AN1305

MIFARE Classic as NFC Type MIFARE Classic Tag

Rev. 1.3 — 2 October 2012
130513

Application note
COMPANY PUBLIC

Document information

Info	Content
Keywords	NFC Forum, NFC data mapping, MIFARE Classic 1K/4K, MIFARE Classic 1K, MIFARE Classic 4K, MIFARE Plus X/S, NFC Type MIFARE Tag
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. The “NFC Type MIFARE Tag” application note has been developed to describe how the Reader device (also called NFC device) can store NDEF data inside an MIFARE Classic or MIFARE Plus tag. This document provides extended functionalities, and additional information to the “NFC Type MIFARE Tag” application note regarding how the NFC device manages the MIFARE Classic or MIFARE Plus products to store NDEF and proprietary data.

Revision history

Rev	Date	Description
1.3	20121002	Section License updated
1.2	20110503	Editorial Review: added MIFARE Plus X/S, replaced NFC Forum sector with NFC sector, replaced NFC Forum AID with NFC AID and other editorial updates.
1.1	20070821	Review and rewording of chapter 2: removal of the "2nd NFC sector configuration", correction in the "Card Identification Procedure", added section 6.4.9 "Transitions from READ/WRITE to MIFARE BLOCKED READ-ONLY", added chapter 7 "Additional Features"
1.0	20061111	Final revision
0.1	20060721	First draft version

Contact information

For additional 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 NDEF data) inside current contactless card products a mapping model is required. The application note “NFC Type MIFARE Tag” describes this mapping model and how the NFC device manages a MIFARE Classic or MIFARE Plus tags to store NFC Forum defines data.

The MIFARE Classic and MIFARE Plus product (see [MF1K, MF4K, MFPLUS]) is a contactless card currently available with 1Kbyte, 2Kbyte and 4Kbyte of EEPROM memory. The MIFARE Classic or MIFARE Plus supports data transfer up to 106 kbit/s, mutual three pass authentication, data encryption of RF-channel with replay attack protection, and CRYPTO1 stream cipher for secure data exchange.

This document specifies:

- how to identify and format a MIFARE Classic or MIFARE Plus to contain NDEF data,
- how to manage more than one NDEF Message and proprietary data, and
- how to exploit the features of MIFARE Classic or MIFARE Plus not used by “NFC Type MIFARE Tag” application note.

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 [ANNFCMF] using MIFARE Classic or MIFARE Plus card, and the ones required by implementer or customer requirements.

It is RECOMMENDED to implement at least the features below to support [ANNFCMF] using MIFARE Classic or MIFARE Plus cards:

- 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 6.4.4, 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: Initialisation and Anticollision
[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.
[MF1K]	“MF1 IC S50, Functional Specification”, NXP Semiconductors, Product Data Sheet, Revision 5.2, 19 December 2006, Document Identifier 0010.

[MF4K] "MF1 IC S70, Standard 4 kByte Card IC Functional Specification", NXP Semiconductors, Product Data Sheet, Revision 4.0, 7 February 2007, Document Identifier 0435.

[MFPLUS] "MF1PLUSx0y1, Mainstream Contactless Smart Card IC For Fast And Easy Solution Development", Revision 3.1, 19 April 2010, Document Identifier 1635.

[MAD] "AN MAD, MIFARE Application Directory", NXP Semiconductors, Application Note, Revision 3.0, 4 May 2007, Document Identifier 0018.

[SMX] Application Note, SmartMX Platform Features, Rev. 1.0, 24 March 2004.

[ANNFCMF] "NFC Type MIFARE Tag Operation", NXP Semiconductors, Application Note, 02 April 2011, Document Identifier 1304.

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 (see [NDEF]) 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).

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 Glossary

Table 1. Terms and definitions

Term	Definition
Access Bits	Bits of the sector trailer that controls the access rights to the whole sector
card	A MIFARE Classic 1k/4k contactless card, see [MF1K, MF4K]
$C1_{0...3}$, $C2_{0...3}$, $C3_{0...3}$.	access bits of the sector trailer
DA	MAD available bit, see [MAD]
data area access bits / data block access bits	Access bits to set the access configuration on the blocks of the sector
GPB	General Purpose Byte, see [MAD]
Key A	6 bytes key of the sector
Key B	6 bytes key of the sector
lsb	least significant bit
LSB	least significant byte
MAD	MIFARE Application Directory, see [MAD]
MAD1	MIFARE Application Directory 1, see [MAD]
MAD2	MIFARE Application Directory 2, see [MAD]
MAD sector	A sector containing the MAD, see [MAD].
Mandatory NDEF Message TLV or 1st NDEF Message TLV	The NDEF Message TLV identified by the NDEF Detection Procedure (see [ANNFCMF]). The [ANNFCMF] mandates to support at least one NDEF Message TLV, this NDEF Message TLV is called mandatory or 1st one being the 1st NDEF Message TLV if more consecutive NDEF Message TLVs are present into the MIFARE Classic or MIFARE Plus tag.
msb	most significant bit
MSB	most significant byte
NDEF	NFC Data Exchange Protocol, see [NDEF]
NDEF Message	Data packet structured as specified by the [NDEF] specification.
NDEF Message TLV	TLV block that contains an NDEF Message.
NFC	Near Field Communication
NFC Forum	Standardization body, see http://www.nfc-forum.org/home
NDEF data	Data contained inside a MIFARE Classic or MIFARE Plus defined by the NFC Forum e.g. NDEF Message
NFC device	NFC Reader device capable to operate MIFARE Classic tags

Term	Definition
NFC sector	Sector that contains NDEF data. In this application note with the name NFC sector(s) it is meant both proprietary and non-proprietary NFC sector(s).
Non-mandatory NDEF Message TLVs	NDEF Message TLV(s) not identified by the NDEF Detection Procedure (see [ANNFCMF]). These NDEF Message TLVs are present inside the MIFARE Classic or MIFARE Plus only when more than one NDEF message TLV is stored. The Non-mandatory NDEF Message TLVs are the NDEF Message TLVs that are not the Mandatory one.
Non-proprietary NFC sector	NFC sector used by the [ANNFCMF] to read and write the mandatory NDEF Message TLV.
NULL TLV	Single byte TLV block mainly used for padding.
PCD	Proximity Coupling Device according the ISO 14443. The term PCD describes a reader/writer for contactless cards
PICC	Proximity Card according to the ISO/IEC 14443. The MIFARE Classic or MIFARE Plus contactless card
Proprietary TLV	TLV block that contains proprietary data
Proprietary NFC sector	NFC sector not used by the [ANNFCMF] to read and write the mandatory NDEF Message TLV. This sector has proprietary data and configuration settings
Reader device /Reader	Reader/writer for contactless cards. It may be a NFC device or a PCD device.
RF	Radio Frequency
RFU	Reserved for Future Use
SAK	Selective Acknowledge see [ISOIEC 14443-3]
Sector trailer access bits	Access bits to set the access configuration of the sector trailer
tag	A MIFARE Classic or MIFARE Plus tag, see [MF1K, MF4K, MFPLUS]
Terminator TLV	Last TLV block of the tag
TLV	Type Length Value block, data structure element to store different kind of data.
UID	Unique Identifier or serial number, see [MF1K, MF4K, MFPLUS]

2. Memory Layout

MIFARE Classic or MIFARE Plus are based on a particular memory chip with a certain memory size and space for data. The following sections describe the details of such memory chips and in particular their memory structure and management (for more details see [MF1K, MF4K, MFPLUS]).

A memory structure (or memory layout) is defined for each MIFARE Classic or MIFARE Plus product to store NDEF data (see [ANNFCMF]). Table 2 gives an overview of the MIFARE Classic products.

MIFARE Plus SHALL be configured in Security Level 1: backwards functional compatibility mode (with MIFARE Classic 1K and MIFARE Classic 4K) with optional AES authentication.

Table 2. Overview on MIFARE Classic products

	Name	EEPROM
MIFARE Classic 1k	MF1 S50	1 Kbyte
MIFARE Classic 4k	MF1 S70	4 Kbyte
MIFARE Plus X	MF1 PLUS 60	2 Kbyte
	MF1 PLUS 80	4 Kbyte
MIFARE Plus S	MF1 SPLUS 60	2 Kbyte
	MF1 SPLUS 80	4 Kbyte

The memory structure of MIFARE Classic or MIFARE Plus is divided in sectors. Each sector contains 4 or 16 blocks. The first block of each sector is called sector trailer (see [MF1K, MF4K, MFPLUS]).

Sectors that contain MAD data are called MAD sectors and sectors that contain NDEF data are called NFC sectors (see [ANNFCMF]).

2.1 NFC sector Configurations

In this application note the NFC sectors are classified into two types:

- Non-proprietary NFC sectors. These are the only sectors used by the [ANNFCMF] to read and write the NDEF Message (see section 6.4.1, 6.4.2 and 6.4.3 of [ANNFCMF]). These sectors contain the mandatory NDEF message TLV, and they might contain non-mandatory NDEF Message TLVs and other TLV blocks.

  In particular the non-proprietary NFC sectors have the following settings:

  - the read access field of the GPB equal to 00b and the write access field of the GPB equal to 00b or 11b (depending on the state see section 6.2.1),
  - the access bits value as described in section 2.4.2 of [ANNFCMF], and
  - the key A equal to the public key A for NFC sectors (see Table 6).
- Proprietary NFC sectors. These sectors are not used by [ANNFCMF] to read and write the NDEF Message. The NDEF Detection Procedure (see section 6.4.1 of [ANNFCMF]) jumps over the proprietary NFC sectors. The proprietary NFC sectors do not contain the mandatory NDEF Message TLV and Terminator TLV but they

might contain non-mandatory NDEF Message TLVs, Proprietary TLVs and NULL TLVs.

In particular these sectors allow having different settings:

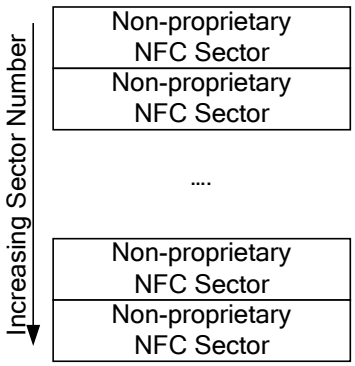
- of the read and write access field of the GPB,
- of the access bits that are different from the values described in section 2.4.2 of [ANNFCMF], and
- of the key A value. Key A might be different from the public key A of NFC sectors (see Table 6). E.g. these sectors might not be authenticable using the public key A of NFC sectors.

In this application note with the name NFC sector(s) it is meant both proprietary and non-proprietary NFC sector(s).

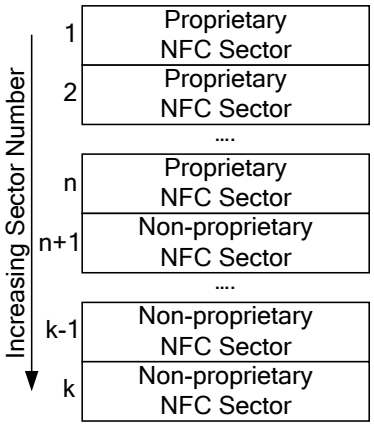
The proprietary NFC sectors with their different settings of the GPB, access bits and key A might introduce different access configurations that can be difficult to manage and to test. For this reason only the following two configurations of are mandated by this application note (see Fig 1):

1. The Simple Configuration. In this configuration only non-proprietary NFC sectors are present.
2. Mixed Configuration. In this configuration the first n NFC sectors are proprietary ones, and the remaining k-n NFC sectors are non-proprietary ones.

Note that as described in the [ANNFCMF] if the NFC sectors are contiguous (except in case the MIFARE Classic 4k is used with the MAD sector 16, see section 6.1 of [ANNFCMF]).



a. Simple Configuration: only non-proprietary NFC sectors are present



b. Mixed Configuration: proprietary NFC sectors are present in the NFC sector with smaller sector number

Fig 1. NFC sector Configurations

It is not allowed a configuration where the proprietary NFC sector are interlaced with the non-proprietary ones e.g. first 2 proprietary NFC sectors, then 3 non-proprietary ones and finally again 4 proprietary ones.

This application note explicitly describes how to create, identify and manage the proprietary and non-proprietary NFC sectors according to the Simple and Mixed Configuration. [ANNFCMF] is compatible with these two NFC sector configurations.

2.2 Mapping of NDEF data using MIFARE Classic 1k/4k card ICs

The mapping of NDEF data inside MIFARE Classic or MIFARE Plus SHALL be done using the MIFARE Application Directory and the TLV blocks (see [ANNFCMF]).

The MIFARE Classic or MIFARE Plus SHALL contain the following TLV blocks:

1. one or more NDEF Message TLV,
2. zero, one or more Proprietary TLV,
3. zero, one or more NULL TLV,
4. zero or one Terminator TLV.

