AN1304

NFC Type MIFARE Classic Tag Operation

Rev. 1.2 — 3 May 2011
130412

Application note
PUBLIC

Document information

Info	Content
Keywords	NDEF, NDEF data mapping, NDEF Data Exchange Format MIFARE Classic 1K, MIFARE Classic 4K, MIFARE Classic 1K/4K, MIFARE Plus X/S, NFC-enabled tag, 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 a contactless tag. The NFC Forum has also defined four different tag types that are able to stored NDEF data. This document extends the tag types of the NFC Forum describing how the Reader device (called NFC device) can store NDEF data inside either MIFARE Classic 1K, MIFARE Classic 4K, MIFARE Plus X and MIFARE Plus S.

Revision history

Rev	Date	Description
1.2	20110503	Editorial Review: added MIFARE Plus X and MIFARE Plus S, replaced NFC Forum sector with NFC sector, replaced NFC Forum AID with NFC AID and other editorial updates.
1.1	20070821	Corrected and rephrased some text element, added figures, updated “NDEF Detection Procedure” section 6.4.1, added chapter 9. ANNEX C, added chapter 10. ANNEX D, added chapter 11. ANNEX E
1.0	20061111	Final Revision
0.1	20060629	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 or application is currently specified in the NFC Forum and it is called NFC Data Exchange Format (NDEF, see [NDEF]). To store NDEF formatted data (or also called NDEF data) inside a contactless tag product a mapping model is required.

The MIFARE Classic and MIFARE Plus tag products (see [MF1K, MF4K, MFPLUS]) are ICs enabling a contactless card/tag and are currently available with 1Kbyte, 2Kbyte and 4Kbyte of EEPROM memory. The MIFARE Classic and MIFARE Plus support file data transfer in 106 kbit/s, mutual three pass authentication, data encryption of RF-channel with replay attack protection, and an encrypted data link for the data exchange.

This application note describes:

- the mapping model to store one NDEF Message (or NDEF formatted data) inside MIFARE Classic 1k/4k card platform,
- the command set and the life cycle of the MIFARE Classic and MIFARE Plus to manage the NDEF Message, and
- how the Reader device (also called NFC device) can detect, read and write the NDEF Message in the MIFARE Classic and MIFARE Plus tag platform,

1.1 Applicable Documents

[ISOIEC 14443-2]	ISO/IEC 14443-2 Type A Identification Cards- Contactless Integrated circuit(s) cards- Proximity Cards- Part 2: Radio frequency power and signal interface
[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]	RFC 2119 - Key words for use in RFCs to Indicate Requirement Levels.
[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.

1.2 Convention and notations

1.2.1 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 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].

1.4 Glossary

Table 1. Terms and definitions

Term	Definition
Access Bits	Bits of the sector trailer that controls the access rights to the whole sector
$C1_{0...3}$, $C2_{0...3}$, $C3_{0...3}$.	access bits of the sector trailer
card	A MIFARE Classic or MIFARE Plus contactless card, see [MF1K, MF4K, MFPLUS]
CC	Capability Container, the CC stores control data for managing the NDEF data inside the tag
DA	MAD available bit, see [MAD]
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]

Term	Definition
MAD1	MIFARE Application Directory 1, see [MAD]
MAD2	MIFARE Application Directory 2, see [MAD]
MAD sector	A sector containing the MAD, see [MAD].
msb	most significant bit
MSB	most significant byte
NDEF	NFC Data Exchange Format, see [NDEF]
NDEF data	Data contained inside a MIFARE Classic or MIFARE Plus defined by the NFC Forum e.g. NDEF Message
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
NFC device	Reader device capable to read MIFARE Classic tags
NFC Sector	Sector that contains NDEF data
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
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]
tag	A MIFARE Classic or MIFARE Plus contactless card, 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, also called serial number in the [MF1K, MF4K, MFPLUS] specification

2. Memory Structure and Management

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

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 gives an overview of the MIFARE Classic products.

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 (or memory layout) is defined for each MIFARE Classic 1k and 4k products. The memory structures are divided into sectors containing 4 or 16 blocks each. Each block is numbered from 0 to 3 or from 0 to 15. The number associated to a block is called block number. Each block contains 16 bytes numbered from 0 to 15. For each block byte 0 is the MSB and byte 15 is the LSB. Byte 0 of block 0 in sector 0 indicates the MSB. The LSB is indicated by: Byte 15 of block 3 in sector 15 for MIFARE Classic 1k, byte 15 of block 3 in sector 31 for MIFARE Plus X/S with 2 Kbytes, and byte 15 of block 15 in sector 39 for MIFARE Classic 4k and MIFARE Plus X/S with 4 Kbytes.

In this document the bit and byte order when defining packets and messages follows the big-endian byte order.

The next two sections describe in detail the memory structures (also called layouts) of MIFARE Classic and MIFARE Plus.

2.1 MIFARE Classic 1k Layout

Fig 1 outlines the memory layout of the MIFARE Classic 1k.

The memory area of the MIFARE 1k is organized in 16 numbered sectors from 0 to 15. Each sector contains 4 blocks (block 0 to 3). Block 3 of each sector is called sector trailer and contains information (called access bits) to handle the sector access conditions and the secret keys (key A and key B). Depending on the setting of the access bits the Reader device has to perform an authentication with key A or key B to read or write the sector.

Byte 9 of the sector trailer (see Fig 1) is called General Purpose Byte (GPB).

Block 0 of sector 0 (i.e. Manufacturer Block also called Manufacturer Data) contains the IC manufacturer data, and the Unique Identifier (UID, also called Serial Number, see [ISOIEC 14443-3] for a detailed definition).

For more information about MIFARE Classic 1k see [MF1K].

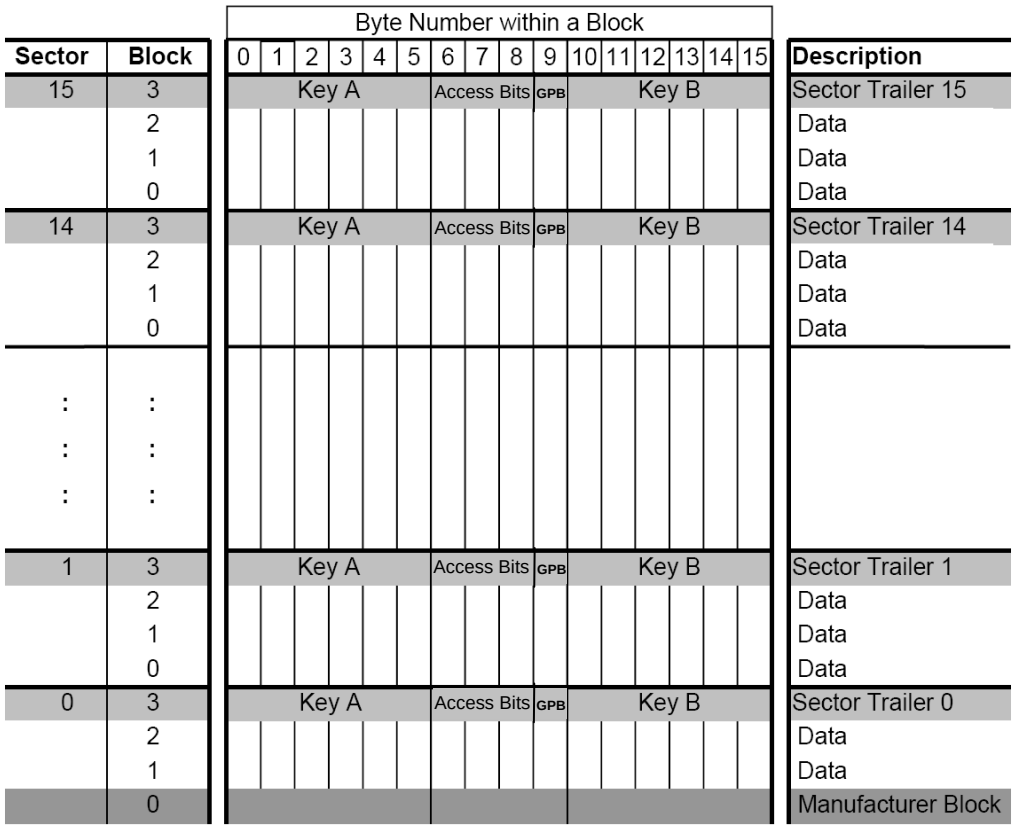


Fig 1. MIFARE Classic 1k Memory Layout

2.2 MIFARE Plus X/S with 2 Kbytes Layout

Fig 2 outlines the memory layout of the MIFARE Plus X/S with 2 Kbytes.

The memory area is organized in 32 numbered sectors from 0 to 31. Each sector contains 4 blocks (block 0 to 3). Block 3 of each sector is called sector trailer and contains information (called access bits) to handle the sector access conditions and the secret keys (key A and key B). Depending on the setting of the access bits the Reader device has to perform an authentication with key A or key B to read or write the sector.

Byte 9 of the sector trailer (see Fig 2) is called General Purpose Byte (GPB).

Block 0 of sector 0 (i.e. Manufacturer Block also called Manufacturer Data) contains the IC manufacturer data, and the Unique Identifier (UID, also called Serial Number, see [ISOIEC 14443-3] for a detailed definition).

For more information about MIFARE Plus X/S with 2 Kbytes see [MFPLUS].

