

NXP Type MF1K/4K Tag Operation

Storing NFC Forum data in Mifare Standard 1k/4k

Rev. 1.1 — 21 August 2007

Application Note

Document information

Info	Content
Keywords	NFC Forum, NFC Forum data mapping, Mifare Standard 1k, Mifare Standard 4k, Mifare Standard 1k/4k,
Abstract	<p>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.</p> <p>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.</p> <p>This document extends the tag types of the NFC Forum describing how the Reader device (called NFC Forum device) can store NDEF data inside either Mifare Standard 1k or Mifare Standard 4k.</p>

Revision history		
Rev	Date	Description
0.1	2006-06-29	First draft version
1.0	2006-11-11	Final Revision
1.1	2007-08-21	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. 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 or NFC Forum data) inside a contactless tag product a mapping model is required.

The Mifare Standard 1k/4k tag product (see [MF1K, MF4K]) is a contactless card currently available with 1Kbyte and 4Kbyte of EEPROM memory. The Mifare Standard 1k/4k supports file 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 application note describes:

- the mapping model to store one NDEF Message (or NDEF formatted data) inside Mifare Standard 1k/4k card platform,
- the command set and the life cycle of the Mifare Standard 1k/4k to manage the NDEF Message, and
- how the Reader device (also called NFC Forum device) can detect, read and write the NDEF Message in the Mifare Standard 1k/4k 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 001052.
[MF4K]	“MF1 IC S70, Standard 4 kByte Card IC Functional Specification”, NXP Semiconductors, Product Data Sheet, Revision 4.0, 7 February 2007, Document Identifier 043540.
[MAD]	“AN MAD, MIFARE Application Directory”, NXP Semiconductors, Application Note, Revision 3.0, 4 May 2007, Document Identifier 001830.

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 tiling 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 Acronyms or Definitions or 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 Standard 1k/4k contactless card, see [MF1K, MF4K]
CC	Capability Container, the CC stores control data for managing the NFC Forum defined 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

Term	Definition
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]. In case of Mifare Standard 1k the MAD sector is the sector 0, and in case of Mifare Standard 4k the MAD sectors are the sector 0 and the sector 16.
msb	most significant bit
MSB	most significant byte
NDEF	NFC Data Exchange Format, 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
NFC Forum defined data	Data contained inside a Mifare Standard 1k/4k defined by the NFC Forum e.g. NDEF Message
NFC Forum device	Reader device compliant to the NFC Forum
NFC Forum sector	Sector that contains NFC Forum 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 Standard 1k/4k contactless card
Proprietary TLV	TLV block that contains proprietary data
Reader device / Reader	Reader/writer for contactless cards. It may be a NFC Forum device or a PCD device.
RF	Radio Frequency
RFU	Reserved for Future Use
SAK	Selective Acknowledge see [ISOIEC 14443-3]
tag	A Mifare Standard 1k/4k contactless card, see [MF1K, MF4K]
Terminator TLV	Last TLV block of the tag

Term	Definition
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] specification

2. Memory Structure and Management

Mifare Standard 1k and 4k 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]).

[Table 2](#) gives an overview of the Mifare Standard products.

Table 2. Overview on Mifare Standard products

	Mifare Standard 1k	Mifare Standard 4k
Name	MF1 S50	MF1 S70
EEPROM	1 Kbyte	4 Kbyte

The memory structure (or memory layout) is defined for each Mifare Standard 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. Byte 15 of block 3 in sector 15 for Mifare Standard 1k or byte 15 of block 15 in sector 39 for Mifare Standard 4k indicates the LSB.

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 Standard 1k and Mifare Standard 4k.

2.1 Mifare Standard 1k Layout

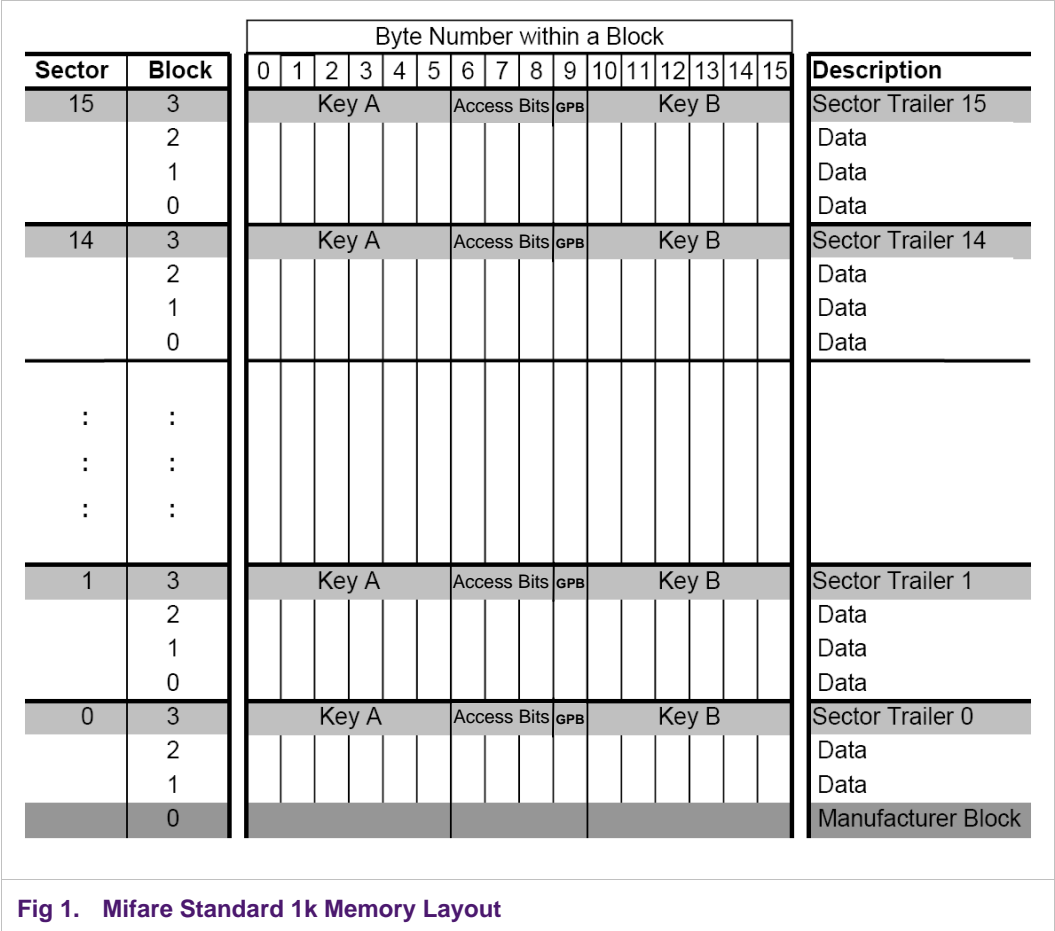
[Fig 1](#) outlines the memory layout of the Mifare Standard 1k.