In this application note the mandatory NDEF Message TLV is defined as the 1st NDEF Message TLV found by the NDEF Detection Procedure (see section 6.4.1 in [ANNFCMF]).

2.3 Card Identification Procedure

This section describes the Card Identification Procedure performed by a Reader device to be able to identify the type of card i.e. MIFARE Classic or MIFARE Plus and the card settings.

Two different card settings have been considered by the Card Identification Procedure: settings of card after the production phase (also called blank cards) and settings of card in a valid state as defined in chapter 6. To be able to distinguish between these two settings, the Card Identification Procedure is composed of a set of common operations and two different branches depending on the card settings that is need to be identified. The two branches are called “Card Identification Procedure for MIFARE Classic and MIFARE Plus card after production phase” and “Card Identification Procedure for MIFARE Classic or MIFARE Plus card in a valid state”.

In this section only the common operations are described. The “Card Identification Procedure for MIFARE Classic or MIFARE Plus card after production phase” (see section 2.3.1) is mainly used before the Formatting Procedure (see section 6.5).

The “Card Identification Procedure for MIFARE Classic or MIFARE Plus card in a valid state” (see section 2.3.2) is mainly used before the NDEF Detection Procedure (see section 6.4.1 of [ANNFCMF]).

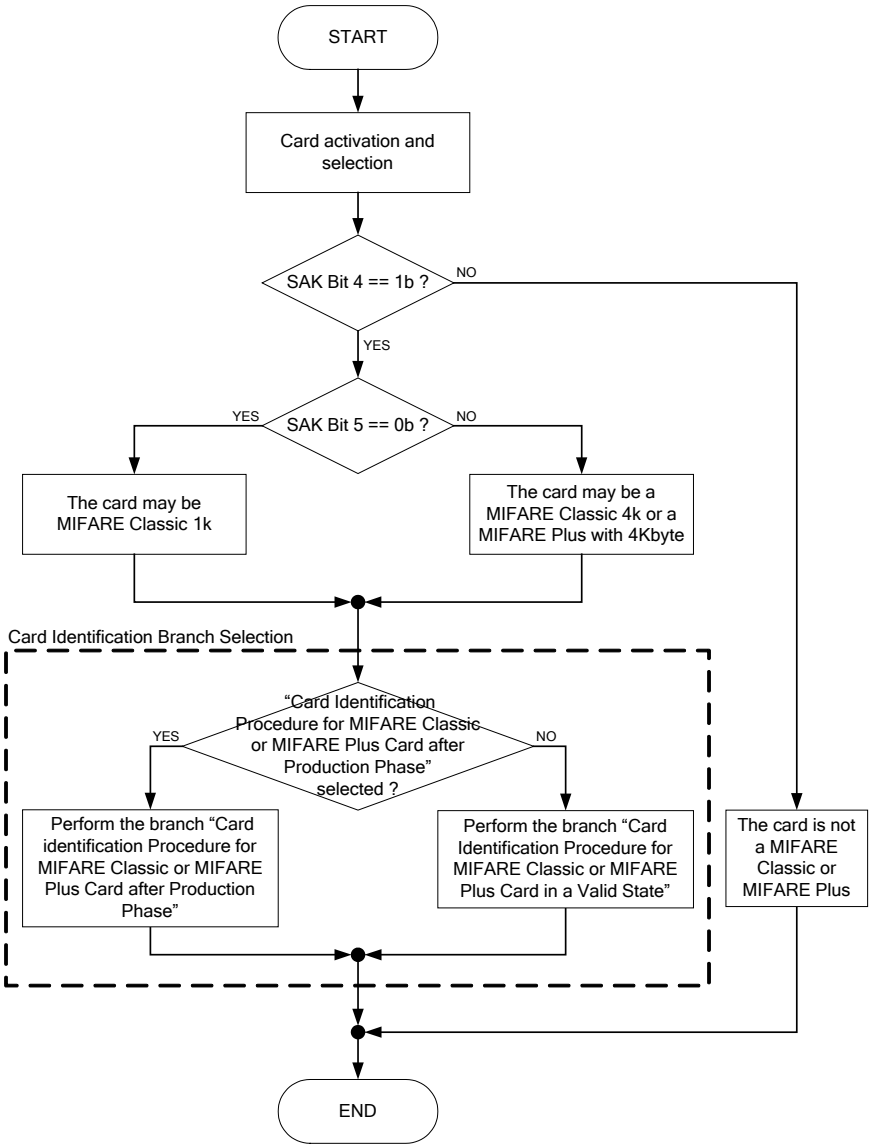


Fig 2. Card Identification Procedure: Common Operations and Branch Selection

The common operations of the Card Identification Procedure that SHALL performed by the Reader device are (see Fig 2):

1. checking of bit 4 of the Selective Acknowledge (SAK, see [ISOIEC 14443-3]) to be equal to 1b, and
2. checking of bit 5 of the Selective Acknowledge (SAK, see [ISOIEC 14443-3]) that indicates the memory size of the MIFARE Classic or MIFARE Plus tag:
   - Bit 5 equal to 0b indicates that the tag is potentially a MIFARE Classic 1k, and
   - Bit 5 equal to 1b indicates that the tag is potentially a MIFARE Classic 4k or MIFARE Plus with 4Kbyte.

If the previous operations are done successfully, they do not surely identify that the card is a MIFARE Classic or MIFARE Plus card. The Reader device SHALL send an

additional Authentication operation to really identify that the card is a MIFARE Classic 1k/4k. These Authentication operations are included in the two branches of the Card Identification Procedures.

After the common operations the Reader device SHALL choose one of the two branches of the Card Identification Procedure described in the next two sections (see section 2.3.1, section 2.3.2 and Fig 2).

If it is not known in advance which card settings the Reader device has to look for and hence which Card Identification branch is needed, a try-fail approach can be done: trying first one branch of the Card Identification Procedure and if it fails trying the other one. After the failure of one branch before trying the other, the card needs to be reactivated and selected.

Based on the SAK it is not possible to distinguish between MIFARE Classic 1k and MIFARE Plus with 2Kbyte in Security Level 1. Hence the Card Identification recognizes a MIFARE Plus with 2Kbyte in Security Level 1 as MIFARE Classic 1k.

2.3.1 Card Identification Procedure for MIFARE Classic or MIFARE Plus Card after Production Phase

After production phase (i.e. blank card) the MIFARE Classic or MIFARE Plus card all sectors are set with:

- Key A equal to the default one see Table 3,
- Key B equal to the default one see Table 3, and
- access condition bits related to the sector trailer are configured in two different ways to allow either:
  - read and write access when the previously authentication with Key A was successful (this configuration is called transport configuration, see ANNEX B Table 11 and [MF1K, MF4K; MFPLUS]), or
  - read and write access when previously the authentication with Key B was successful (see ANNEX B Table 11 and [MF1K, MF4K, MFPLUS]).

Table 3. Default Key A and Key B

Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5
FFh	FFh	FFh	FFh	FFh	FFh

[1] The byte number on the header row indicates the bite number of the sector trailer.

The previous settings are also valid for SmartMX products that include the MIFARE Classic emulation (see [SMX]).

The Card Identification Procedure for MIFARE Classic or MIFARE Plus cards after production phase is composed by the following steps in addition to the common ones described in section 2.3:

1. Perform the Authentication operation of sector 0 using default key A (see Table 3).
2. If the authentication is successful go to the next item. If the authentication is not successful, the card is not a MIFARE Classic or MIFARE Plus after production phase.
3. Use the Read operation to read the sector trailer of sector 0.

4. If the Read operation is successful go to the next item. If the Read operation is not successful, the card is not a MIFARE Classic or MIFARE Plus after production phase.
5. If the Bytes 6-8 (also called access conditions or access bits) of the sector trailer of sector 0 are equal to FF0780h, go to the next item. Otherwise go to item 7.
6. After the sector 0, for each subsequent sectors:

   a. perform an Authentication operation with the default key A (see Table 3),

   b. read the sector trailer, and

   c. check if bytes 6-8 of the sector trailer are equal to FF0780h.

   If the authentication and read operations are successful and bytes 6-8 of the sector trailer are equal to FF0780h, the card is a MIFARE Classic or MIFARE Plus after production phase. The Authentication operation with the default key A (see Table 3) SHALL be used by the Formatting Procedure (see section 6.5).

   If the authentication or the read operations are not successful, the card is not a MIFARE Classic or MIFARE Plus after production phase.
7. If the Bytes 6-8 of the sector trailer of the sector 0 are equal to 7F0788h, go to the next item. Otherwise the card is not a MIFARE Classic or MIFARE Plus after production phase.
8. After the sector 0, for each subsequent sectors:

   a. perform an Authentication operation with the default key B (see Table 3),

   b. read the sector trailer, and

   c. check if bytes 6-8 of the sector trailer are equal to 7F0788h.

   If the authentication and read operations are successful and bytes 6-8 of the sector trailer are equal to 7F0788h, the card is a MIFARE Classic or MIFARE Plus after production phase. The Authentication operation with the default key B (see Table 3) SHALL be used by the Formatting Procedure (see section 6.5).

   If the authentication or the read operations are successful, the card is not a MIFARE Classic or MIFARE Plus after production phase.

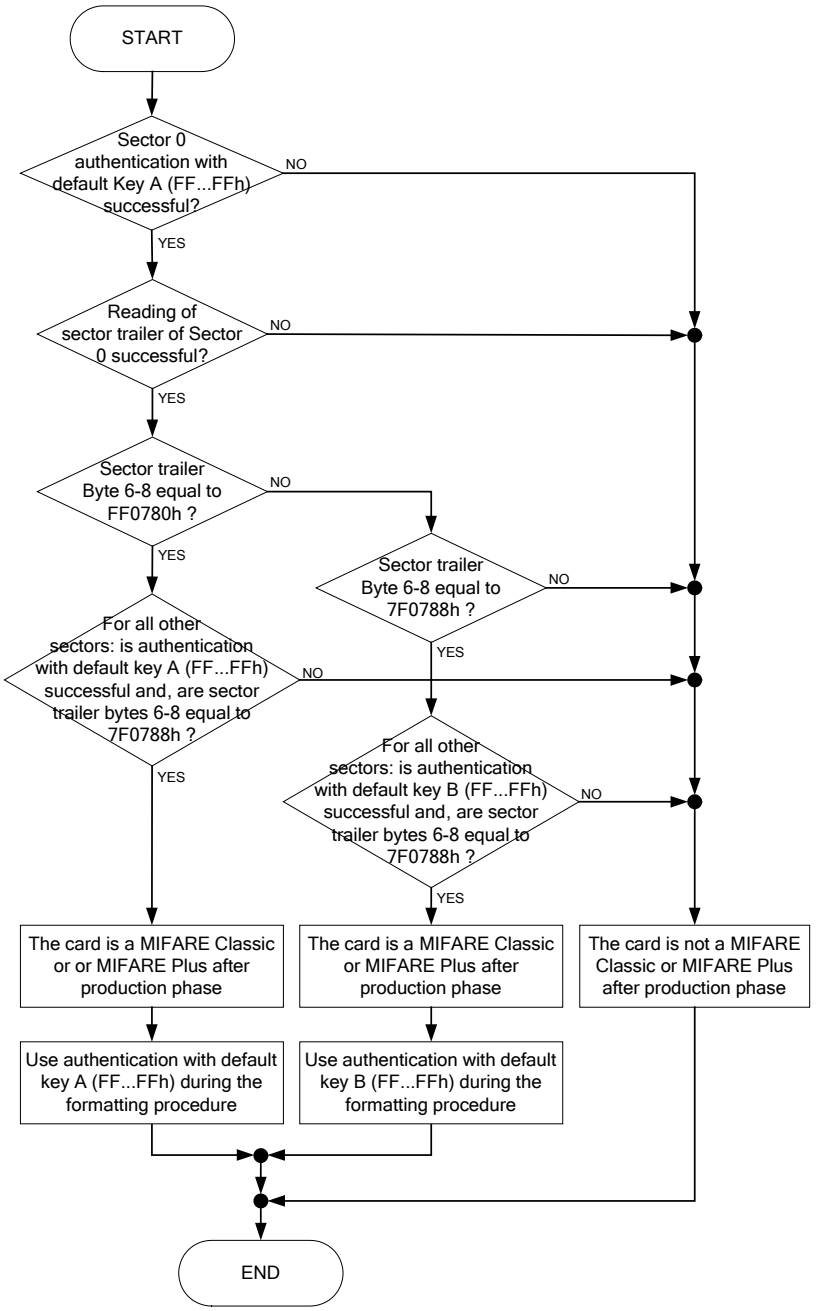


Fig 3. Card Identification Procedure for MIFARE Classic or MIFARE Plus Card after Production Phase

If needed the Card Identification Procedure for MIFARE Classic or MIFARE Plus cards after production phase MAY be modified to be integrated and optimized together with the Formatting Procedures (see section 6.5).

