

# MF0ICU2

## MIFARE Ultralight C - Contactless ticket IC

Rev. 3.3 — 30 July 2019

137633

Product data sheet  
COMPANY PUBLIC

## 1 General description

NXP Semiconductors has developed the MIFARE Ultralight C - Contactless ticket IC MF0ICU2 to be used in a contactless smart ticket or smart card in combination with Proximity Coupling Devices (PCD). The communication layer (MIFARE RF Interface) complies to parts 2 and 3 of the ISO/IEC 14443 Type A standard (see [Ref. 1](#) and [Ref. 2](#)).

The MF0ICU2 is primarily designed for limited use applications such as public transportation, event ticketing and loyalty applications.

### 1.1 Contactless energy and data transfer

In the MIFARE system, the MF0ICU2 is connected to a coil with a few turns. The MF0ICU2 fits for the TFC.0 (Edmonson) and TFC.1 ticket formats as defined in EN 753-2.

TFC.1 ticket formats are supported by the MF0xxU20 chip featuring an on-chip resonance capacitor of 16 pF.

The smaller TFC.0 tickets are supported by the MFxxU21 chip holding an on-chip resonance capacitor of 50 pF.

When the ticket is positioned in the proximity of the coupling device (PCD) antenna, the high speed RF communication interface allows the transmission of the data with a baud rate of 106 kbit/s.

### 1.2 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.

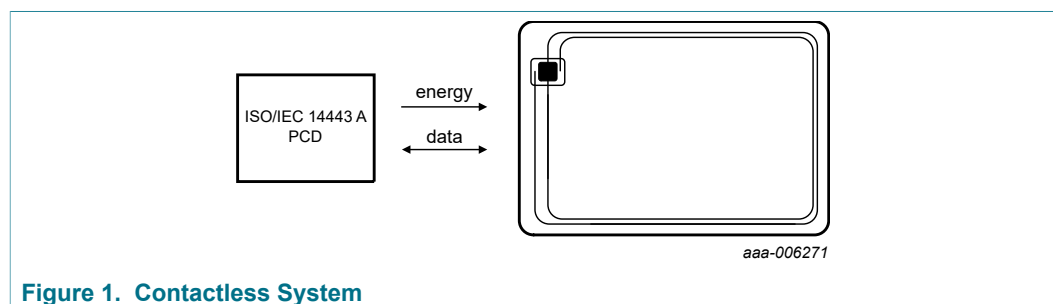


Figure 1. Contactless System

The anticollision function is based on an IC individual serial number called Unique IDentification. The UID of the MF0ICU2 is 7 bytes long and supports cascade level 2 according to ISO/IEC 14443-3.



**1.3 Security**

- 3DES Authentication
- Anti-cloning support by unique 7-byte serial number for each device
- 32-bit user programmable OTP area
- Field programmable read-only locking function per page for first 512-bit
- Read-only locking per block for the memory above 512 bit

**1.4 Naming conventions**

**Table 1. Naming conventions**

| MF0xxU2w01Dyy | Description  |
|---------------|--|
| MF            | MIFARE family  |
| 0             | Ultralight product family  |
| xx            | Two character identifier for the package type<br>IC ... bare die<br>MO ... contactless module  |
| U2            | Product: Ultralight C  |
| w             | One character identifier for input capacitance<br>0 ... 16 pF<br>1 ... 50 pF   |
| 01D           | Fixed  |
| yy            | This is a two character identifier for the package type<br>UF ... bare die, 75 µm thickness<br>UD ... bare die, 120 µm thickness<br>A4 ... MOA4 contactless module<br>A8 ... MOA8 contactless module |

**2 Features and benefits**

**2.1 MIFARE RF Interface (ISO/IEC 14443 A)**

- Contactless transmission of data and supply energy
- Operating frequency of 13.56 MHz
- Data integrity of 16-bit CRC, parity, bit coding, bit counting
- 7 byte serial number (cascade level 2 according to ISO/IEC 14443-3)
- Fast counter transaction: < 10 ms
- Operating distance up to 100 mm depending on antenna geometry and reader configuration
- Data transfer of 106 kbit/s
- True anticollision
- Typical ticketing transaction: < 35 ms

**2.2 EEPROM**

- 1536-bit total memory
- 512-bit compatible to MF0ICU1

- 36 pages, 1152-bit user r/w area
- Field programmable read-only locking function per page for first 512-bit
- 32-bit user definable One-Time Programmable (OTP) area
- Data retention of 10 years
- Field programmable read-only locking function per block
- 16-bit one-way counter
- Write endurance 100000 cycles

### 3 Quick reference data

Table 2. Characteristics

| Symbol                        | Parameter         | Conditions                            | Min       | Typ   | Max   | Unit  |
|-------------------------------|-------------------|---------------------------------------|-----------|-------|-------|-------|
| $f_i$                         | input frequency   |                                       | -         | 13.56 | -     | MHz   |
| $C_i$                         | input capacitance | 16 pF version (bare silicon and MOA4) | [1] 14.08 | 16    | 17.92 | pF    |
|                               |                   | 50 pF version                         | [1] 44    | 50    | 56    | pF    |
| <b>EEPROM characteristics</b> |                   |                                       |           |       |       |       |
| $t_{cy(W)}$                   | write cycle time  |                                       | -         | 4.1   | -     | ms    |
| $t_{ret}$                     | retention time    | $T_{amb} = 22\text{ °C}$              | 10        | -     | -     | year  |
| $N_{endu(W)}$                 | write endurance   | $T_{amb} = 22\text{ °C}$              | 100000    | -     | -     | cycle |

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

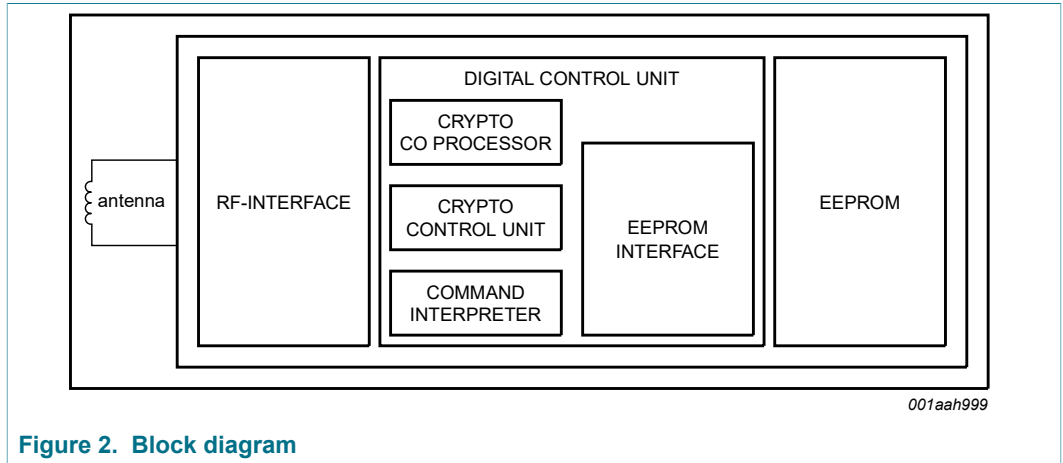
### 4 Ordering information

Table 3. Ordering information

| Type number   | Package |   |          |
|---------------|---------|---|----------|
|               | Name    | Description   | Version  |
| MF0ICU2001DUF | -       | 8 inch wafer (laser diced; 75 $\mu\text{m}$ thickness, on film frame carrier; electronic fail die marking according to SECSII format); 16 pF input capacitance  | -        |
| MF0ICU2101DUF | -       | 8 inch wafer (laser diced; 75 $\mu\text{m}$ thickness, on film frame carrier; electronic fail die marking according to SECSII format), 50pF input capacitance   | -        |
| MF0ICU2001DUD | -       | 8 inch wafer (laser diced; 120 $\mu\text{m}$ thickness, on film frame carrier; electronic fail die marking according to SECSII format); 16 pF input capacitance | -        |
| MF0ICU2101DUD | -       | 8 inch wafer (laser diced; 120 $\mu\text{m}$ thickness, on film frame carrier; electronic fail die marking according to SECSII format), 50pF input capacitance  | -        |
| MF0MOU2001DA4 | PLLMC   | MOA4 plastic leadless module carrier package; 35 mm wide tape; 16 pF input capacitance  | SOT500-2 |
| MF0MOU2101DA4 | PLLMC   | MOA4 plastic leadless module carrier package; 35 mm wide tape; 50 pF input capacitance  | SOT500-2 |
| MF0MOU2001DA8 | PLLMC   | MOA8 plastic leadless module carrier package; 35 mm wide tape; 16 pF input capacitance  | SOT500-4 |

| Type number   | Package |  |          |
|---------------|---------|--|----------|
|               | Name    | Description  | Version  |
| MF0MOU2101DA8 | PLLMC   | MOA8 plastic leadless module carrier package; 35 mm wide tape; 50 pF input capacitance | SOT500-4 |

## 5 Block diagram



## 6 Pinning information

### 6.1 Smart card contactless module

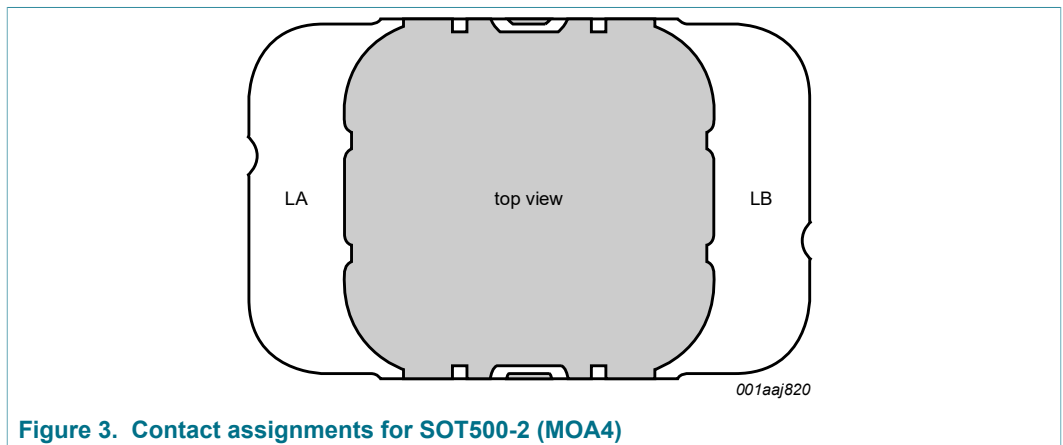


Table 4. Pin allocation table

| Antenna contacts | Symbol | Description                |
|------------------|--------|----------------------------|
| LA               | LA     | Antenna coil connection LA |
| LB               | LB     | Antenna coil connection LB |

