Based on the definition Nobody is not considered as role.

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

FDP_ACC.1	**Subset access control**
Hierarchical to:	No other components.

[2] [assignment: the authorised identified roles]

FDP_ACC.1.1 The TSF shall enforce the *Access Control Policy* [3] on *all subjects, objects, operations and attributes defined by the Access Control Policy* [4].

Dependencies: FDP_ACF.1 Security attribute based access control

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

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the *Access Control Policy* [5] to objects based on the following: *all subjects, objects and attributes* [6].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- *The Administrator can create and delete applications.*
- *The Application Manager of an application can delete this application, create data file and values within this application, delete data files and values within this application.*
- *An Application User can read or write a data file; read, increase or decrease a value based on the access control settings in the respective file attribute.* [7]

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

- *Everybody can create applications if this is allowed by a specific card attribute.*
- *Everybody can create and delete data files or values of a specific application if this is allowed by a specific application attribute.*
- *Everybody can read or write a data file; read, increase or decrease a value if this is allowed by a specific file attribute.* [8]

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the *rules:*

[3] [assignment: access control SFP]

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

[5] [assignment: access control SFP]

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

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

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

- *Nobody can read or write a data file; read, increase or decrease a value if this is explicitly set for the respective operation on the respective data file or value.* [9]

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

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

FMT_MSA.3 **Static attribute initialisation**

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the *Access Control Policy* [10] to provide *permissive* [11] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow *no subject* [12] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

Application Note: The only initial attributes are the card attributes. All other attributes have to be defined at the same time the respective object is created.

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

FMT_MSA.1 **Management of security attributes**

Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the *Access Control Policy* [13] to restrict the ability to *modify or freeze* [14] the security attributes *card attributes, application attributes and file attributes* [15] to *the Administrator, Application Manager and Application User, respectively* [16].

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

[9] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]
[10] [assignment: access control SFP, information flow control SFP]
[11] [selection, choose one of: restrictive, permissive, [assignment: other property]]
[12] [assignment: the authorised identified roles]
[13] [assignment: access control SFP, information flow control SFP]
[14] [selection: change_default, query, modify, delete, [assignment: other operations]]
[15] [assignment: list of security attributes]
[16] [assignment: the authorised identified roles]

Refinement:	The detailed management abilities are:

- The Administrator can modify the card attributes. The card attributes contain a flag that when set will prevent any further change of the card attributes, thereby allowing to freeze the card attributes.
- The Application Manager can modify the application attributes. The application attributes contain a flag that when set will prevent any further change of the application attributes, thereby allowing to freeze the application attributes.
- The Application Manager can decide to restrict the ability to modify the file attributes to the Application Manager, an Application User, Everybody or to Nobody. The restriction to Nobody is equivalent to freezing the file attributes.
- As an implication of the last rule, any subject that receives the modify abilities from the Application Manger gets these abilities transferred.
- The implication given in the previous rule includes the possibility for an Application User to modify the file attributes if the Application Manager decides to transfer this ability. If there is no such explicit transfer an Application User does not have the ability to modify the file attributes.

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

FMT_SMF.1	**Specification of Management Functions**
Hierarchical to:	No other components.
FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: *Authenticate a user,* *Invalidating the current authentication state based on the functions: Selecting an application or the card, Changing a key, Occurrence of any error during the execution of a command, Reset;* *Changing a security attribute,* *Creating or deleting an application, a value or a data file.* [17]
Dependencies:	No dependencies

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

FDP_ITC.2	**Import of user data with security attributes**
Hierarchical to:	No other components.

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

FDP_ITC.2.1 The TSF shall enforce the *Access Control Policy* [18] when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: *no additional rules* [19].

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]
FPT_TDC.1 Inter-TSF basic TSF data consistency

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

FPT_TDC.1 Inter-TSF basic TSF data consistency

Hierarchical to: No other components.

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret *data files and values* [20] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use *the rule: data files or values can only be modified by their dedicated type-specific operations honouring the type-specific boundaries* [21] when interpreting the TSF data from another trusted IT product.

Dependencies: No dependencies.

Application Note: The TOE does not interpret the *contents* of the data, e.g. it can not determine if data stored in a specific data file is an identification number that adheres to a specific format. Instead the TOE distinguishes different types of files and ensures that type-specific boundaries can not be violated, e.g. values do not overflow, single records are limited by their size and cyclic records are handled correctly.

[18] [assignment: access control SFP and/or information flow control SFP]

[19] [assignment: additional importation control rules]

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

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

Implications of the Access Control Policy

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

- The TOE end-user does normally not belong to the group of authorised users (Administrator, Application Manager, Application User), but regarded as ‘Everybody’ by the TOE. This means that the TOE cannot determine if it is used by its intended end-user (in other words: it cannot determine if the current card holder is the owner of the card).
- The Administrator can have the exclusive right to create and delete applications on the Smart Card, however he can also grant this privilege to Everybody. Additionally, changing the Smart Card attributes is reserved for the Administrator. Application keys, at delivery time should be personalized to a preliminary, temporary key only known to the Administrator and the Application Manager.
- At application personalization time, the Application Manager uses the preliminary application key in order to personalize the application keys, whereas all keys, except the application master key, can be personalized to a preliminary, temporary key only known to the Application Manager and the Application User. Furthermore, the Application Manager has the right to create files within his application scope.

5.1.1.3 Additional SFRs regarding confidentiality and authentication

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

FCS_COP.1[DES]	**Cryptographic operation**
Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform *encryption and decryption* [22] in accordance with a specified cryptographic algorithm *Triple Data Encryption Algorithm (TDEA)* [23] and cryptographic key sizes *of 112 or 168 bit* [24] that meet the following *list of standards* [25]: *FIPS PUB 46-3 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION DATA ENCRYPTION STANDARD (DES) Reaffirmed 1999 October 25, keying options 1 and 2.*
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, FMT_MSA.2 Secure security attributes.
Note:	The cryptographic functionality FCS_COP.1[DES] provided by the TOE achieves a security level of maximum 80 Bits, if keying option 2 is used.

