MF0ICU2

MIFARE Ultralight C

Rev. 3.1 — 2 April 2009
137631

Product data sheet
CONFIDENTIAL

1. General description

NXP has developed MIFARE MF0ICU2 - MIFARE Ultralight C - to be used with Proximity Coupling Devices (PCD) according to ISO/IEC 14443A (see Ref. 1 “ISO/IEC 14443”). The communication layer (MIFARE RF Interface) complies to parts 2 and 3 of the ISO/IEC 14443A standard. The MF0ICU2 is primarily designed for limited use applications such as public transportation, event ticketing and NFC Forum Tag Type 2 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 16.9 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 baudrate of 106 kBit/s.

1.2 Anticollision

An intelligent anticollision function according to ISO/IEC 14443 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 data corruption resulting from other cards in the field.

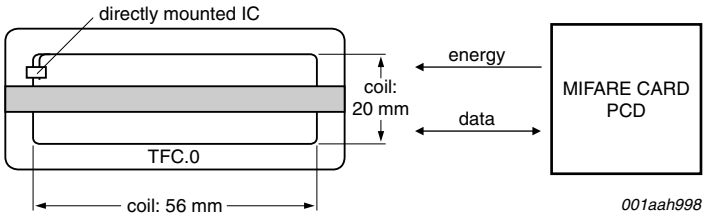


Fig 1. MIFARE card reader

1.2.1 Cascaded UID

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 rest of memory

1.4 Naming conventions

Table 1. Naming conventions

MF0xxU2w01Dyy / rrffbpL	Description
MF	MIFARE family
0	Ultralight product family
xx	Two character identifier for the package type
U2	Product: Ultralight C
w	One character identifier for input capacitance
01D	Fixed
yy	This is a two character identifier for the package type.

2. Features

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

- Contactless transmission of data and supply energy (no battery needed)
- Operating distance: up to 100 mm (depending on field strength and antenna geometry)
- Operating frequency: 13.56 MHz
- Fast data transfer: 106 kbit/s
- High data integrity: 16-bit CRC, parity, bit coding, bit counting
- True anticollision
- 7 byte serial number (cascade level 2 according to ISO/IEC 14443-3)
- Typical ticketing transaction: < 35 ms
- Fast counter transaction: < 10 ms

2.2 EEPROM

- 1536-bit total memory
- 1184-bit user memory
- 36 pages user r/w area
- 512 bits compatible to MF0ICU1
- Field programmable read-only locking function per page for first 512-bit
- Field programmable read-only locking function per block
- 32-bit user definable One Time Programmable (OTP) area
- 16-bit counter
- Data retention of 5 years
- Write endurance 10000 cycles

3. Ordering information

Table 2. Ordering information

Type number	Package		
	Name	Description	Version
MF0ICU2001DUD	-	8 inch wafer (sawn, laser diced; 120 μm thickness, on film frame carrier; electronic fail die marking according to SECSII format), 17pF version	-
MF0ICU2101DUD	-	8 inch wafer (sawn, laser diced; 120 μm thickness, on film frame carrier; electronic fail die marking according to SECSII format), 50pF version	-
MF0MOU2001DA4	PLLMC	plastic leadless module carrier package; 35 mm wide tape, 17pF version	SOT500-2
MF0MOU2101DA4	PLLMC	plastic leadless module carrier package; 35 mm wide tape, 50pF version	SOT500-2

4. Block diagram

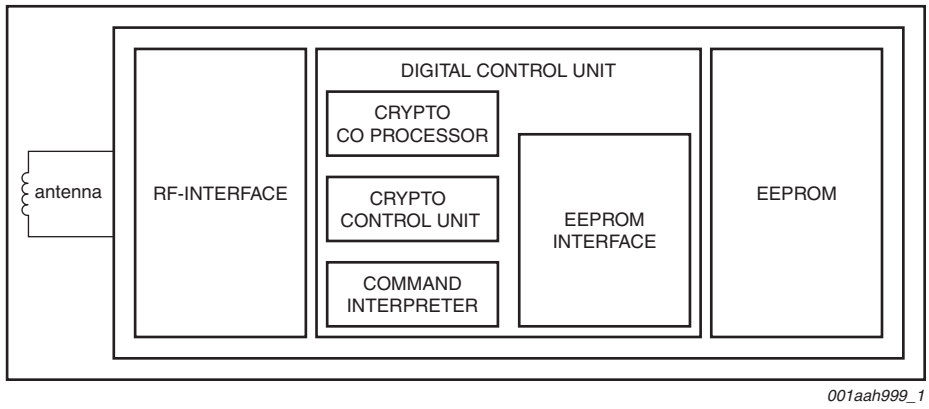


Fig 2. Block diagram

5. Pinning information

5.1 Smart card contactless module

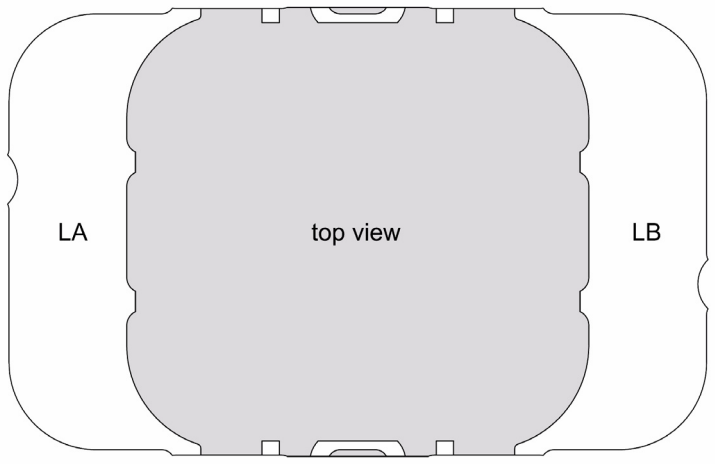


Fig 3. Contact assignments for SOT500-2 (MOA4)

Table 3. Bonding pad assignments to smart card contactless module

Contactless interface module		MF0ICU2DA4/01
Antenna contacts	**Symbol**	**Description**
LA	LA	Antenna coil connection LA
LB	LB	Antenna coil connection LB

6. Mechanical specification

6.1 Wafer

- Diameter: 8” wafer, 200 mm unsawn
min: 200 mm
typ: 206 mm
max: 210 mm
- Thickness: 120 µm ± 15 µm
- Flatness: not applicable
- PGDW: 61942
- Sawing method: Laser dicing

6.2 Wafer backside

- Material: Si
- Treatment: ground and stress relieve
- Roughness: R_a max 0.2 µm
R_t max 2 µm

6.3 Chip dimensions

- Chip size: 0.673 x 0.673 mm
- Scribe lines: x-line: 15 µm
y-line: 15 µm

6.4 Passivation

- Type: sandwich structure
- Material: Nitride
- Thickness: 1.75 µm

6.5 Au bump

- Bump material: > 99.9 % pure Au
- Bump hardness: 35 – 80 HV 0.005
- Bump shear strength: > 70 MPa
- Bump height: 18 µm
- Bump height uniformity:
  - within a die: ± 2 µm
  - within a wafer: ± 3 µm
  - wafer to wafer: ± 4 µm
- Bump flatness: ± 1.5 µm
- Bump size:
  - LA, LB 60 x 60 µm
  - TP1;TP2;VSS 60 x 60 µm
- Bump size variation: ± 5 µm
- Under bump metallization: sputtered TiW