When the MIFARE Classic or MIFARE Plus tag has different access conditions than FF0780h or 7F0788h, using the default Key A or the default Key B it might still be possible to use the Formatting Procedures (see section 6.5).

2.3.2 Card Identification Procedure for MIFARE Classic or MIFARE Plus Card in a Valid State

To identify a MIFARE Classic or MIFARE Plus card in a valid state as defined in chapter 6, the Reader device SHALL perform the following steps (see Fig 4) in addition to the common ones described in section 2.3:

1. An Authentication operation is performed with public key A for MAD sector described in Table 9 to access Sector 0 i.e. the MAD sector.
2. If the Authentication operation returns successfully, the card is a MIFARE Classic 1k/4k card and the NDEF Detection Procedure (see [ANNFCMF]) is used. Otherwise the card is not a MIFARE Classic or MIFARE Plus card in a valid state.
3. If the NDEF Detection Procedure is successful, the check of the state of the NFC sectors is done following chapter 6.
4. If the check of the state is successful the card is a MIFARE Classic or MIFARE Plus in a valid state. The transitions defined in section 6.4 MAY be used.

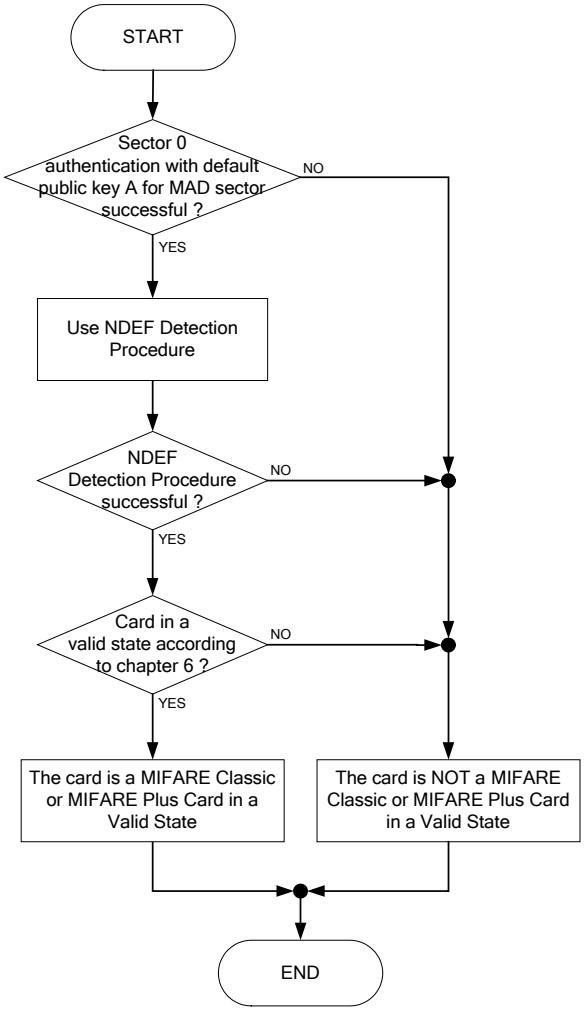


Fig 4. Card Identification Procedure for MIFARE Classic or MIFARE Plus Card in a Valid State

3. Read/Write Access

Current version of MIFARE Classic or MIFARE Plus has a flexible and powerful method for specifying the access conditions or the access rights based on access bits and two keys per sector.

For more information see [MF1K, MF4K, MFPLUS].

4. Framing / Transmission Handling

The framing and the transmission handling for MIFARE Classic or MIFARE Plus is specified in [ANNFCMF].

5. Command Set

The following operations have to be supported in the reader side (PCD) in order to read from or write to MIFARE Classic or MIFARE Plus the NDEF data (see [ANNFC1K4K, MF1K, MF4K, MFPLUS]):

- Read operation,
- Write operation, and
- Authentication operation.

6. Life Cycle

The states below refer to the NFC sector(s) only. A state is reflected by the content and configuration settings of the NFC sectors (see below in this section for a more detailed description of the content and configuration settings). In this document the state of the NFC sectors is also called the state of the MIFARE Classic or MIFARE Plus tag.

Each state has its own valid operations called transactions or state changes. An entry is an operation to prepare the MIFARE Classic or MIFARE Plus tag 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-like life cycle (see section 6.1). This life cycle is the one described in the application note [ANNFCMF]. It is called NFC-like life cycle because it is similar to that one defined in the NFC Forum technical specifications.
- The MIFARE life cycle (see section 6.2). This life cycle shows the NFC-like life cycle together with additional states and transitions that make use of additional MIFARE Classic or MIFARE Plus features. The additional transitions and states MAY be partially implemented to satisfy specific requirements that are not covered by [ANNFCMF].

After the description of the life cycle the different states, transitions (state changes) and entries (Formatting Procedures) are shown (see section 6.3, 6.4, and 6.5).

6.1 NFC-like Life Cycle

The application note [ANNFCMF] describes the life cycle from the Reader device perspective as a combination of states, transitions and entries. Fig 5 describes this life cycle (called NFC-like life cycle). The dashed arrows indicate the entries in the life cycle. The entries also called Formatting Procedures are described in section 6.5. The continuous arrows indicate the transitions or also called state changes.

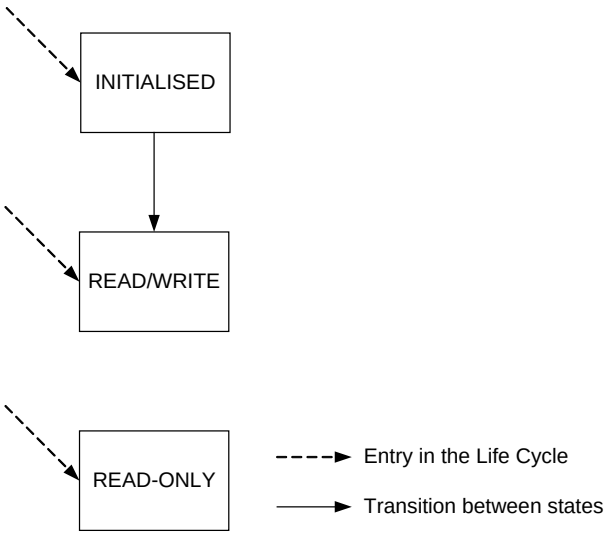


Fig 5. NFC-like Life Cycle

6.2 MIFARE Life Cycle

The MIFARE Classic or MIFARE Plus tag MAY be in additional states than the ones specified in the [ANNFCMF]. These additional states together with the additional transitions and the NFC-like life cycle states and transitions (see Fig 5) form the MIFARE life cycle (see Fig 6).

The additional states are named in Fig 6 using the prefix “MIFARE”. A round square indicates parts of the MIFARE life cycle that corresponds to the NFC-like life cycle (see Fig 5).

To guarantee compatibility with the [ANNFCMF] application note, the MIFARE INITIALISED state, the MIFARE READ/WRITE state, MIFARE BLOCKED READ/WRITE state, MIFARE READ-ONLY state and MIFARE BLOCKED READ-ONLY state are seeing from a Reader device that implements only the [ANNFCMF] specification as INITILIASED state, READ/WRITE state and READ-ONLY state. Table 4 shows the relations between the states defined in [ANNFCMF] (see Fig 5) and the states defined in this application note (see Fig 6).

Table 4. Relation between the [ANNFCMF] states and the states defined by this application note

States detected by a Reader device implementing only the [ANNFCMF] application note	States detected by a Reader device implementing this application note
INITIALISED	INITIALISED
	MIFARE INITIALISED
READ/WRITE	READ/WRITE
	MIFARE READ/WRITE
	MIFARE BLOCKED READ/WRITE
READ-ONLY	READ-ONLY
	MIFARE READ-ONLY
	MIFARE BLOCKED READ-ONLY

For all NFC sectors the INITIALISED, READ/WRITE and READ-ONLY states make use of:

- a secret key B that is kept secret by the Reader device that writes the tag or it is shared between different Reader devices,
- a public Key A of NFC sectors (see Table 6), and
- fixed settings of the access bits in the sector trailer as described in [ANNFCMF].

This NFC sectors are only non-proprietary NFC sectors. I.e. in INITIALISED, READ/WRITE and READ-ONLY state the MIFARE Classic or MIFARE Plus uses the Simple Configuration (see section 2.1).

However some applications may need NFC sectors with:

- a secret Key A that is kept secret by the Reader device that writes the tag or it is shared between different Reader devices and it may be different from NFC sector to NFC sector, and/or
- different settings of the access bits that may be different from NFC sector to NFC sector and different from what is specified by [ANNFCMF].

For this reason the MIFARE INITIALISED, the MIFARE READ/WRITE state, MIFARE BLOCKED READ/WRITE state, MIFARE READ-ONLY state and MIFARE BLOCKED READ-ONLY states have been introduced. These application specific NFC sectors are proprietary NFC sectors. I.e. in MIFARE INITIALISED, MIFARE READ/WRITE, MIFARE BLOCKED READ/WRITE, MIFARE READ-ONLY and MIFARE BLOCKED READ-ONLY state the MIFARE Classic or MIFARE Plus uses the Mixed Configuration (see section 2.1).

Note that in MIFARE INITIALISED state, MIFARE READ/WRITE state, MIFARE BLOCKED READ/WRITE state, MIFARE READ-ONLY state and MIFARE BLOCKED READ-ONLY states, the Reader device SHALL set at least one or more but not all NFC sectors as proprietary ones. Without any proprietary NFC sector(s) the only possible states are INITIALISED, READ/WRITE and READ-ONLY state.

The identification of these states MAY required a failed or successful authentication with key A, being key A secret and unknown at priori to the Reader device.

The entries or Formatting Procedures are exactly the same one shown in the NFC-like life cycle (see section 6.1).

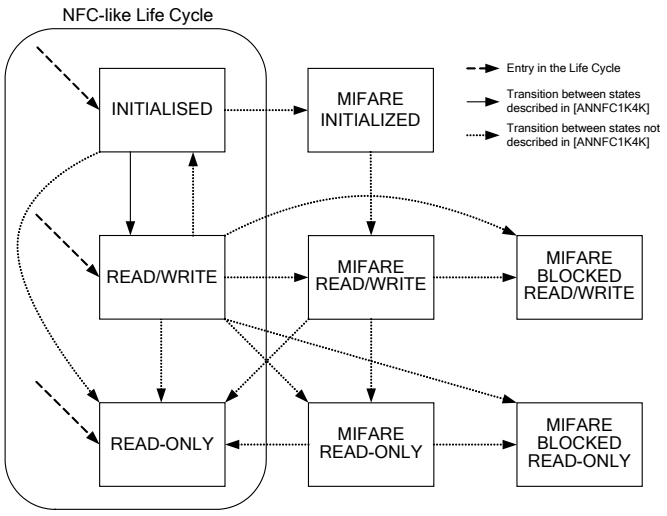


Fig 6. MIFARE life cycle

Looking Fig 6 overall there are 8 states, 3 entries/Formatting Procedures and 15 transitions. It is not compulsory to support all states, entries and transitions in the Reader device. An implementation MAY be tailored to support a subset of states, entries and transitions of the MIFARE life cycle. In Fig 6 the dotted arrows indicate the additional transitions that are not described in the [ANNFCMF].

The differences between the states are based on different settings of:

- sector trailer access bits of MAD sector(s) and NFC sector(s),
- data area access bits of MAD sector(s), and NFC sector(s),
- key A value, and
- length field value of the mandatory NDEF Message TLV.

Table 5 compares the MIFARE life cycle states highlighting the differences between them (see also Table 7 and Table 8). Concerning the meaning of access bits settings (see [MF1K, MF4K]).

The MIFARE life cycle states have the following common settings (see [MF1K, MF4K]):

- Key A for MAD sectors is set as described in Table 9 (see [MAD]).
- Key A of the non-proprietary NFC sector (where the mandatory NDEF Message TLV is contained) is set as described in Table 6.
- Key B of MAD sectors or NFC sectors is either secret or shared within a limited set of Reader devices.

The key B MAY be used to write or read MAD sectors or NFC sectors. The key B of MAD sectors MAY be either different from or equal to key B of NFC sectors.

In Table 5 and in the text below it is referred as:

- sector trailer access bits: the access bits used to set the access configuration of the sector trailer, and
- data area access bits: the access bits used to set the access configuration of the blocks of the sector without the sector trailer.

