

# MF1S50YYX\_V1

MIFARE Classic EV1 1K - Mainstream contactless smart card IC for fast and easy solution development

Rev. 3.2 — 23 May 2018  
279232

Product data sheet  
COMPANY PUBLIC

## 1 General description

NXP Semiconductors has developed the MIFARE Classic EV1 contactless IC MF1S50yyX/V1 to be used in a contactless smart card according to ISO/IEC 14443 Type A.

The MIFARE Classic EV1 with 1K memory MF1S50yyX/V1 IC is used in applications like public transport ticketing and can also be used for various other applications.

### 1.1 Anticollision

An intelligent anticollision function allows to operate more than one card in the field simultaneously. The anticollision algorithm selects each card individually and ensures that the execution of a transaction with a selected card is performed correctly without interference from another card in the field.

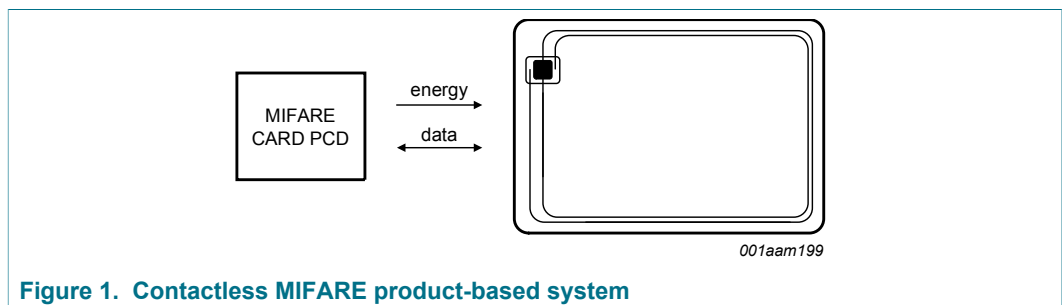


Figure 1. Contactless MIFARE product-based system

### 1.2 Simple integration and user convenience

The MF1S50yyX/V1 is designed for simple integration and user convenience which allows complete ticketing transactions to be handled in less than 100 ms.

### 1.3 Security and privacy

- Manufacturer programmed 7-byte UID or 4-byte NUID identifier for each device
- Random ID support
- Mutual three pass authentication (ISO/IEC DIS 9798-2)
- Individual set of two keys per sector to support multi-application with key hierarchy

### 1.4 Delivery options

- 7-byte UID, 4-byte NUID
- Bumped die on sawn wafer



# MF3ICDx21\_41\_81

## MIFARE DESFire EV1 contactless multi-application IC

Rev. 3.2 — 9 December 2015  
145632

Product short data sheet  
COMPANY PUBLIC

### 1. General description

---

MIFARE DESFire EV1 (MF3ICD(H) 21/41/81), a Common Criteria (EAL4+) certified product, is ideal for service providers wanting to use secure multi-application smart cards in public transport schemes, access management or closed-loop e-payment applications. It fully complies with the requirements for fast and highly secure data transmission, flexible memory organization and interoperability with existing infrastructure.

MIFARE DESFire EV1 is based on open global standards for both air interface and cryptographic methods. It is compliant to all 4 levels of ISO/IEC 14443A and uses optional ISO/IEC 7816-4 commands.

Featuring an on-chip backup management system and the mutual three-pass authentication, a MIFARE DESFire EV1 card can hold up to 28 different applications and 32 files per application. The size of each file is defined at the moment of its creation, making MIFARE DESFire EV1 a truly flexible and convenient product.

Additionally, an automatic anti-tear mechanism is available for all file types, which guarantees transaction-oriented data integrity. With MIFARE DESFire EV1, data transfer rates up to 848 kbit/s can be achieved, allowing fast data transmission.

The main characteristics of this device are denoted by its name “DESFire”: DES indicates the high level of security using a 3DES or AES hardware cryptographic engine for enciphering transmission data and Fire indicates its outstanding position as a fast, innovative, reliable and secure IC in the contactless proximity transaction market. Hence, MIFARE DESFire EV1 brings many benefits to end users. Cardholders can experience convenient contactless ticketing while also having the possibility to use the same device for related applications such as payment at vending machines, access control or event ticketing. In other words, the MIFARE DESFire EV1 silicon solution offers enhanced consumer-friendly system design, in combination with security and reliability.

MIFARE DESFire EV1 delivers the perfect balance of speed, performance and cost efficiency. Its open concept allows future seamless integration of other ticketing media such as smart paper tickets, key fobs, and mobile ticketing based on Near Field Communication (NFC) technology. It is also fully compatible with the existing MIFARE reader hardware platform. MIFARE DESFire EV1 is your ticket to contactless systems worldwide.



## 2. Features and benefits

### 2.1 RF interface: ISO/IEC 14443 Type A

- Contactless transmission of data and powered by the RF-field (no battery needed)
- Operating distance: up to 100 mm (depending on power provided by the PCD and antenna geometry)
- Operating frequency: 13.56 MHz
- Fast data transfer: 106 kbit/s, 212 kbit/s, 424 kbit/s, 848 kbit/s
- High data integrity: 16/32 bit CRC, parity, bit coding, bit counting
- True deterministic anticollision
- 7 bytes unique identifier (cascade level 2 according to ISO/IEC 14443-3 and option for random ID)
- Uses ISO/IEC 14443-4 protocol

### 2.2 ISO/IEC 7816 compatibility

- Supports ISO/IEC 7816-3 APDU message structure
- Supports ISO/IEC 7816-4 INS code 'A4' for SELECT FILE
- Supports ISO/IEC 7816-4 INS code 'B0' for READ BINARY
- Supports ISO/IEC 7816-4 INS code 'D6' for UPDATE BINARY
- Supports ISO/IEC 7816-4 INS code 'B2' for READ RECORDS
- Supports ISO/IEC 7816-4 INS code 'E2' for APPEND RECORD
- Supports ISO/IEC 7816-4 INS code '84' for GET CHALLENGE
- Supports ISO/IEC 7816-4 INS code '88' for INTERNAL AUTHENTICATE
- Supports ISO/IEC 7816-4 INS code '82' for EXTERNAL AUTHENTICATE

### 2.3 Non-volatile memory

- 2 kB or 4 kB or 8 kB NV-Memory
- Data retention of 10 years
- Write endurance typical 500 000 cycles

### 2.4 NV-memory organization

- Flexible file system
- Up to 28 applications simultaneously on one PICC
- Up to 32 files in each application (standard data file, back-up data file, value file, linear record file and cyclic record file)
- File size is determined during creation

### 2.5 Security

- Common Criteria Certification: EAL4+ (Hardware and Software)
- Unique 7 bytes serial number for each device
- Optional "RANDOM" ID for enhance security and privacy
- Mutual three-pass authentication
- Mutual authentication according to ISO/IEC 7816-4

- 1 card master key and up to 14 keys per application
- Hardware DES using 56/112/168 bit keys featuring key version, data authenticity by 8 byte CMAC
- Hardware AES using 128-bit keys featuring key version, data authenticity by 8 byte CMAC
- Data encryption on RF-channel
- Authentication on application level
- Hardware exception sensors
- Self-securing file system
- Backward compatibility to MF3ICD40: 4 byte MAC, CRC 16

## 2.6 Special features

- Transaction-oriented automatic anti-tear mechanism
- Configurable ATS information for card personalization
- Backward compatibility mode to MF3ICD40
- Optional high input capacitance (70 pF) for small form factor design (MF3ICDH 21/41/81)

## 3. Applications

---

- Advanced public transportation schema
- Highly secure access management
- Closed-loop e-payment scheme
- Event ticketing
- eGovernment applications

## 4. Quick reference data

Table 1. Quick reference data [1][2]

| Symbol                        | Parameter                             | Conditions  | Min       | Typ    | Max   | Unit  |
|-------------------------------|---------------------------------------|---|-----------|--------|-------|-------|
| $f_i$                         | input frequency                       |   | -         | 13.56  | -     | MHz   |
| $C_i$                         | input capacitance for MF3ICD21/41/81  | $T_{amb} = 22\text{ °C}$ ; $f_i = 13.56\text{ MHz}$ ; 2.8 V RMS | [3] 14.96 | 17.0   | 19.04 | pF    |
|                               | input capacitance for MF3ICDH21/41/81 |   | 64        | 69     | 74    | pF    |
| <b>EEPROM characteristics</b> |                                       |   |           |        |       |       |
| $t_{ret}$                     | retention time                        | $T_{amb} = 22\text{ °C}$  | 10        | -      | -     | year  |
| $N_{endu(W)}$                 | write endurance                       | $T_{amb} = 22\text{ °C}$  | 200000    | 500000 | -     | cycle |
| $t_{cy(W)}$                   | write cycle time                      | $T_{amb} = 22\text{ °C}$  | -         | 2.9    | -     | ms    |

[1] Stresses above one or more of the values may cause permanent damage to the device.

[2] Exposure to limiting values for extended periods may affect device reliability.

[3] Measured with LCR meter.

## 5. Ordering information

Table 2. Ordering information

| Type number       | Package  |   | Version  |
|-------------------|----------|---|----------|
|                   | Name     | Description   |          |
| MF3ICD8101DUD/05  | FFC      | 8 inch wafer (sawn; 120 $\mu\text{m}$ thickness, on film frame carrier; electronic fail die marking according to SECSII format); see <a href="#">Ref. 4</a> , 8K EEPROM, 17pF input capacitance | -        |
| MF3ICD4101DUD/05  | FFC      | 8 inch wafer (sawn; 120 $\mu\text{m}$ thickness, on film frame carrier; electronic fail die marking according to SECSII format); see <a href="#">Ref. 4</a> , 4K EEPROM, 17pF input capacitance | -        |
| MF3ICD2101DUD/05  | FFC      | 8 inch wafer (sawn; 120 $\mu\text{m}$ thickness, on film frame carrier; electronic fail die marking according to SECSII format); see <a href="#">Ref. 4</a> , 2K EEPROM, 17pF input capacitance | -        |
| MF3ICDH8101DUD/05 | FFC      | 8 inch wafer (sawn; 120 $\mu\text{m}$ thickness, on film frame carrier; electronic fail die marking according to SECSII format); see <a href="#">Ref. 5</a> , 8K EEPROM, 70pF input capacitance | -        |
| MF3ICDH4101DUD/05 | FFC      | 8 inch wafer (sawn; 120 $\mu\text{m}$ thickness, on film frame carrier; electronic fail die marking according to SECSII format); see <a href="#">Ref. 5</a> , 4K EEPROM, 70pF input capacitance | -        |
| MF3ICDH2101DUD/05 | FFC      | 8 inch wafer (sawn; 120 $\mu\text{m}$ thickness, on film frame carrier; electronic fail die marking according to SECSII format); see <a href="#">Ref. 5</a> , 2K EEPROM, 70pF input capacitance | -        |
| MF3MOD8101DA4/05  | PLLMC[1] | plastic leadless module carrier package; 35 mm wide tape; see <a href="#">Ref. 6</a> , 8K EEPROM, 17pF input capacitance  | SOT500-2 |
| MF3MOD4101DA4/05  | PLLMC[1] | plastic leadless module carrier package; 35 mm wide tape; see <a href="#">Ref. 6</a> , 4K EEPROM, 17pF input capacitance  | SOT500-2 |
| MF3MOD2101DA4/05  | PLLMC[1] | plastic leadless module carrier package; 35 mm wide tape; see <a href="#">Ref. 6</a> , 2K EEPROM, 17pF input capacitance  | SOT500-2 |
| MF3MODH8101DA4/05 | PLLMC[1] | plastic leadless module carrier package; 35 mm wide tape; see <a href="#">Ref. 6</a> , 8K EEPROM, 70pF input capacitance  | SOT500-2 |

Table 2. Ordering information *?continued*

| Type number       | Package              |  | Version  |
|-------------------|----------------------|--|----------|
|                   | Name                 | Description  |          |
| MF3MODH4101DA4/05 | PLLMC <sup>[1]</sup> | plastic leadless module carrier package; 35 mm wide tape; see <a href="#">Ref. 6</a> , 4K EEPROM, 70pF input capacitance | SOT500-2 |
| MF3MODH2101DA4/05 | PLLMC <sup>[1]</sup> | plastic leadless module carrier package; 35 mm wide tape; see <a href="#">Ref. 6</a> , 2K EEPROM, 70pF input capacitance | SOT500-2 |
| MF3MOD8101DA8/05  | PLLMC <sup>[2]</sup> | plastic leadless module carrier package; 35 mm wide tape; see <a href="#">Ref. 6</a> , 8K EEPROM, 17pF input capacitance | SOT500-4 |
| MF3MOD4101DA8/05  | PLLMC <sup>[2]</sup> | plastic leadless module carrier package; 35 mm wide tape; see <a href="#">Ref. 6</a> , 4K EEPROM, 17pF input capacitance | SOT500-4 |
| MF3MOD2101DA8/05  | PLLMC <sup>[2]</sup> | plastic leadless module carrier package; 35 mm wide tape; see <a href="#">Ref. 6</a> , 2K EEPROM, 17pF input capacitance | SOT500-4 |
| MF3MODH8101DA8/05 | PLLMC <sup>[2]</sup> | plastic leadless module carrier package; 35 mm wide tape; see <a href="#">Ref. 6</a> , 8K EEPROM, 70pF input capacitance | SOT500-4 |
| MF3MODH4101DA8/05 | PLLMC <sup>[2]</sup> | plastic leadless module carrier package; 35 mm wide tape; see <a href="#">Ref. 6</a> , 4K EEPROM, 70pF input capacitance | SOT500-4 |
| MF3MODH2101DA8/05 | PLLMC <sup>[2]</sup> | plastic leadless module carrier package; 35 mm wide tape; see <a href="#">Ref. 6</a> , 2K EEPROM, 70pF input capacitance | SOT500-4 |

- [1] This package is also known as MOA4.
- [2] This package is also known as MOA8

## 6. Block diagram

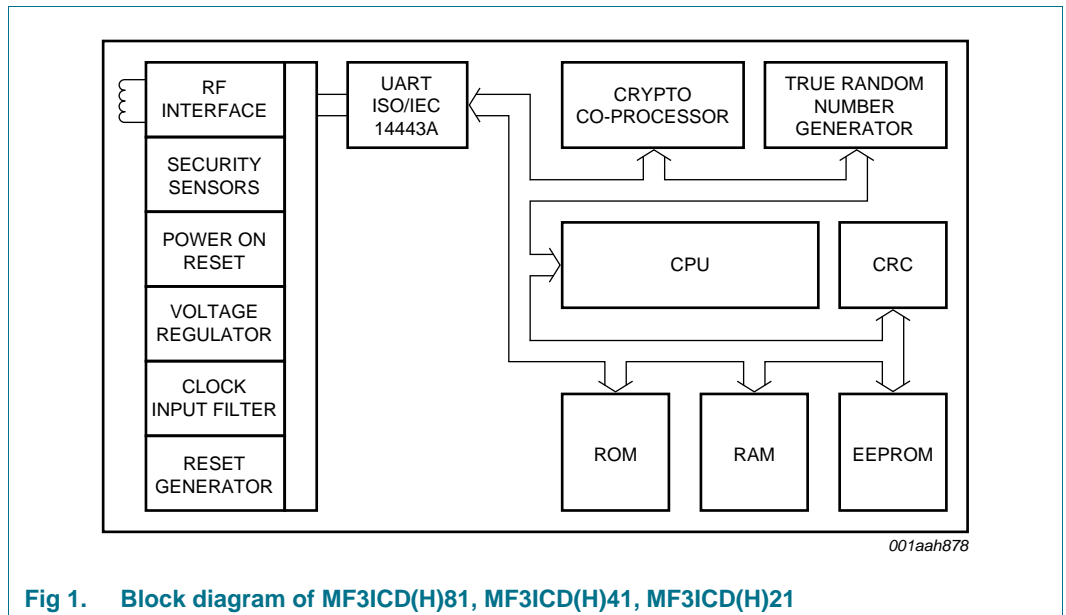


Fig 1. Block diagram of MF3ICD(H)81, MF3ICD(H)41, MF3ICD(H)21

## 7. Limiting values

**Table 3. Limiting values** [\[1\]](#)[\[2\]](#)

*In accordance with the Absolute Maximum Rating System (IEC 60134).*

| Symbol         | Parameter                           | Conditions | Min                   | Max | Unit |
|----------------|-------------------------------------|------------|-----------------------|-----|------|
| $I_I$          | input current                       |            | -                     | 30  | mA   |
| $P_{tot}/pack$ | total power dissipation per package |            | -                     | 200 | mW   |
| $T_{stg}$      | storage temperature                 |            | -55                   | 125 | °C   |
| $T_{amb}$      | ambient temperature                 |            | -25                   | 70  | °C   |
| $V_{ESD}$      | electrostatic discharge voltage     |            | <a href="#">[3]</a> 2 | -   | kV   |
| $I_{lu}$       | latch-up current                    |            | ±100                  | -   | mA   |

[1] Stresses above one or more of the limiting values may cause permanent damage to the device.

[2] Exposure to limiting values for extended periods may affect device reliability.

[3] MIL Standard 883-C method 3015; human body model: C = 100 pF, R = 1.5 kΩ.

## 8. Functional description

### 8.1 Contactless energy and data transfer

In the MIFARE system, the MIFARE DESFire EV1 is connected to a coil consisting of a few turns embedded in a standard ISO/IEC smart card (see [Ref. 8](#)). A battery is not needed. When the card is positioned in the proximity of the PCD antenna, the high-speed RF communication interface allows data to be transmitted up to 848 kbit/s.

### 8.2 Anti-collision

An intelligent anti-collision mechanism allows more than one MIFARE DESFire EV1 in the field to be handled simultaneously. The anti-collision algorithm selects each MIFARE DESFire EV1 individually and ensures that the execution of a transaction with a selected MIFARE DESFire EV1 is performed correctly without data corruption resulting from other MIFARE DESFire EV1s in the field.

### 8.3 UID/serial number

The unique 7 byte (UID) is programmed into a locked part of the NV memory which is reserved for the manufacturer. Due to security and system requirements these bytes are write-protected after being programmed by the IC manufacturer at production time. According to ISO/IEC 14443-3 (see [Ref. 12](#)) during the first anti-collision loop the cascade tag returns a value of 88h and also the first 3 bytes of the UID, UID0 to UID2 and BCC. The second anti-collision loop returns bytes UID3 to UID6 and BCC.

UID0 holds the manufacturer ID for NXP (04h) according to ISO/IEC 14443-3 and ISO/IEC 7816-6 AMD 1.

MIFARE DESFire EV1 also allows Random ID to be used. In this case MIFARE DESFire EV1 only uses a single anti-collision loop. The 3 byte random number is generated after RF reset of the MIFARE DESFire EV1.

### 8.4 Memory organization

The 2/4/8 KB NV memory is organized using a flexible file system. This file system allows a maximum of 28 different applications on one MIFARE DESFire EV1. Each application provides up to 32 files. Every application is represented by its 3 bytes Application Identifier (AID).

Five different file types are supported; see [Section 8.5](#).

A guideline to assign MIFARE DESFire AIDs can be found in the application note *MIFARE Application Directory* (MAD); see [Ref. 9](#).

Each file can be created either at MIFARE DESFire EV1 initialization (card production/card printing), at MIFARE DESFire EV1 personalization (vending machine) or in the field.

If a file or application becomes obsolete in operation, it can be permanently invalidated.

Commands which have impact on the file structure itself (e.g. creation or deletion of applications, change of keys) activate an automatic rollback mechanism, which protects the file structure from being corrupted.



If this rollback is necessary, it is done without user interaction before carrying out further commands. To ensure data integrity on application level, a transaction-oriented backup is implemented for all file types with backup. It is possible to mix file types with and without backup within one application.

As the commands are the same for MF3ICD(H)81, MF3ICD(H)41 and MF3ICD(H)21, the command details are available in [Ref. 1](#). Only the memory size and input capacitance are different between the devices.

## 8.5 Available file types

The files within an application can be any of the following types:

- Standard data files
- Backup data files
- Value files with backup
- Linear record files with backup
- Cyclic record files with backup

## 8.6 Security

The 7 byte UID is fixed, programmed into each device during production. It cannot be altered and ensures the uniqueness of each device.

The UID may be used to derive diversified keys for each ticket. Diversified MIFARE DESFire EV1 keys contribute to gain an effective anti-cloning mechanism and increase the security of the original key; see [Ref. 7](#).

Prior to data transmission a mutual three-pass authentication can be done between MIFARE DESFire EV1 and PCD depending on the configuration employing either 56-bit DES (single DES, DES), 112-bit 3DES (triple DES, 2K3DES), 168-bit 3DES (3 key triple DES, 3K3DES) or AES. During the authentication the level of security of all further commands during the session is set. In addition, the communication settings of the file/application result in the following options of secure communication between MIFARE DESFire EV1 and PCD:

- Plain data transfer (only possible within the backwards-compatible mode to MF3ICD40)
- Plain data transfer with cryptographic checksum (MAC): Authentication with backwards-compatible mode to MF3ICD40: 4 byte MAC, all other authentications based on DES/3DES/AES: 8 byte CMAC
- Encrypted data transfer (secured by CRC before encryption): Authentication with backwards-compatible mode to MF3ICD40: A 16-bit CRC is calculated over the stream and attached. The resulting stream is encrypted using the chosen cryptographic method. All other authentications-based DES/3DES/AES: A 32-bit CRC is calculated over the stream and attached. The resulting stream is encrypted using the chosen cryptographic method.

Find more information on the security concept of the product in [Ref. 1](#). Be aware not all levels of security are recommended. The recommended secure handling of the product can be seen in [Ref. 2](#) and in [Ref. 11](#).

## 9. DESFire command set

A detailed description of all commands is provided in [Ref. 1](#).

### 9.1 ISO/IEC 14443-3

Table 4. ISO/IEC 14443-3

| Command                              | Description   |
|--------------------------------------|---|
| REQA                                 | REQA and ATQA are implemented fully according to ISO/IEC 14443-3  |
| WUPA                                 | WUPA is implemented fully according to ISO/IEC 14443-3  |
| ANTICOLLISION/SELECT Cascade Level 1 | ANTICOLLISION and SELECT commands are implemented fully according to ISO/IEC 14443-3; the response is part 1 of the UID |
| ANTICOLLISION/SELECT Cascade Level 2 | ANTICOLLISION and SELECT commands are implemented fully according to ISO/IEC 14443-3; the response is part 2 of the UID |
| HALT                                 | brings MIFARE DESFire EV1 to the HALT state   |

### 9.2 ISO/IEC 14443-4

Table 5. ISO/IEC 14443-4

| Command  | Description   |
|----------|---|
| RATS     | identifies the MIFARE DESFire EV1 type to the PCD   |
| PPS      | allows individual selection of the communication baud rate between PCD and MIFARE DESFire EV1; for DESFire it is possible to set different communication baud rates for each direction i.e. DESFire allows a non-symmetrical information interchange speed. |
| WTX      | if the MIFARE DESFire EV1 needs more time than the defined FWT to respond to a PCD command it requests a Waiting Time eXtension (WTX)   |
| DESELECT | allows MIFARE DESFire EV1 to be brought to the HALT state   |

### 9.3 MIFARE DESFire EV1 command set overview – security related commands

Table 6. Security related commands

| Command            | Description   |
|--------------------|---|
| Authenticate       | MIFARE DESFire EV1 and the reader device show in an encrypted way that they possess the same secret which especially means the same key; this not only confirms that both entities are permitted to perform operations on each other but also creates a session key which can be used to keep the further communication path secure; as the name “session key” implicitly indicates, each time a new authentication procedure is successfully completed a new key for further cryptographic operations is generated |
| Change KeySettings | changes the master key settings on MIFARE DESFire EV1 and application level   |
| Set Configuration  | configures the card and pre-personalizes the card with a key, defines if the UID or the random ID is sent back during communication setup and configures the ATS string   |
| Change Key         | changes any key stored on the MIFARE DESFire EV1  |
| Get Key Version    | reads out the current key version of any key stored on the MIFARE DESFire EV1   |

**Remark:** All command and data frames are exchanged between MIFARE DESFire EV1 and PCD by using block format as defined in ISO/IEC 14443-4.

### 9.4 MIFARE DESFire EV1 command set overview – MIFARE DESFire EV1 level commands

Table 7. Level commands

| Command              | Description   |
|----------------------|---|
| Create Application   | creates new applications on the MIFARE DESFire EV1  |
| Delete Application   | permanently deactivates applications on the MIFARE DESFire EV1  |
| Get Applications IDs | returns the Application IDentifiers of all applications on a MIFARE DESFire EV1   |
| Free Memory          | returns the free memory available on the card   |
| GetDFNames           | returns the DF names  |
| Get KeySettings      | gets information on the MIFARE DESFire EV1 and application master key settings; in addition it returns the maximum number of keys which are configured for the selected application |
| Select Application   | selects one specific application for further access   |
| FormatMF3ICD81       | releases the MF3ICD81 user memory   |
| Get Version          | returns manufacturing related data of the MIFARE DESFire EV1  |
| GetCardUID           | returns the UID   |

**Remark:** All command and data frames are exchanged between MIFARE DESFire EV1 and PCD by using block format as defined in ISO/IEC 14443-4.

### 9.5 MIFARE DESFire EV1 command set overview – application level commands

Table 8. Application level commands

| Command                 | Description   |
|-------------------------|---|
| Get FileIDs             | returns the File IDentifiers of all active files within the currently selected application  |
| Get FileSettings        | gets information on the properties of a specific file   |
| Change FileSettings     | changes the access parameters of an existing file   |
| Create StdDataFile      | creates files for the storage of plain unformatted user data within an existing application on the MIFARE DESFire EV1   |
| Create BackupDataFile   | creates files for the storage of plain unformatted user data within an existing application on the MIFARE DESFire EV1, additionally supporting the feature of an integrated backup mechanism  |
| Create ValueFile        | creates files for the storage and manipulation of 32-bit signed integer values within an existing application on the MIFARE DESFire EV1   |
| Create LinearRecordFile | creates files for multiple storage of similar structural data, for example, loyalty programs within an existing application on the MIFARE DESFire EV1; once the file is filled completely with data records, further writing to the file is not possible unless it is cleared   |
| Create CyclicRecordFile | creates files for multiple storage of similar structural data, for example, logging transactions within an existing application on the MIFARE DESFire EV1; once the file is filled completely with data records, the MIFARE DESFire EV1 automatically overwrites the oldest record with the latest written one (this wrap is fully transparent for the PCD) |
| DeleteFile              | permanently deactivates a file within the file directory of the currently selected application  |

**Remark:** All command and data frames are exchanged between MIFARE DESFire EV1 and PCD by using block format as defined in ISO/IEC 14443-4.

### 9.6 MIFARE DESFire EV1 command set overview – data manipulation commands

Table 9. Data manipulation commands

| Command        | Description  |
|----------------|--|
| Read Data      | reads data from Standard Data files or Backup Data files   |
| Write Data     | writes data to Standard Data files or Backup Data files  |
| Get Value      | reads the currently stored value from Value files  |
| Credit         | increases a value stored in a Value file   |
| Debit          | decreases a value stored in a Value file   |
| Limited Credit | allows a limited increase of a value stored in a Value file without having full Credit permissions to the file |
| Write Record   | writes data to a record in a Cyclic or Linear Record file  |
| Read Records   | reads out a set of complete records from a Cyclic or Linear Record file  |

**Table 9.** Data manipulation commands *?continued*

| Command            | Description   |
|--------------------|---|
| Clear RecordFile   | resets a Cyclic or Linear Record file to empty state  |
| Commit Transaction | validates all previous write accesses on Backup Data files, Value files and Record files within one application   |
| Abort Transaction  | invalidates all previous write accesses on Backup Data files, Value files and Record files within one application |

**Remark:** All command and data frames are exchanged between MIFARE DESFire EV1 and PCD by using block format as defined in ISO/IEC 14443-4.

## 9.7 MIFARE DESFire EV1 command set - ISO/IEC 7816 APDU commands

The MIFARE DESFire EV1 provides the following commands according to ISO/IEC 7816-4:

- INS code 'A4' SELECT
- INS code 'B0' READ BINARY
- INS code 'D6' UPDATE BINARY
- INS code 'B2' READ RECORDS
- INS code 'E2' APPEND RECORD
- INS code '84' GET CHALLENGE
- INS code '88' INTERNAL AUTHENTICATE
- INS code '82' EXTERNAL AUTHENTICATE

### 9.7.1 ISO/IEC 7816-4 APDU message structure

MIFARE DESFire EV1 supports the APDU message structure according to ISO/IEC 7816-4 for:

- an optional wrapping of the native MIFARE DESFire EV1 APDU format
- additionally implemented ISO/IEC 7816-4 commands

Find more information on the ISO/IEC 7816-4 commands in [Ref. 1](#).

## 10. Abbreviations

Table 10. Abbreviations

| Acronym | Description   |
|---------|---|
| AES     | Advanced Encryption Standard                        |
| AID     | Application Identifier                              |
| APDU    | Application Protocol Data Unit                      |
| ATS     | Answer to Select                                    |
| CC      | Common Criteria                                     |
| CMAC    | Cryptic Message Authentication Code                 |
| CRC     | Cyclic Redundancy Check                             |
| DES     | Digital Encryption Standard                         |
| DF      | Dedicated File                                      |
| EAL     | Evaluation Assurance Level                          |
| EEPROM  | Electrically Erasable Programmable Read-Only Memory |
| FWT     | Frame Waiting Time                                  |
| ID      | Identifier  |
| INS     | Instructions  |
| LCR     | inductance, Capacitance, Resistance                 |
| MAC     | Message Authentication Code                         |
| MAD     | MIFARE Application Directory                        |
| NV      | Non-Volatile Memory                                 |
| PCD     | Proximity Coupling Device                           |
| PPS     | Protocol Parameter Selection                        |
| RATS    | Request Answer To Select                            |
| REQA    | Request Answer                                      |
| RF      | Radio Frequency                                     |
| UID     | Unique Identifier                                   |
| WTX     | Waiting Time eXtension                              |
| WUPA    | Wake Up Protocol A                                  |

## 11. References

- [1] **Data sheet** — *MF3ICD81 MIFARE DESFire EV1*, document number: 13403\*\*1.
- [2] **Data sheet** — *MF3ICD81 Guidance, Delivery and Operation Manual*, document number: 1469\*\*.
- [3] **Data sheet** — *Specification addendum MF3ICD81*, document number: 1673\*\*.
- [4] **Data sheet** — *MF3ICD8101 Sawn bumped 120 μm wafer addendum*, document number: 1318\*\*.
- [5] **Data sheet** — *MF3ICDH8101 Sawn bumped 120 μm wafer addendum*, document number: 1970\*\*.
- [6] **Data sheet** — *MF3MODx21\_41\_81 Contactless chip card module*, document number: 1439\*\*.
- [7] **Application note** — *MIFARE DESFire - Implementation hints and examples*, document number: 0945\*\*.
- [8] **Application note** — *Card Coil Design Notes for MIFARE DESFire EV1*, document number: 1713\*\*.
- [9] **Application note** — *MIFARE Application Directory*, document number: 0018\*\*.
- [10] **Application note** — *MIFARE ISO/IEC 14443 PICC Selection*, document number: 1308\*\*.
- [11] **Application note** — *End to end system security risk considerations for implementing contactless cards*, document number: 1550\*\*.
- [12] **ISO/IEC Standard** — *ISO/IEC 14443 Identification cards - Contactless integrated circuit cards - Proximity cards*.

1. \*\* ... BU-ID document version number

## 12. Revision history

Table 11. Revision history

| Document ID              | Release date  | Data sheet status          | Change notice | Supersedes               |
|--------------------------|---|----------------------------|---------------|--------------------------|
| MF3ICDX21_41_81_SDS v3.2 | 20151209  | Product short data sheet   | -             | MF3ICDX21_41_81_SDS v3.1 |
| Modifications:           | <ul style="list-style-type: none"> <li>• <a href="#">Section 5</a>: MOA8 types added</li> </ul>   |                            |               |                          |
| MF3ICDX21_41_81_SDS v3.1 | 20101221  | Product short data sheet   | -             | MF3ICD21_41_81_SDS_2     |
| Modifications:           | <ul style="list-style-type: none"> <li>• Data sheet title updated</li> <li>• <a href="#">Section 1</a>, <a href="#">Section 2</a>, <a href="#">Section 3</a>, <a href="#">Section 11</a>, <a href="#">Section 13</a>: updated</li> <li>• <a href="#">Section 5</a>: type number MF3ICD801DUD/04 changed to MF3ICD8101DUD/05</li> </ul>  |                            |               |                          |
| MF3ICD21_41_81_SDS_2     | 20090306  | Product short data sheet   | -             | MF3ICD8101_SDS_N_1       |
| Modifications:           | <ul style="list-style-type: none"> <li>• Section 5 "Ordering information": type number MF3ICD8101DUD/01 changed to MF3ICD8101DUD/04</li> <li>• Section 5 "Ordering information": added root type numbers MF3ICD41 and MF3ICD21</li> <li>• Section 1 "General description", Section 2 "Features and benefits" and Section 3 "Applications": updated</li> <li>• Section 11 "References": added</li> </ul> |                            |               |                          |
| MF3ICD8101_SDS_N_1       | 20071213  | Objective short data sheet | -             | -                        |



## 13. Legal information

### 13.1 Data sheet status

| Document status <sup>[1][2]</sup> | Product status <sup>[3]</sup> | Definition  |
|-----------------------------------|-------------------------------|---|
| Objective [short] data sheet      | Development                   | This document contains data from the objective specification for product development. |
| Preliminary [short] data sheet    | Qualification                 | This document contains data from the preliminary specification.                       |
| Product [short] data sheet        | Production                    | This document contains the product specification.                                     |

[1] Please consult the most recently issued document before initiating or completing a design.

[2] The term 'short data sheet' is explained in section "Definitions".

[3] The product status of device(s) described in this document may have changed since this document was published and may differ in case of multiple devices. The latest product status information is available on the Internet at URL <http://www.nxp.com>.

### 13.2 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.

**Short data sheet** — A short data sheet is an extract from a full data sheet with the same product type number(s) and title. A short data sheet is intended for quick reference only and should not be relied upon to contain detailed and full information. For detailed and full information see the relevant full data sheet, which is available on request via the local NXP Semiconductors sales office. In case of any inconsistency or conflict with the short data sheet, the full data sheet shall prevail.

**Product specification** — The information and data provided in a Product data sheet shall define the specification of the product as agreed between NXP Semiconductors and its customer, unless NXP Semiconductors and customer have explicitly agreed otherwise in writing. In no event however, shall an agreement be valid in which the NXP Semiconductors product is deemed to offer functions and qualities beyond those described in the Product data sheet.

### 13.3 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. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

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 and its suppliers accept 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.

**Limiting values** — Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) will cause permanent damage to the device. Limiting values are stress ratings only and (proper) operation of the device at these or any other conditions above those given in the Recommended operating conditions section (if present) or the Characteristics sections of this document is not warranted. Constant or repeated exposure to limiting values will permanently and irreversibly affect the quality and reliability of the device.

**Terms and conditions of commercial sale** — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at <http://www.nxp.com/profile/terms>, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

**No offer to sell or license** — Nothing in this document may be interpreted or construed as an offer to sell products that is open for acceptance or the grant, conveyance or implication of any license under any copyrights, patents or other industrial or intellectual property rights.

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

**Quick reference data** — The Quick reference data is an extract of the product data given in the Limiting values and Characteristics sections of this document, and as such is not complete, exhaustive or legally binding.