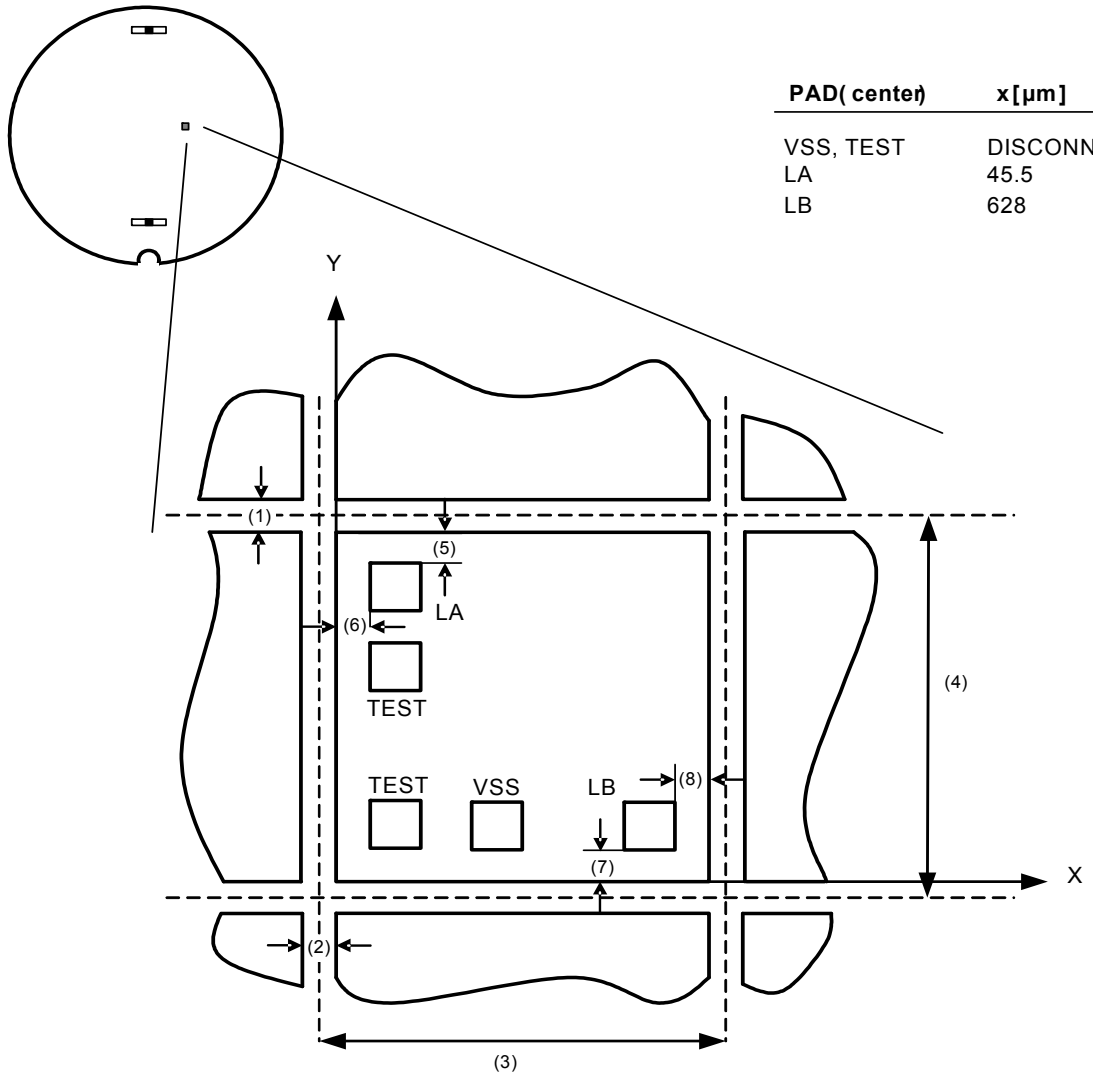
Remark: Substrate is connected to VSS.

6.6 Fail die identification

Electronic wafer mapping covers the electrical test results and additionally the results of mechanical/ visual inspection.

No inkdots are applied.

7. Chip orientation and bond pad locations



(1) Y- Scribeline width : see Table 3
(2) X- Scribeline width : see Table 3
(3) Chip step, x-length : 688 µm
(4) Chip step, y-length : 688 µm
(5) LA bump edge to chip edge, y-length: 14.9 µm
(6) LA bump edge to chip edge, x-length: 15 µm
(7) LB bump edge to chip edge, y-length: 21.296 µm
(8) LB bump edge to chip edge, x-length: 15 µm

(1) Lower left corner of metal sealring (X,Y) = 0,0

(2) The scribeline width is not constant for laser diced wafers.

Fig 4. Chip orientation and bond pad locations

Table 4. Scribeline width

Min	Typ	Unit
5	22	µm

8. Functional description

8.1 Block description

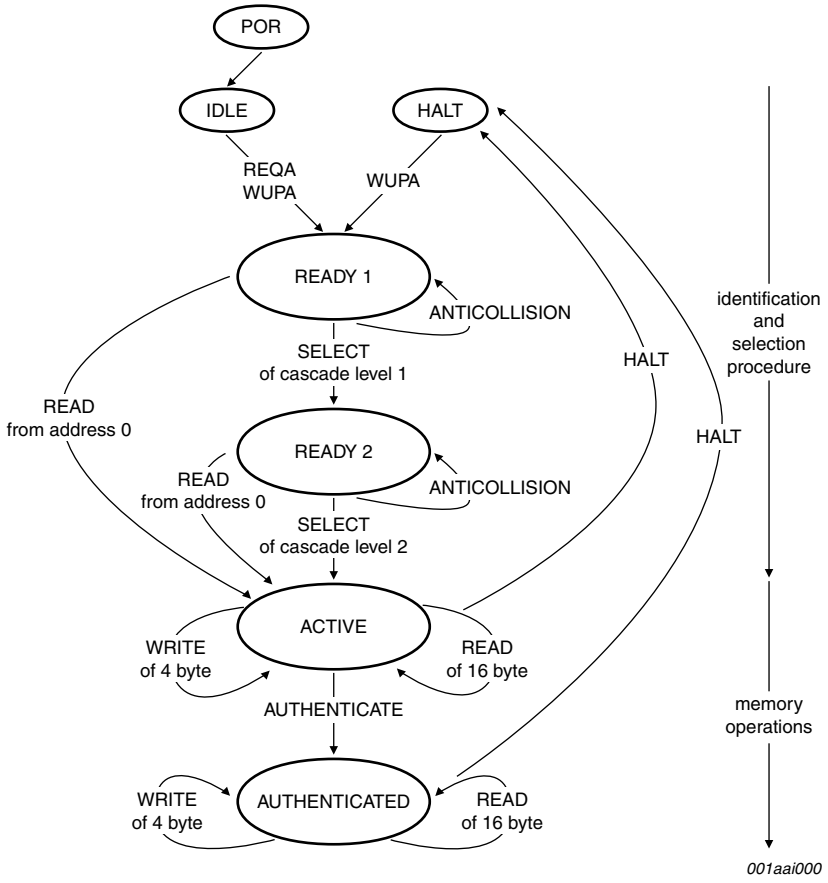
The MF0ICU2 chip consists of the 1536-bit EEPROM, the RF-Interface and the Digital Control Unit. Energy and data are transferred via an antenna, which consists of a coil with a few turns directly connected to the MF0ICU2. No further external components are necessary. (For details on antenna design please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

- 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.

8.2 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 5 “State diagram”) and generates the appropriate response.

