AN11004

MIFARE DESFire as Type 4 Tag

Rev. 2.4 — 22 May 2013
130224

Application note
COMPANY PUBLIC

Document information

Info	Content
Keywords	NFC Forum, NFC Forum data mapping, NFC Forum Type 4 Tag Operation version 2.0, Type 4 Tag version 2.0, MIFARE DESFire EV1, NDEF Tag Application
Abstract	The NFC Forum is a standardization consortium that was formed to advance the use of Near Field Communication technology by developing specifications, ensuring interoperability among devices and services, and educating the market about NFC technology. The NFC Forum has defined a data format called NDEF to store different kind of application data. NDEF structured data may be stored inside contactless tag. In the NFC Forum the “NFC Forum Type 4 Tag Operation” version 2.0 technical specification has been developed to describe how the reader device (called NFC Forum device) can store NDEF data inside an NFC Forum Type 4 Tag platform. The NXP product MIFARE DESFire EV1 is compatible with the “NFC Forum Type 4 Tag Operation” version 2.0 technical specification and the Type 4 Tag platform. This document extends the information and the functionalities about how the NFC Forum device manages the MIFARE DESFire EV1 product as an NFC Forum Type 4 Tag platform.

Revision history

Rev	Date	Description
2.4	20130522	Changed MLe value from 003Bh to 003Ah
2.3	20120823	Section 8.2 added
2.2	20120104	Corrected File-ID and key settings Step 2 in section 8.1. Updated step 1 of section 6.4.1, 6.4.2, 6.4.6 and 6.4.7. Added note to step 3.a of section 6.5.1.
2.1	20110321	Security status changed into public, rephrased and corrected section 6.2, rephrased and corrected section 6.5.1, removed authentication from section 8.1, removed section 8.2,
2.0	20101210	Updated with MIFARE DESFire EV1
1.1	20070821	Updated examples to correct typing errors, corrected and rephrased some text element, added figures, rewording of chapter 2 and 3, added “Additional Features” chapter 7
1.0	20061016	Final revision
0.1	20060714	First draft version

Contact information

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

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

1. Introduction

The NFC technology allows to access standard ISO 14443A card products as the MIFARE family. A specification to store data for any kind of service and application is currently specified in the NFC Forum and it is called NFC Data Exchange Format (see [NDEF]). To store NDEF formatted data (or also called NDEF data or NFC Forum data) inside current contactless card products a mapping model is required. The specification [NFCT4TV2] describes this mapping model and how the NFC Forum device manages a NFC Forum Type 4 Tag platform to store NFC Forum defined data.

The MIFARE DESFire EV1 card IC product (see [MFDESEV1]) is a contactless card currently available with 8Kbyte, 4Kbyte and 2Kbyte of EEPROM memory. The MIFARE DESFire EV1 supports high data rates of up to 848 kBit/s, a flexible file system with different file and access types including data integrity checks and encryption options as some of the main features. It supports an ISO/IEC 7816-4 compliant command (APDU, see [ISOIEC 7816-4]) handling of the native MIFARE DESFire EV1 command as well as some ISO/IEC 7816-4 defined APDU like SELECT FILE, READ BINARY and UPDATE BINARY.

This document specifies:

- how to identify a MIFARE DESFire EV1 card IC,
- how to format a MIFARE DESFire EV1 card IC as NFC Forum Type 4 Tag,
- how to use a MIFARE DESFire EV1 card IC as NFC Forum Type 4 Tag, and
- how to manage and exploit the additional features of the MIFARE DESFire EV1 card IC when operating as NFC Forum Type 4 Tag.

1.1 Implementation Guidelines

Implementers MAY decide to NOT implement all the possible features (procedures, states…) that this document specifies, but only the recommended ones that are needed to support [NFCT4TV2] using MIFARE DESFire EV1 card, and the ones required by implementers themselves or customer requirements.

It is RECOMMENDED to implement at least the features below to support [NFCT4TV2] using MIFARE DESFire EV1 card:

- the memory layout, and the relative card identification procedure, see chapter 2,
- the command set described in chapter 5,
- the basic states: INITIALISED, READ/WRITE, READ-ONLY, see chapter 6,
- the transitions from READ/WRITE to READ-ONLY, see section 6.4, and
- the formatting procedures, see section 6.5.

1.2 Applicable Documents

[ISOIEC 14443-3]	ISO/IEC14443-3 Type A Identification Cards- Contactless Integrated circuit(s) cards- Proximity Cards- Part 3: Initialization and Anticollision
[ISOIEC 7816-4]	ISO/IEC 7816-4 Identification cards - Integrated circuit cards - Organization, security and commands for interchange.
[NDEF]	“NFC Data Exchange Format (NDEF)” NFC Forum™, Technical Specification, May 2006.

[RFC2119] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, Harvard University, March 1997.

[MFDESEV1] “MF3ICD81 MIFARE DESFire”, NXP Semiconductors, ID 1340xx, Product Data Sheet.

[NFCT4TV2] “NFC Forum Type 4 Tag Operation”, NFC Forum™, version 2.0, Technical Specification, 2010.

1.3 Convention and notations

1.3.1 Representation of numbers

The following conventions and notations apply in this document unless otherwise stated.

Binary numbers are represented by strings of digits 0 and 1 shown with the most significant bit (msb) left and the least significant bit (lsb) right, “b” is added at the end.

Example: 11110101b

Hexadecimal numbers are represented is using the numbers 0 - 9 and the characters A – F, an “h” is added at the end. The Most Significant Byte (MSB) is shown on the left, the Least Significant Byte (LSB) on the right.

Example: F5h

Decimal numbers are represented as is (without any tailing character).

Example: 245

1.3.2 Terms and Definition

According to the NDEF specification, data is represented in Network Byte Order (i.e. big endian). This means Most Significant Byte first and most significant bit first (MSB first, msb first).

Please note that the MIFARE DESFire EV1 is using the LSB first notations for APDU communication.

1.4 Special Word Usage

The key words "SHALL", "SHALL NOT", "REQUIRED", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are used to signify the requirements in this document.

SHALL, and REQUIRED have the same meaning. SHOULD and RECOMMENDED have the same meaning. MAY and OPTIONAL mean also the same. The key words are interpreted as described in [RFC2119].

1.5 Acronyms or Definitions or Glossary

Table 1. Terms and definitions

Term	Definition
3DES	Triple Data Encryption Standard
APDU	Application Protocol Data Unit, see [ISOIEC 7816-4]
card	A MIFARE DESFire EV1 contactless card, see [MFDESEV1]
CC	Capability Container, the CC stores control data for managing the

Term	Definition
	NFC Forum defined data inside the tag
ComSet	Common Settings, see [MFDESEV1]
DES	Data Encryption Standard
DESFire AID	DESFire Application IDentifier
DESFire FID	DESFire File IDentifier
EF	Elementary File, see [ISOIEC 7816-4]
FID	File IDentifier
FileNo	File Number
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization, see: www.nxp.com/redirect/iso
ISO FID	ISO File IDentifier
lsb	least significant bit
LSB	Least Significant Byte
mandatory NDEF File	The mandatory NDEF File is the NDEF File indicated in the mandatory NDEF Message Control TLV present at the offset 0007h of the CC File.
ML_c	Maximum data Length C-APDU, see [NFCT4TV2]
ML_e	Maximum data Length R-APDU, see [NFCT4TV2]
msb	most significant bit
MSB	Most Significant Byte
NDEF	NFC Data Exchange Format, see [NDEF]
NDEF File	EF that contains the NDEF data
NDEF File Control TLV	TLV block that contains control information of the NDEF File
NDEF Message	Data packet structured as specified by [NDEF]
NFC	Near Field Communication
NFC Forum	Standardization body, see www.nxp.com/redirect/nfc-forum
NDEF Tag Application	Application stored inside the tag that contains NFC Forum defined data
NFC Forum device	Reader device compliant to the NFC Forum that may partially implements this application note as well.
NLEN	NDEF length, length of the NDEF Message
PICC	Proximity Card according to the ISO/IEC 14443. The MIFARE

Term	Definition
	DESFire EV1 contactless card
Proprietary File	EF that contains the proprietary data
Proprietary File Control TLV	TLV block that contains control information of the Proprietary File
Reader	NFC Forum device that is able to operate a MIFARE DESFire EV1 card
RFU	Reserved for Future Use
SAK	Selective Acknowledge, see [ISOIEC 14443-3]
tag	A MIFARE DESFire EV1 contactless card, see [MFDESEV1]
TLV	Type Length Value block, data structure element to store different kind of data.
Type 4 Tag	Tag defined in the NFC Forum technical specification [NFCT4TV2] related to the MIFARE DESFire EV1 contactless card
UID	Unique IDentifier, also called serial number in the [MFUL] specification
UID0	Byte 0 of the Unique IDentifier

2. Memory Layout

The MIFARE DESFire EV1 memory layout is organized using a flexible file structure. Different applications and files of different sizes MAY be created on it.

The MIFARE DESFire EV1 is used as a container to store the NDEF data (see [NDEF]).

2.1 Mapping of NFC Forum data using MIFARE DESFire EV1 card ICs

The mapping of NFC Forum data (e.g. NDEF Message) inside MIFARE DESFire EV1 SHALL be done creating a specific application called NDEF Tag Application.

