Chipsmall Limited consists of a professional team with an average of over 10 year of expertise in the distribution of electronic components. Based in Hongkong, we have already established firm and mutual-benefit business relationships with customers from,Europe,America and south Asia,supplying obsolete and hard-to-find components to meet their specific needs.

With the principle of “Quality Parts,Customers Priority,Honest Operation,and Considerate Service”,our business mainly focus on the distribution of electronic components. Line cards we deal with include Microchip,ALPS,ROHM,Xilinx,Pulse,ON,Everlight and Freescale. Main products comprise IC,Modules,Potentiometer,IC Socket,Relay,Connector.Our parts cover such applications as commercial,industrial, and automotives areas.

We are looking forward to setting up business relationship with you and hope to provide you with the best service and solution. Let us make a better world for our industry!

Contact us

Tel: +86-755-8981 8866 Fax: +86-755-8427 6832
Email & Skype: info@chipsmall.com Web: www.chipsmall.com
Address: A1208, Overseas Decoration Building, #122 Zhenhua RD., Futian, Shenzhen, China

MF0ULX1

MIFARE Ultralight EV1 - Contactless ticket IC

Rev. 3.2 — 23 November 2017
234532

Product data sheet
COMPANY PUBLIC

1 General description

NXP Semiconductors developed the MIFARE Ultralight EV1 MF0ULx1 for use in a contactless smart ticket, smart card or token in combination with a Proximity Coupling Device (PCD). The MF0ULx1 is designed to work in an ISO/IEC 14443 Type A compliant environment (see [1]). The target applications include single trip or limited use tickets in public transportation networks, loyalty cards or day passes for events. The MF0ULx1 serves as a replacement for conventional ticketing solutions such as paper tickets, magnetic stripe tickets or coins. It is also a perfect ticketing counterpart to contactless card families such as MIFARE DESFire or MIFARE Plus.

The MIFARE Ultralight EV1 is succeeding the MIFARE Ultralight ticketing IC and is fully functional backwards compatible. Its enhanced feature and command set enable more efficient implementations and offer more flexibility in system designs.

The mechanical and electrical specifications of MIFARE Ultralight EV1 are tailored to meet the requirements of inlay and paper ticket manufacturers.

1.1 Contactless energy and data transfer

In a contactless system, the MF0ULx1 is connected to a coil with a few turns. The MF0ULx1 fits the TFC.0 (Edmondson) and TFC.1 (ISO) ticket formats as defined in Ref. 8.

The MF0ULx1 chip, which is available with 17 pF or 50 pF on-chip resonance capacitor, supports both TFC.1 and TFC.0 ticket formats.

1.2 Anticollision

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

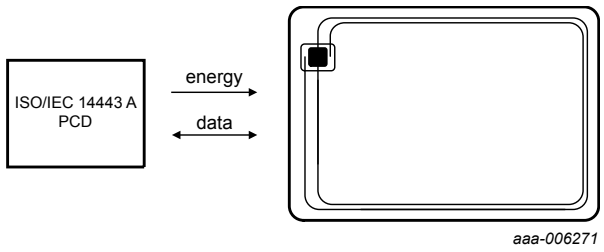


Figure 1. Contactless system

1.3 Simple integration and user convenience

The MF0ULx1 is designed for simple integration and user convenience which allows complete ticketing transactions to be handled in less than 35 ms.

1.4 Security

- Manufacturer programmed 7-byte UID for each device
- 32-bit user definable One-Time Programmable (OTP) area
- 3 independent 24-bit true one-way counters
- Field programmable read-only locking function per page (per 2 pages for the extended memory section)
- ECC based originality signature
- 32-bit password protection to prevent unintended memory operations

1.5 Naming conventions

Table 1. Naming conventions

MF0ULHx101Dyy	Description
MF	MIFARE product family
0	Ultralight product family
UL	Product: MIFARE Ultralight
H	If present, defining high input capacitance H... 50 pF input capacitance
x	One character identifier defining the memory size 1... 640 bit total memory, 384 bit free user memory 2... 1312 bit total memory, 1024 bit free user memory
Dyy	yy defining the delivery type UF... bare die, 75 µm thickness, Au bumps, e-map file UD... bare die, 120 µm thickness, Au bumps, e-map file A8... MOA8 contactless module

2 Features and benefits

- 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

2.1 EEPROM

- 640-bit or 1312-bit, organized in 20 or 41 pages with 4 bytes per page
- Field programmable read-only locking function per page for the first 512 bits
- 32-bit user definable One-Time Programmable (OTP) area
- 3 independent, true one-way 24-bit counters on top of the user area
- Configurable password protection with optional limit of unsuccessful attempts
- Data retention time of 10 years
- Write endurance for one-way counters 1.000.000 cycles
- First 512 bits compatible to MF0ICU1
- Field programmable read-only locking function per 2 pages above page 15
- 384-bit or 1024-bit freely available user Read/ Write area (12 or 32 pages)
- Anti-tearing support for counters, OTP area and lock bits
- ECC based originality signature
- Write endurance 100.000 cycles

3 Applications

- Public transportation
- Event ticketing
- Loyalty

4 Quick reference data

Table 2. Quick reference data

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
C_i	input capacitance MF0ULx1		[1]	-	17.0	-	pF
C_i	input capacitance MF0ULHx1		[1]	-	50.0	-	pF
f_i	input frequency			-	13.56	-	MHz
EEPROM characteristics							
t_{ret}	retention time	T_{amb} = 22 °C		10	-	-	year
$N_{endu(W)}$	write endurance	T_{amb} = 22 °C		100000	-	-	cycle
$N_{endu(W)}$	write endurance counters	T_{amb} = 22 °C		100000	1000000	-	cycle