For a correct implementation of an anticollision procedure please refer to the documents in Section 13 “References”.



Remark: Not shown in this diagram: In each state the command interpreter returns to the Idle state if an unexpected command is received. If the IC has already been in the Halt state before it returns to the Halt state in such a case.

Fig 5. State diagram

8.2.1 Idle

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

8.2.2 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 SELECT command of cascade level 1.

There are two possibilities to leave this state:

- With the SELECT command of cascade level 1 the PCD brings the MF0ICU2 into state Ready2 where the second part of the UID has to 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

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. Any other data received in state Ready1 state is interpreted as an error and the MF0ICU2 jumps back to its waiting state (IDLE or HALT, depending on it´s previous state).

The response of the MF0ICU2 to the SELECT of cascade level 1 command is the SAK (Select Acknowledge) byte with value 04h. It indicates that UID is not complete by now and another anticollision sequence is required.

8.2.3 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 SELECT command of cascade level 2.

Alternatively, state Ready2 may be skipped via a READ (from address 00h) command as described in state Ready1.

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.

The response of the MF0ICU2 to the SELECT of cascade level 2 command is the SAK (Select Acknowledge) byte with value 00h. According to ISO/IEC14443 this byte indicates whether the anticollision cascade procedure is finished (see Ref. 5 “MIFARE Ultralight as Type 2 Tag”). In addition it defines for the MIFARE architecture platform the type of the selected device. At this stage MF0ICU2 is uniquely selected and only this 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 jumps back to its waiting state (IDLE or HALT, depending on it´s previous state).

8.2.4 Active

In the Active state Read (16 bytes), Write (4 bytes), Compatibility Write (16 bytes) or an authentication can be performed.

After a successful authentication the state ”Authenticated” is reached, see Section 8.2.6 “Authenticated”.

After a valid HALT command the state will be left to 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 it´s previous state).

8.2.5 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 HALT 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. Any other data received in this state is interpreted as an error and the MF0ICU2 remains in this state.

8.2.6 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 8.5.4 “3DES Authentication”.

8.3 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)

8.4 RF interface

The RF-interface is according to the standard for contactless smart cards ISO/IEC 14443A (see Ref. 1 “ISO/IEC 14443”).

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 address of the selected block 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).

8.5 Memory organization

The 1536 bits 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			
dec.	**hex.**	**0**	**1**	**2**	**3**
0	00h	SN0	SN1	SN2	BCC0
1	01h	SN3	SN4	SN5	SN6
2	02h	BCC1	internal	Lock byte 0	Lock byte 1
3	03h	OTP	OTP	OTP	OTP
4 to 39	04h to 27h	user	user	user	user
40	28h	Lock byte 2	Lock byte 3	rfu	rfu
41	29h	CNT	CNT	rfu	rfu
42	2Ah	AUTH0	rfu	rfu	rfu
43	2Bh	AUTH1	rfu	rfu	rfu
44	2Ch	Key	Key	Key	Key
45	2Dh	Key	Key	Key	Key
46	2Eh	Key	Key	Key	Key
47	2Fh	Key	Key	Key	Key

8.5.1 UID/serial number

The unique 7 byte serial number (UID) and its two Block Check Characters 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 write-protected after having been programmed by the IC manufacturer after production.

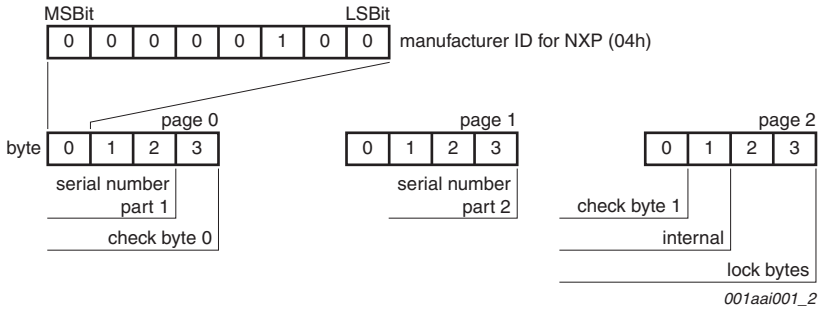


Fig 6. UID/serial number

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

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

8.5.2 Lock bytes

Lock bytes enable the user to lock parts of the complete memory area for writing. A Read from user memory area can not be restricted via lock bytes functionality. For this, please refer to the authentication functionality, (see Section 8.5.4 “3DES Authentication”).

The lock bytes functionality is enabled with a WRITE command (see Section 8.8.7 “WRITE”) or COMPATIBILTIY WRITE command (see Section 8.8.8 “COMPATIBILITY WRITE”), where 2 out of 4 bytes transmitted are used for setting the lock bytes. Two corresponding bytes - either bytes 2 and 3 for page 02h or bytes 0 and 1 for page 28h - and the actual content of the lock bytes are bit-wise “OR-ed”. The result of OR operation becomes the new content of the lock bytes. Two unused bytes do not have to be considered. Although included in the COMPATIBILITY WRITE or WRITE command, they are ignored when programming the memory.

Table 6. Lock bytes

Name	Page		Function
	Number	Address	
Lock byte 0	2	02h	page and block locking
Lock byte 1	2	02h	page locking
Lock byte 2	40	28h	page and block locking
Lock byte 3	40	28h	functionality and block locking

Due to build-in bitwise OR operation this process is irreversible. If a bit is set to “1”, it cannot be changed back to “0” again. Therefore, before locking the lock bytes, the user has to ensure that the corresponding user memory area and/or configuration bytes are correctly written.

The configuration written in the lock bytes is active upon the next REQA or WUPA command.

The single bits of the 4 bytes available for locking incorporate 3 different functions:

- the read-only locking of the single pages or blocks of the user memory area
- the read-only locking of the single bytes of the configuration memory area
- the locking of the lock bits themselves

For the compatibility reasons, the first 512 bits of the memory area have the same functionality as MF0ICU2 (see also Ref. 6 “MF0ICU1 Functional specification MIFARE Ultralight”), meaning that the two lock bytes used for the configuration of this memory area are identically configured. The mapping of single bits to memory area for the first 512 bits is shown in Figure 7.

The bits of byte 2 and 3 of page 02h represent the field-programmable read-only locking mechanism. Each page x from 03h (OTP bits) to 0Fh may be locked individually to prevent further write access by setting the corresponding locking bit Lx to 1. After locking the page is read-only memory.

The 3 least significant bits of lock byte 0 of page 2 are the block-locking bits. Bit 2 handles pages 0Fh to 0Ah, bit 1 pages 09h to 04h and bit 0 page 03h (OTP bits). Once the block locking bits are set, the locking configuration for the corresponding memory area is frozen.