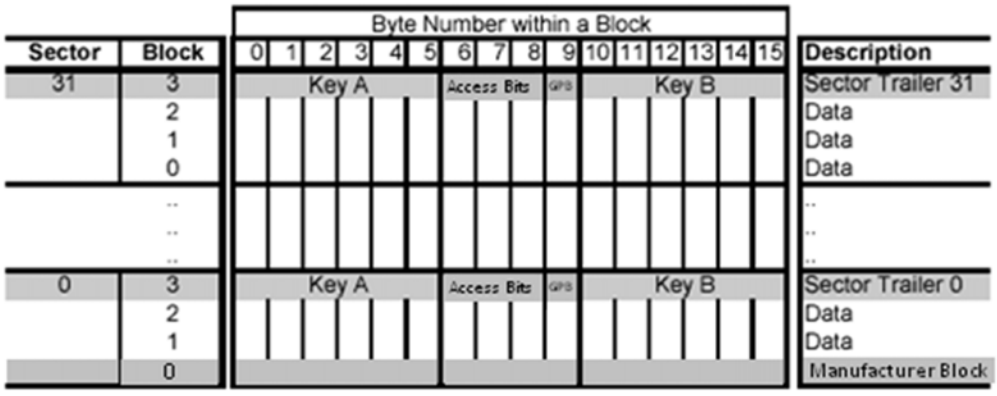


Fig 2. MIFARE Plus X/S with 2 Kbytes Layout

2.3 MIFARE Classic 4k and MIFARE Plus X/S with 4 Kbytes Layout

Fig 3 outlines the memory layout of the MIFARE Classic 4k tag.

The memory area of the MIFARE Classic 4k and MIFARE Plus X/S with 4 Kbytes is organized in numbered sectors from 0 to 39. Each sector contains 4 or 16 blocks (block 0 to 3 or block 0 to 15).). Block 3 of sector 0 to 31, and block 15 of sector 32 to 39 is called sector trailer, and it contains information (called access bits) to handle the sector access conditions and the secret keys (key A and key B). Depending on the setting of the access bits the Reader device has to perform an authentication with key A or key B to read or write the sector.

Byte 9 of the sector trailer (see Fig 3) is called General Purpose Byte (GPB).

Block 0 of sector 0 (i.e. Manufacturer Block also called Manufacturer Data) contains the IC manufacturer data, and the Unique Identifier (UID, also called Serial Number, see [ISOIEC 14443-3] for a detailed definition).

For more information about MIFARE Classic 4k and MIFARE Plus X/S with 4 Kbytes see [MF4K, MFPLUS].

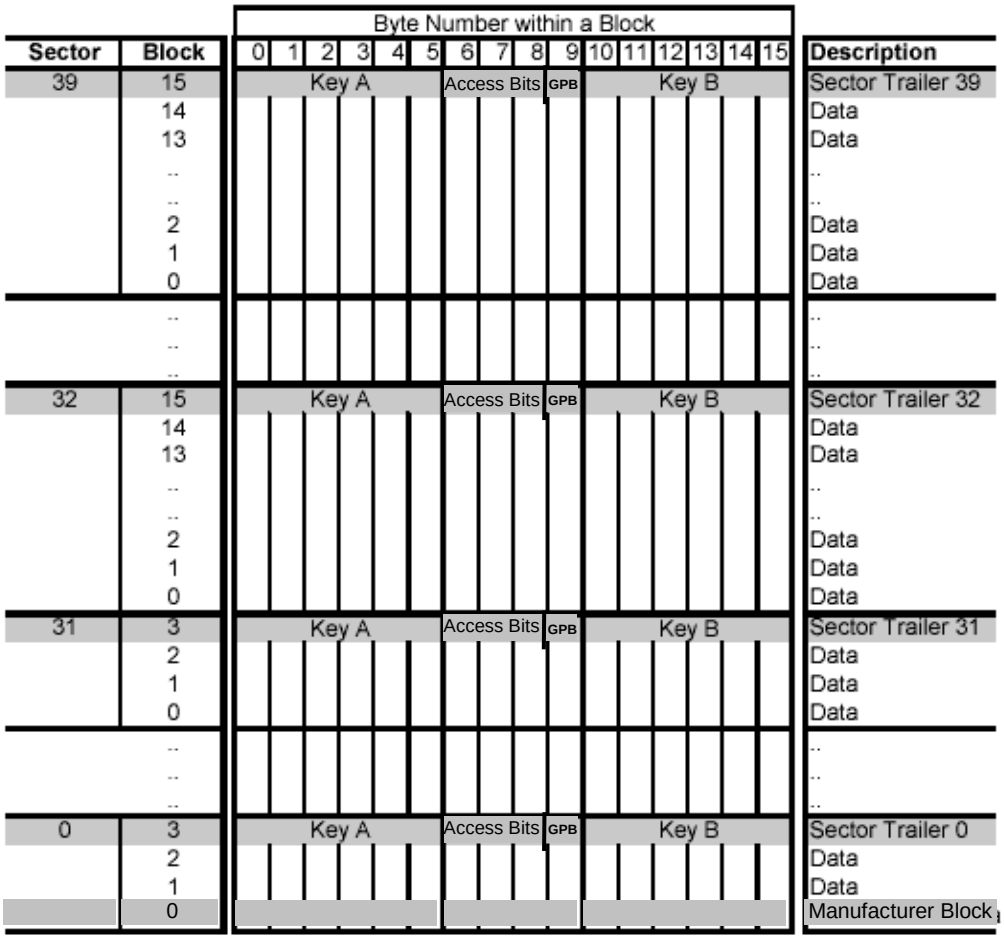


Fig 3. MIFARE Classic 4k and MIFARE Plus X/S with 4 Kbytes Memory Layout

2.4 MIFARE Application Directory

The memory mapping of NDEF data for the MIFARE Classic and MIFARE Plus IC uses the MIFARE application directory structure (see [MAD]).

The MIFARE application directory (MAD) identifies to which application the information stored inside each memory sector belongs.

Two MIFARE application directories have been specified:

1. MIFARE application directory 1 (MAD1): MAD1 MAY be used in any MIFARE Classic compliant product. The MAD1 is located in the MAD sector (sector 00h), In case the MAD1 is used on products with a memory size bigger than 1Kbytes, only 1Kbytes memory can be used and addressed by the MAD1. The remaining memory is therefore not used for NDEF storage and stays free.
2. MIFARE application directory 2 (MAD2): MAD1 MAY be used in any MIFARE Classic compliant product with a memory size bigger than 1Kbytes. MAD2 is not applicable for products with a memory size smaller or equal to 1Kbytes. The MAD2 is located in the MAD sectors (sector 00h and 10h)

To each application the MAD associates a unique application identifier (AID). The application identifiers (AIDs) are stored inside MAD sector(s) 00h.

The AID is two byte long, and it is divided into 2 fields of one byte each:

1. the function cluster code (1 byte) that identifies the cluster to which the application belongs to, and
2. the application code (1 byte) that identifies the application inside the cluster.

For more information about MAD1 and MAD2 see [MAD].

The General Purpose Byte (GPB) of the MAD sector SHALL be set with DA bit equal to 1b (DA bit is the MAD available bit of the GPB, see [MAD] for more information).

All currently unused sectors SHOULD be write-protected with secret keys defined by the tag issuer in order to prevent unintended redefinition of access conditions and keys. It is RECOMMENDED to use different keys for all free sectors. This enables future release of some sectors to new service providers without the need of releasing all free sectors.

2.5 MIFARE Classic and MIFARE Plus Access Mechanism (Access Bits)

MIFARE Classic and MIFARE Plus provide a mechanism based on keys and access bits to grant read and write access (see [MF1K, MF4K, MFPLUS]).

Each memory sector has associated two keys called key A, and key B, and 12 access condition bits called $C1_{0...3}$, $C2_{0...3}$ and $C3_{0...3}$. By setting the access bits, it is possible to grant read and write access based on key A and/or key B. The access condition bits are called $C1_{0...3}$, $C2_{0...3}$ and $C3_{0...3}$. Their locations inside byte 6 to 8 of the Sector Trailer are described in Fig 4. The value and also the negated value of each access bit are stored inside the sector trailer e.g. $C1_0 = 0b$ and $\overline{C1_0} = 1b$.

The Annex C in chapter 9 shows different values of the byte 6 to 8 depending on the access bits values.

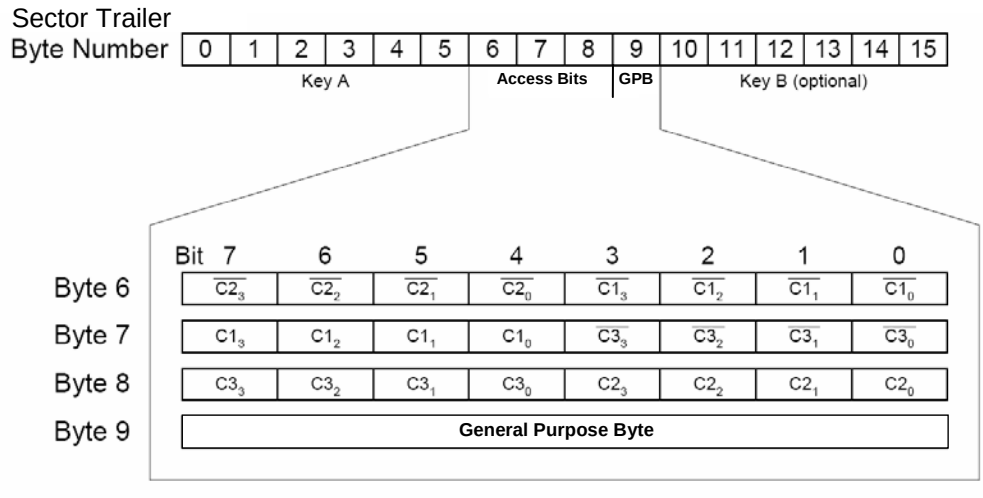


Fig 4. Access Bits location in the Sector Trailer

The General Purpose Byte (GPB, see section 2.1 and section 2.3) of the sector trailer is not used in the access mechanism of MIFARE Classic and MIFARE Plus tags. However it indicates the version of the mapping document (i.e. this application note) and the read/write access (see section 6.1).