A TLV block MAY be written using one or more contiguous NFC sectors having the same sector trailer access bits settings, data area access bits settings, Key A and Key B. A TLV block MAY also be written in NFC sectors across the MAD sector 16 e.g. NFC sector 15 and 17 (see also the definition of contiguous NFC sectors in section 6.1 of [ANNFCMF]).

A TLV block SHALL NOT be written using one or more NFC sectors with different sector trailer access bits settings, data area access bits settings, Key A or Key B. To respect this rule the NULL TLV MAY be used to shift the TLV blocks. In other words a whole TLV block SHALL be written into either non-proprietary or proprietary NFC sectors. A TLV block SHALL NOT be written across both non-proprietary and proprietary NFC sectors.

The addition and/or deletion of non-mandatory NDEF Message TLVs, and Proprietary TLVs MAY be performed in any transition, and in any state except the READ-ONLY state. These operations MAY change the state of the MIFARE Classic or MIFARE Plus tag.

A more comprehensive description of the states is given in section 6.3.

Table 5. Comparative table between the different states

STATE	Sector Trailer Access bits ($C1_3$ $C2_3$ $C3_3$)			Data Area Access Bits ($C1_{0,1,2}$ $C2_{0,1,2}$ $C3_{0,1,2}$)			Key A of proprietary NFC sector	Length Field Value of Mandatory NDEF Message TLV
	MAD Sector Trailer Access Bits	Sector Trailer Access Bits of the non-proprietary NFC sectors	Sector Trailer Access Bits of proprietary NFC sector	MAD data area Access Bits	Data area Access Bits of the non-proprietary NFC sector	Data area Access Bits of the proprietary NFC sector		
INITIALISED	011b	011b	N.A.[3]	100b	000b	N.A.[3]	N.A.[3]	00h
MIFARE INITIALISED	011b	011b	Any value[1]	100b	000b	Any value[1]	Table 6 or Secret[2]	00h
READ/WRITE	011b	011b	N.A.[3]	100b	000b	N.A.[3]	N.A.[3]	≠00h
MIFARE READ/WRITE	011b	011b	Any value[1]	100b	000b	Any value[1]	Table 6 or Secret[2]	≠00h
MIFARE BLOCKED READ/WRITE	110b	110b	110b	010b	000b	Any value[1]	Table 6 or Secret[2]	≠00h
READ-ONLY	110b	110b	N.A.[3]	010b	010b	N.A.[3]	N.A.[3]	≠00h
MIFARE READ-ONLY	011b	110b	Any value[1]	100b	010b	Any value[1]	Table 6 or Secret[2]	≠00h
MIFARE BLOCKED READ-ONLY	110b	110b	110b	010b	010b	Any value[1]	Table 6 or Secret[2]	≠00h

[1] The value for the access bits MAY be chosen in the range from 000b to 111b independently for each proprietary NFC sector. Some combinations MAY identify a different state (see section 6.3).

[2] Key A for proprietary NFC sectors (NOT containing the mandatory NDEF Message TLV) MAY be secret and it MAY be shared within a limited set of Reader devices. Note that to check the value of the Key A only a try-fail approach can be used, performing one or more Authentication operations with different Key A values.

[3] N.A. Not Applicable. In INITIALISED, READ/WRITE and READ-ONLY state only non-proprietary NFC sector(s) are present.

Table 6. NFC sector Public Key A

Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5
D3h	F7h	D3h	F7h	D3h	F7h

[4] The byte number on the header row indicates the bite number of the sector trailer.

Table 7. Access Bits Settings for Sector Trailer, see also [MF1K, MF4K]

Access bits			Access condition for					
			KEY A		Access bits		KEY B	
$C1_{0,1,2}$	$C2_{0,1,2}$	$C3_{0,1,2}$	read	write	read	write	read	write
0b	1b	1b	never	Key B	Key A or B	Key B	never	Key B
1b	1b	0b	never	never	Key A or B	never	never	never

[5] Note: see ANNEX 9 and 10 for byte values of the access bits.

Table 8. Access Bits Settings for Data Area, see also [MF1K, MF4K, MFPLUS]

Access bits			Access condition for	
$C1_{0,1,2}$	$C2_{0,1,2}$	$C3_{0,1,2}$	read	write
0b	0b	0b	Key A or B	Key A or B
0b	1b	0b	Key A or B	Never
1b	0b	0b	Key A or B	Key B
1b	1b	0b	Key A or B	Key B
0b	0b	1b	Key A or B	Never
0b	1b	1b	Key B	Key B
1b	0b	1b	Key B	Never
1b	1b	1b	never	Never

[6] Note: see ANNEX 9 and 10 for byte values of the access bits.

Table 9. Public Key A settings to access MAD sectors

Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5
A0h	A1h	A2h	A3h	A4h	A5h

[7] The byte number on the header row indicates the bite number of the sector trailer.

In the [ANNFCMF] the INITIALISED, READ/WRITE and READ/ONLY states are identified using the General Purpose Bytes (GPB) of the non-proprietary NFC sector where the mandatory NDEF Message TLV starts and the length filed value of the mandatory NDEF Message TLV. However to identify any of the 8 MIFARE Classic 1k/4k states only the following parameters SHALL be used (see Table 5):

- the settings of the sector trailer access bits of MAD sectors,
- the settings of the data area access bits of MAD sectors,
- the settings of the sector trailer access bits of non-proprietary NFC sectors,
- the settings of the data area access bits of non-proprietary NFC sectors,
- the settings of the sector trailer access bits of proprietary NFC sectors,
- the settings of the data area access bits of proprietary NFC sectors,
- the key A value, and
- the length field value of the mandatory NDEF Message TLV (note that the mandatory NDEF Message TLV is always contained into non-proprietary NFC sector).

Note that to check the value of the key A only a try-fail approach can be used, performing one or more Authentication operations with different key A values. In fact it is not possible to read the key A value from the sector trailer using the Read operation (see also [MF1K, MF4K, MFPLUS]).

6.2.1 Setting of Write and Read Access Condition Field of the GPB of each NFC sector

The Reader device SHALL set the write and read access condition field (2 bits field) of the GPB of each NFC sector following the rule on Table 10.

Table 10. Setting of the write and read access condition field (2 bits field) of the GPB

GPB setting in the Read / Write Access conditions (2bits)			
Read Access conditions (2 bits)		**Write Access conditions (2 bits)**	
Non-proprietary NFC sector	**Proprietary NFC sector**	**Non-proprietary NFC sector[1]**	**Proprietary NFC sector**
00b	01b	00b or 11b	01b

[1] The write access condition depends on the state:

a) in INITIALISED, MIFARE INITIALISED, READ/WRITE, MIFARE READ/WRITE and MIFARE BLOCKED READ/WRITE, the write access conditions of the non-proprietary NFC sectors is equal to 00b, and

b) in READ-ONLY, MIFARE READ-ONLY and MIFARE BLOCKED READ-ONLY, the write access conditions of the non-proprietary NFC sectors is equal to 11b.

The proprietary NFC sectors are identified by:

- the read and write access conditions of the GPB equal to 01b, and
- the Key A value different from the public Key A for NFC sectors.

Concerning the GPBs of the non-proprietary NFC sectors (that contains the mandatory NDEF Message TLV), the read access condition is always set to 00b and the write access condition is set to either 00b or 11b depending on the state.

6.3 States

This section completes the settings for each MIFARE Classic or MIFARE Plus state that are described in the previous section 6.2 and Table 5. The common settings of all states are described in the previous section 6.2. Also the common settings SHALL be checked to detect the MIFARE Classic or MIFARE Plus in a valid state.

6.3.1 INITIALISED State

The INITIALISED state is the state where the mandatory NDEF Message TLV is empty (Length field equal to 00h). The Formatting Procedure to prepare the MIFARE Classic or MIFARE Plus tag in this state is described in section 6.5.1.

A MIFARE Classic or MIFARE Plus tag SHALL be detected in INITIALISED state when:

1. the access bits for MAD and NFC sectors follow Table 5:
   a. the sector trailers of all MAD and NFC sectors and the data area of the MAD sectors are readable authenticating with key A or key B and writable only authenticating with Key B, and
   b. the data area of the NFC sectors is read/write authenticating with key A or key B.
2. the key A of NFC sector(s) is equal to Table 6, and
3. the length field value of the mandatory NDEF Message TLV is equal to 00h.

In INITIALISED state all NFC sectors are non-proprietary NFC sectors.

6.3.2 MIFARE INITIALISED State

The MIFARE INITIALISED state is a special case of the INITIALISED state.

A MIFARE Classic or MIFARE Plus tag SHALL be detected in MIFARE INITIALISED state when:

1. the data area and sector trailer access bits of MAD sector(s) are set as described in Table 5,
2. the data area and sector trailer access bits of proprietary and non NFC sector(s) are set as described in Table 5,
3. Key A value for the proprietary NFC sector(s) MAY be:
   a. Secret. The authentication with key A fails because one or more proprietary NFC sectors use a Key A different from the one defined in Table 6 or not known by the Reader device or
   b. Known by the Reader device i.e. key A is equal to that one defined in Table 6 or different but known by the Reader device, and
4. the length field value of the mandatory NDEF Message TLV is equal to 00h.

A MIFARE Classic or MIFARE Plus tag in MIFARE INITIALISED state MAY have the proprietary NFC sectors with:

- Sector trailer access bits set to any value i.e. from 000b to 111b, and
- Data area access bits set to any value i.e. from 000b to 111b.

For proprietary NFC sector when key A is the public one (see Table 6), it is STRONGLY RECOMMENDED to avoid the combinations of sector trailer access bits that allow writing the sector trailer using key A: ($C1_3$ $C2_3$ $C3_3$) equal to 000b, 010b and 001b.

A Reader device that implements only the [ANNFCMF] specification detects in INITIALISED state a MIFARE Classic or MIFARE Plus tag that is MIFARE INITIALISED state.

The MIFARE INITALISED state MAY be used to protect Proprietary TLVs or Non-mandatory NDEF Message TLVs making the relative (proprietary) NFC sectors read-only, but keeping the remaining (non-proprietary) ones readable and writeable to store the mandatory NDEF Message TLV and the Terminator TLV.

6.3.3 READ/WRITE State

The READ/WRITE state is the state where the mandatory NDEF Message TLV contains NDEF data (Length field different from 00h). The Formatting Procedure to prepare the MIFARE Classic or MIFARE Plus tag in this state is described in section 6.5.2.

A MIFARE Classic or MIFARE Plus tag SHALL be detected in READ/WRITE state when:

1. the access bits for MAD and NFC sectors follow Table 5 i.e. the sector trailer for all sectors and the data area of MAD sectors are readable authenticating with Key A or B and writable authenticating with Key B, and the data area of NFC sectors is read/write authenticating with Key A or B.
2. the Key A of NFC sector is equal to Table 6, and
3. the length field value of the mandatory NDEF Message TLV is different from 00h.

In READ/WRITE state all NFC sectors are non-proprietary NFC sectors.

6.3.4 READ-ONLY State

In READ-ONLY state the MAD sector(s) and NFC sector(s) are read-only. The Formatting Procedure to prepare the MIFARE Classic or MIFARE Plus tag in this state is described in section 6.5.3.

A MIFARE Classic or MIFARE Plus tag SHALL be detected in READ-ONLY state when:

1. the access bits for MAD and NFC sectors follow Table 5 i.e. data area and sector trailer of MAD and NFC sectors are read-only authenticating with public Key A or secret Key B, and
2. the length field value of the mandatory NDEF Message TLV is different from 00h.

In READ-ONLY state all NFC sectors are non-proprietary NFC sectors.

6.3.5 MIFARE READ/WRITE State

The MIFARE READ/WRITE state is a special case of the READ/WRITE state.

A MIFARE Classic or MIFARE Plus tag SHALL be detected in MIFARE READ/WRITE state when:

1. the data area and sector trailer access bits of MAD sector(s) are set as described in Table 5,
2. the data area and sector trailer access bits of proprietary and non NFC sectors are set as described in Table 5,
3. Key A value for the proprietary NFC sector(s) MAY be:
   a. Secret. The authentication with Key A fails because one or more proprietary NFC sectors use a Key A different from the one defined in Table 6 or not known by the Reader device or
   b. Known by the Reader device i.e. Key A is equal to that one defined in Table 6 or different but known by the Reader device, and
4. the length field value of the mandatory NDEF Message TLV is different from 00h.

A MIFARE Classic or MIFARE Plus tag in MIFARE READ/WRITE state MAY have the proprietary NFC sectors with:

- Sector trailer access bits set to any value i.e. from 000b to 111b, and
- Data area access bits set to any value i.e. from 000b to 111b.