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

5 Ordering information

Table 3. Ordering information

Type number	Package		
	Name	Description	Version
MF0UL1101DUF	FFC Bump	8 inch wafer, 75 µm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 384 bit user memory, 17 pF input capacitance	-
MF0UL1101DUD	FFC Bump	8 inch wafer, 120 µm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 384 bit user memory, 17 pF input capacitance	-
MF0UL1101DUD2	FFC Bump	12 inch wafer, 120 µm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 384 bit user memory, 17 pF input capacitance	-
MF0ULH1101DUF	FFC Bump	8 inch wafer, 75 µm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 384 bit user memory, 50 pF input capacitance	-
MF0ULH1101DUD	FFC Bump	8 inch wafer, 120 µm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 384 bit user memory, 50 pF input capacitance	-
MF0UL2101DUF	FFC Bump	8 inch wafer, 75 µm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 1024 bit user memory, 17 pF input capacitance	-
MF0UL2101DUD	FFC Bump	8 inch wafer, 120 µm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 1024 bit user memory, 17 pF input capacitance	-
MF0UL2101DUD2	FFC Bump	12 inch wafer, 120 µm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 1024 bit user memory, 17 pF input capacitance	-
MF0ULH2101DUF	FFC Bump	8 inch wafer, 75 µm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 1024 bit user memory, 50 pF input capacitance	-
MF0ULH2101DUD	FFC Bump	8 inch wafer, 120 µm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 1024 bit user memory, 50 pF input capacitance	-
MF0UL2101DA8	MOA8	plastic lead less module carrier package; 35 mm wide tape, 1024 bit user memory, 17 pF input capacitance	SOT500-4

6 Block diagram

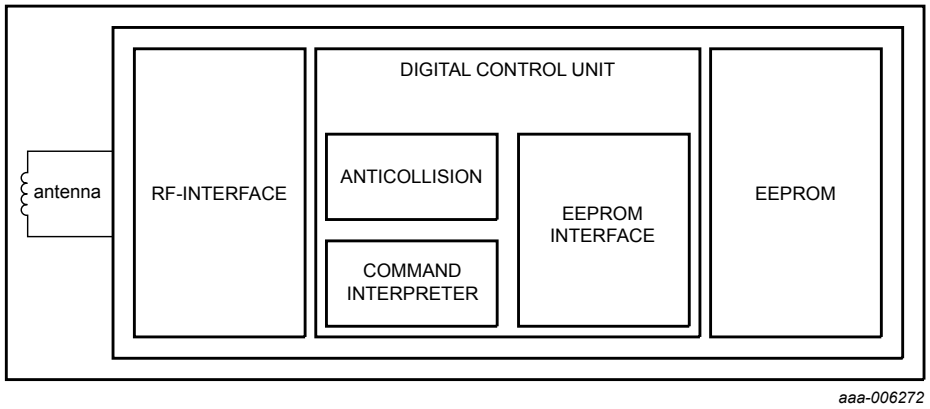


Figure 2. Block diagram of MF0ULx1

7 Pinning information

7.1 Pinning

The pinning for the MF0ULx1DAx is shown Figure 3 for a contactless MOA8 module.

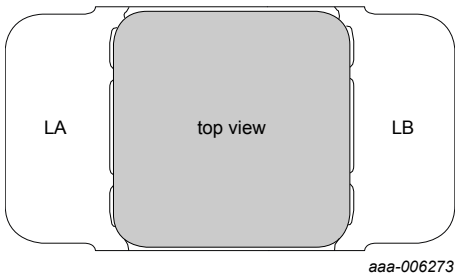


Figure 3. Pin configuration for SOT500-4 (MOA8)

Table 4. Pin allocation table

Pin	Symbol	
LA	LA	antenna coil connection LA
LB	LB	antenna coil connection LB

8 Functional description

8.1 Block description

The MF0ULx1 chip consists of a 640-bit or a 1312-bit EEPROM, RF interface and Digital Control Unit (DCU). Energy and data are transferred via an antenna consisting of a coil with a few turns which is directly connected to the MF0ULx1. No further external components are necessary. Refer to Ref. 2 for details on antenna design.

- RF interface:
  - modulator/demodulator
  - rectifier
  - clock regenerator
  - Power-On Reset (POR)
  - voltage regulator
- Anticollision: multiple cards may be selected and managed in sequence
- Command interpreter: processes memory access commands that the MF0ICU1 supports
- EEPROM interface
- EEPROM: 640 bit, organized in 20 pages of 4 byte per page.
  - 208 bit reserved for manufacturer and configuration data
  - 16 bit used for the read-only locking mechanism
  - 32 bit available as OTP area
  - 384 bit user programmable read/write memory
- EEPROM: 1312 bit, organized in 41 pages of 4 byte per page.
  - 208 bit reserved for manufacturer and configuration data
  - 31 bit used for the read-only locking mechanism
  - 32 bit available as OTP area
  - 1024 bit user programmable read/write memory

8.2 RF interface

The RF-interface is based on the ISO/IEC 14443 Type A standard for contactless smart cards.

During operation, the reader generates an RF field. This RF field must always be present (with short pauses for data communication), as 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 an odd parity bit at the end. The LSB of the byte with the lowest address of the selected block is transmitted first. The maximum length of a PCD to PICC frame is 208 bits (21 data bytes + 2 CRC bytes = 20×9 + 2×9 + 1 start bit). The maximum length for a fixed size PICC to PCD frame is 307 bits (32 data bytes + 2 CRC bytes = 32×9 + 2×9 + 1 start bit). The FAST_READ response has a variable frame length depending on the start and end address parameters. When issuing this command, take into account the maximum frame length that the PCD supports.