[22] [assignment: list of cryptographic operations]

[23] [assignment: cryptographic algorithm]

[24] [assignment: cryptographic key sizes]

[25] [assignment: list of standards]

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

FCS_COP.1[AES]	**Cryptographic operation**
Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform *encryption and decryption* [26] in accordance with a specified cryptographic algorithm *Advanced Encryption Standard (AES) algorithm* [27] and cryptographic key sizes *of 128 bit* [28] that meet the following *list of standards* [29]: *FIPS PUB 197 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, ADVANCED ENCRYPTION STANDARD (AES), National Institute of Standards and Technology, 2001 November 26.*
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], FCS_CKM.4 Cryptographic key destruction, FMT_MSA.2 Secure security attributes.

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

FIA_UID.2	**User identification before any action**
Hierarchical to:	FIA_UID.1
FIA_UID.2.1	The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	No dependencies.
Application Note:	Identification of a user is performed upon an authentication request based on the 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 Application Manager of the respective application. Before any authentication request is issued the user is identified as ‘Everybody’.

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

FIA_UAU.2	**User authentication before any action**
Hierarchical to:	FIA_UAU.1

[26] [assignment: list of cryptographic operations]

[27] [assignment: cryptographic algorithm]

[28] [assignment: cryptographic key sizes]

[29] [assignment: list of standards]

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

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

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

FIA_UAU.5.1 The TSF shall provide *‘none’ and cryptographic authentication* [30] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the *following rules:*

- *The ‘none’ authentication is performed with anyone who communicates with the TOE without issuing an explicit authentication request. The ‘none’ authentication implicitly and solely authorises the ‘Everybody’ subject.*
- *The cryptographic authentication is used to authorise the Administrator, Application Manager and Application User.* [31].

Dependencies: No dependencies.

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

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to *change_default, modify or freeze* [32] the *card master key, application master keys and application keys* [33] to *the Administrator, Application Manager and Application User* [34].

Refinement: The detailed management abilities are:

- The Administrator can modify the card master key. The card attributes contains a flag that when set will prevent any further change of the card master key, thereby allowing to freeze the card master key.
- The Administrator can change the default key that is used for the application master key and for the application keys when an application is created.

[30] [assignment: list of multiple authentication mechanisms]

[31] [assignment: rules describing how the multiple authentication mechanisms provide authentication]

[32] [selection: change_default, query, modify, delete, clear, [assignment: other operations]]

[33] [assignment: list of TSF data]

[34] [assignment: the authorised identified roles]

- The Application Manager of an application can modify the application master key of this application. The application attributes contain a flag that when set will prevent any further change of the application master key, thereby allowing to freeze the application master key.
- The Application Manager can decide to restrict the ability to modify the application keys to the Application Manager, the Application Users or to Nobody. The restriction to Nobody is equivalent to freezing the application keys. The Application Users can either change their own keys or one Application User can be defined that can change all keys of the Application Users within an application.
- As an implication of the last rule, any subject that receives the modify abilities from the Application Manger gets these abilities transferred.

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

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

FTP_TRP.1	**Trusted path**
Hierarchical to	No other components.
FTP_TRP.1.1	The TSF shall provide a communication path between itself and *remote* [35] 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 or disclosure.
FTP_TRP.1.2	The TSF shall permit *remote users* [36] to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for *authentication requests with DES and AES, confidentiality and/or data integrity verification for data transfers protected with AES and based on a setting in the file attributes* [37].
Dependencies:	No dependencies.

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

FCS_CKM.4	**Cryptographic key destruction**
Hierarchical to:	No other components.

[35] [selection: remote, local]

[36] [selection: the TSF, local users, remote users]

[37] [selection: initial user authentication,[assignment: other services for which trusted path is required]]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *overwriting of memory* [38] that meets the following: *none* [39].

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]
FMT_MSA.2 Secure security attributes

5.1.1.4 Additional SFRs regarding the robustness

The TOE shall meet the requirement “Basic rollback (FDP_ROL.1)” as specified below.

FDP_ROL.1 Basic rollback

Hierarchical to: No other components.

FDP_ROL.1.1 The TSF shall enforce *Access Control Policy* [40] to permit the rollback of the *operations that modify the value or data file objects* [41] on the *backup files* [42].

FDP_ROL.1.2 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, (re-)authentication (either successful or not), select command, explicit commit, explicit abort, command failure* [43].

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

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

FPT_RPL.1 Replay detection

Hierarchical to: No other components.

FPT_RPL.1.1 The TSF shall detect replay for the following entities: *authentication requests with DES and AES, confidentiality and/or data integrity verification for data transfers protected with AES and based on a setting in the file attributes* [44].

FPT_RPL.1.2 The TSF shall perform *rejection of the request* [45] when replay is detected.

Dependencies: No dependencies.

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

[38] [assignment: cryptographic key destruction method]

[39] [assignment: list of standards]

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

[41] [assignment: list of operations]

[42] [assignment: information and/or list of objects]

[43] [assignment: boundary limit to which rollback may be performed]

[44] [assignment: list of identified entities]

[45] [assignment: list of specific actions]

FPR_UNL.1 **Unlinkability**

Hierarchical to: No other components.

FPR_UNL.1.1 The TSF shall ensure that *unauthorised subjects other than the card holder* [46] are unable to determine whether *any operation of the TOE* [47] *were caused by the same user* [48].

Dependencies: No dependencies.

5.1.1.5 SOF claim for TOE security functional requirements

Since the assurance level is augmented with AVA_VLA.4 the required level for the Strength of Function (SOF) of the above listed security functional requirements level is “SOF-high”.

5.1.2 TOE Security Assurance Requirements

Table 11 below lists all security assurance components that are valid for this Security Target. These security assurance components are required by EAL4 (see section 1.3) or by the Protection Profile.

Considering the Application Note 18 of [7] the ST does not change the augmentation or assurance level defined in the PP.

