MF0ICU2

MIFARE Ultralight C

Rev. 3.2 — 19 May 2009
171432

Product short data sheet
PUBLIC

1. General description

NXP Semiconductors 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”). 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 baud rate 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.

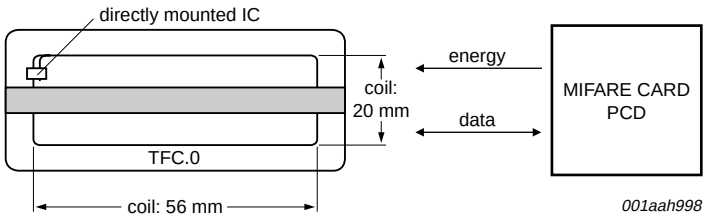


Fig 1. MIFARE card reader

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

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-bit 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. Applications

- Public transport
- Event ticketing
- Prepaid applications
- Loyalty schemes
- NFC Forum Tag Type 2
- Toy and amusement

4. Quick reference data

Table 1. Quick reference data[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
		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.

5. 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)[1]	-
MF0ICU2101DUD	-	8 inch wafer (sawn, laser diced; 120 µm thickness, on film frame carrier; electronic fail die marking according to SECSII format)[2]	-
MF0MOU2001DA4	PLLMC	plastic leadless module carrier package; 35 mm wide tape[1]	SOT500-2
MF0MOU2101DA4	PLLMC	plastic leadless module carrier package; 35 mm wide tape[2]	SOT500-2

[1] 17 pF version.

[2] 50 pF version.

6. Block diagram

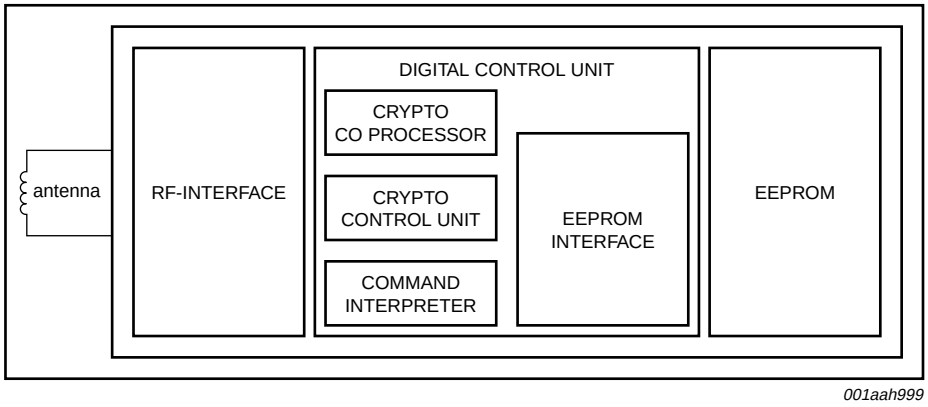


Fig 2. Block diagram

7. Functional description

7.1 Block description

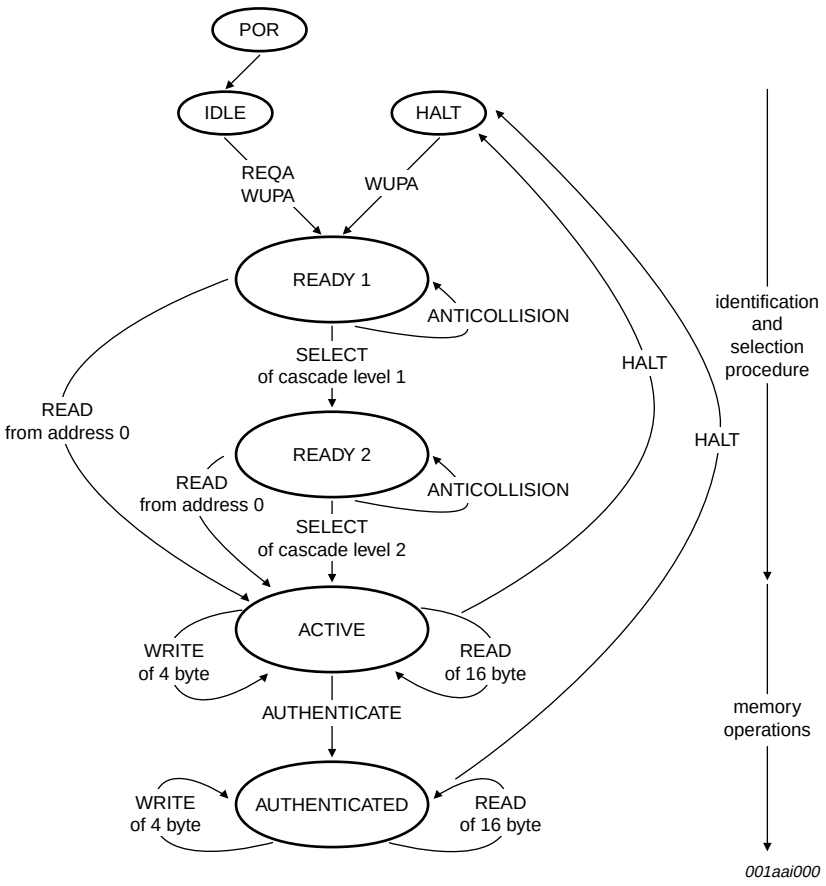
The MF0ICU2 chip consists of the 1536-bit EEPROM, the RF-Interface and the Digital Control Unit. Energy and data are transferred via an antenna, which consists of a coil with a few turns directly connected to the MF0ICU2. No further external components are necessary. (For details on antenna design please refer to the document Ref. 6 “MIFARE (Card) 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 an 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 3 “State diagram”) and generates the appropriate response.