The NDEF Tag Application SHALL contain the following files:

1. one NDEF File, and
2. one capability container (CC) file with ISO file identifier (ISO FID) equal to E103h,

The NDEF Tag Application MAY contain:

1. two or more NDEF Files,
2. zero, one or more Proprietary Files, and

The files described above SHALL be standard data files of the MIFARE DESFire EV1 (see [MFDESEV1]). The files SHALL be created to fit at least the size of the CC and the size of the NDEF data to be written into it. For more information about CC File and the relative NDEF File (see [NFCT4TV2]).

In this specification the mandatory NDEF File is the NDEF File indicated in the mandatory NDEF Message Control TLV present at the offset 0007h of the CC File.

2.2 Card Identification Procedure

The card identification procedure is a set of commands and responses sent by the NFC Forum device to check if the counterpart contactless tag is a MIFARE DESFire EV1 and if the MIFARE DESFire EV1 contains the NDEF Tag Application (see [NFCT4TV2]).

To perform the card identification procedure, the NFC Forum device SHALL (see also Fig 1):

1. Check the bit values (using ISO notation, this notation counts from 1 (lsb) to 8 (msb) the bits inside a byte, for more information see [ISOIEC 14443]) in the Selective Acknowledge (SAK, see [ISOIEC 14443-3]) are set as below:
   a. bit 2 is equal to 0b, and
   b. bit 4 is equal to 0b, and
   c. bit 5 is equal to 0b, and
   d. bit 6 is equal to 1b
2. send successfully the RATS Command
3. send successfully using the “Wrapping of Native DESFire APDUs“ (see section 9.7.4 of [MFDESEV1]) the MIFARE DESFire EV1 GetVersion command (see section 5.2 and section 8.2) retrieving from the command response the version and the memory size of the MIFARE DESFire EV1 (see bold characters below).
   a. If the received data is the following, the card is the DESFire EV1 with 2 Kbytes
      Software Major Version bigger or equal to 0x01
      Software Storage Size exactly 2048 Byte
   b. If the received data is the following, the card is the DESFire EV1 with 4 Kbytes
      Software Major Version bigger or equal to 0x01

Software Storage Size exactly 4096 Byte

c. If the received data is the following, the card is the DESFire EV1 with 8 Kbytes
Software Major Version bigger or equal to 0x01
Software Storage Size exactly 8192 bytes

If all previous steps are done successfully the tag is a MIFARE DESFire EV1.

To check if the MIFARE DESFire EV1 contains the NDEF Tag Application, the NFC Forum device SHALL execute the NDEF Detection Procedure (see section 6.4.1 in [NFCT4TV2]):

1. if the NDEF Detection Procedure returns successfully, then the MIFARE DESFire EV1 contains the NDEF Tag Application compliant with Type 4 Tag Version 2.0.
2. If the NDEF Detection Procedure does not return successfully, then the MIFARE DESFire EV1 does not contain the NDEF Tag Application. The Formatting Procedures (see section 6.5) MAY be used.

The overall memory size of the MIFARE DESFire EV1 retrieved using the MIFARE DESFire EV1 GetVersion command card SHALL be used by the NFC Forum device to create the files in the NDEF Tag Application taking into account possible additional MIFARE DESFire EV1 applications and relative files.

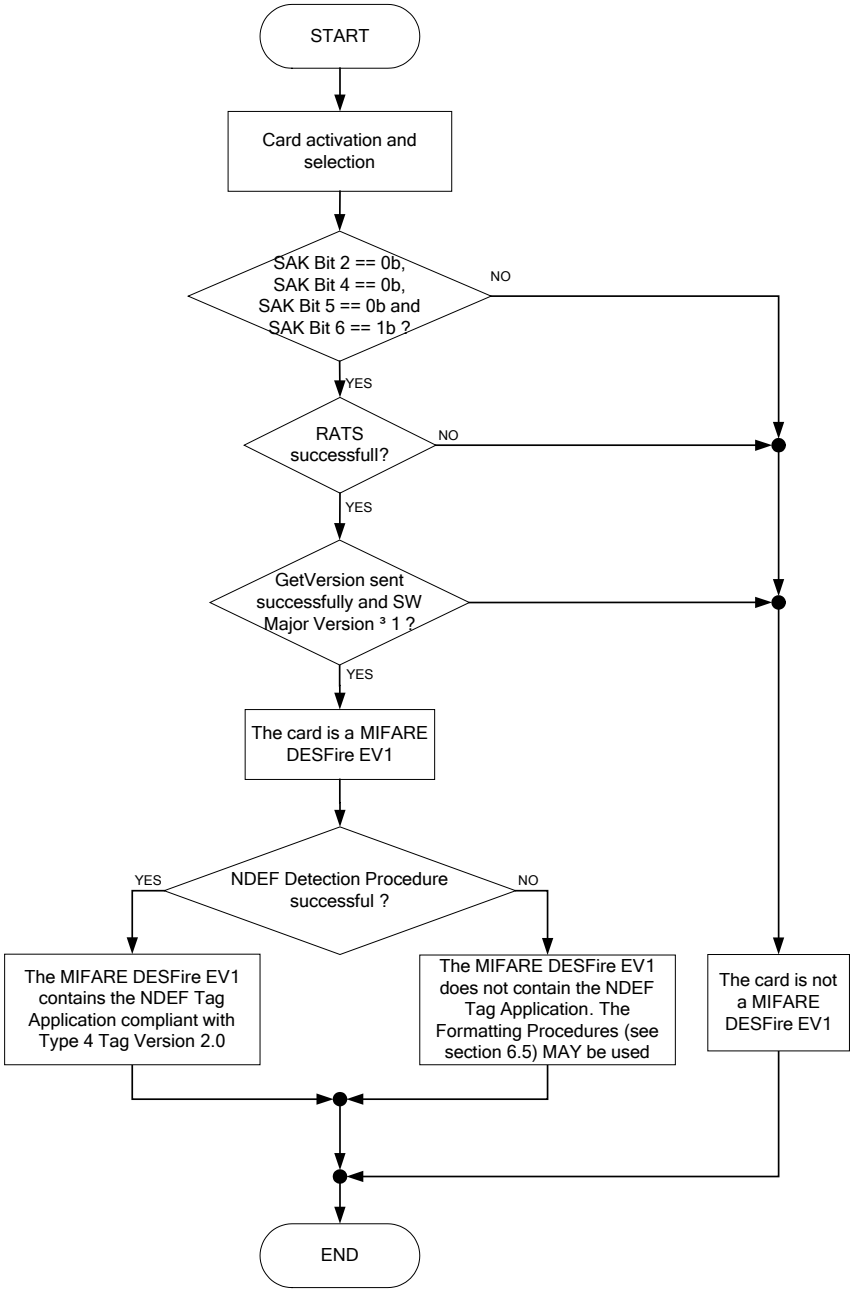

Fig 1. DESFire EV1 Card Identification Procedure

3. Read/Write Access

A MIFARE DESFire EV1 has different access conditions for accessing (for more information see [MFDESEV1]):

- the MIFARE DESFire EV1 (PICC) itself,
- the applications, and
- the files of each application.

It is RECOMMENDED that the PICC master key and the application master key of the NDEF Tag Application are kept secret to avoid (see [MFDESEV1]):

- formatting of MIFARE DESFire EV1 (PICC),
- creation/deletion of applications,
- change of the PICC/application master key settings,
- creation/deletion of files, and
- change of the file access rights.

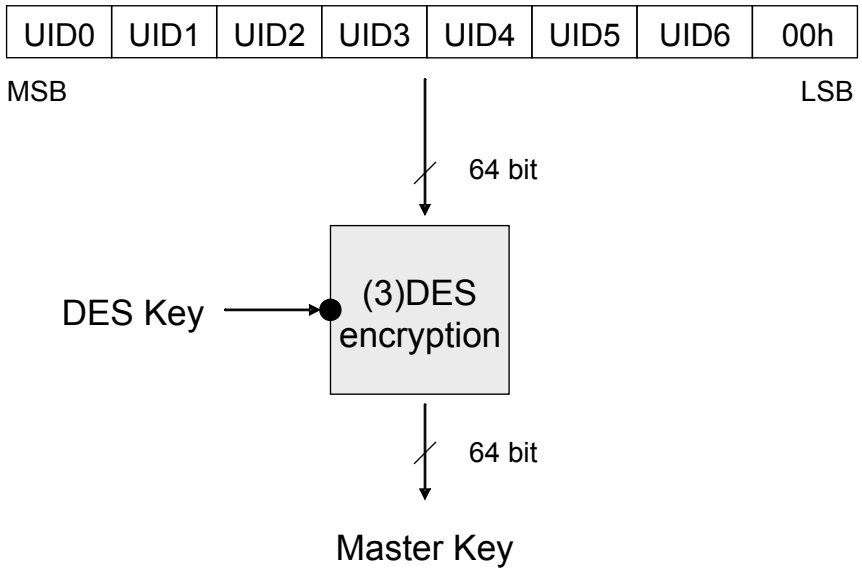

Fig 2. Example key diversification based on UID and DES or 3DES algorithm

To improve the security the key diversification based on the unique identifier (UID) MAY be applied for PICC master key and/or application master key. The example in Fig 2 shows how the DES or 3DES algorithm MAY be applied for the key diversification to generate different master key (PICC or application master key per each MIFARE DESFire EV1 card) based on the UID and the DES encryption key.

4. Framing / Transmission Handling

The framing and the transmission handling for MIFARE DESFire EV1 is specified in [NFCT4TV2].