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 4 bytes Unique Identifier (UID, also called Serial Number, see [ISOIEC 14443-3] for a detailed definition).

For more information about Mifare Standard 1k see [MF1K].



2.2 Mifare Standard 4k Layout

[Fig 2](#) outlines the memory layout of the Mifare Standard 4k tag.

The memory area of the Mifare Standard 4k 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 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 4 bytes Unique Identifier (UID, also called Serial Number, see [ISOIEC 14443-3] for a detailed definition).

For more information about Mifare Standard 4k see [MF4K].

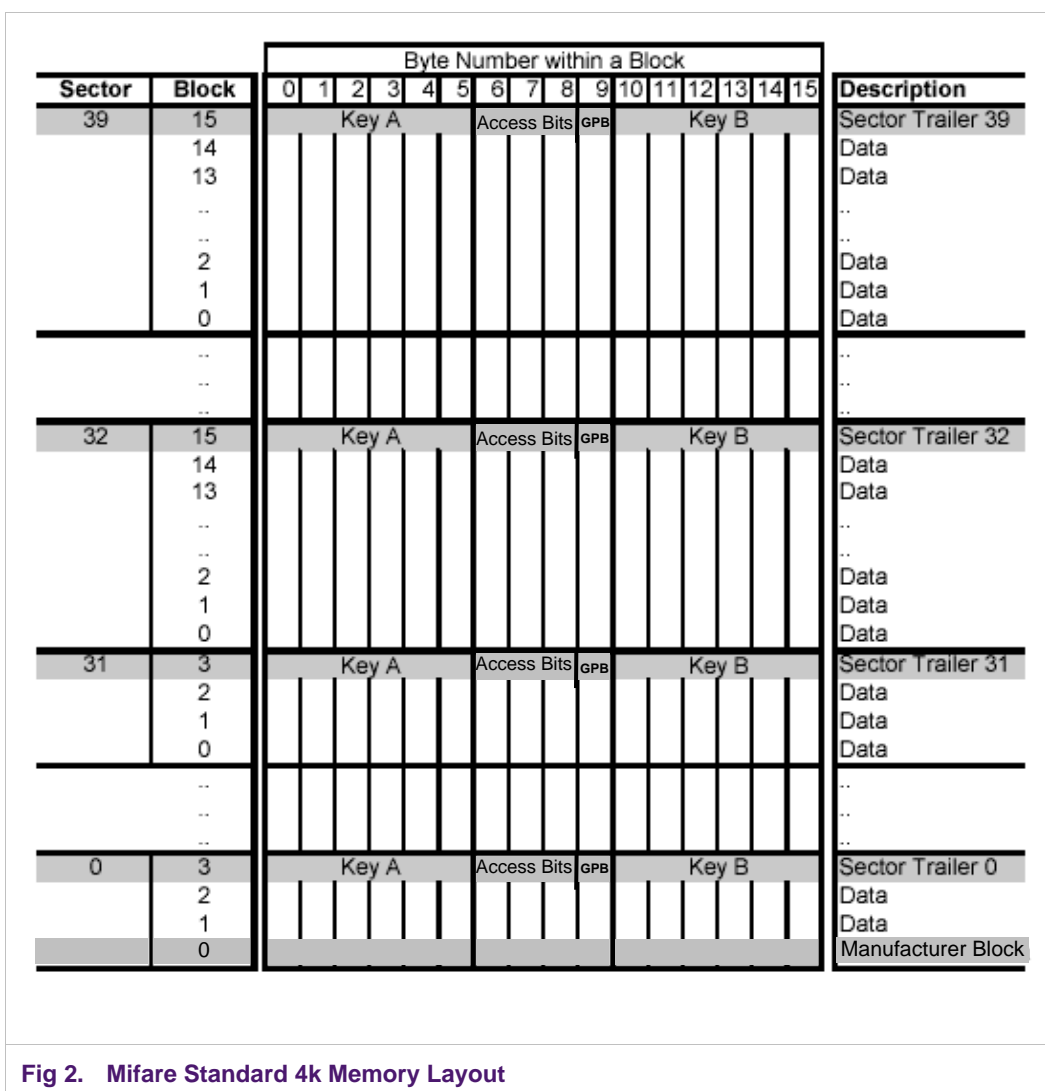


Fig 2. Mifare Standard 4k Memory Layout

2.3 Mifare Application Directory

The memory mapping of NFC Forum data for the Mifare Standard 1k or 4k 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) for Mifare Standard 1k, and
2. Mifare application directory 2 (MAD2) for Mifare Standard 4k.

To each application the MAD associates a unique application identifier (AID). The application identifiers (AIDs) are stored inside sector 00h for the Mifare Standard 1k, or sectors 00h and 10h for the Mifare Standard 4k. Sector 00h and sector 10h (or sector 0 and sector 16) are called MAD sectors.

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).