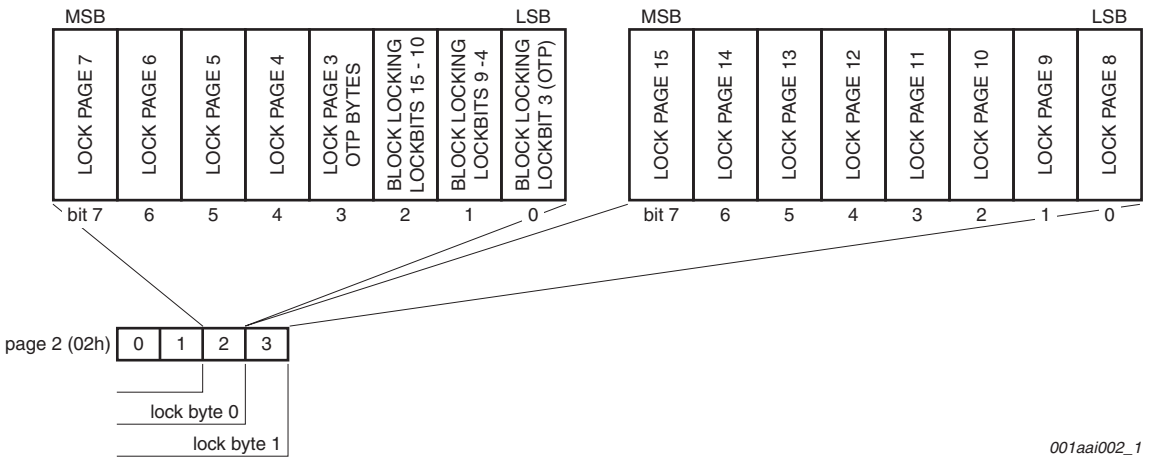


Fig 7. Lock bytes 1 and 2

For locking of pages starting at page address 10h onwards, lock bytes located in page 28h are used. Those two lock bytes cover the memory area of 96 data bytes together with configuration area from page address 28h onwards. Therefore, the granularity is larger then for the first 512 bits a shown in Figure 8 “Lock bytes 3 and 4”.

The functionality beyond page address 28h which can be locked read-only is:

- the key
- the counter
- the authentication configuration
- the lock bytes themselves

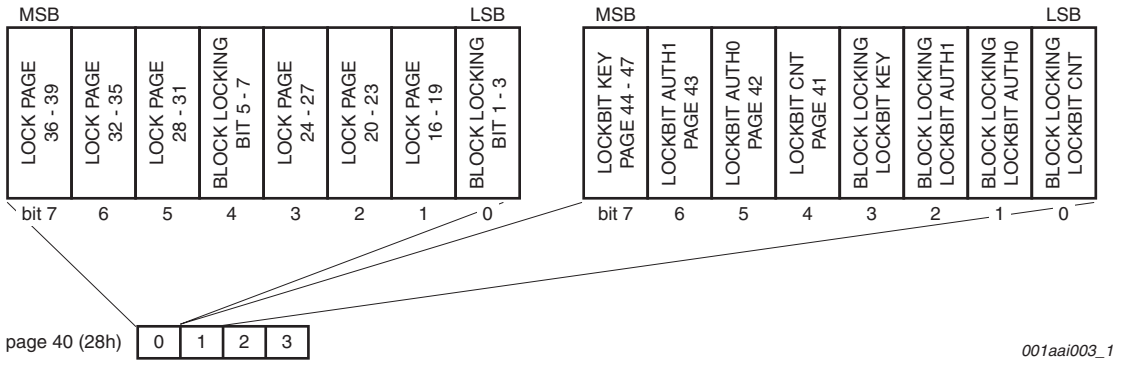
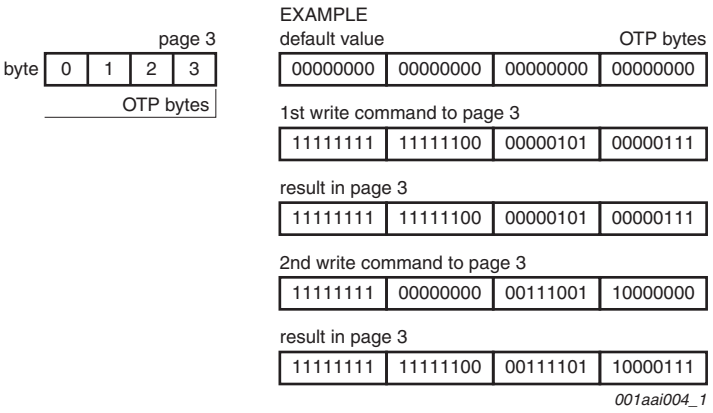


Fig 8. Lock bytes 3 and 4

8.5.3 OTP bytes

Page 3 is the OTP page. It is pre-set to all “0” after production. These bytes may be bit-wise modified by a WRITE command.



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

Fig 9. OTP bytes

The bytes of the WRITE command and the current contents of the OTP bytes are bit-wise “OR-ed” and the result becomes 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.

8.5.4 3DES Authentication

3DES Authentication proves that two entities have the same secret and each entity can be seen as a reliable partner for the coming communication. The applied encryption algorithm ek() is 2 key 3DES encryption (see Ref. 7 “NIST SP800-67: Recommondation for the TripleData Encryption Algorithm (TDEA) Block Chipher, Version 1.1 May 19, 2008”) in Cipher-Block Chaining (CBC) mode as described in ISO/IEC 10116 (see Ref. 8 “ISO/IEC 10116: Information technology - Security techniques - Modes of operation for an n-bit block chiper, February 1, 2006”). 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 received.

The following figure shows the communication flow during authentication:

Table 7. 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” → Authenticate		Step 1
2		← 8 bytes *ek(RndB)*	The PICC generates an 8 byte random number *RndB*. This random number is **en**ciphered with the key, denoted by *ek(RndB),* and is then transmitted to the PCD.	
3	The PCD itself generates an 8 byte random number *RndA*. This *RndA* is concatenated with *RndB*’ and **en**ciphered with the key. This token *ek(RndA* || *RndB’)* is sent to the PICC.	→ 16 bytes *ek(RndA* || *RndB’)*		
4		← 8 bytes *ek(RndA’)*	The PICC runs an **de**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. A successful verification proves to the PICC that the PICC and the PCD posses the same secret. If the verification fails, the PICC stops the authentication procedure and returns an error message. 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 **en**ciphered again, resulting in *ek(RndA’).* This token is sent to the PCD.	Step 2
5	The PCD runs a **de**cipherment on the received *ek(RndA’)* and thus gains *RndA’* for comparison with the PCD-internally rotated *RndA’*. If the comparison fails, the PCD exits the procedure and may halt the PICC.			
6			The PICC sets the state to authenticate.	

Crypto method is based on 3DES; CBC mode

See command details in Section 8.8.9 “AUTHENTICATE”. The used key is a double length DES Key; where the parity bits are not checked or used.

8.5.5 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 8 “Key memory configuration”. The key itself can be written during personalization or at any later moment using the commands WRITE (see Section 8.8.7 “WRITE”) or COMPATIBILITY WRITE (see Section 8.8.8 “COMPATIBILITY WRITE”). Byte 0 is always sent first using both of the mentioned commands.

Table 8. 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 9 “Memory content based on example configuration”.

Table 9. 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 reading of those pages with the use of READ command is not possible, independent on configuration.

8.5.6 Configuration for memory access via 3DES Authentication

Behaviour 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 “Memory organization”).

- AUTH0 defines the page address from which the authentication is required. Valid address range for byte AUTH0 is from 03h to 30h.
- AUTH1 determines if write access is restricted or both read and write access are restricted, see Table 10 “AUTH1 bit description”

Table 10. 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

8.5.7 Data pages

MF0ICU2 features 144 bytes of data memory. The address range from page 04h to 27h constitute the read/write area.

Initial state of each byte in the user area is 00h.

A write access to data memory is done with WRITE (see Section 8.8.7 “WRITE”) or COMPATIBILITY WRITE (see Section 8.8.8 “COMPATIBILITY WRITE”) command. In both cases, 4 bytes of memory - one page - will be overwritten. Write access to data memory can be permanently restricted via lock bytes (see Section 8.5.2 “Lock bytes”) and/or permanently or temporary restricted using an authentication (see Section 8.5.4 “3DES Authentication”).