5. Command Set

The command set described in this chapter SHALL be used to personalize the MIFARE DESFire EV1 as an NFC Forum Type 4 Tag (see [NFCT4TV2]).

The command set is based on ISO/IEC 7816-4 compliant APDUs (see section 5.1) and it is divided into two groups (see next two sections). The section 5.3 highlights the relationship between the different File ID notations and codings.

5.1 NFC Forum Command Set

The NFC Forum command set is a subset of the ISO APDU commands defined in [ISOIEC 7816-4]. The following commands have to be supported in order to read from or write to MIFARE DESFire EV1 the NFC Forum defined data (see [MFDESEV1]). These commands are also specified in the NFC Forum specification [NFCT4TV2].

- ISO/IEC 7816-4 UPDATE BINARY
- ISO/IEC 7816-4 READ BINARY
- ISO/IEC 7816-4 SELECT FILE

The following Application Note uses also the “Wrapping of Native DESFire APDUs“ (see section 9.7.4 of [MFDESEV1]). The message structure is used to encapsulate MIFARE DESFire EV1 native command into the ISO APDU command structure (see section 5.2).

5.2 MIFARE DESFire EV1 native command Set

MIFARE DESFire EV1 supports a native command set (see [MFDESEV1]). The native commands SHALL be sent encapsulated inside the “Wrapping of Native DESFire APDUs“ (see section 9.7.4 of [MFDESEV1]).

The following native commands are used in this document:

- MIFARE DESFire GetVersion
- MIFARE DESFire CreateApplication
- MIFARE DESFire CreateStdDataFile
- MIFARE DESFire ChangeFileSettings
- MIFARE DESFire Authenticate
- MIFARE DESFire ChangeKey
- MIFARE DESFire ChangeKeySettings
- MIFARE DESFire FormatPICC

Following commands MAY also be used:

- MIFARE DESFire WriteData
- MIFARE DESFire ReadData
- MIFARE DESFire SelectApplication

5.3 File Identifier Coding and Notation

The MIFARE DESFire EV1 native command set and the NFC Forum command set have different coding for the File Identifier and the Application Identifier. MIFARE DESFire EV1 native command set uses the MIFARE DESFire file identifier (DESFire FID or DESFire File ID) and the MIFARE DESFire application identifier (DESFire AID). Instead the NFC

Forum command set uses the ISO File Identifier (ISO FID or File ID), and ISO Application Identifier (ISO AID or Application ID).

In the following chapters the DESFire FID and the ISO FID may be named only FID omitting the DESFire and the ISO prefix. It is clear from the context which type of FID it is referred to.

[MFDESEV1] calls FileNo the DESFire FID when it is used as parameter in MIFARE DESFire native command.

6. Life Cycle

The NDEF Tag Application can be in different states of a so called life cycle. The state is reflected by the content and configuration settings of the NDEF Tag Application. The NDEF Tag Application SHALL be only in one state in turn i.e. the NDEF Tag Application cannot be in two different states at the same time.

The state of the NDEF Tag Application is also called: MIFARE DESFire state (in particular when the NDEF Tag Application is the only application of the DESFire tag) or Type 4 Tag platform state in the [NFCT4TV2] technical specification.

Each state has its own valid operations called transitions. An entry is a set of operations to prepare a MIFARE DESFire that does not contain the NDEF Tag Application into a specific state. The entries are also called formatting procedures (see section 6.5).

In this document two life cycles are presented:

- *The NFC Forum life cycle.* This life cycle shows the life cycle specified by [NFCT4TV2]. The transitions of the life cycle SHALL be implemented in the NFC Forum device to manage Type 4 Tag. MIFARE DESFire is fully compliant with the NFC Forum life cycle.
- *The MIFARE DESFire life cycle.* This life cycle shows the life cycle specified by the NFC Forum together with additional states, entries and transitions that make use of specific MIFARE DESFire features. The entries, the transitions and the states MAY be partially supported by an NFC Forum device according to specific requirements that are not covered by the NFC Forum technical specification [NFCT4TV2].

6.1 NFC Forum Life Cycle

The specification [NFCT4TV2] describes the life cycle from the NFC Forum perspective as a combination of states, transition and entries. To carry out the transition, the [NFCT4TV2] specifies the NFC Forum command set (see section 5.1)

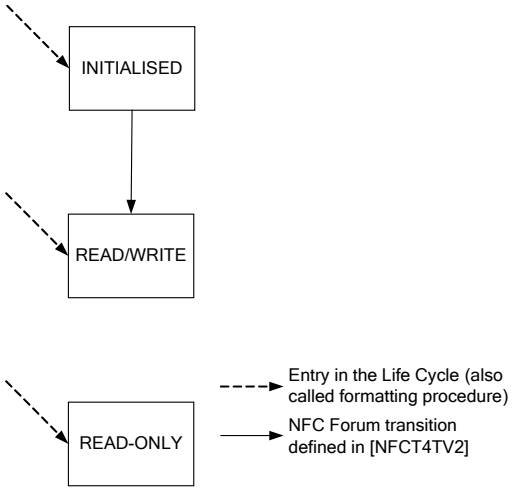

Fig 3. NFC Forum Life Cycle

Fig 3 describes this life cycle defined in the NFC Forum for the Type 4 Tag platform. The three entries, one for each state, are briefly presented in the [NFCT4TV2]. The entries, also called formatting procedures, are described in details in section 6.5.

The states of the NFC Forum life cycle are called Type 4 Tag platform state.

6.2 MIFARE DESFire Life Cycle

The MIFARE DESFire MAY be in additional states than that one specified in the [NFCT4TV2]. These additional states together with entries and additional transitions create the MIFARE DESFire life cycle (see Fig 4). The states of the MIFARE DESFire life cycle are called MIFARE DESFire state.

The additional states are named in Fig 4 using the prefix “DESFire” being MIFARE DESFire specific. A rounded square indicates parts of the MIFARE DESFire life cycle that corresponds to the NFC Forum life cycle.

To guarantee compatibility with [NFCT4TV2], the DESFire READ/WRITE state and DESFire READ-ONLY state are seeing from a NFC Forum device that implements only [NFCT4TV2] respectively as READ/WRITE state and READ-ONLY state. Table 2 shows these relations between the Type 4 Tag platform states and the MIFARE DESFire state.

Table 2. Relation between the Type 4 Tag platform states and the MIFARE DESFire states

Type 4 Tag platform states detected by an NFC Forum device implementing only the [NFCT4TV2] technical specification	MIFARE DESFire state
INITIALISED	INITIALISED
READ/WRITE	READ/WRITE
	DESFire READ/WRITE
READ-ONLY	READ-ONLY
	DESFire READ-ONLY

In Fig 4 the dotted arrows indicate the additional transitions. To carry out the additional transitions, MIFARE DESFire native commands need to be used (see section 5.2).

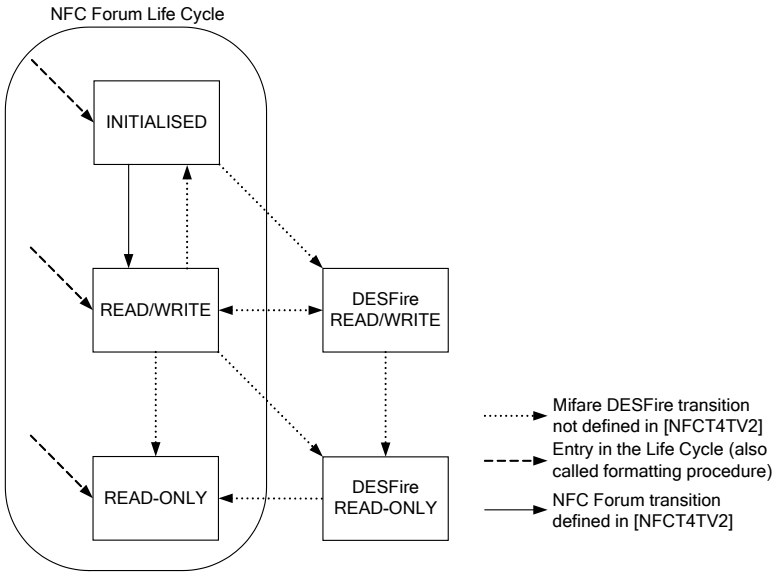

Fig 4. MIFARE DESFire Life Cycle

Overall in the MIFARE DESFire Life Cycle there are 5 states, 3 entries/formatting procedures and 8 transitions. It is not compulsory the support of all states, entries and transitions in the NFC Forum device. An implementation MAY be tailored to support a subset of states, entries and transitions.

During any formatting procedure or transition the MIFARE DESFire needs to be hold close to the NFC Forum device to be continuously powered. This can be communicated to the user e.g. showing a message on the user interface. It is up to the implementers to design the recovery mechanisms in case of interruption or error during a formatting procedure or a transition.

The differences between the states are based on different parameters: the CC File access settings, the mandatory NDEF File access settings, the NLEN field value of the mandatory NDEF File, the non-mandatory NDEF File access settings and the Proprietary File access settings. Table 3 summarizes the different states highlighting the differences between them (see also [MFDESEV1]). A more comprehensive description of the MIFARE DESFire states is given in section 6.3.