For a multi-byte parameter, the least significant byte is always transmitted first. As an example, take reading from the memory using the READ command. Byte 0 from the addressed block is transmitted first after which, byte 1 to byte 3 are transmitted. The same sequence continues for the next block and all subsequent blocks.

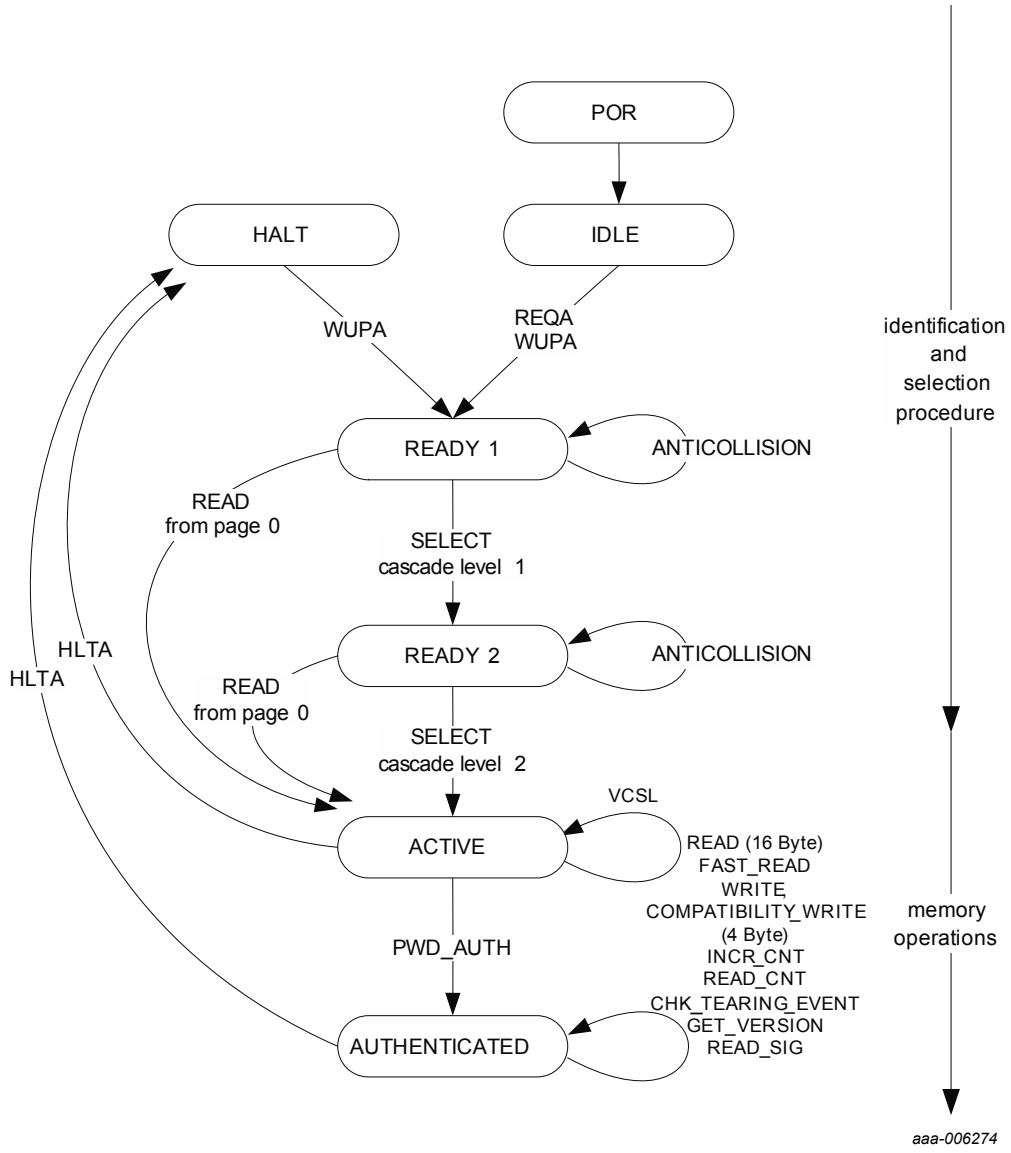
8.3 Data integrity

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

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

8.4 Communication principle

The reader initiates the commands and the Digital Control Unit of the MF0ULx1 controls them. The command response is depending on the state of the IC and for memory operations also on the access conditions valid for the corresponding page.



Remark: In all states, the command interpreter returns to the idle state on receipt of an unexpected command. If the IC was previously in the HALT state, it returns to that state

Remark: The VCSL command is only allowed in the ACTIVE state

Figure 4. State diagram

8.4.1 IDLE state

After a power-on reset (POR), the MF0ULx1 switches to the IDLE state. It only exits this state when a REQA or a WUPA command is received from the PCD. Any other data received while in this state is interpreted as an error and the MF0ULx1 remains in the IDLE state.

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, for example out of the ACTIVE or AUTHENTICATED state, the default waiting state changes from IDLE to HALT. This state can then be exited with a WUPA command only.

8.4.2 READY1 state

In this state, the PCD resolves the first part of the UID (3 bytes) using the ANTICOLLISION or SELECT commands in cascade level 1. This state is exited correctly after execution of either of the following commands:

- SELECT command from cascade level 1: the PCD switches the MF0ULx1 into READY2 state where the second part of the UID is resolved.
- READ command (from address 0): all anticollision mechanisms are bypassed and the MF0ULx1 switches directly to the ACTIVE state.