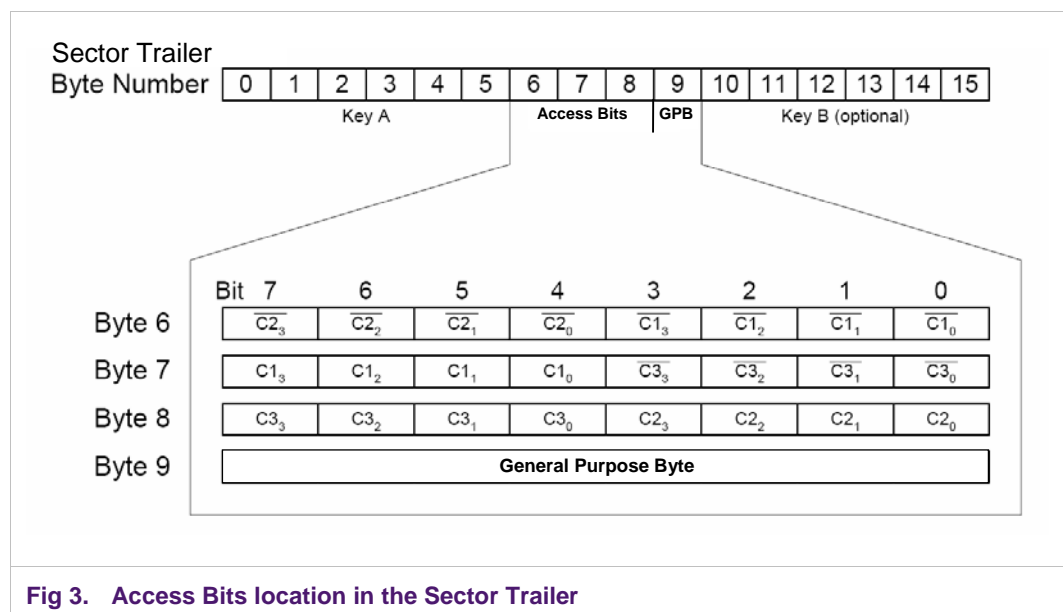
All currently unused sectors SHOULD be write-protected with secret keys defined by the tag issuer in order to prevent unintended redefinition of access conditions and keys. It is RECOMMENDED to use different keys for all free sectors. This enables future release of some sectors to new service providers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

2.4 Mifare Standard 1k/4k Access Mechanism (Access Bits)

Mifare Standard 1k/4k provides a mechanism based on keys and access bits to grant read and write access (see [MF1K, MF4K]).

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 3. 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.



The General Purpose Byte (GPB, see [section 2.1](#) and [section 2.2](#)) of the sector trailer is not used in the access mechanism of Mifare Standard 1k/4k 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.

2.4.1 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:

- for Mifare Standard 1k (MAD1) the MAD sector is 00h (sector 0), and
- for Mifare Standard 4k (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]).

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 Standard 1k/4k 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[1]	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: <ul style="list-style-type: none"> • 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.
[1] 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[1]	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: <ul style="list-style-type: none"> • 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.
[1] Recommended value for the access bits C1 ₀ C2 ₀ C3 ₀ of sector 0 (manufacturer block).		

2.4.2 NFC Forum Sector Access

A sector MAY contain NFC Forum defined data. A sector that contains NFC Forum defined data is called NFC Forum sector.

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

Table 6. Public Key A value of NFC Forum 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 Forum sectors are set to either:

- as described in [Table 7](#) if the NFC Forum sector has read and write access granted, or
- as described in [Table 8](#) if the NFC Forum sector has read-only access granted.

In this context the term read and write access granted means that for NFC Forum 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 Forum 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 Forum 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: <ul style="list-style-type: none"> • 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 Forum 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: <ul style="list-style-type: none"> • 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.

2.5 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 4](#) 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 FFEh. The value FFFFh is reserved for future use (RFU).

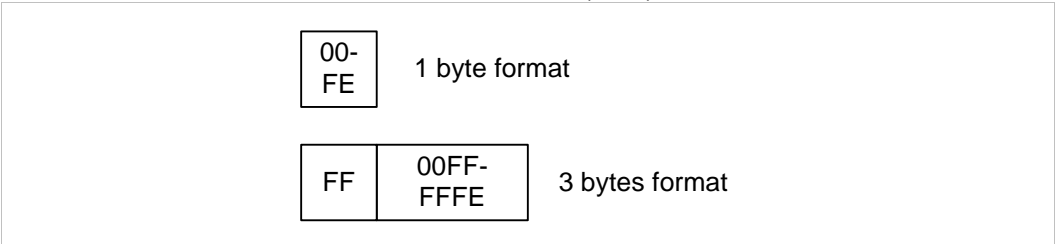


Fig 4. Length Field Formats

- 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 Forum sector (sector containing NFC Forum defined data) with the smallest address.
- A TLV block MAY be memorized across two or more NFC Forum sectors.
- If present the Terminator TLV is the last TLV block on the Mifare Standard 1k/4k 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.

2.5.1 NDEF Message TLV

At least one NDEF Message TLV SHALL be always present inside the Mifare Standard 1k/4k 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](#).

2.5.2 Proprietary TLV

The Proprietary TLV contains proprietary information. A Mifare Standard 1k/4k 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 Value field.

V SHALL contain any proprietary data.

2.5.3 NULL TLV

The NULL TLV MAY be used for padding of the data area. A Mifare Standard 1k/4k 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.

2.5.4 Terminator TLV

The Terminator TLV MAY be present inside the Mifare Standard 1k/4k 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 Standard 1k/4k complies with the RF interface as defined in the [ISO/IEC 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 Forum device, and the PICC is called Mifare Standard 1k/4k tag.

4. Framing/Transmission Handling

The framing and transmission handling of the Mifare Standard 1k/4k tag SHALL follow [MF1K, MF4K].

5. Command Set

This chapter describes the command set as well as the overall state diagram of the Mifare Standard 1k/4k tag. It provides the basis to: detect and activate the Mifare Standard 1k/4k tag, detect the NFC Forum data, get read and write access to the NFC Forum data, and deactivate the Mifare Standard 1k/4k tag.

5.1 Tag Commands and Responses Set

The Mifare Standard 1k/4k tag accepts the following command set, sent by the Reader device. [Table 10](#) shows the command set (here called memory operations) of the Mifare Standard 1k/4k tag (see [MF1K, MF4K]).