**Non-automotive qualified products** — Unless this data sheet expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

**Translations** — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

## 13.4 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.

## 13.5 Trademarks

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

**MIFARE** — is a trademark of NXP Semiconductors N.V.

**DESFire** — is a trademark of NXP Semiconductors N.V.

## 14. Contact information

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

For sales office addresses, please send an email to: [salesaddresses@nxp.com](mailto:salesaddresses@nxp.com)

15. Tables

|  |    |   |    |
|--|----|---|----|
| Table 1. Quick reference data [1][2] . . . . . | 4  | Table 7. Level commands . . . . .             | 10 |
| Table 2. Ordering information . . . . .        | 4  | Table 8. Application level commands . . . . . | 11 |
| Table 3. Limiting values [1][2] . . . . .      | 6  | Table 9. Data manipulation commands . . . . . | 11 |
| Table 4. ISO/IEC 14443-3 . . . . .             | 9  | Table 10. Abbreviations . . . . .             | 13 |
| Table 5. ISO/IEC 14443-4 . . . . .             | 9  | Table 11. Revision history . . . . .          | 15 |
| Table 6. Security related commands . . . . .   | 10 |   |    |

16. Figures

Fig 1. Block diagram of MF3ICD(H)81, MF3ICD(H)41, MF3ICD(H)215

17. Contents

|          |  |          |           |  |           |
|----------|--|----------|-----------|--|-----------|
| <b>1</b> | <b>General description . . . . .</b>   | <b>1</b> | 9.6       | MIFARE DESFire EV1 command set overview – data manipulation commands . . . . . | 11        |
| <b>2</b> | <b>Features and benefits . . . . .</b>   | <b>2</b> | 9.7       | MIFARE DESFire EV1 command set - ISO/IEC 7816 APDU commands . . . . .          | 12        |
| 2.1      | RF interface: ISO/IEC 14443 Type A . . . . .   | 2        | 9.7.1     | ISO/IEC 7816-4 APDU message structure . . . . .                                | 12        |
| 2.2      | ISO/IEC 7816 compatibility . . . . .   | 2        | <b>10</b> | <b>Abbreviations . . . . .</b>   | <b>13</b> |
| 2.3      | Non-volatile memory. . . . .   | 2        | <b>11</b> | <b>References. . . . .</b>   | <b>14</b> |
| 2.4      | NV-memory organization . . . . .   | 2        | <b>12</b> | <b>Revision history . . . . .</b>  | <b>15</b> |
| 2.5      | Security. . . . .  | 2        | <b>13</b> | <b>Legal information . . . . .</b>   | <b>16</b> |
| 2.6      | Special features . . . . .   | 3        | 13.1      | Data sheet status . . . . .  | 16        |
| <b>3</b> | <b>Applications . . . . .</b>  | <b>3</b> | 13.2      | Definitions . . . . .  | 16        |
| <b>4</b> | <b>Quick reference data . . . . .</b>  | <b>4</b> | 13.3      | Disclaimers . . . . .  | 16        |
| <b>5</b> | <b>Ordering information. . . . .</b>   | <b>4</b> | 13.4      | Licenses. . . . .  | 17        |
| <b>6</b> | <b>Block diagram . . . . .</b>   | <b>5</b> | 13.5      | Trademarks . . . . .   | 17        |
| <b>7</b> | <b>Limiting values. . . . .</b>  | <b>6</b> | <b>14</b> | <b>Contact information . . . . .</b>   | <b>17</b> |
| <b>8</b> | <b>Functional description . . . . .</b>  | <b>7</b> | <b>15</b> | <b>Tables. . . . .</b>   | <b>18</b> |
| 8.1      | Contactless energy and data transfer. . . . .  | 7        | <b>16</b> | <b>Figures . . . . .</b>   | <b>18</b> |
| 8.2      | Anti-collision . . . . .   | 7        | <b>17</b> | <b>Contents. . . . .</b>   | <b>18</b> |
| 8.3      | UID/serial number. . . . .   | 7        |           |  |           |
| 8.4      | Memory organization . . . . .  | 7        |           |  |           |
| 8.5      | Available file types . . . . .   | 8        |           |  |           |
| 8.6      | Security. . . . .  | 8        |           |  |           |
| <b>9</b> | <b>DESFire command set. . . . .</b>  | <b>9</b> |           |  |           |
| 9.1      | ISO/IEC 14443-3 . . . . .  | 9        |           |  |           |
| 9.2      | ISO/IEC 14443-4 . . . . .  | 9        |           |  |           |
| 9.3      | MIFARE DESFire EV1 command set overview – security related commands. . . . .         | 10       |           |  |           |
| 9.4      | MIFARE DESFire EV1 command set overview – MIFARE DESFire EV1 level commands. . . . . | 10       |           |  |           |
| 9.5      | MIFARE DESFire EV1 command set overview – application level commands . . . . .       | 11       |           |  |           |

Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.

© NXP Semiconductors N.V. 2015. All rights reserved.

For more information, please visit: <http://www.nxp.com>  
 For sales office addresses, please send an email to: [salesaddresses@nxp.com](mailto:salesaddresses@nxp.com)

Date of release: 9 December 2015  
 145632

- MOA4 and MOA8 contactless module

## 2 Features and benefits

- Contactless transmission of data and energy supply
- Operating frequency of 13.56 MHz
- Data integrity of 16-bit CRC, parity, bit coding, bit counting
- Typical ticketing transaction time of < 100 ms (including backup management)
- Random ID support (7 Byte UID version)
- Operating distance up to 100 mm depending on antenna geometry and reader configuration
- Data transfer of 106 kbit/s
- Anticollision
- 7 Byte UID or 4 Byte NUID
- NXP Originality Check support

### 2.1 EEPROM

- 1 kB, organized in 16 sectors of 4 blocks (one block consists of 16 byte)
- Data retention time of 10 years
- User definable access conditions for each memory block
- Write endurance 200000 cycles

## 3 Applications

- Public transportation
- Electronic toll collection
- School and campus cards
- Internet cafés
- Access management
- Car parking
- Employee cards
- Loyalty

## 4 Quick reference data

Table 1. Quick reference data

| Symbol                        | Parameter         | Conditions               |     | Min    | Typ    | Max  | Unit  |
|-------------------------------|-------------------|--------------------------|-----|--------|--------|------|-------|
| C <sub>i</sub>                | input capacitance |                          | [1] | 14.9   | 16.9   | 19.0 | pF    |
| f <sub>i</sub>                | input frequency   |                          |     | -      | 13.56  | -    | MHz   |
| <b>EEPROM characteristics</b> |                   |                          |     |        |        |      |       |
| t <sub>ret</sub>              | retention time    | T <sub>amb</sub> = 22 °C |     | 10     | -      | -    | year  |
| N <sub>endu(W)</sub>          | write endurance   | T <sub>amb</sub> = 22 °C |     | 100000 | 200000 | -    | cycle |

[1] T<sub>amb</sub>=22°C, f=13,56Mhz, V<sub>LdLb</sub> = 1,5 V RMS

## 5 Ordering information

Table 2. Ordering information

| Type number      | Package  |  | Version  |
|------------------|----------|--|----------|
|                  | Name     | Description  |          |
| MF1S5001XDUD/V1  | FFC Bump | 8 inch wafer, 120 µm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 7-byte UID            | -        |
| MF1S5001XDUD2/V1 | FFC Bump | 12 inch wafer, 120 µm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 7-byte UID           | -        |
| MF1S5001XDUF/V1  | FFC Bump | 8 inch wafer, 75 µm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 7-byte UID             | -        |
| MF1S5000XDA4/V1  | MOA4     | plastic leadless module carrier package; 35 mm wide tape, 7-byte UID   | SOT500-2 |
| MF1S5000XDA8/V1  | MOA8     | plastic leadless module carrier package; 35 mm wide tape, 7-byte UID   | SOT500-4 |
| MF1S5031XDUD/V1  | FFC Bump | 8 inch wafer, 120 µm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 4-byte non-unique ID  | -        |
| MF1S5031XDUD2/V1 | FFC Bump | 12 inch wafer, 120 µm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 4-byte non-unique ID | -        |
| MF1S5031XDUF/V1  | FFC Bump | 8 inch wafer, 75 µm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 4-byte non-unique ID   | -        |
| MF1S5030XDA4/V1  | MOA4     | plastic leadless module carrier package; 35 mm wide tape, 4-byte non-unique ID   | SOT500-2 |
| MF1S5030XDA8/V1  | MOA8     | plastic leadless module carrier package; 35 mm wide tape, 4-byte non-unique ID   | SOT500-4 |

## 6 Block diagram

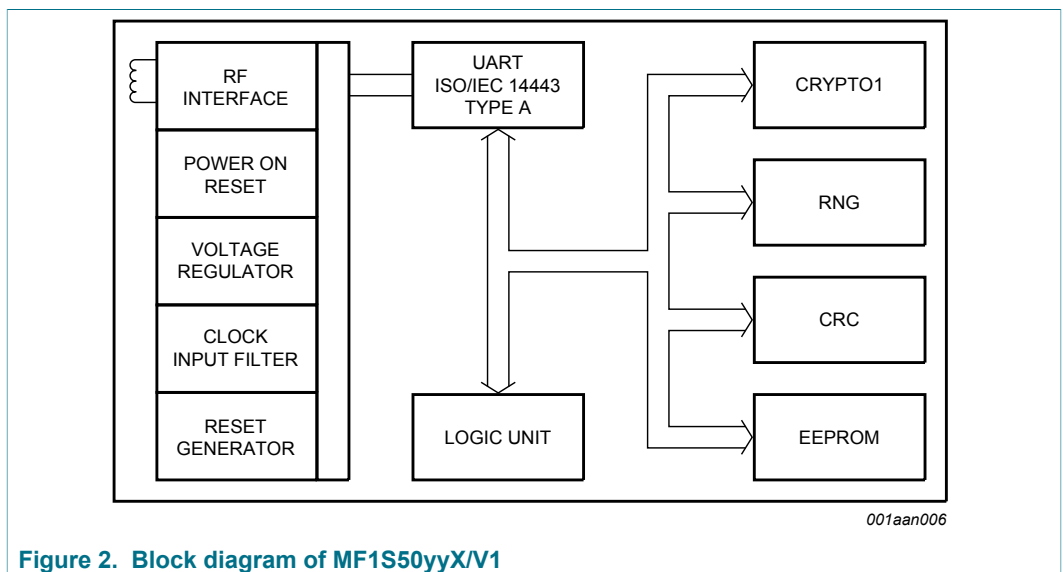


Figure 2. Block diagram of MF1S50yyX/V1

## 7 Pinning information

### 7.1 Pinning

The pinning for the MF1S50yyX/V1DAx is shown as an example in [Figure 3](#) for the MOA4 contactless module. For the contactless module MOA8, the pinning is analogous and not explicitly shown.

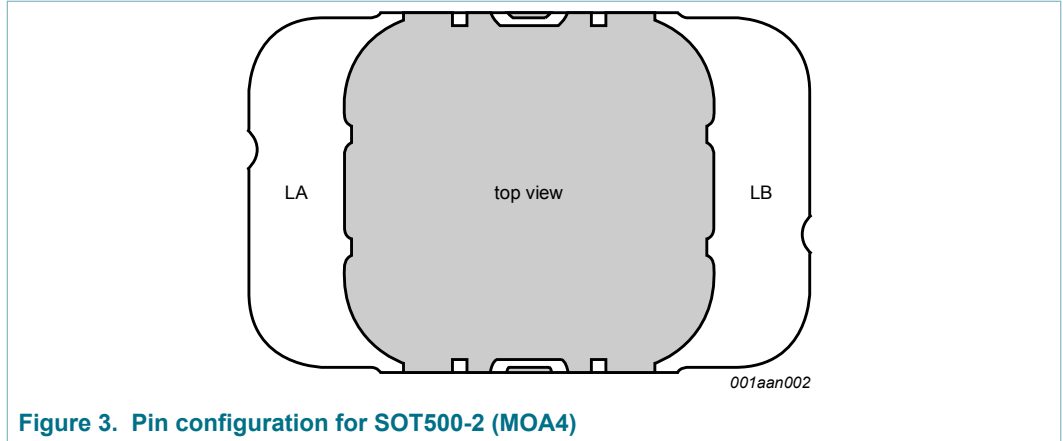


Figure 3. Pin configuration for SOT500-2 (MOA4)

Table 3. Pin allocation table

| Pin | Symbol |                            |
|-----|--------|----------------------------|
| LA  | LA     | Antenna coil connection LA |
| LB  | LB     | Antenna coil connection LB |

## 8 Functional description

### 8.1 Block description

The MF1S50yyX/V1 chip consists of a 1 kB EEPROM, RF interface and Digital Control Unit. Energy and data are transferred via an antenna consisting of a coil with a small number of turns which is directly connected to the MF1S50yyX/V1. No further external components are necessary. Refer to the document [Ref. 1](#) for details on antenna design.

- RF interface:
  - Modulator/demodulator
  - Rectifier
  - Clock regenerator
  - Power-On Reset (POR)
  - Voltage regulator
- Anticollision: Multiple cards in the field may be selected and managed in sequence
- Authentication: Preceding any memory operation the authentication procedure ensures that access to a block is only possible via the two keys specified for each block

- Control and Arithmetic Logic Unit: Values are stored in a special redundant format and can be incremented and decremented
- EEPROM interface
- Crypto unit: The CRYPTO1 stream cipher of the MF1S50yyX/V1 is used for authentication and encryption of data exchange.
- EEPROM: 1 kB is organized in 16 sectors of 4 blocks. One block contains 16 bytes. The last block of each sector is called "trailer", which contains two secret keys and programmable access conditions for each block in this sector.

## 8.2 Communication principle

The commands are initiated by the reader and controlled by the Digital Control Unit of the MF1S50yyX/V1. The command response is depending on the state of the IC and for memory operations also on the access conditions valid for the corresponding sector.

### 8.2.1 Request standard / all

After Power-On Reset (POR) the card answers to a request REQA or wakeup WUPA command with the answer to request code (see [Section 9.4](#), ATQA according to ISO/IEC 14443A).

### 8.2.2 Anticollision loop

In the anticollision loop the identifier of a card is read. If there are several cards in the operating field of the reader, they can be distinguished by their identifier and one can be selected (select card) for further transactions. The unselected cards return to the idle state and wait for a new request command. If the 7-byte UID is used for anticollision and selection, two cascade levels need to be processed as defined in ISO/IEC 14443-3.

**Remark:** For the 4-byte non-unique ID product versions, the identifier retrieved from the card is not defined to be unique. For further information regarding handling of non-unique identifiers see [Ref. 6](#).

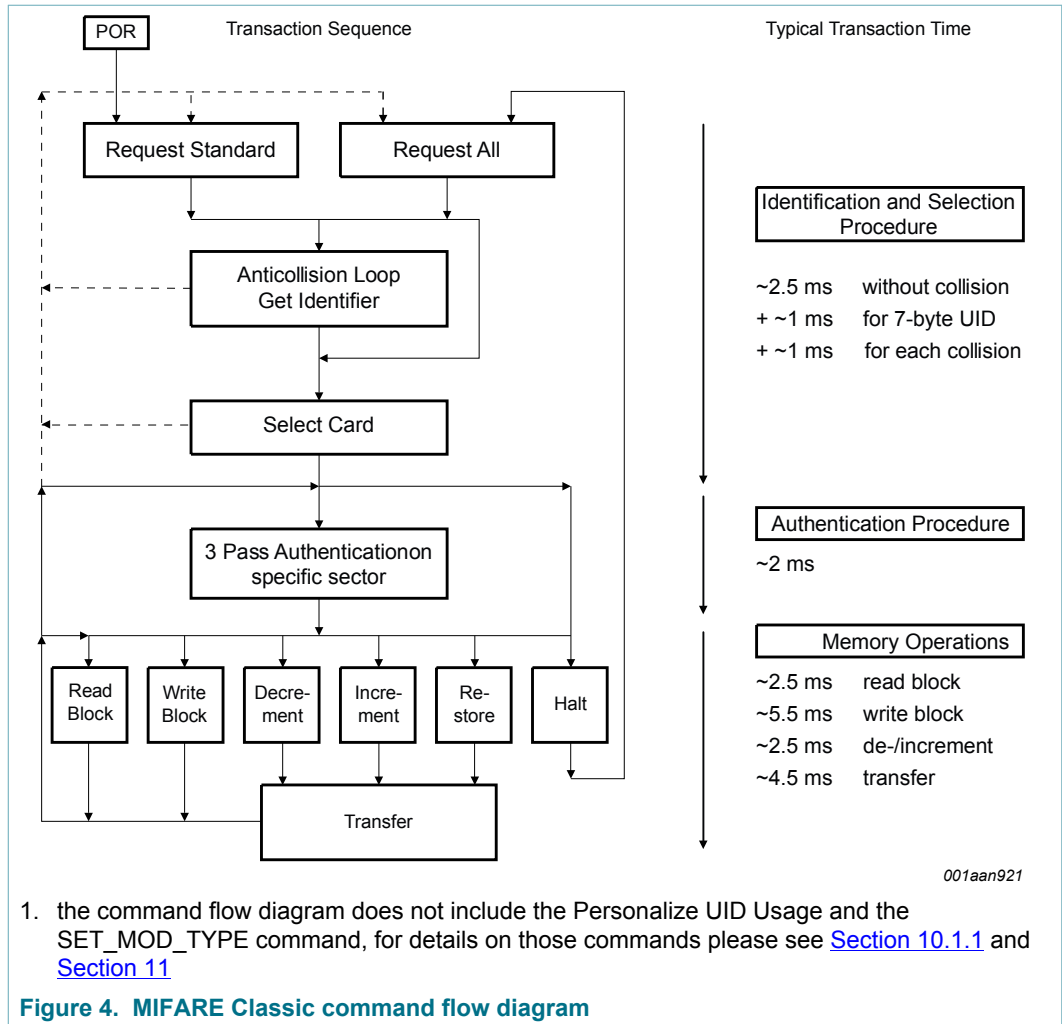
### 8.2.3 Select card

With the select card command the reader selects one individual card for authentication and memory related operations. The card returns the Select Acknowledge (SAK) code which determines the type of the selected card, see [Section 9.4](#). For further details refer to the document [Ref. 2](#).

### 8.2.4 Three pass authentication

After selection of a card the reader specifies the memory location of the following memory access and uses the corresponding key for the three pass authentication procedure. After a successful authentication all commands and responses are encrypted.

**Remark:** The HLTA command needs to be sent encrypted to the PICC after a successful authentication in order to be accepted.



### 8.2.5 Memory operations

After authentication any of the following operations may be performed:

- Read block
- Write block
- Decrement: Decrements the contents of a block and stores the result in the internal Transfer Buffer
- Increment: Increments the contents of a block and stores the result in the internal Transfer Buffer
- Restore: Moves the contents of a block into the internal Transfer Buffer
- Transfer: Writes the contents of the internal Transfer Buffer to a value block

### 8.3 Data integrity

Following mechanisms are implemented in the contactless communication link between reader and card to ensure very reliable data transmission:

- 16 bits CRC per block
- Parity bits for each byte



- Bit count checking
- Bit coding to distinguish between "1", "0" and "no information"
- Channel monitoring (protocol sequence and bit stream analysis)

#### 8.4 Three pass authentication sequence

1. The reader specifies the sector to be accessed and chooses key A or B.
2. The card reads the secret key and the access conditions from the sector trailer. Then the card sends a number as the challenge to the reader (pass one).
3. The reader calculates the response using the secret key and additional input. The response, together with a random challenge from the reader, is then transmitted to the card (pass two).
4. The card verifies the response of the reader by comparing it with its own challenge and then it calculates the response to the challenge and transmits it (pass three).
5. The reader verifies the response of the card by comparing it to its own challenge.

After transmission of the first random challenge the communication between card and reader is encrypted.

#### 8.5 RF interface

The RF-interface is according to the standard for contactless smart cards ISO/IEC 14443A.

For operation, the carrier field from the reader always needs to be present (with short pauses when transmitting), as it is used for the power supply of the card.

For both directions of data communication there is only one start bit at the beginning of each frame. Each byte is transmitted with a parity bit (odd parity) at the end. The LSB of the byte with the lowest address of the selected block is transmitted first. The maximum frame length is 163 bits (16 data bytes + 2 CRC bytes =  $16 \times 9 + 2 \times 9 + 1$  start bit).

#### 8.6 Memory organization

The  $1024 \times 8$  bit EEPROM memory is organized in 16 sectors of 4 blocks. One block contains 16 bytes.

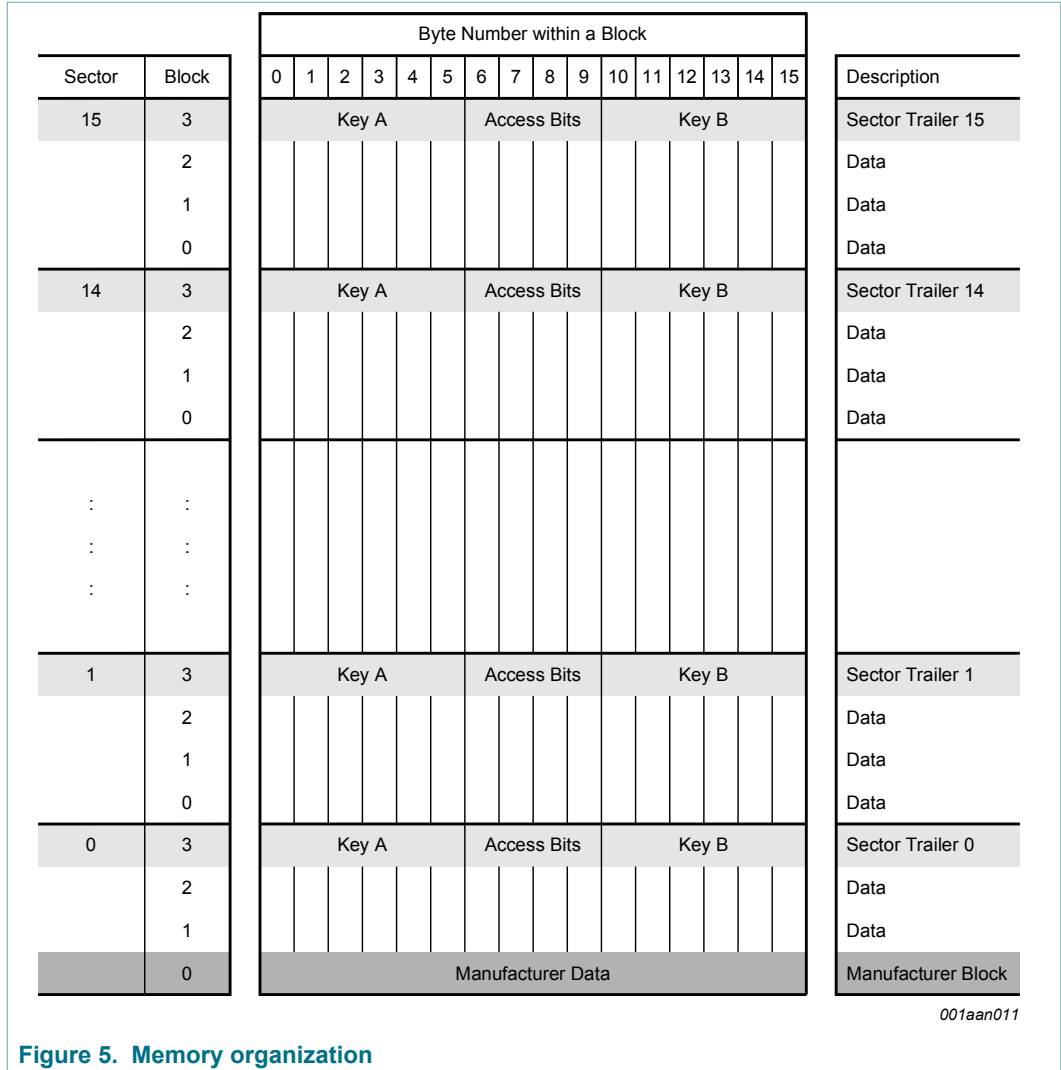


Figure 5. Memory organization

8.6.1 Manufacturer block

This is the first data block (block 0) of the first sector (sector 0). It contains the IC manufacturer data. This block is programmed and write protected in the production test. The manufacturer block is shown in Figure 6 and Figure 7 for the 4-byte NUID and 7-byte UID version respectively.

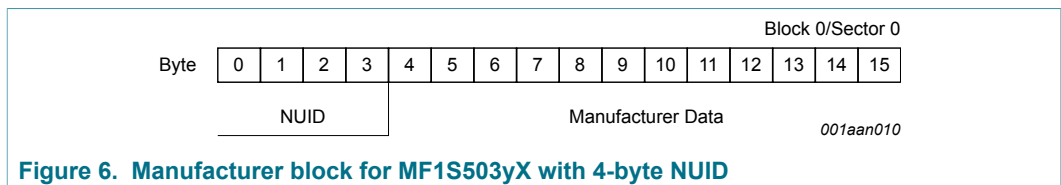


Figure 6. Manufacturer block for MF1S503yX with 4-byte NUID

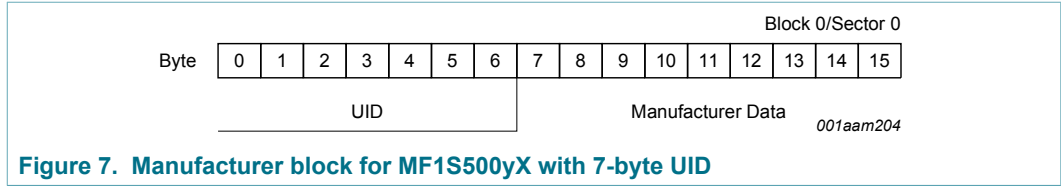


Figure 7. Manufacturer block for MF1S500yX with 7-byte UID

8.6.2 Data blocks

All sectors contain 3 blocks of 16 bytes for storing data (Sector 0 contains only two data blocks and the read-only manufacturer block).

The data blocks can be configured by the access bits as

- read/write blocks
- value blocks

Value blocks can be used for e.g. electronic purse applications, where additional commands like increment and decrement for direct control of the stored value are provided

A successful authentication has to be performed to allow any memory operation.

**Remark:** The default content of the data blocks at delivery is not defined.

8.6.2.1 Value blocks

Value blocks allow performing electronic purse functions (valid commands are: read, write, increment, decrement, restore, transfer). Value blocks have a fixed data format which permits error detection and correction and a backup management.

A value block can only be generated through a write operation in value block format:

- Value: Signifies a signed 4-byte value. The lowest significant byte of a value is stored in the lowest address byte. Negative values are stored in standard 2’s complement format. For reasons of data integrity and security, a value is stored three times, twice non-inverted and once inverted.
- Adr: Signifies a 1-byte address, which can be used to save the storage address of a block, when implementing a powerful backup management. The address byte is stored four times, twice inverted and non-inverted. During increment, decrement, restore and transfer operations the address remains unchanged. It can only be altered via a write command.

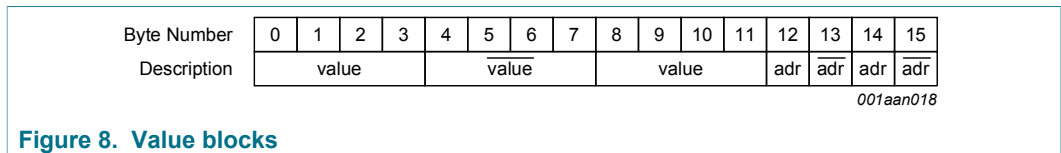


Figure 8. Value blocks

An example of a valid value block format for the decimal value 1234567d and the block address 17d is shown in Table 4. First, the decimal value has to be converted to the hexadecimal representation of 0012D687h. The LSByte of the hexadecimal value is stored in Byte 0, the MSByte in Byte 3. The bit inverted hexadecimal representation of the value is FFED2978h where the LSByte is stored in Byte 4 and the MSByte in Byte 7.

The hexadecimal value of the address in the example is 11h, the bit inverted hexadecimal value is EEh.

Table 4. Value block format example

| Byte Number  | 0     | 1  | 2  | 3  | 4     | 5  | 6  | 7  | 8     | 9  | 10 | 11 | 12  | 13  | 14  | 15  |
|--------------|-------|----|----|----|-------|----|----|----|-------|----|----|----|-----|-----|-----|-----|
| Description  | value |    |    |    | value |    |    |    | value |    |    |    | adr | adr | adr | adr |
| Values [hex] | 87    | D6 | 12 | 00 | 78    | 29 | ED | FF | 87    | D6 | 12 | 00 | 11  | EE  | 11  | EE  |

### 8.6.3 Sector trailer

The sector trailer is the last block (block 3) in one sector. Each sector has a sector trailer containing the

- secret keys A (mandatory) and B (optional), which return logical "0"s when read and
- the access conditions for the blocks of that sector, which are stored in bytes 6...9. The access bits also specify the type (data or value) of the data blocks.

If key B is not needed, the last 6 bytes of the sector trailer can be used as data bytes. The access bits for the sector trailer have to be configured accordingly, see [Section 8.7.2](#).

Byte 9 of the sector trailer is available for user data. For this byte the same access rights as for byte 6, 7 and 8 apply.

When the sector trailer is read, the key bytes are blanked out by returning logical zeros. If key B is configured to be readable, the data stored in bytes 10 to 15 is returned, see [Section 8.7.2](#).

All keys are set to FFFF FFFF FFFFh at chip delivery and the bytes 6, 7 and 8 are set to FF0780h.

| Byte Number | 0     | 1 | 2 | 3 | 4 | 5           | 6 | 7 | 8                | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|-------------|-------|---|---|---|---|-------------|---|---|------------------|---|----|----|----|----|----|----|
| Description | Key A |   |   |   |   | Access Bits |   |   | Key B (optional) |   |    |    |    |    |    |    |

*001aan013*

Figure 9. Sector trailer

## 8.7 Memory access

Before any memory operation can be done, the card has to be selected and authenticated as described in [Section 8.2](#). The possible memory operations for an addressed block depend on the key used during authentication and the access conditions stored in the associated sector trailer.

Table 5. Memory operations

| Operation | Description  | Valid for Block Type                 |
|-----------|--|--------------------------------------|
| Read      | reads one memory block   | read/write, value and sector trailer |
| Write     | writes one memory block  | read/write, value and sector trailer |
| Increment | increments the contents of a block and stores the result in the internal Transfer Buffer | value                                |
| Decrement | decrements the contents of a block and stores the result in the internal Transfer Buffer | value                                |

| Operation | Description   | Valid for Block Type |
|-----------|---|----------------------|
| Transfer  | writes the contents of the internal Transfer Buffer to a block  | value and read/write |
| Restore   | reads the contents of a block into the internal Transfer Buffer | value                |

8.7.1 Access conditions

The access conditions for every data block and sector trailer are defined by 3 bits, which are stored non-inverted and inverted in the sector trailer of the specified sector.

The access bits control the rights of memory access using the secret keys A and B. The access conditions may be altered, provided one knows the relevant key and the current access condition allows this operation.

**Remark:** With each memory access the internal logic verifies the format of the access conditions. If it detects a format violation the whole sector is irreversibly blocked.

**Remark:** In the following description the access bits are mentioned in the non-inverted mode only.

The internal logic of the MF1S50yyX/V1 ensures that the commands are executed only after a successful authentication.

Table 6. Access conditions

| Access Bits   | Valid Commands                                       |   | Block | Description    |
|---|--|---|-------|----------------|
| C <sub>13</sub> , C <sub>23</sub> , C <sub>33</sub> | read, write  | → | 3     | sector trailer |
| C <sub>12</sub> , C <sub>22</sub> , C <sub>32</sub> | read, write, increment, decrement, transfer, restore | → | 2     | data block     |
| C <sub>11</sub> , C <sub>21</sub> , C <sub>31</sub> | read, write, increment, decrement, transfer, restore | → | 1     | data block     |
| C <sub>10</sub> , C <sub>20</sub> , C <sub>30</sub> | read, write, increment, decrement, transfer, restore | → | 0     | data block     |

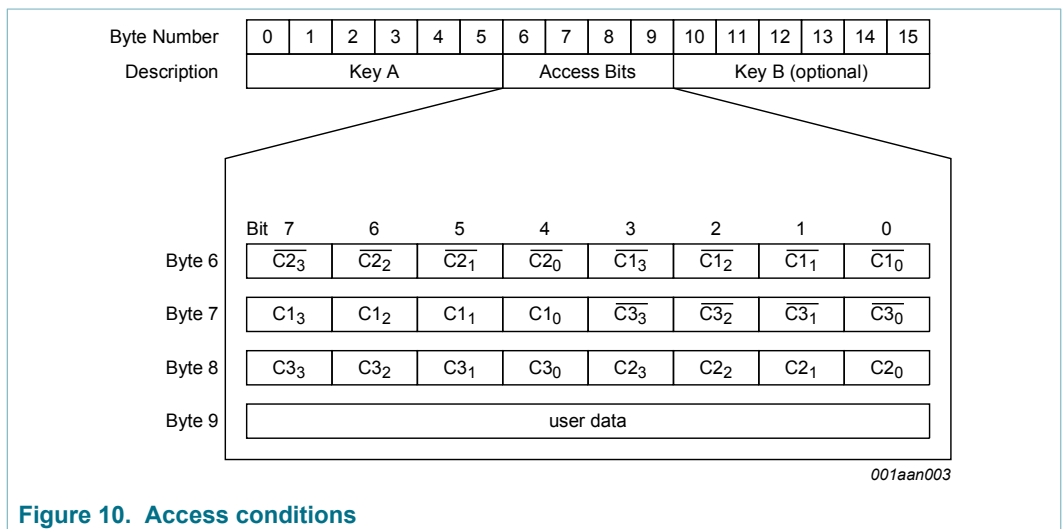


Figure 10. Access conditions

8.7.2 Access conditions for the sector trailer

Depending on the access bits for the sector trailer (block 3) the read/write access to the keys and the access bits is specified as ‘never’, ‘key A’, ‘key B’ or key A|B’ (key A or key B).

On chip delivery the access conditions for the sector trailers and key A are predefined as transport configuration. Since key B may be read in the transport configuration, new cards must be authenticated with key A. Since the access bits themselves can also be blocked, special care has to be taken during the personalization of cards.

Table 7. Access conditions for the sector trailer

| Access bits |    |    | Access condition for |       |             |       |       |       | Remark  |
|-------------|----|----|----------------------|-------|-------------|-------|-------|-------|---|
|             |    |    | KEYA                 |       | Access bits |       | KEYB  |       |   |
| C1          | C2 | C3 | read                 | write | read        | write | read  | write |   |
| 0           | 0  | 0  | never                | key A | key A       | never | key A | key A | Key B may be read <sup>[1]</sup>                          |
| 0           | 1  | 0  | never                | never | key A       | never | key A | never | Key B may be read <sup>[1]</sup>                          |
| 1           | 0  | 0  | never                | key B | key A B     | never | never | key B |   |
| 1           | 1  | 0  | never                | never | key A B     | never | never | never |   |
| 0           | 0  | 1  | never                | key A | key A       | key A | key A | key A | Key B may be read, transport configuration <sup>[1]</sup> |
| 0           | 1  | 1  | never                | key B | key A B     | key B | never | key B |   |
| 1           | 0  | 1  | never                | never | key A B     | key B | never | never |   |
| 1           | 1  | 1  | never                | never | key A B     | never | never | never |   |

[1] For this access condition key B is readable and may be used for data

8.7.3 Access conditions for data blocks

Depending on the access bits for data blocks (blocks 0...2) the read/write access is specified as ‘never’, ‘key A’, ‘key B’ or ‘key A|B’ (key A or key B). The setting of the relevant access bits defines the application and the corresponding applicable commands.

- Read/write block: the operations read and write are allowed.
- Value block: Allows the additional value operations increment, decrement, transfer and restore. With access condition ‘001’ only read and decrement are possible which reflects a non-rechargeable card. For access condition ‘110’ recharging is possible by using key B.
- Manufacturer block: the read-only condition is not affected by the access bits setting!
- Key management: in transport configuration key A must be used for authentication

Table 8. Access conditions for data blocks

| Access bits |    |    | Access condition for |         |           |                              | Application                            |
|-------------|----|----|----------------------|---------|-----------|------------------------------|--|
| C1          | C2 | C3 | read                 | write   | increment | decrement, transfer, restore |  |
| 0           | 0  | 0  | key A B              | key A B | key A B   | key A B                      | transport configuration <sup>[1]</sup> |

| Access bits |   |   | Access condition for |       |       |         | Application                     |
|-------------|---|---|----------------------|-------|-------|---------|---------------------------------|
| 0           | 1 | 0 | key A B              | never | never | never   | read/write block <sup>[1]</sup> |
| 1           | 0 | 0 | key A B              | key B | never | never   | read/write block <sup>[1]</sup> |
| 1           | 1 | 0 | key A B              | key B | key B | key A B | value block <sup>[1]</sup>      |
| 0           | 0 | 1 | key A B              | never | never | key A B | value block <sup>[1]</sup>      |
| 0           | 1 | 1 | key B                | key B | never | never   | read/write block <sup>[1]</sup> |
| 1           | 0 | 1 | key B                | never | never | never   | read/write block <sup>[1]</sup> |
| 1           | 1 | 1 | never                | never | never | never   | read/write block                |

[1] If key B may be read in the corresponding Sector Trailer it cannot serve for authentication (see grey marked lines in [Table 7](#)). As a consequences, if the reader authenticates any block of a sector which uses such access conditions for the Sector Trailer and using key B, the card will refuse any subsequent memory access after authentication.