In this section and in the next two sub-sections the access bits description is provided for sake of completeness and they might not be used in this application note for any purpose.

2.5.1 MAD Sector Access

The memory sectors where the MAD1 and MAD2 are stored (see [MAD]), are protected using the key A and key B. According to [MAD] the memory sectors are:

- MAD1: the MAD sector is 00h (sector 0), and
- MAD2: the MAD sectors are 00h and 10h (sector 0 and sector 16).

Anybody SHALL be allowed to read the MAD sectors. This is achieved by using a public key A described in Table 3 (see also [MAD]).

Table 3. Public Key A value of MAD sector(s)

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

The access bits for the MAD sector(s) are set to either:

- as described in Table 4 if the MAD sector has read and write access granted, or
- as described in Table 5 if the MAD sector has read-only access granted (see also [MF1K, MF4K, MFPLUS]).

In this context the term read and write access granted means that for MAD sectors that have been previously authenticated with the secret key B, it is possible to read and write all sector blocks apart from the sector trailer block (see of Table 4 for more details).

Instead the term read-only access granted means that for MAD sectors that have been previously authenticated with the public key A of Table 3 or secret key B, it is possible to only read all sector blocks apart from the sector trailer block (see Table 5 for more details).

Using the key A it is always only possible to read the blocks of the MAD sector. Sector trailers have a particular access configuration when read/write access or read-only access is granted (see Table 4 and Table 5).

The MAD sectors SHOULD be write-protected by means of the secret key B (e.g. defined by the tag issuer), or setting the MIFARE Classic and MIFARE Plus tag as read-only using the access bits.

Table 4. Access bits setting for MAD sector with read and write access granted

Access bits setting for sector 0 of MAD1 or MAD2 and for sector 16 of MAD2		
Access Bits	**Values**	**Remarks**
$C1_0$ $C2_0$ $C3_0$	100b[i]	The block 0 is read with key A or key B and written with key B

$C1_1$ $C2_1$ $C3_1$	100b	The block 1 is read with key A or key B and written with key B
$C1_2$ $C2_2$ $C3_2$	100b	The block 2 is read with key A or key B and written with key B
$C1_3$ $C2_3$ $C3_3$	011b	The sector trailer block: • Key A is written with key B and never read, • Access bits is read with key A or key B and written with key B, • Key B is written with key B and never read.

i. Recommended value for the access bits $C1_0$ $C2_0$ $C3_0$ of sector 0 (manufacturer block).

Table 5. Access bits setting for MAD sector with read-only access granted

Access bits setting for sector 0 of MAD1 or MAD2 and for sector 16 of MAD2		
Access Bits	**Values**	**Remarks**
$C1_0$ $C2_0$ $C3_0$	010b[i]	The block 0 is read with key A or key B
$C1_1$ $C2_1$ $C3_1$	010b	The block 1 is read with key A or key B
$C1_2$ $C2_2$ $C3_2$	010b	The block 2 is read with key A or key B
$C1_3$ $C2_3$ $C3_3$	110b	The sector trailer block: • Key A is never written and read, • Access bits is read with key A or key B and never written, • Key B is never written and read.

i. Recommended value for the access bits $C1_0$ $C2_0$ $C3_0$ of sector 0 (manufacturer block).

2.5.2 NFC Sector Access

A sector MAY contain NDEF data. A sector that contains NDEF data is called NFC Sector.

An NFC Sector is readable authenticating it with the public key A defined in Table 6. Public key A for NFC Sector is different from public key A for MAD sector (compare Table 3 and Table 6).

Table 6. Public Key A value of NFC Sectors

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

The access bits for the data blocks and sector trailer of the NFC Sectors are set to either:

- as described in Table 7 if the NFC Sector has read and write access granted, or
- as described in Table 8 if the NFC Sector has read-only access granted.

In this context the term read and write access granted means that for NFC Sectors that have been previously authenticating using the public key A of Table 6, it is possible to

read and write all sector blocks apart from the sector trailer block (see Table 7 for more details).

Instead the term read-only access granted means that for NFC Sectors that have been previously authenticated using the public key A of Table 6, it is possible to read all sector blocks apart from the sector trailer block (see Table 8 for more details).

Key B SHALL be a secret key (e.g. defined by the tag issuer). Key B SHALL be used to modify the sector trailer i.e. key A, access bits, GPB and key B.

Table 7. Access bits setting for NFC Sectors with read and write access granted

Access Bits	Values	Remarks
$C1_0$ $C2_0$ $C3_0$	000b	The block 0 is read and written with key A or key B
$C1_1$ $C2_1$ $C3_1$	000b	The block 1 is read and written with key A or key B
$C1_2$ $C2_2$ $C3_2$	000b	The block 2 is read and written with key A or key B
$C1_3$ $C2_3$ $C3_3$	011b	The sector trailer block: • Key A is written with key B and never read, • Access bits is read with key A or key B and written with key B, • Key B is written with key B and never read.

Table 8. Access bits setting for NFC Sectors with read-only access granted

Access Bits	Values	Remarks
$C1_0$ $C2_0$ $C3_0$	010b	The block 0 is read with key A or key B
$C1_1$ $C2_1$ $C3_1$	010b	The block 1 is read with key A or key B
$C1_2$ $C2_2$ $C3_2$	010b	The block 2 is read with key A or key B
$C1_3$ $C2_3$ $C3_3$	110b	The sector trailer block: • Key A can never be written and read, • Access bits is read with key A or key B and never written, • Key B can never be written and read.

2.6 TLV blocks

A TLV block consists of one to three fields:

T (tag field, or T field) SHALL identify the type of the TLV block (see Table 9) and SHALL consist of a single byte encoding a number from 00h to FFh. The tag values 01h, 02h, 04h to FCh and FFh are reserved for future use.

L (length field, or L field) SHALL provide the size in bytes of the value field. It has two different formats composed of one, or three bytes. The Reader device SHALL understand all two length field formats. Fig 5 shows the two different length field structures. However, depending on the tag field value, the length field MAY not be present.

- One byte format: The one byte format SHALL code the length of the value field between 00h and FEh bytes. This byte SHALL be interpreted as a cardinal if the value is between 00h and FEh. If it contains FFh the value SHALL be interpreted as flag that specifies that the length field is composed of more than one byte.
- Three consecutive bytes format: This format SHALL code the length of the value field between 00FFh and FFFEh bytes. The first byte is assumed to be a flag equal to FFh indicating that two more bytes length SHALL be interpreted as word. This word SHALL be interpreted as a cardinal if the value is between 00FFh and FFFEh. The value FFFFh is reserved for future use (RFU).

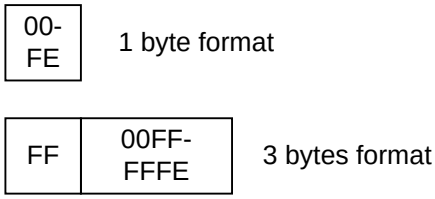


Fig 5. Length Field Formats

V (value field, or V field) If the length field is equal to 00h or there is no length field, there SHALL NOT be the value field, i.e. the TLV block is empty. If there is the length field and indicates a length of the value field N bigger than zero (N>0), the value field SHALL consist of N consecutive bytes.

Table 9 lists the TLV blocks specified by this document that are described in the following sections.

Table 9. Defined TLV blocks

TLV Block Name	Tag Field Value	Short Description
NULL TLV	00h	It might be used for padding of memory areas and the Reader device SHALL ignore this
NDEF Message TLV	03h	It contains the NDEF Message, see [NDEF]
Proprietary TLV	FDh	Tag proprietary information
Terminator TLV	FEh	Last TLV block in the data area

The Reader device SHALL write the TLV blocks in a specific order inside the data area following the rules below:

- The TLV blocks SHALL be written in order starting from byte 0 of block 0 of the NFC Sector (sector containing NDEF data) with the smallest address.
- A TLB block MAY be memorized across two or more NFC Sectors.
- If present the Terminator TLV is the last TLV block on the MIFARE Classic and MIFARE Plus tag.

NULL TLV and Terminator TLV are the only TLV blocks that are 1 byte long (e.g. composed of only the Tag field, see below).

Reader devices SHALL ignore and jump over those TLV blocks that make use of reserved tag field values (see above). To jump over a TLV block with reserved tag field values, the Reader device SHALL read the length field to understand the length of the value field.

Future definitions of TLV blocks composed of only the tag field are not backward compatible with this application note.