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 and 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, 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 Standard 1k/4k 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 NFC Forum defined data (e.g. NDEF Message) SHALL be stored and accessed in the Mifare Standard 1k/4k tag.

The NDEF Message that this application note manages inside a Mifare Standard 1k/4k, 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 NFC Forum defined data (e.g. NDEF Message) inside the Mifare Standard 1k/4k tag the MAD SHALL be used (see [section 2.3](#)) together with the GPB of the NFC Forum sectors.

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

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

One or more NFC Forum sectors MAY be present inside a Mifare Standard 1k/4k tag.

If more than one NFC Forum sector is present, the NFC Forum sectors SHALL be contiguous. In case of Mifare Standard 4k, it SHALL be considered contiguous a sequence of NFC Forum sectors that includes the MAD sector 16.

Example of contiguous NFC Forum sectors are:

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

An example of non-contiguous NFC Forum sectors is:

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

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

The General Purpose Byte (GPB, see [section 2.1](#) and [section 2.2](#)) of each NFC Forum sector provides information about the version number of the mapping model used to store the NFC Forum defined data into the Mifare Standard 1k/4k (see [section 6.1.1](#)) and the write access of the NFC Forum 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 Forum 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 Standard 1k/4k tag the NFC Forum 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 Standard 1k/4k 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 Forum sectors contains the mapping version number of the applied mapping model of the Mifare Standard 1k/4k 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 Standard 1k/4k 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 Standard 1k/4k tag and SHALL use all features of the applied mapping document to this Mifare Standard 1k/4k 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 Standard 1k/4k tag can be accessed. The Reader device SHALL use all its features and SHALL access this Mifare Standard 1k/4k tag.
3	If major NFCDevVNo is smaller than major MSVNo	Incompatible data format. The Reader device cannot understand the Mifare Standard 1k/4k tag data. The Reader device SHALL reject this Mifare Standard 1k/4k 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 Standard 1k/4k tag. On the contrary, in case the Reader device has not the support from previous version, it SHALL reject the Mifare Standard 1k/4k 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 2.5.1](#)) using one or more NFC Forum sectors. NFC Forum sectors are identified by the NFC Forum AID in the MAD sector(s).

6.3 Life Cycle

The NFC Forum sectors of a Mifare Standard 1k/4k tag MAY be in the following states INITIALISED, READ/WRITE or READ-ONLY. The NFC Forum sectors SHALL be in only one state in a specific moment in time. The state SHALL be reflected by the content of the NFC Forum sectors. The state is not related to a single NFC Forum sector but to all NFC Forum sectors together. The states are described in the following sections.

If the Mifare Standard 1k/4k tag contains only NFC Forum sectors the state of the NFC Forum sectors is called the state of the Mifare Standard 1k/4k tag. In the description below the state of the Mifare Standard 1k/4k tag is confused with (i.e. equal to) the state of the NFC Forum 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 Standard 1k/4k tags.

The different states are identified comparing the GPB of the NFC Forum 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 2.4](#), are not used in this application note to identify the specific state.

If the Mifare Standard 1k/4k tag is not in a valid state according to this application note, the NFC Forum data of the Mifare Standard 1k/4k tag in all NFC Forum sectors SHALL be ignored. The reasons MAY be:

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

6.3.1 INITIALISED State

A Mifare Standard 1k/4k 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 Forum 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 Forum device MAY modify the content of the mandatory NDEF Message TLV writing an NDEF Message in it. The [Annex D in chapter 10](#) and the [Annex E in chapter 11](#) show two examples of respectively Mifare Standard 1k and Mifare Standard 4k both in INITIALISED state.

6.3.2 READ/WRITE State

A Mifare Standard 1k/4k 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 Forum 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 Forum 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 Standard 1k/4k 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 Forum sector(s), and
- the length field of the mandatory NDEF Message TLV SHALL be different from zero.

In READ-ONLY state all NFC Forum sectors have read-only access granted. The Mifare Standard 1k/4k 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 NFC Forum defined data e.g. the mandatory NDEF Message TLV inside the NFC Forum sector(s). The different state

changes or transitions between the states of the Mifare Standard 1k/4k 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 Forum sector (see [section 2.4](#)).