Remark: If more than one MF0ULx1 is in the PCD field, a READ command from address 0 selects all MF0ULx1 devices. In this case, a collision occurs due to the different serial numbers. Any other data received in the READY1 state is interpreted as an error. Depending on its previous state, the MF0ULx1 returns to either the IDLE state or HALT state.

8.4.3 READY2 state

In this state, the MF0ULx1 supports the PCD in resolving the second part of its UID (4 bytes) with the cascade level 2 ANTICOLLISION command. This state is usually exited using the cascade level 2 SELECT command.

Alternatively, READY2 state can be skipped using a READ command (from address 0) as described for the READY1 state.

Remark: The response of the MF0ULx1 to the cascade level 2 SELECT command is the select acknowledge (SAK) byte. In accordance with ISO/IEC 14443, this byte indicates if the anticollision cascade procedure has finished. It also defines the type of device selected for the MIFARE architecture platform. The MF0ULx1 is now uniquely selected and only this device communicates with the PCD even when other contactless devices are present in the PCD field. If more than one MF0ULx1 is in the PCD field, a READ command from address 0 selects all MF0ULx1 devices. In this case, a collision occurs due to the different serial numbers. Any other data received when the device is in this state is interpreted as an error. Depending on its previous state the MF0ULx1 returns to either the IDLE state or HALT state.

8.4.4 ACTIVE state

All memory operations and other functions like the originality signature read-out are operated in the ACTIVE state.

The ACTIVE state is gratefully exited with the HLTA command and upon reception the MF0ULx1 transits to the HALT state. Any other data received when the device is in this state is interpreted as an error. Depending on its previous state the MF0ULx1 returns to either the IDLE state or HALT state.

The MF0ULx1 transits to the AUTHENTICATED state after successful password verification using the PWD_AUTH command.

8.4.5 AUTHENTICATED state

In this state, all operations on memory pages, which are configured as password verification protected, can be accessed.

The AUTHENTICATED state is gratefully exited with the HLTA command and upon reception the MF0ULx1 transits to the HALT state. Any other data received when the device is in this state is interpreted as an error. Depending on its previous state the MF0ULx1 returns to either the IDLE state or HALT state.

8.4.6 HALT state

The HALT and IDLE states constitute the two wait states implemented in the MF0ULx1. An already processed MF0ULx1 can be set into the HALT state using the HLTA command. In the anticollision phase, this state helps the PCD to distinguish between processed cards and cards yet to be selected. The MF0ULx1 can only exit this state on execution of the WUPA command. Any other data received when the device is in this state is interpreted as an error and the MF0ULx1 state remains unchanged. Refer to Ref. 4 for correct implementation of an anticollision procedure based on the IDLE and HALT states and the REQA and WUPA commands.

8.5 Memory organization

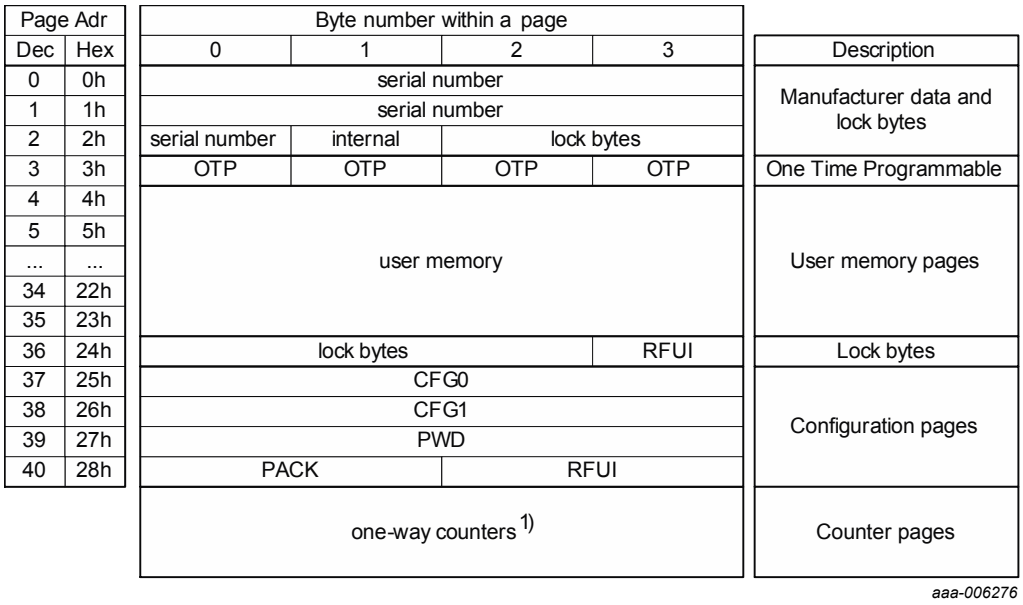
The EEPROM memory is organized in pages with 4 bytes per page. The MF0UL11 variant has 20d pages and the MF0UL21 variant has 41d pages in total. The memory organization can be seen in Figure 5 and Figure 6, the functionality of the different memory sections is described in the following sections.