2.6.1 NDEF Message TLV

At least one NDEF Message TLV SHALL be always present inside the MIFARE Classic and MIFARE Plus tag. The NDEF Message TLV stores the NDEF Message inside the Value field (see [NDEF]). The Reader device SHALL be able to read and process the NDEF Message TLV found by the NDEF Detection Procedure (also called mandatory NDEF Message TLV or first NDEF Message TLV, see section 6.4.1); anyhow further NDEF Message TLV blocks MAY be present. Below the encoding of the 3 TLV fields of NDEF Message TLV is shown:

T SHALL be equal to 03h (see Table 9).

L SHALL be equal to the size in bytes of the stored NDEF Message.

V SHALL store the NDEF Message (see [NDEF]).

An empty NDEF Message TLV SHALL be defined as an NDEF Message TLV with L field equal to 00h, and no V field (i.e. no NDEF Message is present in the V field, see [NDEF]).

A non-empty NDEF Message TLV MAY contain either empty or non-empty NDEF Messages. The definition of empty NDEF Message is given in chapter 7.

2.6.2 Proprietary TLV

The Proprietary TLV contains proprietary information. A MIFARE Classic and MIFARE Plus tag SHALL contain zero, one or more Proprietary TLV. The Reader device might ignore the data contained in this TLV block. Below the encoding of the 3 TLV fields of Proprietary TLV are shown:

T SHALL be equal to FDh (see Table 9).

L SHALL be equal to the size in bytes of the proprietary data in the Vale field.

V SHALL contain any proprietary data.

2.6.3 NULL TLV

The NULL TLV MAY be used for padding of the data area. A MIFARE Classic and MIFARE Plus tag MAY contain zero, one or more NULL TLV. The Reader device SHALL ignore this TLV block. NULL TLV SHALL be composed of 1 byte tag field. Below the encoding of the tag field of the NULL TLV are shown:

T SHALL be equal to 00h (see Table 9).

L SHALL NOT be present.

V SHALL NOT be present.

2.6.4 Terminator TLV

The Terminator TLV MAY be present inside the MIFARE Classic and MIFARE Plus tag, and an Reader device SHALL be able to read/process it. The Terminator TLV is the last TLV block in the data memory area. Terminator TLV SHALL be composed of 1 byte tag field. Below the encoding of the tag field of the Terminator TLV are shown:

T SHALL be equal to FEh (see Table 9).

L SHALL NOT be present.

V SHALL NOT be present.

3. RF Interface

The MIFARE Classic and MIFARE Plus comply with the RF interface as defined in the [ISOIEC 14443-2].

The ISO/IEC 14443 terminology uses the term PCD for Proximity Coupling Device and PICC for Proximity Integrated Circuit(s) Card. In this application note the PCD is called reader device or NFC device, and the PICC is called MIFARE Classic or MIFARE Plus tag.

4. Framing/Transmission Handling

The framing and transmission handling of the MIFARE Classic and MIFARE Plus tag SHALL follow [MF1K, MF4K, MFPLUS].

5. Command Set

This chapter describes the command set as well as the overall state diagram of the MIFARE Classic and MIFARE Plus tag. It provides the basis to: detect and activate the MIFARE Classic and MIFARE Plus tag, detect the NDEF data, get read and write access to the NDEF data, and deactivate the MIFARE Classic and MIFARE Plus tag.

5.1 Tag Commands and Responses Set

The MIFARE Classic and MIFARE Plus tag accepts the following command set, sent by the Reader device. Table 10 shows the command set (here called memory operations) of the MIFARE Classic and MIFARE Plus tag (see [MF1K, MF4K, MFPLUS]).

Table 10. Command Set / Memory Operations

Memory Operations	
Operation	**Description**
Identification and Selection	It identifies the tag and it selects it
Authentication	Three pass authentication, this operation requires to read an write a memory sector
Read	It reads one memory block (16 bytes)
Write	It writes one memory block (16 bytes)

5.1.1 Identification and Selection Operation

The identification and selection (or selection and anticollision) operation is defined by [MF1K, MF4K, MFPLUS, ISOIEC 14443-3].

5.1.2 Authentication Operation

The authentication operation is based on three pass authentication using either the key A or the key B. The MIFARE Classic and MIFARE Plus allows memory access only if the authentication of the specific sector has been performed successfully. The authentication is sector specific. Even if different sectors contain the same key A or key B, the authentication SHALL be performed for each sector before having access to the blocks.

If the sector authentication is successful, depending on the settings of the access bits reading and/or writing MAY be allowed or not.

5.1.3 Read operation

The Read operation allows to read a block (16 bytes) of a sector.

5.1.4 Write operation

The Write operation allows to write a block (16 bytes) of a sector.

The Write operation is block-wise i.e. it writes always the 16 bytes of the whole block. To change parts of the block, the new byte values SHALL be written together with the ones that remain fixed. The block MAY be read first (i.e. Read operation), if the fixed byte values are not known in advance.

6. NDEF Detection and Access

This chapter describes how NDEF data (e.g. NDEF Message) SHALL be stored and accessed in the MIFARE Classic and MIFARE Plus tag.

The NDEF Message that this application note manages inside a MIFARE Classic and MIFARE Plus, is stored inside a NDEF Message TLV that is called mandatory NDEF Message TLV or first NDEF Message TLV. The mandatory NDEF Message TLV is also the NDEF Message TLV found by the NDEF Detection Procedure (see section 6.4.1).

6.1 NDEF Management

To detect and access NDEF data (e.g. NDEF Message) inside the MIFARE Classic and MIFARE Plus tag the MAD SHALL be used (see section 2.4) together with the GPB of the NFC Sectors.

An application identifier (AID) of the MAD, called NFC AID, has been reserved to identify sectors with NDEF data. A sector with NDEF data is called NFC Sector. The two fields of the NFC AID are set as following:

1. the function cluster code is equal to E1h to identify the cluster of sectors with NDEF data, and
2. the application code is equal to 03h to identify the NFC Sector that this application note is related to.

One or more NFC Sectors MAY be present inside a MIFARE Classic 1k/4k tag.

If more than one NFC Sector is present, the NFC Sectors SHALL be contiguous. In case of MIFARE Classic 4k or MIFARE Plus with 4 Kbytes, it SHALL be considered contiguous a sequence of NFC Sectors that includes the MAD sector 16.

Example of contiguous NFC Sectors are:

- NFC Sectors from sector 2 to sector 3, and
- NFC Sectors from sector 1 to sector 39. In this case the MAD sector 16 is contained but still as defined above the NFC Sectors are considered contiguous.

An example of non-contiguous NFC Sectors is:

- sector 3 and sector 5 without sector 4 are NFC Sectors. In this case sector 4 is not an NFC Sector so the two remaining NFC Sectors are not contiguous.

The NDEF data SHALL be written starting from the NFC Sector with the smallest sector number to the biggest one.

The General Purpose Byte (GPB, see section 2.1 and section 2.3) of each NFC Sector provides information about the version number of the mapping model used to store the NDEF data into the MIFARE Classic and MIFARE Plus (see section 6.1.1) and the write access of the NFC Sectors. GPB SHALL be coded as describe in Table 11.

Table 11. General Purpose Byte structure

msb Bit 7	**Bit 6**	**Bit 5**	**Bit 4**	**Bit 3**	**Bit 2**	**Bit 1**	**lsb Bit 0**
Mapping version number				Access conditions			
Major version number		Minor version number		Read access condition		Write access condition	

The 4 least significant bits (lsb) of the GPB indicate the access conditions of the NFC Sector:

- Bit 2-3 indicates the read access condition:
  - The value 00b indicates read access granted without any security.
  - The value 11b indicates no read access granted at all.
  - Any other value indicates that vendor security operations are required to grant read access i.e. proprietary.
- Bit 0-1 indicates the write access condition:
  - The value 00b indicates write access granted without any security.
  - The value 11b indicates no write access granted at all.
  - Any other value indicates that vendor security operations are required to grant write access i.e. proprietary.

The 4 most significant bits (msb) indicate the mapping version number (see section 6.1.1):

- Bit 7-6 (the 2 msb of mapping version number field) indicate the major version number.
- Bit 5-4 (the 2 lsb of mapping version number field) indicate the minor version number.

Inside a MIFARE Classic and MIFARE Plus tag the NFC Sector(s) containing the mandatory NDEF Message TLV SHALL be set with read access condition equal to 00h and write access conditions equal to either 00b or 11b (see section 6.3).

The Reader device implementing this application note SHALL manage MIFARE Classic and MIFARE Plus tags with major version number equal to 01b and the minor version number equal to 00b i.e. mapping version 1.0.

6.1.1 Version Treating

The GPB of the NFC Sectors contains the mapping version number of the applied mapping model of the MIFARE Classic 1k/4k or MIFARE Plus tag. The mapping version number is indicated with two numbers: major version number and minor version number.

The handling of the different major and minor version numbers of the MIFARE Classic or MIFARE Plus tag (called MSVNo) and the one implemented in the Reader device (called NFCDevVNo) is explained in the 4 cases of Table 12.

Table 12. Handling of the mapping document version numbers

No	Version Number Case	Handling
1	Major NFCDevVNo is equal to major MSVNo, and minor NFCDevVNo is bigger than or equal to minor MSVNo	The Reader device SHALL access the MIFARE Classic or MIFARE Plus tag and SHALL use all features of the applied mapping document to this MIFARE Classic or MIFARE Plus tag.
2	If major NFCDevVNo is equal to major MSVNo, and minor NFCDevVNo is lower than minor MSVNo	Possibly not all features of the MIFARE Classic or MIFARE Plus tag can be accessed. The Reader device SHALL use all its features and SHALL access this MIFARE Classic or MIFARE Plus tag.