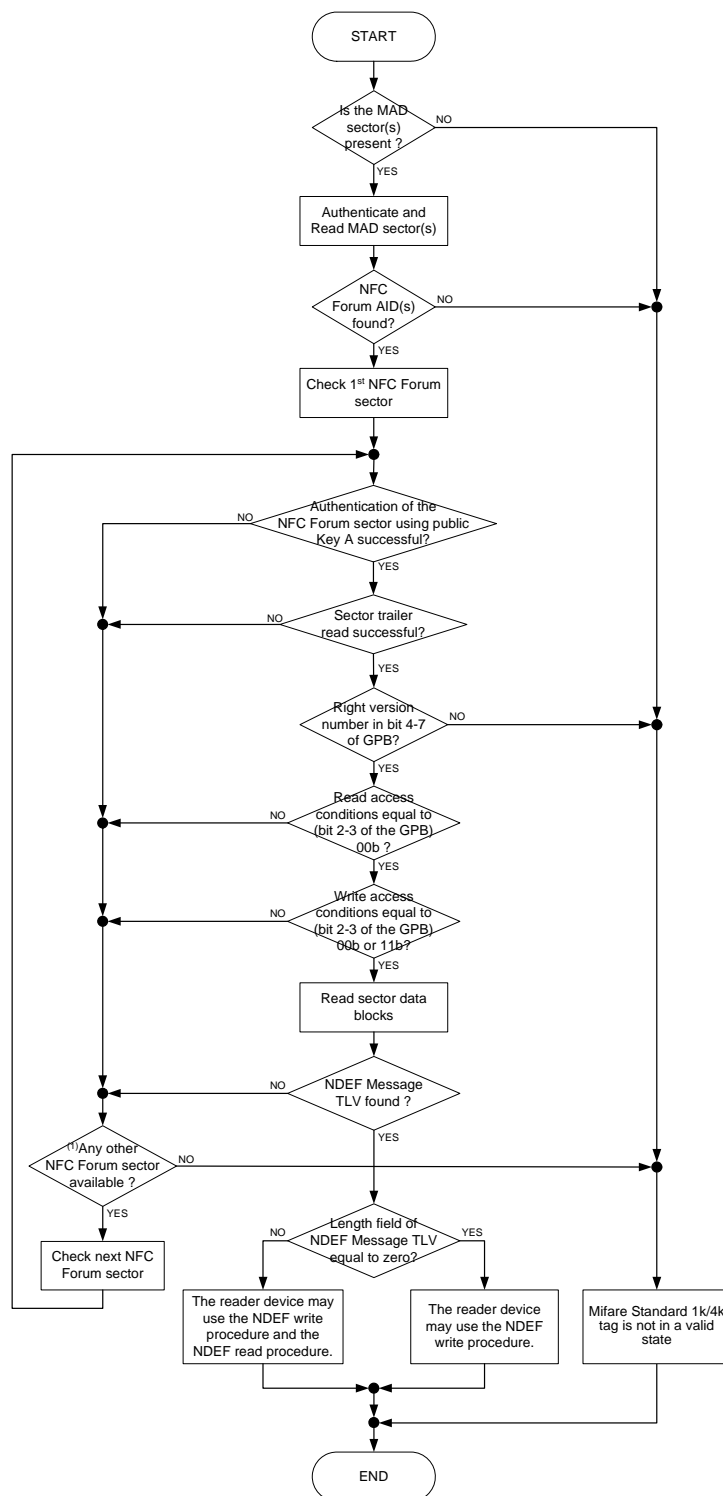
6.4.1 NDEF Detection Procedure

The NDEF Detection Procedure SHALL be used to detect the mandatory NDEF Message (see [NDEF]) inside a Mifare Standard 1k/4k tag.

The NDEF Detection Procedure is based on the check of:

- the MAD sector(s),
- the NFC Forum 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 Standard 1k/4k 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 Standard 1k/4k 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 5. NDEF Detection Procedure

To execute the NDEF Detection Procedure the Reader device (or NFC Forum device) SHALL perform the following operations (see also [Fig 5](#)) on the Mifare Standard 1k/4k:

1. Check the existence of the MAD sector(s) (see [section 2.3](#), [section 2.4.1](#) 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 Forum AID related to one or more contiguous sector(s) are found, then go to item 4. Otherwise no NFC Forum AID is detected in the Mifare Standard 1k/4k tag and the Mifare Standard 1k/4k tag is not in a valid state.
4. For each NFC Forum 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 Forum sector using the public key A for NFC Forum sectors (see [Table 6](#)).
 - b. If the authentication and the read operations are successful, check the sector trailer of the NFC Forum sector. Otherwise if the authentication or the read operation fails, a proprietary NFC Forum sector (see description of the NFC Forum 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 Standard 1k/4k 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 field (bit 0-1) value of the GPB is equal to either 00b or 11b, read the data blocks of the relative NFC Forum 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 field (bit 0-1) value of the GPB is different from 00b and 11b, a proprietary NFC Forum sector (see description of the NFC Forum 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 Forum sector and go to item a. Otherwise if no more NFC Forum sectors are available, stop the procedure because no NDEF Message TLV is found. The Mifare Standard 1k/4k 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 Standard 1k/4k 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 Standard 1k/4k 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 Forum sectors. The proprietary NFC Forum sector is defined as an NFC Forum sector that is: either non-authenticable with the public key A for NFC Forum sectors or the read access field value of the GPB is different from 00b or the write access condition field (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 Standard 1k/4k remains silent and it does not respond anymore to any commands. In this situation in order to continue the NDEF Detection Procedure the Mifare Standard 1k/4k 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 Standard 1k/4k 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 2.5.1](#)).

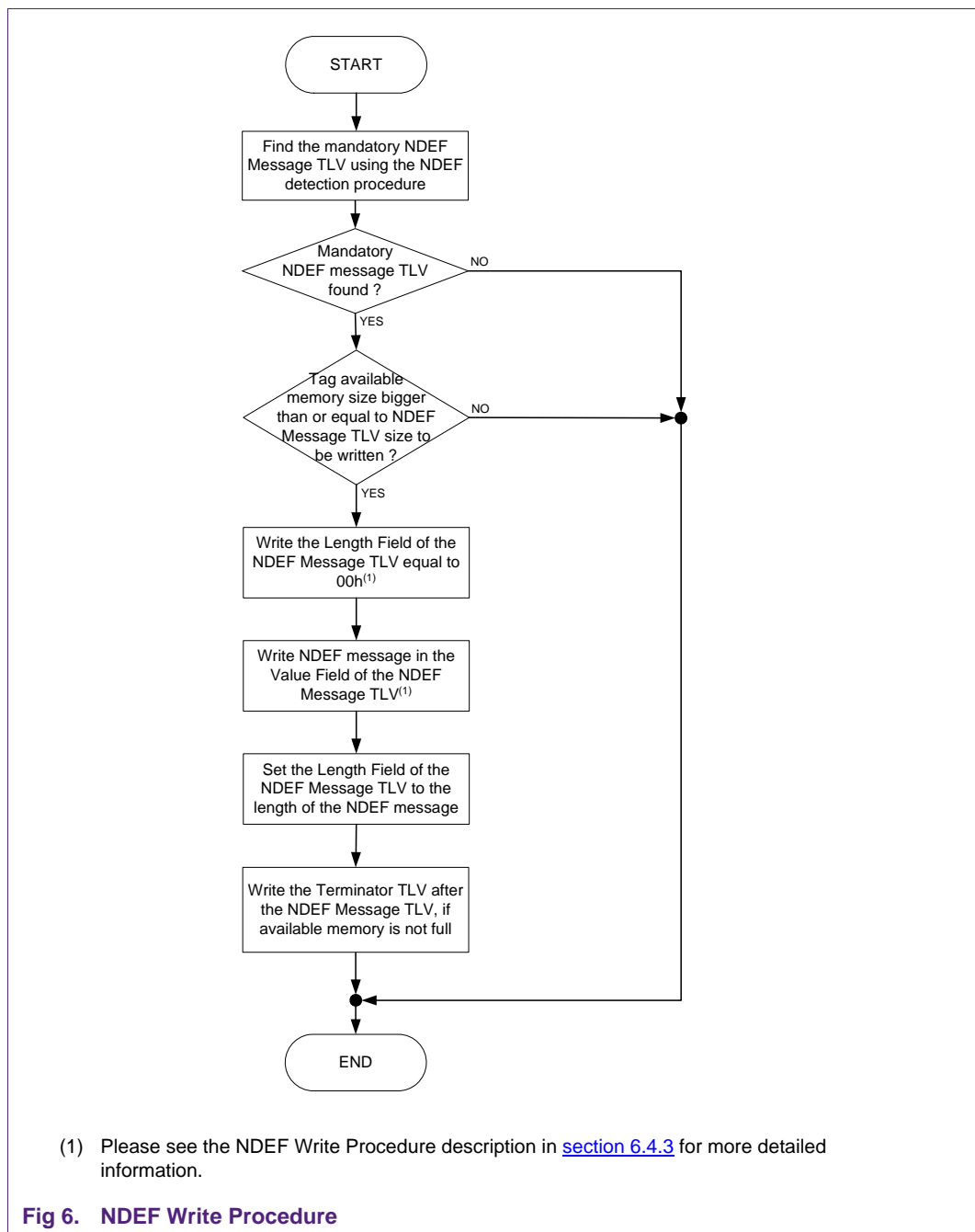
If the mandatory NDEF Message TLV is stored in one or more NFC Forum sectors, the Reader device SHALL be able to authenticate all these sectors with the public Key A for NFC Forum sectors (see [Table 6](#)). In case the authentication procedure fails the Mifare Standard 1k/4k tag is not in a valid state.