<table>
<tr><th colspan="2">Page Adr</th><th colspan="4">Byte number within a page</th><th></th></tr>
<tr><th>Dec</th><th>Hex</th><th>0</th><th>1</th><th>2</th><th>3</th><th>Description</th></tr>
<tr><td>0</td><td>0h</td><td colspan="4">serial number</td><td rowspan="2">Manufacturer data and lock bytes</td></tr>
<tr><td>1</td><td>1h</td><td colspan="4">serial number</td></tr>
<tr><td>2</td><td>2h</td><td>serial number</td><td>internal</td><td colspan="2">lock bytes</td><td></td></tr>
<tr><td>3</td><td>3h</td><td>OTP</td><td>OTP</td><td>OTP</td><td>OTP</td><td>One Time Programmable</td></tr>
<tr><td>4</td><td>4h</td><td colspan="4" rowspan="12">user memory</td><td rowspan="12">User memory pages</td></tr>
<tr><td>5</td><td>5h</td></tr>
<tr><td>...</td><td>...</td></tr>
<tr><td>14</td><td>Eh</td></tr>
<tr><td>15</td><td>Fh</td></tr>
<tr><td>16</td><td>10h</td></tr>
<tr><td>17</td><td>11h</td></tr>
<tr><td>18</td><td>12h</td></tr>
<tr><td>19</td><td>13h</td><td colspan="4">CFG0</td><td rowspan="4">Configuration pages</td></tr>
<tr><td></td><td></td><td colspan="4">CFG1</td></tr>
<tr><td></td><td></td><td colspan="4">PWD</td></tr>
<tr><td></td><td></td><td colspan="2">PACK</td><td colspan="2">RFUI</td></tr>
<tr><td colspan="2"></td><td colspan="4">One-Way counters [1]</td><td>Counter pages</td></tr>
</table>

aaa-006275

1. counter pages are only accessible with READ_CNT and INCR_CNT commands

Figure 5. Memory organization MF0UL11



1. counter pages are only accessible with READ_CNT and INCR_CNT commands

Figure 6. Memory organization MF0UL21

8.5.1 UID/serial number

The unique 7-byte serial number (UID) and its two check bytes are programmed into the first 9 bytes of memory covering page addresses 00h, 01h and the first byte of page 02h. The second byte of page address 02h is reserved for internal data. These bytes are programmed and write protected in the production test.

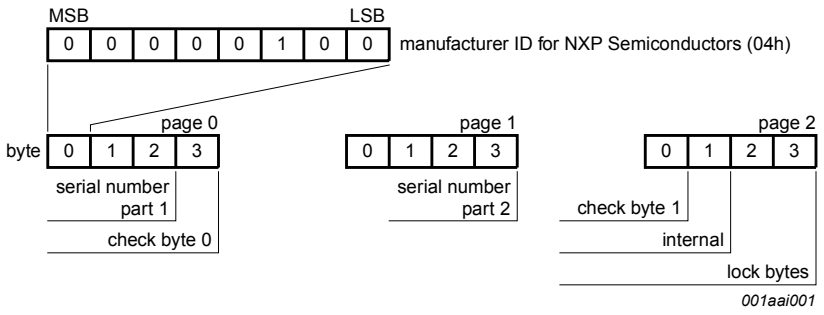


Figure 7. UID/serial number

In accordance with ISO/IEC 14443-3 check byte 0 (BCC0) is defined as CT Å SN0 Å SN1 Å SN2. Check byte 1 (BCC1) is defined as SN3 Å SN4 Å SN5 Å SN6.

SN0 holds the Manufacturer ID for NXP Semiconductors (04h) in accordance with ISO/IEC 14443-3 and ISO/IEC 7816-6 AMD.1

8.5.2 Lock byte 0 and byte 1

The bits of byte 2 and byte 3 of page 02h represent the field programmable 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 page becomes read-only memory.

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.

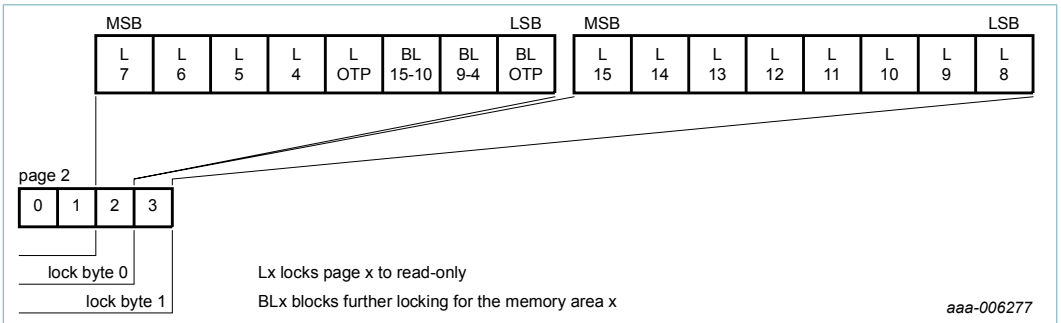


Figure 8. Lock bytes 0 and 1

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.

The contents of bytes 0 and 1 of page 02h are unaffected by the corresponding data bytes of the WRITE or COMPATIBILITY_WRITE command.

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

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

Remark: Setting a lock bit to 1 immediately prevents write access to the respective page

8.5.3 Lock byte 2 to byte 4

To lock the pages of the MF0UL21 starting at page address 10h onwards, the lock bytes 2-4 located in page 24h are used. Those three lock bytes cover the memory area of 80 data bytes. The granularity is 2 pages, compared to a single page for the first 512 bits as shown in Figure 9.