No	Version Number Case	Handling
3	If major NFCDevVNo is smaller than major MSVNo	Incompatible data format. The Reader device cannot understand the MIFARE Classic or MIFARE Plus tag data. The Reader device SHALL reject this MIFARE Classic or MIFARE Plus tag.
4	If major NFCDevVNo is bigger than major MSVNo	The Reader device might implement the support for previous versions of this specification in addition to its main version. In case the Reader device has the support from previous version, it SHALL access the MIFARE Classic or MIFARE Plus tag. On the contrary, in case the Reader device has not the support from previous version, it SHALL reject the MIFARE Classic or MIFARE Plus tag.

6.2 NDEF Storage

The data format of the NDEF Message is defined in [NDEF]. The NDEF Message SHALL be stored inside the value field of the NDEF Message TLV (see section 2.6.1) using one or more NFC Sectors. NFC Sectors are identified by the NFC AID in the MAD sector(s).

6.3 Life Cycle

The NFC Sectors of a MIFARE Classic or MIFARE Plus tag MAY be in the following states INITIALISED, READ/WRITE or READ-ONLY. The NFC Sectors SHALL be in only one state in a specific moment in time. The state SHALL be reflected by the content of the NFC Sectors. The state is not related to a single NFC Sector but to all NFC Sectors together. The states are described in the following sections.

If the MIFARE Classic or MIFARE Plus tag contains only NFC Sectors the state of the NFC Sectors is called the state of the MIFARE Classic or MIFARE Plus tag. In the description below the state of the MIFARE Classic or MIFARE Plus tag is confused with (i.e. equal to) the state of the NFC Sectors.

Every state has its own valid operations called transitions or state changes. The state transitions are only relevant for reader devices, which are capable of writing MIFARE Classic or MIFARE Plus tags.

The different states are identified comparing the GPB of the NFC Sector where the mandatory NDEF Message TLV starts, and the fields of the mandatory NDEF Message TLV. Note that the access bits of the sector trailer described in section 2.5, are not used in this application note to identify the specific state.

If the MIFARE Classic or MIFARE Plus tag is not in a valid state according to this application note, the NDEF data of the MIFARE Classic or MIFARE Plus tag in all NFC Sectors SHALL be ignored. The reasons MAY be:

- Non-contiguous NFC Sectors.
- No NFC Sectors are present inside the tag i.e. no sectors are indicated by the MAD using the NFC AID.
- Mismatch between overall TLV blocks length and actual length of the data area.
- Invalid TLV block.

6.3.1 INITIALISED State

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

- the GPB is set as described in section 6.1, in particular with bit 0-1 equal to 00b and bit 2-3 equal to 00b (read and write access granted),
- the NFC Sector(s) contains one NDEF Message TLV (the mandatory one), and
- the length field of the mandatory NDEF Message TLV is equal to 00h.

In INITIALISED state the NFC device MAY modify the content of the mandatory NDEF Message TLV writing an NDEF Message in it. The Annex D in chapter 10, the Annex E in chapter 0 and Annex F in chapter 12 show two examples of respectively MIFARE Classic 1k, MIFARE Plus with 2 Kbytes, and MIFARE Classic 4k or MIFARE Plus with 4 Kbytes all in INITIALISED state.

6.3.2 READ/WRITE State

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

- the GPB is set as described in section 6.1, in particular with bit 0-1 equal to 00b and bit 2-3 equal to 00b (read and write access granted),
- the mandatory NDEF Message TLV is present in the NFC Sector(s), and
- the length field of the mandatory NDEF Message TLV is different from zero.

The READ/WRITE state SHALL be reached via the INITIALISED state. In this state the NFC device MAY modify the content of the mandatory NDEF Message TLV writing an NDEF Message in it.

6.3.3 READ-ONLY State

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

- the GPB is set as described in section 6.1, in particular with bit 0-1 equal to 11b and bit 2-3 equal to 00b (no write access is granted, only read access is granted),
- the mandatory NDEF Message TLV is present in the NFC Sector(s), and
- the length field of the mandatory NDEF Message TLV SHALL be different from zero.

In READ-ONLY state all NFC Sectors have read-only access granted. The MIFARE Classic or MIFARE Plus tag remains in READ-ONLY state for the remaining life cycle.

6.4 Command Sequence Description

In this section several procedures are described to manage NDEF data e.g. the mandatory NDEF Message TLV inside the NFC Sector(s). The different state changes or transitions between the states of the MIFARE Classic or MIFARE Plus tag are shown in detail as well.

Each involved sector in the procedures SHALL be authenticated using the Authentication operation (see section 5.1.2) before reading or writing it. The public key A SHALL be selected based on the sector type i.e. MAD sector or NFC Sector (see section 2.5).

6.4.1 NDEF Detection Procedure

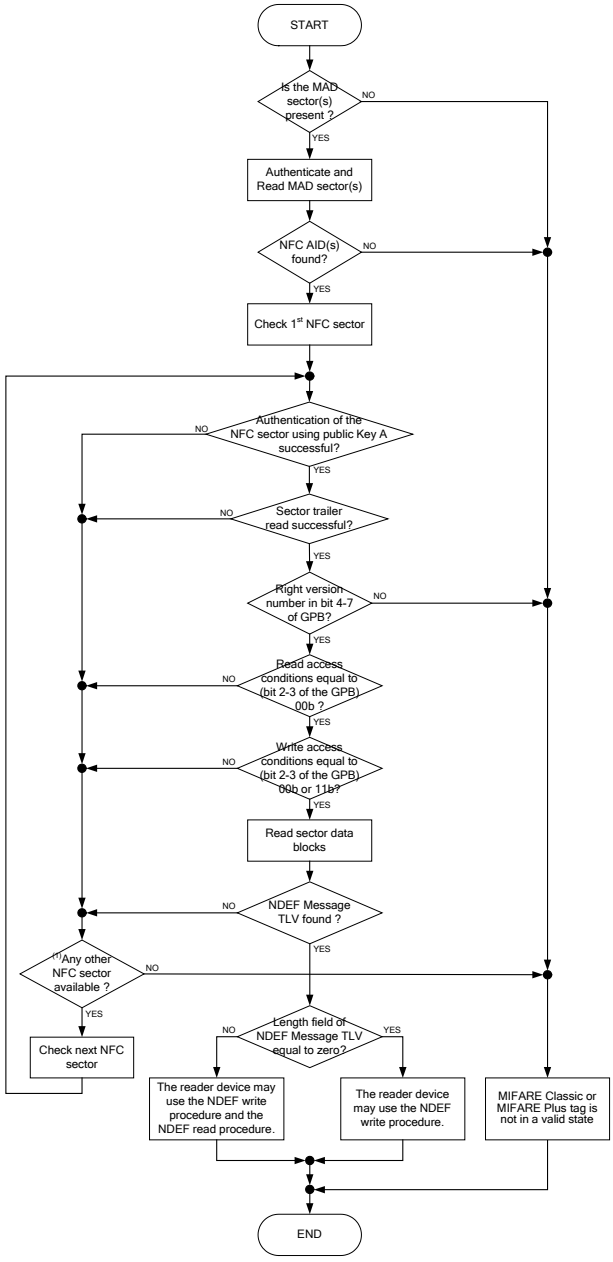
The NDEF Detection Procedure SHALL be used to detect the mandatory NDEF Message (see [NDEF]) inside a MIFARE Classic or MIFARE Plus tag.

The NDEF Detection Procedure is based on the check of:

- the MAD sector(s),

- the NFC Sector(s), and
- the mandatory NDEF Message TLV that contains the NDEF Message.

As already mentioned the NDEF Message TLV found by the NDEF Detection Procedure is called mandatory NDEF Message TLV or first NDEF Message TLV. When the MIFARE Classic or MIFARE Plus is in READ/WRITE or READ-ONLY state, this NDEF Message TLV contains an NDEF Message. In INITIALISED state the NDEF Message TLV is empty.



(1) After an Authentication or a Read operation fails, the MIFARE Classic or MIFARE Plus does not respond anymore to any commands and it needs to be re-activated and selected in order to continue the NDEF Detection Procedure.

Fig 6. NDEF Detection Procedure

To execute the NDEF Detection Procedure the Reader device (or NFC device) SHALL perform the following operations (see also Fig 6) on the MIFARE Classic or MIFARE Plus:

1. Check the existence of the MAD sector(s) (see section 2.4, section 2.5.1 and [MAD]).
2. Authenticate and Read the MAD sector(s): sector 0 for MAD1, or sector 0 and 16 for MAD2 using the Read operation specified in section 5.1.3.