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 Standard 1k/4k 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 Standard 1k/4k tag SHALL be in INITIALISED or READ/WRITE state i.e. the mandatory NDEF Message TLV SHALL be already present inside the Mifare Standard 1k/4k tag.



To execute the NDEF Write Procedure, the Reader device SHALL do the following operations (see also [Fig 7](#)) on the Mifare Standard 1k/4k 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 Standard 1k/4k tag, the NDEF Message SHALL NOT be written in the Mifare Standard 1k/4k 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 Forum sector i.e. the NFC Forum 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 2.5](#)) 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 Forum sectors with the exception of MAD sector 16 in case Mifare Standard 4k is used (see also the definition of contiguous NFC Forum 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 Forum 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 Forum sector, and
- the whole memory space of the NFC Forum sectors following the sector containing the mandatory NDEF Message TLV. The following NFC Forum sectors MAY have a size of 48 bytes (3 blocks) or 240 bytes (15 blocks). The information about the following available NFC Forum 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 Standard 1k/4k tag. [Fig 7](#) 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 Standard 1k/4k tag in INITIALISED state, READ/WRITE state or even in READ-ONLY state.

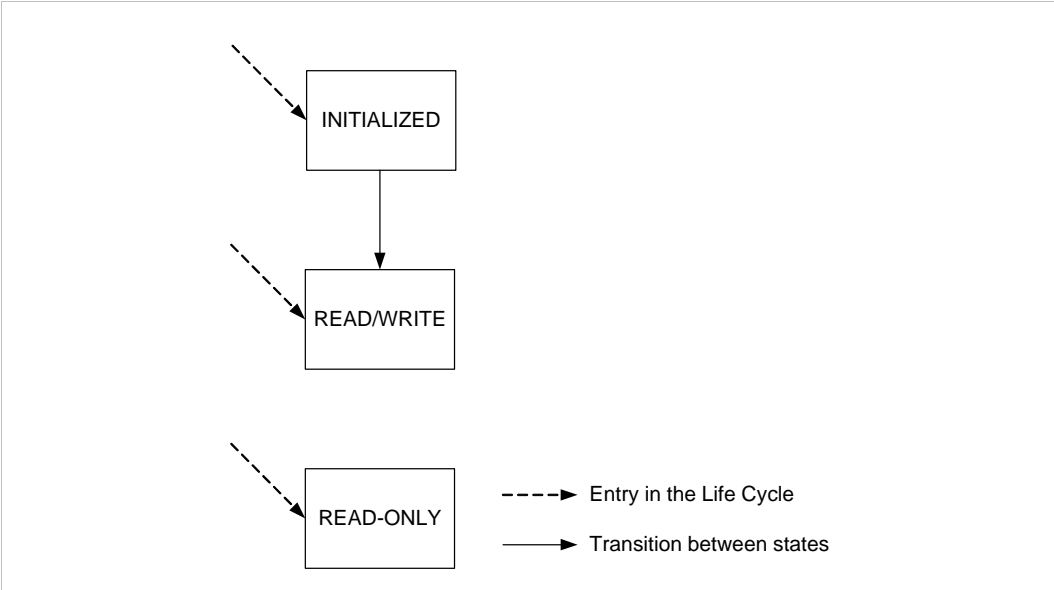


Fig 7. Life Cycle with State Change (transition)

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 Standard 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 2.4](#) 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 Forum 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	MAD1 and MAD2 Sectors			MAD1 and MAD2 Sector Trailer Bytes Values			NFC Forum Sector Trailer Bytes Values		
	Access Bits	Access Bits Values	Access Bits Values	Byte 6	Byte 7	Byte 8	Byte 6	Byte 7	Byte 8
INITIALIZED 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 C1₀ C2₀ C3₀ of sector 0 (related to the manufacturer block) is suggested and it may change.

10.ANNEX D: Example of Mifare Standard 1k in INITIALISED State

In this ANNEX an example of Mifare Standard 1k in INITIALISED state is given (see [Fig 8](#)).

In this example the sectors from sector 1 to sector 15 are NFC Forum sectors. The MAD sector contains 15 NFC Forum AID equal to 03E1h. Being in INTIALISED state the Mifare Standard 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 Forum sector is equal to 40h indicating version number 1.0 and read/write access granted.