## 9 Command overview

**Note:** In this document the term „MIFARE Classic card“ refers to a MIFARE Classic IC-based contactless card.

The MIFARE Classic card activation follows the ISO/IEC 14443 Type A. After the MIFARE Classic card has been selected, it can either be deactivated using the ISO/IEC 14443 Halt command, or the MIFARE Classic commands can be performed. For more details about the card activation refer to [Ref. 4](#).

### 9.1 MIFARE Classic command overview

All MIFARE Classic commands typically use the MIFARE Classic using Crypto1 and require an authentication.

All available commands for the MIFARE Classic EV1 with 1K memory are shown in [Table 9](#).

**Table 9. Command overview**

| Command                   | ISO/IEC 14443     | Command code (hexadecimal) |
|---------------------------|-------------------|----------------------------|
| Request                   | REQA              | 26h (7 bit)                |
| Wake-up                   | WUPA              | 52h (7 bit)                |
| Anticollision CL1         | Anticollision CL1 | 93h 20h                    |
| Select CL1                | Select CL1        | 93h 70h                    |
| Anticollision CL2         | Anticollision CL2 | 95h 20h                    |
| Select CL2                | Select CL2        | 95h 70h                    |
| Halt                      | Halt              | 50h 00h                    |
| Authentication with Key A | -                 | 60h                        |
| Authentication with Key B | -                 | 61h                        |
| Personalize UID Usage     | -                 | 40h                        |
| SET_MOD_TYPE              | -                 | 43h                        |
| MIFARE Read               | -                 | 30h                        |

| Command          | ISO/IEC 14443 | Command code (hexadecimal) |
|------------------|---------------|----------------------------|
| MIFARE Write     | -             | A0h                        |
| MIFARE Decrement | -             | C0h                        |
| MIFARE Increment | -             | C1h                        |
| MIFARE Restore   | -             | C2h                        |
| MIFARE Transfer  | -             | B0h                        |

All commands use the coding and framing as described in [Ref. 3](#) and [Ref. 4](#) if not otherwise specified.

### 9.2 Timings

The timing shown in this document are not to scale and values are rounded to 1 μs.

All given times refer to the data frames including start of communication and end of communication. A PCD data frame contains the start of communication (1 "start bit") and the end of communication (one logic 0 + 1 bit length of unmodulated carrier). A PICC data frame contains the start of communication (1 "start bit") and the end of communication (1 bit length of no subcarrier).

The minimum command response time is specified according to [Ref. 4](#) as an integer n which specifies the PCD to PICC frame delay time. The frame delay time from PICC to PCD is at least 87 μs. The maximum command response time is specified as a time-out value. Depending on the command, the T<sub>ACK</sub> value specified for command responses defines the PCD to PICC frame delay time. It does it for either the 4-bit ACK value specified in [Section 9.3](#) or for a data frame.

All command timings are according to ISO/IEC 14443-3 frame specification as shown for the Frame Delay Time in [Figure 11](#). For more details refer to [Ref. 3](#) and [Ref. 4](#).

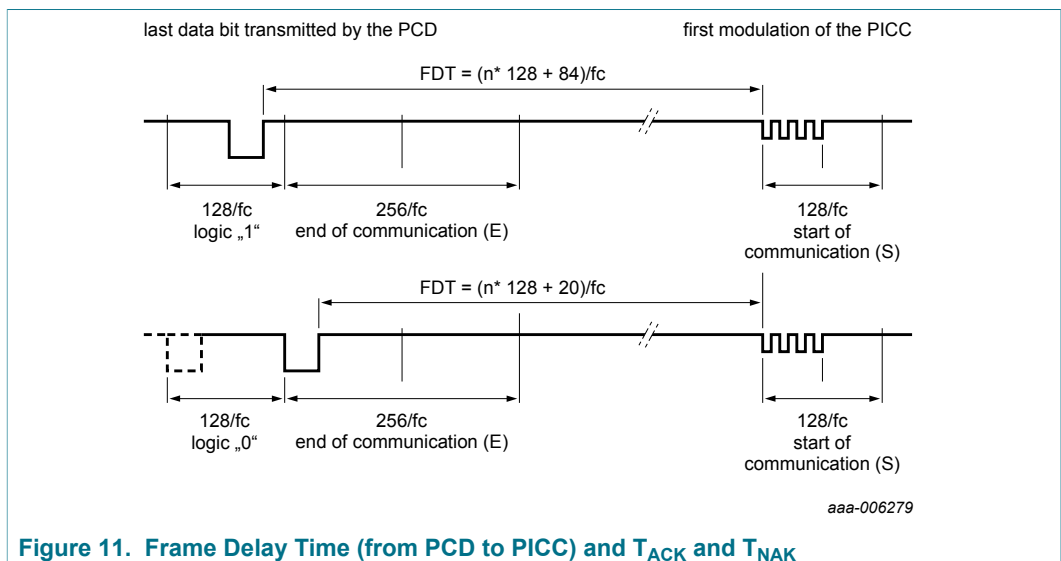


Figure 11. Frame Delay Time (from PCD to PICC) and T<sub>ACK</sub> and T<sub>NAK</sub>

**Remark:** Due to the coding of commands, the measured timings usually excludes (a part of) the end of communication. Consider this factor when comparing the specified with the measured times.



### 9.3 MIFARE Classic ACK and NAK

The MIFARE Classic uses a 4 bit ACK / NAK as shown in [Table 10](#).

**Table 10. MIFARE ACK and NAK**

| Code (4-bit) | Transfer Buffer Validity | Description         |
|--------------|--------------------------|---------------------|
| Ah           |                          | Acknowledge (ACK)   |
| 0h           | valid                    | invalid operation   |
| 1h           | valid                    | parity or CRC error |
| 4h           | invalid                  | invalid operation   |
| 5h           | invalid                  | parity or CRC error |

### 9.4 ATQA and SAK responses

For details on the type identification procedure please refer to [Ref. 2](#).

The MF1S50yyX/V1 answers to a REQA or WUPA command with the ATQA value shown in [Table 11](#) and to a Select CL1 command (CL2 for the 7-byte UID variant) with the SAK value shown in [Table 12](#).

**Table 11. ATQA response of the MF1S50yyX/V1**

| Sales Type | Hex Value          | Bit Number |    |    |    |    |    |    |   |   |   |   |   |   |   |   |   |
|------------|--------------------|------------|----|----|----|----|----|----|---|---|---|---|---|---|---|---|---|
|            |                    | 16         | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| MF1S500yX  | 00 44h             | 0          | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 |
| MF1S503yX  | 00 04h             | 0          | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| MF1S700yX  | 00 42 <sub>h</sub> | 0          | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 |
| MF1S703yX  | 00 02 <sub>h</sub> | 0          | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |

**Table 12. SAK response of the MF1S50yyX/V1**

| Sales Type   | Hex Value | Bit Number |   |   |   |   |   |   |   |
|--------------|-----------|------------|---|---|---|---|---|---|---|
|              |           | 8          | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| MF1S50yyX/V1 | 08h       | 0          | 0 | 0 | 0 | 1 | 0 | 0 | 0 |

**Remark:** The ATQA coding in bits 7 and 8 indicate the UID size according to ISO/IEC 14443 independent from the settings of the UID usage.

**Remark:** The bit numbering in the ISO/IEC 14443 starts with LSBit = bit 1, but not LSBit = bit 0. So one byte counts bit 1 to 8 instead of bit 0 to 7.

## 10 UID Options and Handling

The MF1S50yyX/V1 product family offers two delivery options for the UID which is stored in block 0 of sector 0.

- 7-byte UID
- 4-byte NUID (Non-Unique ID)

This section describes the MIFARE Classic MF1S50yyX/V1 operation when using one of the 2 UID options with respect to card selection, authentication and personalization. See also [Ref. 6](#) for details on how to handle UIDs and NUIDs with MIFARE Classic products.

### 10.1 7-byte UID Operation

All MF1S500yXDyy products are featuring a 7-byte UID. This 7-byte UID is stored in block 0 of sector 0 as shown in [Figure 7](#). The behaviour during anti-collision, selection and authentication can be configured during personalization for this UID variant.

#### 10.1.1 Personalization Options

The 7-byte UID variants of the MF1S50yyX/V1 can be operated with four different functionalities, denoted as UIDFn (UID Functionality n).

1. UIDF0: anti-collision and selection with the double size UID according to ISO/IEC 14443-3
2. UIDF1: anti-collision and selection with the double size UID according to ISO/IEC 14443-3 and optional usage of a selection process shortcut
3. UIDF2: anti-collision and selection with a single size random ID according to ISO/IEC 14443-3
4. UIDF3: anti-collision and selection with a single size NUID according to ISO/IEC 14443-3 where the NUID is calculated out of the 7-byte UID

The anti-collision and selection procedure and the implications on the authentication process are detailed in [Section 10.1.2](#) and [Section 10.1.3](#).

The default configuration at delivery is option 1 which enables the ISO/IEC 14443-3 compliant anti-collision and selection. This configuration can be changed using the 'Personalize UID Usage' command. The execution of this command requires an authentication to sector 0. Once this command has been issued and accepted by the PICC, the configuration is automatically locked. A subsequently issued 'Personalize UID Usage' command is not executed and a NAK is replied by the PICC.

**Remark:** As the configuration is changeable at delivery, it is strongly recommended to send this command at personalization of the card to prevent unwanted changes in the field. This should also be done if the default configuration is used.

**Remark:** The configuration becomes effective only after PICC unselect or PICC field reset.

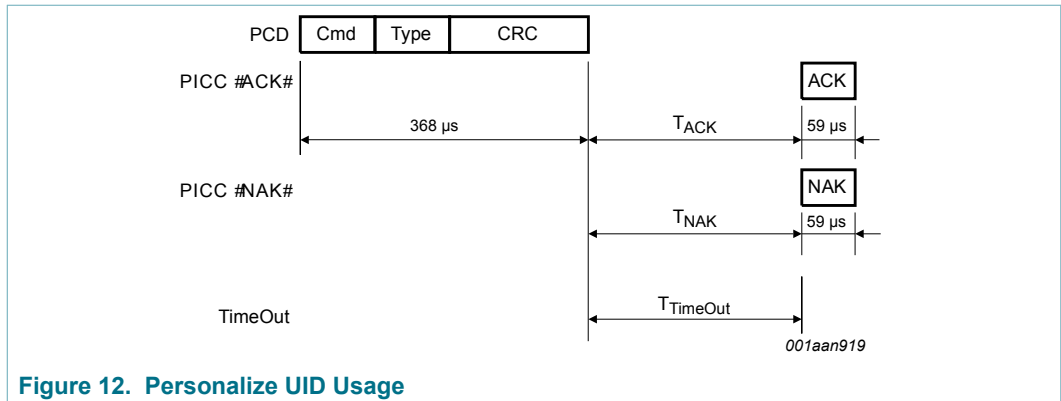


Figure 12. Personalize UID Usage

Table 13. Personalize UID Usage command

| Name     | Code                         | Description  | Length  |
|----------|------------------------------|--|---------|
| Cmd      | 40h                          | Set anti-collision, selection and authentication behaviour                         | 1 byte  |
| Type     | -                            | Encoded type of UID usage:<br>UIDF0: 00h<br>UIDF1: 40h<br>UIDF2: 20h<br>UIDF3: 60h | 1 byte  |
| CRC      | -                            | CRC according to <a href="#">Ref. 4</a>  | 2 bytes |
| ACK, NAK | see <a href="#">Table 10</a> | see <a href="#">Section 9.3</a>  | 4-bit   |

Table 14. Personalize UID Usage timing

|                       | T <sub>ACK min</sub> | T <sub>ACK max</sub> | T <sub>NAK min</sub> | T <sub>NAK max</sub> | T <sub>TimeOut</sub> |
|-----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|
| Personalize UID Usage | n=9                  | T <sub>TimeOut</sub> | n=9                  | T <sub>TimeOut</sub> | 10 ms                |

### 10.1.2 Anti-collision and Selection

Depending on the chosen personalization option there are certain possibilities to perform anti-collision and selection. To bring the MIFARE Classic contactless IC into the ACTIVE state according to ISO/IEC 14443-3, the following sequences are available.

Sequence 1: ISO/IEC 14443-3 compliant anti-collision and selection using the cascade level 1 followed by the cascade level 2 SEL command

Sequence 2: using cascade level 1 anti-collision and selection procedure followed by a Read command from block 0

Sequence 3: ISO/IEC 14443-3 compliant anti-collision and selection using the cascade level 1 SEL command

**Remark:** The Read from Block 0 in Sequence 2 does not require a prior authentication to Sector 0 and is transmitted in plain data. For all other sequences, the readout from Block 0 in Sector 0 is encrypted and requires an authentication to that sector.

**Remark:** The settings done with Personalize UID Usage do not change the ATQA coding.

**Table 15. Available activation sequences for 7-byte UID options**

| UID Functionality | Available Activation Sequences |
|-------------------|--------------------------------|
| UIDF0             | Sequence 1                     |
| UIDF1             | Sequence 1, Sequence 2         |
| UIDF2             | Sequence 3                     |
| UIDF3             | Sequence 3                     |

### 10.1.3 Authentication

During the authentication process, 4-byte of the UID are passed on to the MIFARE Classic Authenticate command of the contactless reader IC. Depending on the activation sequence, those 4-byte are chosen differently. In general, the input parameter to the MIFARE Classic Authenticate command is the set of 4 bytes retrieved during the last cascade level from the ISO/IEC 14443-3 Type A anticollision.

**Table 16. Input parameter to MIFARE Classic Authenticate**

| UID Functionality | Input to MIFARE Classic Authenticate Command |
|-------------------|--|
| Sequence 1        | CL2 bytes (UID3...UID6)                      |
| Sequence 2        | CL1 bytes (CT, UID0...UID2)                  |
| Sequence 3        | 4-byte NUID/RID (UID0...UID3)                |

## 10.2 4-byte UID Operation

All MF1S503yXDyy products are featuring a 4-byte NUID. This 4-byte NUID is stored in block 0 of sector 0 as shown in [Figure 6](#).

### 10.2.1 Anti-collision and Selection

The anti-collision and selection process for the product variants featuring 4-byte NUIDs is done according to ISO/IEC 14443-3 Type A using cascade level 1 only.

### 10.2.2 Authentication

The input parameter to the MIFARE Classic Authenticate command is the full 4-byte UID retrieved during the anti-collision procedure. This is the same as for the activation Sequence 3 in the 7-byte UID variant.

## 11 Load Modulation Strength Option

The MIFARE Classic EV1 with 1K memory features the possibility to set the load modulation strength to high or normal. The default level is set to a high modulation strength and it is recommended for optimal performance to maintain this level and only switch to the low load modulation strength if the contactless system requires it.

**Remark:** The configuration becomes effective only after a PICC unselect or a PICC field reset. The configuration can be changed multiple times by asserting the command.

**Remark:** The MIFARE Classic EV1 with 1K memory needs to be authenticated to sector 0 with Key A to perform the SET\_MOD\_TYPE command. The Access Bits for sector 0 are irrelevant.

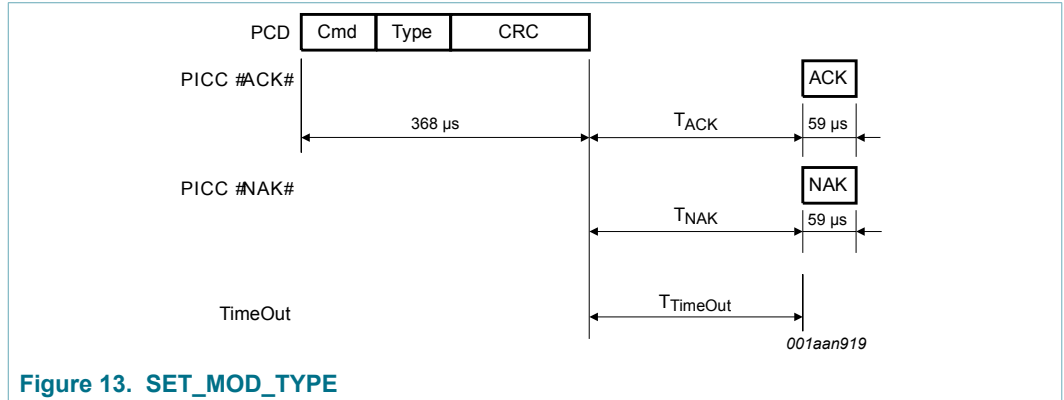


Figure 13. SET\_MOD\_TYPE

Table 17. SET\_MOD\_TYPE command

| Name     | Code                         | Description   | Length  |
|----------|------------------------------|---|---------|
| Cmd      | 43h                          | Set load modulation strength  | 1 byte  |
| Type     | -                            | Encoded load modulation strength:<br>strong modulation: 01h (default)<br>normal modulation: 00h | 1 byte  |
| CRC      | -                            | CRC according to <a href="#">Ref. 4</a>   | 2 bytes |
| ACK, NAK | see <a href="#">Table 10</a> | see <a href="#">Section 9.3</a>   | 4-bit   |

Table 18. SET\_MOD\_TYPE timing

|              | T <sub>ACK min</sub> | T <sub>ACK max</sub> | T <sub>NAK min</sub> | T <sub>NAK max</sub> | T <sub>TimeOut</sub> |
|--------------|----------------------|----------------------|----------------------|----------------------|----------------------|
| SET_MOD_TYPE | n=9                  | T <sub>TimeOut</sub> | n=9                  | T <sub>TimeOut</sub> | 5 ms                 |

The configured load modulation is shown in the manufacturer data of block 0 in sector 0. The exact location is shown below in [Figure 14](#) and [Table 19](#).

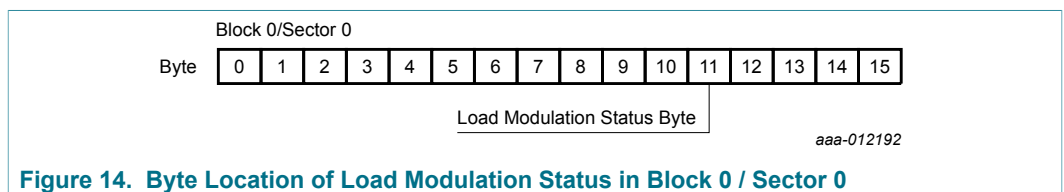


Figure 14. Byte Location of Load Modulation Status in Block 0 / Sector 0

Table 19. Load Modulation Status Indication

| Load Modulation Type   | Hex Value     | Bit Number |   |   |   |   |   |   |   |
|------------------------|---------------|------------|---|---|---|---|---|---|---|
|                        |               | 7          | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| strong load modulation | 20h (default) | 0          | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| normal load modulation | 00h           | 0          | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

## 12 MIFARE Classic commands

### 12.1 MIFARE Classic Authentication

The MIFARE Classic authentication is a 3-pass mutual authentication which needs two pairs of command-response. These two parts, MIFARE Classic authentication part 1 and part 2 are shown in [Figure 15](#), [Figure 16](#) and [Table 20](#).

[Table 21](#) shows the required timing.

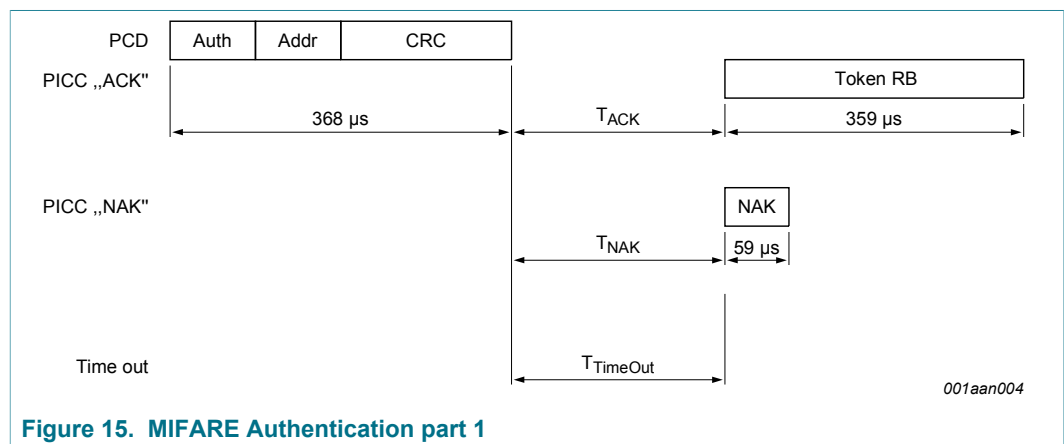


Figure 15. MIFARE Authentication part 1

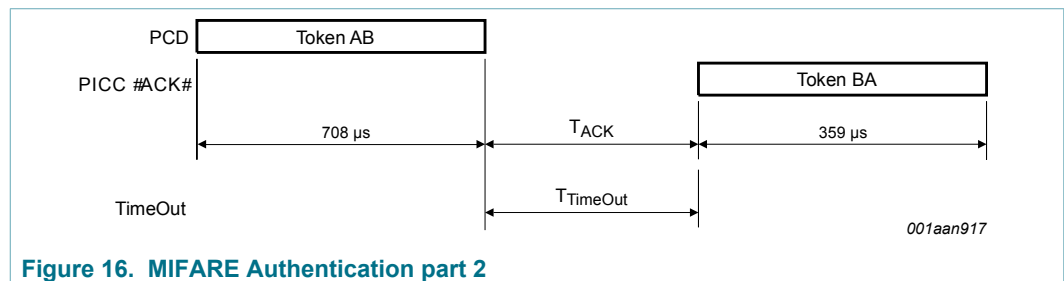


Figure 16. MIFARE Authentication part 2

Table 20. MIFARE Classic authentication command

| Name              | Code                         | Description                             | Length  |
|-------------------|------------------------------|---|---------|
| Auth (with Key A) | 60h                          | Authentication with Key A               | 1 byte  |
| Auth (with Key B) | 61h                          | Authentication with Key B               | 1 byte  |
| Addr              | -                            | MIFARE Block address (00h to FFh)       | 1 byte  |
| CRC               | -                            | CRC according to <a href="#">Ref. 4</a> | 2 bytes |
| Token RB          | -                            | Challenge 1 (Random Number)             | 4 bytes |
| Token AB          | -                            | Challenge 2 (encrypted data)            | 8 bytes |
| Token BA          | -                            | Challenge 2 (encrypted data)            | 4 bytes |
| NAK               | see <a href="#">Table 10</a> | see <a href="#">Section 9.3</a>         | 4-bit   |

**Table 21. MIFARE Classic authentication timing**

|                       | T <sub>ACK min</sub> | T <sub>ACK max</sub> | T <sub>NAK min</sub> | T <sub>NAK max</sub> | T <sub>TimeOut</sub> |
|-----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|
| Authentication part 1 | n=9                  | T <sub>TimeOut</sub> | n=9                  | n=9                  | 1 ms                 |
| Authentication part 2 | n=9                  | T <sub>TimeOut</sub> |                      |                      | 1 ms                 |

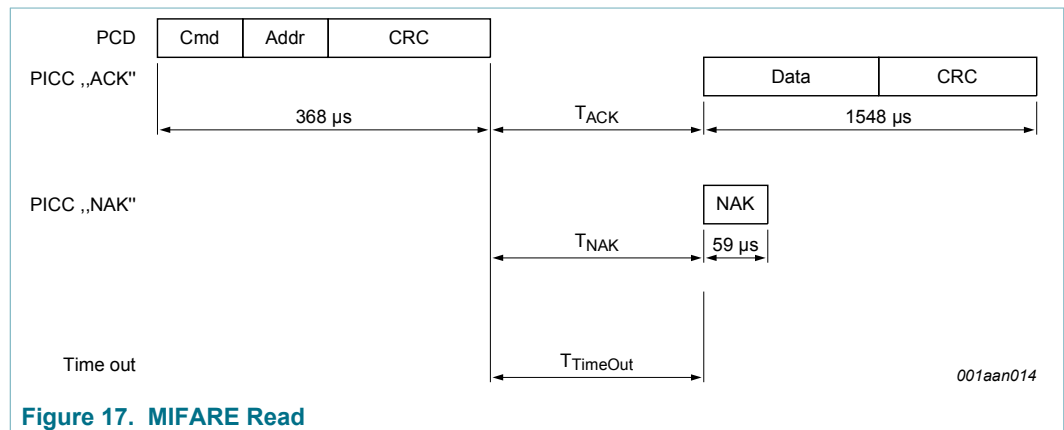
**Remark:** The minimum required time between MIFARE Classic Authentication part 1 and part 2 is the minimum required FDT according to [Ref. 4](#). There is no maximum time specified.

**Remark:** The MIFARE Classic authentication and encryption requires an NFC reader IC for MIFARE products (e.g. the CL RC632). For more details about the authentication command refer to the corresponding data sheet (e.g. [Ref. 5](#)). The 4-byte input parameter for the MIFARE Classic Authentication is detailed in [Section 10.1.3](#) and [Section 10.2.2](#).

## 12.2 MIFARE Read

The MIFARE Read requires a block address, and returns the 16 bytes of one MIFARE Classic block. The command structure is shown in [Figure 17](#) and [Table 22](#).

[Table 23](#) shows the required timing.



**Figure 17. MIFARE Read**

**Table 22. MIFARE Read command**

| Name | Code                         | Description                             | Length   |
|------|------------------------------|---|----------|
| Cmd  | 30h                          | Read one block                          | 1 byte   |
| Addr | -                            | MIFARE Block address (00h to FFh)       | 1 byte   |
| CRC  | -                            | CRC according to <a href="#">Ref. 4</a> | 2 bytes  |
| Data | -                            | Data content of the addressed block     | 16 bytes |
| NAK  | see <a href="#">Table 10</a> | see <a href="#">Section 9.3</a>         | 4-bit    |

**Table 23. MIFARE Read timing**

|      | T <sub>ACK min</sub> | T <sub>ACK max</sub> | T <sub>NAK min</sub> | T <sub>NAK max</sub> | T <sub>TimeOut</sub> |
|------|----------------------|----------------------|----------------------|----------------------|----------------------|
| Read | n=9                  | T <sub>TimeOut</sub> | n=9                  | T <sub>TimeOut</sub> | 5 ms                 |

### 12.3 MIFARE Write

The MIFARE Write requires a block address, and writes 16 bytes of data into the addressed MIFARE Classic EV1 with 1K memory block. It needs two pairs of command-response. These two parts, MIFARE Write part 1 and part 2 are shown in [Figure 18](#) and [Figure 19](#) and [Table 24](#).

[Table 25](#) shows the required timing.

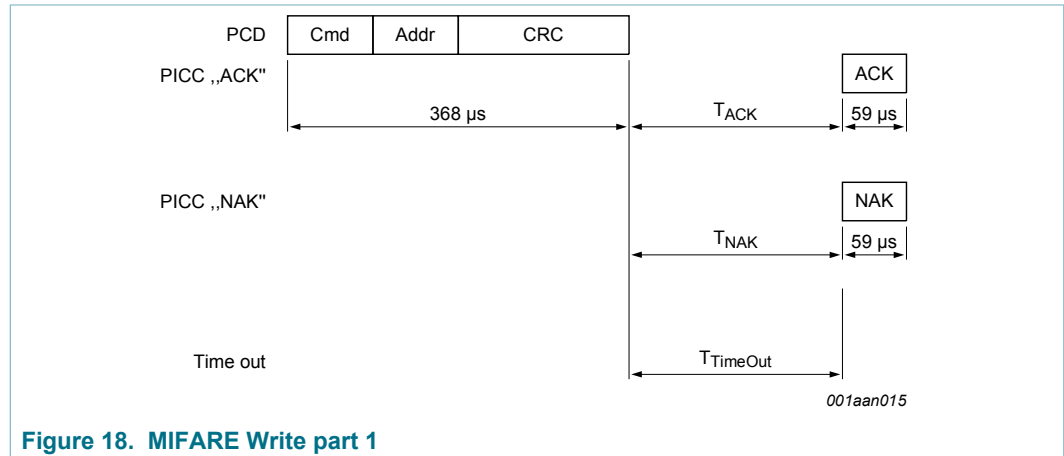


Figure 18. MIFARE Write part 1

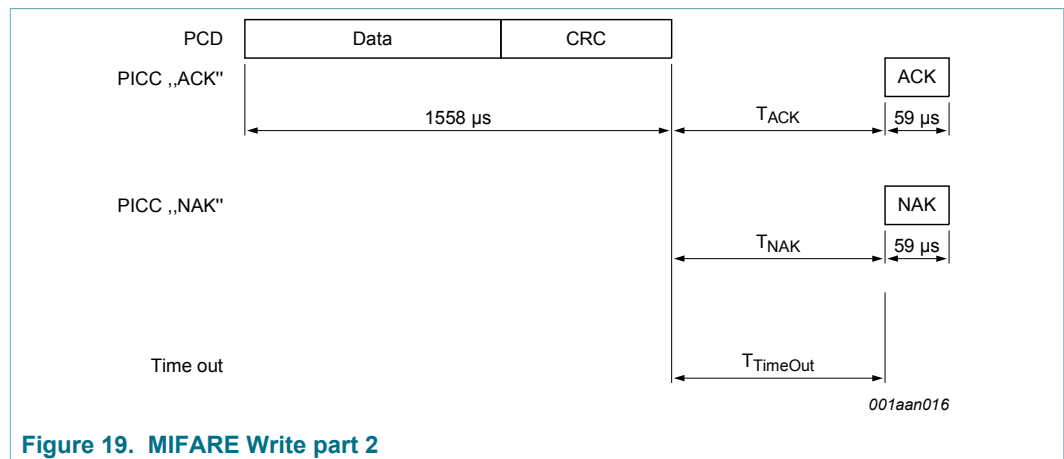


Figure 19. MIFARE Write part 2

Table 24. MIFARE Write command

| Name | Code                         | Description                               | Length   |
|------|------------------------------|---|----------|
| Cmd  | A0h                          | Write one block                           | 1 byte   |
| Addr | -                            | MIFARE Block or Page address (00h to FFh) | 1 byte   |
| CRC  | -                            | CRC according to <a href="#">Ref. 4</a>   | 2 bytes  |
| Data | -                            | Data                                      | 16 bytes |
| NAK  | see <a href="#">Table 10</a> | see <a href="#">Section 9.3</a>           | 4-bit    |



Table 25. MIFARE Write timing

|              | T <sub>ACK min</sub> | T <sub>ACK max</sub> | T <sub>NAK min</sub> | T <sub>NAK max</sub> | T <sub>TimeOut</sub> |
|--------------|----------------------|----------------------|----------------------|----------------------|----------------------|
| Write part 1 | n=9                  | T <sub>TimeOut</sub> | n=9                  | T <sub>TimeOut</sub> | 5 ms                 |
| Write part 2 | n=9                  | T <sub>TimeOut</sub> | n=9                  | T <sub>TimeOut</sub> | 10 ms                |

**Remark:** The minimum required time between MIFARE Write part 1 and part 2 is the minimum required FDT according to Ref. 4. There is no maximum time specified.

### 12.4 MIFARE Increment, Decrement and Restore

The MIFARE Increment requires a source block address and an operand. It adds the operand to the value of the addressed block, and stores the result in the Transfer Buffer.

The MIFARE Decrement requires a source block address and an operand. It subtracts the operand from the value of the addressed block, and stores the result in the Transfer Buffer.

The MIFARE Restore requires a source block address. It copies the value of the addressed block into the Transfer Buffer. The 4 byte Operand in the second part of the command is not used and may contain arbitrary values.

All three commands are responding with a NAK to the first command part if the addressed block is not formatted to be a valid value block, see Section 8.6.2.1.

The two parts of each command are shown in Figure 20 and Figure 21 and Table 26.

Table 27 shows the required timing.

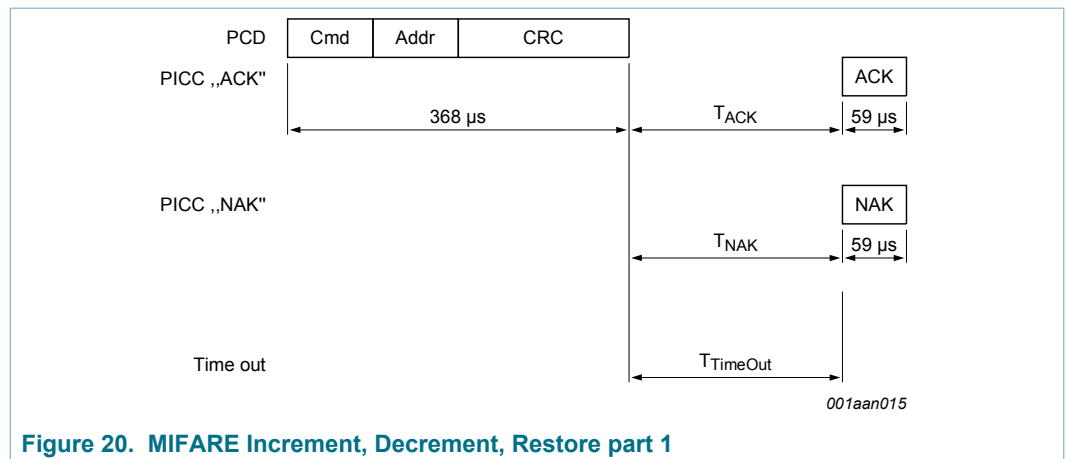
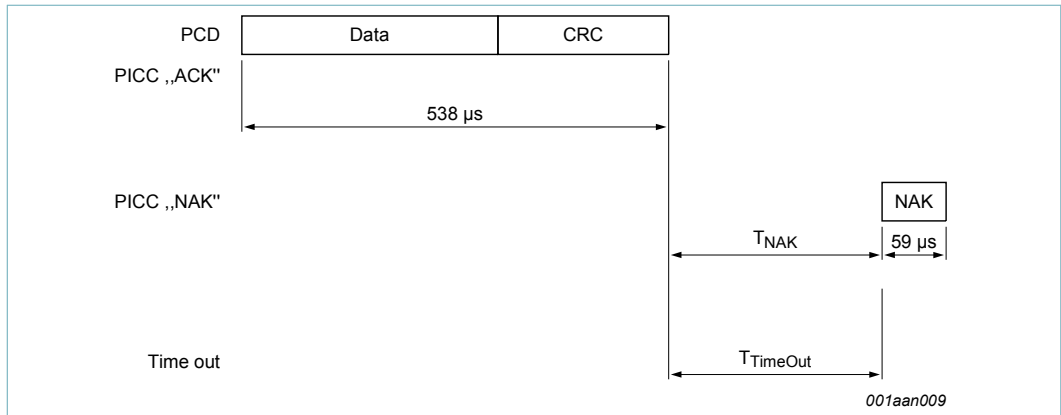


Figure 20. MIFARE Increment, Decrement, Restore part 1



1. Increment, Decrement and Restore part 2 does not acknowledge

Figure 21. MIFARE Increment, Decrement, Restore part 2

Table 26. MIFARE Increment, Decrement and Restore command

| Name | Code                         | Description                              | Length  |
|------|------------------------------|--|---------|
| Cmd  | C1h                          | Increment                                | 1 byte  |
| Cmd  | C0h                          | Decrement                                | 1 byte  |
| Cmd  | C2h                          | Restore                                  | 1 byte  |
| Addr | -                            | MIFARE source block address (00h to FFh) | 1 byte  |
| CRC  | -                            | CRC according to <a href="#">Ref. 4</a>  | 2 bytes |
| Data | -                            | Operand (4 byte signed integer)          | 4 bytes |
| NAK  | see <a href="#">Table 10</a> | see <a href="#">Section 9.3</a>          | 4-bit   |

Table 27. MIFARE Increment, Decrement and Restore timing

|  | T <sub>ACK min</sub> | T <sub>ACK max</sub> | T <sub>NAK min</sub> | T <sub>NAK max</sub> | T <sub>TimeOut</sub> |
|--|----------------------|----------------------|----------------------|----------------------|----------------------|
| Increment, Decrement, and Restore part 1 | n=9                  | T <sub>TimeOut</sub> | n=9                  | T <sub>TimeOut</sub> | 5 ms                 |
| Increment, Decrement, and Restore part 2 | n=9                  | T <sub>TimeOut</sub> | n=9                  | T <sub>TimeOut</sub> | 5 ms                 |

**Remark:** The minimum required time between MIFARE Increment, Decrement, and Restore part 1 and part 2 is the minimum required FDT according to [Ref. 4](#). There is no maximum time specified.