3. If inside the MAD one or more AID(s) equal to the NFC AID related to one or more contiguous sector(s) are found, then go to item 4. Otherwise no NFC AID is detected in the MIFARE Classic or MIFARE Plus tag and the MIFARE Classic or MIFARE Plus tag is not in a valid state.
4. For each NFC Sector, perform the following operations starting from the smallest sector number to the highest one:
   a. Authenticate and read (using the Read operation specified in section 5.1.3) the sector trailer of the NFC Sector using the public key A for NFC Sectors (see Table 6).
   b. If the authentication and the read operations are successful, check the sector trailer of the NFC Sector. Otherwise if the authentication or the read operation fails, a proprietary NFC Sector (see description of the NFC Sector below) is found then go to item f.
   c. If bits 4-7 of the GPB describe the right version number according to the rules defined in section 6.1.1 then go to item d. Otherwise stop the procedure because the MIFARE Classic or MIFARE Plus tag is not in a valid state.
   d. If read access condition field (bit 2-3) value of the GPB is equal to 00b and the write access condition filed (bit 0-1) value of the GPB is equal to either 00b or 11b, read the data blocks of the relative NFC Sector using the Read operation specified in section 5.1.3, look for NDEF Message TLVs, and go to item e. Otherwise if read access field value of the GPB is different from 00h or the write access condition filed (bit 0-1) value of the GPB is different from 00b and 11b, a proprietary NFC Sector (see description of the NFC Sector below) is found then go to item f.
   e. If an NDEF Message TLV is found, this is the (i.e. the first one) mandatory NDEF Message TLV then go to item 5. Otherwise if no NDEF Message TLV is found go to item f.
   f. If available check the next NFC Sector and go to item a. Otherwise if no more NFC Sectors are available, stop the procedure because no NDEF Message TLV is found. The MIFARE Classic or MIFARE Plus tag is not in a valid state.
5. If the length field of the mandatory NDEF Message TLV is different from zero, the NDEF Message (see [NDEF]) is detected in the MIFARE Classic or MIFARE Plus tag and the Reader device MAY use the NDEF Read Procedure or the NDEF Write Procedure (see sections 6.4.2 and 6.4.3). If the length field is equal to zero, no NDEF Message is detected in the MIFARE Classic or MIFARE Plus tag and the Reader device MAY use the NDEF Write Procedure (see section 6.4.3, the tag might be in INITIALISED state).

The NDEF Detection Procedure does not relate to a valid NDEF Message (see [NDEF]). It reads the NDEF Message length from the length field of the NDEF Message TLV but does not parse the NDEF Message.

The Reader device SHALL ignore and jump over the proprietary NFC Sectors. The proprietary NFC Sector is defined as an NFC Sector that is: either non-authenticable with the public key A for NFC Sectors or the read access field value of the GPB is different from 00b or the write access condition filed (bit 0-1) value of the GPB is different from 00b and 11b.

Each time an Authentication operation, a Read operation or a Write operation fails, the MIFARE Classic or MIFARE Plus remains silent and it does not respond anymore to any

commands. In this situation in order to continue the NDEF Detection Procedure the MIFARE Classic or MIFARE Plus needs to be re-activated and selected.

6.4.2 NDEF Read Procedure

The NDEF Read Procedure is used by the Reader device to read the NDEF Message from the mandatory NDEF Message TLV. Before reading the NDEF Message the NDEF Detection Procedure SHALL be executed (see section 6.4.1), and the MIFARE Classic or MIFARE Plus tag SHALL be in a valid state.

Using the NDEF Read Procedure the Reader device SHALL read the whole NDEF Message from the mandatory NDEF Message TLV using one or more Read operations (see section 5.1.3). The length of the NDEF Message to be read is provided from the length field of the mandatory NDEF Message TLV (see section 2.6.1).

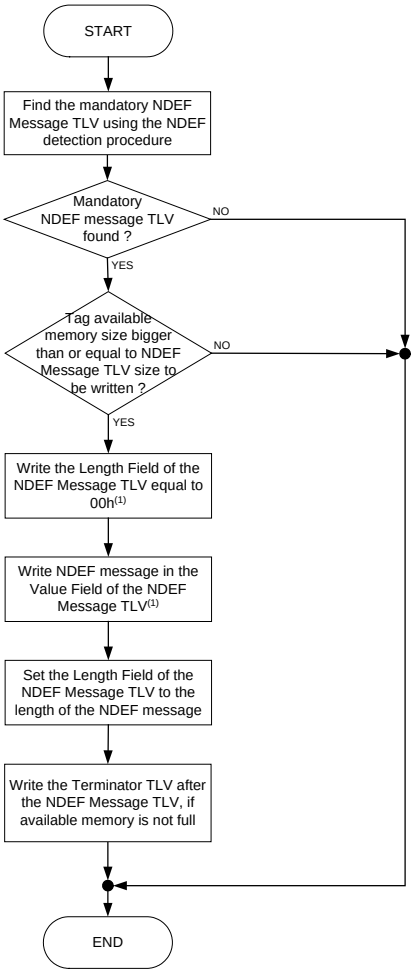
If the mandatory NDEF Message TLV is stored in one or more NFC Sectors, the Reader device SHALL be able to authenticate all these sectors with the public Key A for NFC Sectors (see Table 6). In case the authentication procedure fails the MIFARE Classic or MIFARE Plus tag is not in a valid state.

6.4.3 NDEF Write Procedure

The NDEF Write Procedure SHALL be used by the Reader device to write the mandatory NDEF Message TLV containing an NDEF Message inside a MIFARE Classic or MIFARE Plus tag.

The NDEF Write Procedure uses the Read and Write operations (see section 5.1.3 and section 5.1.4).

To write the NDEF Message the MIFARE Classic or MIFARE Plus tag SHALL be in INITIALISED or READ/WRITE state i.e. the mandatory NDEF Message TLV SHALL be already present inside the MIFARE Classic or MIFARE Plus tag.



(1) Please see the NDEF Write Procedure description in section 6.4.3 for more detailed information.

Fig 7. NDEF Write Procedure

To execute the NDEF Write Procedure, the Reader device SHALL do the following operations (see also Fig 8) on the MIFARE Classic or MIFARE Plus tag:

1. Use the NDEF Detection Procedure (see section 6.4.1) to find the mandatory NDEF Message TLV. If the mandatory NDEF Message TLV is found go to item 2. Otherwise if no NDEF Message TLV is found, end the procedure.
2. If the available memory size for the NDEF Message TLV is equal to or bigger than the NDEF Message size, the operations below SHALL be done in the following order using one or more Write operations (see section 5.1.4):
   a. the length field of the mandatory NDEF Message TLV SHALL be one byte long and its value SHALL be set to 00h,
   b. the new NDEF Message SHALL be written in the value field of the mandatory NDEF Message TLV, and

c. the length field of the mandatory NDEF Message TLV SHALL be updated with the length of the NDEF Message.

Otherwise if not enough memory space is available in the MIFARE Classic or MIFARE Plus tag, the NDEF Message SHALL NOT be written in the MIFARE Classic or MIFARE Plus tag.

3. If the item 2 is done successfully, the Reader device SHALL write the Terminator TLV in the next byte after the NDEF Message TLV using the Write operation (see section 5.1.4). The Terminator TLV SHALL NOT be written when the mandatory NDEF Message TLV ends at the last byte of the last available NFC Sector i.e. the NFC Sector with the biggest sector number.

Concerning the operation item 2.b, the writing of the value field of the found NDEF Message TLV SHALL leave 1 or 3 bytes for the length field (see section 2.6) that are needed by the next operation item 2.c to store the length of the NDEF Message.

The NDEF Write Procedure does not change the starting position of the mandatory NDEF Message TLV.

The NDEF Write Procedure MAY write the NDEF Message TLV across contiguous NFC Sectors with the exception of MAD sector 16 in case MIFARE Classic 4k and MIFARE Plus with 4 Kbytes is used (see also the definition of contiguous NFC Sectors in section 6.1).

The available memory size for the mandatory NDEF Message TLV is calculated from the position of the mandatory NDEF Message TLV as the sum of:

- the free memory space of the NFC Sector containing the mandatory NDEF Message TLV. The free memory space starts from the beginning of the mandatory NFC Message TLV and finishes at the end of the NFC Sector, and
- the whole memory space of the NFC Sectors following the sector containing the mandatory NDEF Message TLV. The following NFC Sectors MAY have a size of 48 bytes (3 blocks) or 240 bytes (15 blocks). The information about the following available NFC Sectors SHALL be retrieved from the MAD sectors.

For the Write operation the reading of not completely updated blocks is needed first (see section 5.1.4) when e.g. the NDEF Message TLV starts in the middle of a block.

6.4.4 State Changes

This section describes the possible state changes of the MIFARE Classic or MIFARE Plus tag. Fig 8 shows the states and the state change (also called transition) between them. In this application note the only specified transition is from INITIALISED to READ/WRITE.

The Reader device MAY issue a MIFARE Classic or MIFARE Plus tag in INITIALISED state, READ/WRITE state or even in READ-ONLY state.