## 7 Functional description

### 7.1 Block description

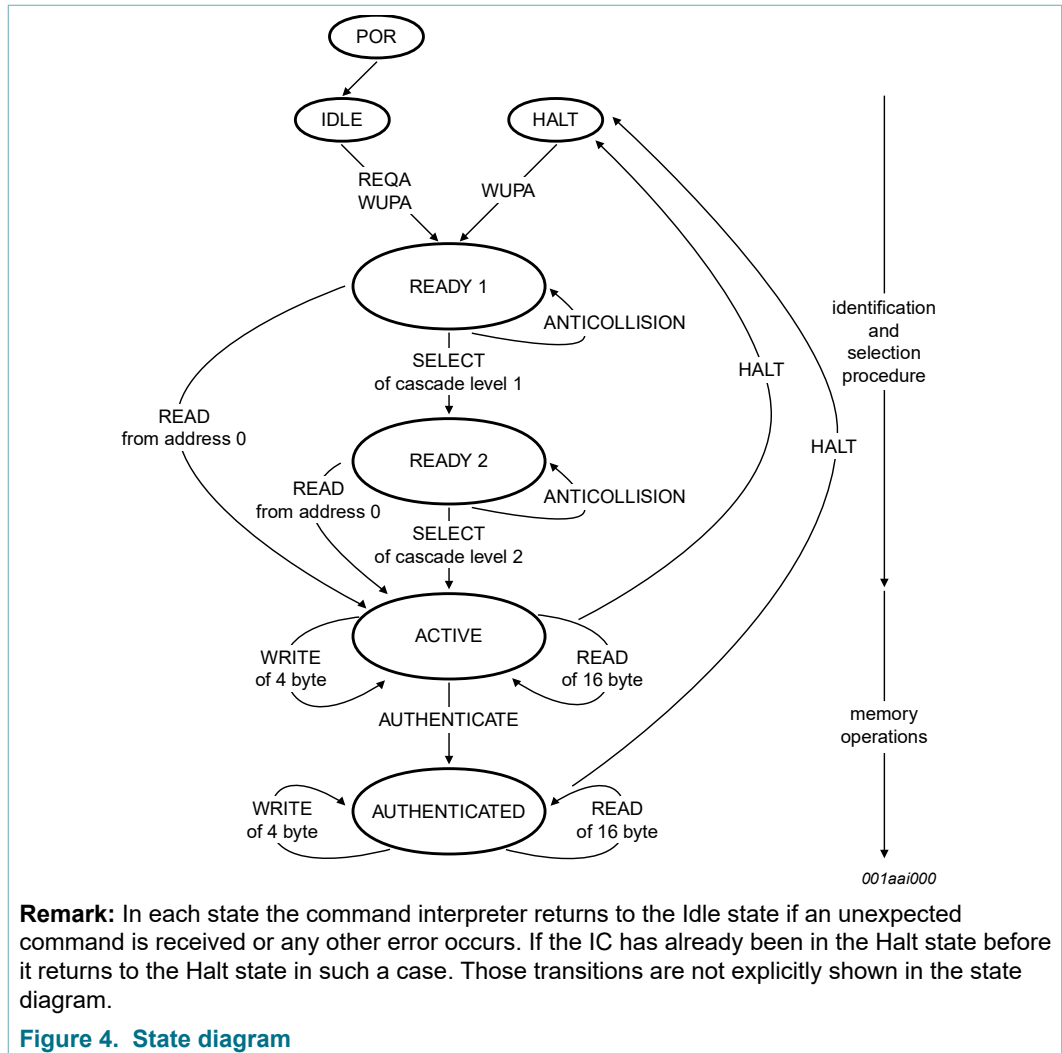
The MF0ICU2 chip consists of a 1536-bit EEPROM, an RF-Interface and the Digital Control Unit. Energy and data are transferred via an antenna, which consists of a coil with a few turns directly connected to the MF0ICU2. No further external components are necessary. For details on antenna design please refer to the document [Ref. 7](#).

- RF-Interface:
  - Modulator/Demodulator
  - Rectifier
  - Clock Regenerator
  - Power On Reset
  - Voltage Regulator
- Crypto coprocessor: Triple - Data Encryption Standard (3DES) coprocessor
- Crypto control unit: controls Crypto coprocessor operations
- Command Interpreter: Handles the commands supported by the MF0ICU2 in order to access the memory
- EEPROM-Interface
- EEPROM: The 1536 bits are organized in 48 pages with 32 bits each. 80 bits are reserved for manufacturer data. 32 bits are used for the read-only locking mechanism. 32 bits are available as OTP area. 1152 bits are user programmable read/write memory.

### 7.2 State diagram and logical states description

The commands are initiated by the PCD and controlled by the Command Interpreter of the MF0ICU2. It handles the internal states (as shown in [Figure 4](#)) and generates the appropriate response.

For a correct implementation of an anticollision procedure please refer to the documents in [Section 14](#).



7.2.1 IDLE

After Power On Reset (POR) the MF0ICU2 enters IDLE state. With a REQA or a WUPA command sent from the PCD transits to the READY1 state. Any other data received in this state is interpreted as an error and the MF0ICU2 remains waiting in the Idle state.

Please refer to [Ref. 4](#) for implementation hints for a card polling algorithm that respects relevant timing specifications from ISO/IEC 14443 Type A.

After a correctly executed HLTA command i.e. out of the ACTIVE or AUTHENTICATED state, the default waiting state changes from the IDLE state to the HALT state. This state can then be exited with a WUPA command only.

7.2.2 READY1

In the READY1 state the MF0ICU2 supports the PCD in resolving the first part of its UID (3 bytes) with the ANTICOLLISION or a cascade level 1 SELECT command.

There are two possibilities to leave this state:

- With the cascade level 1 SELECT command the PCD transits the MF0ICU2 into the READY2 state where the second part of the UID can be resolved
- With the READ (from page address 00h) command the complete anticollision mechanism may be skipped and the MF0ICU2 changes directly into the ACTIVE state

**Remark:** If more than one MF0ICU2 is in the field of the PCD, a read from address 0 will cause a collision because of the different serial numbers, but all MF0ICU2 devices will be selected.

**Remark:** Any other data received in state READY1 state is interpreted as an error and the MF0ICU2 falls back to its waiting state (IDLE or HALT, depending on its previous state).

The response of the MF0ICU2 to the cascade level 1 SELECT command is the SAK byte with value 04h. It indicates that the UID has not been complete received by the PCD yet and another anticollision level is required.

### 7.2.3 READY2

In the READY2 state the MF0ICU2 supports the PCD in resolving the second part of its UID (4 bytes) with the ANTICOLLISION command of cascade level 2. This state is left with the cascade level 2 SELECT command.

Alternatively, state READY2 state may be skipped via a READ (from block address 00h) command as described in state READY1.

**Remark:** If more than one MF0ICU2 is in the field of the PCD, a read from address 00h will cause a collision because of the different serial numbers, but all MF0ICU2 devices will be selected.

**Remark:** The response of the MF0ICU2 to the cascade level 2 SELECT command is the SAK byte with value 00h. According to ISO/IEC14443 this byte indicates whether the anticollision cascade procedure is finished (see [Ref. 6](#)). In addition it defines for the MIFARE architecture platform the type of the selected device. At this stage the MF0ICU2 is uniquely selected and only a single device will continue communication with the PCD even if other contactless devices are in the field of the PCD.

Any other command received in this state is interpreted as an error and the MF0ICU2 falls back to its waiting state (IDLE or HALT, depending on its previous state).

### 7.2.4 ACTIVE

In the ACTIVE state READ (16 bytes), WRITE (4 bytes), COMPATIBILITY WRITE (16 bytes) commands or an authentication can be performed.

After a successful authentication the state "AUTHENTICATED" is reached, see [Section 7.2.6](#).

The ACTIVE state is gratefully exited with the HLTA command and upon reception the MF0ICU2 transits to the HALT state.

Any other command received in this state is interpreted as an error and the MF0ICU2 goes back to its waiting state (IDLE or HALT, depending on its previous state).

### 7.2.5 HALT

Besides the IDLE state the HALT state constitutes the second waiting state implemented in the MF0ICU2. A MF0ICU2 that has already been processed can be set into this

state via the HLTA command. This state helps the PCD to distinguish between already processed cards and cards that have not been selected yet. The only way to get the MF0ICU2 out of this state is the WUPA command or a RF reset. Any other data received in this state is interpreted as an error and the MF0ICU2 remains in this state.

**7.2.6 AUTHENTICATED**

In the AUTHENTICATED state either a READ or a WRITE command may be performed to memory areas, which are only readable and/or writeable after authentication.

Authentication is performed using the 3DES Authentication described in [Section 7.5.5](#).

**7.3 Data integrity**

The following mechanisms are implemented in the contactless communication link between PCD and MF0ICU2 to ensure a reliable data transmission:

- 16 bits CRC per block
- Parity bit for each byte
- Bit count checking
- Bit coding to distinguish between "1", "0", and no information
- Channel monitoring (protocol sequence and bit stream analysis)

**7.4 RF interface**

The RF-interface is implemented according to the standard for contactless smart cards ISO/IEC 14443 Type A (see [Ref. 1](#) and [Ref. 2](#)).

The RF-field from the PCD is always present (with short modulation pulses when transmitting), because it is used for the power supply of the card.

For both directions of data communication there is one start bit at the beginning of each frame. Each byte is transmitted with a parity bit (odd parity) at the end. The LSBit of the byte with the lowest byte address within selected page is transmitted first. The maximum frame length is 164 bits (16 data bytes + 2 CRC bytes = 16 \* 9 + 2 \* 9 + 1 start bit + 1 end bit).

**7.5 Memory organization**

The 1536-bit EEPROM memory is organized in 48 pages with 32 bits each. In the erased state the EEPROM cells are read as a logical "0", in the written state as a logical "1".

**Table 5. Memory organization**

| Page address |            | Byte number   |             |             |             |
|--------------|------------|---------------|-------------|-------------|-------------|
| Decimal      | Hex        | 0             | 1           | 2           | 3           |
| 0            | 00h        | serial number |             |             |             |
| 1            | 01h        | serial number |             |             |             |
| 2            | 02h        | serial number | internal    | lock bytes  | lock bytes  |
| 3            | 03h        | OTP           | OTP         | OTP         | OTP         |
| 4 to 39      | 04h to 27h | user memory   | user memory | user memory | user memory |
| 40           | 28h        | lock bytes    | lock bytes  | -           | -           |



| Page address |            | Byte number                  |                |   |   |
|--------------|------------|------------------------------|----------------|---|---|
| Decimal      | Hex        | 0                            | 1              | 2 | 3 |
| 41           | 29h        | 16-bit counter               | 16-bit counter | - | - |
| 42           | 2Ah        | authentication configuration |                |   |   |
| 43           | 2Bh        | authentication configuration |                |   |   |
| 44 to 47     | 2Ch to 2Fh | authentication key           |                |   |   |

7.5.1 UID/serial number

The unique 7 byte serial number (UID) and its two Block Check Character Bytes (BCC) are programmed into the first 9 bytes of the memory. It therefore covers page 00h, page 01h and the first byte of page 02h. The second byte of page 02h is reserved for internal data. Due to security and system requirements these bytes are programmed and write-protected in the production test.

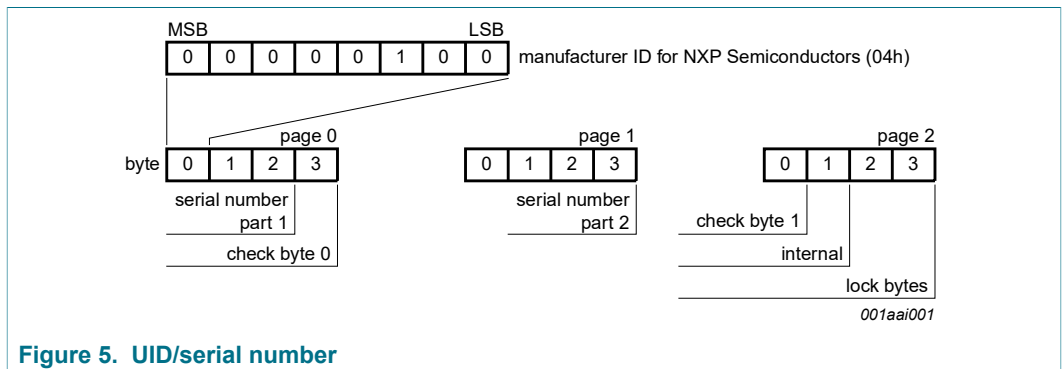


Figure 5. UID/serial number

SN0 holds the Manufacturer ID for NXP (04h) according to ISO/IEC14443-3 and ISO/IEC 7816-6 AMD.1.

According to ISO/IEC14443-3 BCC0 is defined as  $CT \oplus SN0 \oplus SN1 \oplus SN2$ . Abbreviations CT stays for Cascade Tag byte (88h) and BCC1 is defined as  $SN3 \oplus SN4 \oplus SN5 \oplus SN6$ .

7.5.2 Lock byte 0 and 1

The bits of byte 2 and byte 3 of page 02h represent the field programmable permanent read-only locking mechanism. Each page from 03h (OTP) to 0Fh can be individually locked by setting the corresponding locking bit Lx to logic 1 to prevent further write access. After locking, the corresponding locking page becomes read-only memory. To restrict read access to the memory refer to the authentication functionality (see Section 7.5.5).

The three least significant bits of lock byte 0 are the block-locking bits. Bit 2 deals with pages 0Ah to 0Fh, bit 1 deals with pages 04h to 09h and bit 0 deals with page 03h (OTP). Once the block-locking bits are set, the locking configuration for the corresponding memory area is frozen. The functionality of the bits inside the lock bytes 0 and 1 are shown in Table 6.