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

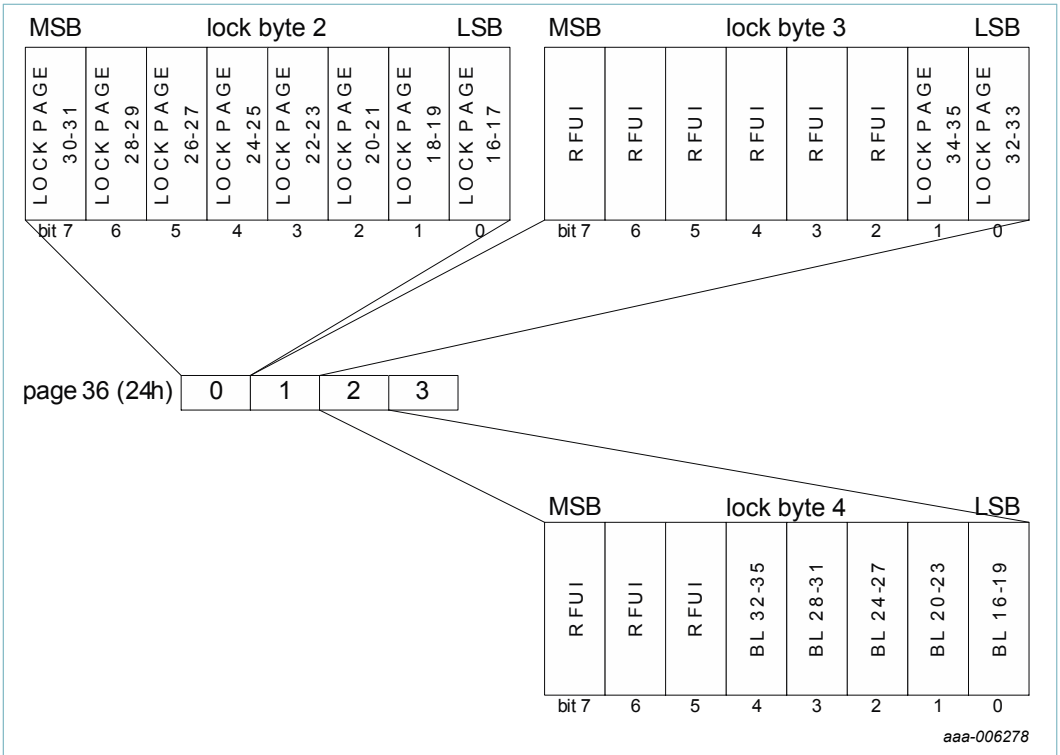


Figure 9. Lock bytes 2-4

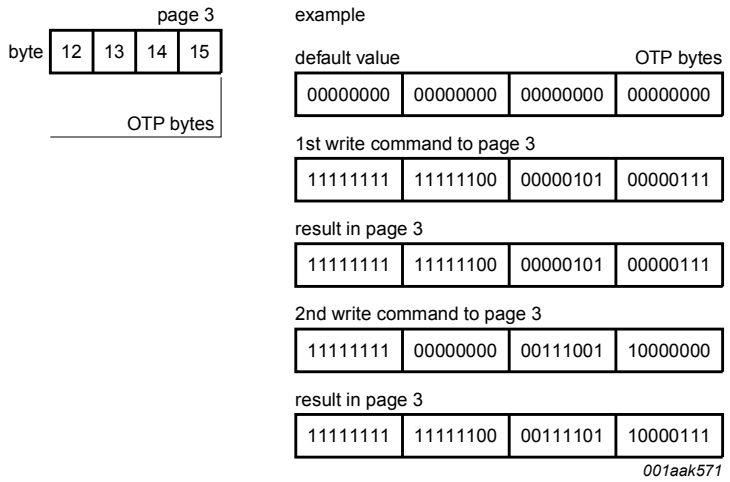
The default value of lock bytes 2-4 is 00 00 00h. The value of byte 3 on page 36 (see Figure 9) is always BDh when read.

Any write operation to the lock bytes 2-4, features anti-tearing support.

Remark: Setting a lock bit to 1 immediately prevents write access to the respective pages

8.5.4 OTP bytes

Page 03h is the OTP page and it is preset so that all bits are set to logic 0 after production. These bytes can be bit-wise modified using the WRITE or COMPATIBILITY_WRITE command.



This memory area can be used as a 32 tick one-time counter.

Figure 10. OTP bytes

The parameter bytes of the WRITE command and the current contents of the OTP bytes are bit-wise OR'ed. The result is the new OTP byte contents. This process is irreversible and once a bit is set to logic 1, it cannot be changed back to logic 0.

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

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

8.5.5 Data pages

Pages 04h to 0Fh for the MF0UL11 and 04h to 23h for the MF0UL21 are the user memory read/write area.

The access to a part of the user memory area can be restricted using a password verification. See Section 8.6 for further details.

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

8.5.6 Configuration pages

Pages 10h-13h for the MF0UL11 and pages 25h-28h for the MF0UL21 variant, are used to configure the memory access restriction of the MF0ULx1. They are also used to configure the response to a VCSL command. The memory content of the configuration pages is detailed in Table 5, Table 7 and Table 8.

Table 5. Configuration Pages

Page Address		Byte number			
Dec	Hex	0	1	2	3
16/37	10h/25h	MOD	RFUI	RFUI	AUTH0
17/38	11h/26h	ACCESS	VCTID	RFUI	RFUI
18/39	12h/27h	PWD			
19/40	13h/28h	PACK		RFUI	RFUI