NFC Forum Type 2 Tag compliancy

MF0ICU2 has been designed to be compliant with NFC Forum Type 2 Tag specification (see also Ref. 5 “MIFARE Ultralight as Type 2 Tag”). With its 144 bytes of data memory, it can easily support use cases like Smart Poster, Handover, SMS, URL or Call Request.

8.5.8 Initial memory configuration

The memory configuration of MF0ICU2 in delivery state is shown in Table 11 “Initial memory organization”:

Table 11. 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	**00h**	**00h**	**00h**	**00h**
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	Key	Key	Key	Key
45	2Dh	Key	Key	Key	Key
46	2Eh	Key	Key	Key	Key
47	2Fh	Key	Key	Key	Key

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

8.6 Counter

MF0ICU2 features 16-bit one way counter, located at first two bytes of page 29h. In its delivery state, counter value is set to 0000h.

The first[1] valid Write or Compatibility write to the address 29h can be performed with any value in the range between 0001h and FFFFh and corresponds to initial counter value. Every consequent valid 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.

If - after initial write - a value higher then 000Fh is used as a parameter, the MF0ICU2 will answer with NAK. Once counter value reaches FFFFh and an increment is performed via valid command, MF0ICU2 will answer with NAK. If the sum of counter value and increment is higher than FFFFh, MF0ICU2 will answer with NAK and will not update the counter.

Increment by zero (00h) is always possible, but does not have any impact to counter value.

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

8.7 PICC response to a command from PCD

MIFARE Ultralight C 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 5 “State diagram”).

MIFARE Ultralight C distinguishes between positive (ACK) and negative (NAK) acknowledge. Valid values for ACK and NAK are shown in Table 12 “ACK and NAK values”.

Table 12. ACK and NAK values

Answer value	Answer explanation
Ah	positive acknowledge (ACK)
1h	parity or CRC error (NAK)
0h	any other error (NAK)

After every NAK MF0ICU2 will perform an internal reset.

1. First valid write is defined as write to a counter value of zero with an argument different then zero

8.8 Command set

The ATQA and SAK are identical as for MF0ICU1 (see Ref. 6 “MF0ICU1 Functional specification MIFARE Ultralight”). For information on ISO 14443 card activation, see Ref. 3 “MIFARE ISO/IEC 14443 PICC Selection”. Summary of data relevant for device identification is given in Section 8.9 “Summary of relevant data for device identification”.

The MF0ICU2 comprises the following command set:

8.8.1 REQA

Table 13. REQA

Code	Parameter	Data	Integrity mechanism	Response
26h (7-bit)	-	-	Parity	0044h

Description: The MF0ICU2 accepts the REQA command in Idle state only. The response is the 2-byte ATQA (0044h). REQA and ATQA are implemented fully according to ISO/IEC14443-3.

Remark: Time units are not to scale and rounded off to 10 µs

Fig 10. REQA

8.8.2 WUPA

Table 14. WUPA

Code	Parameter	Data	Integrity mechanism	Response
52h (7-bit)	-	-	Parity	0044h

Description: The MF0ICU2 accepts the WUPA command in the Idle and Halt state only. The response is the 2-byte ATQA (0044h). WUPA is implemented fully according to ISO/IEC14443-3.

Remark: Time units are not to scale and rounded off to 10 µs

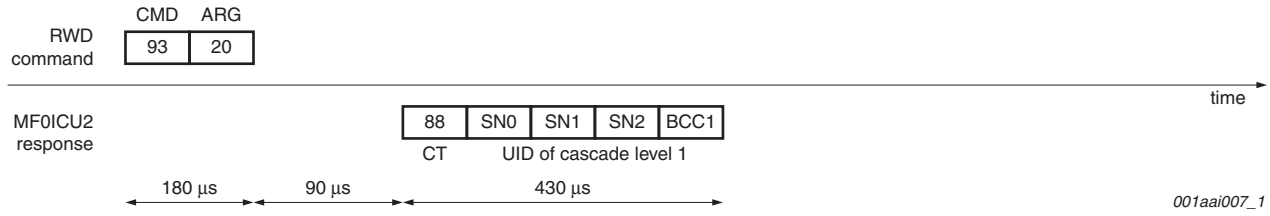
Fig 11. WUPA

8.8.3 ANTICOLLISION and SELECT of cascade level 1

Table 15. ANTICOLLISION and SELECT of cascade level 1

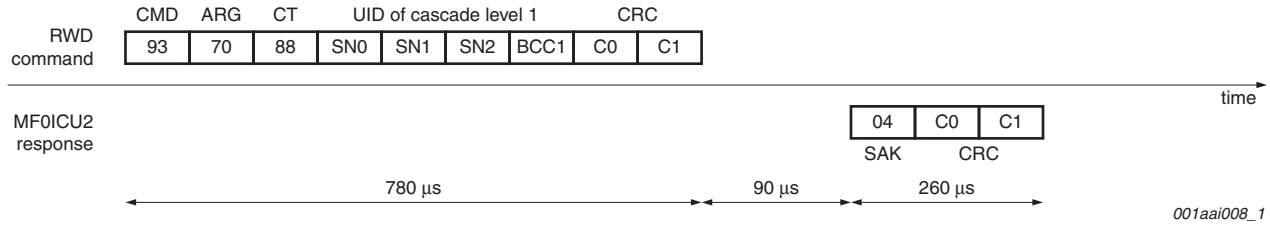
Code	Parameter	Data	Integrity mechanism	Response
Anticollision: 93h	20h	-	Parity, BCC	-
Anticollision: 93h	21h to 67h	Part of the UID	Parity, BCC	Parts of UID
Select: 93h	70h	First 3 bytes of UID	Parity, BCC, CRC	SAK ('04')

Description: The ANTICOLLISION and SELECT commands are based on the same command code. They differ only in the Parameter byte. This byte is per definition 70h in case of SELECT. The MF0ICU2 accepts these commands in the Ready1 state only. The response is part 1 of the UID. Even with incorrect CRC value, the SELECT command will be fully functional.