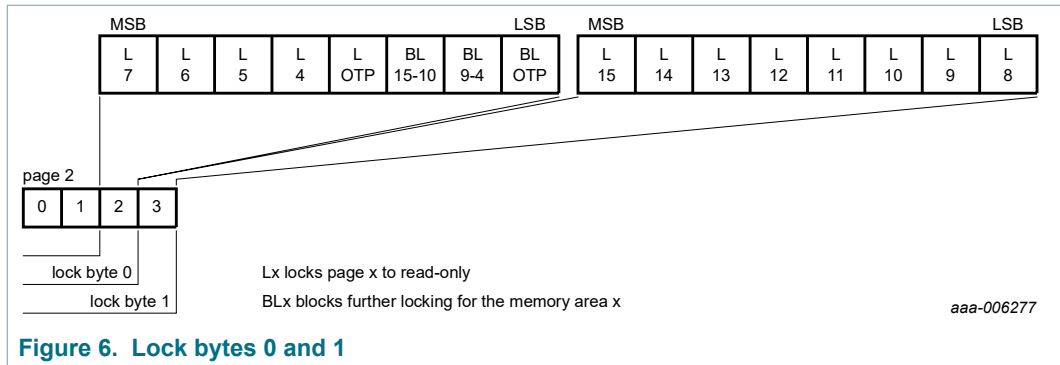


Figure 6. Lock bytes 0 and 1

For example if BL15-10 is set to logic 1, then bits L15 to L10 (lock byte 1, bit[7:2]) can no longer be changed. A WRITE command or COMPATIBILITY\_WRITE command to page 02h, sets the locking and block-locking bits. Byte 2 and byte 3 of the WRITE or COMPATIBILITY\_WRITE command, and the contents of the lock bytes are bit-wise OR'ed and the result then becomes the new content of the lock bytes. This process is irreversible. If a bit is set to logic 1, it cannot be changed back to logic 0. Therefore, before writing the lock bytes, the user has to ensure that the corresponding user memory area and/or configuration bytes to be locked are correctly written.

The contents of bytes 0 and 1 of page 02h are unaffected by the corresponding data bytes of the WRITE (see Section 9.3) or COMPATIBILITY\_WRITE (see Section 9.4) command.

The default value of the static lock bytes is 00 00h.

For compatibility reasons, the first 512 bits of the memory area have the same functionality as the MIFARE Ultralight MF0ICU1 (see also Ref. 8), meaning that the two lock bytes used for the configuration of this memory area have identical functionality. The mapping of single lock bits to memory area for the first 512 bits is shown in Figure 6 and Table 6.

Table 6. Functionality of lock bits in lock byte 0 and 1

| Lock Byte | Bit | Function      | Block Locking in Lock Byte | Block Locking in Bit |
|-----------|-----|---------------|----------------------------|----------------------|
| 0         | 3   | lock OTP page | 0                          | 0                    |
| 0         | 4   | lock page 4   | 0                          | 1                    |
| 0         | 5   | lock page 5   | 0                          | 1                    |
| 0         | 6   | lock page 6   | 0                          | 1                    |
| 0         | 7   | lock page 7   | 0                          | 1                    |
| 1         | 0   | lock page 8   | 0                          | 1                    |
| 1         | 1   | lock page 9   | 0                          | 1                    |
| 1         | 2   | lock page 10  | 0                          | 2                    |
| 1         | 3   | lock page 11  | 0                          | 2                    |
| 1         | 4   | lock page 12  | 0                          | 2                    |
| 1         | 5   | lock page 13  | 0                          | 2                    |
| 1         | 6   | lock page 14  | 0                          | 2                    |
| 1         | 7   | lock page 15  | 0                          | 2                    |

Any write operation to the lock bytes 0 and 1, features anti-tearing support.

**Remark:** The configuration written in the lock bytes is valid upon the next REQA or WUPA command.

### 7.5.3 Lock byte 2 and 3

To lock the pages of the MF0UL21 starting at page address 10h onwards, the lock bytes 2 and 3 located in page 28h (byte 0 and 1 as shown in [Figure 7](#)) are used. Those two lock bytes cover the memory area of 96 data bytes in pages 10h (16d) to 27h (39d) and the configuration area from page address 28h onwards. The granularity is 4 pages, compared to a single page for the first 512 bits as shown in [Figure 7](#). The functionality of the bits inside the lock bytes 2 and 3 are shown in [Table 7](#).

**Remark:** Set all bits marked with RFUI to 0, when writing to the lock bytes.

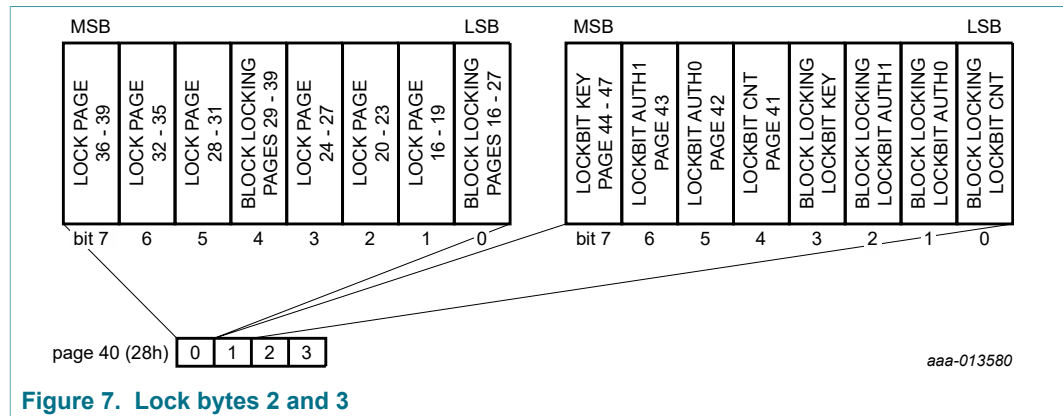


Figure 7. Lock bytes 2 and 3

The default value of lock bytes 2 and 3 is 00 00h. The value of byte 3 on page 28h (see [Figure 7](#)) is always BDh when read.

The contents of bytes 2 and 3 of page 28h are unaffected by the corresponding data bytes of the WRITE (see [Section 9.3](#)) or COMPATIBILITY\_WRITE (see [Section 9.4](#)) command.

Table 7. Functionality of lock bits in lock byte 2 and 3

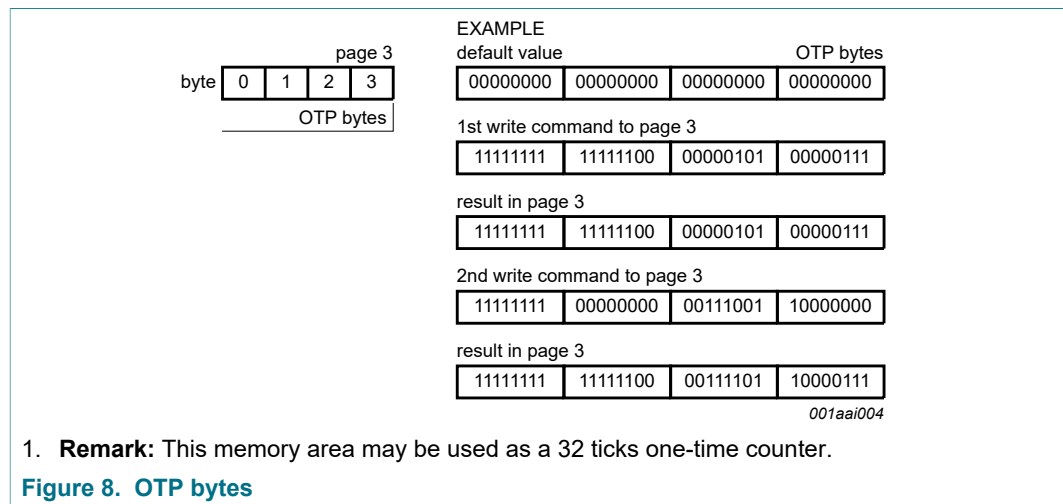
| Lock Byte | Bit | Function        | Block Locking in Lock Byte | Block Locking in Bit |
|-----------|-----|-----------------|----------------------------|----------------------|
| 2         | 1   | lock page 16-19 | 2                          | 0                    |
| 2         | 2   | lock page 20-23 | 2                          | 0                    |
| 2         | 3   | lock page 24-27 | 2                          | 0                    |
| 2         | 5   | lock page 28-31 | 2                          | 4                    |
| 2         | 6   | lock page 32-35 | 2                          | 4                    |
| 2         | 7   | lock page 36-39 | 2                          | 4                    |
| 3         | 4   | lock Counter    | 3                          | 0                    |
| 3         | 5   | lock AUTH0      | 3                          | 1                    |
| 3         | 6   | lock AUTH1      | 3                          | 2                    |
| 3         | 7   | lock Key        | 3                          | 3                    |

Any write operation to the lock bytes 2 and 3, features anti-tearing support.

**Remark:** The configuration written in the lock bytes is valid upon the next REQA or WUPA command.

**7.5.4 OTP bytes**

Page 3 is the OTP page. It is preset to all "0" after production. These bytes may be bit-wise modified by the WRITE or COMPATIBILITY WRITE command.



1. **Remark:** This memory area may be used as a 32 ticks one-time counter.

**Figure 8. OTP bytes**

The bytes of the WRITE command and the current contents of the OTP bytes are bit-wise "OR-ed" and the result forms the new content of the OTP bytes. This process is irreversible. If a bit is set to "1", it cannot be changed back to "0" again.

The default value of the OTP bytes is 00 00 00 00h.

Any write operation to the OTP bytes features anti-tearing support.

**7.5.5 3DES Authentication**

The 3DES Authentication implemented in the MF0ICU2 proves that two entities hold the same secret and each entity can be seen as a reliable partner for onwards communication. The applied encryption algorithm ek() is the 2 key 3DES encryption (see [Ref. 9](#)) in Cipher-Block Chaining (CBC) mode as described in ISO/IEC 10116 (see [Ref. 10](#)). The Initial Value (IV) of the first encryption of the protocol is the all zero block. For the subsequent encryptions the IV consists of the last ciphertext block.

The following table shows the communication flow during authentication:

**Table 8. 3DES authentication**

| # | PCD  | Data exchanged             | PICC   |
|---|--|----------------------------|--------|
| 1 | The reader device is always the entity which starts an authentication procedure. This is done by sending the command AUTHENTICATE. | "1Ah"<br>→<br>AUTHENTICATE | Step 1 |

| # | PCD   | Data exchanged                                   | PICC  |        |
|---|---|--|---|--------|
| 2 |   | ←<br>"AFh"   <br>8 bytes<br>$ek(RndB)$           | The PICC generates a 8 byte random number $RndB$ . This random number is <b>en</b> ciphered with the key, denoted by $ek(RndB)$ , and is then transmitted to the PCD.   |        |
| 3 | The PCD itself generates a 8 byte random number $RndA$ . This $RndA$ is concatenated with $RndB'$ and <b>en</b> ciphered with the key. $RndB'$ is generated by rotating the original $RndB$ left by 8 bits. This token $ek(RndA    RndB')$ is sent to the PICC. | →<br>"AFh"   <br>16 bytes<br>$ek(RndA    RndB')$ |   |        |
| 4 |   | ←<br>"00h"   <br>8 bytes<br>$ek(RndA')$          | The PICC runs an <b>de</b> cipherment on the received token and thus gains $RndA + RndB'$ . The PICC can now verify the sent $RndB'$ by comparing it with the $RndB'$ obtained by rotating the original $RndB$ left by 8 bits internally.<br><br>A successful verification proves to the PICC that the PICC and the PCD posses the same secret key.<br><br>If the verification fails, the PICC stops the authentication procedure and returns an error message.<br><br>As the PICC also received the random number $RndA$ , generated by the PCD, it can perform a rotate left operation by 8 bits on $RndA$ to gain $RndA'$ , which is <b>en</b> ciphered again, resulting in $ek(RndA')$ . This token is sent to the PCD. | Step 2 |
| 5 | The PCD runs a <b>de</b> cipherment on the received $ek(RndA')$ and thus gains $RndA'$ for comparison with the PCD-internally rotated $RndA'$ .<br><br>If the comparison fails, the PCD exits the procedure and may halt the PICC.                              |  |   |        |
| 6 |   |  | The PICC sets the state to authenticate.  |        |

The cryptographic method is based on 3DES in CBC mode.