Table 11. Security Assurance Requirements according to PP

SAR	Title
ACM_AUT.1	Partial CM automation
ACM_CAP.4	Generation support and acceptance procedures
ACM_SCP.2	Problem tracking CM coverage
ADO_DEL.2	Detection of modification
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.2	Fully defined external interfaces
ADV_HLD.2	Security enforcing high-level design
ADV_IMP.2	Implementation of the TSF
ADV_LLD.1	Descriptive low-level design
ADV_RCR.1	Informal correspondence demonstration
ADV_SPM.1	Informal TOE security policy model
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ALC_DVS.2	Sufficiency of security measures

[46] [assignment: set of users and/or subjects]

[47] [assignment: list of operations]

[48] [selection: were caused by the same user, are related as follows[assignment: list of relations]]

SAR	Title
ALC_LCD.1	Developer defined life-cycle model
ALC_TAT.1	Well-defined development tools
ATE_COV.2	Analysis of coverage
ATE_DPT.1	Testing: high-level design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_MSU.3	Analysis and testing for insecure states
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.4	Highly resistant

5.1.3 Refinements of the TOE Security Assurance Requirements

The ST claims conformance to the Protection Profile “Smartcard IC Platform Protection Profile”, and therefore it has to be conform to the refinements of the TOE security assurance requirements made by the PP. Refinements are defined in [7] for the Security Assurance Requirements ACM_CAP.4, ACM_SCP.2, ADO_DEL.2, ADO_IGS.1, ADV_FSP.2, AGD_ADM.1, AGD_USR.1, ALC_DVS.2 and ATE_COV.2. With regard to Application Note 19 of the PP the ST does not claim conformance to hierarchically higher assurance requirements.

5.2 Security Requirements for the Environment

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

5.2.1 Security Requirements for the IT-Environment

There are no Security Requirements for the IT-Environment defined in the PP “Smartcard IC Platform Protection Profile”. In this ST two additional Security Requirements for the IT-Environment are defined, one due to a dependency of a security functional requirement and one based on an objective for the environment.

The dependency FMT_MSA.2 derived from the added security functional requirements for cryptographic operation (FCS_COP.1[DES], FCS_COP.1[AES] and FCS_CKM.4) is defined as Security Requirements for the IT-Environment in this Security Target. Since the requirements must be fulfilled by the authorised users of the TOE it is consequently seen as IT-Environment.

FMT_MSA.2 requires that “The TSF shall ensure that only secure values are accepted for security attributes.” This is clearly out of scope for the TOE. The design concept of the TOE and the systems in which the TOE is used is based on the fact that the authorised users can protect their data stored by the TOE by using secret keys and a secure access configuration. Therefore the TOE can not ensure that the security attributes are secure, this is the primary responsibility of the authorised users. Note that FMT_MSA.2 is a dependency of the added security functional requirements for cryptographic operation (FCS_COP.1[DES], FCS_COP.1[AES] and FCS_CKM.4) and the cryptographic keys used by the TOE are considered as authentication data and not security attributes by the

Common Criteria, however the argumentation does not change: secure keys must be used by the authorised users, therefore FMT_MSA.2 is a security requirement for the IT environment. Note that the TOE does allow Single-DES, but this shall not be used in the evaluated product.

The IT Environment shall meet the requirement “Terminal support to ensure integrity and confidentiality (RE.Terminal_Support)” as specified below.

RE.Terminal_Support Terminal support to ensure integrity and confidentiality

The terminal shall verify information sent by the TOE in order to ensure integrity and confidentiality of the communication. This involves checking of MAC values, verification of redundancy information according to the cryptographic protocol and secure closing of the communication session. If any of these actions fail this shall be considered as attack which must be handled in the environment.

The following table summarises the Security Requirements for the IT-Environment.

Table 12. Security Requirements for the IT Environment

SFR	Name	Note
FMT_MSA.2	Secure security attributes	The security attributes must be defined and assigned by the authorised users of the TOE (Administrator, Application Manager, Application User).
RE.Terminal_Support	Terminal support to ensure integrity and confidentiality	The terminal shall verify information sent by the TOE in order to ensure integrity and confidentiality of the communication. This involves checking of MAC values, verification of redundancy information according to the cryptographic protocol and secure closing of the communication session.

5.2.2 Security Requirements for the Non-IT-Environment

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

- *RE.Phase-1 (already met by the TOE, refer to below)*
- RE.Process-Card

However the requirement RE.Phase-1 is already fulfilled by the TOE and therefore no longer part of the Security Requirements for the Non-IT-Environment.

Clarification of “Protection during Packaging, Finishing and Personalisation (RE.Process-Card)”

The Protection Profile defined RE.Process-Card that explicitly requires protection during personalisation. The personalisation is performed after TOE delivery and before delivery to the end-user. It is required that the personalization is performed in a secure and controlled environment. The secure environment must ensure that communication with the TOE can not be eavesdropped. Furthermore unprocessed devices shall be kept physically secure. If the personalization involved multiple steps, sites or parties all these different parts must ensure this assumption.

6. TOE Summary Specification

This chapter is divided in the sections “TOE Security Functions” and “Assurance Measures”.

6.1 TOE Security Functions

F.AUTH: Authentication

The TOE provides an authentication mechanism to separate authorised subjects from unauthorised subjects. The authentication of subjects is performed by a cryptographic challenge-response. The TOE supports the cryptographic algorithms 2-key Triple-DES, 3-key Triple-DES and 128-bit AES; for DES according to FIPS PUB 46-3 [11] and for AES according to FIPS PUB 197 [12]. A hardware random number generator according to AIS31, functionality class P2, is used to protect the authentication against attacks like e.g. replay.

F.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 F.AUTH identifies and authenticates the role Everybody. The roles Administrator, Application Manager and Application User are authenticated during the authentication request by the knowledge of the respective cryptographic key.

The authentication state is remembered by F.AUTH and the authentication need 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 (Everybody). Additionally, if the Application Manager deletes his application the authentication state will be reset as an implication.

Note that the TOE does also allow Single-DES, but this shall not be used in the evaluated product. The TOE supports a backward compatible DES authentication in addition to the standard DES authentication. The backward compatible DES authentication shall not be used in the evaluated product.