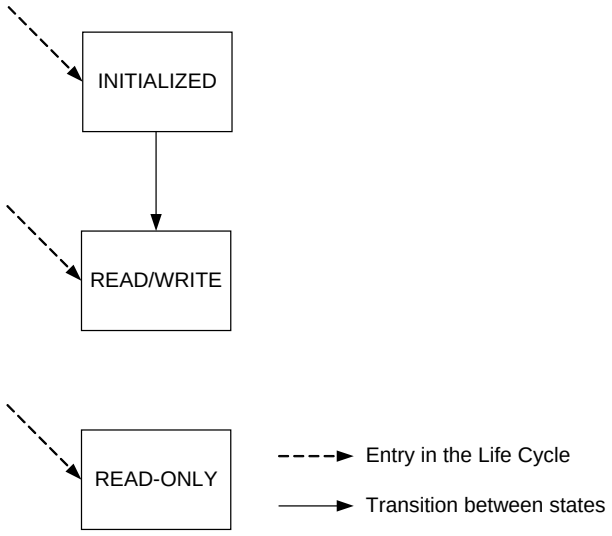


Fig 8. Life Cycle with State Change (transition)

6.4.4.1 Transition from INITIALISED to READ/WRITE

To perform the transition from INITIALISED to READ/WRITE the Reader device SHALL do the following operation: a non-empty NDEF Message TLV (length field different from zero) SHALL replace the previous empty NDEF Message TLV using the NDEF Write Procedure (see section 6.4.3). The NDEF Message TLV is the mandatory one detected by means of the NDEF Detection Procedure (see section 6.4.1).

The empty NDEF Message (see chapter 3) MAY be used to replace a non-empty NDEF Message.

7. ANNEX A: Empty NDEF Message

An empty NDEF Message (see [NDEF]) is defined as an NDEF Message composed of one NDEF record. The NDEF record uses the NDEF short-record layout (SR=1b) with: Type Name Format (TNF) field value equal to 00h (empty, TYPE_LENGTH=00h, PAYLOAD_LENGTH=00h), no ID_LENGTH field (IL=0b), MB=1b, ME=1b, CF=0b. The empty NDEF record (i.e. the empty NDEF Message) is composed of 3 bytes and it is equal to D00000h.

8. ANNEX B: Example of sector trailer using MAD1

This example refers to a MIFARE Classic 1k tag with MAD1 in sector 0. The trailer of sector 0 is set as described in Table 13 (GPB is the General Purpose Byte see [MF1K], and [MAD]).

Table 13. Example for sector trailer for sector 0, block 3 settings

Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	Byte 8	Byte 9	Byte 10	Byte 11	Byte 12	Byte 13	Byte 14	Byte 15
Key A						Access Conditions			GPB	Key B					
A0h	A1h	A2h	A3h	A4h	A5h	78h	77h	88h	C1h	Secret Key					

9. ANNEX C: Access bits Coding into byte 6 to 8 of the sector trailer

In section 2.5 is shown the coding of the access bits 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 access bit values into the relative byte 6 to 8 values.

Table 14. Access bits coding of byte 6 to 8 of the sector trailer.

Life Cycle State	Access Bits	MAD1 and MAD2 Sectors Access Bits Values	NFC Sectors Access Bits Values	MAD1 and MAD2 Sector Trailer Bytes Values Byte 6	Byte 7	Byte 8	NFC Sector Trailer Bytes Values Byte 6	Byte 7	Byte 8
INITIALIZED and READ/WRITE	$C1_0$ $C2_0$ $C3_0$	100b[i]	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[i]	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						

i. 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.

10. ANNEX D: Example of MIFARE Classic 1k in INITIALISED State

In this ANNEX an example of MIFARE Classic 1k in INITIALISED state is given (see Fig 9).

In this example the sectors from sector 1 to sector 15 are NFC Sectors. The MAD sector contains 15 NFC AID equal to 03E1h. Being in INTIALISED state the MIFARE Classic 1k contains an empty NDEF message TLV. At the end of the empty NDEF Message TLV a Terminator TLV is present.

The GPB of the NFC Sector is equal to 40h indicating version number 1.0 and read/write access granted.

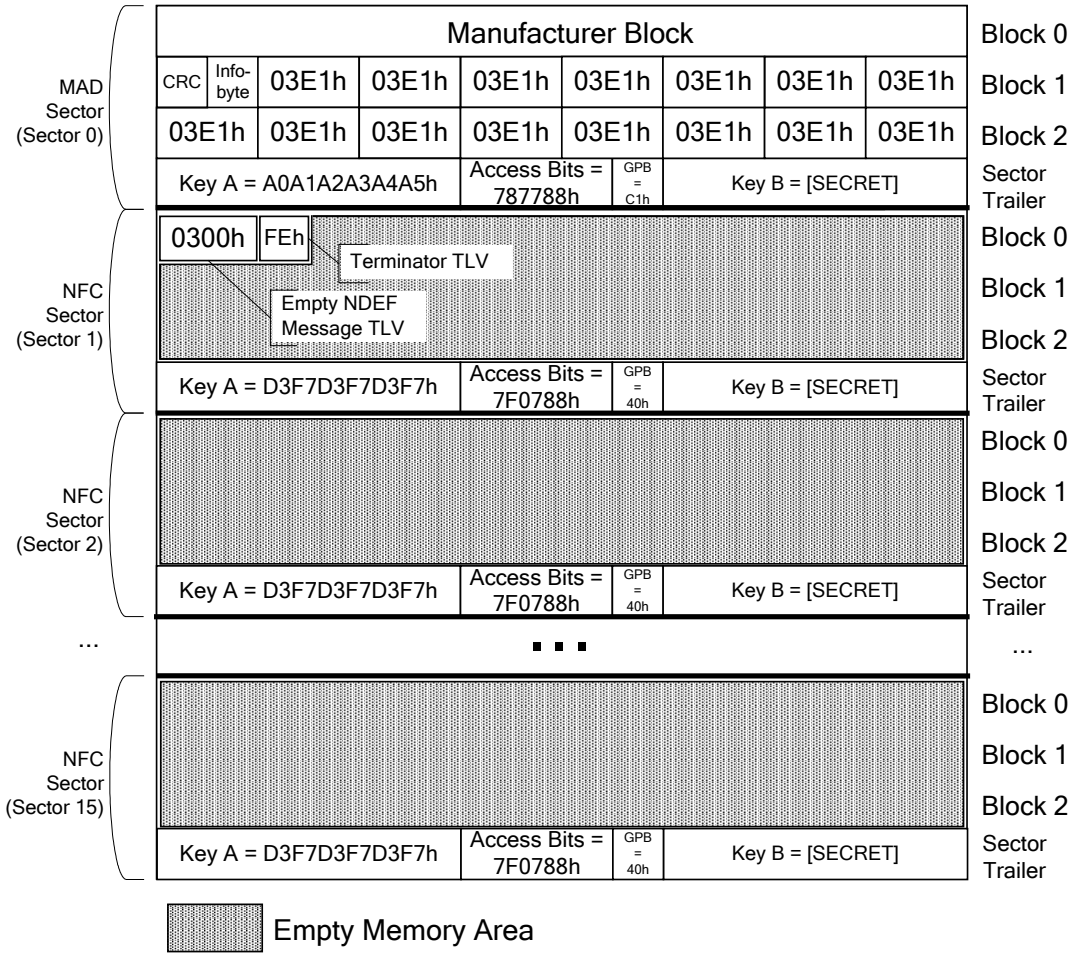


Fig 9. Example of MIFARE Classic 1k in INITIALISED State

11. ANNEX E: Example of MIFARE Plus with 2 Kbytes in INITIALISED State

In this ANNEX an example of MIFARE Plus with 2 Kbytes in INITIALISED state is given (see Fig 11).

In this example the sectors from sector 1 to sector 15 and from sector 17 to sector 31 are NFC Sectors. The MAD sectors contain overall 30 NFC AID equal to 03E1h in sector 0 and sector 16. Being in INTIALISED state the MIFARE Plus with 2 Kbytes contains an empty NDEF message TLV. At the end of the empty NDEF Message TLV a Terminator TLV is present.

The GPB of the NFC Sector is equal to 40h indicating version number 1.0 and read/write access granted.