The states in Table 3 and section 6.3 have the following common settings (see [MFDESEV1]):

- PICC master key Settings SHALL be set to (see [MFDESEV1]):
  - Successful PICC master key authentication is needed to execute the commands CreateApplication and DeleteApplication, and
  - the execution of the commands GetApplicationIDs and GetKeySettings is allowed.
- NDEF Tag Application master Key Settings SHALL be set to (see [MFDESEV1]):
  - Successful application master key authentication is needed to execute the CreateFile and DeleteFile commands, and
  - Successful application master key authentication is needed to execute the GetFileIDs, GetFileSettings and GetKeySettings commands.

Table 3. Comparative table between the different states

STATE	CC File access rights[2] / Communication mode[3]	NDEF File write access condition field of the mandatory NDEF File Control TLV	Mandatory NDEF File access rights / Communication mode	NLEN field value of the mandatory NDEF File	Read access condition field of the non-mandatory NDEF and Proprietary File Control TLV(s)	Write access condition field of the non-mandatory NDEF and Proprietary File Control TLV(s)	Non-mandatory NDEF File and Proprietary file access rights[2] / Communication mode[3]
INITIALISED	E000h / Plain	00h	EEE0h / Plain	0000h	00h	00h	EEE0h / Plain
READ/WRITE	E000h / Plain	00h	EEE0h / Plain	≠ 0000h	00h	00h	EEE0h / Plain
DESFire READ/WRITE	E000h / Plain	00h	EEE0h / Plain	≠ 0000h	00h-FFh	00h-FFh	Any[1]
READ-ONLY	EFFFh / Plain	FFh	EFFFh / Plain	≠ 0000h	00h	FFh	EFFFh / Plain
DESFire READ-ONLY	E000h / Plain	FFh	EFFFh / Plain	≠ 0000h	00h-FFh	00h-FFh	Any[1]

[1] "Any" means:
- the file access values of the non-mandatory NDEF Files and Proprietary Files MAY be any value defined by [MFDESEV1], and
- the communication mode MAY be anyone defined by [MFDESEV1]
- at least one file between the non-mandatory NDEF File and the Proprietary File SHALL have file access or communication mode or both different from EEE0h / Plain.

[2] Concerning more information about the access rights, see section 8.3 in [MFDESEV1]

[3] Concerning more information about the communication mode, see section 8.2 in [MFDESEV1]

In [NFCT4TV2] the states INITIALISED, READ/WRITE and READ/ONLY are identified using the CC File (this is done checking the NDEF File write access condition field of the NDEF File Control TLV that is located at the offset 0007h of the CC File) and the NLEN filed value of the mandatory NDEF File. However the NFC Forum device that implements either the DESFire READ/WRITE state or the DESFire READ/ONLY state or both SHALL identify the states using the following parameters: the NLEN field value of the mandatory NDEF File, and both the settings of the file access rights and the communication mode of each Proprietary File and each NDEF File (see [MFDESEV1]). The NDEF File write access condition field of the NDEF File Control TLV that is located at the offset 0007h (called mandatory NDEF File Control TLV, see [NFCT4TV2]) of the CC File is overridden by the previous parameters.

The addition and/or deletion of non-mandatory NDEF Files, and Proprietary Files MAY be performed in any transition, and in any state except the READ-ONLY state. These operation MAY change the state of the MIFARE DESFire.

6.2.1 Read/Write Access Condition Field Settings Of The NDEF and Proprietary File Control TLV

The read and write access condition filed of the NDEF and Proprietary File Control TLVs SHALL be set as described in the following sub-sections.

A reader device SHALL ignore the Read Access Condition field of the NDEF and Proprietary File Control TLV, when writing the relative NDEF or Proprietary File.

A reader device SHALL ignore the Write Access Condition field of the NDEF and Proprietary File Control TLV, when reading the relative NDEF or Proprietary File.

6.2.1.1 The Write Access Condition Field Settings Of The Mandatory NDEF File Control TLV

The write access condition field of the mandatory NDEF File Control TLV SHALL be set following Table 3.

6.2.1.2 The Read Access Condition Field Settings Of The Mandatory NDEF File Control TLV

The read access condition field of the mandatory NDEF File Control TLV SHALL be set always to 00h.

6.2.1.3 The Write Access Condition Field Settings Of The Non-mandatory NDEF And Proprietary File Control TLVs

The write access condition field of the non-mandatory NDEF and Proprietary File Control TLVs SHALL be set according to the DESFire coding of the access right (see section 8.3 of [MFDESEV1]) following the rules below (see also Table 3):

- If the write access of the non-mandatory NDEF or Proprietary File is set to “free” i.e. “Write Access” and “Read&Write Access” values are equal to Eh (see section 8.3 of [MFDESEV1]), the value of the write access condition field of the NDEF/Proprietary File Control TLV is set to 00h.
- If the write access of the non-mandatory NDEF or Proprietary File is set to “deny” i.e. “Write Access” and “Read&Write Access” values are equal to Fh (see section 8.3 of [MFDESEV1]), the value of the write access condition field of the NDEF/Proprietary File Control TLV is set to FFh.
- If the write access of the non-mandatory NDEF or Proprietary File is not set to “free” or “deny” i.e. “Write Access” and/or “Read&Write Access” values are different from Eh and Fh (see section 8.3 of [MFDESEV1]), the value of the write access condition field of the NDEF/Proprietary File Control TLV is set as described below in order from the msb to the lsb (see Fig 5):
  - the first field (1 bit long, msb) SHALL be always set to 1b,
  - the RFU field (1 bit long) SHALL be RFU and set to 0b,
  - the CommMode field (2 bits) SHALL indicate the communication mode as described in Table 4 (see section 8.2 in [MFDESEV1]), and
  - the Key# field (4 bits) SHOULD indicate the key number of the “Write Access” (see [MFDESEV1]). Key# equal to Eh and Fh are RFU. It is RECOMMENDED that the “Read&Write Access” (see section 8.3 of [MFDESEV1]) of all non-mandatory NDEF or Proprietary File is set to “deny” i.e. Fh.

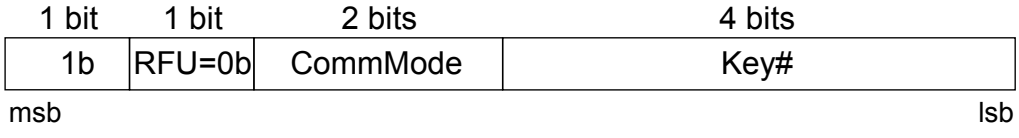

Fig 5. Write access condition field settings

Table 4. CommMode value

MIFARE DESFire Communication Mode	CommMode value
Plain	00h
Plain communication secured by DES/3K3DES/AES MACing	01h
RFU	10h
Fully DES/3DES/3K3DES/AES enciphered communication	11h

6.2.1.4 The Read Access Condition Field Settings Of The Non-mandatory NDEF And Proprietary File Control TLVs

The read access condition field of the non-mandatory NDEF and Proprietary File Control TLVs SHALL be set according to the DESFire coding of the access rights as described below in order from the msb to the lsb (see section 8.3 of [MFDESEV1]):

- If the read access of the non-mandatory NDEF or Proprietary File is set to “free” i.e. “Read Access” and “Read&Write Access” values are equal to Eh (see section 8.3 of [MFDESEV1]), the value of the read access condition field of the NDEF/Proprietary File Control TLV is set to 00h.
- If the read access of the non-mandatory NDEF or Proprietary File is set to “deny” i.e. “Read Access” and “Read&Write Access” values are equal to Fh (see section 8.3 of [MFDESEV1]), the value of the read access condition field of the NDEF/Proprietary File Control TLV is set to FFh.
- If the read access of the non-mandatory NDEF or Proprietary File is not set to “free” or “deny” i.e. “Read Access” and/or “Read&Write Access” values are different from Eh and Fh (see section 8.3 of [MFDESEV1]), the value of the read access condition field of the NDEF/Proprietary File Control TLV is set as described below in order from the msb to the lsb (see also Fig 5):
  - the first field (1 bit long, msb) SHALL be always set to 1b,
  - the three RFU fields (1 bit long) SHALL be RFU and set to 0b. No field indicates the communication mode, that SHALL be derived from the write access condition field, and
  - the Key# field (4 bits) SHOULD indicate the key number of the read access (see section 8.3 of [MFDESEV1]). Key# equal to Eh and Fh are RFU. It is RECOMMENDED that the “Read&Write Access” (see section 8.3 of [MFDESEV1]) of all non-mandatory NDEF or Proprietary File is set to “deny” i.e. Fh.

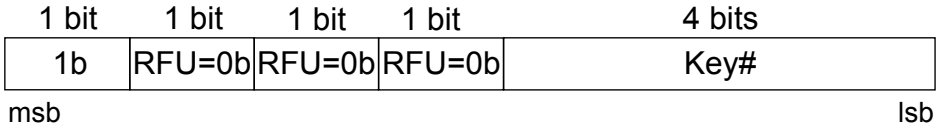

Fig 6. Read access condition field settings

6.3 States

This section describes the different MIFARE DESFire states shown in Fig 4. The state identification is based on the following elements:

- the NLEN field value of the mandatory NDEF File (NLEN was also used in [NFCT4TV2] to identify the NFC Forum life cycle states),
- the settings of the file access rights of each Proprietary File and each non-mandatory NDEF File. These elements are DESFire specific (see section 8.3 in [MFDESEV1] and section 6.2.1), and
- the communication modes of each Proprietary File and non-mandatory NDEF File. These elements are DESFire specific (see section 8.2 in [MFDESEV1] and section 6.2.1).