For proprietary NFC sectors when key A is the public one (see Table 6), it is STRONGLY RECOMMENDED to avoid the combinations of sector trailer access bits that allow writing the sector trailer using key A: ($C1_3$ $C2_3$ $C3_3$) equal to 000b, 010b and 001b.

A Reader device that implements only the [ANNFCMF] specification detects in READ/WRITE state a MIFARE Classic or MIFARE Plus tag that is MIFARE READ/WRITE state.

The MIFARE READ/WRITE state MAY be used to protect Proprietary TLVs or Non-mandatory NDEF Message TLVs making the relative (proprietary) NFC sectors read-only, but keeping the remaining (non-proprietary) ones readable and writeable to store the mandatory NDEF Message TLV and the Terminator TLV.

6.3.6 MIFARE BLOCKED READ/WRITE State

The MIFARE BLOCKED READ/WRITE state is a special case of the READ/WRITE state. In this state the access configurations of the NFC sectors and MAD sectors are blocked.

In MIFARE BLOCKED READ/WRITE state, the differences compared to MIFARE READ/WRITE state are:

- the setting of the access bits of all NFC sector trailers is 110b,
- the setting of the access bits of all MAD sector trailers is 110b, and
- the setting of the access bits of all MAD data area is 010b.

A MIFARE Classic or MIFARE Plus tag SHALL be detected in MIFARE BLOCKED READ/WRITE state when:

1. the data area and sector trailer access bits of MAD sector(s) are set as described in Table 5,
2. the data area and sector trailer access bits of proprietary and non NFC sectors are set as described in Table 5,
3. Key A value of the proprietary NFC sectors MAY be:
   a. Secret. The authentication with Key A fails because one or more proprietary NFC sectors use a Key A different from the one defined in Table 6 or not known by the Reader device, or
   b. Known by the Reader device i.e. Key A is equal to that one defined in Table 6 or different but known by the Reader device, and
4. the length field value of the mandatory NDEF Message TLV is different from 00h.

A MIFARE Classic or MIFARE Plus tag in MIFARE BLOCKED READ/WRITE state MAY have the proprietary NFC sectors with data area access bits set to any value i.e. from 000b to 111b.

A Reader device that implements only the [ANNFCMF] specification detects in READ/WRITE state a MIFARE Classic or MIFARE Plus tag in MIFARE BLOCKED READ/WRITE state.

The MIFARE BLOCKED READ/WRITE state MAY be used to protect Proprietary TLVs or Non-mandatory NDEF Message TLVs making the relative (proprietary) NFC sectors read-only, but keeping the remaining (non-proprietary) ones readable and writeable to store the mandatory NDEF Message TLV and Terminator TLV.

6.3.7 MIFARE READ-ONLY State

The MIFARE READ-ONLY state is a special case of the READ-ONLY one.

A MIFARE Classic or MIFARE Plus tag SHALL be detected in MIFARE READ-ONLY state when:

1. the data area and sector trailer access bits of MAD sector(s) are set as described in Table 5,
2. the data area and sector trailer access bits of proprietary and non NFC sectors are set as described in Table 5,
3. Key A value of proprietary NFC sectors MAY be:
   a. Secret. The authentication with Key A fails because one or more NFC sectors use a Key A different from the one defined in Table 6 or not known by the Reader device or
   b. Known by the Reader device i.e. Key A is equal to that one defined in Table 6 or different but known by the Reader device, and
4. the length field value of the mandatory NDEF Message TLV is different from 00h.

A MIFARE Classic or MIFARE Plus tag in MIFARE READ-ONLY state MAY have the proprietary NFC sectors with:

- Sector trailer access bits set to any value i.e. from 000b to 111b, and
- Data area access bits set to any value i.e. from 000b to 111b.

For proprietary NFC sector when key A is the public one (see Table 6), it is STRONGLY RECOMMENDED to avoid the combinations of sector trailer access bits that allow writing the sector trailer using key A: ($C1_3$ $C2_3$ $C3_3$) equal to 000b, 010b and 001b.

A Reader device that implements only the [ANNFCMF] specification detects in READ-ONLY state a MIFARE Classic or MIFARE Plus tag that is MIFARE READ-ONLY state.

The MIFARE READ-ONLY state MAY be used to keep readable and writeable Proprietary TLVs or Non-mandatory NDEF Message TLVs making the relative (proprietary) NFC sectors readable and writeable, but keeping the remaining (non-proprietary) ones read-only where the mandatory NDEF Message TLV and Terminator TLV are stored.

6.3.8 MIFARE BLOCKED READ-ONLY State

The MIFARE BLOCKED READ-ONLY state is a special case of the READ-ONLY state. In this state the access configurations of the NFC sectors and MAD sectors are blocked.

In MIFARE BLOCKED READ-ONLY state, the differences compared to MIFARE READ-ONLY state are:

- the setting of the access bits of all NFC sector trailers is 110b,
- the setting of the access bits of all MAD sector trailers is 110b, and
- the setting of the access bits of all MAD data area is 010b.

A MIFARE Classic or MIFARE Plus tag SHALL be detected in MIFARE BLOCKED READ-ONLY state when:

1. the data area and sector trailer access bits of MAD sector(s) are set as described in Table 5,
2. the data area and sector trailer access bits of proprietary and non NFC sectors are set as described in Table 5,
3. Key A value of proprietary NFC sectors MAY be:
   a. Secret. The authentication with Key A fails because one or more proprietary NFC sectors use a Key A different from the one defined in Table 6 or not known by the Reader device or
   b. Known by the Reader device i.e. Key A is equal to that one defined in Table 6 or different but known by the Reader device, and
4. the length field value of the mandatory NDEF Message TLV is different from 00h.

A MIFARE Classic or MIFARE Plus tag in MIFARE BLOCKED READ-ONLY state MAY have the proprietary NFC sectors with data area access bits set to any value i.e. from 000b to 111b.

A Reader device that implements only the [ANNFCMF] specification detects in READ-ONLY state a MIFARE Classic or MIFARE Plus tag in MIFARE BLOCKED READ-ONLY state.

The MIFARE BLOCKED READ-ONLY state MAY be used to make writeable or read/write protected Proprietary TLVs or Non-mandatory NDEF Message TLVs making

the relative (proprietary) NFC sectors readable and writable, but keeping the remaining (non-proprietary) ones read-only where the mandatory NDEF Message TLV and the Terminator TLV is stored.

6.4 State Changes/Transitions

This section describes the possible state changes (also called transitions) of the MIFARE life cycle. Fig 6 shows the states and the state changes between them. Only the MIFARE Classic transitions are described in the sections below (i.e. dotted arrows in Fig 6).

For each sector before using the Write or Read operations, the Authentication operation SHALL be provided to authenticate the relative sector using key A or key B.

It SHALL be checked that the state of the MIFARE Classic or MIFARE Plus tag is in a valid state (see section 6.2 and 6.3). If the MIFARE Classic or MIFARE Plus tag is in a valid state, any transitions described below and in [ANNFCMF] from that state can be performed.

6.4.1 Transitions from INITIALISED to MIFARE INITIALISED

The transition from INITIALISED to MIFARE INITIALISED is defined as any command sequence that:

- does not change the access bit settings of the MAD sectors,
- does not change the access bit settings of the non-proprietary NFC sectors containing the mandatory NDEF Message TLV,
- change:
  - the access bit settings of any non-proprietary NFC sector that does not contain the mandatory NDEF Message TLV (note that the NFC sectors become proprietary NFC sectors), or/and
  - Key A of any non-proprietary NFC sector that does not contain the mandatory NDEF Message TLV (note that the NFC sectors become proprietary NFC sectors),
- set the GPB of each new proprietary NFC sector according to section 6.2.1 and Table 10, and
- changes the NFC sector configuration from the Simple configuration to the Mixed configuration (see section 2.1).

6.4.2 Transitions from MIFARE INITIALISED to MIFARE READ/WRITE

To perform the transition from MIFARE INITIALISED to MIFARE READ/WRITE state the Reader device SHALL:

1. Detect the mandatory NDEF Message TLV using the NDEF Detection Procedure described in [ANNFCMF].
2. Write an NDEF Message into the mandatory NDEF Message TLV.

6.4.3 Transition from READ/WRITE to INITIALSED

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

To perform the transition from READ/WRITE to INITIALISED state the Reader device SHALL:

1. Detect the mandatory NDEF Message TLV using the NDEF Detection Procedure described in [ANNFCMF].

2. Replace the mandatory NDEF Message TLV with an empty NDEF Message TLV (i.e. length field equal to 00h, and no value field) using the one or more Write operations.
3. Write the Terminator TLV in the first byte after the mandatory NDEF Message TLV using the Write operation.

The transition invalidates but does not delete all data written after the Terminator TLV that was present before. To really delete and clear all the data bytes after the Terminator TLV a sequence of Write operations and Authentication operations (when there are more than one NFC sector) SHALL be used.

6.4.4 Transitions from READ/WRITE to READ-ONLY

The transition from READ/WRITE to READ-ONLY requires the knowledge of the secret key B.

To perform the transition from READ/WRITE to READ-ONLY state the Reader device SHALL do the following operations authenticating the relative sector with the secret key B:

1. For each MAD sector the access bits of sector trailer block SHALL be set as described in Table 5 (i.e. access bits setting for MAD sector with read-only access granted).
2. For each non-proprietary NFC sector the access bits of the sector trailer SHALL be set as described in Table 5 (i.e. access bit setting for NFC sectors with read-only access granted), and bit 0-1 of the GPB SHALL be set to 11b (i.e. write access not granted, only read access granted).

To set the access bits of different MAD sectors and NFC sectors one or more Write operation SHALL be used. For the write operation the reading of not completely updated blocks is needed first (see section 5.1.4 of [ANNFCMF]).

6.4.5 Transition from INITIALISED to READ-ONLY

To perform the transition from INITIALISED to READ-ONLY, the Reader device SHALL:

- write of a non-empty NDEF Message using the transition from INITLIASED to READ/WRITE as defined in section 6.4.4.1 of [ANNFCMF], and
- apply the transition from READ/WRITE to READ-ONLY described in section 6.4.4.

6.4.6 Transitions from READ/WRITE to MIFARE READ/WRITE

The transition from READ/WRITE to MIFARE READ/WRITE is defined as any command sequence that:

- does not change the access bit settings of the MAD sectors,
- does not change the access bit settings of non-proprietary NFC sectors containing the mandatory NDEF Message TLV,
- MAY change:
  - the access bit settings of any non-proprietary NFC sector that does not contain the mandatory NDEF Message TLV (note that the NFC sectors become proprietary NFC sectors), or/and
  - changes Key A of any non-proprietary NFC sector that does not contain the mandatory NDEF Message TLV (note that the NFC sectors become proprietary NFC sectors),
- set the GPB of each NFC sector according to section 6.2.1 and Table 10, and

- changes the NFC sector configuration from the Simple configuration to the Mixed configuration (see section 2.1).

6.4.7 Transitions from MIFARE READ/WRITE to MIFARE BLOCKED READ/WRITE

The transition from MIFARE READ/WRITE to MIFARE BLOCKED READ/WRITE is defined as any command sequence that:

- set all the access bits of the sector trailer of the MAD sectors to 110b,
- set all the access bits of the data area of the MAD sectors to 010b, and
- set all the access bits of the sector trailer of all the NFC sectors to 110b.

It is possible that specific proprietary NFC sectors are blocked or they MAY have a secret Key A different from that one define in Table 6, or they share a secret Key B. In this case it might not be possible to perform the transition to MIFARE BLOCKED READ/WRITE.

6.4.8 Transitions from READ/WRITE to MIFARE BLOCKED READ/WRITE

The transition from READ/WRITE to MIFARE BLOCKED READ/WRITE is defined as any command sequence that:

- set all the access bits of the sector trailer of the MAD sectors to 110b,
- set all the access bits of the data area of the MAD sectors to 010b,
- set all the access bits of the sector trailer of all the NFC sectors to 110b,
- MAY change:
  - the data area access bit settings of any non-proprietary NFC sector that does not contain the mandatory NDEF Message TLV (note that the NFC sectors become proprietary NFC sectors), and/or
  - change Key A of any non-proprietary NFC sector that does not contain the mandatory NDEF Message TLV (note that the NFC sectors become proprietary NFC sectors),
- set the GPB of each NFC sector according to section 6.2.1 and Table 10, and
- changes the NFC sector configuration from the Simple configuration to the Mixed configuration (see section 2.1).