For a correct implementation of an anticollision procedure please refer to the documents in Section 10 “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 3. State diagram

7.3 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 3. 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	-	-
41	29h	16-bit counter	16-bit counter	-	-
42	2Ah	authentication configuration			
43	2Bh	authentication configuration			
44 to 47	2Ch to 2Fh	authentication key			

7.3.1 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. Due to security and system requirements these bytes are write-protected after having been programmed by the IC manufacturer after production.

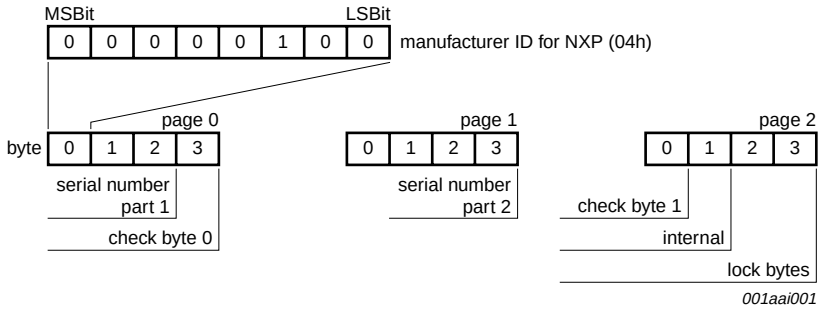


Fig 4. UID/serial number

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.

7.3.2 Lock bytes

Lock bytes enable the user to lock parts of the complete memory area for writing. A Read from user memory area cannot be restricted via lock bytes functionality. For this, please refer to the authentication functionality, (see Section 7.3.4 “3DES Authentication”).

7.3.3 OTP bytes

OPT bytes are pre-set to all “0” after production. These bytes may be bit-wise modified by a WRITE command.

7.3.4 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. 9 “NIST SP800-67: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Version 1.1 May 19, 2008”) in Cipher-Block Chaining (CBC) mode as described in ISO/IEC 10116 (see Ref. 10 “ISO/IEC 10116: Information technology - Security techniques - Modes of operation for an n-bit block cipher, February 1, 2006”).

7.3.5 Data pages

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

A write access to data memory is achieved with WRITE (see Section 7.5.7 “WRITE”) or COMPATIBILITY WRITE (see Section 7.5.8 “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 7.3.2 “Lock bytes”) and/or permanently or temporary restricted using an authentication (see Section 7.3.4 “3DES Authentication”).

NFC Forum Type 2 Tag compliancy

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

7.4 Counter

MF0ICU2 features 16-bit one way counter. In its delivery state, counter value is set to 0000h.

7.5 Command set

The ATQA and SAK are identical as for MF0ICU1 (see Ref. 7 “MF0ICU1 Functional specification MIFARE Ultralight”). For information on ISO 14443 card activation, see Ref. 3 “MIFARE ISO/IEC 14443 PICC Selection”.

The MF0ICU2 comprises the following command set:

7.5.1 REQA

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

7.5.2 WUPA

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

7.5.3 ANTICOLLISION and SELECT of cascade level 1

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.

7.5.4 ANTICOLLISION and SELECT of cascade level 2

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.

7.5.5 READ

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.

7.5.6 HALT

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 their UIDs.

7.5.7 WRITE

The WRITE command is used to program the lock bytes in page 02h, 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.

7.5.8 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'.

7.5.9 AUTHENTICATE

The authentication is performed in two steps, therefore MF0ICU2 command set supports two AUTHENTICATE commands.

The commands are performed in the same protocol as READ, WRITE and COMPATIBILITY WRITE.

8. Limiting values

Table 4. 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.

9. Abbreviations

Table 5. Abbreviations

Acronym	Description
ATQA	Answer To ReQuest, type A
BCC	Block Check Characters byte
CBC	Cipher-Block Chaining
CRC	Cyclic Redundancy Check
EEPROM	Electrically Erasable Programmable Read-Only Memory
NAK	Negative AcKnowledge
OTP	One Time Programmable
PCD	Proximity Coupling Device
PICC	Proximity Integrated Circuit Card
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

10. References

[1] **ISO/IEC —** International Organization for Standardization/International Electrotechnical Commission

[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] **MIFARE (Card) Coil Design Guide —** Application note, BL-ID Doc. No.: 011732

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

[8] **MF0ICU2 MIFARE Ultralight C —** Product data sheet, BL-ID Doc. No. 137631

[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. Revision history

Table 6. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
MF0ICU2_SDS_32	20090519	Product short data sheet PUBLIC	-	-

12. Legal information

12.1 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.

12.2 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.

12.3 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.

12.4 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.

12.5 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.

13. Contact information

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

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

14. Tables

15. Figures

16. 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: 19 May 2009
171432