The values of the fields of the NDEF File Control TLVs and Proprietary File Control TLVs and of the CC File are not use to identify the state however they SHALL be set as define in the previous section 6.2 to be compatible with the [NFCT4TV2] technical specification.

The sections below complete the settings description for each MIFARE DESFire state that have been presented in the previous section 6.2 and Table 3.

6.3.1 INITIALISED State

The INITIALISED state is the state where the mandatory NDEF File is empty i.e. NLEN=0000h. Section 6.5 describes the formatting procedure to personalize the MIFARE DESFire in INITIALISED state.

In INITIALISED state the following MIFARE DESFire configuration is applied (see [MFDESEV1]):

- CC File has read access “free”, and the write access, the read&write access and the change of access rights are given previous authentication with Key 0 (NDEF Tag Application master key).
- Mandatory NDEF File, non-mandatory NDEF Files and Proprietary Files have read access “free”, write access “free”, read&write access “free”, and its change access rights field is set to 0h i.e. authentication with Key 0 (NDEF Tag Application master key) is required to change the access rights.
- Plain communication mode is applied for CC File, mandatory NDEF File, non-mandatory NDEF Files and Proprietary Files.
- NLEN field value of the mandatory NDEF File is equal to 0000h.

6.3.2 READ/WRITE State

The READ/WRITE state is the state where the mandatory NDEF File contains NDEF data i.e. NLEN≠0000h. Section 6.5 describes the formatting procedure to personalize the MIFARE DESFire in READ/WRITE state.

In READ/WRITE state the same MIFARE DESFire configuration of the INITIALISED state is applied except from the NLEN field value of the mandatory NDEF File that SHALL be different from 0000h.

6.3.3 READ-ONLY State

In READ-ONLY state the files of the NDEF Tag Application are read-only. Section 6.5 describes the formatting procedure to personalize the MIFARE DESFire in READ-ONLY state.

In READ-ONLY state the following MIFARE DESFire configuration is applied (see [MFDESEV1]):

- CC File has read access “free”, write access “deny”, read&write access “deny”, and its change access rights field is set to “deny”.
- All NDEF Files of the NDEF Tag Application have read access “free”, write access “deny”, read&write access “deny”, and their change access rights field is set to “deny”.
- All Proprietary Files of the NDEF Tag Application have read access “free”, write access “deny”, read&write access “deny”, and their change access rights field is set to “deny”.
- Plain communication mode is applied for CC File, all NDEF Files, and all Proprietary Files.
- The NLEN field value of the mandatory NDEF File that SHALL be different from 0000h

Any transition from the READ-ONLY state SHOULD NOT be allowed (see chapter 8.2).

6.3.4 DESFire READ/WRITE State

The DESFire READ/WRITE state can be seen as a special case of the READ/WRITE state. Particular settings of file access rights and communication mode identifies this state (see section 6.2 and Table 3).

In DESFire READ/WRITE state the following MIFARE DESFire configuration is applied (see [MFDESEV1]):

- CC File has read access “free”, and the write access, the read&write access and the change of access rights are given previous authentication with Key 0 (NDEF Tag Application master key).
- Mandatory NDEF File has read access “free”, write access “free”, read&write access “free”, and its change access rights field is set to 0h i.e. authentication with Key 0 (NDEF Tag Application master key) is required to change the access rights.
- Plain communication mode is applied for CC File and mandatory NDEF File.
- Each Proprietary File and each non-mandatory NDEF File of the NDEF Tag Application MAY have any kind of access rights.
- Each Proprietary Files and each non-mandatory NDEF Files MAY have any kind of communication mode.
- The NLEN field value of the mandatory NDEF File that SHALL be different from 0000h.

A reader that only implements the [NFCT4TV2] specification sees in READ/WRITE state a MIFARE DESFire in DESFire READ/WRITE state (see section 6.2 and Table 2).

6.3.5 DESFire READ-ONLY State

The DESFire READ-ONLY state can be seen a special case of the READ-ONLY state. Particular settings of file access rights, and communication mode identifies this state (see section 6.2 and Table 3).

In DESFire READ-ONLY state the following MIFARE DESFire configuration is applied (see [MFDESEV1]):

- CC File has read access “free”, and the write access, the read&write access and the change of access rights are given previous authentication with Key 0 (NDEF Tag Application master key).
- Mandatory NDEF File has read access “free”, write access “deny”, read&write access “deny” and its change access rights field are set to “deny”.
- Plain communication mode is applied for CC File and mandatory NDEF File.
- Each Proprietary File and each non-mandatory NDEF File of the NDEF Tag Application MAY have any kind of access rights.
- Each Proprietary File and each non-mandatory NDEF File MAY have any kind of communication mode.
- The NLEN field value of the mandatory NDEF File that SHALL be different from 0000h.

A reader that only implements the [NFCT4TV2] specification sees in READ-ONLY state a MIFARE DESFire in DESFire READ-ONLY state (see section 6.2 and Table 2).

6.4 State Changes/Transitions

This section describes the operations of the state changes (also called transitions) done by the NFC Forum device. Fig 4 shows the states and the state changes between them.

6.4.1 Transition from READ/WRITE to INITIALISED

This transition SHOULD NOT be implemented. It is described in this document only for sake of completeness.

To perform the transition from READ/WRITE to INITIALISED it is assumed that the MIFARE DESFire is configured to allow the transition e.g. CC File change access rights are not set to Fh (“never”). If needed authentication with PICC master key or application master key MAY be done before a MIFARE DESFire native command. The keys for write-access have been defined by a preceding MIFARE DESFire Authenticate and ChangeKey command.

The transition operations are described below:

1. If the NDEF Tag Application is not selected, send MIFARE DESFire SelectApplication to select the NDEF Tag Application (the AID to be used depends on the chip configuration, see section 6.5.1).
2. Read the CC File located from offset 0007h. All TLV NDEF/Proprietary Control TLV blocks SHALL be read from the CC File using either the ISO commands (i.e. ISO/IEC 7816-4 SELECT FILE and ISO/IEC 7816-4 READ BINARY) or the native commands (i.e. MIFARE DESFire ReadData command).
3. All NDEF and Proprietary Files, apart from the NDEF File identified by the TLV block at the offset 7h in the CC File, SHALL be deleted using the MIFARE DESFire DeleteFile.

4. The NLEN field of the NDEF File identified by the TLV block at the offset 0007h in the CC File SHALL be set to 0000h. The ISO commands (i.e. ISO/IEC 7816-4 SELECT FILE and ISO/IEC 7816-4 UPDATE BINARY) or the native commands (i.e. MIFARE DESFire WriteData command) MAY be used.
5. The CCLEN field of the CC File SHALL be set to 000Fh.

A FormatPICC command (see [MFDESEV1]) MAY be used together with the INITIALISED formatting procedure described in section 6.5 to set the MIFARE DESFire in INITIALISED state. Using the FormatPICC command all the allocated memory is released and can be used for the NDEF Tag Application, however also non-NDEF Tag Application(s) and relative files are deleted.

6.4.2 Transition from READ/WRITE to READ-ONLY

To perform the transition from READ/WRITE to READ-ONLY it is assumed that the MIFARE DESFire is configured to allow the transition e.g. NDEF File change access rights are not set to Fh (never). If needed authentication with PICC master key or application master key MAY be done before a MIFARE DESFire native command. The keys for write access have been defined by a preceding MIFARE DESFire Authenticate and ChangeKey command.

The transition operations are described below:

1. If the NDEF Tag Application is not selected, send MIFARE DESFire SelectApplication to select the NDEF Tag Application (the AID to be used depends on the chip configuration, see section 6.5.1).
2. Update all NDEF File Control TLVs and Proprietary File Control TLVs of the CC File. The content SHALL be written into the CC File using either the ISO commands (i.e. ISO/IEC 7816-4 SELECT FILE and ISO/IEC 7816-4 UPDATE BINARY) or the native commands (i.e. MIFARE DESFire WriteData command). The NDEF File write access condition fields and the Proprietary File write access condition fields of each NDEF File Control TLV and each Proprietary File Control TLV SHALL be set to FFh.
3. Send MIFARE DESFire ChangeFileSettings to change the setting of the CC File. The CC SHALL be read-only. In order to have plain (not encrypted) read-only access the MIFARE DESFire ChangeFileSettings SHALL have the following parameters:
   a. FileNo (the DESFire FID) SHALL be equal to the CC DESFire FID = 03h (derived from the ISO FID of the CC File equal to E103h).
   b. Access Rights SHALL be set to: the read access is set to “free”, instead write access, read&write access, and change access rights are set to “deny”, and
   c. CommSettings SHALL be set to plain communication (no encryption is used).

   If the File Identifier (FID) of the all NDEF Files and all Proprietary Files is not available an ISO/IEC 7816-4 READ BINARY or a MIFARE DESFire ReadData command SHALL be sent to read the CC File, and to extract the File Identifiers from the NDEF File Control TLVs and Proprietary File Control TLVs (note that the NDEF File Control TLV and the Proprietary File Control TLV contain the ISO FID of the NDEF and Proprietary Files).
4. Send MIFARE DESFire ChangeFileSettings to change the setting of all NDEF Files and Proprietary Files. In order to have plain (not encrypted) read-only access to the file, the parameters:
   a. FileNo (the DESFire FID) SHALL be equal to the DESFire FID (derived from the ISO FID of the NDEF or Proprietary File).

b. Access Rights SHALL be set to: the read access is free, instead write access, read&write access, and change access rights needs authentication with application master key, and

c. CommSettings SHALL be set to plain communication (no encryption is used).