6.4.9 Transitions from READ/WRITE to MIFARE BLOCKED READ-ONLY

The transition from READ/WRITE to MIFARE BLOCKED READ-ONLY is defined as any command sequence that:

- set all the access bits of the sector trailer of the MAD sectors to 110b,
- set all the access bits of the data area of the MAD sectors to 010b,
- set the access bits of the sector trailer of the non-proprietary NFC sectors to 110b,
- set the access bits of the data area of the non-proprietary NFC sectors to 010b that contain the mandatory NDEF Message TLV,
- MAY change
  - the data area access bit settings of any non-proprietary NFC sector that does not contain the mandatory NDEF Message TLV (note that the NFC sectors become proprietary NFC sectors), and/or
  - change Key A of any non-proprietary NFC sector that does not contain the mandatory NDEF Message TLV (note that the NFC sectors become proprietary NFC sectors),

- set the GPB of each non-proprietary NFC sector according to section 6.2.1 and Table 10, and in particular setting bit 0-1 of the GPB to 11b (i.e. write access not granted), and
- set the GPB of each proprietary NFC sector according to section 6.2.1 and Table 10.

6.4.10 Transitions from MIFARE READ/WRITE to MIFARE READ-ONLY

The transition from MIFARE READ/WRITE to MIFARE READ-ONLY is defined as any command sequence that:

- set the access bits of the sector trailer of the non-proprietary NFC sectors to 110b,
- set the access bits of the data area of the non-proprietary NFC sectors to 010b, and
- set the GPB of each non-proprietary NFC sector according to section 6.2.1 and Table 10, and in particular setting bit 0-1 of the GPB to 11b (i.e. write access not granted).

6.4.11 Transitions from MIFARE READ/WRITE to READ-ONLY

The transition from MIFARE READ/WRITE to READ-ONLY SHALL be equal to the transition from READ/WRITE to READ-ONLY (see section 6.4.4) except from access bits that are already set correctly.

Specific proprietary NFC sectors may be blocked or they may have a secret Key A different from that one define in Table 6, or they share a secret Key B. In this case it might not be possible to perform the transition to READ-ONLY because the settings of access bits, Key A and Key B are not respected.

6.4.12 Transitions from READ/WRITE to MIFARE READ-ONLY

The transition from READ/WRITE to MIFARE READ-ONLY is defined as any command sequence that:

- execute the transition from READ/WRITE to MIFARE READ/WRITE (see section 6.4.6), and
- execute the transition from MIFARE READ/WRITE to MIFARE READ-ONLY (see section 6.4.10).

6.4.13 Transitions from MIFARE READ-ONLY to READ-ONLY

The transition from MIFARE READ-ONLY to READ-ONLY SHALL be equal to the transition from READ/WRITE to READ-ONLY (see section 6.4.4) except from access bits that are already set correctly.

Specific proprietary NFC sectors may be blocked or they may have a secret Key A different from that one define in Table 6, or they share a secret Key B. In this case it might not be possible to perform the transition to READ-ONLY because the settings of access bits, Key A and Key B are not respected.

6.4.14 Transitions from MIFARE READ-ONLY to MIFARE BLOCKED READ-ONLY

The transition from MIFARE READ-ONLY to MIFARE BLOCKED READ-ONLY is defined as any command sequence that:

- set all the access bits of the sector trailer of all NFC sectors to 110b,
- set all the access bits of the sector trailer of all MAD sectors to 110b, and
- set all the access bits of the data area of all MAD sectors to 010b.

It is possible that specific proprietary NFC sectors may be blocked or they may have a secret Key A different from that one define in Table 6, or they share a secret Key B. In this case it might not be possible to perform the transition to MIFARE BLOCKED READ-ONLY because the settings of access bits, Key A and Key B are not respected.

6.5 Formatting Procedures

In this application note the Formatting Procedures for MIFARE Classic or MIFARE Plus tag SHOULD be used to prepare the tag after production phase (i.e. blank tag) in INITIALISED, READ/WRITE and READ-ONLY state. The Formatting Procedures are executed after a successful Card Identification Procedure for MIFARE Classic or MIFARE Plus tag after production phase (see section 2.3 and 2.3.1).

The mandatory NDEF Message TLV SHALL be written during the Formatting Procedures. It is left to the implementers to modify the Formatting Procedures to include the writing of proprietary NFC sectors, additional NDEF Message TLV, Proprietary TLVs etc. This modified Formatting Procedure SHALL always set the NFC sector(s) in one of the MIFARE life cycle state.

6.5.1 INITIALISED Formatting Procedure

The INITIALISED Formatting Procedure described herein SHOULD be used to prepare the tag to store NDEF data (e.g. NDEF message) in INITIALISED state (see section 6.3.1). After this procedure the MIFARE Classic or MIFARE Plus tag contains the empty mandatory NDEF Message TLV and the Terminator TLV.

The INITIALISED Formatting Procedure sets the Simple Configuration (see section 2.1 into the MIFARE Classic or MIFARE Plus.

It is assumed that the MIFARE Classic or MIFARE Plus tag is configured to allow the INITIALISED Formatting Procedure e.g. unmodified delivery state or blank state. The sectors SHALL be authenticated using the Authentication operation (see chapter 5) before reading or writing them. For authenticating the key A or the key B SHALL be selected based on the indication provided by the Card Identification Procedure for MIFARE Classic or MIFARE Plus tag after production phase (see section 2.3.1).

The INITIALISED Formatting Procedure is described below and in Fig 7. During this procedure the Reader device SHALL (see [MF1K, MF4K, MFPLUS] for command details):

1. Use the Authentication operation and Write operation to prepare the MAD sector(s) as described in the [MAD] document and writing at least one field of the MIFARE Application Directory (MAD) with the NFC application identifier i.e. NFC AID 03E1h. If more than one NFC AID are written, they SHALL be indicate contiguous NFC sectors (in case of MIFARE Classic 4k or MIFARE Plus with 4 Kbyte, it SHALL be considered contiguous a sequence of NFC sectors that includes the MAD sector 16 as well, see section 6.1 of [ANNFCMF]).
2. Use the Authentication operation and Write operation to:
   a. set key A equal to the public key A of NFC sector (see Table 6), and the secret Key B for each NFC sector,
   b. write the access bits and GPB of the sector trailer of all NFC sector as described in section 6.2 and 6.3.1 for each NFC sector,
   c. write in the first (i.e. smallest in term of sector number) NFC sector an empty (the mandatory) NDEF Message TLV i.e. NDEF Message TLV with L field equal to 00h.

d. write after the NDEF Message TLV the Terminator TLV. Between the NDEF Message TLV and the Terminator TLV one or more NULL TLVs MAY be written.

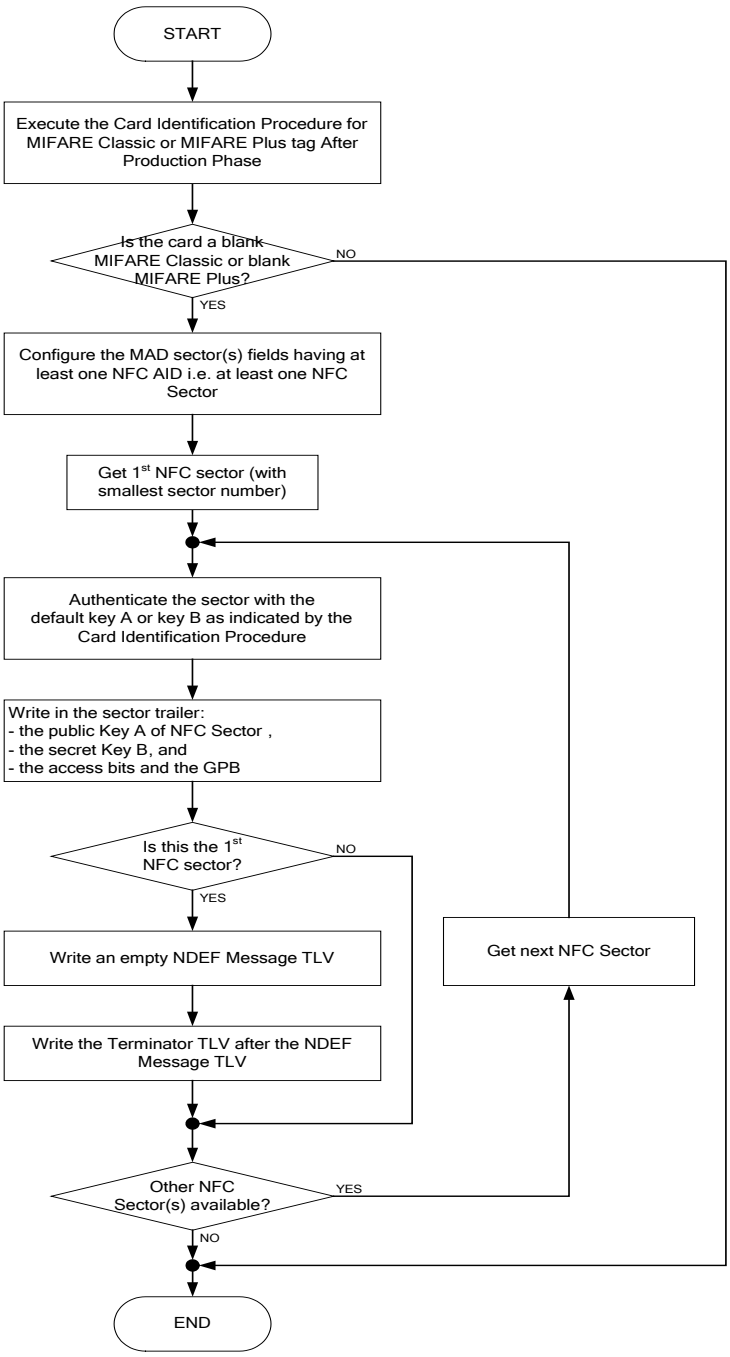


Fig 7. INITIALISED Formatting Procedure

6.5.2 READ/WRITE Formatting Procedure

The READ/WRITE Formatting Procedure SHOULD be used to prepare the tag in READ/WRITE state (see section 6.3.1). After this procedure the MIFARE Classic or MIFARE Plus tag contains the mandatory NDEF Message TLV and the Terminator TLV.

The READ/WRITE Formatting Procedure sets the Simple Configuration (see section 2.1) in the MIFARE Classic or MIFARE Plus.

To perform the READ/WRITE Formatting Procedure the Reader device SHALL:

1. execute the INITIALISED Formatting Procedure (see section 6.5.1), and
2. execute the transition from INITIALISED to READ/WRITE (see [ANNFCMF]).

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

6.5.3 READ-ONLY Formatting Procedure

The READ-ONLY Formatting Procedure SHOULD be used to prepare the tag in READ-ONLY state (see section 6.3.1). After this procedure the MIFARE Classic or MIFARE Plus tag contains a mandatory NDEF Message TLV and the Terminator TLV.

The READ/ONLY Formatting Procedure sets the Simple Configuration (see section 2.1) in the MIFARE Classic or MIFARE Plus.

To perform the READ-ONLY Formatting Procedure the Reader device SHALL:

1. execute the INITIALISED Formatting Procedure (see section 6.5.1),
2. execute the transition from INITIALISED to READ/WRITE (see [ANNFCMF]), and
3. execute the transition from READ/WRITE to READ-ONLY (see section 6.4.4).

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 Classic or MIFARE Plus MAY support. Even implementing these features the MIFARE Classic or MIFARE Plus SHALL remain compatible with the application note [ANNFCMF].

7.1 Several NDEF Message TLVs and Several Proprietary TLVs

A MIFARE Classic or MIFARE Plus tag MAY contain one or more NDEF Message TLVs and zero, one or more Proprietary TLVs (see [ANNFCMF]). Reader devices compliant to [ANNFCMF] specification are able to read only the mandatory NDEF Message TLV, and no Proprietary TLVs.

7.2 MIFARE READ/WRITE and MIFARE BLOCKED READ/WRITE

The MIFARE READ/WRITE state is used to make read-only or restrict the access to specific NFC sectors of the MIFARE Classic or MIFARE Plus tag.

For instance the proprietary NFC sectors related to the non-mandatory NDEF Message TLV(s) or the Proprietary TLV(s) can be made read-only to avoid future changes. The NULL TLV can be used to completely fill the sectors containing these TLV blocks (see example in section 8.2 ANNEX A) avoiding to partially make read-only other TLV blocks that are written across two or more NFC sectors.

The MIFARE BLOCKED READ/WRITE state is used to make read-only the access configuration of the MIFARE Classic or MIFARE Plus tag. An example where this state can be used is to avoid malicious or accidental changes of the access configurations (i.e. sector trailers) of proprietary NFC sectors containing Proprietary TLVs, or Non-mandatory NDEF Message TLVs.

7.3 MIFARE READ-ONLY , and MIFARE BLOCKED READ-ONLY

The MIFARE READ-ONLY state is used to avoid to make read-only specific sectors of the MIFARE Classic or MIFARE Plus tag.