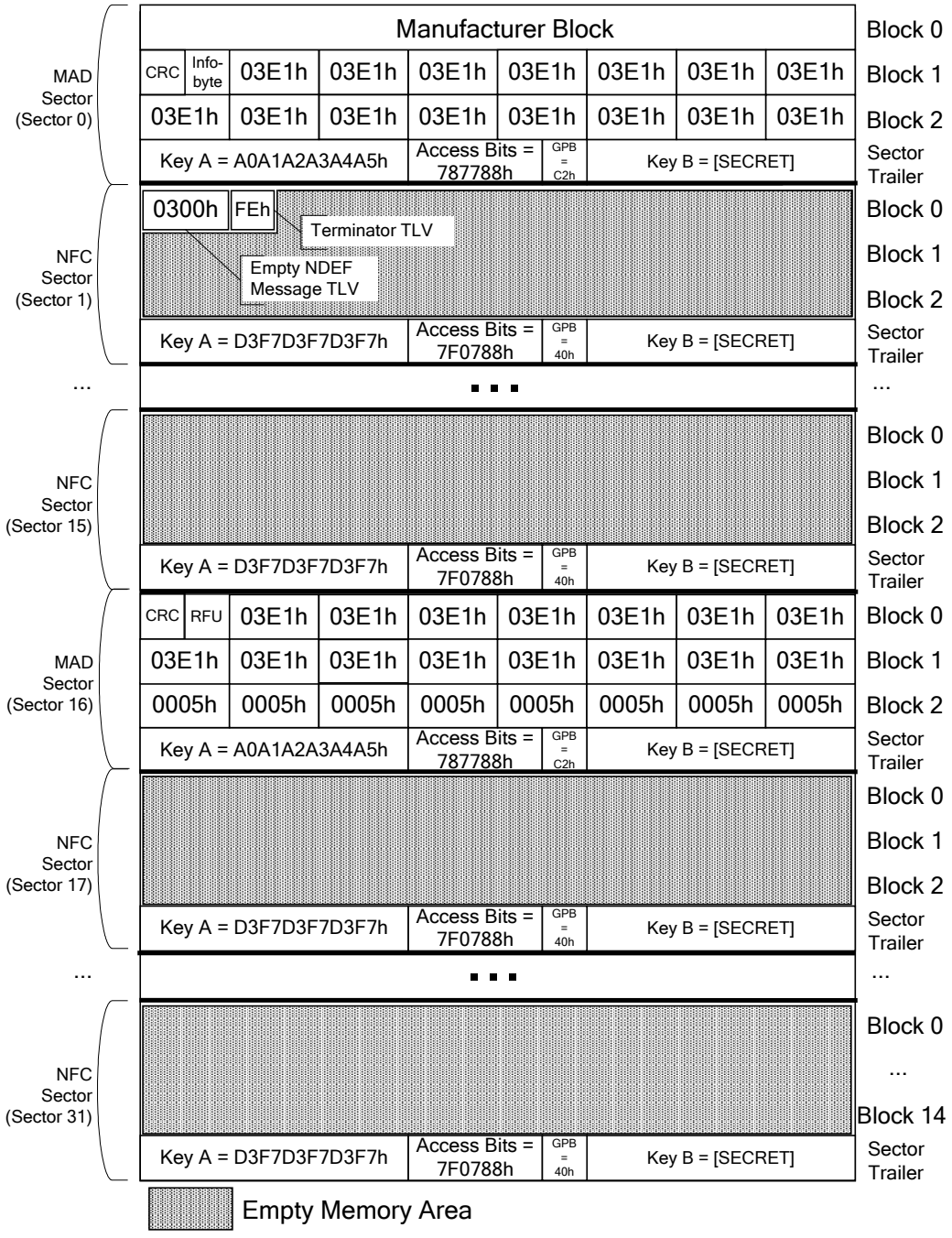


Fig 10. Example of MIFARE Plus with 2 Kbytes in INITIALISED State

12. ANNEX F: Example of MIFARE Classic 4k or MIFARE Plus with 4 Kbytes in INITIALISED State

In this ANNEX an example of MIFARE Classic 4k in INITIALISED state is given (see Fig 11).

In this example the sectors from sector 1 to sector 15 and from sector 17 to sector 39 are NFC Sectors. The MAD sectors contain overall 38 NFC AID equal to 03E1h in sector 0 and sector 16. Being in INTIALISED state the MIFARE Classic 4k contains an empty NDEF message TLV. At the end of the empty NDEF Message TLV a Terminator TLV is present.

The GPB of the NFC Sector is equal to 40h indicating version number 1.0 and read/write access granted.

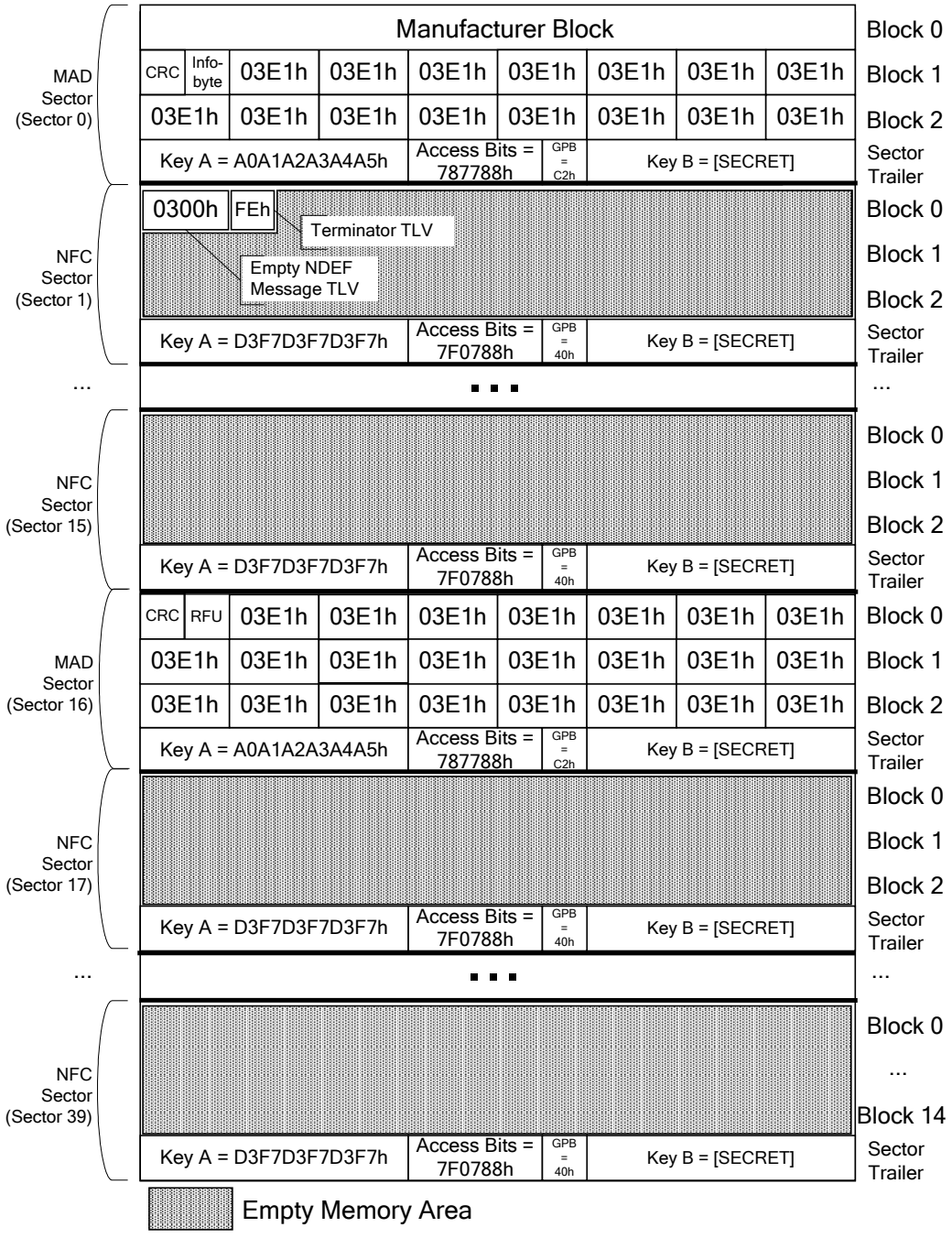


Fig 11. Example of MIFARE Classic 4k or MIFARE Plus with 4 Kbytes in INITIALISED State

13. Legal information

13.1 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.

13.2 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 national 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.

13.3 Licenses

ICs with DPA Countermeasures functionality

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

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. A license for the patents portfolio of NXP B.V. for the NFC standards needs to be obtained at Via Licensing, the pool agent of the NFC Patent Pool, e-mail: info@vialicensing.com.

13.4 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.

14. Contents

1. Introduction 3
1.1 Applicable Documents 3
1.2 Convention and notations 4
1.2.1 Representation of numbers 4
1.3 Special Word Usage 4
1.4 Glossary 4
2. Memory Structure and Management 6
2.1 MIFARE Classic 1k Layout 6
2.2 MIFARE Plus X/S with 2 Kbytes Layout 7
2.3 MIFARE Classic 4k and MIFARE Plus X/S with 4 Kbytes Layout 8
2.4 MIFARE Application Directory 9
2.5 MIFARE Classic and MIFARE Plus Access Mechanism (Access Bits) 10
2.5.1 MAD Sector Access 11
2.5.2 NFC Sector Access 12
2.6 TLV blocks 13
2.6.1 NDEF Message TLV 15
2.6.2 Proprietary TLV 15
2.6.3 NULL TLV 15
2.6.4 Terminator TLV 15
3. RF Interface 16
4. Framing/Transmission Handling 16
5. Command Set 17
5.1 Tag Commands and Responses Set 17
5.1.1 Identification and Selection Operation 17
5.1.2 Authentication Operation 17
5.1.3 Read operation 17
5.1.4 Write operation 17
6. NDEF Detection and Access 18
6.1 NDEF Management 18
6.1.1 Version Treating 19
6.2 NDEF Storage 20
6.3 Life Cycle 20
6.3.1 INITIALISED State 21
6.3.2 READ/WRITE State 21
6.3.3 READ-ONLY State 21
6.4 Command Sequence Description 21
6.4.1 NDEF Detection Procedure 21
6.4.2 NDEF Read Procedure 25
6.4.3 NDEF Write Procedure 25
6.4.4 State Changes 27
6.4.4.1 Transition from INITIALISED to READ/WRITE 28
7. ANNEX A: Empty NDEF Message 29
8. ANNEX B: Example of sector trailer using MAD1 29
9. ANNEX C: Access bits Coding into byte 6 to 8 of the sector trailer 29
10. ANNEX D: Example of MIFARE Classic 1k in INITIALISED State 30
11. ANNEX E: Example of MIFARE Plus with 2 Kbytes in INITIALISED State 31
12. ANNEX F: Example of MIFARE Classic 4k or MIFARE Plus with 4 Kbytes in INITIALISED State 33
13. Legal information 35
13.1 Definitions 35
13.2 Disclaimers 35
13.3 Licenses 35
13.4 Trademarks 35
14. Contents 36

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

Date of release: 3 May 2011
130412
Document identifier: AN1304