6.4.3 Transitions from READ/WRITE to DESFire READ/WRITE

The transition from READ/WRITE to DESFire READ/WRITE is defined as any command sequence that changes the access rights and communication mode settings from the READ/WRITE state of non-mandatory NDEF Files and Proprietary Files. The transition does not change the CC and mandatory NDEF File access rights and communication modes.

The transition MAY NOT be reversible in the sense that it MAY NOT be possible to change the settings back to READ/WRITE state (see section 6.4.4).

6.4.4 Transitions from DESFire READ/WRITE to READ/WRITE

The transition from DESFire READ/WRITE to READ/WRITE is defined as any command sequence that changes the settings of file access rights and communication modes of all NDEF Tag Application files as described for READ/WRITE state (see section 6.3.2).

The transition MAY NOT be possible. An example of non-reversible transition is when the setting of a non-mandatory NDEF File change access rights is set to “deny”, and its write access is also set to “deny” (see [MFDESEV1]).

6.4.5 Transition from INITIALISED to DESFire READ/WRITE

The transition from INITIALISED to DESFire READ/WRITE is a combination of two transitions in the following order:

- the transition from INITIALISED to READ/WRITE defined by the NFC Forum (see [NFCT4TV2]), and
- the transition from READ/WRITE to DESFire READ/WRITE (see section 6.4.3).

6.4.6 Transitions from READ/WRITE to DESFire READ-ONLY

The transition from READ/WRITE to DESFire READ-ONLY is similar to the transition from READ/WRITE to READ-ONLY (see section 6.4.2) but it is only applied to the CC File, and mandatory NDEF File. If needed authentication with PICC master key or application master key MAY be done before a MIFARE DESFire native command. The keys for write access have been defined by a preceding MIFARE DESFire Authenticate and ChangeKey command.

The transition operations are described below:

1. If the NDEF Tag Application is not selected, send MIFARE DESFire SelectApplication to select the NDEF Tag Application (the AID to be used depends on the chip configuration, see section 6.5.1).
2. Update NDEF File Control TLV of the CC File at the offset 0007h (i.e. the NDEF File Control TLV of the mandatory NDEF File). The content SHALL be written into the CC File using either the ISO commands (i.e. ISO/IEC 7816-4 SELECT FILE and ISO/IEC 7816-4 UPDATE BINARY) or the native commands (i.e. MIFARE DESFire WriteData command). The NDEF File write access condition field of the NDEF File Control TLV SHALL be set to FFh.
3. If the File Identifier (FID) of the mandatory NDEF File is not available an ISO/IEC 7816-4 READ BINARY or a MIFARE DESFire ReadData command SHALL be sent

to read the CC File, and extract the File Identifier from the NDEF File Control TLV at the offset 0007h (note that the NDEF File Control TLV contains the ISO FID of the NDEF File).

4. Send MIFARE DESFire ChangeFileSettings to change the setting of the mandatory NDEF File. In order to have plain (not encrypted) read-only access to the NDEF File, the parameters:
5. FileNo (the DESFire FID) SHALL be equal to the DESFire FID (derived from the ISO FID of the NDEF File).
6. Access Rights SHALL be set to EFFFh, the read access is free, instead write access, read&write access, and change access rights needs authentication with application master key, and
7. the CommSettings SHALL be set to 00h, plain communication (no encryption is used).

In addition to this sequence, the commands to modify access settings or communication mode of the non-mandatory NDEF Files and Proprietary Files MAY be sent.

6.4.7 Transitions from DESFire READ/WRITE to DESFire READ-ONLY

The transition from DESFire READ/WRITE to DESFire READ-ONLY is similar to the transition from READ/WRITE to READ-ONLY (see section 6.4.2) but it is only applied to the CC File, and the mandatory NDEF File. If needed authentication with PICC master key or application master key MAY be done before a MIFARE DESFire native command. The keys for write-access have been defined by a preceding MIFARE DESFire Authenticate and ChangeKey command.

The transition operations are described below:

1. If the NDEF Tag Application is not selected, send MIFARE DESFire SelectApplication to select the NDEF Tag Application (the AID to be used depends on the chip configuration, see section 6.5.1).
2. Update NDEF File Control TLV of the CC File at the offset 0007h (i.e. the NDEF File Control TLV of the mandatory NDEF File). The content SHALL be written into the CC File using either the ISO commands (i.e. ISO/IEC 7816-4 SELECT FILE and ISO/IEC 7816-4 UPDATE BINARY) or the native commands (i.e. MIFARE DESFire WriteData command). The NDEF File write access condition field of the NDEF File Control TLV SHALL be set to FFh.
3. If the File Identifier (FID) of the mandatory NDEF File is not available an ISO/IEC 7816-4 READ BINARY or a MIFARE DESFire ReadData command SHALL be sent to read the CC File, and extract the File Identifier from the NDEF File Control TLV (note that the NDEF File Control TLV contains the ISO FID of the NDEF File).
4. Send MIFARE DESFire ChangeFileSettings to change the setting of the mandatory NDEF File. In order to have plain (not encrypted) read-only access to the NDEF File, the parameters:
5. FileNo (the DESFire FID) SHALL be equal to the DESFire FID (derived from the ISO FID of the NDEF File).
6. Access Rights SHALL be set to EFFFh, the read access is free, instead write access, read&write access, and change access rights needs authentication with application master key, and
7. the CommSettings SHALL be set to 00h, plain communication (no encryption is used).

In addition to this sequence, the commands to modify access settings or communication mode of the non-mandatory NDEF Files and Proprietary Files MAY be sent.

6.4.8 Transitions from DESFire READ-ONLY to READ-ONLY

The transition from DESFire READ-ONLY to READ-ONLY is defined as any command sequence that changes the settings of file access rights and communication modes of all NDEF Tag Application files as described for the READ-ONLY state (see section 6.3.3).

The transition MAY NOT be possible. An example of non-reversible transition is when the setting of a non-mandatory NDEF File change access rights is set to “deny”, and its write access is also set to “free” (see [MFDESEV1]).

6.5 Formatting Procedures for DESFire EV1 (2KB, 4KB or 8KB)

The formatting procedures for MIFARE DESFire EV1 are sequences of commands encapsulated in the ISO/IEC 7816-4 message structure ([MFDESEV1EV1]) that SHOULD be used in case the MIFARE DESFire does not contain the NDEF Tag Application. The formatting procedures MAY be used after the Card Identification Procedure (see section 2.2).Using the formatting procedures the NDEF Tag Application described in [NFCT4TV2] is created. In detail the following ones SHALL be created:

- the NDEF Tag Application with ISO AID equal to D2760000850101h,
- the capability container (CC) file with ISO File Identifier (ISO FID) equal to E103h,
- the mandatory NDEF File. The ISO File Identifier (ISO FID) SHALL be in the range from E104h to E10Fh or equal to E100h or E101h.

Note The NFC Forum Device MUST NOT format or update a previously already formatted MIFARE DESFire EV1.

6.5.1 INITIALISED Formatting Procedure

The NFC Forum device SHOULD use the INITIALISED formatting procedure to prepare the MIFARE DESFire to store NFC Forum defined data (e.g. NDEF Message) in INITIALISED state (see section 6.3.1). After this procedure the MIFARE DESFire contains the NDEF Tag Application with two EF files (see [ISOIEC 7816-4]): the Capability Container (CC) file and the NDEF File (see chapter 2 in [NFCT4TV2]).

It is assumed that the MIFARE DESFire is configured to allow the INITIALISED formatting procedure e.g. unmodified delivery state. If needed authentication with PICC default master key or NDEF Tag Application master key MAY be done before a MIFARE DESFire native command. Below the INITIALISED formatting procedure is shown in details (see [MFDESEV1] for command details and default key values).

The INITIALISED formatting procedure MAY or MAY NOT include authentication. Depending on this choice the procedure changes as indicated below.

The INITIALISED formatting procedure is composed of the following steps:

If authentication is NOT DONE jump over item 1 and 2 below.

1. Send MIFARE DESFire SelectApplication with AID equal to 000000h to select the PICC level.
2. Send MIFARE DESFire ChangeKeySetting to change the PICC master key settings into:
   a. CreateApplication and DeleteApplication commands are allowed with PICC master key authentication.
   b. GetApplicationIDs, and GetKeySettings are allowed.

3. Create the NDEF Tag Application sending MIFARE DESFire CreateApplication command with (authentication with PICC master key MAY be needed to issue this command):

   Common settings:

   a. Application Identifier,

      The AID has to be set to EEEE10h for DESFire MF3ICD40 product or it can be set to any value, except 000000h, for other DESFire series products. The default AID value used for other DESFire products is 000001h.

   b. KeySettings2

      NumOfKeys equal to 1h, the application stores up to one key for cryptographic purpose. When required this value MAY be bigger than one. In this case the steps below of the formatting procedure MAY change.

      ISO/IEC 7816-4 File Identifier supported equal to 1b

      crypto method for the application is equal to 00b. DES or 3DES operation mode for the whole application.

   c. ISO File ID equal to E110h

   d. ISO 7816-4 DF name equal to D2760000850101h

   If authentication is DONE, set:

   e. KeySettings 1 equal to:

      CreateFile and DeleteFile commands are allowed with master key authentication.

      GetFileIDs, GetFileSettings and GetKeySettings are allowed with key authentication.