**Remark:** The MIFARE Increment, Decrement, and Restore commands require a MIFARE Transfer to store the value into a destination block.

**Remark:** The MIFARE Increment, Decrement, and Restore command part 2 does not provide an acknowledgement, so the regular time out has to be used instead.

12.5 MIFARE Transfer

The MIFARE Transfer requires a destination block address, and writes the value stored in the Transfer Buffer into one MIFARE Classic block. The command structure is shown in Figure 22 and Table 28.

Table 29 shows the required timing.

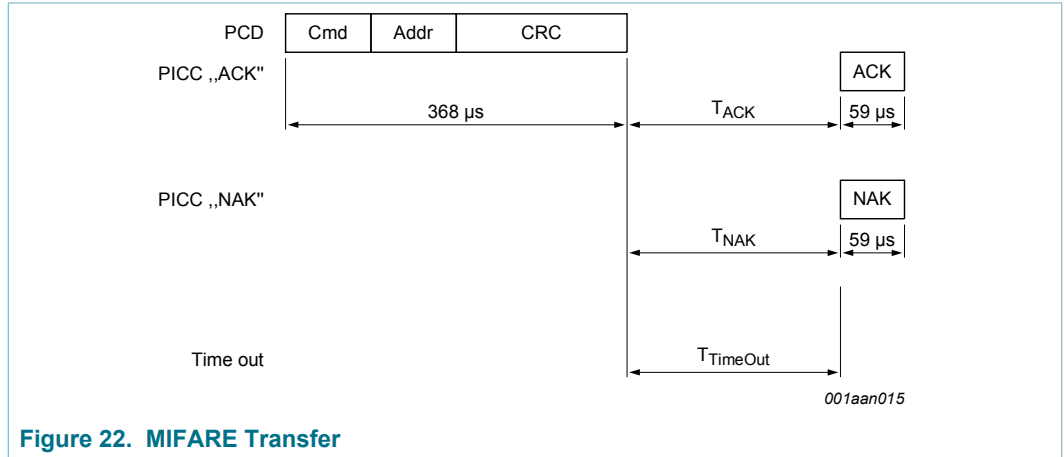


Figure 22. MIFARE Transfer

Table 28. MIFARE Transfer command

| Name | Code         | Description   | Length  |
|------|--------------|---|---------|
| Cmd  | B0h          | Write the value from the Transfer Buffer into destination block | 1 byte  |
| Addr | -            | MIFARE destination block address (00h to FFh)                   | 1 byte  |
| CRC  | -            | CRC according to Ref. 4   | 2 bytes |
| NAK  | see Table 10 | see Section 9.3   | 4-bit   |

Table 29. MIFARE Transfer timing

|          | T <sub>ACK min</sub> | T <sub>ACK max</sub> | T <sub>NAK min</sub> | T <sub>NAK max</sub> | T <sub>TimeOut</sub> |
|----------|----------------------|----------------------|----------------------|----------------------|----------------------|
| Transfer | n=9                  | T <sub>TimeOut</sub> | n=9                  | T <sub>TimeOut</sub> | 10 ms                |

13 Limiting values

Stresses above one or more of the limiting values may cause permanent damage to the device. Exposure to limiting values for extended periods may affect device reliability.


Table 30. Limiting values

In accordance with the Absolute Maximum Rating System (IEC 60134).

| Symbol                 | Parameter                           | Min | Max | Unit |
|------------------------|-------------------------------------|-----|-----|------|
| I <sub>I</sub>         | input current                       | -   | 30  | mA   |
| P <sub>tot</sub> /pack | total power dissipation per package | -   | 120 | mW   |

| Symbol           | Parameter   | Min | Max | Unit |
|------------------|---|-----|-----|------|
| T <sub>stg</sub> | storage temperature                                     | -55 | 125 | °C   |
| T <sub>amb</sub> | ambient temperature                                     | -25 | 70  | °C   |
| V <sub>ESD</sub> | electrostatic discharge voltage on LA/LB <sup>[1]</sup> | 2   | -   | kV   |

[1] ANSI/ESDA/JEDEC JS-001; Human body model: C = 100 pF, R = 1.5 kΩ

| CAUTION   |   |
|---|---|
|  | <p>This device has limited built-in ElectroStatic Discharge (ESD) protection. The leads should be shorted together or the device placed in conductive foam during storage or handling to prevent electrostatic damage to the gates.</p> |

## 14 Characteristics

Table 31. Characteristics

| Symbol                        | Parameter         | Conditions               | Min    | Typ    | Max  | Unit  |
|-------------------------------|-------------------|--------------------------|--------|--------|------|-------|
| C <sub>i</sub>                | input capacitance | [1]                      | 14.9   | 16.9   | 19.0 | pF    |
| f <sub>i</sub>                | input frequency   |                          | -      | 13.56  | -    | MHz   |
| <b>EEPROM characteristics</b> |                   |                          |        |        |      |       |
| t <sub>ret</sub>              | retention time    | T <sub>amb</sub> = 22 °C | 10     | -      | -    | year  |
| N <sub>endu(W)</sub>          | write endurance   | T <sub>amb</sub> = 22 °C | 100000 | 200000 | -    | cycle |

[1] T<sub>amb</sub>=22°C, f=13,56MHz, V<sub>LaLb</sub> = 1,5 V RMS

## 15 Wafer specification

For more details on the wafer delivery forms see [Ref. 9](#).

Table 32. Wafer specifications MF1S50yyXDUy

| Wafer                                 |   |
|---------------------------------------|---|
| diameter                              | 200 mm typical (8 inches)<br>300 mm typical (12 inches) |
| maximum diameter after foil expansion | 210 mm (8 inches)<br>not applicable (12 inches)         |
| die separation process                | laser dicing (8 inches)<br>blade dicing (12 inches)     |
| thickness MF1S50yyXDUD                | 120 μm ± 15 μm  |
| MF1S50yyXDUF                          | 75 μm ± 10 μm   |
| flatness                              | not applicable  |
| Potential Good Dies per Wafer (PGDW)  | 64727 (8 inches)<br>147540 (12 inches)                  |
| <b>Wafer backside</b>                 |   |
| material                              | Si  |

|   |   |
|---|---|
| treatment                                   | ground and stress relieve   |
| roughness                                   | $R_a$ max = 0.5 $\mu\text{m}$   |
|   | $R_t$ max = 5 $\mu\text{m}$   |
| <b>Chip dimensions</b>                      |   |
| step size <sup>[1]</sup>                    | x = 658 $\mu\text{m}$ (8 inches)  |
|   | x = 660 $\mu\text{m}$ (12 inches)   |
| gap between chips <sup>[1]</sup>            | y = 713 $\mu\text{m}$ (8 inches)  |
|   | y = 715 $\mu\text{m}$ (12 inches)   |
| gap between chips <sup>[1]</sup>            | typical = 19 $\mu\text{m}$  |
|   | minimum = 5 $\mu\text{m}$<br>not applicable (12 inches)                   |
| <b>Passivation</b>                          |   |
| type  | sandwich structure  |
| material                                    | PSG / nitride   |
| thickness                                   | 500 nm / 600 nm   |
| <b>Au bump (substrate connected to VSS)</b> |   |
| material                                    | > 99.9 % pure Au  |
| hardness                                    | 35 to 80 HV 0.005   |
| shear strength                              | > 70 MPa  |
| height                                      | 18 $\mu\text{m}$  |
| height uniformity                           | within a die = $\pm 2 \mu\text{m}$  |
|   | within a wafer = $\pm 3 \mu\text{m}$                                      |
|   | wafer to wafer = $\pm 4 \mu\text{m}$                                      |
| flatness                                    | minimum = $\pm 1.5 \mu\text{m}$   |
| size  | LA, LB, VSS, TEST <sup>[2]</sup> = 66 $\mu\text{m} \times 66 \mu\text{m}$ |
| size variation                              | $\pm 5 \mu\text{m}$   |
| under bump metallization                    | sputtered TiW   |

[1] The step size and the gap between chips may vary due to changing foil expansion

[2] Pads VSS and TESTIO are disconnected when wafer is sawn.

## 15.1 Fail die identification

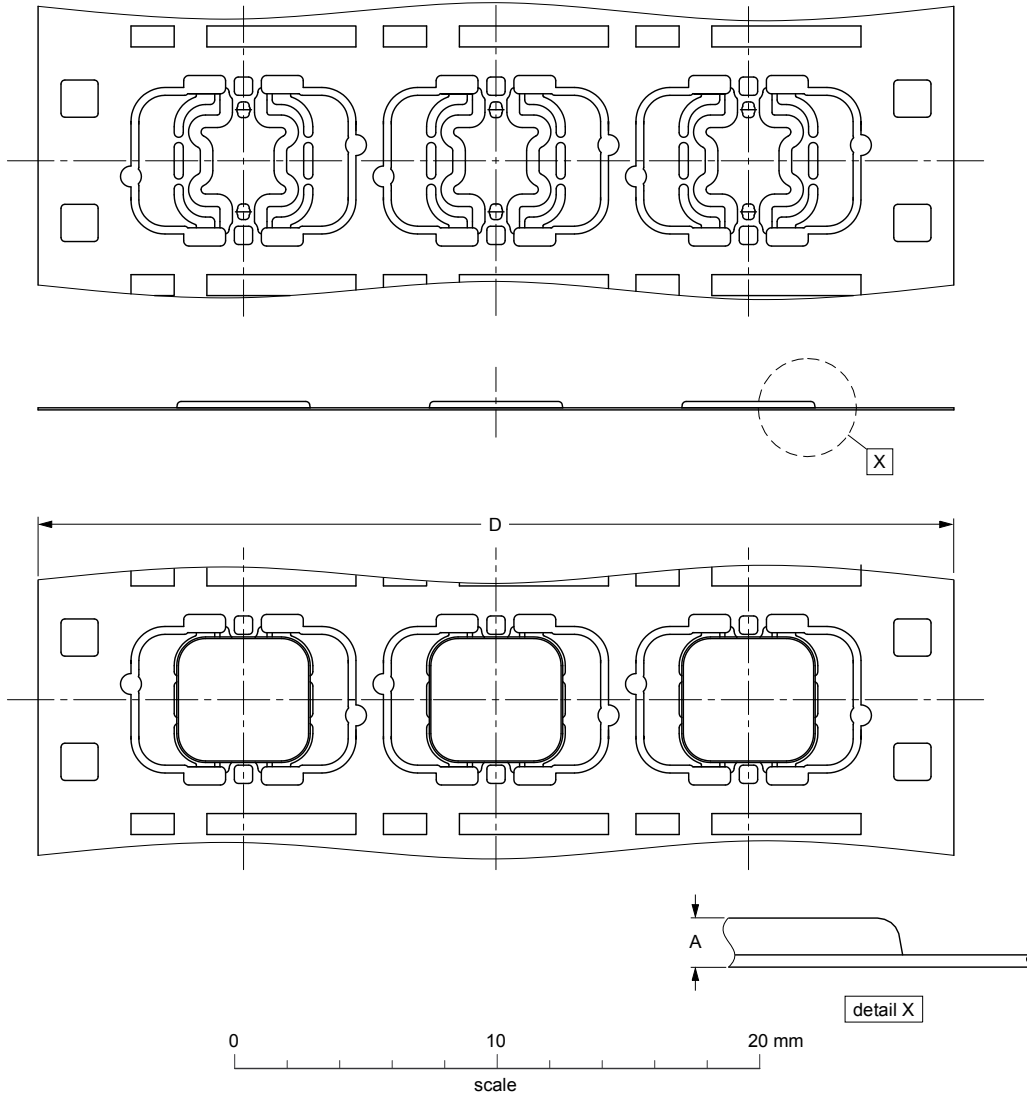
Electronic wafer mapping covers the electrical test results and additionally the results of mechanical/visual inspection. No ink dots are applied.

## 15.2 Package outline

For more details on the contactless modules MOA4 and MOA8 please refer to [Ref. 7](#) and [Ref. 8](#).

PLLMC: plastic leadless module carrier package; 35 mm wide tape

SOT500-2



**DIMENSIONS (mm are the original dimensions)**

| UNIT | A <sup>(1)</sup><br>max. | D              | For unspecified dimensions see PLLMC-drawing given in the subpackage code. |
|------|--------------------------|----------------|--|
| mm   | 0.33                     | 35.05<br>34.95 |  |

**Note**

1. Total package thickness, exclusive punching burr.

| OUTLINE VERSION | REFERENCES |       |       | EUROPEAN PROJECTION | ISSUE DATE           |
|-----------------|------------|-------|-------|---------------------|----------------------|
|                 | IEC        | JEDEC | JEITA |                     |                      |
| SOT500-2        | ---        | ---   | ---   |                     | 03-09-17<br>06-05-22 |

Figure 23. Package outline SOT500-2

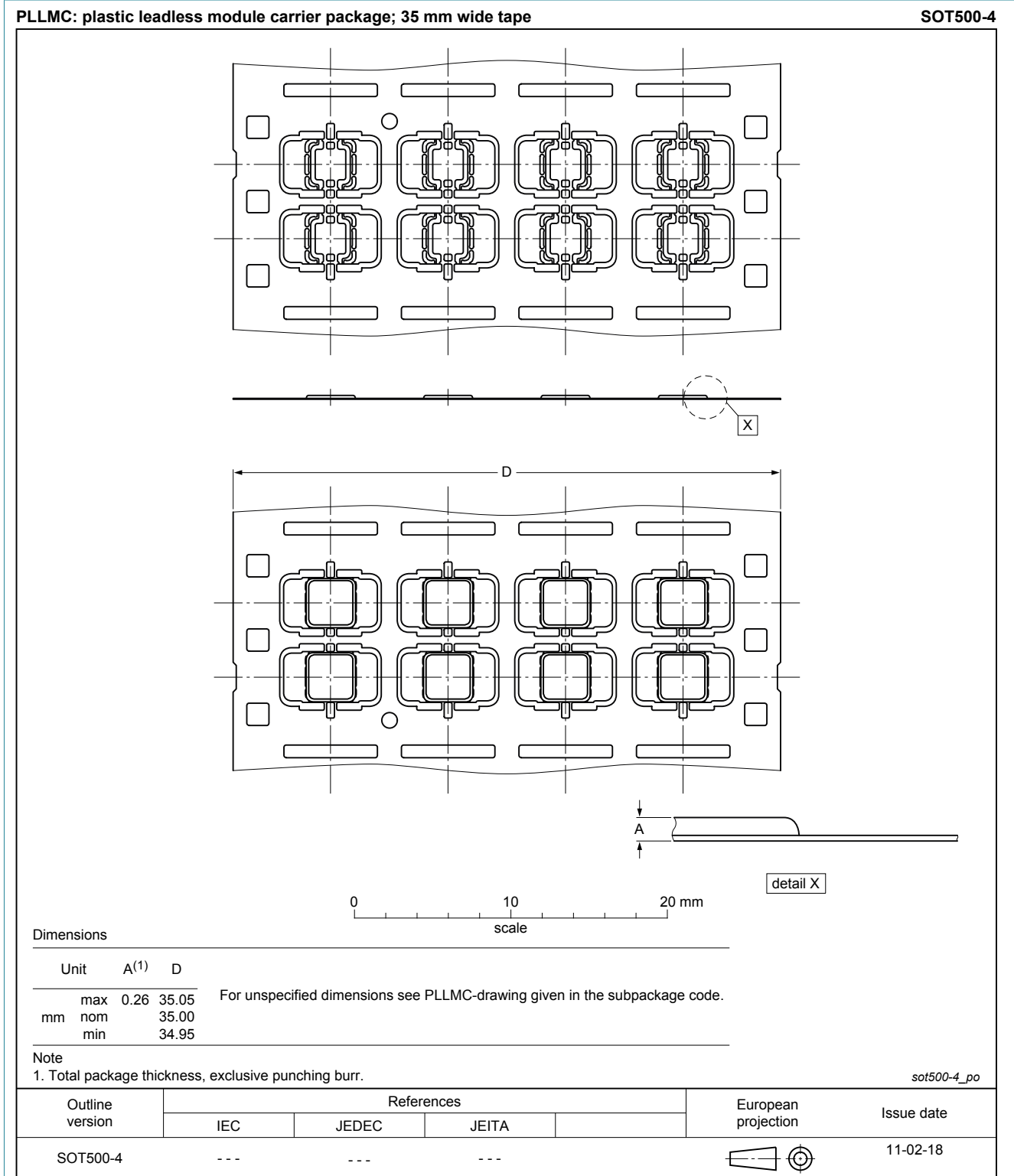
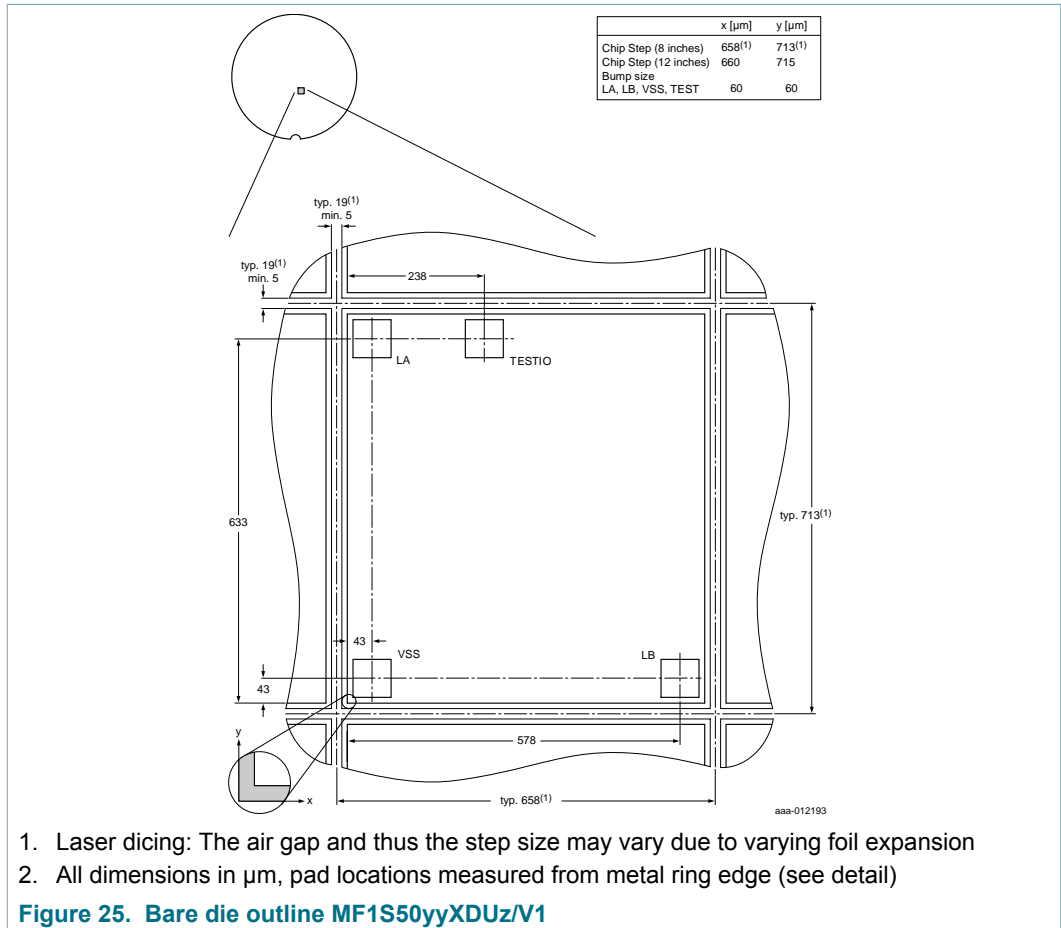


Figure 24. Package outline SOT500-4

## 16 Bare die outline

For more details on the wafer delivery forms, see [Ref. 9](#).



## 17 Abbreviations

Table 33. Abbreviations and symbols

| Acronym | Description  |
|---------|--|
| ACK     | ACKnowledge  |
| ATQA    | Answer To reQuest, Type A                                    |
| CRC     | Cyclic Redundancy Check                                      |
| CT      | Cascade Tag (value 88h) as defined in ISO/IEC 14443-3 Type A |
| EEPROM  | Electrically Erasable Programmable Read-Only Memory          |
| FDT     | Frame Delay Time   |
| FFC     | Film Frame Carrier   |
| IC      | Integrated Circuit   |
| LCR     | L = inductance, Capacitance, Resistance (LCR meter)          |
| LSB     | Least Significant Bit  |



| Acronym | Description  |
|---------|--|
| NAK     | Not AcKnowledge                                      |
| NUID    | Non-Unique IDentifier                                |
| NV      | Non-Volatile memory                                  |
| PCD     | Proximity Coupling Device (Contactless Reader)       |
| PICC    | Proximity Integrated Circuit Card (Contactless Card) |
| REQA    | REQuest command, Type A                              |
| RID     | Random ID  |
| RF      | Radio Frequency                                      |
| RMS     | Root Mean Square                                     |
| RNG     | Random Number Generator                              |
| SAK     | Select AcKnowledge, type A                           |
| SECS-II | SEMI Equipment Communications Standard part 2        |
| TiW     | Titanium Tungsten                                    |
| UID     | Unique IDentifier                                    |
| WUPA    | Wake-Up Protocol type A                              |

## 18 References

[1]

### MIFARE (Card) Coil Design Guide

Application note, BU-ID Document number 0117\*\*<sup>1</sup>

[2]

### MIFARE Type Identification Procedure

Application note, BU-ID Document number 0184\*\*<sup>1</sup>

[3]

### ISO/IEC 14443-2

2001

[4]

### ISO/IEC 14443-3

2001

[5]

### MIFARE & I-CODE CL RC632 Multiple protocol contactless reader IC

Product data sheet

[6]

### MIFARE product and handling of UIDs

<sup>1</sup> \*\* ... document version number

Application note, BU-ID Document number 1907\*\*<sup>1</sup>

[7]

**Contactless smart card module specification MOA4**

Delivery Type Description, BU-ID Document number 0823\*\*<sup>1</sup>

[8]

**Contactless smart card module specification MOA8**

Delivery Type Description, BU-ID Document number 1636\*\*<sup>1</sup>

[9]

**General specification for 8" wafer on UV-tape; delivery types**

Delivery Type Description, BU-ID Document number 1005\*\*<sup>1</sup>

## 19 Revision history

Table 34. Revision history

| Document ID        | Release date   | Data sheet status  | Change notice | Supersedes         |
|--------------------|--|--------------------|---------------|--------------------|
| MF1S50yyX/V1 v.3.2 | 20180523   | Product data sheet | -             | MF1S50yyX/V1 v.3.1 |
| Modifications:     | <ul style="list-style-type: none"> <li>• Editorial updates.</li> </ul>   |                    |               |                    |
| MF1S50yyX/V1 v.3.1 | 20171121   | Product data sheet | -             | MF1S50yyX/V1 v.3.0 |
| Modifications:     | <ul style="list-style-type: none"> <li>• 12 inch FFC delivery forms added</li> <li>• Format updated</li> </ul> |                    |               |                    |
| MF1S50yyX/V1 v.3.0 | 20140303   | Product data sheet | -             | -                  |

## 20 Legal information

### 20.1 Data sheet status

| Document status <sup>[1][2]</sup> | Product status <sup>[3]</sup> | Definition  |
|-----------------------------------|-------------------------------|---|
| Objective [short] data sheet      | Development                   | This document contains data from the objective specification for product development. |
| Preliminary [short] data sheet    | Qualification                 | This document contains data from the preliminary specification.                       |
| Product [short] data sheet        | Production                    | This document contains the product specification.                                     |

[1] Please consult the most recently issued document before initiating or completing a design.

[2] The term 'short data sheet' is explained in section "Definitions".

[3] The product status of device(s) described in this document may have changed since this document was published and may differ in case of multiple devices. The latest product status information is available on the Internet at URL <http://www.nxp.com>.

### 20.2 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.

**Short data sheet** — A short data sheet is an extract from a full data sheet with the same product type number(s) and title. A short data sheet is intended for quick reference only and should not be relied upon to contain detailed and full information. For detailed and full information see the relevant full data sheet, which is available on request via the local NXP Semiconductors sales office. In case of any inconsistency or conflict with the short data sheet, the full data sheet shall prevail.

**Product specification** — The information and data provided in a Product data sheet shall define the specification of the product as agreed between NXP Semiconductors and its customer, unless NXP Semiconductors and customer have explicitly agreed otherwise in writing. In no event however, shall an agreement be valid in which the NXP Semiconductors product is deemed to offer functions and qualities beyond those described in the Product data sheet.

### 20.3 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. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors. 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 and its suppliers accept 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.

**Limiting values** — Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) will cause permanent damage to the device. Limiting values are stress ratings only and (proper) operation of the device at these or any other conditions above those given in the Recommended operating conditions section (if present) or the Characteristics sections of this document is not warranted. Constant or repeated exposure to limiting values will permanently and irreversibly affect the quality and reliability of the device.

**Terms and conditions of commercial sale** — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at <http://www.nxp.com/profile/terms>, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

**No offer to sell or license** — Nothing in this document may be interpreted or construed as an offer to sell products that is open for acceptance or the grant, conveyance or implication of any license under any copyrights, patents or other industrial or intellectual property rights.

---

**MIFARE Classic EV1 1K - Mainstream contactless smart card IC for fast and easy solution development**

**Quick reference data** — The Quick reference data is an extract of the product data given in the Limiting values and Characteristics sections of this document, and as such is not complete, exhaustive or legally binding.

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

**Non-automotive qualified products** — Unless this data sheet expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications. In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP

Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

**Translations** — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

## 20.4 Trademarks

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

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

**MIFARE Classic** — is a trademark of NXP B.V.

Tables

|          |   |    |          |   |    |
|----------|---|----|----------|---|----|
| Tab. 1.  | Quick reference data .....                                  | 2  | Tab. 18. | SET_MOD_TYPE timing .....                             | 19 |
| Tab. 2.  | Ordering information .....                                  | 3  | Tab. 19. | Load Modulation Status Indication .....               | 19 |
| Tab. 3.  | Pin allocation table .....                                  | 4  | Tab. 20. | MIFARE Classic authentication command .....           | 20 |
| Tab. 4.  | Value block format example .....                            | 10 | Tab. 21. | MIFARE Classic authentication timing .....            | 21 |
| Tab. 5.  | Memory operations .....                                     | 10 | Tab. 22. | MIFARE Read command .....                             | 21 |
| Tab. 6.  | Access conditions .....                                     | 11 | Tab. 23. | MIFARE Read timing .....                              | 21 |
| Tab. 7.  | Access conditions for the sector trailer .....              | 12 | Tab. 24. | MIFARE Write command .....                            | 22 |
| Tab. 8.  | Access conditions for data blocks .....                     | 12 | Tab. 25. | MIFARE Write timing .....                             | 23 |
| Tab. 9.  | Command overview .....                                      | 13 | Tab. 26. | MIFARE Increment, Decrement and Restore command ..... | 24 |
| Tab. 10. | MIFARE ACK and NAK .....                                    | 15 | Tab. 27. | MIFARE Increment, Decrement and Restore timing .....  | 24 |
| Tab. 11. | ATQA response of the MF1S50yyX/V1 .....                     | 15 | Tab. 28. | MIFARE Transfer command .....                         | 25 |
| Tab. 12. | SAK response of the MF1S50yyX/V1 .....                      | 15 | Tab. 29. | MIFARE Transfer timing .....                          | 25 |
| Tab. 13. | Personalize UID Usage command .....                         | 17 | Tab. 30. | Limiting values .....                                 | 25 |
| Tab. 14. | Personalize UID Usage timing .....                          | 17 | Tab. 31. | Characteristics .....                                 | 26 |
| Tab. 15. | Available activation sequences for 7-byte UID options ..... | 18 | Tab. 32. | Wafer specifications MF1S50yyXDUy .....               | 26 |
| Tab. 16. | Input parameter to MIFARE Classic Authenticate .....        | 18 | Tab. 33. | Abbreviations and symbols .....                       | 30 |
| Tab. 17. | SET_MOD_TYPE command .....                                  | 19 | Tab. 34. | Revision history .....                                | 32 |

Figures

|          |   |    |          |   |    |
|----------|---|----|----------|---|----|
| Fig. 1.  | Contactless MIFARE product-based system .....               | 1  | Fig. 14. | Byte Location of Load Modulation Status in Block 0 / Sector 0 ..... | 19 |
| Fig. 2.  | Block diagram of MF1S50yyX/V1 .....                         | 3  | Fig. 15. | MIFARE Authentication part 1 .....                                  | 20 |
| Fig. 3.  | Pin configuration for SOT500-2 (MOA4) .....                 | 4  | Fig. 16. | MIFARE Authentication part 2 .....                                  | 20 |
| Fig. 4.  | MIFARE Classic command flow diagram .....                   | 6  | Fig. 17. | MIFARE Read .....   | 21 |
| Fig. 5.  | Memory organization .....                                   | 8  | Fig. 18. | MIFARE Write part 1 .....   | 22 |
| Fig. 6.  | Manufacturer block for MF1S503yX with 4-byte NUID .....     | 8  | Fig. 19. | MIFARE Write part 2 .....   | 22 |
| Fig. 7.  | Manufacturer block for MF1S500yX with 7-byte UID .....      | 9  | Fig. 20. | MIFARE Increment, Decrement, Restore part 1 .....                   | 23 |
| Fig. 8.  | Value blocks .....  | 9  | Fig. 21. | MIFARE Increment, Decrement, Restore part 2 .....                   | 24 |
| Fig. 9.  | Sector trailer .....  | 10 | Fig. 22. | MIFARE Transfer .....   | 25 |
| Fig. 10. | Access conditions .....                                     | 11 | Fig. 23. | Package outline SOT500-2 .....                                      | 28 |
| Fig. 11. | Frame Delay Time (from PCD to PICC) and TACK and TNAK ..... | 14 | Fig. 24. | Package outline SOT500-4 .....                                      | 29 |
| Fig. 12. | Personalize UID Usage .....                                 | 17 | Fig. 25. | Bare die outline MF1S50yyXDUz/V1 .....                              | 30 |
| Fig. 13. | SET_MOD_TYPE .....  | 19 |          |   |    |

## Contents

|           |  |           |           |                                  |           |
|-----------|--|-----------|-----------|----------------------------------|-----------|
| <b>1</b>  | <b>General description</b> .....               | <b>1</b>  | <b>13</b> | <b>Limiting values</b> .....     | <b>25</b> |
| 1.1       | Anticollision .....                            | 1         | <b>14</b> | <b>Characteristics</b> .....     | <b>26</b> |
| 1.2       | Simple integration and user convenience .....  | 1         | <b>15</b> | <b>Wafer specification</b> ..... | <b>26</b> |
| 1.3       | Security and privacy .....                     | 1         | 15.1      | Fail die identification .....    | 27        |
| 1.4       | Delivery options .....                         | 1         | 15.2      | Package outline .....            | 27        |
| <b>2</b>  | <b>Features and benefits</b> .....             | <b>2</b>  | <b>16</b> | <b>Bare die outline</b> .....    | <b>30</b> |
| 2.1       | EEPROM .....                                   | 2         | <b>17</b> | <b>Abbreviations</b> .....       | <b>30</b> |
| <b>3</b>  | <b>Applications</b> .....                      | <b>2</b>  | <b>18</b> | <b>References</b> .....          | <b>31</b> |
| <b>4</b>  | <b>Quick reference data</b> .....              | <b>2</b>  | <b>19</b> | <b>Revision history</b> .....    | <b>32</b> |
| <b>5</b>  | <b>Ordering information</b> .....              | <b>3</b>  | <b>20</b> | <b>Legal information</b> .....   | <b>33</b> |
| <b>6</b>  | <b>Block diagram</b> .....                     | <b>3</b>  |           |                                  |           |
| <b>7</b>  | <b>Pinning information</b> .....               | <b>4</b>  |           |                                  |           |
| 7.1       | Pinning .....                                  | 4         |           |                                  |           |
| <b>8</b>  | <b>Functional description</b> .....            | <b>4</b>  |           |                                  |           |
| 8.1       | Block description .....                        | 4         |           |                                  |           |
| 8.2       | Communication principle .....                  | 5         |           |                                  |           |
| 8.2.1     | Request standard / all .....                   | 5         |           |                                  |           |
| 8.2.2     | Anticollision loop .....                       | 5         |           |                                  |           |
| 8.2.3     | Select card .....                              | 5         |           |                                  |           |
| 8.2.4     | Three pass authentication .....                | 5         |           |                                  |           |
| 8.2.5     | Memory operations .....                        | 6         |           |                                  |           |
| 8.3       | Data integrity .....                           | 6         |           |                                  |           |
| 8.4       | Three pass authentication sequence .....       | 7         |           |                                  |           |
| 8.5       | RF interface .....                             | 7         |           |                                  |           |
| 8.6       | Memory organization .....                      | 7         |           |                                  |           |
| 8.6.1     | Manufacturer block .....                       | 8         |           |                                  |           |
| 8.6.2     | Data blocks .....                              | 9         |           |                                  |           |
| 8.6.2.1   | Value blocks .....                             | 9         |           |                                  |           |
| 8.6.3     | Sector trailer .....                           | 10        |           |                                  |           |
| 8.7       | Memory access .....                            | 10        |           |                                  |           |
| 8.7.1     | Access conditions .....                        | 11        |           |                                  |           |
| 8.7.2     | Access conditions for the sector trailer ..... | 12        |           |                                  |           |
| 8.7.3     | Access conditions for data blocks .....        | 12        |           |                                  |           |
| <b>9</b>  | <b>Command overview</b> .....                  | <b>13</b> |           |                                  |           |
| 9.1       | MIFARE Classic command overview .....          | 13        |           |                                  |           |
| 9.2       | Timings .....                                  | 14        |           |                                  |           |
| 9.3       | MIFARE Classic ACK and NAK .....               | 15        |           |                                  |           |
| 9.4       | ATQA and SAK responses .....                   | 15        |           |                                  |           |
| <b>10</b> | <b>UID Options and Handling</b> .....          | <b>16</b> |           |                                  |           |
| 10.1      | 7-byte UID Operation .....                     | 16        |           |                                  |           |
| 10.1.1    | Personalization Options .....                  | 16        |           |                                  |           |
| 10.1.2    | Anti-collision and Selection .....             | 17        |           |                                  |           |
| 10.1.3    | Authentication .....                           | 18        |           |                                  |           |
| 10.2      | 4-byte UID Operation .....                     | 18        |           |                                  |           |
| 10.2.1    | Anti-collision and Selection .....             | 18        |           |                                  |           |
| 10.2.2    | Authentication .....                           | 18        |           |                                  |           |
| <b>11</b> | <b>Load Modulation Strength Option</b> .....   | <b>18</b> |           |                                  |           |
| <b>12</b> | <b>MIFARE Classic commands</b> .....           | <b>20</b> |           |                                  |           |
| 12.1      | MIFARE Classic Authentication .....            | 20        |           |                                  |           |
| 12.2      | MIFARE Read .....                              | 21        |           |                                  |           |
| 12.3      | MIFARE Write .....                             | 22        |           |                                  |           |
| 12.4      | MIFARE Increment, Decrement and Restore ...    | 23        |           |                                  |           |
| 12.5      | MIFARE Transfer .....                          | 25        |           |                                  |           |

Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.

© NXP B.V. 2018.

All rights reserved.

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

For sales office addresses, please send an email to: [salesaddresses@nxp.com](mailto:salesaddresses@nxp.com)

Date of release: 23 May 2018

Document identifier: MF1S50yyX\_V1

Document number: 279232

# MF3ICDx21\_41\_81

## MIFARE DESFire EV1 contactless multi-application IC

Rev. 3.2 — 9 December 2015  
145632

Product short data sheet  
COMPANY PUBLIC

### 1. General description

---

MIFARE DESFire EV1 (MF3ICD(H) 21/41/81), a Common Criteria (EAL4+) certified product, is ideal for service providers wanting to use secure multi-application smart cards in public transport schemes, access management or closed-loop e-payment applications. It fully complies with the requirements for fast and highly secure data transmission, flexible memory organization and interoperability with existing infrastructure.