See command details in [Section 9.5](#). The used key is a double length DES Key; where the parity bits are not checked or used.

### 7.5.6 3DES Authentication example

A numerical example of a 3DES authentication process is shown below in [Table 9](#). The key used in the example has a value of 49454D4B41455242214E4143554F5946h.

Table 9. Numerical 3DES authentication example

| # | PCD                                | Data exchanged | PICC |
|---|------------------------------------|----------------|------|
| 1 | start the authentication procedure | →<br>1Ah       |      |

| # | PCD   | Data exchanged                              | PICC   |
|---|---|---|--|
| 2 |   | ←<br>AF577293FD2F34CA51                     | generate RndB = 51E764602678DF2B<br>IV = 0000000000000000<br>ek(RndB) = 577293FD2F34CA51   |
| 3 | decipher ek(RndB) to retrieve RndB<br>generate RndA = A8AF3B256C75ED40<br>RndB' = E764602678DF2B51<br>RndA+RndB' =<br>A8AF3B256C75ED40E764602678DF2B51<br>IV = 577293FD2F34CA51<br>ek(RndA+RndB') =<br>0A638559FC7737F9F15D7862EBBE967A | →<br>AF0A638559FC7737F9<br>F15D7862EBBE967A |  |
| 4 |   | ←<br>003B884FA07C137CE1                     | decipher ek(RndA+RndB') to retrieve RndA<br>verify RndB'<br>RndA'=AF3B256C75ED40A8<br>IV = F15D7862EBBE967A<br>ek(RndA')= 3B884FA07C137CE1 |
| 5 | decipher and verify ek(RndA')   |   |  |

### 7.5.7 Programming of 3DES key to memory

The 16 bytes of the 3DES key are programmed to memory pages from 2Ch to 2Fh. The keys are stored in memory as shown in [Table 10](#). The key itself can be written during personalization or at any later stage using the WRITE (see [Section 9.3](#)) or COMPATIBILITY WRITE (see [Section 9.4](#)) command. For both commands, Byte 0 is always sent first.

**Table 10. Key memory configuration**

| Byte address |         | 0h        | 1h        | 2h        | 3h        |
|--------------|---------|-----------|-----------|-----------|-----------|
| Page address |         | Byte 0    | Byte 1    | Byte 2    | Byte 3    |
| 2Ch          | Page 44 | Key1 / K0 | Key1 / K1 | Key1 / K2 | Key1 / K3 |
| 2Dh          | Page 45 | Key1 / K4 | Key1 / K5 | Key1 / K6 | Key1 / K7 |
| 2Eh          | Page 46 | Key2 / K0 | Key2 / K1 | Key2 / K2 | Key2 / K3 |
| 2Fh          | Page 47 | Key2 / K4 | Key2 / K5 | Key2 / K6 | Key2 / K7 |

On example of Key1 = 0001020304050607h and Key2 = 08090A0B0C0D0E0Fh, the command sequence needed for key programming with WRITE command is:

- A2 2C 07 06 05 04 CRC
- A2 2D 03 02 01 00 CRC
- A2 2E 0F 0E 0D 0C CRC
- A2 2F 0B 0A 09 08 CRC

The memory content after those (COMPATIBILITY) WRITE commands is shown in [Table 11](#).

Table 11. Memory content based on example configuration

| Byte address |         | 0h     | 1h     | 2h     | 3h     |
|--------------|---------|--------|--------|--------|--------|
| Page address |         | Byte 0 | Byte 1 | Byte 2 | Byte 3 |
| 2Ch          | Page 44 | 07     | 06     | 05     | 04     |
| 2Dh          | Page 45 | 03     | 02     | 01     | 00     |
| 2Eh          | Page 46 | 0F     | 0E     | 0D     | 0C     |
| 2Fh          | Page 47 | 0B     | 0A     | 09     | 08     |

The memory pages holding the authentication key can never be read, independent of the configuration.

**Remark:** A re-programmed authentication key is only valid for authentication after a RF reset or a re-activation.

### 7.5.8 Configuration for memory access via 3DES Authentication

The behavior of the memory access rights depending on the authentication is configured with two configuration bytes, AUTH0 and AUTH1, located in pages 2Ah and 2Bh. Both configuration bytes are located in Byte 0 of the respective pages (see also [Table 5](#)).

- AUTH0 defines the page address from which the authentication is required. Valid address values for byte AUTH0 are from 03h to 30h.
- Setting AUTH0 to 30h effectively disables memory protection.
- AUTH1 determines if write access is restricted or both read and write access are restricted, see [Table 12](#)

Table 12. AUTH1 bit description

| Bit    | Value | Description   |
|--------|-------|---|
| 1 to 7 | any   | ignored   |
| 0      | 1     | write access restricted, read access allowed without authentication |
|        | 0     | read and write access restricted                                    |

### 7.5.9 Data pages

The MF0ICU2 features 144 bytes of data memory. The EEPROM memory is organized in pages with 4 bytes per page. The user memory area ranges from page 04h to 27h.

**Remark:** The default content of the user memory pages 04h to 27h at delivery is not defined.

A write access to data memory is done with a WRITE (see [Section 9.3](#)) or a COMPATIBILITY WRITE (see [Section 9.4](#)) command. In both cases, 4 bytes of memory - (one page) - will be written. Write access to data memory can be permanently restricted via lock bytes (see [Section 7.5.2](#) and [Section 7.5.3](#)) and/or permanently or temporary restricted using an authentication (see [Section 7.5.5](#)).

Reading data is done using the READ command (see [Section 9.2](#)).

### 7.5.10 Initial memory configuration

The memory configuration of MF0ICU2 in delivery state is shown in [Table 13](#):

Table 13. Initial memory organization

| Page address |            | Byte number |             |             |             |
|--------------|------------|-------------|-------------|-------------|-------------|
| dec.         | hex.       | 0           | 1           | 2           | 3           |
| 0            | 00h        | SN0         | SN1         | SN2         | BCC0        |
| 1            | 01h        | SN3         | SN4         | SN5         | SN6         |
| 2            | 02h        | BCC1        | internal    | 00h         | 00h         |
| 3            | 03h        | 00h         | 00h         | 00h         | 00h         |
| 4 to 39      | 04h to 27h | not defined | not defined | not defined | not defined |
| 40           | 28h        | 00h         | 00h         | rfu         | rfu         |
| 41           | 29h        | 00h         | 00h         | rfu         | rfu         |
| 42           | 2Ah        | 30h         | rfu         | rfu         | rfu         |
| 43           | 2Bh        | 00h         | rfu         | rfu         | rfu         |
| 44           | 2Ch        | 42h         | 52h         | 45h         | 41h         |
| 45           | 2Dh        | 4Bh         | 4Dh         | 45h         | 49h         |
| 46           | 2Eh        | 46h         | 59h         | 4Fh         | 55h         |
| 47           | 2Fh        | 43h         | 41h         | 4Eh         | 21h         |

This configuration ensures that the complete memory area is available for personalization, without knowledge of the authentication key. All lock bytes are set to zero meaning that no page or functionality is locked. The Counter is set to zero.

**Remark:** It is strongly recommended to program the authentication key during personalization in a secure environment and configure the AUTH0 byte at least in a way that the key and the AUTH0 and AUTH1 bytes can only be overwritten with prior authentication. This can be achieved by setting AUTH0 to 2Ah.

7.5.11 Counter

The MF0ICU2 features a 16-bit one-way counter, located at the first two bytes of page 29h. The default counter value is 0000h.

The first<sup>1</sup> valid WRITE or COMPATIBILITY WRITE to address 29h can be performed with any value in the range between 0001h and FFFFh and corresponds to the initial counter value. Every consecutive WRITE command, which represents the increment, can contain values between 0001h and 000Fh. Upon such WRITE command and following mandatory RF reset, the value written to the address 29h is added to the counter content.

After the initial write, only the lower nibble of the first data byte is used for the increment value (0h-Fh) and the remaining part of the data is ignored. Once the counter value reaches FFFFh and an increment is performed via a valid WRITE command, the MF0ICU2 will reply a NAK. If the sum of counter value and increment is higher than FFFFh, MF0ICU2 will reply a NAK and will not increment the counter.

An increment by zero (0000h) is always possible, but does not have any impact to the counter value.

It is recommended to protect the access to the counter functionality by authentication.

An example for the counter functionality is shown in [Figure 9](#).

<sup>1</sup> The first valid write is defined as a write to a counter value of 0000h with an argument different than zero



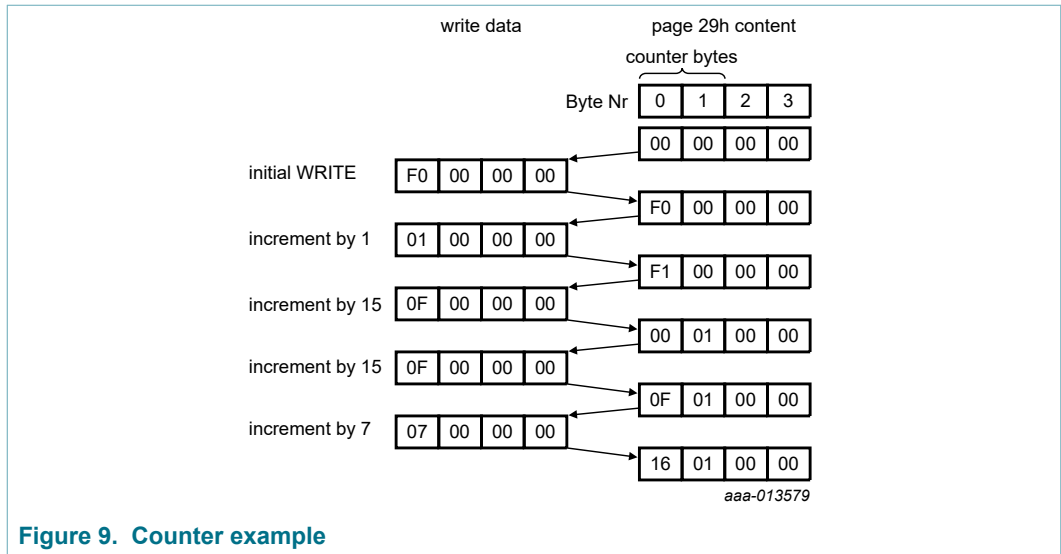


Figure 9. Counter example

## 8 Command overview

The MIFARE Ultralight C card activation follows the ISO/IEC 14443 Type A. After the MIFARE Ultralight C card has been selected, it can either be deactivated using the ISO/IEC 14443 Halt command, or the MIFARE Ultralight C commands can be performed. For more details about the card activation refer to [Ref. 2](#).

### 8.1 MIFARE Ultralight C command overview

All available commands for the MIFARE Ultralight C are shown in [Table 14](#). All memory access commands are transmitted in plain, only the AUTHENTICATE command uses 3DES encryption, see [Section 9.5](#).

Table 14. 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                    |
| READ                | -                 | 30h                        |
| WRITE               | -                 | A2h                        |
| COMPATIBILITY WRITE | -                 | A0h                        |
| AUTHENTICATE        | -                 | 1Ah                        |

All commands use the coding and framing as described in [Ref. 1](#) and [Ref. 2](#) if not otherwise specified.

### 8.2 Timings

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

All given command and response transmission 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. 2 as an integer n which specifies the PCD to PICC frame delay time. The frame delay time (FDT) from PICC to PCD is at least 87 μs which corresponds to a n=9. 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/NAK value specified in Section 8.3 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 10. For more details refer to Ref. 1 and Ref. 2.