F.ACC_CTRL: Access Control

F.ACC_CTRL provides an access control mechanism to the objects and security attributes that are part of the Access Control Policy. The access control mechanism assigns subjects - (possibly multiple) Application Users - to 4 different groups of operations on files. For data files, the operations are “read”, “write”, “read and write” and “change attribute”. For values the operations are “read and decrease”, “read, decrease, limited increase”, “read, decrease, limited increase, increase” and “change attribute”. One subject can be assigned to each group of file operations. The special subjects “Everybody” and “Nobody” can also be assigned.

For applications the operations are “create file” and “delete file”. These operations can be assigned to the Application Manager or to Everybody. The assignment is stored in the application attributes. If a file is created the file attributes must be supplied with the create request.

For the card the operations are “create application” and “delete application”. These operations can be assigned to the Administrator or to Everybody. The assignment is stored in the card attributes. If an application is created the application attributes must be supplied with the create request. A “delete application” operation will securely delete all application keys by overwriting them with random values.

F.ACC_CTRL also controls access to the security attributes and the authentication data. The card attributes and the card master key can only be changed by the Administrator, as long as the Administrator does not freeze the card attributes or freezes the card master key. The application attributes and application master keys can be changed by the Application Manager, as long as the Application Manager does not freeze the application attributes or the application master key. Additionally the Application Manager can change the Application User keys and decide if the Application Users can change their keys or not. For files, the attributes can be changed by the subject that has the “change attribute” right. F.ACC_CTRL allows the Administrator to specify a default application master key and application keys that will be used when an application is created.

Finally F.ACC_CTRL ensures the type consistency of the file types stored by the TOE. It ensures that values can not over- or underflow. Furthermore size limitations of files are obeyed and F.ACC_CTRL ensures that records read/writes are handled specific to the type of the record file.

F.CONFID: Confidentiality

The TSF F.CONFID 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, however F.CONFID only supports the AES algorithm, therefore it is bound to authentications with this algorithm. Note that the TSF F.CONFID is active after authentication performed with F.AUTH.

F.CONFID 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, F.CONFID also 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 card up to the current encrypted frame. Therefore F.CONFID can detect any injected/modified frame in the communication before the transfer of the encrypted frame, but it can not detect what frame was injected/modified.

F.TRANS: Transaction

The transaction mechanism implemented by F.TRANS 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, linear record files and cyclic record 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.

F.TRANS 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, an authentication request, a ‘select’ command or any failure of a command.

F.NO_TRACE: Preventing traceability

F.NO_TRACE provides an option to use a random UID during the ISO14443 anti-collision sequence. If this option is set, the TOE does not send its internal ID number, but generates a new random ID number during every anti-collision 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. All card specific information can be read out only by the Administrator, Application Manager and Application User if the option for the random UID is set. Setting this option is restricted to the Administrator.

Note that F.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 F.ACC_CTRL.

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

F.OPC: Control of Operating Conditions

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

The TOE ensures its correct operation and prevents any malfunction using the following sub-functions: filtering of power supply and clock input as well as monitoring of power supply, the frequency of the clock and the temperature of the chip by means of sensors. Light sensors are distributed over the chip surface and used to detect light attacks. The thresholds allowed for these parameters are defined within the range where the TOE ensures its correct operation. Specific functional units of the TOE are equipped with special circuitry to detect a number of single fault injection attacks. The TOE software has additional means to detect integrity violations.

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

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

F.PHY: Protection against Physical Manipulation

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

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

F.LOG: Logical Protection

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

The cryptographic co-processors include special features to prevent SPA/DPA analysis of shape and amplitude of the power consumption and ensure that the calculation time is independent from any key and plain/cipher text. Additional features comprise the clock configurations that are used to prevent the possibility to synchronise the internal operation with the external clock or to synchronise with the characteristics of the power consumption that can be used as trigger signal to support leakage attacks.

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

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

F.COMP: Protection of Mode Control

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

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

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

F.COMP also provides the possibility to store initialisation data in the so-called "System Information" area. The configuration of the EEPROM memory size is stored in this area. It is also used to store a unique identification for each die.

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

SOF claim

According to the CEM [4] a Security Target shall identify all mechanisms which can be assessed according to the assurance requirement AVA_SOF.1.

The following mechanisms contributing to these functions were identified, which can be analysed for their permutational or probabilistic properties:

1. The output of the Random Number Generator provided by F.AUTH can be analysed with probabilistic methods.
2. The quality of the mechanism contributing to the leakage attacks of F.LOG especially for the cryptographic algorithms (DES and AES) provided by F.AUTH can be analysed using probabilistic methods on power consumption of the TOE.
3. The authentication mechanism provided by F.AUTH.

Therefore an explicit SOF claim of “high” is made for these mechanisms.

Note: The cryptographic algorithms for DES and AES of F.AUTH can also be analysed with permutational or probabilistic methods but that this is not in the scope of CC evaluations.

6.2 Assurance Measures

Appropriate assurance measures will be employed to satisfy the security assurance requirements defined in section 5.1.2. The developer will provide documents containing the measures and further information needed to examine conformance of the measures to the assurance requirements. The following table gives a mapping between the assurance requirements and the documents containing the information needed for the respective requirement either directly or referring to further documents containing this information.

Table 13. List of documents describing the measures regarding the assurance requirements

Document containing or referring the relevant information	Input evidence according to CC Part 3, which is contained or referred to in the document	Input for assurance classes and families (according to developer actions in CC Part 3)
Security Target, Functional Specification	informal functional specification	ADV_FSP
	correspondence analysis between the TOE summary specification and the functional specification	ADV_RCR
Security Target	TSP model (informal)	ADV_SPM
High Level Design, Design Report	high-level design (informal)	ADV_HLD
	correspondence analysis between functional specification and high-level design	ADV_RCR
Correspondence Demonstration, Design Report	low level design	ADV_LLD
	correspondence analysis between high-level design and low-level design	ADV_RCR
	correspondence analysis between low-level design and implementation representation	ADV_RCR
Implementation representation, Source Code	implementation representation	ADV_IMP
Quality Management Manual and Security Management Manual	configuration management documentation	ACM
	development tools documentation	ALC
	development security documentation	
	life cycle definition documentation	
	parts of the delivery documentation	ADO
Functional Specification	administrator guidance	AGD_ADM, AVA_MSU
	secure installation, generation, and start-up procedures	ADO_IGS
	user guidance	AGD_USR, AVA_MSU
	parts of the delivery documentation	ADO_DEL
Vulnerability Assessment, Design Report	vulnerability assessment	AVA
	covert channel analysis	
	strength of function claims analysis	