MIFARE DESFire EV1 is based on open global standards for both air interface and cryptographic methods. It is compliant to all 4 levels of ISO/IEC 14443A and uses optional ISO/IEC 7816-4 commands.

Featuring an on-chip backup management system and the mutual three-pass authentication, a MIFARE DESFire EV1 card can hold up to 28 different applications and 32 files per application. The size of each file is defined at the moment of its creation, making MIFARE DESFire EV1 a truly flexible and convenient product.

Additionally, an automatic anti-tear mechanism is available for all file types, which guarantees transaction-oriented data integrity. With MIFARE DESFire EV1, data transfer rates up to 848 kbit/s can be achieved, allowing fast data transmission.

The main characteristics of this device are denoted by its name “DESFire”: DES indicates the high level of security using a 3DES or AES hardware cryptographic engine for enciphering transmission data and Fire indicates its outstanding position as a fast, innovative, reliable and secure IC in the contactless proximity transaction market. Hence, MIFARE DESFire EV1 brings many benefits to end users. Cardholders can experience convenient contactless ticketing while also having the possibility to use the same device for related applications such as payment at vending machines, access control or event ticketing. In other words, the MIFARE DESFire EV1 silicon solution offers enhanced consumer-friendly system design, in combination with security and reliability.

MIFARE DESFire EV1 delivers the perfect balance of speed, performance and cost efficiency. Its open concept allows future seamless integration of other ticketing media such as smart paper tickets, key fobs, and mobile ticketing based on Near Field Communication (NFC) technology. It is also fully compatible with the existing MIFARE reader hardware platform. MIFARE DESFire EV1 is your ticket to contactless systems worldwide.



## 2. Features and benefits

### 2.1 RF interface: ISO/IEC 14443 Type A

- Contactless transmission of data and powered by the RF-field (no battery needed)
- Operating distance: up to 100 mm (depending on power provided by the PCD and antenna geometry)
- Operating frequency: 13.56 MHz
- Fast data transfer: 106 kbit/s, 212 kbit/s, 424 kbit/s, 848 kbit/s
- High data integrity: 16/32 bit CRC, parity, bit coding, bit counting
- True deterministic anticollision
- 7 bytes unique identifier (cascade level 2 according to ISO/IEC 14443-3 and option for random ID)
- Uses ISO/IEC 14443-4 protocol

### 2.2 ISO/IEC 7816 compatibility

- Supports ISO/IEC 7816-3 APDU message structure
- Supports ISO/IEC 7816-4 INS code 'A4' for SELECT FILE
- Supports ISO/IEC 7816-4 INS code 'B0' for READ BINARY
- Supports ISO/IEC 7816-4 INS code 'D6' for UPDATE BINARY
- Supports ISO/IEC 7816-4 INS code 'B2' for READ RECORDS
- Supports ISO/IEC 7816-4 INS code 'E2' for APPEND RECORD
- Supports ISO/IEC 7816-4 INS code '84' for GET CHALLENGE
- Supports ISO/IEC 7816-4 INS code '88' for INTERNAL AUTHENTICATE
- Supports ISO/IEC 7816-4 INS code '82' for EXTERNAL AUTHENTICATE

### 2.3 Non-volatile memory

- 2 kB or 4 kB or 8 kB NV-Memory
- Data retention of 10 years
- Write endurance typical 500 000 cycles

### 2.4 NV-memory organization

- Flexible file system
- Up to 28 applications simultaneously on one PICC
- Up to 32 files in each application (standard data file, back-up data file, value file, linear record file and cyclic record file)
- File size is determined during creation

### 2.5 Security

- Common Criteria Certification: EAL4+ (Hardware and Software)
- Unique 7 bytes serial number for each device
- Optional "RANDOM" ID for enhance security and privacy
- Mutual three-pass authentication
- Mutual authentication according to ISO/IEC 7816-4



- 1 card master key and up to 14 keys per application
- Hardware DES using 56/112/168 bit keys featuring key version, data authenticity by 8 byte CMAC
- Hardware AES using 128-bit keys featuring key version, data authenticity by 8 byte CMAC
- Data encryption on RF-channel
- Authentication on application level
- Hardware exception sensors
- Self-securing file system
- Backward compatibility to MF3ICD40: 4 byte MAC, CRC 16

## 2.6 Special features

- Transaction-oriented automatic anti-tear mechanism
- Configurable ATS information for card personalization
- Backward compatibility mode to MF3ICD40
- Optional high input capacitance (70 pF) for small form factor design (MF3ICDH 21/41/81)

## 3. Applications

---

- Advanced public transportation schema
- Highly secure access management
- Closed-loop e-payment scheme
- Event ticketing
- eGovernment applications

## 4. Quick reference data

Table 1. Quick reference data [1][2]

| Symbol                        | Parameter                             | Conditions  | Min       | Typ    | Max   | Unit  |
|-------------------------------|---------------------------------------|---|-----------|--------|-------|-------|
| $f_i$                         | input frequency                       |   | -         | 13.56  | -     | MHz   |
| $C_i$                         | input capacitance for MF3ICD21/41/81  | $T_{amb} = 22\text{ °C}$ ; $f_i = 13.56\text{ MHz}$ ; 2.8 V RMS | [3] 14.96 | 17.0   | 19.04 | pF    |
|                               | input capacitance for MF3ICDH21/41/81 |   | 64        | 69     | 74    | pF    |
| <b>EEPROM characteristics</b> |                                       |   |           |        |       |       |
| $t_{ret}$                     | retention time                        | $T_{amb} = 22\text{ °C}$  | 10        | -      | -     | year  |
| $N_{endu(W)}$                 | write endurance                       | $T_{amb} = 22\text{ °C}$  | 200000    | 500000 | -     | cycle |
| $t_{cy(W)}$                   | write cycle time                      | $T_{amb} = 22\text{ °C}$  | -         | 2.9    | -     | ms    |

[1] Stresses above one or more of the values may cause permanent damage to the device.

[2] Exposure to limiting values for extended periods may affect device reliability.

[3] Measured with LCR meter.

## 5. Ordering information

Table 2. Ordering information

| Type number       | Package  |   | Version  |
|-------------------|----------|---|----------|
|                   | Name     | Description   |          |
| MF3ICD8101DUD/05  | FFC      | 8 inch wafer (sawn; 120 $\mu\text{m}$ thickness, on film frame carrier; electronic fail die marking according to SECSII format); see <a href="#">Ref. 4</a> , 8K EEPROM, 17pF input capacitance | -        |
| MF3ICD4101DUD/05  | FFC      | 8 inch wafer (sawn; 120 $\mu\text{m}$ thickness, on film frame carrier; electronic fail die marking according to SECSII format); see <a href="#">Ref. 4</a> , 4K EEPROM, 17pF input capacitance | -        |
| MF3ICD2101DUD/05  | FFC      | 8 inch wafer (sawn; 120 $\mu\text{m}$ thickness, on film frame carrier; electronic fail die marking according to SECSII format); see <a href="#">Ref. 4</a> , 2K EEPROM, 17pF input capacitance | -        |
| MF3ICDH8101DUD/05 | FFC      | 8 inch wafer (sawn; 120 $\mu\text{m}$ thickness, on film frame carrier; electronic fail die marking according to SECSII format); see <a href="#">Ref. 5</a> , 8K EEPROM, 70pF input capacitance | -        |
| MF3ICDH4101DUD/05 | FFC      | 8 inch wafer (sawn; 120 $\mu\text{m}$ thickness, on film frame carrier; electronic fail die marking according to SECSII format); see <a href="#">Ref. 5</a> , 4K EEPROM, 70pF input capacitance | -        |
| MF3ICDH2101DUD/05 | FFC      | 8 inch wafer (sawn; 120 $\mu\text{m}$ thickness, on film frame carrier; electronic fail die marking according to SECSII format); see <a href="#">Ref. 5</a> , 2K EEPROM, 70pF input capacitance | -        |
| MF3MOD8101DA4/05  | PLLMC[1] | plastic leadless module carrier package; 35 mm wide tape; see <a href="#">Ref. 6</a> , 8K EEPROM, 17pF input capacitance  | SOT500-2 |
| MF3MOD4101DA4/05  | PLLMC[1] | plastic leadless module carrier package; 35 mm wide tape; see <a href="#">Ref. 6</a> , 4K EEPROM, 17pF input capacitance  | SOT500-2 |
| MF3MOD2101DA4/05  | PLLMC[1] | plastic leadless module carrier package; 35 mm wide tape; see <a href="#">Ref. 6</a> , 2K EEPROM, 17pF input capacitance  | SOT500-2 |
| MF3MODH8101DA4/05 | PLLMC[1] | plastic leadless module carrier package; 35 mm wide tape; see <a href="#">Ref. 6</a> , 8K EEPROM, 70pF input capacitance  | SOT500-2 |

Table 2. Ordering information *?continued*

| Type number       | Package              |  | Version  |
|-------------------|----------------------|--|----------|
|                   | Name                 | Description  |          |
| MF3MODH4101DA4/05 | PLLMC <sup>[1]</sup> | plastic leadless module carrier package; 35 mm wide tape; see <a href="#">Ref. 6</a> , 4K EEPROM, 70pF input capacitance | SOT500-2 |
| MF3MODH2101DA4/05 | PLLMC <sup>[1]</sup> | plastic leadless module carrier package; 35 mm wide tape; see <a href="#">Ref. 6</a> , 2K EEPROM, 70pF input capacitance | SOT500-2 |
| MF3MOD8101DA8/05  | PLLMC <sup>[2]</sup> | plastic leadless module carrier package; 35 mm wide tape; see <a href="#">Ref. 6</a> , 8K EEPROM, 17pF input capacitance | SOT500-4 |
| MF3MOD4101DA8/05  | PLLMC <sup>[2]</sup> | plastic leadless module carrier package; 35 mm wide tape; see <a href="#">Ref. 6</a> , 4K EEPROM, 17pF input capacitance | SOT500-4 |
| MF3MOD2101DA8/05  | PLLMC <sup>[2]</sup> | plastic leadless module carrier package; 35 mm wide tape; see <a href="#">Ref. 6</a> , 2K EEPROM, 17pF input capacitance | SOT500-4 |
| MF3MODH8101DA8/05 | PLLMC <sup>[2]</sup> | plastic leadless module carrier package; 35 mm wide tape; see <a href="#">Ref. 6</a> , 8K EEPROM, 70pF input capacitance | SOT500-4 |
| MF3MODH4101DA8/05 | PLLMC <sup>[2]</sup> | plastic leadless module carrier package; 35 mm wide tape; see <a href="#">Ref. 6</a> , 4K EEPROM, 70pF input capacitance | SOT500-4 |
| MF3MODH2101DA8/05 | PLLMC <sup>[2]</sup> | plastic leadless module carrier package; 35 mm wide tape; see <a href="#">Ref. 6</a> , 2K EEPROM, 70pF input capacitance | SOT500-4 |

- [1] This package is also known as MOA4.
- [2] This package is also known as MOA8

## 6. Block diagram

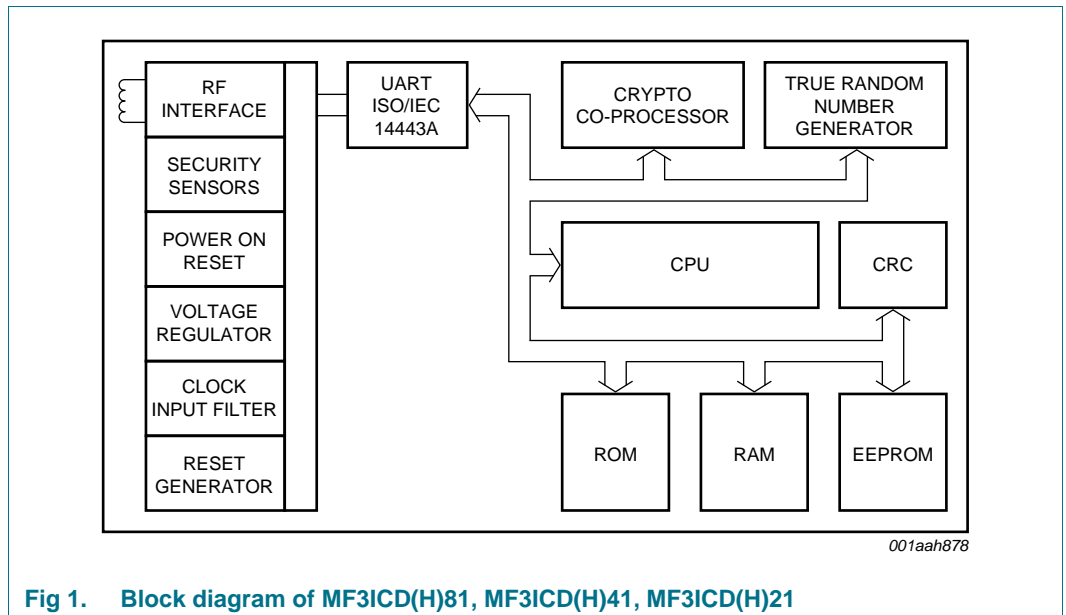


Fig 1. Block diagram of MF3ICD(H)81, MF3ICD(H)41, MF3ICD(H)21

## 7. Limiting values

**Table 3. Limiting values** [\[1\]](#)[\[2\]](#)

*In accordance with the Absolute Maximum Rating System (IEC 60134).*

| Symbol         | Parameter                           | Conditions | Min                   | Max | Unit |
|----------------|-------------------------------------|------------|-----------------------|-----|------|
| $I_I$          | input current                       |            | -                     | 30  | mA   |
| $P_{tot}/pack$ | total power dissipation per package |            | -                     | 200 | mW   |
| $T_{stg}$      | storage temperature                 |            | -55                   | 125 | °C   |
| $T_{amb}$      | ambient temperature                 |            | -25                   | 70  | °C   |
| $V_{ESD}$      | electrostatic discharge voltage     |            | <a href="#">[3]</a> 2 | -   | kV   |
| $I_{lu}$       | latch-up current                    |            | ±100                  | -   | mA   |

[1] Stresses above one or more of the limiting values may cause permanent damage to the device.

[2] Exposure to limiting values for extended periods may affect device reliability.

[3] MIL Standard 883-C method 3015; human body model: C = 100 pF, R = 1.5 kΩ.

## 8. Functional description

### 8.1 Contactless energy and data transfer

In the MIFARE system, the MIFARE DESFire EV1 is connected to a coil consisting of a few turns embedded in a standard ISO/IEC smart card (see [Ref. 8](#)). A battery is not needed. When the card is positioned in the proximity of the PCD antenna, the high-speed RF communication interface allows data to be transmitted up to 848 kbit/s.

### 8.2 Anti-collision

An intelligent anti-collision mechanism allows more than one MIFARE DESFire EV1 in the field to be handled simultaneously. The anti-collision algorithm selects each MIFARE DESFire EV1 individually and ensures that the execution of a transaction with a selected MIFARE DESFire EV1 is performed correctly without data corruption resulting from other MIFARE DESFire EV1s in the field.

### 8.3 UID/serial number

The unique 7 byte (UID) is programmed into a locked part of the NV memory which is reserved for the manufacturer. Due to security and system requirements these bytes are write-protected after being programmed by the IC manufacturer at production time. According to ISO/IEC 14443-3 (see [Ref. 12](#)) during the first anti-collision loop the cascade tag returns a value of 88h and also the first 3 bytes of the UID, UID0 to UID2 and BCC. The second anti-collision loop returns bytes UID3 to UID6 and BCC.

UID0 holds the manufacturer ID for NXP (04h) according to ISO/IEC 14443-3 and ISO/IEC 7816-6 AMD 1.

MIFARE DESFire EV1 also allows Random ID to be used. In this case MIFARE DESFire EV1 only uses a single anti-collision loop. The 3 byte random number is generated after RF reset of the MIFARE DESFire EV1.

### 8.4 Memory organization

The 2/4/8 KB NV memory is organized using a flexible file system. This file system allows a maximum of 28 different applications on one MIFARE DESFire EV1. Each application provides up to 32 files. Every application is represented by its 3 bytes Application Identifier (AID).

Five different file types are supported; see [Section 8.5](#).

A guideline to assign MIFARE DESFire AIDs can be found in the application note *MIFARE Application Directory (MAD)*; see [Ref. 9](#).

Each file can be created either at MIFARE DESFire EV1 initialization (card production/card printing), at MIFARE DESFire EV1 personalization (vending machine) or in the field.

If a file or application becomes obsolete in operation, it can be permanently invalidated.

Commands which have impact on the file structure itself (e.g. creation or deletion of applications, change of keys) activate an automatic rollback mechanism, which protects the file structure from being corrupted.

If this rollback is necessary, it is done without user interaction before carrying out further commands. To ensure data integrity on application level, a transaction-oriented backup is implemented for all file types with backup. It is possible to mix file types with and without backup within one application.

As the commands are the same for MF3ICD(H)81, MF3ICD(H)41 and MF3ICD(H)21, the command details are available in [Ref. 1](#). Only the memory size and input capacitance are different between the devices.

## 8.5 Available file types

The files within an application can be any of the following types:

- Standard data files
- Backup data files
- Value files with backup
- Linear record files with backup
- Cyclic record files with backup

## 8.6 Security

The 7 byte UID is fixed, programmed into each device during production. It cannot be altered and ensures the uniqueness of each device.

The UID may be used to derive diversified keys for each ticket. Diversified MIFARE DESFire EV1 keys contribute to gain an effective anti-cloning mechanism and increase the security of the original key; see [Ref. 7](#).

Prior to data transmission a mutual three-pass authentication can be done between MIFARE DESFire EV1 and PCD depending on the configuration employing either 56-bit DES (single DES, DES), 112-bit 3DES (triple DES, 2K3DES), 168-bit 3DES (3 key triple DES, 3K3DES) or AES. During the authentication the level of security of all further commands during the session is set. In addition, the communication settings of the file/application result in the following options of secure communication between MIFARE DESFire EV1 and PCD:

- Plain data transfer (only possible within the backwards-compatible mode to MF3ICD40)
- Plain data transfer with cryptographic checksum (MAC): Authentication with backwards-compatible mode to MF3ICD40: 4 byte MAC, all other authentications based on DES/3DES/AES: 8 byte CMAC
- Encrypted data transfer (secured by CRC before encryption): Authentication with backwards-compatible mode to MF3ICD40: A 16-bit CRC is calculated over the stream and attached. The resulting stream is encrypted using the chosen cryptographic method. All other authentications-based DES/3DES/AES: A 32-bit CRC is calculated over the stream and attached. The resulting stream is encrypted using the chosen cryptographic method.

Find more information on the security concept of the product in [Ref. 1](#). Be aware not all levels of security are recommended. The recommended secure handling of the product can be seen in [Ref. 2](#) and in [Ref. 11](#).

## 9. DESFire command set

A detailed description of all commands is provided in [Ref. 1](#).

### 9.1 ISO/IEC 14443-3

Table 4. ISO/IEC 14443-3

| Command                              | Description   |
|--------------------------------------|---|
| REQA                                 | REQA and ATQA are implemented fully according to ISO/IEC 14443-3  |
| WUPA                                 | WUPA is implemented fully according to ISO/IEC 14443-3  |
| ANTICOLLISION/SELECT Cascade Level 1 | ANTICOLLISION and SELECT commands are implemented fully according to ISO/IEC 14443-3; the response is part 1 of the UID |
| ANTICOLLISION/SELECT Cascade Level 2 | ANTICOLLISION and SELECT commands are implemented fully according to ISO/IEC 14443-3; the response is part 2 of the UID |
| HALT                                 | brings MIFARE DESFire EV1 to the HALT state   |

### 9.2 ISO/IEC 14443-4

Table 5. ISO/IEC 14443-4

| Command  | Description   |
|----------|---|
| RATS     | identifies the MIFARE DESFire EV1 type to the PCD   |
| PPS      | allows individual selection of the communication baud rate between PCD and MIFARE DESFire EV1; for DESFire it is possible to set different communication baud rates for each direction i.e. DESFire allows a non-symmetrical information interchange speed. |
| WTX      | if the MIFARE DESFire EV1 needs more time than the defined FWT to respond to a PCD command it requests a Waiting Time eXtension (WTX)   |
| DESELECT | allows MIFARE DESFire EV1 to be brought to the HALT state   |

### 9.3 MIFARE DESFire EV1 command set overview – security related commands

Table 6. Security related commands

| Command            | Description   |
|--------------------|---|
| Authenticate       | MIFARE DESFire EV1 and the reader device show in an encrypted way that they possess the same secret which especially means the same key; this not only confirms that both entities are permitted to perform operations on each other but also creates a session key which can be used to keep the further communication path secure; as the name “session key” implicitly indicates, each time a new authentication procedure is successfully completed a new key for further cryptographic operations is generated |
| Change KeySettings | changes the master key settings on MIFARE DESFire EV1 and application level   |
| Set Configuration  | configures the card and pre-personalizes the card with a key, defines if the UID or the random ID is sent back during communication setup and configures the ATS string   |
| Change Key         | changes any key stored on the MIFARE DESFire EV1  |
| Get Key Version    | reads out the current key version of any key stored on the MIFARE DESFire EV1   |

**Remark:** All command and data frames are exchanged between MIFARE DESFire EV1 and PCD by using block format as defined in ISO/IEC 14443-4.

### 9.4 MIFARE DESFire EV1 command set overview – MIFARE DESFire EV1 level commands

Table 7. Level commands

| Command              | Description   |
|----------------------|---|
| Create Application   | creates new applications on the MIFARE DESFire EV1  |
| Delete Application   | permanently deactivates applications on the MIFARE DESFire EV1  |
| Get Applications IDs | returns the Application IDentifiers of all applications on a MIFARE DESFire EV1   |
| Free Memory          | returns the free memory available on the card   |
| GetDFNames           | returns the DF names  |
| Get KeySettings      | gets information on the MIFARE DESFire EV1 and application master key settings; in addition it returns the maximum number of keys which are configured for the selected application |
| Select Application   | selects one specific application for further access   |
| FormatMF3ICD81       | releases the MF3ICD81 user memory   |
| Get Version          | returns manufacturing related data of the MIFARE DESFire EV1  |
| GetCardUID           | returns the UID   |

**Remark:** All command and data frames are exchanged between MIFARE DESFire EV1 and PCD by using block format as defined in ISO/IEC 14443-4.



### 9.5 MIFARE DESFire EV1 command set overview – application level commands

Table 8. Application level commands

| Command                 | Description   |
|-------------------------|---|
| Get FileIDs             | returns the File IDentifiers of all active files within the currently selected application  |
| Get FileSettings        | gets information on the properties of a specific file   |
| Change FileSettings     | changes the access parameters of an existing file   |
| Create StdDataFile      | creates files for the storage of plain unformatted user data within an existing application on the MIFARE DESFire EV1   |
| Create BackupDataFile   | creates files for the storage of plain unformatted user data within an existing application on the MIFARE DESFire EV1, additionally supporting the feature of an integrated backup mechanism  |
| Create ValueFile        | creates files for the storage and manipulation of 32-bit signed integer values within an existing application on the MIFARE DESFire EV1   |
| Create LinearRecordFile | creates files for multiple storage of similar structural data, for example, loyalty programs within an existing application on the MIFARE DESFire EV1; once the file is filled completely with data records, further writing to the file is not possible unless it is cleared   |
| Create CyclicRecordFile | creates files for multiple storage of similar structural data, for example, logging transactions within an existing application on the MIFARE DESFire EV1; once the file is filled completely with data records, the MIFARE DESFire EV1 automatically overwrites the oldest record with the latest written one (this wrap is fully transparent for the PCD) |
| DeleteFile              | permanently deactivates a file within the file directory of the currently selected application  |

**Remark:** All command and data frames are exchanged between MIFARE DESFire EV1 and PCD by using block format as defined in ISO/IEC 14443-4.

### 9.6 MIFARE DESFire EV1 command set overview – data manipulation commands

Table 9. Data manipulation commands

| Command        | Description  |
|----------------|--|
| Read Data      | reads data from Standard Data files or Backup Data files   |
| Write Data     | writes data to Standard Data files or Backup Data files  |
| Get Value      | reads the currently stored value from Value files  |
| Credit         | increases a value stored in a Value file   |
| Debit          | decreases a value stored in a Value file   |
| Limited Credit | allows a limited increase of a value stored in a Value file without having full Credit permissions to the file |
| Write Record   | writes data to a record in a Cyclic or Linear Record file  |
| Read Records   | reads out a set of complete records from a Cyclic or Linear Record file  |

**Table 9. Data manipulation commands** *?continued*

| Command            | Description   |
|--------------------|---|
| Clear RecordFile   | resets a Cyclic or Linear Record file to empty state  |
| Commit Transaction | validates all previous write accesses on Backup Data files, Value files and Record files within one application   |
| Abort Transaction  | invalidates all previous write accesses on Backup Data files, Value files and Record files within one application |

**Remark:** All command and data frames are exchanged between MIFARE DESFire EV1 and PCD by using block format as defined in ISO/IEC 14443-4.

## 9.7 MIFARE DESFire EV1 command set - ISO/IEC 7816 APDU commands

The MIFARE DESFire EV1 provides the following commands according to ISO/IEC 7816-4:

- INS code 'A4' SELECT
- INS code 'B0' READ BINARY
- INS code 'D6' UPDATE BINARY
- INS code 'B2' READ RECORDS
- INS code 'E2' APPEND RECORD
- INS code '84' GET CHALLENGE
- INS code '88' INTERNAL AUTHENTICATE
- INS code '82' EXTERNAL AUTHENTICATE

### 9.7.1 ISO/IEC 7816-4 APDU message structure

MIFARE DESFire EV1 supports the APDU message structure according to ISO/IEC 7816-4 for:

- an optional wrapping of the native MIFARE DESFire EV1 APDU format
- additionally implemented ISO/IEC 7816-4 commands

Find more information on the ISO/IEC 7816-4 commands in [Ref. 1](#).

## 10. Abbreviations

Table 10. Abbreviations

| Acronym | Description   |
|---------|---|
| AES     | Advanced Encryption Standard                        |
| AID     | Application Identifier                              |
| APDU    | Application Protocol Data Unit                      |
| ATS     | Answer to Select                                    |
| CC      | Common Criteria                                     |
| CMAC    | Cryptic Message Authentication Code                 |
| CRC     | Cyclic Redundancy Check                             |
| DES     | Digital Encryption Standard                         |
| DF      | Dedicated File                                      |
| EAL     | Evaluation Assurance Level                          |
| EEPROM  | Electrically Erasable Programmable Read-Only Memory |
| FWT     | Frame Waiting Time                                  |
| ID      | Identifier  |
| INS     | Instructions  |
| LCR     | inductance, Capacitance, Resistance                 |
| MAC     | Message Authentication Code                         |
| MAD     | MIFARE Application Directory                        |
| NV      | Non-Volatile Memory                                 |
| PCD     | Proximity Coupling Device                           |
| PPS     | Protocol Parameter Selection                        |
| RATS    | Request Answer To Select                            |
| REQA    | Request Answer                                      |
| RF      | Radio Frequency                                     |
| UID     | Unique Identifier                                   |
| WTX     | Waiting Time eXtension                              |
| WUPA    | Wake Up Protocol A                                  |

## 11. References

- [1] **Data sheet** — *MF3ICD81 MIFARE DESFire EV1*, document number: 13403\*\*1.
- [2] **Data sheet** — *MF3ICD81 Guidance, Delivery and Operation Manual*, document number: 1469\*\*.
- [3] **Data sheet** — *Specification addendum MF3ICD81*, document number: 1673\*\*.
- [4] **Data sheet** — *MF3ICD8101 Sawn bumped 120 μm wafer addendum*, document number: 1318\*\*.
- [5] **Data sheet** — *MF3ICDH8101 Sawn bumped 120 μm wafer addendum*, document number: 1970\*\*.
- [6] **Data sheet** — *MF3MODx21\_41\_81 Contactless chip card module*, document number: 1439\*\*.
- [7] **Application note** — *MIFARE DESFire - Implementation hints and examples*, document number: 0945\*\*.
- [8] **Application note** — *Card Coil Design Notes for MIFARE DESFire EV1*, document number: 1713\*\*.
- [9] **Application note** — *MIFARE Application Directory*, document number: 0018\*\*.
- [10] **Application note** — *MIFARE ISO/IEC 14443 PICC Selection*, document number: 1308\*\*.
- [11] **Application note** — *End to end system security risk considerations for implementing contactless cards*, document number: 1550\*\*.
- [12] **ISO/IEC Standard** — *ISO/IEC 14443 Identification cards - Contactless integrated circuit cards - Proximity cards*.

1. \*\* ... BU-ID document version number

## 12. Revision history

Table 11. Revision history

| Document ID              | Release date  | Data sheet status          | Change notice | Supersedes               |
|--------------------------|---|----------------------------|---------------|--------------------------|
| MF3ICDX21_41_81_SDS v3.2 | 20151209  | Product short data sheet   | -             | MF3ICDX21_41_81_SDS v3.1 |
| Modifications:           | <ul style="list-style-type: none"> <li>• <a href="#">Section 5</a>: MOA8 types added</li> </ul>   |                            |               |                          |
| MF3ICDX21_41_81_SDS v3.1 | 20101221  | Product short data sheet   | -             | MF3ICD21_41_81_SDS_2     |
| Modifications:           | <ul style="list-style-type: none"> <li>• Data sheet title updated</li> <li>• <a href="#">Section 1</a>, <a href="#">Section 2</a>, <a href="#">Section 3</a>, <a href="#">Section 11</a>, <a href="#">Section 13</a>: updated</li> <li>• <a href="#">Section 5</a>: type number MF3ICD801DUD/04 changed to MF3ICD8101DUD/05</li> </ul>  |                            |               |                          |
| MF3ICD21_41_81_SDS_2     | 20090306  | Product short data sheet   | -             | MF3ICD8101_SDS_N_1       |
| Modifications:           | <ul style="list-style-type: none"> <li>• Section 5 "Ordering information": type number MF3ICD8101DUD/01 changed to MF3ICD8101DUD/04</li> <li>• Section 5 "Ordering information": added root type numbers MF3ICD41 and MF3ICD21</li> <li>• Section 1 "General description", Section 2 "Features and benefits" and Section 3 "Applications": updated</li> <li>• Section 11 "References": added</li> </ul> |                            |               |                          |
| MF3ICD8101_SDS_N_1       | 20071213  | Objective short data sheet | -             | -                        |

## 13. Legal information

### 13.1 Data sheet status

| Document status <sup>[1][2]</sup> | Product status <sup>[3]</sup> | Definition  |
|-----------------------------------|-------------------------------|---|
| Objective [short] data sheet      | Development                   | This document contains data from the objective specification for product development. |
| Preliminary [short] data sheet    | Qualification                 | This document contains data from the preliminary specification.                       |
| Product [short] data sheet        | Production                    | This document contains the product specification.                                     |

[1] Please consult the most recently issued document before initiating or completing a design.

[2] The term 'short data sheet' is explained in section "Definitions".

[3] The product status of device(s) described in this document may have changed since this document was published and may differ in case of multiple devices. The latest product status information is available on the Internet at URL <http://www.nxp.com>.

### 13.2 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.

**Short data sheet** — A short data sheet is an extract from a full data sheet with the same product type number(s) and title. A short data sheet is intended for quick reference only and should not be relied upon to contain detailed and full information. For detailed and full information see the relevant full data sheet, which is available on request via the local NXP Semiconductors sales office. In case of any inconsistency or conflict with the short data sheet, the full data sheet shall prevail.

**Product specification** — The information and data provided in a Product data sheet shall define the specification of the product as agreed between NXP Semiconductors and its customer, unless NXP Semiconductors and customer have explicitly agreed otherwise in writing. In no event however, shall an agreement be valid in which the NXP Semiconductors product is deemed to offer functions and qualities beyond those described in the Product data sheet.

### 13.3 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. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

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 and its suppliers accept 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.

**Limiting values** — Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) will cause permanent damage to the device. Limiting values are stress ratings only and (proper) operation of the device at these or any other conditions above those given in the Recommended operating conditions section (if present) or the Characteristics sections of this document is not warranted. Constant or repeated exposure to limiting values will permanently and irreversibly affect the quality and reliability of the device.

**Terms and conditions of commercial sale** — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at <http://www.nxp.com/profile/terms>, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

**No offer to sell or license** — Nothing in this document may be interpreted or construed as an offer to sell products that is open for acceptance or the grant, conveyance or implication of any license under any copyrights, patents or other industrial or intellectual property rights.

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

**Quick reference data** — The Quick reference data is an extract of the product data given in the Limiting values and Characteristics sections of this document, and as such is not complete, exhaustive or legally binding.

**Non-automotive qualified products** — Unless this data sheet expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

**Translations** — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

## 13.4 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.

## 13.5 Trademarks

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

**MIFARE** — is a trademark of NXP Semiconductors N.V.

**DESFire** — is a trademark of NXP Semiconductors N.V.

## 14. Contact information

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

For sales office addresses, please send an email to: [salesaddresses@nxp.com](mailto:salesaddresses@nxp.com)

15. Tables

|  |    |   |    |
|--|----|---|----|
| Table 1. Quick reference data [1][2] . . . . . | 4  | Table 7. Level commands . . . . .             | 10 |
| Table 2. Ordering information . . . . .        | 4  | Table 8. Application level commands . . . . . | 11 |
| Table 3. Limiting values [1][2] . . . . .      | 6  | Table 9. Data manipulation commands . . . . . | 11 |
| Table 4. ISO/IEC 14443-3 . . . . .             | 9  | Table 10. Abbreviations . . . . .             | 13 |
| Table 5. ISO/IEC 14443-4 . . . . .             | 9  | Table 11. Revision history . . . . .          | 15 |
| Table 6. Security related commands . . . . .   | 10 |   |    |

16. Figures

Fig 1. Block diagram of MF3ICD(H)81, MF3ICD(H)41, MF3ICD(H)215

17. Contents

|          |  |          |           |  |           |
|----------|--|----------|-----------|--|-----------|
| <b>1</b> | <b>General description . . . . .</b>   | <b>1</b> | 9.6       | MIFARE DESFire EV1 command set overview – data manipulation commands . . . . . | 11        |
| <b>2</b> | <b>Features and benefits . . . . .</b>   | <b>2</b> | 9.7       | MIFARE DESFire EV1 command set - ISO/IEC 7816 APDU commands . . . . .          | 12        |
| 2.1      | RF interface: ISO/IEC 14443 Type A . . . . .   | 2        | 9.7.1     | ISO/IEC 7816-4 APDU message structure . . . . .                                | 12        |
| 2.2      | ISO/IEC 7816 compatibility . . . . .   | 2        | <b>10</b> | <b>Abbreviations . . . . .</b>   | <b>13</b> |
| 2.3      | Non-volatile memory. . . . .   | 2        | <b>11</b> | <b>References. . . . .</b>   | <b>14</b> |
| 2.4      | NV-memory organization . . . . .   | 2        | <b>12</b> | <b>Revision history . . . . .</b>  | <b>15</b> |
| 2.5      | Security. . . . .  | 2        | <b>13</b> | <b>Legal information . . . . .</b>   | <b>16</b> |
| 2.6      | Special features . . . . .   | 3        | 13.1      | Data sheet status . . . . .  | 16        |
| <b>3</b> | <b>Applications . . . . .</b>  | <b>3</b> | 13.2      | Definitions . . . . .  | 16        |
| <b>4</b> | <b>Quick reference data . . . . .</b>  | <b>4</b> | 13.3      | Disclaimers . . . . .  | 16        |
| <b>5</b> | <b>Ordering information. . . . .</b>   | <b>4</b> | 13.4      | Licenses. . . . .  | 17        |
| <b>6</b> | <b>Block diagram . . . . .</b>   | <b>5</b> | 13.5      | Trademarks . . . . .   | 17        |
| <b>7</b> | <b>Limiting values. . . . .</b>  | <b>6</b> | <b>14</b> | <b>Contact information . . . . .</b>   | <b>17</b> |
| <b>8</b> | <b>Functional description . . . . .</b>  | <b>7</b> | <b>15</b> | <b>Tables. . . . .</b>   | <b>18</b> |
| 8.1      | Contactless energy and data transfer. . . . .  | 7        | <b>16</b> | <b>Figures . . . . .</b>   | <b>18</b> |
| 8.2      | Anti-collision . . . . .   | 7        | <b>17</b> | <b>Contents. . . . .</b>   | <b>18</b> |
| 8.3      | UID/serial number. . . . .   | 7        |           |  |           |
| 8.4      | Memory organization . . . . .  | 7        |           |  |           |
| 8.5      | Available file types . . . . .   | 8        |           |  |           |
| 8.6      | Security. . . . .  | 8        |           |  |           |
| <b>9</b> | <b>DESFire command set. . . . .</b>  | <b>9</b> |           |  |           |
| 9.1      | ISO/IEC 14443-3 . . . . .  | 9        |           |  |           |
| 9.2      | ISO/IEC 14443-4 . . . . .  | 9        |           |  |           |
| 9.3      | MIFARE DESFire EV1 command set overview – security related commands. . . . .         | 10       |           |  |           |
| 9.4      | MIFARE DESFire EV1 command set overview – MIFARE DESFire EV1 level commands. . . . . | 10       |           |  |           |
| 9.5      | MIFARE DESFire EV1 command set overview – application level commands . . . . .       | 11       |           |  |           |

Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.