For instance the proprietary NFC sectors related to the mandatory NDEF Message TLV can be made read-only to avoid future changes, instead sectors containing non-mandatory NDEF Message TLVs or the Proprietary TLVs MAY be kept read/write. The NULL TLV MAY be used be used to completely fill the sectors containing these TLV blocks avoiding to partially make read-only other TLV blocks that are written across two or more NFC sectors.

The MIFARE BLOCKED READ-ONLY state is used to make read-only the access configuration of the MIFARE Classic or MIFARE Plus tag keeping the write access for specific sectors. An example where this state can be used is to avoid malicious or accidental changes of the access configuration of proprietary NFC sectors that contain the Non-mandatory NDEF Message TLVs and the Proprietary TLVs.

7.4 Storing of Additional non-TLV Structured Data

The data can be stored inside a MIFARE Classic or MIFARE Plus tag in two different ways apart from using the Proprietary TLV or the NDEF Message TLV (see [ANNFCMF]):

- Writing the data after the Terminator TLV (see section 7.4.1), or
- Using the MAD and the Application Identifiers to specify the data inside one or more sectors that are not NFC sectors (see section 7.4.2).

The information of the existence of the data can be application specific or MAY be provided using the MAD.

7.4.1 Writing the Data after the Terminator TLV

The description of writing the data after the Terminator TLV is given by means of the example in Fig 8. Fig 8 does not show the different sectors (e.g. MAD sector), blocks, sector trailers and manufacturer block, but just described all NFC sectors as a single memory area.

In the example two data areas called Any Data 1 and Any Data 2 are stored after the Terminator TLV. The information about the position and size inside the MIFARE Classic or MIFARE Plus tag are stored inside record 1 and record 2 of the NDEF Message encapsulated inside the NDEF Message TLV located before the NDEF Message TLV.

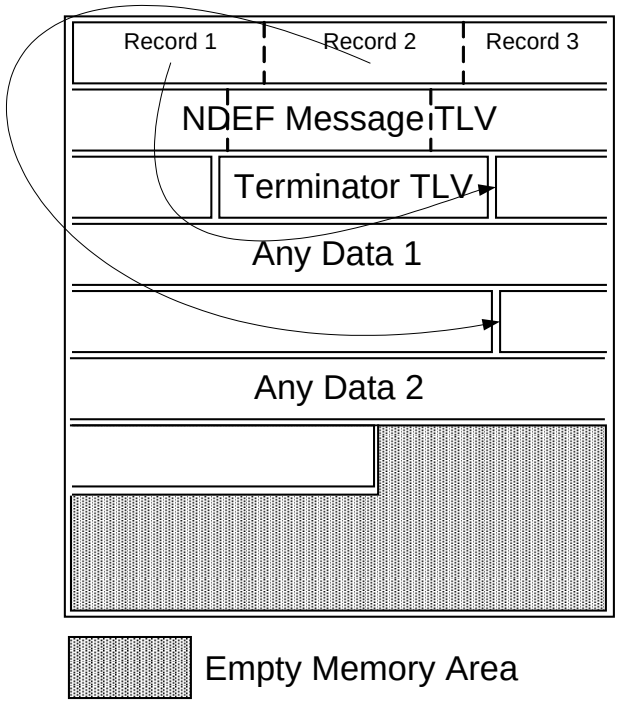


Fig 8. Example of data located after the Terminator TLV

7.4.2 Specifying the Any Data using the MAD and the Application Identifiers

Using the MAD it is possible to store different application data inside the MIFARE Classic or MIFARE Plus tag using Application Identifiers (AIDs) different from the NFC AID. The sectors identified by these AIDs are not NFC sectors but application specific.

For more information see [MAD].

8. ANNEX A: Examples

In this chapter two examples are given regarding the INITIALISED Formatting procedure (see section 6.5.1) and a transition from INITIALISED to MIFARE BLOCKED READ/WRITE. Both examples uses the MIFARE Classic 1k (see [MF1K]).

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

8.1 Example of INITIALISED Formatting Procedure

This example shows how the INITIALISED Formatting Procedure (see section 6.5.1) may be implemented for a MIFARE Classic 1k (see [MF1K]).

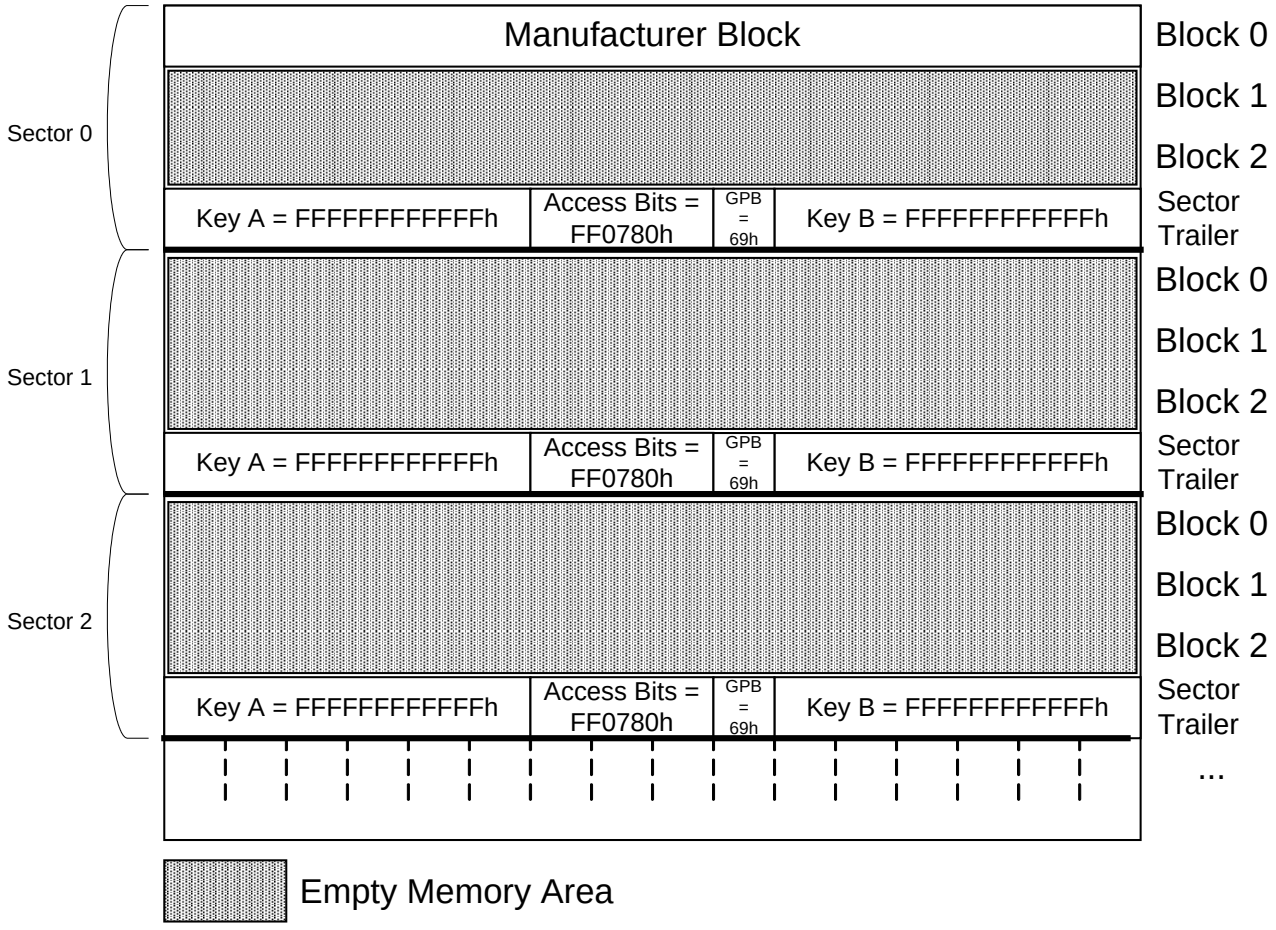


Fig 9. MIFARE Classic 1k tag after Production Phase (blank) before the INITIALISED Formatting Procedure

Fig 9 shows a blank (after production phase) MIFARE Classic 1k tag before the INITIALISED Formatting Procedure. All sectors have:

- default Key A and Key B equal to the value shown in Table 3.

- the General Purpose Byte (GPB) is set to 69h indicating non-personalized tag (see [MAD]), and
- the access bits are equal to FF0780h (transport configuration see [MF1K]).

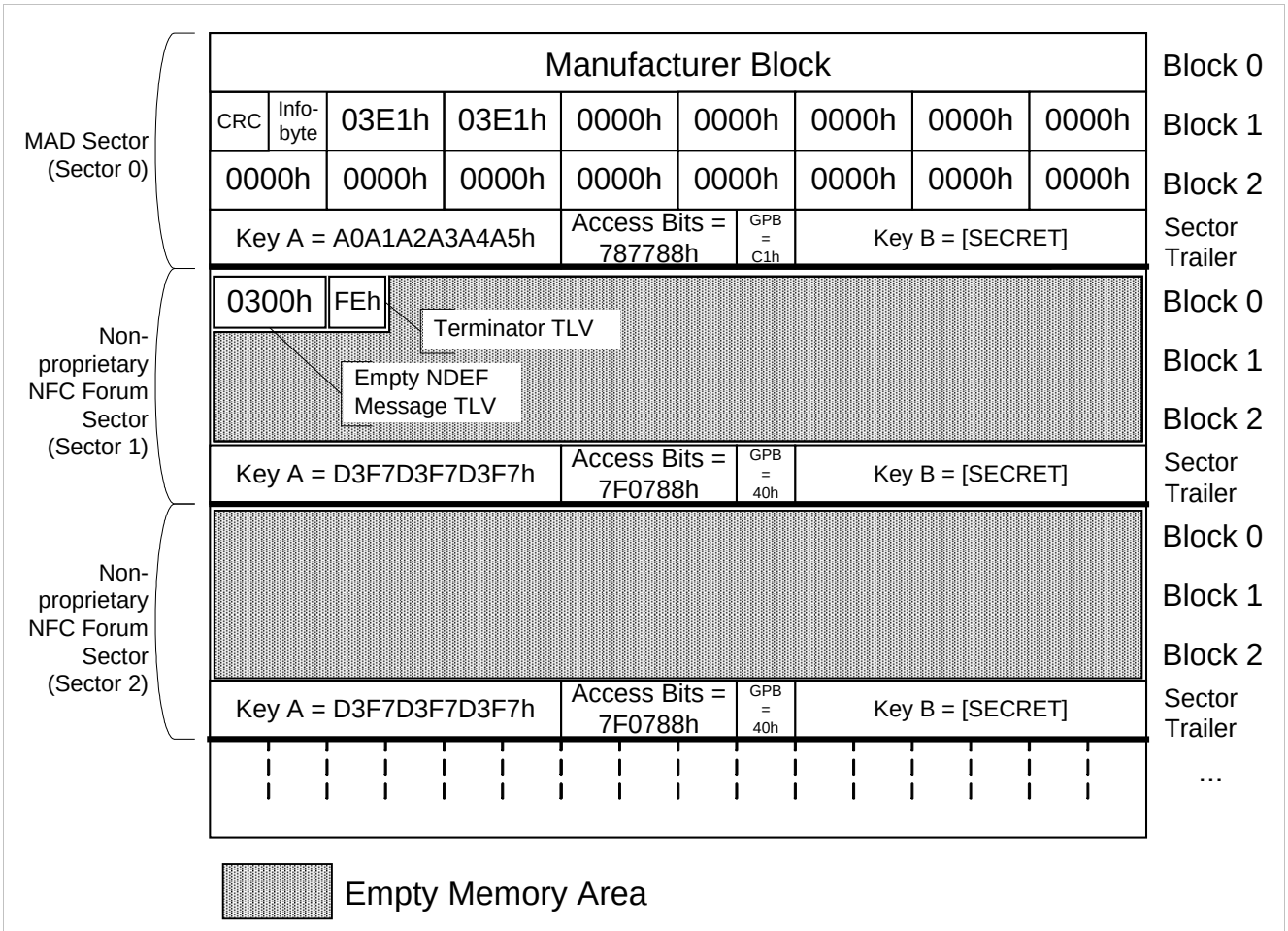


Fig 10. MIFARE Classic 1k tag after the INITIALISED Formatting Procedure

Fig 10 shows the MIFARE Classic 1k tag after the INITIALISED Formatting Procedure:

- MAD sector with:
  - key A equal to Table 9,
  - secret key B,
  - the General Purpose Byte (GPB) is set to C1h: MAD available, multi-application card, MAD Version 1 (see [MAD]), and
  - the Access bits are equal to 787788h (see Table 5).
- NFC sectors with:
  - key A equal to Table 6,
  - secret key B,

- the General Purpose Byte (GPB) is set to 40h: mapping version 1.0, read and write access granted (see [ANNFCMF]), and
- the access bits are equal to 7F0788h (see Table 5).