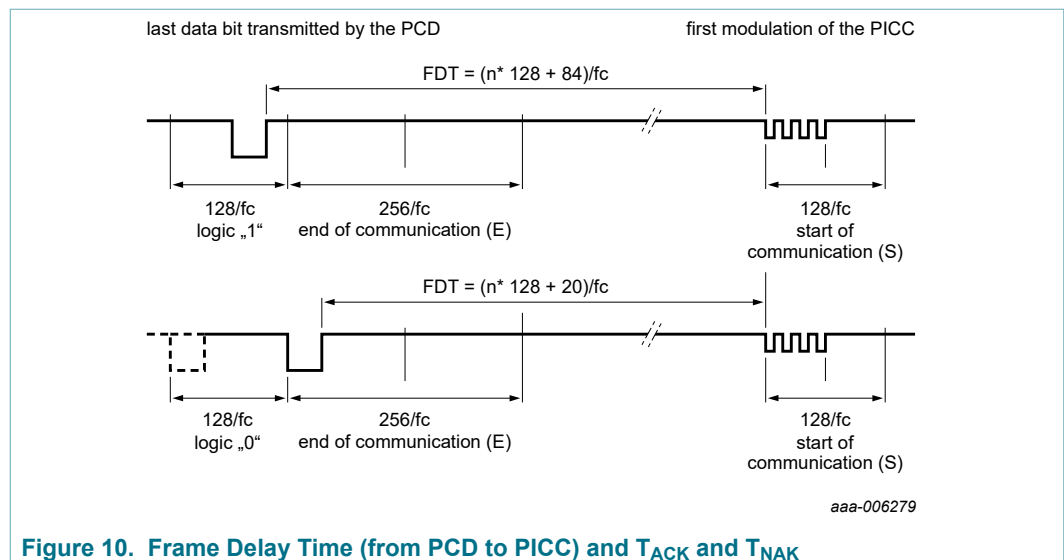


Figure 10. Frame Delay Time (from PCD to PICC) and T<sub>ACK</sub> and T<sub>NAK</sub>

**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.

### 8.3 MIFARE Ultralight C ACK and NAK

The MIFARE Ultralight C - Contactless ticket IC uses, apart from the responses defined in the following sections, two half-byte answers to acknowledge the command received in ACTIVE and AUTHENTICATED state (see Figure 4) abbreviated as ACK and NAK.

The MIFARE Ultralight C - Contactless ticket IC distinguishes between positive (ACK) and negative (NAK) acknowledge. Valid values for ACK and NAK are shown in Table 15.

Table 15. ACK and NAK values

| Answer value | Answer explanation         |
|--------------|----------------------------|
| Ah           | positive acknowledge (ACK) |

| Answer value | Answer explanation          |
|--------------|-----------------------------|
| 2h           | NAK for EEPROM write error  |
| 1h           | NAK for parity or CRC error |
| 0h           | NAK for any other error     |

After every NAK, the MF0ICU2 performs an internal reset and returns to IDLE or HALT state.

**Remark:** Any 4-bit response different from Ah shall be interpreted as NAK, although not all 4-bit values are detailed in [Table 15](#)

### 8.4 Summary of device identification data

For more details on the values below please refer to [Ref. 2](#), [Ref. 3](#) and [Ref. 4](#).

**Table 16. Summary of relevant data for device identification**

| Code                | Length | Value | Binary Format       | Remark   |
|---------------------|--------|-------|---------------------|--|
| ATQA                | 2 Byte | 0044h | 0000 0000 0100 0100 |  |
| CT                  | 1 Byte | 88h   | 1000 1000           | Cascade Tag, ensures collision with cascade level 1 products |
| SAK (casc. level 1) | 1 Byte | 04h   | 0000 0100           | '1' indicates additional cascade level                       |
| SAK (casc. level 2) | 1 Byte | 00h   | 0000 0000           | indicates complete UID and MIFARE Ultralight functionality   |
| Manufacturer Byte   | 1 Byte | 04h   | 0000 0100           | indicates NXP Semiconductors as manufacturer                 |

## 9 MIFARE Ultralight C - Contactless ticket IC commands

### 9.1 MIFARE Ultralight C - Contactless ticket IC card activation

The ATQA and SAK values are identical as for MF0ICU1 (see [Ref. 8](#)). For information on ISO 14443 card activation, see [Ref. 4](#). Summary of data relevant for device identification is given in [Section 8.4](#).

### 9.2 READ

The READ command takes the page address as a parameter. Only addresses 00h to 2Bh are decoded. For higher addresses the MF0ICU2 returns a NAK. The MF0ICU2 responds to the READ command by sending 16 bytes starting from the page address defined in the command (e.g. if ADR is 03h, pages 03h, 04h, 05h, 06h are returned). The command structure is shown in [Figure 11](#) and [Table 17](#).

[Table 18](#) shows the required timing.

A roll-over mechanism is implemented to continue reading from page 00h once the end of the accessible memory is reached. For example, reading from address 29h on a MF0ICU2 results in pages 29h, 2Ah, 2Bh and 00h being returned.

The following conditions apply if part of the memory is protected by the 3DES authentication for read access:

- if the MF0ICU2 is in the ACTIVE state
  - addressing a page which is equal or higher than AUTH0 results in a NAK response
  - addressing a page lower than AUTH0 results in data being returned with the roll-over mechanism occurring just before the AUTH0 defined page
- if the MF0ICU2 is in the AUTHENTICATED state
  - the READ command behaves like on a MF0ICU2 without access protection

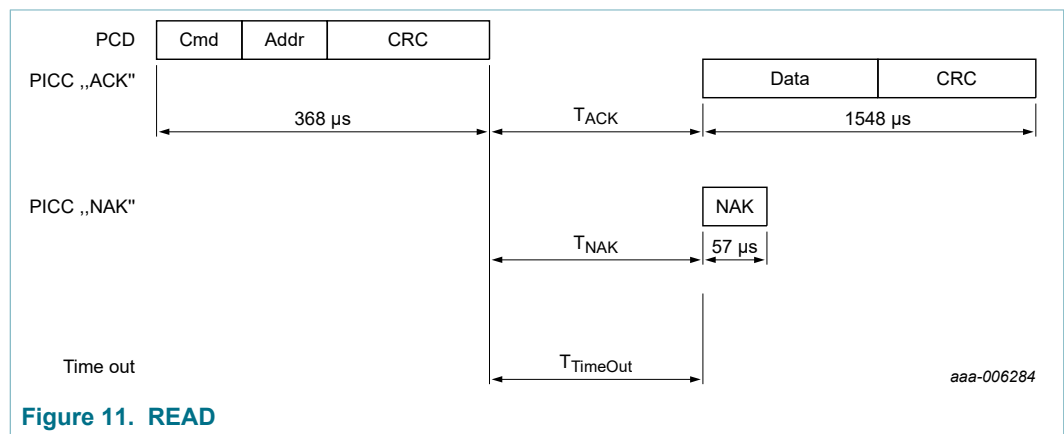


Table 17. READ command

| Name | Code                         | Description                             | Length   |
|------|------------------------------|---|----------|
| Cmd  | 30h                          | read four pages                         | 1 byte   |
| Addr | -                            | start page address '00h' to '2Bh'       | 1 byte   |
| CRC  | -                            | CRC according to <a href="#">Ref. 2</a> | 2 bytes  |
| Data | -                            | data content of the addressed pages     | 16 bytes |
| NAK  | see <a href="#">Table 15</a> | see <a href="#">Section 8.3</a>         | 4-bit    |

Table 18. READ timing

These times exclude the end of communication of the PCD.

|      | 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                 |

### 9.3 WRITE

The WRITE command is used to program the lock bytes in page 02h, the OTP bytes in page 03h, data bytes in pages 04h to 27h, configuration data from page 28h to 2B and keys from page 2Ch to 2Fh. A WRITE command is performed page-wise, programming 4 bytes in a page. The WRITE command is shown in [Figure 12](#) and [Table 19](#).

Table 20 shows the required timing.

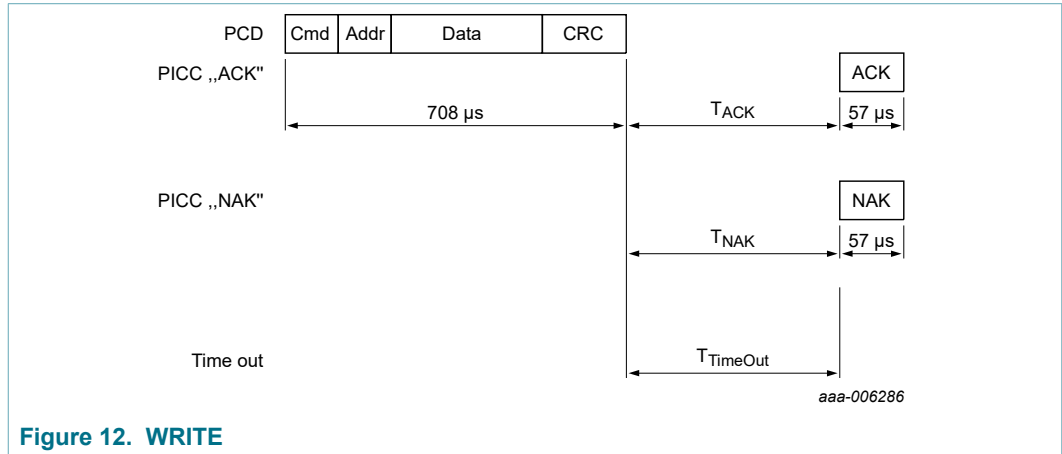


Figure 12. WRITE

Table 19. WRITE command

| Name | Code         | Description                 | Length  |
|------|--------------|-----------------------------|---------|
| Cmd  | A2h          | write one page              | 1 byte  |
| Addr | -            | page address '02h' to '2Fh' | 1 byte  |
| CRC  | -            | CRC according to Ref. 2     | 2 bytes |
| Data | -            | data                        | 4 bytes |
| NAK  | see Table 15 | see Section 8.3             | 4-bit   |

Table 20. WRITE timing

These times exclude the end of communication of the PCD.

|       | 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 | n=9                  | T <sub>TimeOut</sub> | n=9                  | T <sub>TimeOut</sub> | 10 ms                |

### 9.4 COMPATIBILITY WRITE

The COMPATIBILITY WRITE command was implemented to accommodate the established MIFARE PCD infrastructure. Even though 16 bytes are transferred to the MF0ICU2, only the least significant 4 bytes (bytes 0 to 3) will be written to the specified address. It is recommended to set the remaining bytes 4 to 15 to all '0'.

Personalization of authentication key: For writing the authentication key, one needs to write the key with four commands. The first command shall have the 4 least significant bytes of the key and shall be written on page 2Ch, the second 4 bytes shall be written on page 2Dh, the next 4 bytes shall be written on page 2Eh, the last 4 bytes shall be written on page 2Fh.