Remark: Time units are not to scale and rounded off to 10 µs

Fig 12. ANTICOLLISION of cascade level 1



Remark: Time units are not to scale and rounded off to 10 µs

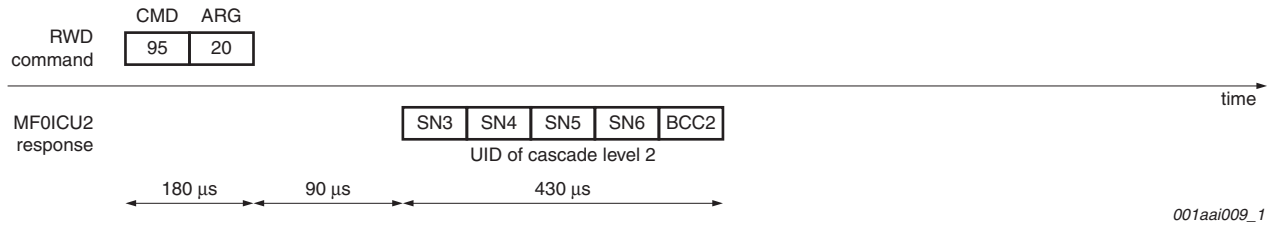
Fig 13. SELECT of cascade level 1

8.8.4 ANTICOLLISION and SELECT of cascade level 2

Table 16. ANTICOLLISION and SELECT of cascade level 2

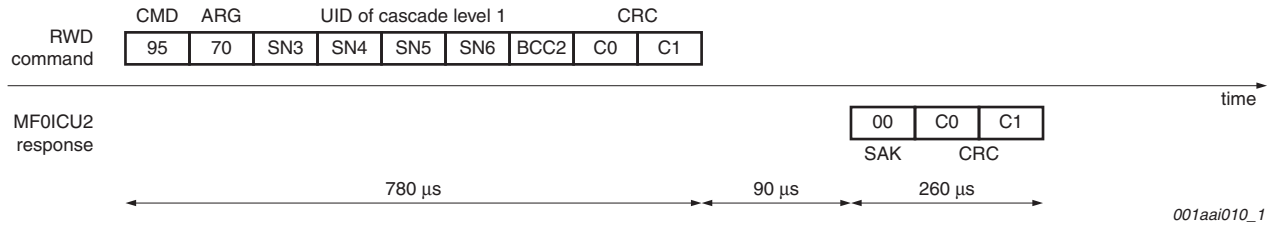
Code	Parameter	Data	Integrity mechanism	Response
Anticollision: 95h	20h	-	Parity, BCC	-
Anticollision: 95h	21h to 67h	Part of the UID	Parity, BCC	Parts of UID
Select: 95h	70h	Second 4 bytes of UID	Parity, BCC, CRC	SAK ('00')

Description: The ANTICOLLISION and SELECT commands are based on the same command code. They differ only in the parameter byte. This byte is per definition 70h in case of SELECT. The MF0ICU2 accepts these commands in the Ready2 state only. The response is part 2 of the UID. Even with incorrect CRC value, the SELECT command will be fully functional.



Remark: Time units are not to scale and rounded off to 10 µs

Fig 14. ANTICOLLISION of cascade level 2



Remark: Time units are not to scale and rounded off to 10 µs

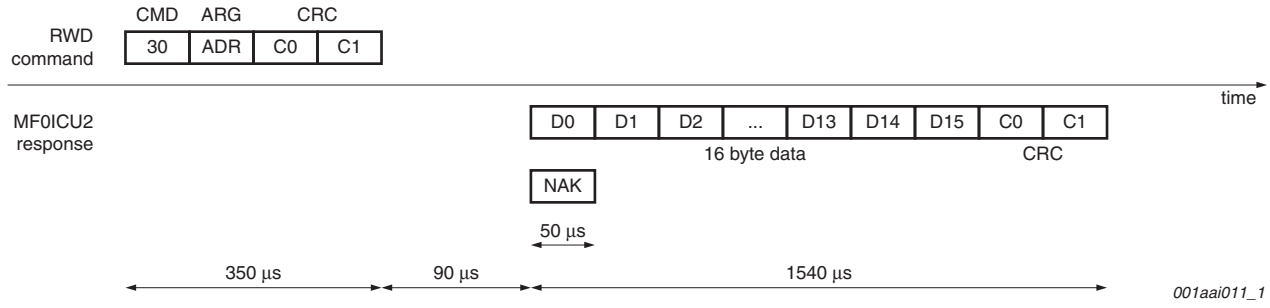
Fig 15. SELECT of cascade level 2

8.8.5 READ

Table 17. READ

Code	Parameter/ARG	Data	Integrity mechanism	Response
30h	ADR: '00h' to '2Bh'	-	Parity, CRC	16 Byte Date

Description: The READ command needs 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). If ADR is '2Bh', the contents of pages 2Bh, 00h, 01h and 02h is returned). This is also applied by configuring the authentication address.



Remark: Time units are not to scale and rounded off to 10 µs

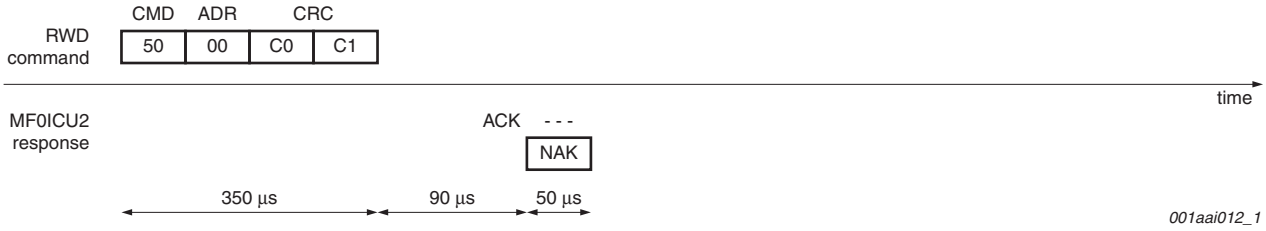
Fig 16. READ

8.8.6 HALT

Table 18. HALT

Code	Parameter	Data	Integrity mechanism	Response
50h	00h	-	Parity, CRC	Passive ACK, NAK

Description: The HALT command is used to set already processed MF0ICU2 devices into a different waiting state (Halt instead of Idle), which allows a simple separation between devices whose UIDs are already known (as they have already passed the anticollision procedure) and devices that have not yet been identified by there UIDs. This mechanism is a very efficient way of finding all contactless devices in the field of a PCD. Even with incorrect parity value, the HALT command will be fully functional. Executing a HALT command results in losing authentication status.



Remark: Time units are not to scale and rounded off to 10 µs

Fig 17. HALT

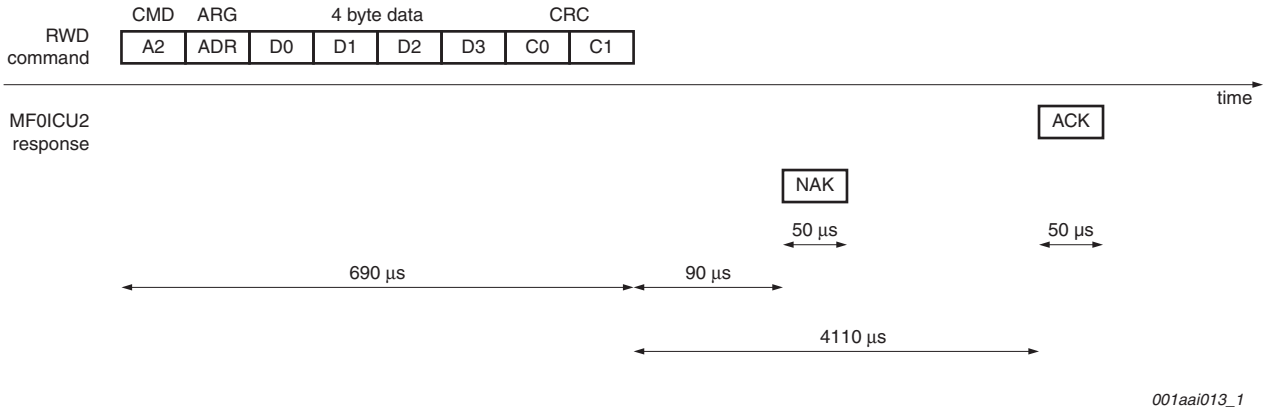
8.8.7 WRITE

Table 19. WRITE

Code	Parameter/ARG	Data	Integrity mechanism	Response
A2h	ADR: '02h' to '2Fh'	4 Byte	Parity, CRC	ACK or NAK

Description: The WRITE command is used to program the lock bytes in page 2, the OTP bytes in page 03h or the data bytes in pages 04h to 05h. A WRITE command is performed page-wise, programming 4 bytes in a page.