Document containing or referring the relevant information	Input evidence according to CC Part 3, which is contained or referred to in the document	Input for assurance classes and families (according to developer actions in CC Part 3)
Test Documentation Roadmap, Verification Test, Characterisation Report, Electrical Test Specification	test documentation	ATE
	test coverage analysis	
	depth of testing analysis	

7. PP Claims

This Security Target claims conformance to the following Protection Profile:

Smartcard IC Platform Protection Profile, Version 1.0, July 2001; registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0002-2001, [7]

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

8. Rationale

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

8.1 Security Objectives Rationale

Section 7.1 of the Protection Profile provides a rationale how the assumptions, threats, and organisational security policies are addressed by the objectives that are subject of the PP “Smartcard IC Platform Protection Profile”. The following Table 14 reproduces the table in section 7.1 of [7].

Table 14. Security Objectives versus Assumptions, Threats or Policies

Assumption, Threat or OSP	Security Objective	Note
A.Plat-Appl	*OE.Plat-Appl*	*(Phase 1)* *Covered by O.Plat-Appl in the ST*
A.Resp-Appl	*OE.Resp-Appl*	*(Phase 1)* *Covered by O.Resp-Appl in the ST*
P.Process-TOE	OE.Process-TOE O.Identification	(Phase 2 – 3)
A.Process-Card	OE.Process-Card	(Phase 4 – 6)
T.Leak-Inherent	O.Leak-Inherent	
T.Phys-Probing	O.Phys-Probing	
T.Malfunction	O.Malfunction	
T.Phys-Manipulation	O.Phys-Manipulation	
T.Leak-Forced	O.Leak-Forced	
T.Abuse-Func	O.Abuse-Func	
T.RND	O.RND	

The following Table 15 provides the justification for the additional security objectives. They are in line with the security objectives of the Protection Profile and supplement these according to the additional threats and organisational security policies.

Table 15. Additional Security Objectives versus Threats or Policies

Threat/Policy	Security Objective	Note
A.Secure_Values	OE.Secure_Values	(Phase 5 – 6)
A.Terminal_Support	OE.Terminal_Support	(Phase 7)

Threat/Policy	Security Objective	Note
T.Data-Modification	O.Access-Control O.Type-Consistency OE.Terminal_Support	
T.Impersonate	O.Authentication	
T.Cloning	O.Access-Control O.Authentication	
P.Confidentiality	O.Confidentiality OE.Terminal_Support	
P.Transaction	O.Transaction	
P.No-Trace	O.No-Trace O.Access-Control O.Authentication	
P.Plat-Appl	O.Plat-Appl	Covers OE.Plat-Appl of the PP.
P.Resp-Appl	O.Resp-Appl	Covers OE.Resp-Appl of the PP.

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

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

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

Since OE.Secure_Values requires from the Administrator, Application Manager or the Application User to use secure values for the configuration of the authentication and access control as assumed in A.Secure_Values, the assumption is covered by the objective.

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

According to threat T.Data-Modification the TOE shall avoid that user data stored by the TOE may be modified by unauthorised subjects. The objective O.Access-Control requires an access control mechanism that limits the ability to modify data elements stored by the TOE. O.Type-Consistency ensures that data types are adhered, so that data can not be modified by abusing type-specific operations. The terminal must support this by checking the TOE responses, which is required by OE.Terminal_Support. Therefore T.Data-Modification is covered by these three objectives.

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

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

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

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

The concern of T.Cloning is that all data stored on the TOE (including keys) may be read out in order to create a duplicate. The objective O.Authentication together with O.Access-Control requires that unauthorised users can not read any information that is restricted to the authorised subjects. The cryptographic keys used for the authentication are stored inside the TOE protected O.Access-Control. This objective states that no keys used for authentication shall ever be output. Therefore the two objectives cover T.Cloning.

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

The policy P.Confidentiality requires the TOE to provide the possibility to protect selected data elements from eavesdropping during contact-less communication. In addition the data transfer is protected in a way that injected and bogus commands within the communication session before the protected data transfer can be detected. The terminal must support this by checking the TOE responses, which is required by OE.Terminal_Support. Since O.Confidentiality requires that the security attribute for a data element contains an option that the communication related to this data element must be encrypted and protected and because OE.Terminal_Support ensures the support by the terminal, the two objectives cover the policy.

The justification related to the policy “Transaction mechanism (P.Transaction)” is as follows:

According to this policy the TOE shall be able to 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. This is exactly the goal of the objective O.Transaction, therefore the policy P.Transaction is covered by O.Transaction.

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

The policy requires that the TOE has the ability to prevent tracing of end-users. Tracing can be performed with the UID or with any freely accessible data element stored by the TOE. The objective O.No-Trace requires that the TOE shall provide an option to prevent the transfer of any information that is suitable for tracing an end-user by an unauthorised subject, which includes the UID. The objectives O.Authentication and O.Access-Control provide means to authorise subjects and to implement access control to data elements in a way that unauthorised subjects can not read any element usable for tracing. Therefore the policy is covered by the three objectives.