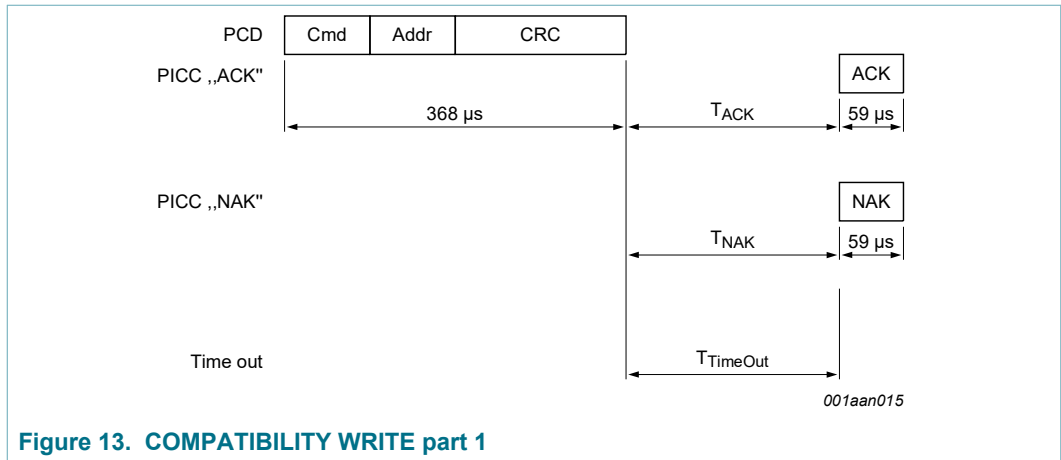


Figure 13. COMPATIBILITY WRITE part 1

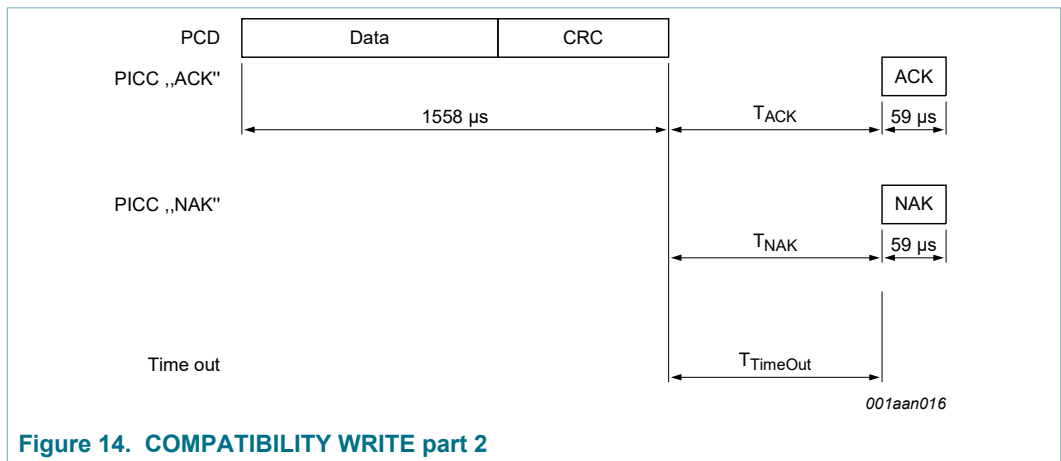


Figure 14. COMPATIBILITY WRITE part 2

Table 21. COMPATIBILITY\_WRITE command

| Name | Code                         | Description  | Length   |
|------|------------------------------|--|----------|
| Cmd  | A0h                          | compatibility write                                      | 1 byte   |
| Addr | -                            | page address '02h' to '2Fh'                              | 1 byte   |
| CRC  | -                            | CRC according to <a href="#">Ref. 2</a>                  | 2 bytes  |
| Data | -                            | 16-byte Data, only least significant 4 bytes are written | 16 bytes |
| NAK  | see <a href="#">Table 15</a> | see <a href="#">Section 8.3</a>                          | 4-bit    |

Table 22. COMPATIBILITY\_WRITE timing

These times exclude the end of communication of the PCD.

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

9.5 AUTHENTICATE

**Description:** The authentication process is detailed [Section 7.5.5](#).

The command is performed in the same protocol as READ, WRITE and COMPATIBILITY WRITE.

Executing a HALT command results in losing the authentication status.

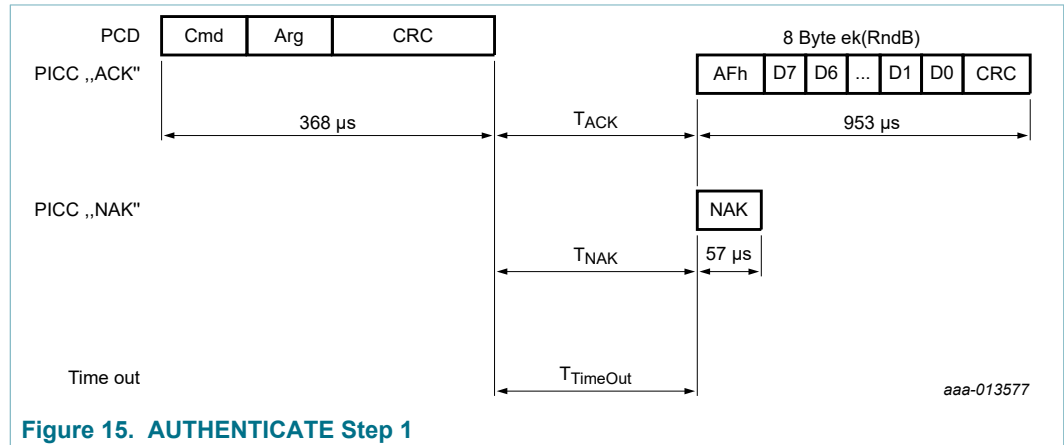


Figure 15. AUTHENTICATE Step 1

Table 23. AUTHENTICATE part 1 command

| Name     | Code                         | Description   | Length  |
|----------|------------------------------|---|---------|
| Cmd      | 1Ah                          | authentication part 1   | 1 byte  |
| Arg      | 00h                          | fixed value 00h as argument   | 1 byte  |
| CRC      | -                            | CRC according to <a href="#">Ref. 2</a>   | 2 bytes |
| AFh      | AFh                          | first response byte indicates that the authentication process needs a second command part | 1 bytes |
| ek(RndB) | -                            | 8-byte encrypted PICC random number RndB  | 8 bytes |
| NAK      | see <a href="#">Table 15</a> | see <a href="#">Section 8.3</a>   | 4-bit   |

Table 24. AUTHENTICATE part 1 timing

These times exclude the end of communication of the PCD.

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

Table 25. AUTHENTICATE Step 2

| Code | Parameter | Data           | Integrity mechanism | Response         |
|------|-----------|----------------|---------------------|------------------|
| AFh  | -         | ek(RndA+RndB') | Parity, CRC         | '00' + ek(RndA') |

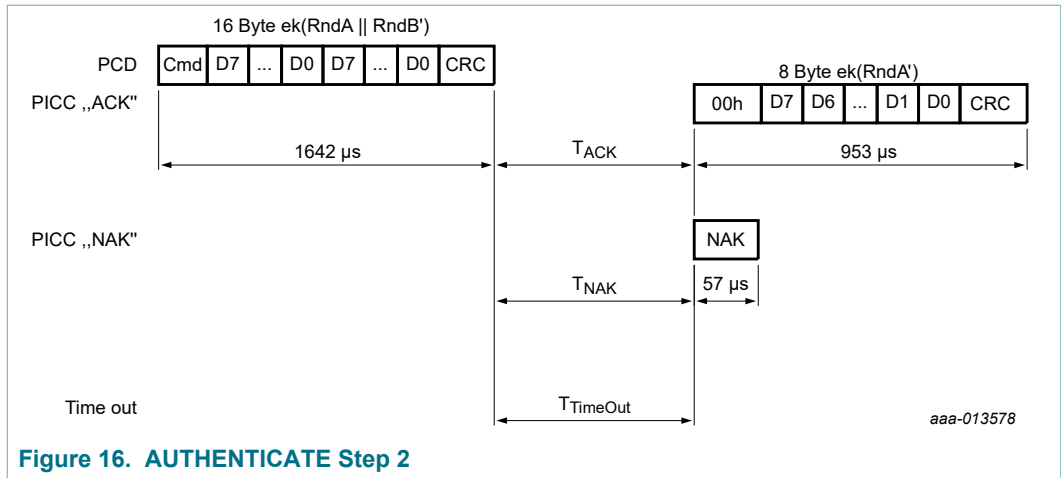


Table 26. AUTHENTICATE part 2 command

| Name              | Code         | Description  | Length   |
|-------------------|--------------|--|----------|
| Cmd               | AFh          | fixed first byte for the AUTHENTICATE part 2 command   | 1 byte   |
| ek(RndA    RndB') | -            | 16-byte encrypted random numbers RND A concatenated by RndB'                                 | 16 bytes |
| CRC               | -            | CRC according to Ref. 2  | 2 bytes  |
| 00h               | 00h          | first response byte indicates that the authentication process is finished after this command | 1 bytes  |
| ek(RndA')         | -            | 8-byte encrypted, shifted PCD random number RndA'  | 8 bytes  |
| NAK               | see Table 15 | see Section 8.3  | 4-bit    |

Table 27. AUTHENTICATE part 2 timing

These times exclude the end of communication of the PCD.

|                     | $T_{ACK}$ min | $T_{ACK}$ max | $T_{NAK}$ min | $T_{NAK}$ max | $T_{TimeOut}$ |
|---------------------|---------------|---------------|---------------|---------------|---------------|
| AUTHENTICATE part 2 | n=9           | $T_{TimeOut}$ | n=9           | $T_{TimeOut}$ | 5 ms          |

## 10 Limiting values

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

Table 28. Limiting values

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

| Symbol    | Parameter           | Min | Max  | Unit        |
|-----------|---------------------|-----|------|-------------|
| $I_I$     | input current       | -   | 30   | mA          |
| $T_{stg}$ | storage temperature | -55 | +125 | $^{\circ}C$ |



| Symbol           | Parameter                                |     | Min | Max | Unit |
|------------------|--|-----|-----|-----|------|
| T <sub>amb</sub> | ambient temperature                      |     | -25 | +70 | °C   |
| V <sub>ESD</sub> | electrostatic discharge voltage on LA/LB | [1] | 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.

## 11 Characteristics

### 11.1 Electrical characteristics

Table 29. Characteristics

| Symbol                        | Parameter         | Conditions                            |     | Min    | Typ   | Max   | Unit  |
|-------------------------------|-------------------|---------------------------------------|-----|--------|-------|-------|-------|
| f <sub>i</sub>                | input frequency   |                                       |     | -      | 13.56 | -     | MHz   |
| C <sub>i</sub>                | input capacitance | 16 pF version (bare silicon and MOA4) | [1] | 14.08  | 16    | 17.92 | pF    |
|                               |                   | 50 pF version                         | [1] | 44     | 50    | 56    | pF    |
| <b>EEPROM characteristics</b> |                   |                                       |     |        |       |       |       |
| t <sub>cy(W)</sub>            | write cycle time  |                                       |     | -      | 4.1   | -     | ms    |
| 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 | -     | -     | cycle |

[1] T<sub>amb</sub> = 22 °C, f = 13.56 MHz, V<sub>LaLb</sub> = 1.5 V RMS

## 12 Wafer specification

Table 30. Wafer specifications MF0ICU2x01DUy

|                                       |                           |
|---------------------------------------|---------------------------|
| <b>Wafer</b>                          |                           |
| diameter                              | 200 mm typical (8 inches) |
| maximum diameter after foil expansion | 210 mm                    |
| die separation process                | laser dicing              |
| thickness MF0ICU2x01XDUD              | 120 μm ± 15 μm            |
| MF0ICU2x01XDUF                        | 75 μm ± 10 μm             |
| flatness                              | not applicable            |
| Potential Good Dies per Wafer (PGDW)  | 61942                     |
| <b>Wafer backside</b>                 |                           |
| material                              | Si                        |

|   |   |
|---|---|
| treatment                                   | ground and stress relieve   |
| roughness                                   | $R_a$ max = 0.2 $\mu\text{m}$   |
|   | $R_t$ max = 2 $\mu\text{m}$   |
| <b>Chip dimensions</b>                      |   |
| step size <sup>[1]</sup>                    | x = 710 $\mu\text{m}$   |
|   | y = 710 $\mu\text{m}$   |
| gap between chips <sup>[1]</sup>            | typical = 22 $\mu\text{m}$  |
|   | minimum = 5 $\mu\text{m}$   |
| <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, TP1, TP2 <sup>[2]</sup> = 60 $\mu\text{m}$ $\times$ 60 $\mu\text{m}$ |
| 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.