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.



Remark: Time units are not to scale and rounded off to 10 µs

Fig 18. WRITE

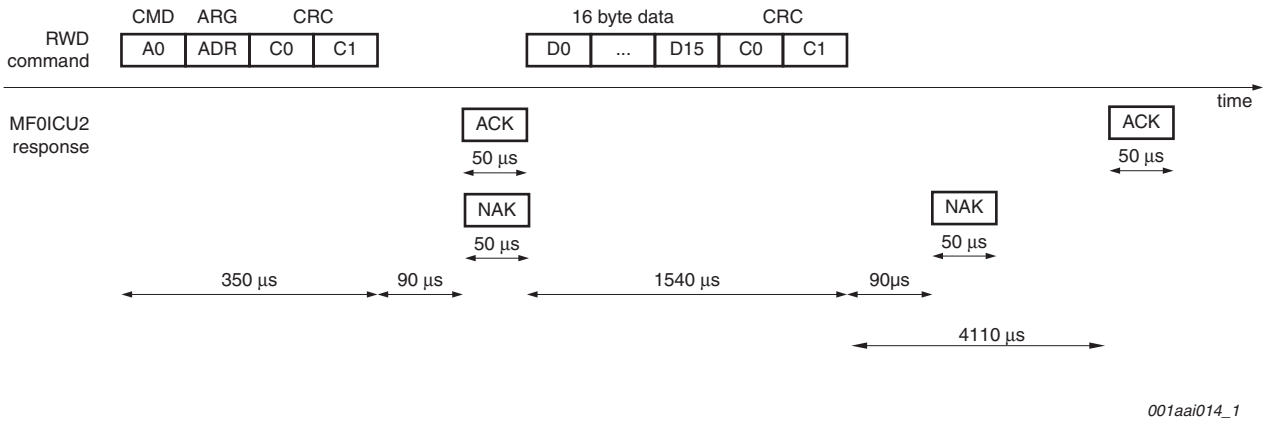
8.8.8 COMPATIBILITY WRITE

Table 20. COMPATIBILITY WRITE

Code	Parameter/ARG	Data	Integrity mechanism	Response
A0h	ADR: '02h' to '2Fh'	16 Byte	Parity, CRC	ACK or NAK

Description: 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.



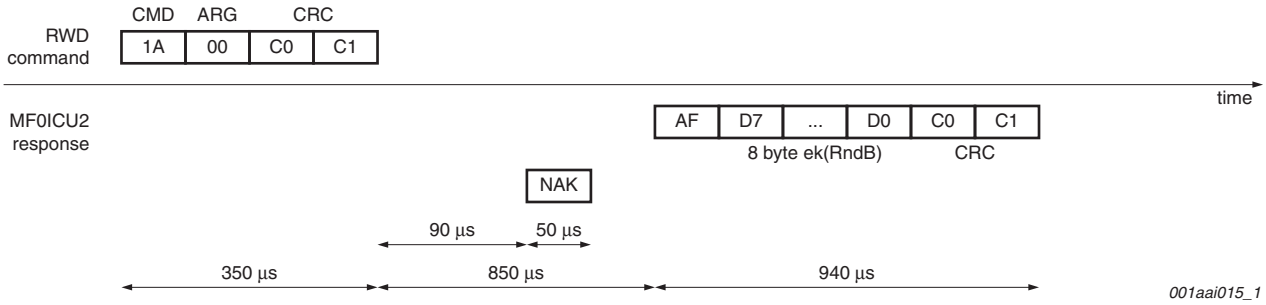
Remark: Time units are not to scale and rounded off to 10 µs

Fig 19. COMPATIBILITY WRITE

8.8.9 AUTHENTICATE

Table 21. AUTHENTICATE Step 1

Code	ARG/ Parameter	Data	Integrity mechanism	Response
1Ah	00	-	Parity, CRC	'AF' + ek(RndB)

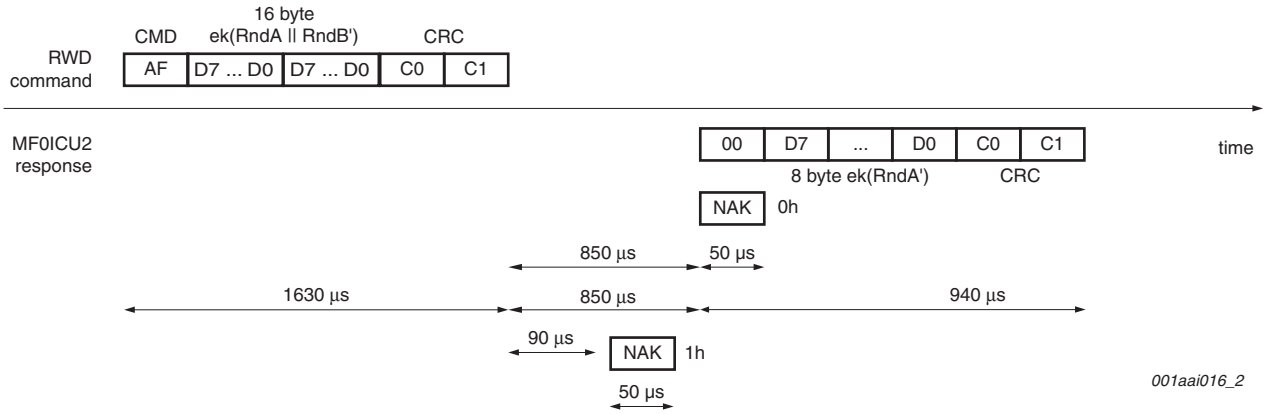


Remark: Time units are not to scale and rounded off to 10 µs

Fig 20. AUTHENTICATE Step 1

Table 22. AUTHENTICATE Step 2

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



Remark: Time units are not to scale and rounded off to 10 µs

Fig 21. AUTHENTICATE Step 2

Description: see more information and a figure showing the authentication process in Section 8.5.4 "3DES Authentication".

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

Executing a HALT command results in losing authentication status.

8.9 Summary of relevant data for device identification

Table 23. Summary of relevant data for device identification

Code	Type	Value	Binary Format	Remark
ATQA	2 Byte	0044h	0000 0000 0100 0100 1st '1' indicates cascade level 2 2nd '1' indicates MIFARE family	OK
CT	1 Byte Cascade Tag	88h	1000 1000 ensures collision with cascade level 1 products	Hard Coded
SAK (casc. level 1)	1 Byte	04h	0000 0100 '1' indicates additional cascade level	OK
SAK (casc. level 2)	1 Byte	00h	0000 0000 indicates complete UID and MF0ICU2 functionality	OK
Manufacturer Byte	1 Byte	04h	0000 0100 indicates manufacturer NXP	Acc. to ISO/IEC 14443-3 and ISO/IEC 7816-6 AMD.1

9. Limiting values

Table 24. 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
T_{stg}	storage temperature			-55	125	°C
T_{amb}	ambient temperature			-25	70	°C
V_{ESD}	electrostatic discharge voltage	measured on pin LA-LB	[3]	2	-	kV

[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

10. Characteristics

10.1 Electrical characteristics

Table 25. Characteristics [1][2][3]

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
f_i	input frequency			-	13.56	-	MHz
C_i	input capacitance	17 pF version (bare silicon and MOA4)	[4]	14.08	16	17.92	pF
C_i	input capacitance	50 pF version	[4]	44	50	56	pF
EEPROM characteristics:							
$t_{cy(W)}$	write cycle time			-	4.1	-	ms
t_{ret}	retention time	T_{amb} = 22 °C		5	-	-	year
$N_{endu(W)}$	write endurance	T_{amb} = 22 °C		10000	-	-	cycle