   If authentication is NOT DONE, set:

   e. KeySettings1 equal to:

      CreateFile and DeleteFile commands are allowed with master key authentication.

      GetFileIDs, GetFileSettings and GetKeySettings are allowed with key authentication.

4. Send MIFARE DESFire SelectApplication to select the previously created NDEF Tag Application.
5. Send MIFARE DESFire CreateStdDataFile to create the CC File with (authentication with NDEF Tag Application master key MAY be needed to create the file):

   a. FileNo equal to 01h (FileNo is the DESFire FID),

   b. ISO File ID is equal to E103h

   c. FileSize bigger than or equal to 00000Fh (the CC size with only the NDEF File Control TLV, see [NFCT4TV2]).

   d. ComSet equal to 00h, plain communication without any encryption mechanism.

   If authentication is DONE, set:

   e. AccessRights equal to E000h, the read access is set to free, instead write access, read&write access, and change access rights need authentication with application master key.

If authentication is NOT DONE, set:

e. AccessRights equal to EEEEh, the read access, instead write access, read&write access, and change access rights are set to free.

6. Write the different fields of the CC. The content of the CC SHALL be written into the CC File using either the ISO commands (i.e. ISO/IEC 7816-4 SELECT FILE and ISO/IEC 7816-4 UPDATE BINARY) or the native commands (i.e. MIFARE DESFire WriteData command). The CC field values are:
   a. CCLEN SHALL be equal to 000Fh,
   b. Mapping Version MAY be equal to 20h, major number 2, minor number 0 i.e. version 2.0.
   c. ML_e SHALL be equal to 003Ah as maximum data size that can be read from PICC using the ISO/IEC 7816-4 READ BINARY (see [MFDESEV1]).
   d. ML_c SHALL be equal to 0034h as maximum data size that can be written to PICC using the ISO/IEC 7816-4 UPDATE BINARY (see [MFDESEV1]).
   e. NDEF File Control TLV field values are:

      T field SHALL be equal to the value specified in [NFCT4TV2].

      L field SHALL be equal to 06h.

      V field value is composed of different fields encoded in the following way: NDEF File Identifier (ISO FID) SHALL be in the range from E104h to E10Fh, or equal to E100h or E101h, Maximum NDEF File size MAY be equal to all available memory in case the MIFARE DESFire is only used to store NDEF data, NDEF File read access condition SHALL be equal to 00h, and NDEF File write access condition SHALL be equal to 00h.
7. Send MIFARE DESFire CreateStdDataFile to create the NDEF File with the following parameter values (authentication with NDEF Tag Application master key MAY be needed to create the file):
   a. FileNo equal to 02h (FileNo is the DESFire FID),
   b. ISO File ID SHALL be equal to the ISO FID defined in the NDEF File Control TLV.
   c. FileSize SHALL be equal to the Maximum NDEF File size defined in the NDEF File Control TLV. The maximum file size for a given MIFARE DESFire EV1 product is given below:

      DESFire EV1 with 2KB, maximum size of 2048 Bytes

      DESFire EV1 with 4KB, maximum size of circa 4096 Bytes

      DESFire EV1 with 8KB, maximum size of circa 7680 Bytes
   d. ComSet equal to 00h, plain communication without any encryption mechanism.

   If authentication is DONE, set:

   e. AccessRights equal to EEE0h: the read access, write access, and read&write access are set to free, and change access rights needs authentication with application master key.

   If authentication is NOT DONE, set:

   e. AccessRights equal to EEEEh: the read access, write access, read&write access, and change access rights are set to free.
8. Write the different fields of the NDEF File. The content of the NDEF File SHALL be written into the NDEF File using either the ISO commands (i.e. ISO/IEC 7816-4

SELECT FILE and ISO/IEC 7816-4 UPDATE BINARY) or the native commands (i.e. MIFARE DESFire WriteData command). The NDEF field values are:

a. NLEN SHALL be equal to 0000h, and

b. NDEF Message field SHALL be empty.

6.5.2 READ/WRITE Formatting Procedure

The READ/WRITE formatting procedure is a combination of the two procedures listed below in the following order:

1. the INITIALISED formatting procedure that SHALL be done first (see section 6.5.1), and
2. the transition from INITIALISED to READ/WRITE (see [NFCT4TV2]).

The previous list also indicates in which order the procedures SHALL be done.

7. Additional Features

This chapter describes the additional features that the MIFARE DESFire MAY support. Even implementing these features the MIFARE DESFire formatted as Type 4 Tag platform SHALL remain compatible with the technical specification [NFCT4TV2].

7.1 Several NDEF Files

An NDEF Tag Application MAY contain more than one NDEF File. In order to specify more than one NDEF File the CC File contains more than one NDEF File Control TLV. In the example of Fig 7 the CC File contains two NDEF File Control TLVs that indicate the two NDEF Files stored in the NDEF Tag Application. The numbers in brackets on top of each file indicates the relative ISO File Identifier (ISO FID). The number on the top-left corner, below the “NDEF Tag Application” name indicates the ISO Application Identifier (ISO AID) of the NDEF Tag Application.

Up to 14 different NDEF Files MAY be contained inside the NDEF Tag Application with ISO FID number in the range E104h to E10Fh or equal to E100h or E101h. ISO FID E103h is used by the CC File. ISO FID E102h is reserved (see [NFCT4TV2]).

The ISO FID for NDEF Files and Proprietary Files SHALL be unique inside the MIFARE DESFire.

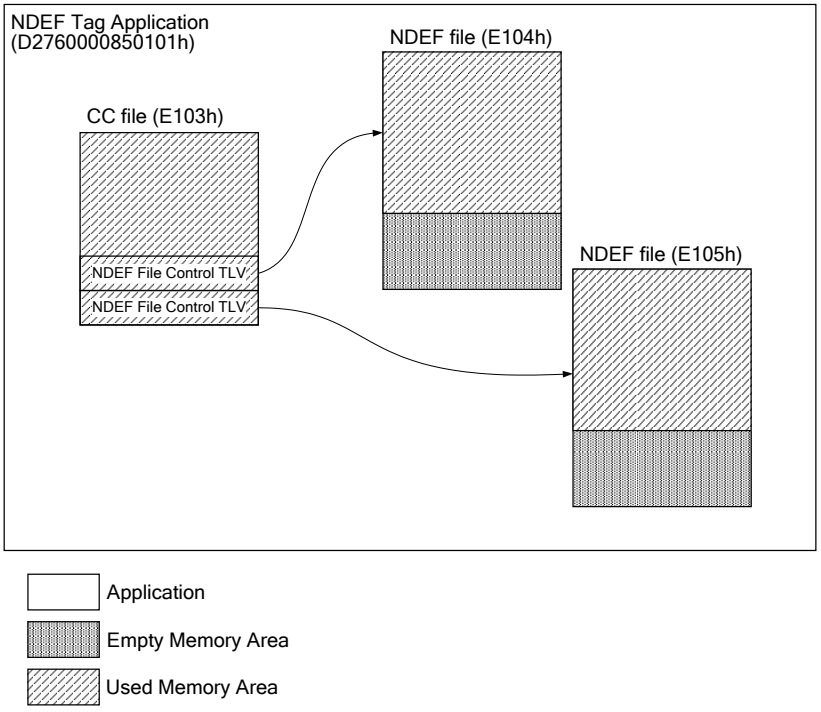

Fig 7. Example of several NDEF Files inside the NDEF Tag Application

7.2 Several NDEF Messages and Proprietary Data inside the same NDEF File

An NDEF File inside an NDEF Tag Application MAY contain more than one NDEF Message (see [NDEF]) and proprietary data as well.

Fig 8 shows an example of NDEF Tag Application with one NDEF Files that contains: three NDEF Messages and a block of proprietary data between NDEF Message 2 and NDEF Message 3. In this example it is supposed that the information like offset and length about the additional NDEF Messages (i.e. NDEF Message 2 and NDEF Message 3) and the proprietary data block is store inside the first three NDEF records of the NDEF Message 1. However based on implementation requirements, this information can be stored differently inside the NDEF Message 1.

The CC File and the NLEN field do not provide any information about the NDEF Message 2, the NDEF Message 3 and the proprietary data block. In the example of Fig 8 the NLEN filed contains the length of the NDEF Message 1 only.

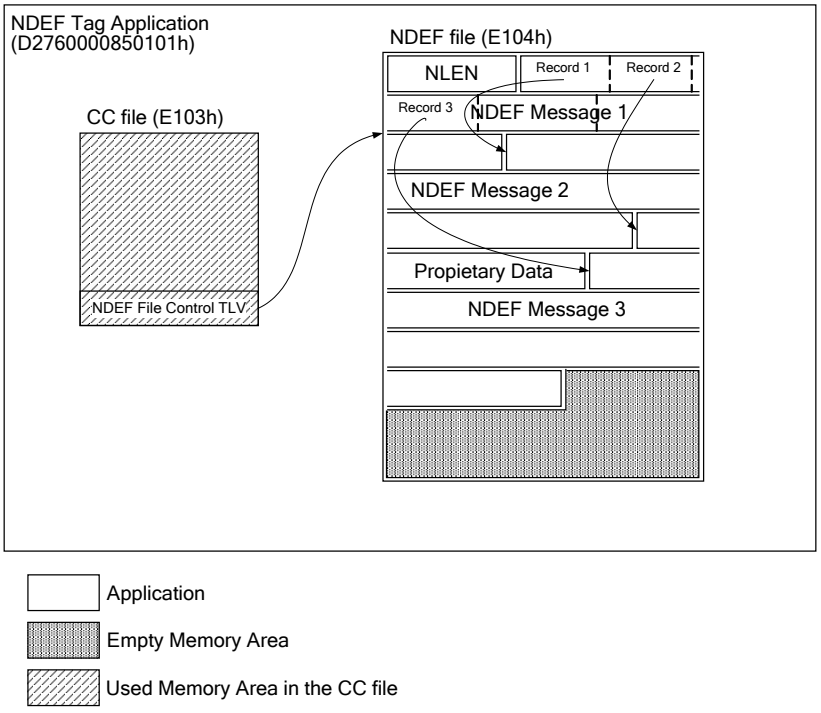

Fig 8. Example of Three NDEF Messages and one Proprietary Data Block inside the same NDEF File

7.3 Proprietary Files

The technical specification [NFCT4TV2] provides the capability to define Proprietary Files that contains proprietary data using the Proprietary File Control TLV inside the CC File.