## 12.1 Fail die identification

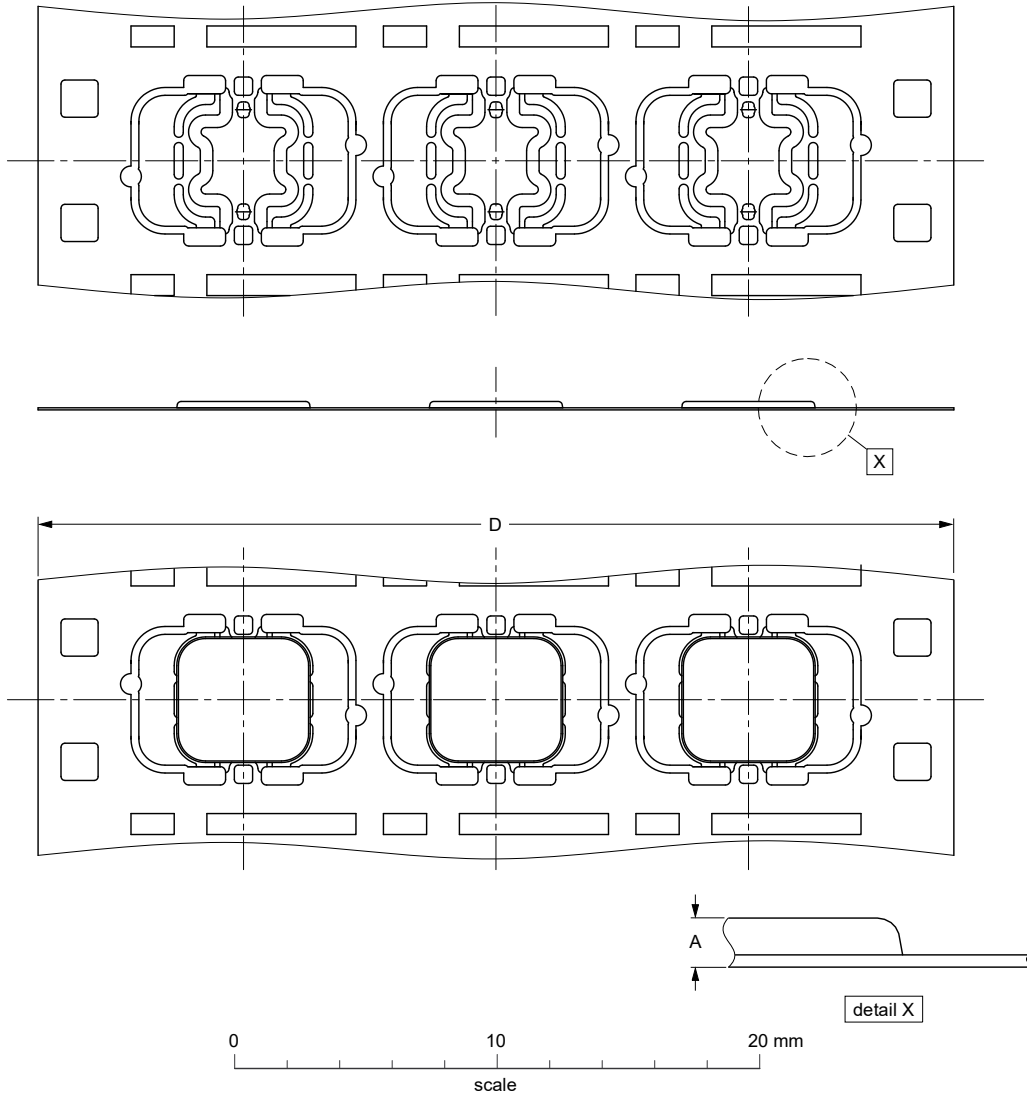
Electronic wafer mapping covers the electrical test results and additionally the results of mechanical/visual inspection. No ink dots are applied.

## 12.2 Package outline

For more details on the contactless modules MOA4 and MOA8 please refer to [Ref. 11](#) and [Ref. 12](#).

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**

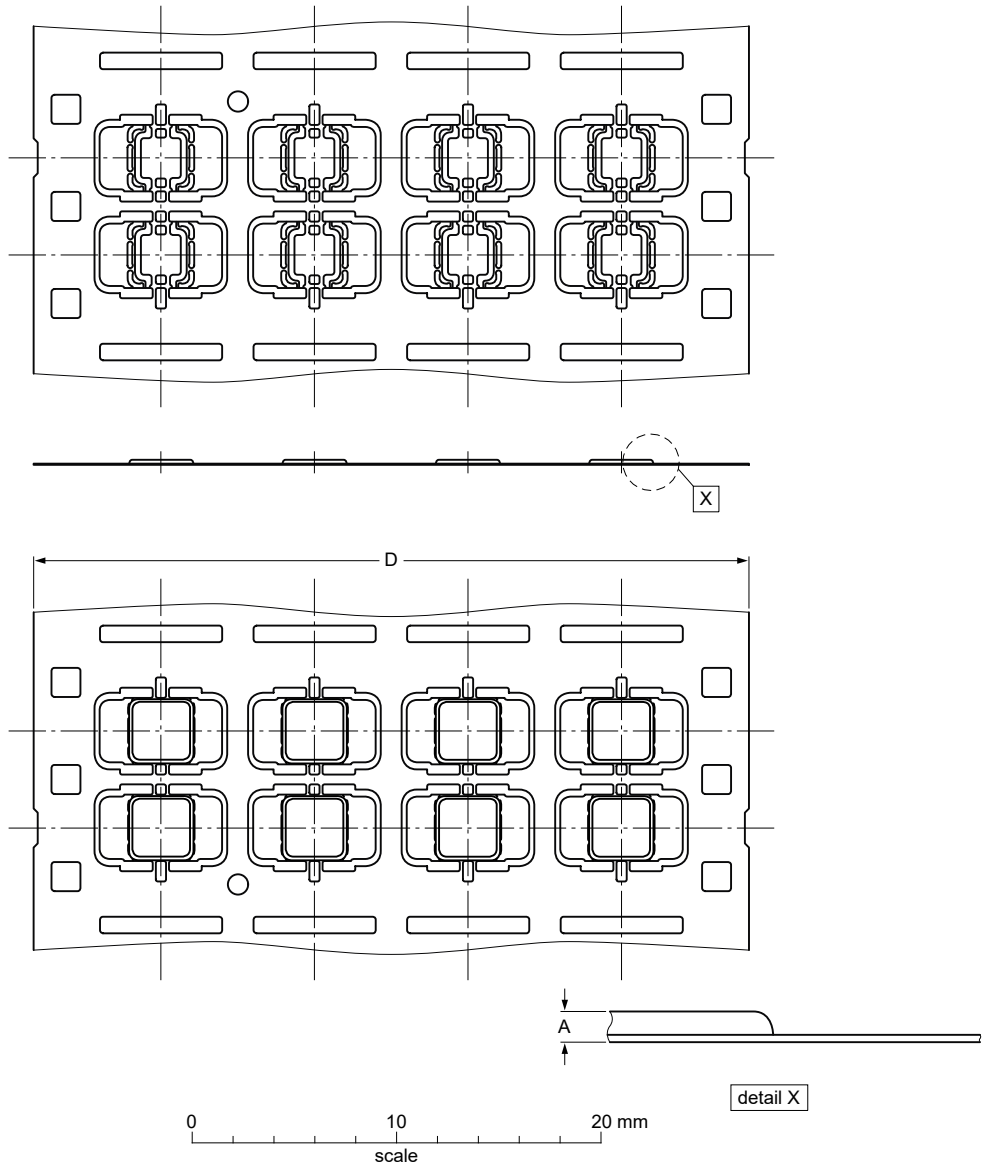
1. Total package thickness, exclusive punching burr.

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

Figure 17. Package outline SOT500-2

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

SOT500-4



Dimensions

| Unit | A <sup>(1)</sup> | D     |
|------|------------------|-------|
| mm   | max 0.26         | 35.05 |
|      | nom 35.00        |       |
|      | min 34.95        |       |

For unspecified dimensions see PLLMC-drawing given in the subpackage code.

Note

1. Total package thickness, exclusive punching burr.

sot500-4\_po

| Outline version | References |       |       | European projection | Issue date |
|-----------------|------------|-------|-------|---------------------|------------|
|                 | IEC        | JEDEC | JEITA |                     |            |
| SOT500-4        | ---        | ---   | ---   |                     | 11-02-18   |

Figure 18. Package outline SOT500-4

12.3 Bare die outline

For more details on the wafer delivery forms see [Ref. 13](#).

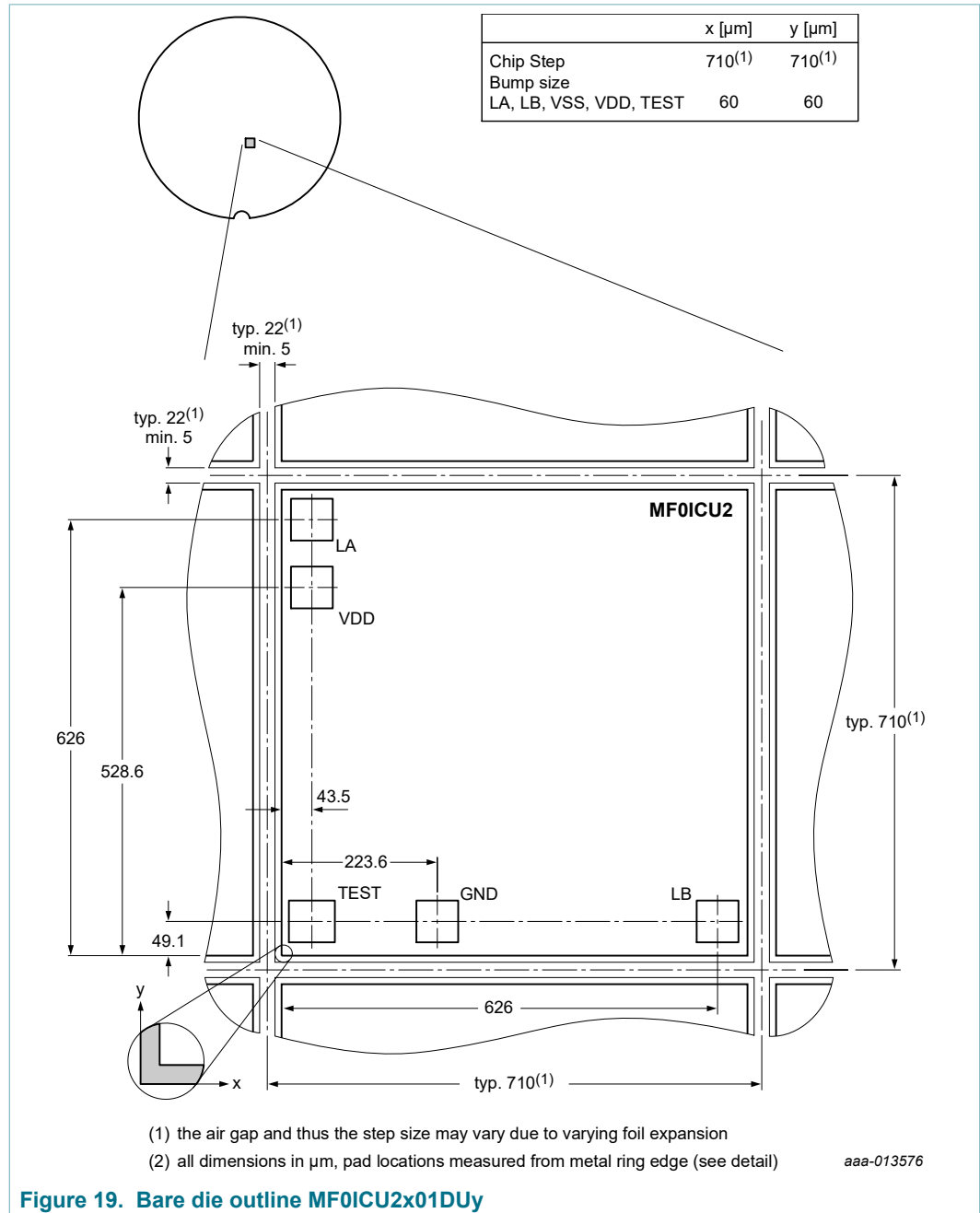


Figure 19. Bare die outline MF0ICU2x01DUy

13 Abbreviations

Table 31. Abbreviations

| Acronym | Description                     |
|---------|---------------------------------|
| 3DES    | Triple Data Encryption Standard |
| ACK     | Positive Acknowledge            |

| Acronym     | Description   |
|-------------|---|
| ATQA        | Answer To ReQuest, type A                           |
| BCC         | Block Check Characters byte                         |
| CBC         | Cipher-Block Chaining                               |
| CRC         | Cyclic Redundancy Check                             |
| CT          | Cascade Tag, Type A                                 |
| EEPROM      | Electrically Erasable Programmable Read-Only Memory |
| fc          | carrier frequency 13.56 MHz                         |
| HLTA        | Halt A command                                      |
| IV          | Initial Value                                       |
| LSB         | Least Significant Bit                               |
| MSB         | Most Significant Bit                                |
| NAK         | Negative Acknowledge                                |
| OTP         | One Time Programmable                               |
| Passive ACK | Implicit acknowledge without PICC answer            |
| PCD         | Proximity Coupling Device                           |
| PICC        | Proximity Integrated Circuit Card                   |
| POR         | Power On Reset                                      |
| REQA        | ReQuest Answer, type A                              |
| RF          | Radio Frequency                                     |
| SAK         | Select Acknowledge, type A                          |
| UID         | Unique Identifier                                   |
| WUPA        | Wake-UP command, type A                             |

## 14 References

[1]

**ISO/IEC 14443-2**

2001

[2]