© NXP Semiconductors N.V. 2015. All rights reserved.

For more information, please visit: <http://www.nxp.com>  
 For sales office addresses, please send an email to: [salesaddresses@nxp.com](mailto:salesaddresses@nxp.com)

Date of release: 9 December 2015  
 145632



# MF1S70YYX\_V1

## MIFARE Classic EV1 4K - Mainstream contactless smart card IC for fast and easy solution development

Rev. 3.2 — 23 November 2017  
279332

Product data sheet  
COMPANY PUBLIC

## 1 General description

NXP Semiconductors has developed the MIFARE Classic MF1S70yyX/V1 to be used in a contactless smart card according to ISO/IEC 14443 Type A.

The MIFARE Classic EV1 4K MF1S70yyX/V1 IC is used in applications like public transport ticketing and can also be used for various other applications.

### 1.1 Anticollision

An intelligent anticollision function allows to operate more than one card in the field simultaneously. The anticollision algorithm selects each card individually and ensures that the execution of a transaction with a selected card is performed correctly without interference from another card in the field.

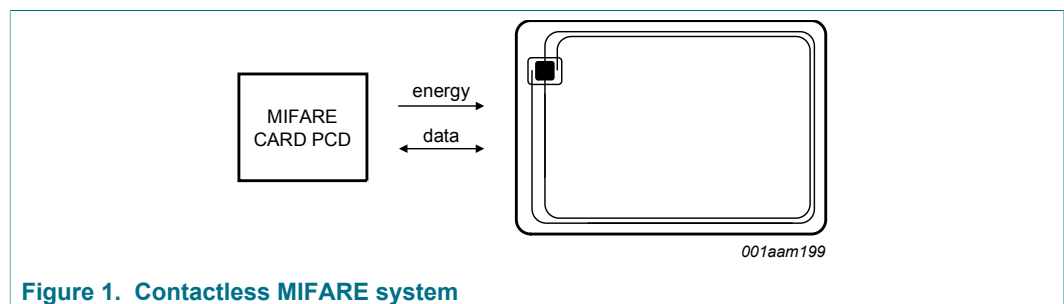


Figure 1. Contactless MIFARE system

### 1.2 Simple integration and user convenience

The MF1S70yyX/V1 is designed for simple integration and user convenience which allows complete ticketing transactions to be handled in less than 100 ms.

### 1.3 Security and privacy

- Manufacturer programmed 7-byte UID or 4-byte NUID identifier for each device
- Random ID support
- Mutual three pass authentication (ISO/IEC DIS 9798-2)
- Individual set of two keys per sector to support multi-application with key hierarchy

### 1.4 Delivery options

- 7-byte UID, 4-byte NUID
- Bumped die on sawn wafer
- MOA4 and MOA8 contactless module



## 2 Features and benefits

- Contactless transmission of data and energy supply
- Operating frequency of 13.56 MHz
- Data integrity of 16-bit CRC, parity, bit coding, bit counting
- Typical ticketing transaction time of < 100 ms (including backup management)
- Random ID support (7 Byte UID version)
- Operating distance up to 100 mm depending on antenna geometry and reader configuration
- Data transfer of 106 kbit/s
- Anticollision
- 7 Byte UID or 4 Byte NUID

### 2.1 EEPROM

- 4 kB, organized in 32 sectors of 4 blocks and 8 sectors of 16 blocks (one block consists of 16 byte)
- Data retention time of 10 years
- User definable access conditions for each memory block
- Write endurance 200000 cycles

## 3 Applications

- Public transportation
- Electronic toll collection
- School and campus cards
- Internet cafés
- Access management
- Car parking
- Employee cards
- Loyalty

## 4 Quick reference data

Table 1. Quick reference data

| Symbol                        | Parameter         | Conditions               |     | Min    | Typ    | Max  | Unit  |
|-------------------------------|-------------------|--------------------------|-----|--------|--------|------|-------|
| $C_i$                         | input capacitance |                          | [1] | 14.9   | 16.9   | 19.0 | pF    |
| $f_i$                         | input frequency   |                          |     | -      | 13.56  | -    | MHz   |
| <b>EEPROM characteristics</b> |                   |                          |     |        |        |      |       |
| $t_{ret}$                     | retention time    | $T_{amb} = 22\text{ °C}$ |     | 10     | -      | -    | year  |
| $N_{endu(W)}$                 | write endurance   | $T_{amb} = 22\text{ °C}$ |     | 100000 | 200000 | -    | cycle |

[1]  $T_{amb}=22\text{°C}$ ,  $f=13.56\text{MHz}$ ,  $V_{LaLb} = 1.5\text{ V RMS}$

## 5 Ordering information

Table 2. Ordering information

| Type number      | Package  |  | Version  |
|------------------|----------|--|----------|
|                  | Name     | Description  |          |
| MF1S7001XDUD/V1  | FFC Bump | 8 inch wafer, 120 µm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 7-byte UID            | -        |
| MF1S7001XDUD2/V1 | FFC Bump | 12 inch wafer, 120 µm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 7-byte UID           | -        |
| MF1S7001XDUF/V1  | FFC Bump | 8 inch wafer, 75 µm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 7-byte UID             | -        |
| MF1S7000XDA4/V1  | MOA4     | plastic leadless module carrier package; 35 mm wide tape, 7-byte UID   | SOT500-2 |
| MF1S7000XDA8/V1  | MOA8     | plastic leadless module carrier package; 35 mm wide tape, 7-byte UID   | SOT500-4 |
| MF1S7031XDUD/V1  | FFC Bump | 8 inch wafer, 120 µm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 4-byte non-unique ID  | -        |
| MF1S7031XDUD2/V1 | FFC Bump | 12 inch wafer, 120 µm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 4-byte non-unique ID | -        |
| MF1S7031XDUF/V1  | FFC Bump | 8 inch wafer, 75 µm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 4-byte non-unique ID   | -        |
| MF1S7030XDA4/V1  | MOA4     | plastic leadless module carrier package; 35 mm wide tape, 4-byte non-unique ID   | SOT500-2 |
| MF1S7030XDA8/V1  | MOA8     | plastic leadless module carrier package; 35 mm wide tape, 4-byte non-unique ID   | SOT500-4 |

## 6 Block diagram

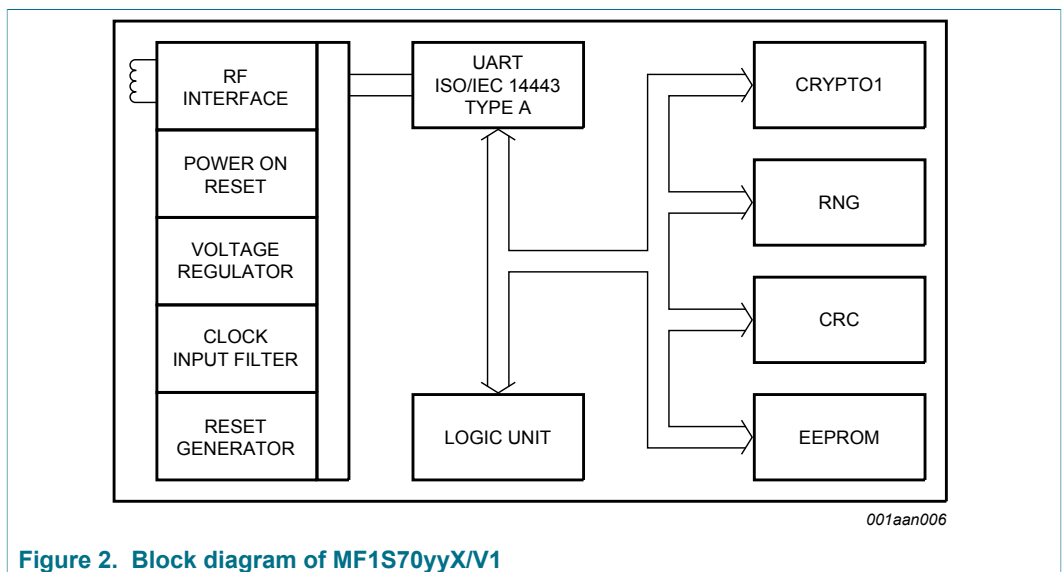


Figure 2. Block diagram of MF1S70yyX/V1

## 7 Pinning information

### 7.1 Pinning

The pinning for the MF1S70yyX/V1Dax is shown as an example in [Figure 3](#) for the MOA4 contactless module. For the contactless module MOA8, the pinning is analogous and not explicitly shown.

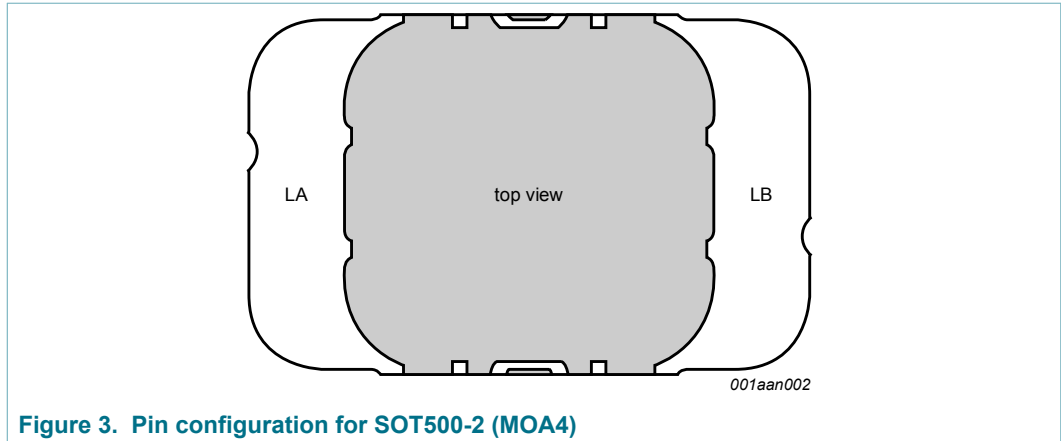


Figure 3. Pin configuration for SOT500-2 (MOA4)

Table 3. Pin allocation table

| Pin | Symbol |                            |
|-----|--------|----------------------------|
| LA  | LA     | Antenna coil connection LA |
| LB  | LB     | Antenna coil connection LB |

## 8 Functional description

### 8.1 Block description

The MF1S70yyX/V1 chip consists of a 4 kB EEPROM, RF interface and Digital Control Unit. Energy and data are transferred via an antenna consisting of a coil with a small number of turns which is directly connected to the MF1S70yyX/V1. No further external components are necessary. Refer to the document [Ref. 1](#) for details on antenna design.

- RF interface:
  - Modulator/demodulator
  - Rectifier
  - Clock regenerator
  - Power-On Reset (POR)
  - Voltage regulator
- Anticollision: Multiple cards in the field may be selected and managed in sequence
- Authentication: Preceding any memory operation the authentication procedure ensures that access to a block is only possible via the two keys specified for each block

- Control and Arithmetic Logic Unit: Values are stored in a special redundant format and can be incremented and decremented
- EEPROM interface
- Crypto unit: The CRYPTO1 stream cipher of the MF1S70yyX/V1 is used for authentication and encryption of data exchange.
- EEPROM: 4 kB is organized in 32 sectors of 4 blocks and 8 sectors of 16 blocks. One block contains 16 bytes. The last block of each sector is called "trailer", which contains two secret keys and programmable access conditions for each block in this sector.

## 8.2 Communication principle

The commands are initiated by the reader and controlled by the Digital Control Unit of the MF1S70yyX/V1. The command response is depending on the state of the IC and for memory operations also on the access conditions valid for the corresponding sector.

### 8.2.1 Request standard / all

After Power-On Reset (POR) the card answers to a request REQA or wakeup WUPA command with the answer to request code (see [Section 9.4](#), ATQA according to ISO/IEC 14443A).

### 8.2.2 Anticollision loop

In the anticollision loop the identifier of a card is read. If there are several cards in the operating field of the reader, they can be distinguished by their identifier and one can be selected (select card) for further transactions. The unselected cards return to the idle state and wait for a new request command. If the 7-byte UID is used for anticollision and selection, two cascade levels need to be processed as defined in ISO/IEC 14443-3.

**Remark:** For the 4-byte non-unique ID product versions, the identifier retrieved from the card is not defined to be unique. For further information regarding handling of non-unique identifiers see [Ref. 6](#).

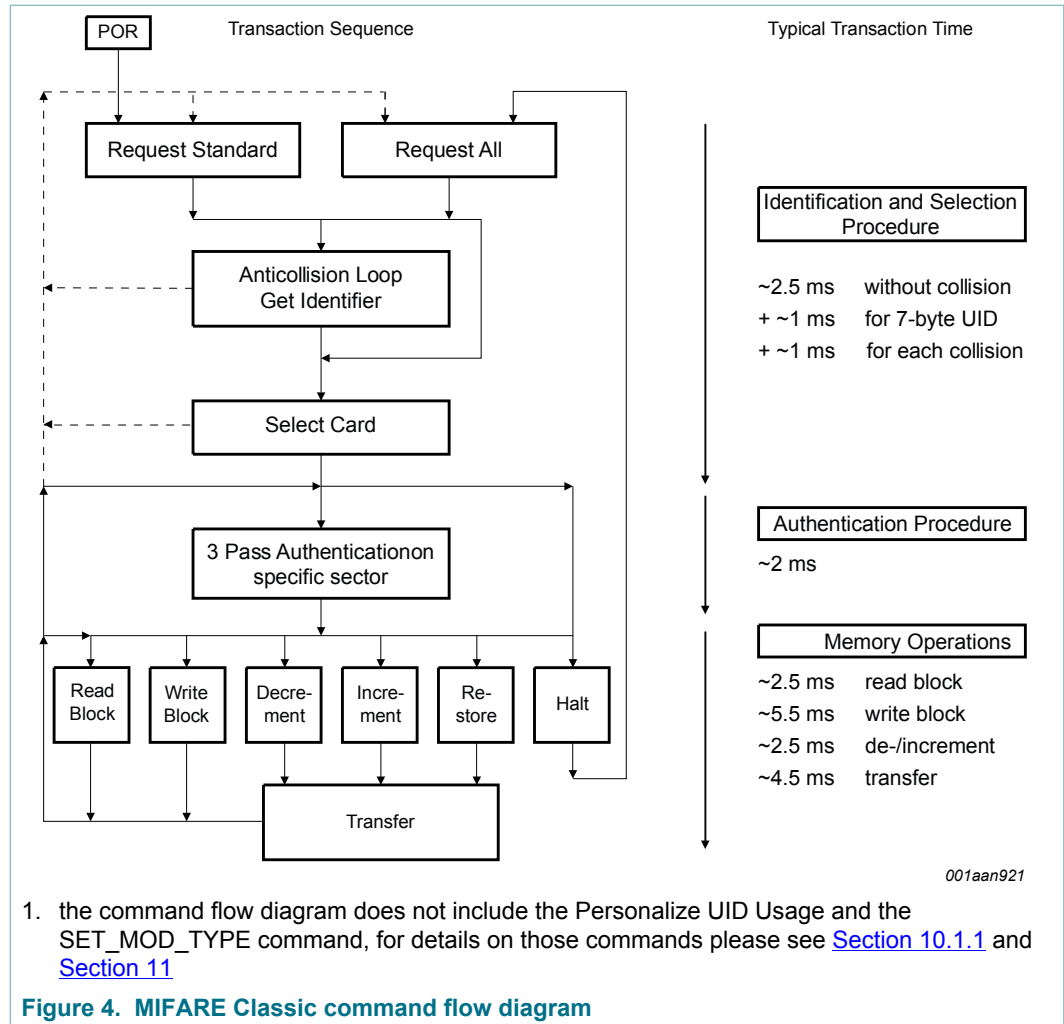
### 8.2.3 Select card

With the select card command the reader selects one individual card for authentication and memory related operations. The card returns the Select Acknowledge (SAK) code which determines the type of the selected card, see [Section 9.4](#). For further details refer to the document [Ref. 2](#).

### 8.2.4 Three pass authentication

After selection of a card the reader specifies the memory location of the following memory access and uses the corresponding key for the three pass authentication procedure. After a successful authentication all commands and responses are encrypted.

**Remark:** The HLTA command needs to be sent encrypted to the PICC after a successful authentication in order to be accepted.



### 8.2.5 Memory operations

After authentication any of the following operations may be performed:

- Read block
- Write block
- Decrement: Decrements the contents of a block and stores the result in the internal Transfer Buffer
- Increment: Increments the contents of a block and stores the result in the internal Transfer Buffer
- Restore: Moves the contents of a block into the internal Transfer Buffer
- Transfer: Writes the contents of the internal Transfer Buffer to a value block

### 8.3 Data integrity

Following mechanisms are implemented in the contactless communication link between reader and card to ensure very reliable data transmission:

- 16 bits CRC per block
- Parity bits for each byte

- Bit count checking
- Bit coding to distinguish between "1", "0" and "no information"
- Channel monitoring (protocol sequence and bit stream analysis)

#### 8.4 Three pass authentication sequence

1. The reader specifies the sector to be accessed and chooses key A or B.
2. The card reads the secret key and the access conditions from the sector trailer. Then the card sends a number as the challenge to the reader (pass one).
3. The reader calculates the response using the secret key and additional input. The response, together with a random challenge from the reader, is then transmitted to the card (pass two).
4. The card verifies the response of the reader by comparing it with its own challenge and then it calculates the response to the challenge and transmits it (pass three).
5. The reader verifies the response of the card by comparing it to its own challenge.

After transmission of the first random challenge the communication between card and reader is encrypted.

#### 8.5 RF interface

The RF-interface is according to the standard for contactless smart cards ISO/IEC 14443A.

For operation, the carrier field from the reader always needs to be present (with short pauses when transmitting), as it is used for the power supply of the card.

For both directions of data communication there is only one start bit at the beginning of each frame. Each byte is transmitted with a parity bit (odd parity) at the end. The LSB of the byte with the lowest address of the selected block is transmitted first. The maximum frame length is 163 bits (16 data bytes + 2 CRC bytes =  $16 \times 9 + 2 \times 9 + 1$  start bit).

#### 8.6 Memory organization

The  $4096 \times 8$  bit EEPROM memory is organized in 32 sectors of 4 blocks and 8 sectors of 16 blocks. One block contains 16 bytes.

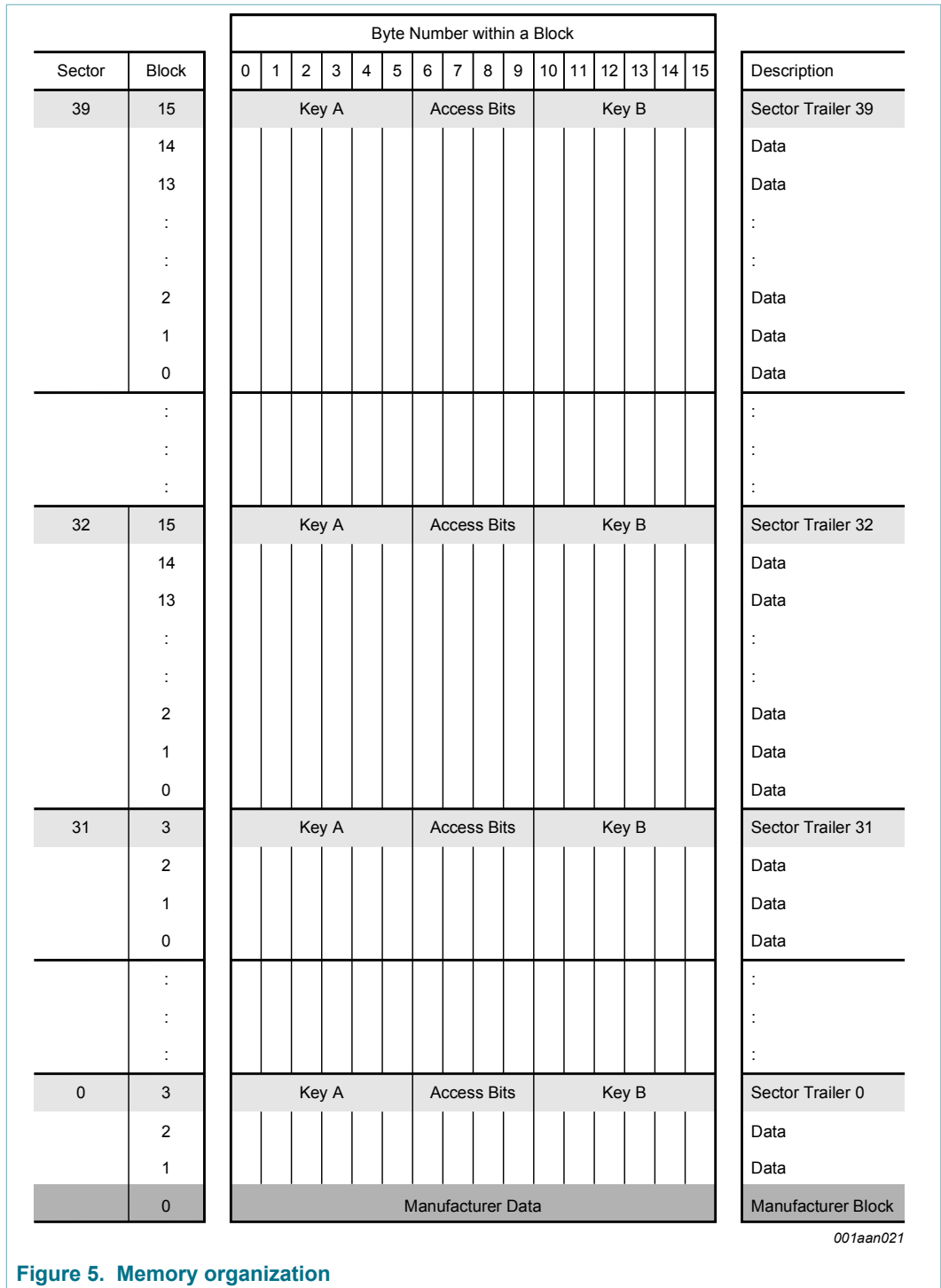
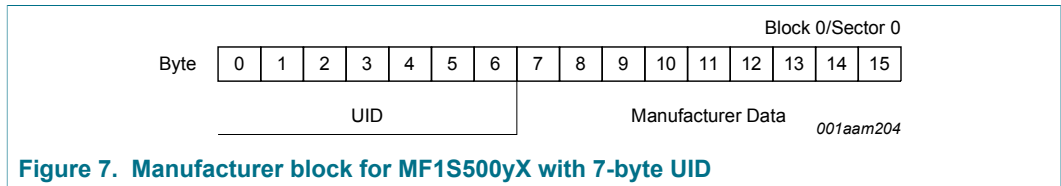
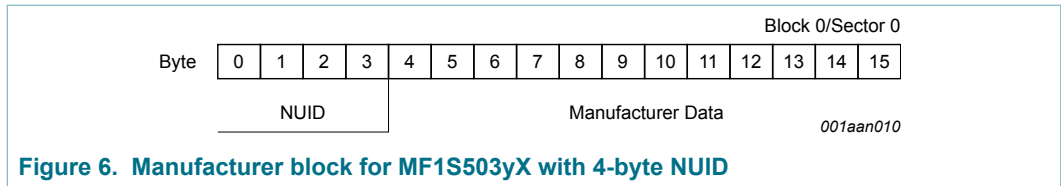


Figure 5. Memory organization

### 8.6.1 Manufacturer block

This is the first data block (block 0) of the first sector (sector 0). It contains the IC manufacturer data. This block is programmed and write protected in the production test. The manufacturer block is shown in [Figure 6](#) and [Figure 7](#) for the 4-byte NUID and 7-byte UID version respectively.





8.6.2 Data blocks

One block consists of 16 bytes. The first 32 sectors contain 3 blocks and the last 8 sectors contain 15 blocks for storing data (Sector 0 contains only two data blocks and the read-only manufacturer block).

The data blocks can be configured by the access bits as

- read/write blocks
- value blocks

Value blocks can be used for e.g. electronic purse applications, where additional commands like increment and decrement for direct control of the stored value are provided

A successful authentication has to be performed to allow any memory operation.

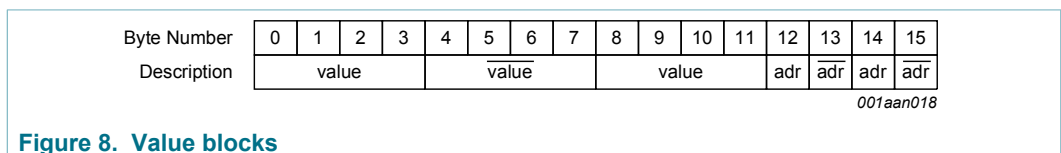
**Remark:** The default content of the data blocks at delivery is not defined.

8.6.2.1 Value blocks

Value blocks allow performing electronic purse functions (valid commands are: read, write, increment, decrement, restore, transfer). Value blocks have a fixed data format which permits error detection and correction and a backup management.

A value block can only be generated through a write operation in value block format:

- Value: Signifies a signed 4-byte value. The lowest significant byte of a value is stored in the lowest address byte. Negative values are stored in standard 2’s complement format. For reasons of data integrity and security, a value is stored three times, twice non-inverted and once inverted.
- Adr: Signifies a 1-byte address, which can be used to save the storage address of a block, when implementing a powerful backup management. The address byte is stored four times, twice inverted and non-inverted. During increment, decrement, restore and transfer operations the address remains unchanged. It can only be altered via a write command.



An example of a valid value block format for the decimal value 1234567d and the block address 17d is shown in Table 4. First, the decimal value has to be converted to the hexadecimal representation of 0012D687h. The LSByte of the hexadecimal value is stored in Byte 0, the MSByte in Byte 3. The bit inverted hexadecimal representation of the value is FFED2978h where the LSByte is stored in Byte 4 and the MSByte in Byte 7.

The hexadecimal value of the address in the example is 11h, the bit inverted hexadecimal value is EEh.

Table 4. Value block format example

| Byte Number  | 0     | 1  | 2  | 3     | 4  | 5  | 6  | 7     | 8  | 9  | 10  | 11  | 12  | 13  | 14 | 15 |  |
|--------------|-------|----|----|-------|----|----|----|-------|----|----|-----|-----|-----|-----|----|----|--|
| Description  | value |    |    | value |    |    |    | value |    |    | adr | adr | adr | adr |    |    |  |
| Values [hex] | 87    | D6 | 12 | 00    | 78 | 29 | ED | FF    | 87 | D6 | 12  | 00  | 11  | EE  | 11 | EE |  |

### 8.6.3 Sector trailer

The sector trailer is always the last block in one sector. For the first 32 sectors this is block 3 and for the remaining 8 sectors it is block 15. Each sector has a sector trailer containing the

- secret keys A (mandatory) and B (optional), which return logical "0"s when read and
- the access conditions for the blocks of that sector, which are stored in bytes 6...9. The access bits also specify the type (data or value) of the data blocks.

If key B is not needed, the last 6 bytes of the sector trailer can be used as data bytes. The access bits for the sector trailer have to be configured accordingly, see Section 8.7.2.

Byte 9 of the sector trailer is available for user data. For this byte the same access rights as for byte 6, 7 and 8 apply.

When the sector trailer is read, the key bytes are blanked out by returning logical zeros. If key B is configured to be readable, the data stored in bytes 10 to 15 is returned, see Section 8.7.2.

All keys are set to FFFF FFFF FFFFh at chip delivery and the bytes 6, 7 and 8 are set to FF0780h.

| Byte Number | 0     | 1 | 2 | 3 | 4 | 5           | 6 | 7 | 8                | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|-------------|-------|---|---|---|---|-------------|---|---|------------------|---|----|----|----|----|----|----|
| Description | Key A |   |   |   |   | Access Bits |   |   | Key B (optional) |   |    |    |    |    |    |    |

*001aan013*

**Figure 9. Sector trailer**

## 8.7 Memory access

Before any memory operation can be done, the card has to be selected and authenticated as described in Section 8.2. The possible memory operations for an addressed block depend on the key used during authentication and the access conditions stored in the associated sector trailer.

Table 5. Memory operations

| Operation | Description            | Valid for Block Type                 |
|-----------|------------------------|--------------------------------------|
| Read      | reads one memory block | read/write, value and sector trailer |

| Operation | Description  | Valid for Block Type                 |
|-----------|--|--------------------------------------|
| Write     | writes one memory block  | read/write, value and sector trailer |
| Increment | increments the contents of a block and stores the result in the internal Transfer Buffer | value                                |
| Decrement | decrements the contents of a block and stores the result in the internal Transfer Buffer | value                                |
| Transfer  | writes the contents of the internal Transfer Buffer to a block                           | value and read/write                 |
| Restore   | reads the contents of a block into the internal Transfer Buffer                          | value                                |

**8.7.1 Access conditions**

The access conditions for every data block and sector trailer are defined by 3 bits, which are stored non-inverted and inverted in the sector trailer of the specified sector.

The access bits control the rights of memory access using the secret keys A and B. The access conditions may be altered, provided one knows the relevant key and the current access condition allows this operation.

**Remark:** With each memory access the internal logic verifies the format of the access conditions. If it detects a format violation the whole sector is irreversibly blocked.

**Remark:** In the following description the access bits are mentioned in the non-inverted mode only.

The internal logic of the MF1S70yyX/V1 ensures that the commands are executed only after a successful authentication.

**Table 6. Access conditions**

| Access Bits | Valid Commands                                       |   | Block (sectors 0 - 31) | Block(s) (sectors 32-39) | Description    |
|-------------|--|---|------------------------|--------------------------|----------------|
| C13 C23 C33 | read, write  | → | 3                      | 15                       | sector trailer |
| C12 C22 C32 | read, write, increment, decrement, transfer, restore | → | 2                      | 10-14                    | data block(s)  |
| C11 C21 C31 | read, write, increment, decrement, transfer, restore | → | 1                      | 5-9                      | data block(s)  |
| C10 C20 C30 | read, write, increment, decrement, transfer, restore | → | 0                      | 0-4                      | data block(s)  |

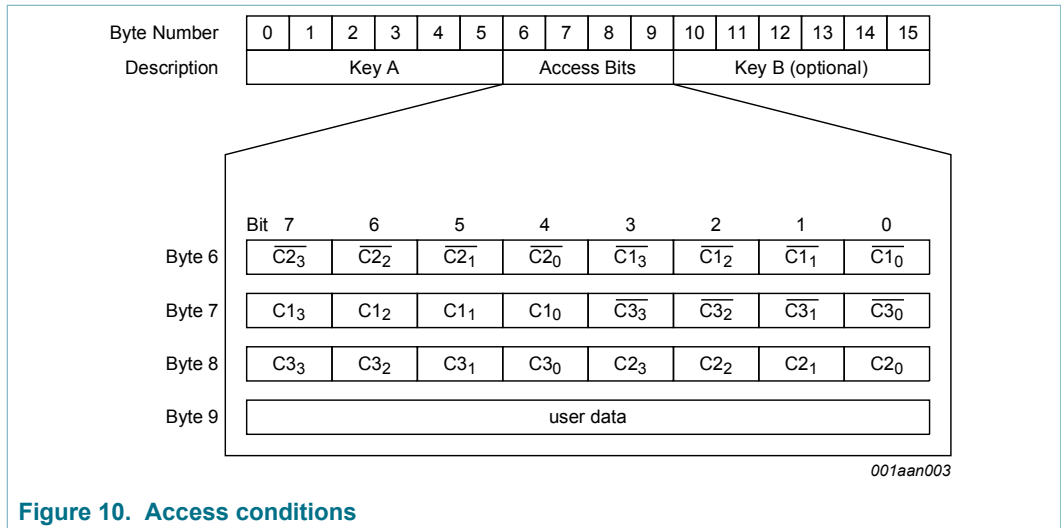


Figure 10. Access conditions

### 8.7.2 Access conditions for the sector trailer

Depending on the access bits for the sector trailer (block 3, respectively block 15) the read/write access to the keys and the access bits is specified as ‘never’, ‘key A’, ‘key B’ or key A|B’ (key A or key B).

On chip delivery the access conditions for the sector trailers and key A are predefined as transport configuration. Since key B may be read in the transport configuration, new cards must be authenticated with key A. Since the access bits themselves can also be blocked, special care has to be taken during the personalization of cards.

Table 7. Access conditions for the sector trailer

| Access bits |    |    | Access condition for |       |             |       |       |       | Remark  |
|-------------|----|----|----------------------|-------|-------------|-------|-------|-------|---|
| C1          | C2 | C3 | KEYA                 |       | Access bits |       | KEYB  |       |   |
|             |    |    | read                 | write | read        | write | read  | write |   |
| 0           | 0  | 0  | never                | key A | key A       | never | key A | key A | Key B may be read <sup>[1]</sup>                          |
| 0           | 1  | 0  | never                | never | key A       | never | key A | never | Key B may be read <sup>[1]</sup>                          |
| 1           | 0  | 0  | never                | key B | key A B     | never | never | key B |   |
| 1           | 1  | 0  | never                | never | key A B     | never | never | never |   |
| 0           | 0  | 1  | never                | key A | key A       | key A | key A | key A | Key B may be read, transport configuration <sup>[1]</sup> |
| 0           | 1  | 1  | never                | key B | key A B     | key B | never | key B |   |
| 1           | 0  | 1  | never                | never | key A B     | key B | never | never |   |
| 1           | 1  | 1  | never                | never | key A B     | never | never | never |   |

[1] For this access condition key B is readable and may be used for data

### 8.7.3 Access conditions for data blocks

Depending on the access bits for data blocks (blocks 0...2) the read/write access is specified as ‘never’, ‘key A’, ‘key B’ or ‘key A|B’ (key A or key B). The setting of the relevant access bits defines the application and the corresponding applicable commands.

- Read/write block: the operations read and write are allowed.
- Value block: Allows the additional value operations increment, decrement, transfer and restore. With access condition '001' only read and decrement are possible which reflects a non-rechargeable card. For access condition '110' recharging is possible by using key B.
- Manufacturer block: the read-only condition is not affected by the access bits setting!
- Key management: in transport configuration key A must be used for authentication

Table 8. Access conditions for data blocks

| Access bits |    |    | Access condition for |         |           |                              | Application                            |
|-------------|----|----|----------------------|---------|-----------|------------------------------|--|
| C1          | C2 | C3 | read                 | write   | increment | decrement, transfer, restore |  |
| 0           | 0  | 0  | key A B              | key A B | key A B   | key A B                      | transport configuration <sup>[1]</sup> |
| 0           | 1  | 0  | key A B              | never   | never     | never                        | read/write block <sup>[1]</sup>        |
| 1           | 0  | 0  | key A B              | key B   | never     | never                        | read/write block <sup>[1]</sup>        |
| 1           | 1  | 0  | key A B              | key B   | key B     | key A B                      | value block <sup>[1]</sup>             |
| 0           | 0  | 1  | key A B              | never   | never     | key A B                      | value block <sup>[1]</sup>             |
| 0           | 1  | 1  | key B                | key B   | never     | never                        | read/write block <sup>[1]</sup>        |
| 1           | 0  | 1  | key B                | never   | never     | never                        | read/write block <sup>[1]</sup>        |
| 1           | 1  | 1  | never                | never   | never     | never                        | read/write block                       |

[1] If key B may be read in the corresponding Sector Trailer it cannot serve for authentication (see grey marked lines in [Table 7](#)). As a consequence, if the reader authenticates any block of a sector which uses such access conditions for the Sector Trailer and using key B, the card will refuse any subsequent memory access after authentication.