1. page address for MF0UL11/MF0UL21

Table 6. MOD configuration byte

Bit number							
7	6	6	4	3	2	1	0
RFUI					STRG_MOD_EN	RFUI	

Table 7. ACCESS configuration byte

Bit number							
7	6	6	4	3	2	1	0
PROT	CFGLCK	RFUI			AUTHLIM		

Table 8. Configuration parameter descriptions

Field	Bit	Default Value	Description
STRG_ MOD_EN	1	0b/1b[1]	STRG MOD_EN defines the modulation mode 0b ... strong modulation mode disabled 1b ... strong modulation mode enabled
AUTH0	8	FFh	AUTH0 defines the page address from which the password verification is required. Valid address range for byte AUTH0 is 00h to FFh. If AUTH0 is set to a page address which is higher than the last user configuration page, the password protection is effectively disabled.
PROT	1	0b	One bit inside the ACCESS byte defining the memory protection 0b ... write access is protected by the password verification 1b ... read and write access is protected by the password verification
CFGLCK	1	0b	Write locking bit for the user configuration 0b ... user configuration open to write access 1b ... user configuration permanently locked against write access
AUTHLIM	3	000b	Limitation of negative password verification attempts 000b... limiting of negative password verification attempts disabled 001b-111b ... maximum number of negative password verification attempts
VCTID	8	05h	Virtual Card Type Identifier which represents the response to a VCSL command. To ensure infrastructure compatibility, it is recommended not to change the default value of 05h.
PWD	32	FFFF FFFFh	32-bit password used for memory access protection
PACK	16	0000h	16-bit password acknowledge used during password verification
RFUI	-	all 0b	Reserved for future use - implemented. Write all bits and bytes denoted as RFUI as 0b.

[1] Values for MF0ULx1/MF0ULHx1. The STRG_MOD_EN feature is only available on the high capacitance variants MF0ULHx1 types. For the MF0ULx1 types, this bit is set to 0b and only the strong modulator is available.

Remark: The CFGLCK bit activates the permanent write protection of the first two configuration pages. The write lock is only activated after a power cycle of the MF0ULx1. If write protection is enabled, each write attempt leads to a NAK response.

8.6 Password verification protection

The memory write or read/write access to a configurable part of the memory can be constrained to a positive password verification. The 32-bit secret password (PWD) and the 16-bit password acknowledge (PACK) are typically programmed into the configuration pages at ticket issuing or personalization. The use of a chip individual password acknowledge response raises the trust level on the PCD side into the PICC.

The AUTHLIM parameter specified in Section 8.5.6 can be used to limit the negative verification attempts.

In the initial state of the MF0ULx1, an AUTH0 value of FFh disables password protection. PWD and PACK are freely writable in this state. Access to the configuration pages and any part of the user memory, can be restricted by setting AUTH0 a page address within the available memory space. The page address is the first one protected.

Remark: Note that the password verification method available in then MF0ULx1 does not offer a high security protection. It is an easy and convenient way to prevent unauthorized memory access. If a higher level of protection is required, cryptographic methods on application layer can be used to increase overall system security.

8.6.1 Programming of PWD and PACK

Program the 32-bit PWD and the 16-bit PACK into the configuration pages, see Section 8.5.6. The password as well as the password acknowledge, are written LSByte first. This byte order is the same as the byte order used during the PWD_AUTH command and its response.

The PWD and PACK bytes can never be read out of the memory. Instead of transmitting the real value on any valid READ or FAST_READ command, only 00h bytes are replied.

If the password verification does not protect the configuration pages, PWD and PACK can be written with normal WRITE and COMPATIBILITY_WRITE commands.

If the password verification protects the configuration pages, PWD and PACK can only be written after a successful PWD_AUTH command.

The PWD and PACK are writable even if the CFGLCK bit is set to 1b. Therefore it is strongly recommended to set AUTH0 to the page where the PWD is located after the password has been written. This page is 12h for the MF0UL11 and 27h for the MF0UL21.

Remark: To improve the overall system security, it is strongly recommended to diversify the password and the password acknowledge using a die individual parameter, that is, the 7-byte UID available on the MF0ULx1.

8.6.2 Limiting negative verification attempts

To prevent brute-force attacks on the password, the maximum allowed number of negative password verification attempts can be set using AUTHLIM. This mechanism is disabled by setting AUTHLIM to a value of 000b which is also the initial state of the MF0ULx1.

If AUTHLIM is not equal to 000b, each negative authentication verification is internally counted. The count operation features anti-tearing support. As soon as this internal counter reaches the number specified in AUTHLIM, any further negative password verification leads to a permanent locking of the protected part of the memory for the

specified access modes. Independent, whether the provided password is correct or not, each subsequent PWD_AUTH fails.

Any successful password verification, before reaching the limit of negative password verification attempts, resets the internal counter to zero.

8.6.3 Protection of special memory segments

The configuration pages can be protected by the password authentication as well. The protection level is defined with the PROT bit.

The protection is enabled by setting the AUTH0 byte to a value that is within the addressable memory space.

All counters can always be incremented and read without prior password verification.

8.7 Counter functionality

The MF0ULx1 features three independent 24-bit one-way counters. These counters are located in a separate part of the NVM which is not directly addressable using READ, FAST_READ, WRITE or COMPATIBILITY_WRITE commands. The actual value can be retrieved by using the READ_CNT command, the counters can be incremented with the INCR_CNT command. The INCR_CNT command features anti-tearing support, thus no undefined values originating from interrupted programing cycles are possible. Either the value is unchanged or the correct, incremented value is correctly programmed into the counter. The occurrence of a tearing event can be checked using the CHECK_TEARING_EVENT command.

In the initial state, the counter values are set to 000000h.

The counters can be incremented by an arbitrary value. The incremented value is valid immediately and does not require a RF reset or re-activation. Once counter value reaches FFFFFFh and an increment is performed via a valid INCR_CNT command, the MF0ULx1 replies a NAK. If the sum of the addressed counter value and the increment value in the INCR_CNT command is higher than FFFFFFh, the MF0ULx1 replies a NAK and does not update the respective counter.

An increment by zero (000000h) is always possible, but does not have any impact on the counter value.