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

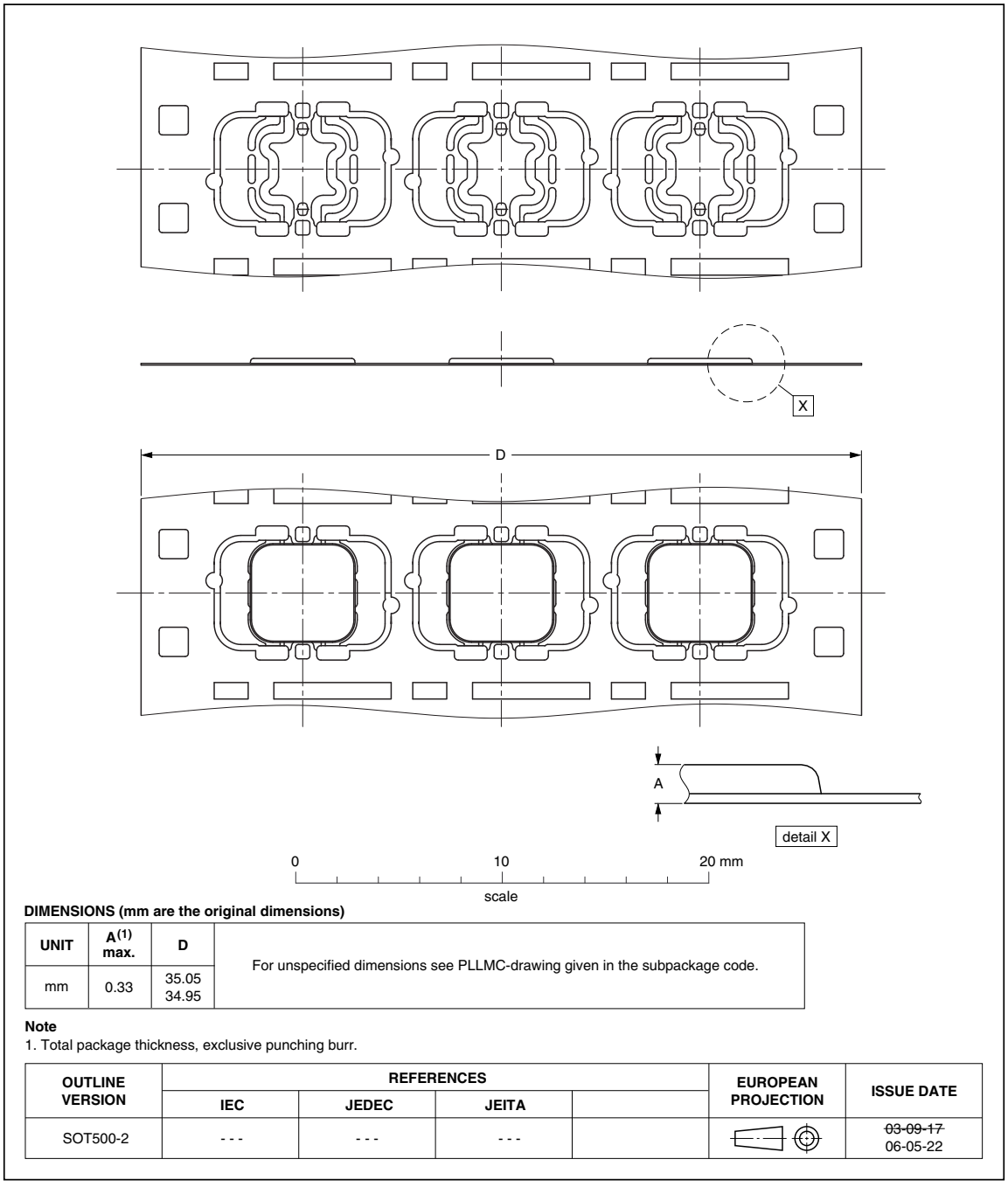
[2] These are stress ratings only. Operation of the device at these or any other conditions above those given in the Characteristics section of the specification is not implied

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

[4] LCR meter HP 4285, T_{amb} = 22 °C, Cp-D, f_i = 13.56 MHz, 2 Veff

11. Package outline

PLLMC: plastic leadless module carrier package; 35 mm wide tape **SOT500-2**



DIMENSIONS (mm are the original dimensions)

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

Note

1. Total package thickness, exclusive punching burr.

OUTLINE VERSION	REFERENCES				EUROPEAN PROJECTION	ISSUE DATE
	IEC	JEDEC	JEITA			
SOT500-2	- - -	- - -	- - -			~~03-09-17~~ 06-05-22

Fig 22. Package outline SOT500-2

12. Abbreviations

Table 26. Abbreviations

Acronym	Description
ACK	Positive Acknowledge
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
IV	Initial Value
MSB	Most Significant Bit
NAK	Negative Acknowledge
LSB	Least Significant Bit
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
3DES	Triple Data Encryption Standard

13. References

[1] ISO/IEC 14443 — International Organziation for Standardization - http://www.iso.org

[2] MIFARE Interface Platform Type Identification Procedure — Application note, BL-ID Doc. No.: 018413

[3] MIFARE ISO/IEC 14443 PICC Selection — Application note, BL-ID Doc. No.: 130810

[4] MIFARE Ultralight Features and Hints — Application note, BL-ID Doc. No.: 073121

[5] MIFARE Ultralight as Type 2 Tag — Application note, BL-ID Doc. No.: 130312

[6] MF0ICU1 Functional specification MIFARE Ultralight — Product data sheet, BL-ID Doc. No. 028635

[7] NIST SP800-67: Recommondation for the TripleData Encryption Algorithm (TDEA) Block Chipher, Version 1.1 May 19, 2008 — National Institute of Standards and Technology

[8] ISO/IEC 10116: Information technology - Security techniques - Modes of operation for an n-bit block chiper, February 1, 2006 — International Organization for Standardization

14. Revision history

Table 27. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
137631	20090402	Product data sheet		137630
Modifications:	• Section 15 “Legal information”: updated			
137630	20090218	Product data sheet	-	137610
Modifications:	• General update			
137610	20080428	Objective data sheet	-	137601
Modifications:	• Update of spelling issues • Redesign of drawings • Update of Section 1.3 “Security” on page 2			
137601	20080404	Objective data sheet	-	-

15. Legal information

15.1 Data sheet status

Document status[1][2]	Product status[3]	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.

15.2 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.

15.3 Disclaimers

General — 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.

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 medical, military, aircraft, space or life support equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors accepts no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

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

Limiting values — Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) may cause permanent damage to the device. Limiting values are stress ratings only and operation of the device at these or any other conditions above those given in the Characteristics sections of this document is not implied. Exposure to limiting values for extended periods may affect device reliability.

Terms and conditions of 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, including those pertaining to warranty, intellectual property rights infringement and limitation of liability, unless explicitly otherwise agreed to in writing by NXP Semiconductors. In case of any inconsistency or conflict between information in this document and such terms and conditions, the latter will prevail.

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 national 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.

15.4 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.

15.5 Trademarks

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

MIFARE — is a trademark of NXP B.V.

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

16. Contact information

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

For sales office addresses, please send an email to: **salesaddresses@nxp.com**

17. Tables

18. Figures

19. Contents

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

Date of release: 2 April 2009
Document identifier: 137631