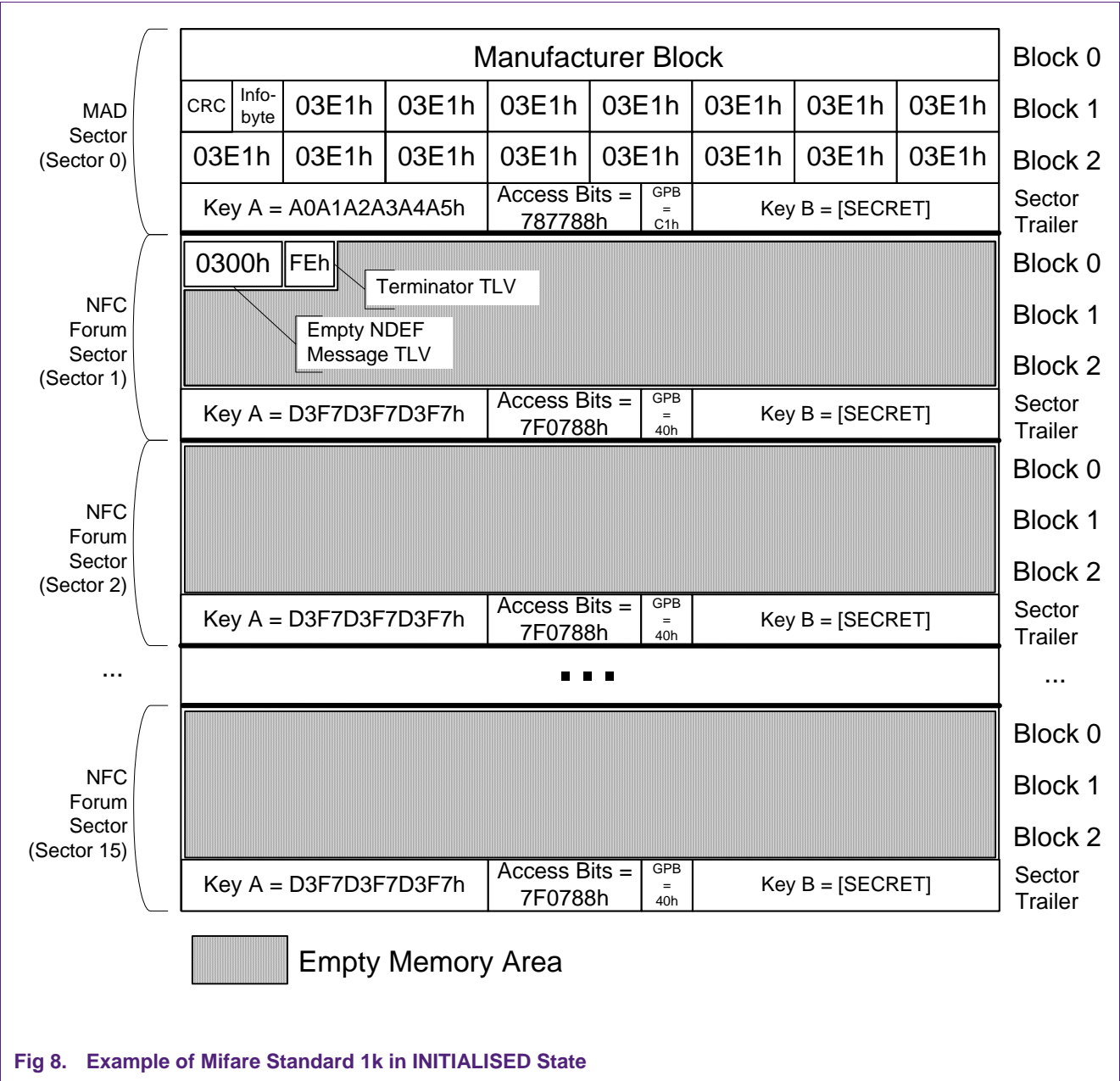


Fig 8. Example of Mifare Standard 1k in INITIALISED State

11.ANNEX E: Example of Mifare Standard 4k in INITIALISED State

In this ANNEX an example of Mifare Standard 4k in INITIALISED state is given (see [Fig 9](#)).

In this example the sectors from sector 1 to sector 15 and from sector 17 to sector 39 are NFC Forum sectors. The MAD sectors contain overall 38 NFC Forum AID equal to 03E1h in sector 0 and sector 16. Being in INITIALISED state the Mifare Standard 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 Forum sector is equal to 40h indicating version number 1.0 and read/write access granted.