Sector 1 and Sector 2 are non-proprietary NFC sectors. The mandatory NDEF Message TLV is stored in Sector 1. The NFC sector configuration is the Simple Configuration because no proprietary NFC sectors are present in the MIFARE Classic 1k (see section 2.1).

The INITIALISED Formatting Procedure operations are described in details below:

1. Authentication operation to authenticate using Key A equal to the value shown in Table 3 the sector 0 i.e. MAD sector.
2. Write operation to write inside block 1 of sector 0:
   a. AID for sector 1, and 2 equal to NFC AID 03E1h,
   b. AID for sector 3 to 7 equal to 0000h (sector free, see [MAD]),
   c. Info-byte, and CRC (see [MAD]).
3. Write operation to write inside block 2 of sector 0:
   a. AID for sector 8, and 15 equal to 0000h.
4. Write operation to write inside the sector trailer of sector 0:
   a. The Key A equal to the value in Table 9,
   b. A secret Key B,
   c. Access bits equal to 787788h, and
   d. The GPB equal to C1h.
5. Authentication operation to authenticate using Key A equal to the value shown in Table 3 the sector 1 i.e. NFC sector.
6. Write operation to write inside block 0 of sector 1:
   a. the empty NDEF Message TLV: T value equal to 03h, and L value equal to 00h, and
   b. the Terminator TLV: T value equal to FEh.
7. Write operation to write inside the sector trailer of sector 1:
   a. The Key A equal to the value in Table 6,
   b. A secret Key B,
   c. Access bits equal to 7F0788h, and
   d. GPB equal to 40h.
8. Authentication operation to authenticate using Key A equal to the value shown in Table 3 the sector 1 i.e. NFC sector.
9. Write operation to write inside the sector trailer of sector 2:
   a. The Key A equal to the value in Table 6,
   b. A secret Key B,
   c. Access bits equal to 7F0788h, and
   d. GPB equal to 40h.

8.2 Example of 2 transitions from INITIALISED to MIFARE BLOCKED READ/WRITE writing two NDEF Message TLVs having different access right settings and keys

This example shows how to set a MIFARE Classic 1k tag from the INITIALISED state to the MIFARE BLOCKED READ/WRITE state. It is also shown the capability of the MIFARE Classic 1k tag to set different NDEF Message TLVs with different access rights and keys.

The example is a combination of:

- transition from INITIALISED to READ/WRITE (see [ANNFCMF]),
- transition from READ/WRITE to MIFARE BLOCKED READ/WRITE (see section 6.4.8).

As precondition the MIFARE Classic 1k tag is in INITILIAZED state (see Fig 10), and the Reader device already knows secret key B of the NFC sectors i.e. sector 1 and sector 2.

After the two transitions the MIFARE Classic 1k is in the MIFARE BLOCKED READ/WRITE state with the following settings (see Fig 11):

- The NDEF Message TLV 1 occupies the block 0 to 1 of sector 1, and the remaining part of sector 1 is occupied by NULL TLVs. The sector 1 has a read-only sector trailer, and the blocks are set to be readable using key A or key B, and writeable using key B only. Sector 1 is a proprietary NFC sector and it has the read and write access field of the GPB set to 01b i.e. 0101b = 5h.
- The NDEF Message TLV 2 and the Terminator TLV occupies block 0 to 1 of sector 2. The sector 2 has a read-only sector trailer, and the blocks are set to be readable and writeable using key A or key B. Sector 2 is a non-proprietary NFC sector.
- The mandatory NDEF Message TLV is the NDEF Message TLV 2 in sector 2. The Sector 1 contains a non-mandatory NDEF Message TLVs.

In this example the NFC sector configuration is the Mixed Configuration (see section 2.1) with one proprietary NFC sector with the smallest sector number (sector 1) and one non-proprietary NFC sector with the biggest sector number (sector 2).

The transition operations of this example are described below (see Fig 11):

1. Authentication operation to authenticate using the secret Key B to sector 1.
2. Write operation to block 0 of sector 1 to write first part of the NDEF Message TLV 1.
3. Write operation to block 1 of sector 1 to write second part of the NDEF Message TLV 1, and to fill the remaining part of block 1 with NULL TLVs.
4. Write operation to block 2 of sector 1 to fill the remaining block of sector 1 with NULL TLVs.
5. Write operation to sector trailer of sector 1 to:
   a. The Key A equal to the value in Table 6,
   b. A secret Key B,
   c. Access bits equal to 70FF08h: sector trailer is read-only with Key A or Key B, data area blocks are readable with Key A or Key B, and writeable with Key B, and
   d. The GPB equal to 45h: mapping version 1.0, write and read access configuration field equal to 01b.
6. Authentication operation to authenticate using the secret Key B to sector 2.

7. Write operation to block 0 of sector 2 to write first part of the NDEF Message TLV 2.
8. Write operation to block 1 of sector 2 to write second part of the NDEF Message TLV 2, and the Terminator TLV.
9. Write operation to sector trailer of sector 2 to:
   a. The Key A equal to the value in Table 6,
   b. A secret Key B,
   c. Access bits equal to 7F0788h: sector trailer is read-only with Key A or Key B, data area blocks are readable and writeable with Key A or Key B, and
   d. The GPB equal to 40h: mapping version 1.0, write and read access configuration field equal to 01b.

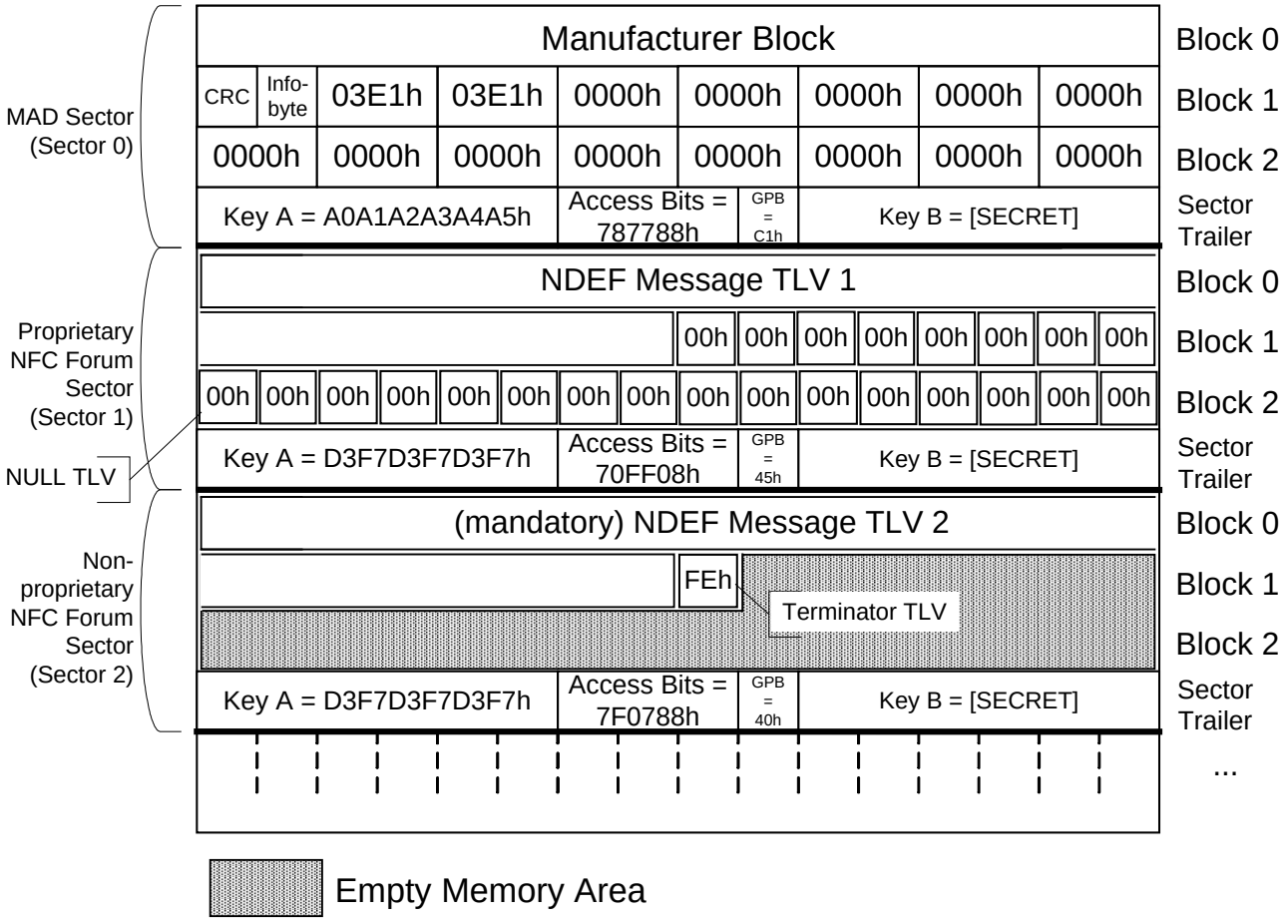


Fig 11. MIFARE Classic 1k tag with an NDEF Message TLV in MIFARE BLOCKED READ/WRITE

9. ANNEX B: Access bits Coding of the sector trailer of MIFARE Classic or MIFARE Plus cards after production phase

The MIFARE Classic or MIFARE Plus cards after production phase may have two different settings of the access bits. Depending on the access bits setting to be able to get read/write access to the sector trailer the authentication should be carried out using either the default Key A or the default Key B (see Table 3).

Table 11 shows the access bits values for the two settings. The setting that makes use of key A is also called transport configuration (see [MF1K, MF4K]).

Table 11. Access bits coding of byte 6 to 8 of the sector trailer for MIFARE Classic or MIFARE Plus cards after production phase.

Setting Description	Access Bits	Access Bits Settings	Block Description	Sector Trailer Access Condition Bytes		
				Byte 6	Byte 7	Byte 8
Key A Authentication needed to get read and write access to the sector trailer (Transport Configuration)	$C1_0$ $C2_0$ $C3_0$	000b	Data Block	FFh	07h	80h
	$C1_1$ $C2_1$ $C3_1$	000b	Data Block			
	$C1_2$ $C2_2$ $C3_2$	000b	Data Block			
	$C1_3$ $C2_3$ $C3_3$	001b	Sector Trailer			
Key B Authentication needed to get read and write access to the sector trailer	$C1_0$ $C2_0$ $C3_0$	000b	Data Block	7Fh	07h	88h
	$C1_1$ $C2_1$ $C3_1$	000b	Data Block			
	$C1_2$ $C2_2$ $C3_2$	000b	Data Block			
	$C1_3$ $C2_3$ $C3_3$	011b	Sector Trailer			

10. ANNEX C: Examples of Access Bits Coding into byte 6 to 8 of the Sector Trailer

This ANNEX shows some examples of the access bits coding of the sector trailers for MAD1 and MAD2 sectors (i.e. sector 0 and sector 16) and NFC sectors. This table can be used to translate the most used access bit values into the relative byte 6 to 8 values of the sector trailer. For more information about the access bits coding see [MF1K, MF4K, MFPLUS].

Table 12. Access bits coding of byte 6 to 8 of the sector trailer.

Life Cycle State	Access Bits	MAD1 and MAD2 Sectors	NFC sectors	MAD1 and MAD2 Sector Trailer Bytes Values			NFC sector Trailer Bytes Values		
		Access Bits Values	Access Bits Values	Byte 6	Byte 7	Byte 8	Byte 6	Byte 7	Byte 8
INITIALISED and READ/WRITE	$C1_0$ $C2_0$ $C3_0$	100b[1]	000b	78h	77h	88h	7Fh	07h	88h
	$C1_1$ $C2_1$ $C3_1$	100b	000b						
	$C1_2$ $C2_2$ $C3_2$	100b	000b						
	$C1_3$ $C2_3$ $C3_3$	011b	011b						
READ-ONLY	$C1_0$ $C2_0$ $C3_0$	010b[1]	010b	07h	8Fh	0Fh	07h	8Fh	0Fh
	$C1_1$ $C2_1$ $C3_1$	010b	010b						
	$C1_2$ $C2_2$ $C3_2$	010b	010b						
	$C1_3$ $C2_3$ $C3_3$	110b	110b						

[1] This value for the access bits $C1_0$ $C2_0$ $C3_0$ of sector 0 (related to the manufacturer block) is suggested and it may change.

11. Legal information

11.1 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.

11.2 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.

11.3 Licenses

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.

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.

11.4 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 Plus — is a trademark of NXP B.V.

12. Contents

continued >>

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

Date of release: 2 October 2012
130513
Document identifier: AN1305