## 9 Command overview

The MIFARE Classic card activation follows the ISO/IEC 14443 Type A. After the MIFARE Classic card has been selected, it can either be deactivated using the ISO/IEC 14443 Halt command, or the MIFARE Classic commands can be performed. For more details about the card activation refer to [Ref. 4](#).

### 9.1 MIFARE Classic command overview

All MIFARE Classic commands typically use the MIFARE CRYPTO1 and require an authentication.

All available commands for the MIFARE Classic EV1 4K are shown in [Table 9](#).

Table 9. Command overview

| Command           | ISO/IEC 14443     | Command code (hexadecimal) |
|-------------------|-------------------|----------------------------|
| Request           | REQA              | 26h (7 bit)                |
| Wake-up           | WUPA              | 52h (7 bit)                |
| Anticollision CL1 | Anticollision CL1 | 93h 20h                    |
| Select CL1        | Select CL1        | 93h 70h                    |

| Command                   | ISO/IEC 14443     | Command code (hexadecimal) |
|---------------------------|-------------------|----------------------------|
| Anticollision CL2         | Anticollision CL2 | 95h 20h                    |
| Select CL2                | Select CL2        | 95h 70h                    |
| Halt                      | Halt              | 50h 00h                    |
| Authentication with Key A | -                 | 60h                        |
| Authentication with Key B | -                 | 61h                        |
| Personalize UID Usage     | -                 | 40h                        |
| SET_MOD_TYPE              | -                 | 43h                        |
| MIFARE Read               | -                 | 30h                        |
| MIFARE Write              | -                 | A0h                        |
| MIFARE Decrement          | -                 | C0h                        |
| MIFARE Increment          | -                 | C1h                        |
| MIFARE Restore            | -                 | C2h                        |
| MIFARE Transfer           | -                 | B0h                        |

All commands use the coding and framing as described in [Ref. 3](#) and [Ref. 4](#) if not otherwise specified.

## 9.2 Timings

The timing shown in this document are not to scale and values are rounded to 1  $\mu$ s.

All given times refer to the data frames including start of communication and end of communication. A PCD data frame contains the start of communication (1 "start bit") and the end of communication (one logic 0 + 1 bit length of unmodulated carrier). A PICC data frame contains the start of communication (1 "start bit") and the end of communication (1 bit length of no subcarrier).

The minimum command response time is specified according to [Ref. 4](#) as an integer  $n$  which specifies the PCD to PICC frame delay time. The frame delay time from PICC to PCD is at least 87  $\mu$ s. The maximum command response time is specified as a time-out value. Depending on the command, the  $T_{ACK}$  value specified for command responses defines the PCD to PICC frame delay time. It does it for either the 4-bit ACK value specified in [Section 9.3](#) or for a data frame.

All command timings are according to ISO/IEC 14443-3 frame specification as shown for the Frame Delay Time in [Figure 11](#). For more details refer to [Ref. 3](#) and [Ref. 4](#).

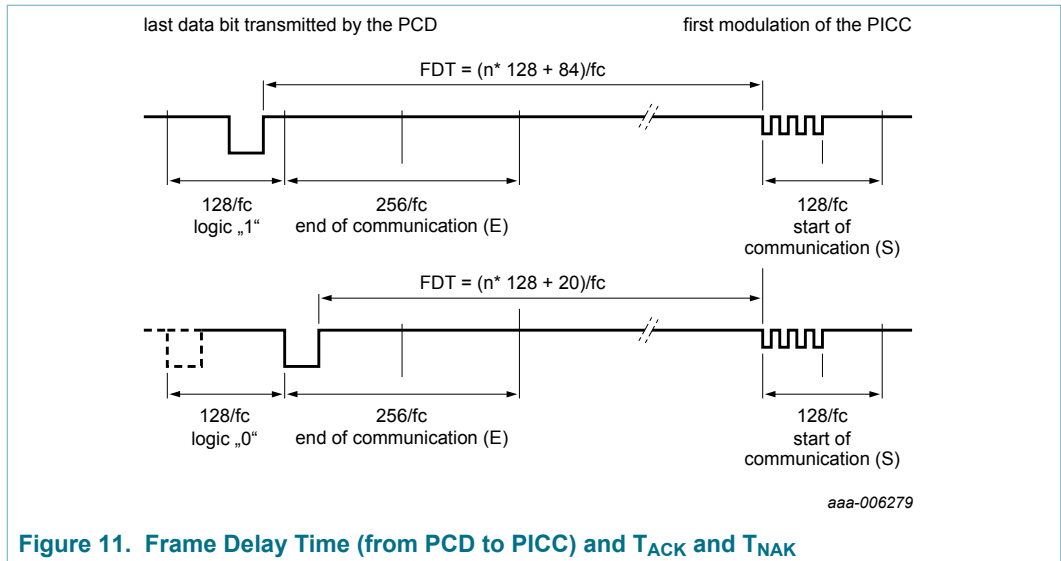


Figure 11. Frame Delay Time (from PCD to PICC) and  $T_{ACK}$  and  $T_{NAK}$

**Remark:** Due to the coding of commands, the measured timings usually excludes (a part of) the end of communication. Consider this factor when comparing the specified with the measured times.

### 9.3 MIFARE Classic ACK and NAK

The MIFARE Classic uses a 4 bit ACK / NAK as shown in [Table 10](#).

Table 10. MIFARE ACK and NAK

| Code (4-bit) | Transfer Buffer Validity | Description         |
|--------------|--------------------------|---------------------|
| Ah           |                          | Acknowledge (ACK)   |
| 0h           | valid                    | invalid operation   |
| 1h           | valid                    | parity or CRC error |
| 4h           | invalid                  | invalid operation   |
| 5h           | invalid                  | parity or CRC error |

### 9.4 ATQA and SAK responses

For details on the type identification procedure please refer to [Ref. 2](#).

The MF1S70yyX/V1 answers to a REQA or WUPA command with the ATQA value shown in [Table 11](#) and to a Select CL1 command (CL2 for the 7-byte UID variant) with the SAK value shown in [Table 12](#).

**Table 11. ATQA response of the MF1S70yyX/V1**

| Sales Type | Hex Value          | Bit Number |    |    |    |    |    |    |   |   |   |   |   |   |   |   |   |   |
|------------|--------------------|------------|----|----|----|----|----|----|---|---|---|---|---|---|---|---|---|---|
|            |                    | 16         | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |   |
| MF1S00yX   | 00 44h             | 0          | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 |
| MF1S03yX   | 00 04h             | 0          | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| MF1S700yX  | 00 42 <sub>h</sub> | 0          | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 |
| MF1S703yX  | 00 02 <sub>h</sub> | 0          | 0  | 0  | 0  | 0  | 0  | 0  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |

**Table 12. SAK response of the MF1S70yyX/V1**

| Sales Type   | Hex Value | Bit Number |   |   |   |   |   |   |   |
|--------------|-----------|------------|---|---|---|---|---|---|---|
|              |           | 8          | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| MF1S70yyX/V1 | 18        | 0          | 0 | 0 | 1 | 1 | 0 | 0 | 0 |

**Remark:** The ATQA coding in bits 7 and 8 indicate the UID size according to ISO/IEC 14443 independent from the settings of the UID usage.

**Remark:** The bit numbering in the ISO/IEC 14443 starts with LSBit = bit 1, but not LSBit = bit 0. So one byte counts bit 1 to 8 instead of bit 0 to 7.

## 10 UID Options and Handling

The MF1S70yyX/V1 product family offers two delivery options for the UID which is stored in block 0 of sector 0.

- 7-byte UID
- 4-byte NUID (Non-Unique ID)

This section describes the MIFARE Classic MF1S70yyX/V1 operation when using one of the 2 UID options with respect to card selection, authentication and personalization. See also [Ref. 6](#) for details on how to handle UIDs and NUIDs with MIFARE Classic products.

### 10.1 7-byte UID Operation

All MF1S70yXDyy products are featuring a 7-byte UID. This 7-byte UID is stored in block 0 of sector 0 as shown in [Figure 7](#). The behaviour during anti-collision, selection and authentication can be configured during personalization for this UID variant.

#### 10.1.1 Personalization Options

The 7-byte UID variants of the MF1S70yyX/V1 can be operated with four different functionalities, denoted as UIDFn (UID Functionality n).



1. UIDF0: anti-collision and selection with the double size UID according to ISO/IEC 14443-3
2. UIDF1: anti-collision and selection with the double size UID according to ISO/IEC 14443-3 and optional usage of a selection process shortcut
3. UIDF2: anti-collision and selection with a single size random ID according to ISO/IEC 14443-3
4. UIDF3: anti-collision and selection with a single size NUID according to ISO/IEC 14443-3 where the NUID is calculated out of the 7-byte UID

The anti-collision and selection procedure and the implications on the authentication process are detailed in [Section 10.1.2](#) and [Section 10.1.3](#).

The default configuration at delivery is option 1 which enables the ISO/IEC 14443-3 compliant anti-collision and selection. This configuration can be changed using the 'Personalize UID Usage' command. The execution of this command requires an authentication to sector 0. Once this command has been issued and accepted by the PICC, the configuration is automatically locked. A subsequently issued 'Personalize UID Usage' command is not executed and a NAK is replied by the PICC.

**Remark:** As the configuration is changeable at delivery, it is strongly recommended to send this command at personalization of the card to prevent unwanted changes in the field. This should also be done if the default configuration is used.

**Remark:** The configuration becomes effective only after PICC unselect or PICC field reset.

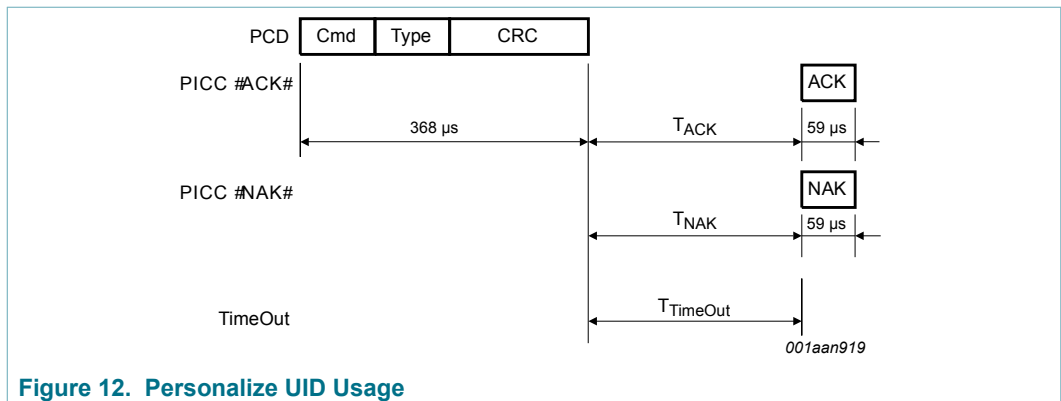


Figure 12. Personalize UID Usage

Table 13. Personalize UID Usage command

| Name     | Code                         | Description  | Length  |
|----------|------------------------------|--|---------|
| Cmd      | 40h                          | Set anti-collision, selection and authentication behaviour                         | 1 byte  |
| Type     | -                            | Encoded type of UID usage:<br>UIDF0: 00h<br>UIDF1: 40h<br>UIDF2: 20h<br>UIDF3: 60h | 1 byte  |
| CRC      | -                            | CRC according to <a href="#">Ref. 4</a>  | 2 bytes |
| ACK, NAK | see <a href="#">Table 10</a> | see <a href="#">Section 9.3</a>  | 4-bit   |

**Table 14. Personalize UID Usage timing**

|                       | T <sub>ACK min</sub> | T <sub>ACK max</sub> | T <sub>NAK min</sub> | T <sub>NAK max</sub> | T <sub>TimeOut</sub> |
|-----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|
| Personalize UID Usage | n=9                  | T <sub>TimeOut</sub> | n=9                  | T <sub>TimeOut</sub> | 10 ms                |

**10.1.2 Anti-collision and Selection**

Depending on the chosen personalization option there are certain possibilities to perform anti-collision and selection. To bring the MIFARE Classic into the ACTIVE state according to ISO/IEC 14443-3, the following sequences are available.

Sequence 1: ISO/IEC 14443-3 compliant anti-collision and selection using the cascade level 1 followed by the cascade level 2 SEL command

Sequence 2: using cascade level 1 anti-collision and selection procedure followed by a Read command from block 0

Sequence 3: ISO/IEC 14443-3 compliant anti-collision and selection using the cascade level 1 SEL command

**Remark:** The Read from Block 0 in Sequence 2 does not require a prior authentication to Sector 0 and is transmitted in plain data. For all other sequences, the readout from Block 0 in Sector 0 is encrypted and requires an authentication to that sector.

**Remark:** The settings done with Personalize UID Usage do not change the ATQA coding.

**Table 15. Available activation sequences for 7-byte UID options**

| UID Functionality | Available Activation Sequences |
|-------------------|--------------------------------|
| UIDF0             | Sequence 1                     |
| UIDF1             | Sequence 1, Sequence 2         |
| UIDF2             | Sequence 3                     |
| UIDF3             | Sequence 3                     |

**10.1.3 Authentication**

During the authentication process, 4-byte of the UID are passed on to the MIFARE Classic Authenticate command of the contactless reader IC. Depending on the activation sequence, those 4-byte are chosen differently. In general, the input parameter to the MIFARE Classic Authenticate command is the set of 4 bytes retrieved during the last cascade level from the ISO/IEC 14443-3 Type A anticollision.

**Table 16. Input parameter to MIFARE Classic Authenticate**

| UID Functionality | Input to MIFARE Classic Authenticate Command |
|-------------------|--|
| Sequence 1        | CL2 bytes (UID3...UID6)                      |
| Sequence 2        | CL1 bytes (CT, UID0...UID2)                  |
| Sequence 3        | 4-byte NUID/RID (UID0...UID3)                |

**10.2 4-byte UID Operation**

All MF1S703yXDyy products are featuring a 4-byte NUID. This 4-byte NUID is stored in block 0 of sector 0 as shown in [Figure 6](#).

10.2.1 Anti-collision and Selection

The anti-collision and selection process for the product variants featuring 4-byte NUIDs is done according to ISO/IEC 14443-3 Type A using cascade level 1 only.

10.2.2 Authentication

The input parameter to the MIFARE Classic Authenticate command is the full 4-byte UID retrieved during the anti-collision procedure. This is the same as for the activation Sequence 3 in the 7-byte UID variant.

11 Load Modulation Strength Option

The MIFARE Classic EV1 4K features the possibility to set the load modulation strength to high or normal. The default level is set to a high modulation strength and it is recommended for optimal performance to maintain this level and only switch to the low load modulation strength if the contactless system requires it.

**Remark:** The configuration becomes effective only after a PICC unselect or a PICC field reset. The configuration can be changed multiple times by asserting the command.

**Remark:** The MIFARE Classic EV1 4K needs to be authenticated to sector 0 with Key A to perform the SET\_MOD\_TYPE command. The Access Bits for sector 0 are irrelevant.

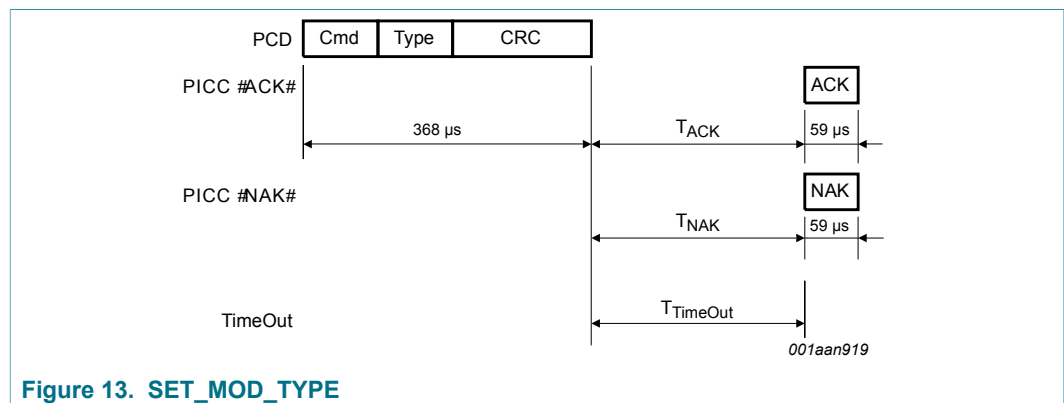


Figure 13. SET\_MOD\_TYPE

Table 17. SET\_MOD\_TYPE command

| Name     | Code                         | Description   | Length  |
|----------|------------------------------|---|---------|
| Cmd      | 43h                          | Set load modulation strength  | 1 byte  |
| Type     | -                            | Encoded load modulation strength:<br>strong modulation: 01h (default)<br>normal modulation: 00h | 1 byte  |
| CRC      | -                            | CRC according to <a href="#">Ref. 4</a>   | 2 bytes |
| ACK, NAK | see <a href="#">Table 10</a> | see <a href="#">Section 9.3</a>   | 4-bit   |

Table 18. SET\_MOD\_TYPE timing

|              | T <sub>ACK min</sub> | T <sub>ACK max</sub> | T <sub>NAK min</sub> | T <sub>NAK max</sub> | T <sub>TimeOut</sub> |
|--------------|----------------------|----------------------|----------------------|----------------------|----------------------|
| SET_MOD_TYPE | n=9                  | T <sub>TimeOut</sub> | n=9                  | T <sub>TimeOut</sub> | 5 ms                 |

The configured load modulation is shown in the manufacturer data of block 0 in sector 0. The exact location is shown below in Figure 14 and Table 19.

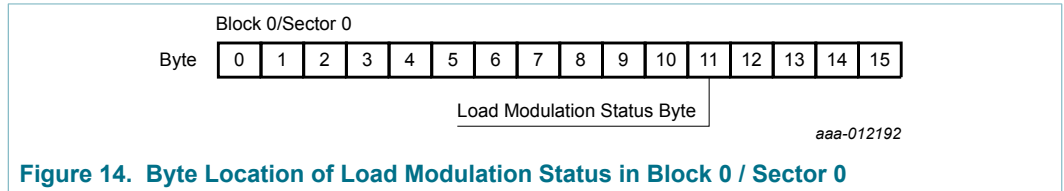


Figure 14. Byte Location of Load Modulation Status in Block 0 / Sector 0

Table 19. Load Modulation Status Indication

| Load Modulation Type   | Hex Value     | Bit Number |   |   |   |   |   |   |   |
|------------------------|---------------|------------|---|---|---|---|---|---|---|
|                        |               | 7          | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| strong load modulation | 20h (default) | 0          | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| normal load modulation | 00h           | 0          | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

## 12 MIFARE Classic commands

### 12.1 MIFARE Authentication

The MIFARE authentication is a 3-pass mutual authentication which needs two pairs of command-response. These two parts, MIFARE authentication part 1 and part 2 are shown in Figure 15, Figure 16 and Table 20.

Table 21 shows the required timing.

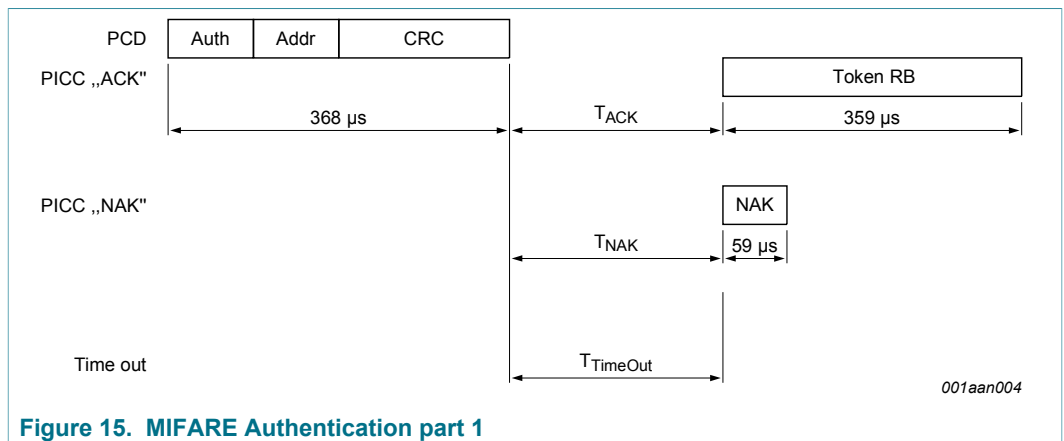


Figure 15. MIFARE Authentication part 1

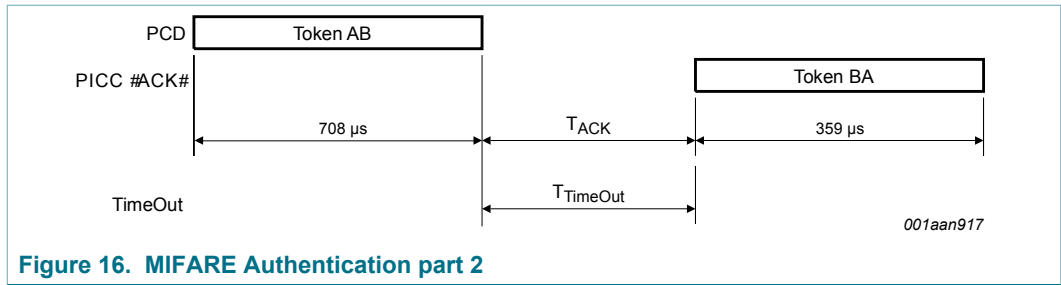


Figure 16. MIFARE Authentication part 2

Table 20. MIFARE authentication command

| Name              | Code                         | Description                             | Length  |
|-------------------|------------------------------|---|---------|
| Auth (with Key A) | 60h                          | Authentication with Key A               | 1 byte  |
| Auth (with Key B) | 61h                          | Authentication with Key B               | 1 byte  |
| Addr              | -                            | MIFARE Block address (00h to FFh)       | 1 byte  |
| CRC               | -                            | CRC according to <a href="#">Ref. 4</a> | 2 bytes |
| Token RB          | -                            | Challenge 1 (Random Number)             | 4 bytes |
| Token AB          | -                            | Challenge 2 (encrypted data)            | 8 bytes |
| Token BA          | -                            | Challenge 2 (encrypted data)            | 4 bytes |
| NAK               | see <a href="#">Table 10</a> | see <a href="#">Section 9.3</a>         | 4-bit   |

Table 21. MIFARE authentication timing

|                       | T <sub>ACK min</sub> | T <sub>ACK max</sub> | T <sub>NAK min</sub> | T <sub>NAK max</sub> | T <sub>TimeOut</sub> |
|-----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|
| Authentication part 1 | n=9                  | T <sub>TimeOut</sub> | n=9                  | n=9                  | 1 ms                 |
| Authentication part 2 | n=9                  | T <sub>TimeOut</sub> |                      |                      | 1 ms                 |

**Remark:** The minimum required time between MIFARE Authentication part 1 and part 2 is the minimum required FDT according to [Ref. 4](#). There is no maximum time specified.

**Remark:** The MIFARE authentication and encryption requires an MIFARE reader IC (e.g. the CL RC632). For more details about the authentication command refer to the corresponding data sheet (e.g. [Ref. 5](#)). The 4-byte input parameter for the MIFARE Classic Authentication is detailed in [Section 10.1.3](#) and [Section 10.2.2](#).

## 12.2 MIFARE Read

The MIFARE Read requires a block address, and returns the 16 bytes of one MIFARE Classic block. The command structure is shown in [Figure 17](#) and [Table 22](#).

[Table 23](#) shows the required timing.

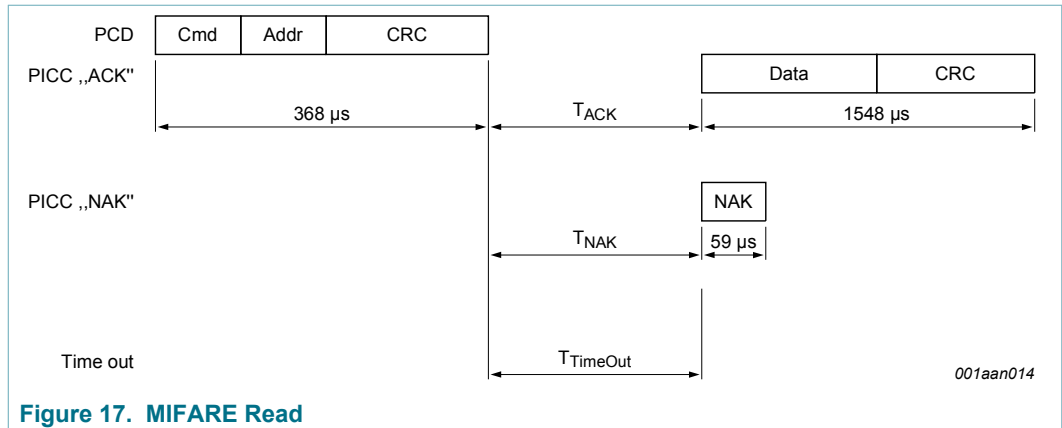


Figure 17. MIFARE Read

Table 22. MIFARE Read command

| Name | Code                         | Description                             | Length   |
|------|------------------------------|---|----------|
| Cmd  | 30h                          | Read one block                          | 1 byte   |
| Addr | -                            | MIFARE Block address (00h to FFh)       | 1 byte   |
| CRC  | -                            | CRC according to <a href="#">Ref. 4</a> | 2 bytes  |
| Data | -                            | Data content of the addressed block     | 16 bytes |
| NAK  | see <a href="#">Table 10</a> | see <a href="#">Section 9.3</a>         | 4-bit    |

Table 23. MIFARE Read timing

|      | T <sub>ACK min</sub> | T <sub>ACK max</sub> | T <sub>NAK min</sub> | T <sub>NAK max</sub> | T <sub>TimeOut</sub> |
|------|----------------------|----------------------|----------------------|----------------------|----------------------|
| Read | n=9                  | T <sub>TimeOut</sub> | n=9                  | T <sub>TimeOut</sub> | 5 ms                 |

### 12.3 MIFARE Write

The MIFARE Write requires a block address, and writes 16 bytes of data into the addressed MIFARE Classic EV1 4K block. It needs two pairs of command-response. These two parts, MIFARE Write part 1 and part 2 are shown in [Figure 18](#) and [Figure 19](#) and [Table 24](#).

[Table 25](#) shows the required timing.

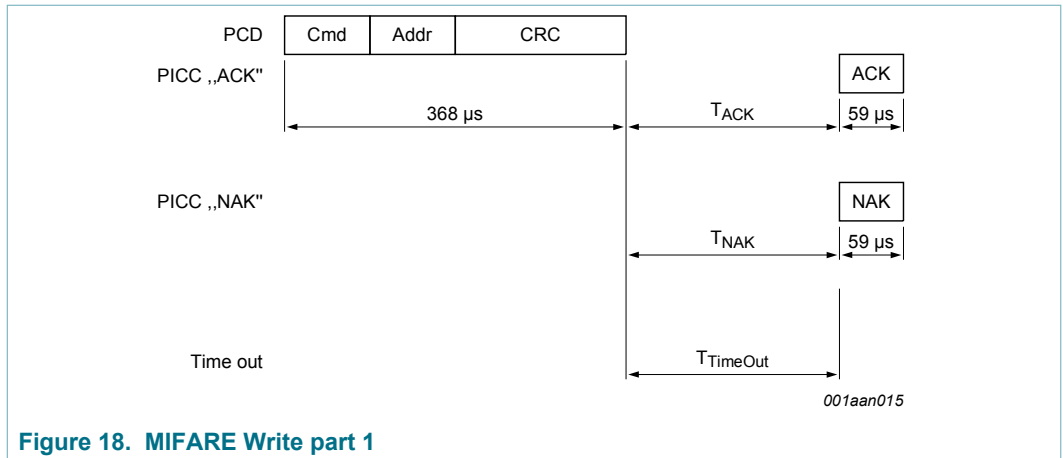


Figure 18. MIFARE Write part 1

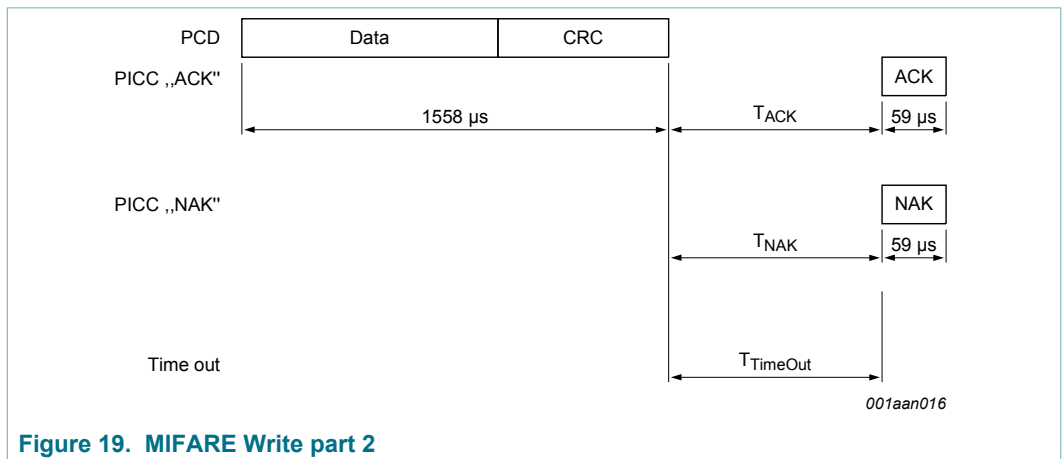


Figure 19. MIFARE Write part 2

Table 24. MIFARE Write command

| Name | Code                         | Description                               | Length   |
|------|------------------------------|---|----------|
| Cmd  | A0h                          | Write one block                           | 1 byte   |
| Addr | -                            | MIFARE Block or Page address (00h to FFh) | 1 byte   |
| CRC  | -                            | CRC according to <a href="#">Ref. 4</a>   | 2 bytes  |
| Data | -                            | Data                                      | 16 bytes |
| NAK  | see <a href="#">Table 10</a> | see <a href="#">Section 9.3</a>           | 4-bit    |

Table 25. MIFARE Write timing

|              | $T_{ACK\ min}$ | $T_{ACK\ max}$ | $T_{NAK\ min}$ | $T_{NAK\ max}$ | $T_{TimeOut}$ |
|--------------|----------------|----------------|----------------|----------------|---------------|
| Write part 1 | n=9            | $T_{TimeOut}$  | n=9            | $T_{TimeOut}$  | 5 ms          |
| Write part 2 | n=9            | $T_{TimeOut}$  | n=9            | $T_{TimeOut}$  | 10 ms         |

**Remark:** The minimum required time between MIFARE Write part 1 and part 2 is the minimum required FDT according to [Ref. 4](#). There is no maximum time specified.

### 12.4 MIFARE Increment, Decrement and Restore

The MIFARE Increment requires a source block address and an operand. It adds the operand to the value of the addressed block, and stores the result in the Transfer Buffer.

The MIFARE Decrement requires a source block address and an operand. It subtracts the operand from the value of the addressed block, and stores the result in the Transfer Buffer.

The MIFARE Restore requires a source block address. It copies the value of the addressed block into the Transfer Buffer. The 4 byte Operand in the second part of the command is not used and may contain arbitrary values.

All three commands are responding with a NAK to the first command part if the addressed block is not formatted to be a valid value block, see [Section 8.6.2.1](#).

The two parts of each command are shown in [Figure 20](#) and [Figure 21](#) and [Table 26](#).

[Table 27](#) shows the required timing.

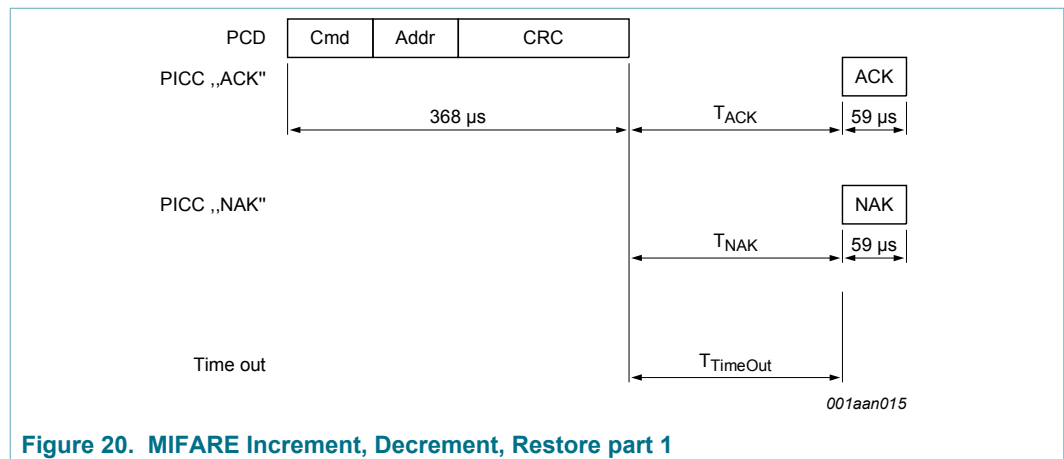
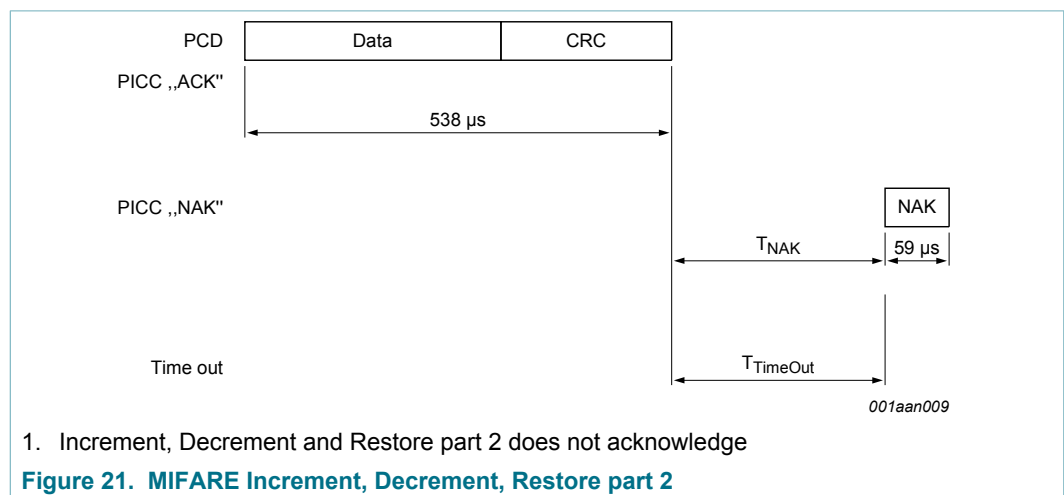


Figure 20. MIFARE Increment, Decrement, Restore part 1



1. Increment, Decrement and Restore part 2 does not acknowledge

Figure 21. MIFARE Increment, Decrement, Restore part 2



Table 26. MIFARE Increment, Decrement and Restore command

| Name | Code                         | Description                              | Length  |
|------|------------------------------|--|---------|
| Cmd  | C1h                          | Increment                                | 1 byte  |
| Cmd  | C0h                          | Decrement                                | 1 byte  |
| Cmd  | C2h                          | Restore                                  | 1 byte  |
| Addr | -                            | MIFARE source block address (00h to FFh) | 1 byte  |
| CRC  | -                            | CRC according to <a href="#">Ref. 4</a>  | 2 bytes |
| Data | -                            | Operand (4 byte signed integer)          | 4 bytes |
| NAK  | see <a href="#">Table 10</a> | see <a href="#">Section 9.3</a>          | 4-bit   |

Table 27. MIFARE Increment, Decrement and Restore timing

|  | T <sub>ACK min</sub> | T <sub>ACK max</sub> | T <sub>NAK min</sub> | T <sub>NAK max</sub> | T <sub>TimeOut</sub> |
|--|----------------------|----------------------|----------------------|----------------------|----------------------|
| Increment, Decrement, and Restore part 1 | n=9                  | T <sub>TimeOut</sub> | n=9                  | T <sub>TimeOut</sub> | 5 ms                 |
| Increment, Decrement, and Restore part 2 | n=9                  | T <sub>TimeOut</sub> | n=9                  | T <sub>TimeOut</sub> | 5 ms                 |

**Remark:** The minimum required time between MIFARE Increment, Decrement, and Restore part 1 and part 2 is the minimum required FDT according to [Ref. 4](#). There is no maximum time specified.