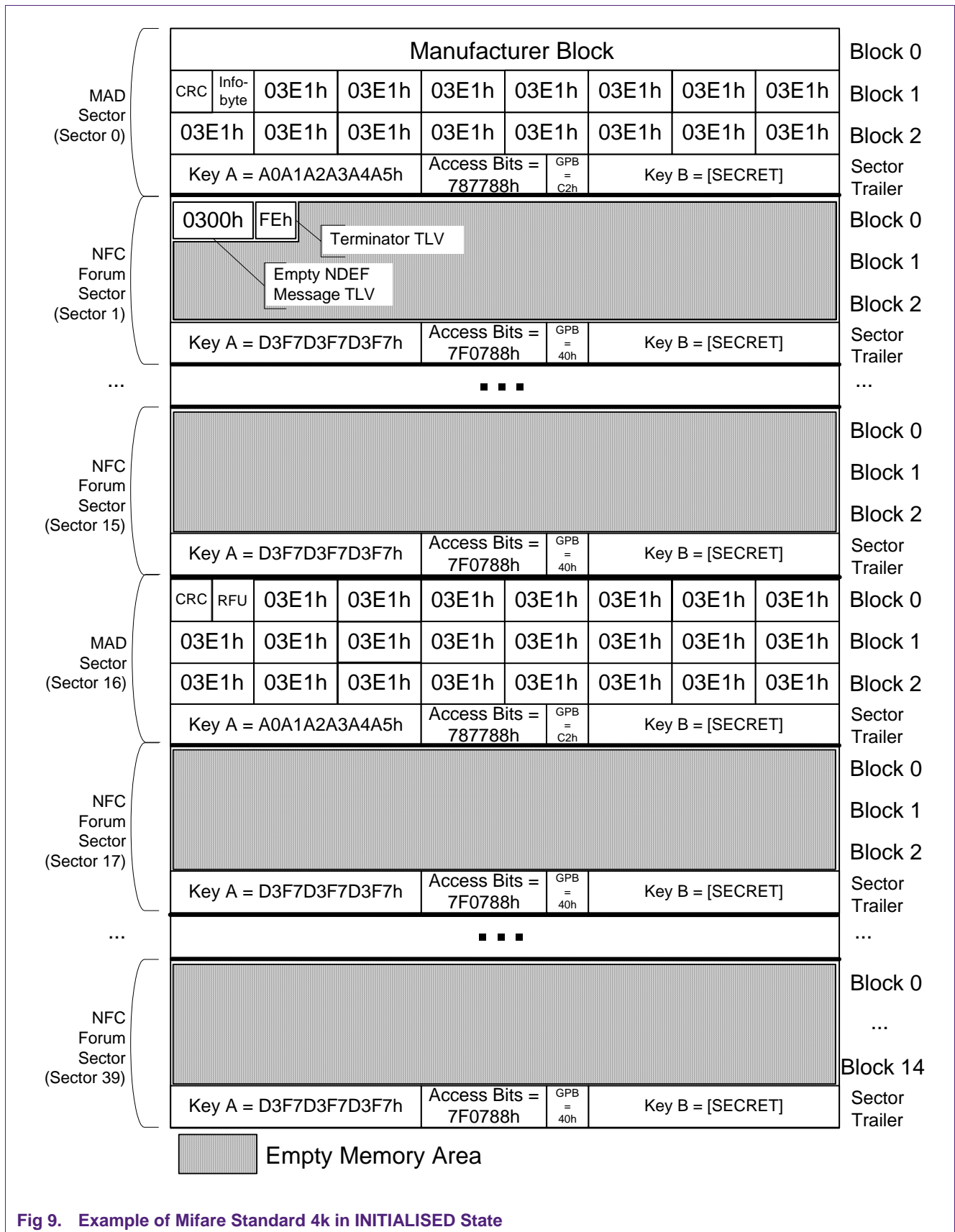


Fig 9. Example of Mifare Standard 4k in INITIALISED State

12. Disclaimers

Life support — These products are not designed for use in life support appliances, devices, or systems where malfunction of these products can reasonably be expected to result in personal injury. NXP Semiconductors customers using or selling these products for use in such applications do so at their own risk and agree to fully indemnify NXP Semiconductors for any damages resulting from such application.

Right to make changes — NXP Semiconductors reserves the right to make changes in the products - including circuits, standard cells, and/or software - described or contained herein in order to improve design and/or performance. When the product is in full production (status 'Production'), relevant changes will be communicated via a Customer Product/Process Change Notification (CPCN). NXP Semiconductors assumes no responsibility or liability for the use of any of these products, conveys no

licence or title under any patent, copyright, or mask work right to these products, and makes no representations or warranties that these products are free from patent, copyright, or mask work right infringement, unless otherwise specified.

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

13. Trademarks

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

Mifare — is a trademark of NXP B.V.

14.Contents

1.	Introduction	3	9.	ANNEX C: Access bits Coding into byte 6 to 8 of the sector trailer	33
1.1	Applicable Documents	3	10.	ANNEX D: Example of Mifare Standard 1k in INITIALISED State	34
1.2	Convention and notations.....	4	11.	ANNEX E: Example of Mifare Standard 4k in INITIALISED State	35
1.2.1	Representation of numbers	4	12.	Disclaimers	37
1.3	Special Word Usage	4	13.	Trademarks	37
1.4	Acronyms or Definitions or Glossary	4	14.	Contents	38
2.	MEMORY STRUCTURE AND MANAGEMENT ...	7			
2.1	Mifare Standard 1k Layout	7			
2.2	Mifare Standard 4k Layout	8			
2.3	Mifare Application Directory	9			
2.4	Mifare Standard 1k/4k Access Mechanism (Access Bits)	10			
2.4.1	MAD Sector Access	11			
2.4.2	NFC Forum Sector Access.....	12			
2.5	TLV blocks	14			
2.5.1	NDEF Message TLV	15			
2.5.2	Proprietary TLV	15			
2.5.3	NULL TLV	16			
2.5.4	Terminator TLV	16			
3.	RF Interface.....	17			
4.	Framing/Transmission Handling.....	18			
5.	Command Set	19			
5.1	Tag Commands and Responses Set	19			
5.1.1	Identification and Selection Operation.....	19			
5.1.2	Authentication Operation.....	19			
5.1.3	Read operation.....	19			
5.1.4	Write operation.....	19			
6.	NDEF Detection and Access	20			
6.1	NDEF Management	20			
6.1.1	Version Treating.....	21			
6.2	NDEF Storage.....	22			
6.3	Life Cycle	22			
6.3.1	INITIALISED State	23			
6.3.2	READ/WRITE State	23			
6.3.3	READ-ONLY State	23			
6.4	Command Sequence Description.....	23			
6.4.1	NDEF Detection Procedure.....	24			
6.4.2	NDEF Read Procedure	27			
6.4.3	NDEF Write Procedure	27			
6.4.4	State Changes	29			
6.4.4.1	Transition from INITIALISED to READ/WRITE	30			
7.	ANNEX A: Empty NDEF Message	31			
8.	ANNEX B: Example of sector trailer using MAD1	32			

© NXP B.V. 2007

All rights are reserved. Reproduction in whole or in part is prohibited without the prior written consent of the copyright owner. The information presented in this document does not form part of any quotation or contract, is believed to be accurate and reliable and MAY be changed without notice. No liability will be accepted by the publisher for any consequence of its use. Publication thereof does not convey nor imply any license under patent- or other industrial or intellectual property rights.

Date of release:21 August 2007
Document number: 130410

Published in Germany