**ISO/IEC 14443-3**

2001

[3]

MIFARE Interface Platform Type Identification Procedure

Application note, BL-ID Doc. No.: 0184\*\*2

[4]

MIFARE ISO/IEC 14443 PICC Selection

2 \*\* ... document version number

Application note, BU S&C Doc. No.: 1308\*\*

[5]

MIFARE Ultralight Features and Hints

Application note, BU S&C Doc. No.: 0731\*\*

[6]

MIFARE Ultralight as Type 2 Tag

Application note, BU S&C Doc. No.: 1303\*\*

[7]

MIFARE (Card) Coil Design Guide

Application note, BU S&C Doc. No.: 0117\*\*

[8]

MF0ICU1 Functional specification MIFARE Ultralight

Product data sheet, BU S&C Doc. No. 0286\*\*

[9]

NIST SP800-67: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Version 1.1 May 19, 2008

National Institute of Standards and Technology

[10]

ISO/IEC 10116: Information technology - Security techniques - Modes of operation for an n-bit block cipher, February 1, 2006

International Organization for Standardization

[11]

**Contactless smart card module specification MOA4**

Delivery Type Description, BU-ID Document number 0823\*\*<sup>2</sup>

[12]

**Contactless smart card module specification MOA8**

Delivery Type Description, BU-ID Document number 1636\*\*<sup>2</sup>

[13]

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

Delivery Type Description, BU-ID Document number 1005\*\*<sup>2</sup>

## 15 Revision history

Table 32. Revision history

| Document ID    | Release date   | Data sheet status    | Change notice | Supersedes     |
|----------------|--|----------------------|---------------|----------------|
| MF0ICU2 v. 3.3 | 20190730   | Product data sheet   | -             | MF0ICU2 v. 3.2 |
| Modifications: | <ul style="list-style-type: none"> <li>Updated descriptive text of the default user memory content, <a href="#">Section 7.5.9</a></li> <li>Update of <a href="#">Table 13</a></li> </ul>   |                      |               |                |
| MF0ICU2 v. 3.2 | 20140617   | Product data sheet   |               | 137631         |
| Modifications: | <ul style="list-style-type: none"> <li>Editorial changes</li> <li>Added 75 µm thin wafer and MOA8 delivery types</li> <li>New bare die outline drawing</li> <li>Corrected descriptive text in delivery forms for the 16 pF input capacitance</li> <li>Extended EEPROM specification with respect to programming cycle endurance and data retention</li> <li>New command descriptions including time-out specification</li> <li>Added descriptions for authentication, counter and lock bytes</li> <li>Removed ISO/IEC 14443-3 anticollision and selection commands and referred to standard</li> </ul> |                      |               |                |
| 137631         | 20090402   | Product data sheet   |               | 137630         |
| Modifications: | <ul style="list-style-type: none"> <li><a href="#">Section 16 "Legal information"</a>: updated</li> </ul>  |                      |               |                |
| 137630         | 20090218   | Product data sheet   | -             | 137610         |
| Modifications: | <ul style="list-style-type: none"> <li>General update</li> </ul>   |                      |               |                |
| 137610         | 20080428   | Objective data sheet | -             | 137601         |
| Modifications: | <ul style="list-style-type: none"> <li>Update of spelling issues</li> <li>Redesign of drawings</li> <li>Update of Section 1.3 "Security" on page 2</li> </ul>  |                      |               |                |
| 137601         | 20080404   | Objective data sheet | -             | -              |



## 16 Legal information

### 16.1 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>.

### 16.2 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.

### 16.3 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.

**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.

**Security** — While NXP Semiconductors has implemented advanced security features, all products may be subject to unidentified vulnerabilities. Customers are responsible for the design and operation of their applications and products to reduce the effect of these vulnerabilities on customer's applications and products, and NXP Semiconductors accepts no liability for any vulnerability that is discovered. Customers should implement appropriate design and operating safeguards to minimize the risks associated with their applications and products.

## 16.4 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 Ultralight** — is a trademark of NXP B.V.

## Tables

|          |   |    |          |  |    |
|----------|---|----|----------|--|----|
| Tab. 1.  | Naming conventions .....                                    | 2  | Tab. 17. | READ command .....                       | 20 |
| Tab. 2.  | Characteristics .....                                       | 3  | Tab. 18. | READ timing .....                        | 20 |
| Tab. 3.  | Ordering information .....                                  | 3  | Tab. 19. | WRITE command .....                      | 21 |
| Tab. 4.  | Pin allocation table .....                                  | 4  | Tab. 20. | WRITE timing .....                       | 21 |
| Tab. 5.  | Memory organization .....                                   | 8  | Tab. 21. | COMPATIBILITY_WRITE command .....        | 22 |
| Tab. 6.  | Functionality of lock bits in lock byte 0 and 1 ...         | 10 | Tab. 22. | COMPATIBILITY_WRITE timing .....         | 22 |
| Tab. 7.  | Functionality of lock bits in lock byte 2 and 3 ...         | 11 | Tab. 23. | AUTHENTICATE part 1 command .....        | 23 |
| Tab. 8.  | 3DES authentication .....                                   | 12 | Tab. 24. | AUTHENTICATE part 1 timing .....         | 23 |
| Tab. 9.  | Numerical 3DES authentication example .....                 | 13 | Tab. 25. | AUTHENTICATE Step 2 .....                | 23 |
| Tab. 10. | Key memory configuration .....                              | 14 | Tab. 26. | AUTHENTICATE part 2 command .....        | 24 |
| Tab. 11. | Memory content based on example<br>configuration .....      | 15 | Tab. 27. | AUTHENTICATE part 2 timing .....         | 24 |
| Tab. 12. | AUTH1 bit description .....                                 | 15 | Tab. 28. | Limiting values .....                    | 24 |
| Tab. 13. | Initial memory organization .....                           | 16 | Tab. 29. | Characteristics .....                    | 25 |
| Tab. 14. | Command overview .....                                      | 17 | Tab. 30. | Wafer specifications MF01CU2x01DUy ..... | 25 |
| Tab. 15. | ACK and NAK values .....                                    | 18 | Tab. 31. | Abbreviations .....                      | 29 |
| Tab. 16. | Summary of relevant data for device<br>identification ..... | 19 | Tab. 32. | Revision history .....                   | 32 |

## Figures

|          |  |    |          |                                      |    |
|----------|--|----|----------|--------------------------------------|----|
| Fig. 1.  | Contactless System .....                                       | 1  | Fig. 11. | READ .....                           | 20 |
| Fig. 2.  | Block diagram .....  | 4  | Fig. 12. | WRITE .....                          | 21 |
| Fig. 3.  | Contact assignments for SOT500-2 (MOA4) .....                  | 4  | Fig. 13. | COMPATIBILITY WRITE part 1 .....     | 22 |
| Fig. 4.  | State diagram .....  | 6  | Fig. 14. | COMPATIBILITY WRITE part 2 .....     | 22 |
| Fig. 5.  | UID/serial number .....  | 9  | Fig. 15. | AUTHENTICATE Step 1 .....            | 23 |
| Fig. 6.  | Lock bytes 0 and 1 .....                                       | 10 | Fig. 16. | AUTHENTICATE Step 2 .....            | 24 |
| Fig. 7.  | Lock bytes 2 and 3 .....                                       | 11 | Fig. 17. | Package outline SOT500-2 .....       | 27 |
| Fig. 8.  | OTP bytes .....  | 12 | Fig. 18. | Package outline SOT500-4 .....       | 28 |
| Fig. 9.  | Counter example .....  | 17 | Fig. 19. | Bare die outline MF01CU2x01DUy ..... | 29 |
| Fig. 10. | Frame Delay Time (from PCD to PICC) and<br>TACK and TNAK ..... | 18 |          |                                      |    |

**Contents**

|           |   |           |           |                            |           |
|-----------|---|-----------|-----------|----------------------------|-----------|
| <b>1</b>  | <b>General description</b>                                  | <b>1</b>  | <b>12</b> | <b>Wafer specification</b> | <b>25</b> |
| 1.1       | Contactless energy and data transfer                        | 1         | 12.1      | Fail die identification    | 26        |
| 1.2       | Anticollision   | 1         | 12.2      | Package outline            | 26        |
| 1.3       | Security  | 2         | 12.3      | Bare die outline           | 29        |
| 1.4       | Naming conventions  | 2         | <b>13</b> | <b>Abbreviations</b>       | <b>29</b> |
| <b>2</b>  | <b>Features and benefits</b>                                | <b>2</b>  | <b>14</b> | <b>References</b>          | <b>30</b> |
| 2.1       | MIFARE RF Interface (ISO/IEC 14443 A)                       | 2         | <b>15</b> | <b>Revision history</b>    | <b>32</b> |
| 2.2       | EEPROM  | 2         | <b>16</b> | <b>Legal information</b>   | <b>33</b> |
| <b>3</b>  | <b>Quick reference data</b>                                 | <b>3</b>  |           |                            |           |
| <b>4</b>  | <b>Ordering information</b>                                 | <b>3</b>  |           |                            |           |
| <b>5</b>  | <b>Block diagram</b>  | <b>4</b>  |           |                            |           |
| <b>6</b>  | <b>Pinning information</b>                                  | <b>4</b>  |           |                            |           |
| 6.1       | Smart card contactless module                               | 4         |           |                            |           |
| <b>7</b>  | <b>Functional description</b>                               | <b>5</b>  |           |                            |           |
| 7.1       | Block description   | 5         |           |                            |           |
| 7.2       | State diagram and logical states description                | 5         |           |                            |           |
| 7.2.1     | IDLE  | 6         |           |                            |           |
| 7.2.2     | READY1  | 6         |           |                            |           |
| 7.2.3     | READY2  | 7         |           |                            |           |
| 7.2.4     | ACTIVE  | 7         |           |                            |           |
| 7.2.5     | HALT  | 7         |           |                            |           |
| 7.2.6     | AUTHENTICATED   | 8         |           |                            |           |
| 7.3       | Data integrity  | 8         |           |                            |           |
| 7.4       | RF interface  | 8         |           |                            |           |
| 7.5       | Memory organization   | 8         |           |                            |           |
| 7.5.1     | UID/serial number   | 9         |           |                            |           |
| 7.5.2     | Lock byte 0 and 1   | 9         |           |                            |           |
| 7.5.3     | Lock byte 2 and 3   | 11        |           |                            |           |
| 7.5.4     | OTP bytes   | 12        |           |                            |           |
| 7.5.5     | 3DES Authentication   | 12        |           |                            |           |
| 7.5.6     | 3DES Authentication example                                 | 13        |           |                            |           |
| 7.5.7     | Programming of 3DES key to memory                           | 14        |           |                            |           |
| 7.5.8     | Configuration for memory access via 3DES Authentication     | 15        |           |                            |           |
| 7.5.9     | Data pages  | 15        |           |                            |           |
| 7.5.10    | Initial memory configuration                                | 15        |           |                            |           |
| 7.5.11    | Counter   | 16        |           |                            |           |
| <b>8</b>  | <b>Command overview</b>                                     | <b>17</b> |           |                            |           |
| 8.1       | MIFARE Ultralight C command overview                        | 17        |           |                            |           |
| 8.2       | Timings   | 18        |           |                            |           |
| 8.3       | MIFARE Ultralight C ACK and NAK                             | 18        |           |                            |           |
| 8.4       | Summary of device identification data                       | 19        |           |                            |           |
| <b>9</b>  | <b>MIFARE Ultralight C - Contactless ticket IC commands</b> | <b>19</b> |           |                            |           |
| 9.1       | MIFARE Ultralight C - Contactless ticket IC card activation | 19        |           |                            |           |
| 9.2       | READ  | 19        |           |                            |           |
| 9.3       | WRITE   | 20        |           |                            |           |
| 9.4       | COMPATIBILITY WRITE   | 21        |           |                            |           |
| 9.5       | AUTHENTICATE  | 23        |           |                            |           |
| <b>10</b> | <b>Limiting values</b>                                      | <b>24</b> |           |                            |           |
| <b>11</b> | <b>Characteristics</b>                                      | <b>25</b> |           |                            |           |
| 11.1      | Electrical characteristics                                  | 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. 2019.

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: 30 July 2019

Document identifier: MF0ICU2

Document number: 137633