Fig 9 shows an example with an NDEF Tag Application with a CC File containing a NDEF File Control TLV and a Proprietary File Control TLV that point respectively to an NDEF File and a Proprietary File.

Up to 13 different Proprietary Files MAY be contained inside the NDEF Tag Application with ISO FID number in the range from E104h to E10Fh or equal to E100h or E101h. ISO FID E103h is used by the CC File. ISO FID E102h is reserved (see [NFCT4TV2]).

The ISO FID of NDEF Files and Proprietary Files SHALL be unique inside the MIFARE DESFire.

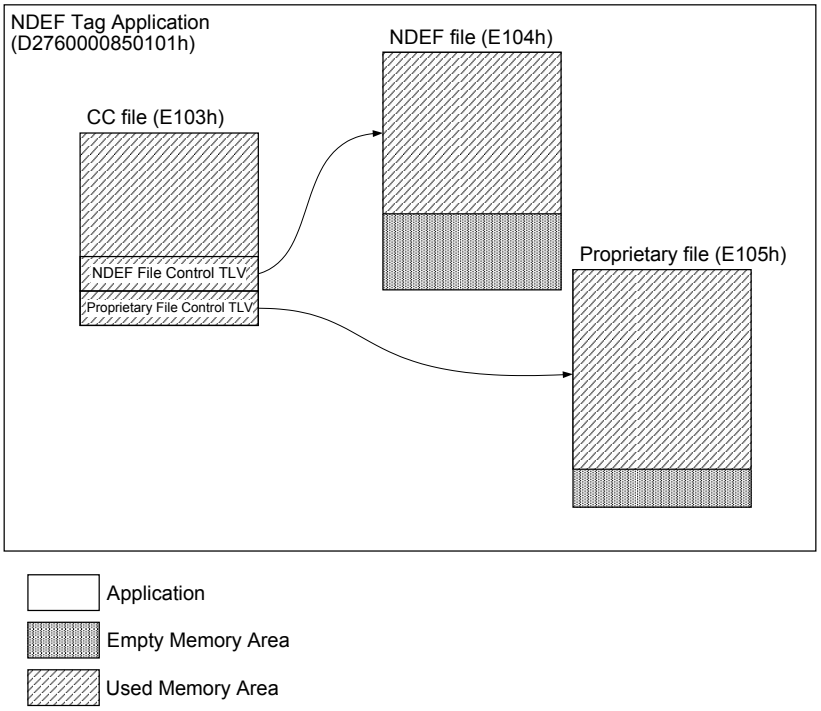

Fig 9. Example of Proprietary File inside the NDEF Tag Application

8. ANNEX: Examples

In the examples below for each command and response are written in hexadecimal format. The top-left byte of each command and response is sent first.

The native MIFARE DESFire commands and responses are sent encapsulated inside the “case 4” ISO/IEC 7816-4 message structure (see section 3.13 of [MFDESEV1]). When it is needed the authentication with the PICC master key or the NDEF Tag Application master key is carried out. For more information about command and response formats see [MFDESEV1].

8.1 Example of INITIALISED Formatting Procedure

This example shows how the INITIALISED Formatting Procedure (see 6.5.1) may be implemented. As a precondition the MIFARE DESFire is formatted with the FormatPICC command, and the PICC master key settings values are equal to the default settings.

The example of INITIALISED Formatting Procedure is described below

1. MIFARE DESFire SelectApplication with AID equal to 000000h (PICC level)

   Command: 90 5a 00 00 03 00 00 00 00h

   Expected Response: 91 00h

2. MIFARE DESFire CreateApplication using the default AID 000001h (see section 6.4.1 for the definition of the allowed AID values), key settings equal to 0Fh, NumOfKeys equal to 01h, File-ID equal to 10E1h, DF-name equal to D2760000850101

   Command: 90 CA 00 00 0E 01 00 00 0F 21 10 E1 D2 76 00 00 85 01 01 00h

   Expected Response: 91 00h

3. MIFARE DESFire SelectApplication (Select previously created application)

   Command: 90 5A 00 00 03 01 00 00 00h

   Expected Response: 91 00h

4. MIFARE DESFire CreateStdDataFile with FileNo equal to 01h (CC File DESFire FID), ISO FileID equal to E103h, ComSet equal to 00h, AccessRights equal to EEEEh, FileSize bigger equal to 00000Fh

   Command: 90 CD 00 00 09 01 03 E1 00 00 E0 0F 00 00 00h

   Expected Response: 91 00h

5. MIFARE DESFire WriteData to write the content of the CC File with CCLEN equal to 000Fh, Mapping Version equal to 20h, ML_e equal to 003Ah, ML_c equal to 0034h, and NDEF File Control TLV equal to: T=04h, L=06h, V=E1 04 (NDEF ISO FID = E104h) 08 00 (NDEF File size = 2048 Bytes) 00 (free read access) 00 (free write access)

   Command: 90 3D 00 00 16 01 00 00 00 0F 00 00 00 0F 20 00 3A 00 34 04 06 E1 04 08 00 00 00 00h

   Expected Response: 91 00h

6. MIFARE DESFire CreateStdDataFile with FileNo equal to 02h (NDEF File DESFire FID), ISO FileID equal to E104h, ComSet equal to 00h, ComSet equal to 00h, AccessRights equal to EEE0h, FileSize equal to 000800h (2048 Bytes)

   Command: 90 CD 00 00 09 02 04 E1 00 E0 EE 00 08 00 00h

   Expected Response: 91 00h

7. MIFARE DESFire WriteData to write the content of the NDEF File with NLEN equal to 0000h, and no NDEF Message

   Command: 90 3D 00 00 09 02 00 00 00 02 00 00 00 00 00h

   Expected Response: 91 00h

8.2 MIFARE DESFire EV1 GetVersion command using the Wrapping of Native DESFire APDUs

The Card Identification Procedure (see section 2.2) requires the sending of the MIFARE DESFire EV1 GetVersion command in order to get the Software Major Version and the Software Storage Size. In the example below the following acronym are used: XX to indicate a generic byte with no relevant meaning, SW byte indicating the Software Major Version and SS indicating the Software Storage code.

The example of MIFARE DESFire EV1 GetVersion command is described below using the wrapping of Native DESFire APDUs:

8. MIFARE DESFire EV1 GetVersion command 1

   Command: 90 60 00 00 00h

   Expected Response: XX XX XX XX XX XX XX 91 AFh

9. MIFARE DESFire EV1 GetVersion command 2. The Storage Size code (SS) value indicates the storage size, in particular: 1Ah indicates 8192 bytes, 18h indicates 4096 bytes and 16h indicates 2048 bytes

   Command: 90 AF 00 00 00h

   Expected Response: XX XX XX SW XX SS XX 91 AFh

10. MIFARE DESFire EV1 GetVersion command 3

    Command: 90 AF 00 00 00h

11. Expected Response: XX XX XX XX XX XX XX XX XX XX XX XX XX 91 00

9. ANNEX: READ-ONLY and DESFire READ-ONLY State Comment

In READ-ONLY and DESFire READ-ONLY state it is possible to perform the operations below using the PICC or NDEF Tag Application master key (see [MFDESEV1] for more detailed information). For this reason it is RECOMMENDED to keep the PICC master key and the application master key of the NDEF Tag Application secret.

Permitted operations previous authentication with PICC master key:

- PICC Format,
- Create/DeleteApplication, and
- ChangeKeySettings.

Permitted operations previous authentication with PICC master key:

- Create/DeleteFile, and
- ChangeKeySettings.

The previous operations allow the change of state of the MIFARE DESFire also when it is in READ-ONLY or DESFire READ-ONLY state. For instance a formatted MIFARE DESFire using the FormatPICC command and the formatting procedure described in section 6.5 can be re-initialized as NFC Forum Type 4 Tag.

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

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

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

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

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

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

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

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

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

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

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

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

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

10.3 Licenses

Purchase of NXP ICs with NFC technology

Purchase of an NXP Semiconductors IC that complies with one of the Near Field Communication (NFC) standards ISO/IEC 18092 and ISO/IEC 21481 does not convey an implied license under any patent right infringed by implementation of any of those standards.

ICs with DPA Countermeasures functionality

LICENSED DPA COUNTERMEASURES™

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

10.4 Trademarks

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

MIFARE — is a trademark of NXP B.V.

MIFARE DESFire — is a trademark of NXP B.V.

11. Contents

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

Date of release: 22 May 2013 130224

Document identifier: AN11004