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

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

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

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

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

8.2 Security Requirements Rationale

8.2.1 Rationale for the security functional requirements

Section 7.2 of the PP “Smartcard IC Platform Protection Profile” provides a rationale for the mapping between security functional requirements and security objectives defined in the Protection Profile. The mapping is reproduced in the following table. The mapping of the addional

Table 16. Security Requirements versus Security Objectives

Objective	TOE Security Functional Requirements	Security Requirements for the environment
O.Leak-Inherent	FDP_ITT.1 “Basic internal transfer protection” FPT_ITT.1 “Basic internal TSF data transfer protection” FDP_IFC.1 “Subset information flow control”	RE.Phase-1 “Design and Implementation of the Smartcard Embedded Software” *(refer to “Note regarding RE.Phase-1 below)*
O.Phys-Probing	FPT_PHP.3 “Resistance to physical attack”	RE.Phase-1 “Design and Implementation of the Smartcard Embedded Software” *(refer to “Note regarding RE.Phase-1” below)*
O.Malfunction	FRU_FLT.2 “Limited fault tolerance FPT_FLS.1 “Failure with preservation of secure state” FPT_SEP.1 “TSF domain separation”	
O.Phys-Manipulation	FPT_PHP.3 “Resistance to physical attack”	RE.Phase-1 “Design and Implementation of the Smartcard Embedded Software” (e.g. by implementing FDP_SDI.1 Stored data integrity monitoring) *(refer to "Note regarding RE.Phase-1” below)*
O.Leak-Forced	All requirements listed for O.Leak-Inherent FDP_ITT.1, FPT_ITT.1, FDP_IFC.1 plus those listed for O.Malfunction and O.Phys-Manipulation FRU_FLT.2, FPT_FLS.1, FPT_SEP.1,	RE.Phase-1 “Design and Implementation of the Smartcard Embedded Software” *(refer to "Note regarding RE.Phase-1” below)*

Objective	TOE Security Functional Requirements	Security Requirements for the environment
	FPT_PHP.3	
O.Abuse-Func	FMT_LIM.1 “Limited capabilities” FMT_LIM.2 “Limited availability” plus those for O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation, O.Leak-Forced FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_PHP.3, FRU_FLT.2, FPT_FLS.1, FPT_SEP.1	
O.Identification	FAU_SAS.1 “Audit storage”	
O.RND	FCS_RND.1 “Quality metric for random numbers” plus those for O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation, O.Leak-Forced FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_PHP.3, FRU_FLT.2, FPT_FLS.1, FPT_SEP.1	RE.Phase-1 “Design and Implementation of the Smartcard Embedded Software” (e.g. by implementing FPT_AMT.1 “Abstract machine testing”) *(refer to "Note regarding RE.Phase-1” below)*
OE.Plat-Appl		RE.Phase-1 “Design and Implementation of the Smartcard Embedded Software” *(refer to "Note regarding RE.Phase-1” below)*
OE.Resp-Appl		RE.Phase-1 “Design and Implementation of the Smartcard Embedded Software” *(refer to "Note regarding RE.Phase-1” below)*
OE.Process-TOE	FAU_SAS.1 “Audit storage”	Assurance Components: refer to below ✷
OE.Process-Card		RE.Process-Card possibly supported by RE.Phase-1 *(refer to "Note regarding RE.Phase-1” below)*

✷ Assurance Components: Delivery (ADO_DEL); Installation, generation, and start-up (ADO_IGS) (using Administrator Guidance (AGD_ADM), User guidance (AGD_USR)); CM automation (ACM_AUT); CM Capabilities (ACM_CAP); CM Scope (ACM_SCP); Development Security (ALC_DVS); Life Cycle Definition (ALC_LCD); Tools and Techniques (ALC_TAT)

Note regarding RE.Phase-1: The security requirement for the environment RE.Phase-1 is not longer part of the requirements due to the fact that the ST has transferred the environment objectives OE.Plat-Appl and OE.Resp-Appl into the TOE objectives O.Plat-Appl and O.Resp-Appl.

The Security Target additionally defines the SFRs for the TOE that are listed in Table 17. In addition Security Requirements for the Environment are defined. The following table gives an overview, how the requirements are combined to meet the security objectives.

Table 17. Mapping of security objectives and requirements

Objective	TOE Security Functional Requirement	Security Requirements for the environment
O.Access-Control	FMT_SMR.1 FDP_ACC.1 FDP_ACF.1 FMT_MSA.3 FMT_MSA.1 FMT_SMF.1 FDP_ITC.2 FCS_CKM.4 FMT_MTD.1	
O.Authentification	FCS_COP.1[DES] FCS_COP.1[AES] FIA_UID.2 FIA_UAU.2 FIA_UAU.5 FTP_TRP.1 FPT_RPL.1	
O.Confidentiality	FCS_COP.1[AES] FTP_TRP.1 FPT_RPL.1	
O.Type-Consistency	FPT_TDC.1	
O.Transaction	FDP_ROL.1	
O.No-Trace	FPR_UNL.1	
O.Plat-Appl	all SFR from the PP	
O.Resp-Appl	all SFR defined additionally in the ST	
OE.Secure_Values		FMT_MSA.2 is a security requirement that must be provided by the IT environment
OE.Terminal_Support		RE.Terminal_Support

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

The SFR FMT_SMR.1 defines the roles of the Access Control Policy. The SFR FDP_ACC.1 and FDP_ACF.1 define the rules and FMT_MSA.3 and FMT_MSA.1 the attributes that the access control is based on. FMT_MTD.1 provides the rules for the management of the authentication data. The management functions are defined by FMT_SMF.1. Since the TOE stores data on behalf of the authorised subjects import of user data with security attributes is defined by FDP_ITC.2. 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. an application is deleted). This is required by FCS_CKM.4. These nine SFR together provide an access control mechanism as required by the objective O.Access-Control.

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

The two SFR FCS_COP.1[DES] and FCS_COP.1[AES] require that the TOE provides the basic cryptographic algorithms that can be used to perform the authentication. The SFR FIA_UID.2, FIA_UAU.2 and FIA_UAU.5 together define that users must be identified and authenticated before any action. The ‘none’ authentication of FIA_UAU.5 also ensures that a specific subject is identified and authenticated before an explicit authentication request is sent to the TOE. FTP_TRP.1 requires a trusted communication path between the TOE and remote users, FTP_TRP.1.3 especially requires “authentication requests”. Together with FPT_RPL.1 which requires a replay detection for these authentication requests the seven SFR fulfil the objective O.Authentication.

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

The SFR FCS_COP.1[AES] requires that the TOE provides the basic cryptographic algorithm AES that can be used to protect the communication by encryption. FTP_TRP.1 requires a trusted communication path between the TOE and remote users, FTP_TRP.1.3 especially requires “confidentiality and/or data integrity verification for data transfers protected with AES and based on a setting in the file attributes”. Together with FPT_RPL.1 which requires replay detection for these data transfers the three SFR fulfil the objective O.Confidentiality.