**Remark:** The MIFARE Increment, Decrement, and Restore commands require a MIFARE Transfer to store the value into a destination block.

**Remark:** The MIFARE Increment, Decrement, and Restore command part 2 does not provide an acknowledgement, so the regular time out has to be used instead.

## 12.5 MIFARE Transfer

The MIFARE Transfer requires a destination block address, and writes the value stored in the Transfer Buffer into one MIFARE Classic block. The command structure is shown in [Figure 22](#) and [Table 28](#).

[Table 29](#) shows the required timing.

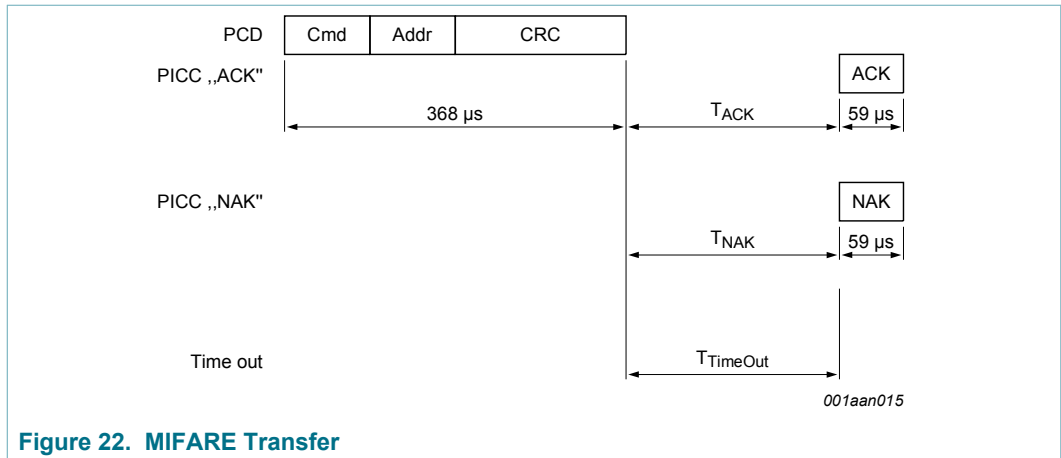


Figure 22. MIFARE Transfer

Table 28. MIFARE Transfer command

| Name | Code                         | Description   | Length  |
|------|------------------------------|---|---------|
| Cmd  | B0h                          | Write the value from the Transfer Buffer into destination block | 1 byte  |
| Addr | -                            | MIFARE destination block address (00h to FFh)                   | 1 byte  |
| CRC  | -                            | CRC according to <a href="#">Ref. 4</a>                         | 2 bytes |
| NAK  | see <a href="#">Table 10</a> | see <a href="#">Section 9.3</a>                                 | 4-bit   |

Table 29. MIFARE Transfer timing

|          | T <sub>ACK min</sub> | T <sub>ACK max</sub> | T <sub>NAK min</sub> | T <sub>NAK max</sub> | T <sub>TimeOut</sub> |
|----------|----------------------|----------------------|----------------------|----------------------|----------------------|
| Transfer | n=9                  | T <sub>TimeOut</sub> | n=9                  | T <sub>TimeOut</sub> | 10 ms                |

### 13 Limiting values

Stresses above one or more of the limiting values may cause permanent damage to the device. Exposure to limiting values for extended periods may affect device reliability.

Table 30. Limiting values

In accordance with the Absolute Maximum Rating System (IEC 60134).

| Symbol                 | Parameter   | Min | Max | Unit |
|------------------------|---|-----|-----|------|
| I <sub>I</sub>         | input current   | -   | 30  | mA   |
| P <sub>tot</sub> /pack | total power dissipation per package                     | -   | 120 | mW   |
| T <sub>stg</sub>       | storage temperature                                     | -55 | 125 | °C   |
| T <sub>amb</sub>       | ambient temperature                                     | -25 | 70  | °C   |
| V <sub>ESD</sub>       | electrostatic discharge voltage on LA/LB <sup>[1]</sup> | 2   | -   | kV   |

[1] ANSI/ESDA/JEDEC JS-001; Human body model: C = 100 pF, R = 1.5 kΩ

**CAUTION**

This device has limited built-in ElectroStatic Discharge (ESD) protection. The leads should be shorted together or the device placed in conductive foam during storage or handling to prevent electrostatic damage to the gates.

## 14 Characteristics

Table 31. Characteristics

| Symbol                        | Parameter         | Conditions                             |     | Min    | Typ    | Max  | Unit  |
|-------------------------------|-------------------|--|-----|--------|--------|------|-------|
| $C_i$                         | input capacitance |  | [1] | 14.9   | 16.9   | 19.0 | pF    |
| $f_i$                         | input frequency   |  |     | -      | 13.56  | -    | MHz   |
| <b>EEPROM characteristics</b> |                   |  |     |        |        |      |       |
| $t_{ret}$                     | retention time    | $T_{amb} = 22\text{ }^{\circ}\text{C}$ |     | 10     | -      | -    | year  |
| $N_{endu(W)}$                 | write endurance   | $T_{amb} = 22\text{ }^{\circ}\text{C}$ |     | 100000 | 200000 | -    | cycle |

[1]  $T_{amb}=22^{\circ}\text{C}$ ,  $f=13,56\text{MHz}$ ,  $V_{LaLb} = 1,5\text{ V RMS}$

## 15 Wafer specification

For more details on the wafer delivery forms see [Ref. 9](#).

Table 32. Wafer specifications MF1S70yyXDUy

| <b>Wafer</b>                          |   |
|---------------------------------------|---|
| diameter                              | 200 mm typical (8 inches)<br>300 mm typical (12 inches)               |
| maximum diameter after foil expansion | 210 mm (8 inches)<br>not applicable (12 inches)                       |
| die separation process                | laser dicing (8 inches)<br>blade dicing (12 inches)                   |
| thickness MF1S70yyXDUD                | 120 $\mu\text{m} \pm 15\text{ }\mu\text{m}$                           |
| MF1S70yyXDUF                          | 75 $\mu\text{m} \pm 10\text{ }\mu\text{m}$                            |
| flatness                              | not applicable  |
| Potential Good Dies per Wafer (PGDW)  | 64727 (8 inches)<br>147540 (12 inches)                                |
| <b>Wafer backside</b>                 |   |
| material                              | Si  |
| treatment                             | ground and stress relieve   |
| roughness                             | $R_a$ max = 0.5 $\mu\text{m}$<br>$R_t$ max = 5 $\mu\text{m}$          |
| <b>Chip dimensions</b>                |   |
| step size <sup>[1]</sup>              | x = 658 $\mu\text{m}$ (8 inches)<br>x = 660 $\mu\text{m}$ (12 inches) |

|   |   |
|---|---|
|   | y = 713 $\mu\text{m}$ (8 inches)<br>y = 715 $\mu\text{m}$ (12 inches)                 |
| gap between chips <sup>[1]</sup>            | typical = 19 $\mu\text{m}$<br>minimum = 5 $\mu\text{m}$<br>not applicable (12 inches) |
| <b>Passivation</b>                          |   |
| type  | sandwich structure  |
| material                                    | PSG / nitride   |
| thickness                                   | 500 nm / 600 nm   |
| <b>Au bump (substrate connected to VSS)</b> |   |
| material                                    | > 99.9 % pure Au  |
| hardness                                    | 35 to 80 HV 0.005   |
| shear strength                              | > 70 MPa  |
| height                                      | 18 $\mu\text{m}$  |
| height uniformity                           | within a die = $\pm 2 \mu\text{m}$  |
|   | within a wafer = $\pm 3 \mu\text{m}$  |
|   | wafer to wafer = $\pm 4 \mu\text{m}$  |
| flatness                                    | minimum = $\pm 1.5 \mu\text{m}$   |
| size  | LA, LB, VSS, TEST <sup>[2]</sup> = 66 $\mu\text{m}$ $\times$ 66 $\mu\text{m}$         |
| size variation                              | $\pm 5 \mu\text{m}$   |
| under bump metallization                    | sputtered TiW   |

[1] The step size and the gap between chips may vary due to changing foil expansion

[2] Pads VSS and TESTIO are disconnected when wafer is sawn.

## 15.1 Fail die identification

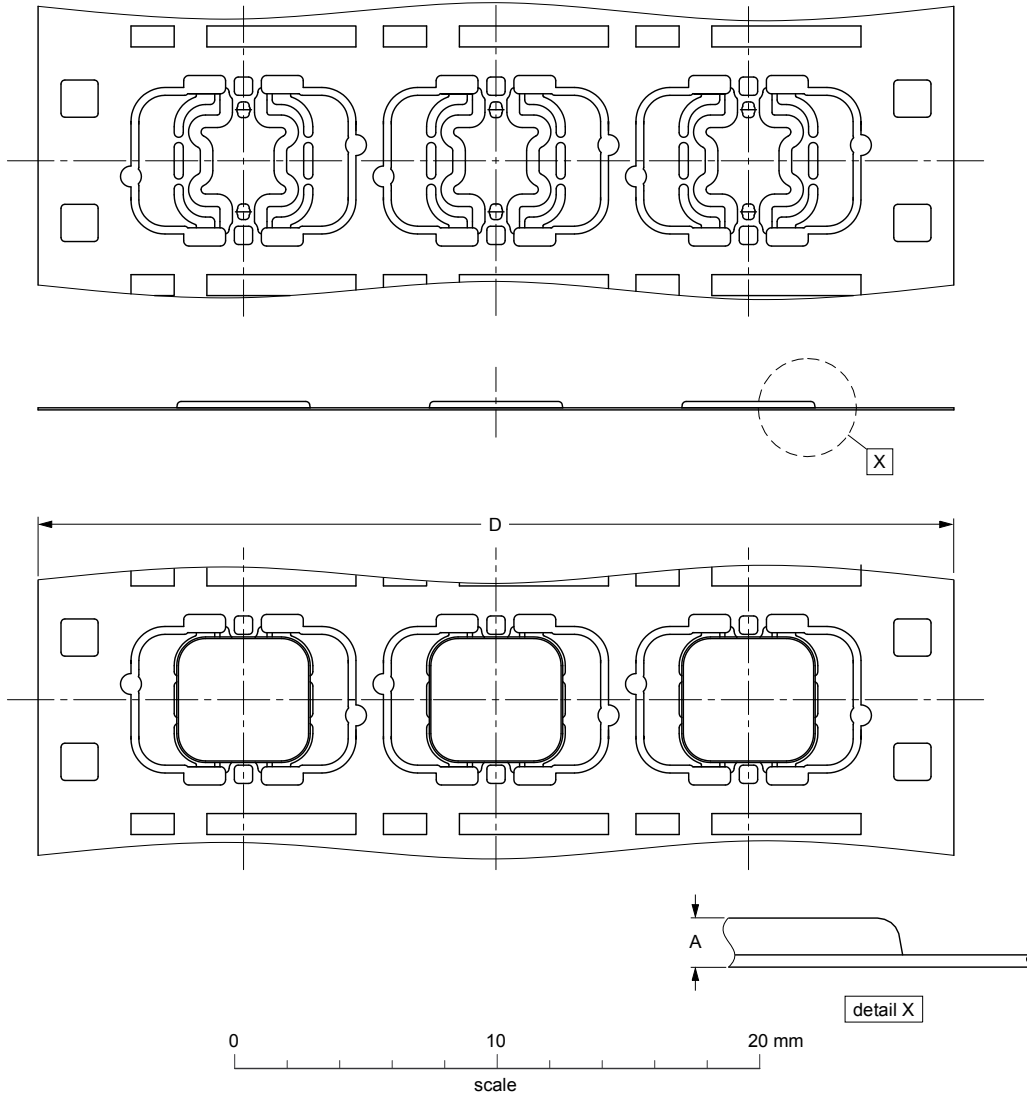
Electronic wafer mapping covers the electrical test results and additionally the results of mechanical/visual inspection. No ink dots are applied.

## 15.2 Package outline

For more details on the contactless modules MOA4 and MOA8 please refer to [Ref. 7](#) and [Ref. 8](#).

PLLMC: plastic leadless module carrier package; 35 mm wide tape

SOT500-2



**DIMENSIONS (mm are the original dimensions)**

| UNIT | A <sup>(1)</sup><br>max. | D              | For unspecified dimensions see PLLMC-drawing given in the subpackage code. |
|------|--------------------------|----------------|--|
| mm   | 0.33                     | 35.05<br>34.95 |  |

**Note**

1. Total package thickness, exclusive punching burr.

| OUTLINE<br>VERSION | REFERENCES |       |       | EUROPEAN<br>PROJECTION | ISSUE DATE           |
|--------------------|------------|-------|-------|------------------------|----------------------|
|                    | IEC        | JEDEC | JEITA |                        |                      |
| SOT500-2           | ---        | ---   | ---   |                        | 03-09-17<br>06-05-22 |

Figure 23. Package outline SOT500-2

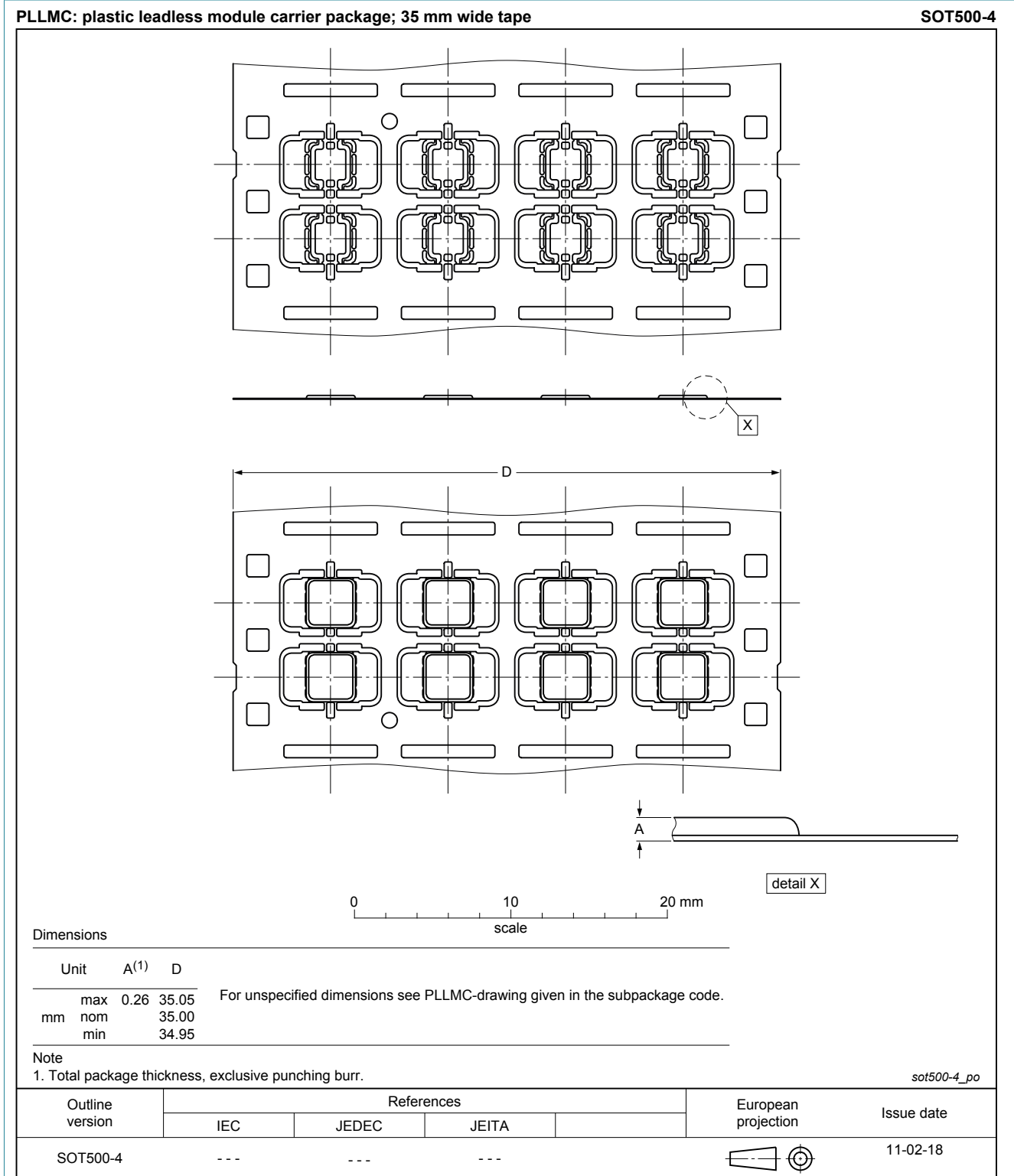
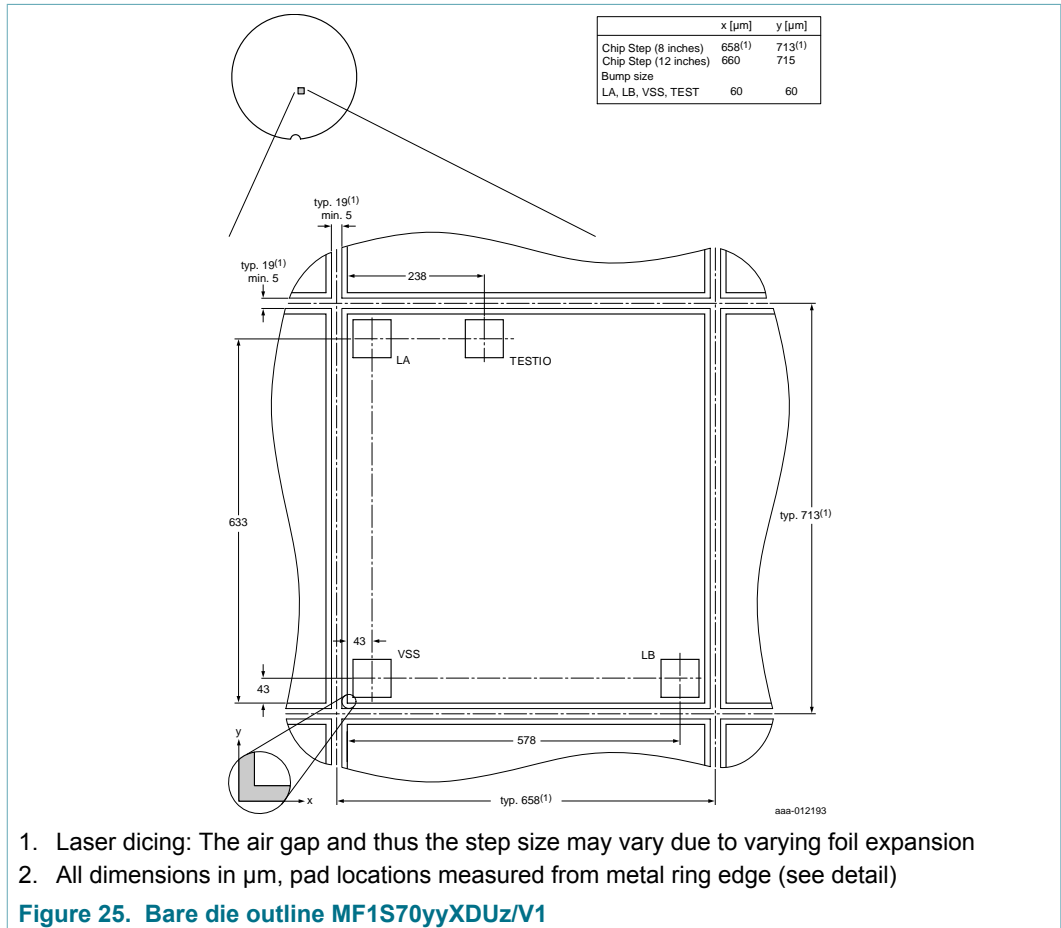


Figure 24. Package outline SOT500-4

## 16 Bare die outline

For more details on the wafer delivery forms, see [Ref. 9](#).



## 17 Abbreviations

Table 33. Abbreviations and symbols

| Acronym | Description  |
|---------|--|
| ACK     | ACKnowledge  |
| ATQA    | Answer To reQuest, Type A                                    |
| CRC     | Cyclic Redundancy Check                                      |
| CT      | Cascade Tag (value 88h) as defined in ISO/IEC 14443-3 Type A |
| EEPROM  | Electrically Erasable Programmable Read-Only Memory          |
| FDT     | Frame Delay Time   |
| FFC     | Film Frame Carrier   |
| IC      | Integrated Circuit   |
| LCR     | L = inductance, Capacitance, Resistance (LCR meter)          |
| LSB     | Least Significant Bit  |

| Acronym | Description  |
|---------|--|
| NAK     | Not AcKnowledge                                      |
| NUID    | Non-Unique IDentifier                                |
| NV      | Non-Volatile memory                                  |
| PCD     | Proximity Coupling Device (Contactless Reader)       |
| PICC    | Proximity Integrated Circuit Card (Contactless Card) |
| REQA    | REQuest command, Type A                              |
| RID     | Random ID  |
| RF      | Radio Frequency                                      |
| RMS     | Root Mean Square                                     |
| RNG     | Random Number Generator                              |
| SAK     | Select AcKnowledge, type A                           |
| SECS-II | SEMI Equipment Communications Standard part 2        |
| TiW     | Titanium Tungsten                                    |
| UID     | Unique IDentifier                                    |
| WUPA    | Wake-Up Protocol type A                              |

## 18 References

[1]

### MIFARE (Card) Coil Design Guide

Application note, BU-ID Document number 0117\*\*<sup>1</sup>

[2]

### MIFARE Type Identification Procedure

Application note, BU-ID Document number 0184\*\*<sup>1</sup>

[3]

### ISO/IEC 14443-2

2001

[4]

### ISO/IEC 14443-3

2001

[5]

### MIFARE & I-CODE CLRC632 Multiple protocol contactless reader IC

Product data sheet

[6]

### MIFARE and handling of UIDs

<sup>1</sup> \*\* ... document version number



Application note, BU-ID Document number 1907\*\*<sup>1</sup>

[7]

**Contactless smart card module specification MOA4**

Delivery Type Description, BU-ID Document number 0823\*\*<sup>1</sup>

[8]

**Contactless smart card module specification MOA8**

Delivery Type Description, BU-ID Document number 1636\*\*<sup>1</sup>

[9]

**General specification for 8" wafer on UV-tape with electronic fail die marking; delivery types**

Delivery Type Description, BU-ID Document number 1093\*\*<sup>1</sup>

## 19 Revision history

Table 34. Revision history

| Document ID        | Release date   | Data sheet status  | Change notice | Supersedes         |
|--------------------|--|--------------------|---------------|--------------------|
| MF1S70yyX_V1 v.3.2 | 20171127   | Product data sheet | -             | MF1S70yyX_V1 v.3.1 |
| Modifications:     | <ul style="list-style-type: none"> <li>• 12 inch FFC delivery forms added</li> <li>• Format updated</li> </ul>   |                    |               |                    |
| MF1S70yyX_V1 v.3.1 | 20140908   | Product data sheet | -             | MF1S70yyX_V1 v.3.0 |
| Modifications:     | <ul style="list-style-type: none"> <li>• NXP originality check support only for 1 kB memory version</li> <li>• Wafer delivery specification reference corrected</li> </ul> |                    |               |                    |
| MF1S70yyX_V1 v.3.0 | 20140303   | Product data sheet | -             | -                  |

## 20 Legal information

### 20.1 Data sheet status

| Document status <sup>[1][2]</sup> | Product status <sup>[3]</sup> | Definition  |
|-----------------------------------|-------------------------------|---|
| Objective [short] data sheet      | Development                   | This document contains data from the objective specification for product development. |
| Preliminary [short] data sheet    | Qualification                 | This document contains data from the preliminary specification.                       |
| Product [short] data sheet        | Production                    | This document contains the product specification.                                     |

- [1] Please consult the most recently issued document before initiating or completing a design.
- [2] The term 'short data sheet' is explained in section "Definitions".
- [3] The product status of device(s) described in this document may have changed since this document was published and may differ in case of multiple devices. The latest product status information is available on the Internet at URL <http://www.nxp.com>.

### 20.2 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.

**Short data sheet** — A short data sheet is an extract from a full data sheet with the same product type number(s) and title. A short data sheet is intended for quick reference only and should not be relied upon to contain detailed and full information. For detailed and full information see the relevant full data sheet, which is available on request via the local NXP Semiconductors sales office. In case of any inconsistency or conflict with the short data sheet, the full data sheet shall prevail.

**Product specification** — The information and data provided in a Product data sheet shall define the specification of the product as agreed between NXP Semiconductors and its customer, unless NXP Semiconductors and customer have explicitly agreed otherwise in writing. In no event however, shall an agreement be valid in which the NXP Semiconductors product is deemed to offer functions and qualities beyond those described in the Product data sheet.

### 20.3 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. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors. 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 and its suppliers accept 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.

**Limiting values** — Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) will cause permanent damage to the device. Limiting values are stress ratings only and (proper) operation of the device at these or any other conditions above those given in the Recommended operating conditions section (if present) or the Characteristics sections of this document is not warranted. Constant or repeated exposure to limiting values will permanently and irreversibly affect the quality and reliability of the device.

**Terms and conditions of commercial sale** — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at <http://www.nxp.com/profile/terms>, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

**No offer to sell or license** — Nothing in this document may be interpreted or construed as an offer to sell products that is open for acceptance or the grant, conveyance or implication of any license under any copyrights, patents or other industrial or intellectual property rights.

---

**MIFARE Classic EV1 4K - Mainstream contactless smart card IC for fast and easy solution development**

**Quick reference data** — The Quick reference data is an extract of the product data given in the Limiting values and Characteristics sections of this document, and as such is not complete, exhaustive or legally binding.

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

**Non-automotive qualified products** — Unless this data sheet expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications. In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP

Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

**Translations** — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

## 20.4 Trademarks

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

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

**MIFARE Classic** — is a trademark of NXP B.V.

## Tables

|          |   |    |          |   |    |
|----------|---|----|----------|---|----|
| Tab. 1.  | Quick reference data .....                                  | 2  | Tab. 18. | SET_MOD_TYPE timing .....                             | 20 |
| Tab. 2.  | Ordering information .....                                  | 3  | Tab. 19. | Load Modulation Status Indication .....               | 20 |
| Tab. 3.  | Pin allocation table .....                                  | 4  | Tab. 20. | MIFARE authentication command .....                   | 21 |
| Tab. 4.  | Value block format example .....                            | 10 | Tab. 21. | MIFARE authentication timing .....                    | 21 |
| Tab. 5.  | Memory operations .....                                     | 10 | Tab. 22. | MIFARE Read command .....                             | 22 |
| Tab. 6.  | Access conditions .....                                     | 11 | Tab. 23. | MIFARE Read timing .....                              | 22 |
| Tab. 7.  | Access conditions for the sector trailer .....              | 12 | Tab. 24. | MIFARE Write command .....                            | 23 |
| Tab. 8.  | Access conditions for data blocks .....                     | 13 | Tab. 25. | MIFARE Write timing .....                             | 23 |
| Tab. 9.  | Command overview .....                                      | 13 | Tab. 26. | MIFARE Increment, Decrement and Restore command ..... | 25 |
| Tab. 10. | MIFARE ACK and NAK .....                                    | 15 | Tab. 27. | MIFARE Increment, Decrement and Restore timing .....  | 25 |
| Tab. 11. | ATQA response of the MF1S70yyX/V1 .....                     | 16 | Tab. 28. | MIFARE Transfer command .....                         | 26 |
| Tab. 12. | SAK response of the MF1S70yyX/V1 .....                      | 16 | Tab. 29. | MIFARE Transfer timing .....                          | 26 |
| Tab. 13. | Personalize UID Usage command .....                         | 17 | Tab. 30. | Limiting values .....                                 | 26 |
| Tab. 14. | Personalize UID Usage timing .....                          | 18 | Tab. 31. | Characteristics .....                                 | 27 |
| Tab. 15. | Available activation sequences for 7-byte UID options ..... | 18 | Tab. 32. | Wafer specifications MF1S70yyXDUy .....               | 27 |
| Tab. 16. | Input parameter to MIFARE Classic Authenticate .....        | 18 | Tab. 33. | Abbreviations and symbols .....                       | 31 |
| Tab. 17. | SET_MOD_TYPE command .....                                  | 19 | Tab. 34. | Revision history .....                                | 33 |

## Figures

|          |   |    |          |   |    |
|----------|---|----|----------|---|----|
| Fig. 1.  | Contactless MIFARE system .....                             | 1  | Fig. 14. | Byte Location of Load Modulation Status in Block 0 / Sector 0 ..... | 20 |
| Fig. 2.  | Block diagram of MF1S70yyX/V1 .....                         | 3  | Fig. 15. | MIFARE Authentication part 1 .....                                  | 20 |
| Fig. 3.  | Pin configuration for SOT500-2 (MOA4) .....                 | 4  | Fig. 16. | MIFARE Authentication part 2 .....                                  | 21 |
| Fig. 4.  | MIFARE Classic command flow diagram .....                   | 6  | Fig. 17. | MIFARE Read .....   | 22 |
| Fig. 5.  | Memory organization .....                                   | 8  | Fig. 18. | MIFARE Write part 1 .....   | 23 |
| Fig. 6.  | Manufacturer block for MF1S503yX with 4-byte NUID .....     | 9  | Fig. 19. | MIFARE Write part 2 .....   | 23 |
| Fig. 7.  | Manufacturer block for MF1S500yX with 7-byte UID .....      | 9  | Fig. 20. | MIFARE Increment, Decrement, Restore part 1 .....                   | 24 |
| Fig. 8.  | Value blocks .....  | 9  | Fig. 21. | MIFARE Increment, Decrement, Restore part 2 .....                   | 24 |
| Fig. 9.  | Sector trailer .....  | 10 | Fig. 22. | MIFARE Transfer .....   | 26 |
| Fig. 10. | Access conditions .....                                     | 12 | Fig. 23. | Package outline SOT500-2 .....                                      | 29 |
| Fig. 11. | Frame Delay Time (from PCD to PICC) and TACK and TNAK ..... | 15 | Fig. 24. | Package outline SOT500-4 .....                                      | 30 |
| Fig. 12. | Personalize UID Usage .....                                 | 17 | Fig. 25. | Bare die outline MF1S70yyXDUz/V1 .....                              | 31 |
| Fig. 13. | SET_MOD_TYPE .....  | 19 |          |   |    |

## Contents

|           |  |           |           |                                  |           |
|-----------|--|-----------|-----------|----------------------------------|-----------|
| <b>1</b>  | <b>General description</b> .....               | <b>1</b>  | <b>13</b> | <b>Limiting values</b> .....     | <b>26</b> |
| 1.1       | Anticollision .....                            | 1         | <b>14</b> | <b>Characteristics</b> .....     | <b>27</b> |
| 1.2       | Simple integration and user convenience .....  | 1         | <b>15</b> | <b>Wafer specification</b> ..... | <b>27</b> |
| 1.3       | Security and privacy .....                     | 1         | 15.1      | Fail die identification .....    | 28        |
| 1.4       | Delivery options .....                         | 1         | 15.2      | Package outline .....            | 28        |
| <b>2</b>  | <b>Features and benefits</b> .....             | <b>2</b>  | <b>16</b> | <b>Bare die outline</b> .....    | <b>31</b> |
| 2.1       | EEPROM .....                                   | 2         | <b>17</b> | <b>Abbreviations</b> .....       | <b>31</b> |
| <b>3</b>  | <b>Applications</b> .....                      | <b>2</b>  | <b>18</b> | <b>References</b> .....          | <b>32</b> |
| <b>4</b>  | <b>Quick reference data</b> .....              | <b>2</b>  | <b>19</b> | <b>Revision history</b> .....    | <b>33</b> |
| <b>5</b>  | <b>Ordering information</b> .....              | <b>3</b>  | <b>20</b> | <b>Legal information</b> .....   | <b>34</b> |
| <b>6</b>  | <b>Block diagram</b> .....                     | <b>3</b>  |           |                                  |           |
| <b>7</b>  | <b>Pinning information</b> .....               | <b>4</b>  |           |                                  |           |
| 7.1       | Pinning .....                                  | 4         |           |                                  |           |
| <b>8</b>  | <b>Functional description</b> .....            | <b>4</b>  |           |                                  |           |
| 8.1       | Block description .....                        | 4         |           |                                  |           |
| 8.2       | Communication principle .....                  | 5         |           |                                  |           |
| 8.2.1     | Request standard / all .....                   | 5         |           |                                  |           |
| 8.2.2     | Anticollision loop .....                       | 5         |           |                                  |           |
| 8.2.3     | Select card .....                              | 5         |           |                                  |           |
| 8.2.4     | Three pass authentication .....                | 5         |           |                                  |           |
| 8.2.5     | Memory operations .....                        | 6         |           |                                  |           |
| 8.3       | Data integrity .....                           | 6         |           |                                  |           |
| 8.4       | Three pass authentication sequence .....       | 7         |           |                                  |           |
| 8.5       | RF interface .....                             | 7         |           |                                  |           |
| 8.6       | Memory organization .....                      | 7         |           |                                  |           |
| 8.6.1     | Manufacturer block .....                       | 8         |           |                                  |           |
| 8.6.2     | Data blocks .....                              | 9         |           |                                  |           |
| 8.6.2.1   | Value blocks .....                             | 9         |           |                                  |           |
| 8.6.3     | Sector trailer .....                           | 10        |           |                                  |           |
| 8.7       | Memory access .....                            | 10        |           |                                  |           |
| 8.7.1     | Access conditions .....                        | 11        |           |                                  |           |
| 8.7.2     | Access conditions for the sector trailer ..... | 12        |           |                                  |           |
| 8.7.3     | Access conditions for data blocks .....        | 12        |           |                                  |           |
| <b>9</b>  | <b>Command overview</b> .....                  | <b>13</b> |           |                                  |           |
| 9.1       | MIFARE Classic command overview .....          | 13        |           |                                  |           |
| 9.2       | Timings .....                                  | 14        |           |                                  |           |
| 9.3       | MIFARE Classic ACK and NAK .....               | 15        |           |                                  |           |
| 9.4       | ATQA and SAK responses .....                   | 16        |           |                                  |           |
| <b>10</b> | <b>UID Options and Handling</b> .....          | <b>16</b> |           |                                  |           |
| 10.1      | 7-byte UID Operation .....                     | 16        |           |                                  |           |
| 10.1.1    | Personalization Options .....                  | 16        |           |                                  |           |
| 10.1.2    | Anti-collision and Selection .....             | 18        |           |                                  |           |
| 10.1.3    | Authentication .....                           | 18        |           |                                  |           |
| 10.2      | 4-byte UID Operation .....                     | 18        |           |                                  |           |
| 10.2.1    | Anti-collision and Selection .....             | 19        |           |                                  |           |
| 10.2.2    | Authentication .....                           | 19        |           |                                  |           |
| <b>11</b> | <b>Load Modulation Strength Option</b> .....   | <b>19</b> |           |                                  |           |
| <b>12</b> | <b>MIFARE Classic commands</b> .....           | <b>20</b> |           |                                  |           |
| 12.1      | MIFARE Authentication .....                    | 20        |           |                                  |           |
| 12.2      | MIFARE Read .....                              | 21        |           |                                  |           |
| 12.3      | MIFARE Write .....                             | 22        |           |                                  |           |
| 12.4      | MIFARE Increment, Decrement and Restore ...    | 24        |           |                                  |           |
| 12.5      | MIFARE Transfer .....                          | 25        |           |                                  |           |

Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.

© NXP B.V. 2017.

All rights reserved.

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

For sales office addresses, please send an email to: [salesaddresses@nxp.com](mailto:salesaddresses@nxp.com)

Date of release: 23 November 2017

Document identifier: MF1S70yyX\_V1

Document number: 279332