The justification related to the security objective “Data type consistency” (O.Type-Consistency) is as follows:

The SFR FPT_TDC.1 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.

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

The SFR FDP_ROL.1 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.

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

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

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

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

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

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

The justification related to the security objective “Generation of secure values (OE.Secure_Values)” is as follows:

A.Secure_Values assumes that the Administrator, Application Manager or the Application User uses adequate measures to generate and configure the authentication and access control during personalisation and during the usage with secure values to prevent unauthorised subjects to successfully authenticate or gain unauthorised access to user data.

The justification related to the security objective “Terminal support to ensure integrity and confidentiality (OE.Terminal_Support)” is as follows:

The requirement RE.Terminal_Support is an immediate transformation of the objective OE.Terminal_Support, therefore it covers the objective.

8.2.2 Dependencies of security functional requirements

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

The following discussion demonstrates how the dependencies defined by Part 2 of the Common Criteria for the requirements specified in sections 5.1.1.2, 5.1.1.3 and 5.1.1.4 are satisfied.

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

Table 18. Dependencies of security functional requirements

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

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

The functional requirement FMT_MSA.2 is not included in this Security Target. FMT_MSA.2 requires that “The TSF shall ensure that only secure values are accepted for security attributes.” This is clearly out of scope for the TOE. The design concept of the TOE and the systems in which the TOE is used is based on the fact that the authorised users can protect their data stored by the TOE by using secret keys and a secure access configuration. Therefore the TOE can not ensure that the security attributes are secure, this is the primary responsibility of the authorised users. Note that FMT_MSA.2 is a dependency of the added security functional requirements for cryptographic operation (FCS_COP.1[DES], FCS_COP.1[AES] and FCS_CKM.4) and the cryptographic keys used by the TOE are considered as authentication data and not security attributes by the Common Criteria, however the argumentation does not change: secure keys must be used by the authorised users, therefore FMT_MSA.2 is a security requirement for the IT environment.

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

The selection of assurance components is based on the underlying Protection Profile [7]. The Security Target uses the same augmentations as the PP including the same assurance level

The rationale for the augmentations is the same as in the PP. The assurance level EAL4 is an elaborated pre-defined level of the CC, part 3 [3]. The assurance components in an EAL level are chosen in a way that they build a mutually supportive and complete set of components. The requirements chosen for augmentation do not add any dependencies, which are not already fulfilled for the corresponding requirements contained in EAL 4. Therefore, these components add additional assurance to EAL 4, but the mutual support of the requirements is still guaranteed.

As stated in the Protection Profile, section 7.2.3, it has to be assumed that attackers with high attack potential try to attack smart cards used for digital signature applications or payment systems. Therefore specifically AVA_VLA.4 was chosen by the PP in order to assure that even these attackers cannot successfully attack the TOE. For the same reason the Strength of Function level “high” is required.

Note that for the document “Smartcard Integrated Circuit Platform Augmentations” [8] as supposed by Application Note 21 was considered regarding assurance requirements, but no additional assurance requirements are proposed in the document.

8.2.4 Security Requirements are Mutually Supportive and Internally Consistent

The discussion of security functional requirements and assurance components in the preceding sections has shown that mutual support and consistency are given for both groups of requirements. The arguments given for the fact that the assurance components are adequate for the functionality of the TOE also 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 PP can be seen as “low-level protection” objectives, while the additional security objectives defined in this ST are “high-level protection” objectives. For example, O.Confidentiality states that the communication can be protected by encryption. While this ensures the rather high-level goal that the communication can not be eavesdropped, the overall goal that the communication is confidential is ensured with the help of the PP objective that prevent attacks on the key and the cryptographic implementation like probing or fault injection attacks.

8.3 TOE Summary Specification Rationale

8.3.1 Rationale for TOE security functions

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

Table 19. Mapping of Security Functional Requirements and the TOE Security Functions

	F.AUTH	F.ACC_CTRL	F.CONFID	F.TRANS	F.NO_TRACE	F.OPC	F.PHY	F.LOG	F.COMP
FAU_SAS.1									X
FCS_RND.1	X								
FDP_IFC.1								X	
FDP_ITT.1								X	
FMT_LIM.1									X
FMT_LIM.2									X
FPT_FLS.1						X			
FPT_ITT.1								X	
FPT_PHP.3							X		
FPT_SEP.1						X			X
FRU_FLT.2						X			
FMT_SMR.1	X	X							
FDP_ACC.1		X							
FDP_ACF.1		X							
FMT_MSA.1		X							
FMT_MSA.3		X							
FMT_SMF.1	X	X							
FDP_ITC.2		X							
FPT_TDC.1		X							
FCS_COP.1[DES]	X								
FCS_COP.1[AES]	X		X						
FIA_UID.2	X								
FIA_UAU.2	X								
FIA_UAU.5	X								

	F.AUTH	F.ACC_CTRL	F.CONFID	F.TRANS	F.NO_TRACE	F.OPC	F.PHY	F.LOG	F.COMP
FMT_MTD.1		X							
FTP_TRP.1	X		X						
FCS_CKM.4		X							
FDP_ROL.1				X					
FPT_RPL.1	X		X						
FPR_UNL.1					X				

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

8.3.2 Rationale for assurance measures

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

As already explained in the Protection Profile, annex 8.1, the development and production process of a smartcard IC is complex. Regarding the great number of assurance measures, a detailed mapping of the assurance measures to the assurance requirements is beyond the scope of this Security Target. Nevertheless the suitability of the assurance measures is subject of different evaluation tasks. The documents "Quality Management Manual" and "Security Management Manual" describe the general benchmark of NXP.

8.4 PP Claims Rationale

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

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

The evaluation assurance level claimed for this target (EAL4+) is shown in section 5.1.1.5 and is identical to the requirements claimed by the PP (EAL4+).

These considerations show that the Security Target correctly claims conformance to the Smartcard IC Platform Protection Profile, [7].

9. Annexes

9.1 Further Information contained in the PP

The Annex of the Protection Profile ([7], chapter 9) provides further information. Section 8.1 of the PP describes the development and production process of smartcards, containing a detailed life-cycle description and a description of the assets of the Integrated Circuits Designer/Manufacturer. Section 8.2 is concerned with security aspects of the Smartcard Embedded Software (further information regarding A.Resp-Appl and examples of specific Functional Requirements for the Smartcard Embedded Software). Section 8.3 gives examples of Attack Scenarios.

9.2 Glossary and Vocabulary

Note: To ease understanding of the used terms the glossary of the Protection Profile [7] is included here.

Administrator
The most powerful subject in the TOE usage scenario.

Card Manufacturer
The customer of the TOE Manufacturer who receives the TOE during TOE Delivery. The Card Manufacturer includes all roles after TOE Delivery up to Phase 7 (refer to [7], Figure 4 on page 17 and Section 8.1.1).

The Card Manufacturer has the following roles (i) the Smartcard Product Manufacturer (Phase 5) and (ii) the Personaliser (Phase 6). If the TOE is delivered after Phase 3 in form of wafers or sawn wafers (dice) he has the role of the IC Packaging Manufacturer (Phase 4) in addition.

Integrated Circuit (IC)
Electronic component(s) designed to perform processing and/or memory functions.

IC Dedicated Software
IC proprietary software embedded in a smartcard IC (also known as IC firmware) and developed by the IC Developer. Such software is required for testing purpose (IC Dedicated Test Software) but may provide additional services to facilitate usage of the hardware and/or to provide additional services (IC Dedicated Support Software).

IC Dedicated Support Software
Part of the IC Dedicated Software (refer to above) which provides functions after TOE Delivery. The usage of parts of the IC Dedicated Software might be restricted to certain phases.

IC Dedicated Test Software
Part of the IC Dedicated Software (refer to above) which is used to test the TOE before TOE Delivery but which does not provide any functionality thereafter.

Initialisation Data
Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 3). These data are for

instance used for traceability and for TOE identification (identification data).

MAC

Message Authentication Code

Memory

The memory comprises of the RAM, ROM and the EEPROM of the TOE.

MIFARE

Contact-less smart card interface standard, complying with ISO14443A.

Security Row

First 64 bytes of the EEPROM memory reserved for configuration purposes and to store life-cycle information about the TOE.

Smartcard

As used in the Protection Profile [7]: Composition of the TOE, the Smartcard Embedded Software, User Data and the package (the smartcard carrier). Note that within this ST “smartcard” refers to the TOE as a combination of hardware and software (in contrast to the focus of the PP the TOE includes Smartcard Embedded Software).

Smartcard Embedded Software

As used in the Protection Profile [7]: Software embedded in a smartcard IC and not being developed by the IC Designer. The Smartcard Embedded Software is designed in Phase 1 and embedded into the Smartcard IC in Phase 3 or in later phases of the smartcard product life-cycle.

As used in this Security Target: In this evaluation the TOE consist of an IC *and* Smartcard Embedded Software.

Special Function Registers

Registers used to access and configure the functions for the communication with an external interface device, the cryptographic co-processors or other functional blocks.

Test Features

All features and functions (implemented by the IC Dedicated Test Software and/or hardware) which are designed to be used before TOE Delivery only and delivered as part of the TOE.

Test Mode

CPU mode for configuration of the TOE executing the IC Dedicated Test Software. The Test Mode is permanently and irreversible disabled after production testing.

TOE Delivery

The period when the TOE is delivered which is (refer to [7], Figure 4 on page 17) either (i) after Phase 3 (or before Phase 4) if the TOE is delivered in form of wafers or sawn wafers (dice) or (ii) after Phase 4 (or

	before Phase 5) if the TOE is delivered in form of modules.
TOE Manufacturer	The TOE Manufacturer must ensure that all requirements for the TOE and its development and production environment are fulfilled (refer to [7], Figure 4 on page 17). The TOE Manufacturer has the following roles: (i) IC Developer (Phase 2) and (ii) IC Manufacturer (Phase 3). If the TOE is delivered after Phase 4 in form of modules, he has the role of the (iii) IC Packaging Manufacturer (Phase 4) in addition.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE (for example configuration data). Note that the TOE is the Smartcard IC.
User Data	All data managed by the Smartcard Embedded Software in the application context. User data comprise all data in the final TOE except the TSF data.

9.3 List of Abbreviations

AES	Advanced Encryption Standard
CC	Common Criteria (Version 2.3 in this ST).
CIU	Contact-less Interface Unit
CPU	Central Processing Unit
DEA	Data Encryption Algorithm.
DES	Data Encryption Standard.
EAL	Evaluation Assurance Level.
IC	Integrated circuit.
IT	Information Technology.
PP	Protection Profile.
SAR	Security Assurance Requirement.
SFP	Security Function Policy.
SFR	Security Functional Requirement.
SOF	Strength of function.
ST	Security Target.
TOE	Target of Evaluation.
TRNG	True Random Number Generator

TSC	TSF Scope of Control.
TSF	TOE Security functions.
TSFI	TSF Interface.
TSP	TOE Security Policy.

9.4 Bibliography

9.4.1 Evaluation Documents

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 2.3, August 2005, CCMB-2005-08-001

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 2.3, August 2005, CCMB-2005-08-002

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security Assurance Requirements, Version 2.3, August 2005, CCMB-2005-08-003

[4] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 2.3, August 2005, CCMB-2005-08-004

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

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

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

[8] Smartcard Integrated Circuit Platform Augmentations, Version 1.00, March 8th, 2002

9.4.2 Developer Documents

[9] MIFARE DESFire EV1 MF3ICD81 Functional Specification, NXP Semiconductors

[10] MIFARE DESFire EV1 MF3ICD81 Guidance, Delivery and Operation Manual , Application Note, NXP Semiconductors

9.4.3 Other Documents

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

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

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

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

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

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

10. Legal information

10.1 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.

10.2 Disclaimers

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

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

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

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

10.3 Trademarks

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

FabKey — is a trademark of NXP B.V.
Mifare — is a trademark of NXP B.V.

11. Contents

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

Date of release: 10 May 2011