8.8 Originality function

The MF0ULx1 features a cryptographically supported originality check. With this feature, it is possible to verify with a certain probability, that the ticket is using an NXP Semiconductors manufactured silicon. This check can also be performed on personalized tickets.

Each MF0ULx1 holds a 32-byte cryptographic signature based on elliptic curve cryptography. This signature can be retrieved using the READ_SIG command and can be verified using the corresponding ECC public key in the PCD.

8.9 Virtual Card Architecture Support

The MF0ULx1 supports the virtual card architecture by replying to a Virtual Card Select Last (VCSL) command with a virtual card type identifier. The VCTID that is replied can be

programmed in the configuration pages. It enables infrastructure supporting this feature to process MIFARE cards across different MIFARE families in a common way.

For example, a contactless system is enabled to select a specific virtual MIFARE card inside a mobile phone. It can use the same card identification principle to detect that the MF0ULx1 belongs to the system.

9 Command overview

The MIFARE Ultralight card activation follows the ISO/IEC 14443 Type A. After the MIFARE Ultralight card has been selected, it can either be deactivated using the ISO/IEC 14443 HLTA command, or the MIFARE Ultralight commands can be performed. For more details about the card activation, refer to Ref. 1.

9.1 MIFARE Ultralight EV1 command overview

All available commands for the MIFARE Ultralight are shown in Table 9.

Table 9. Command overview

Command[1]	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	HLTA	50h 00h
GET_VERSION[2]	-	60h
READ	-	30h
FAST_READ[2]	-	3Ah
WRITE	-	A2h
COMP_WRITE	-	A0h
READ_CNT[2]	-	39h
INCR_CNT[2]	-	A5h
PWD_AUTH[2]	-	1Bh
READ_SIG[2]	-	3Ch
CHECK_TEARING_EVENT[2]	-	3Eh
VCSL[2]	-	4Bh

[1] Unless otherwise specified, all commands use the coding and framing as described in Ref. 1.
[2] this command is new in MIFARE Ultralight EV1 compared to MIFARE Ultralight

9.2 Timing

The command and response timings 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. 1 as an integer **n** which specifies the PCD to PICC frame delay time. The frame delay time from PICC to PCD has a minimum n of 9. The maximum command response time is specified as a time-out value. Depending on the command, the T_{ACK} value specified for command responses defines the PCD to PICC frame delay time. It does it for either the 4-bit ACK value specified in Section 9.3 or for a data frame.

All command timings are according to ISO/IEC 14443-3 frame specification as shown for the Frame Delay Time in Figure 11. For more details, refer to Ref. 1.

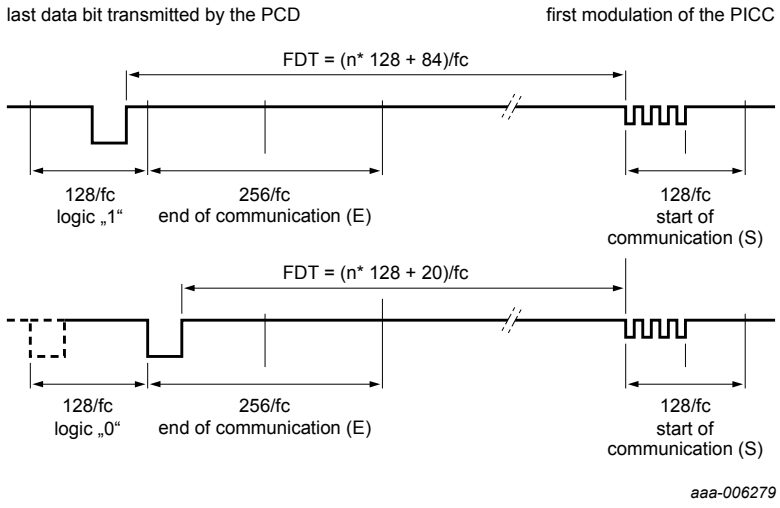


Figure 11. Frame Delay Time (from PCD to PICC)

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 times with the measured times.

9.3 MIFARE Ultralight ACK and NAK

The MIFARE Ultralight uses a 4-bit ACK / NAK as shown in Table 10.

Table 10. ACK and NAK values

Code (4-bit)	ACK/NAK
Ah	Acknowledge (ACK)
0h	NAK for invalid argument (i.e. invalid page address)
1h	NAK for parity or CRC error

Code (4-bit)	ACK/NAK
4h	NAK for counter overflow
5h, 7h	NAK for EEPROM write error
6h, 9h	NAK, other error

9.4 ATQA and SAK responses

For details on the type identification procedure, refer to Ref. 3.

The MF0ULx1 replies to a REQA or WUPA command with the ATQA value shown in Table 11. It replies to a Select CL2 command with the SAK value shown in Table 12. The 2-byte ATQA value is transmitted with the least significant byte first (44h).

Table 11. ATQA response of the MF0ULx1

		Bit number														
Sales type	Hex value	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
MF0ULx1	00 44h	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0

Table 12. SAK response of the MF0ULx1

		Bit number							
Sales type	Hex value	8	7	6	5	4	3	2	1
MF0ULx1	00h	0	0	0	0	0	0	0	0

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

Remark: The bit numbering in the ISO/IEC 14443 starts with LSB = bit 1 and not with LSB = bit 0. So 1 byte counts bit 1 to bit 8 instead of bit 0 to 7.

10 MIFARE Ultralight EV1 commands

10.1 GET_VERSION

The GET_VERSION command is used to retrieve information on the MIFARE family, product version, storage size and other product data required to identify the MF0ULx1.

This command is available on other MIFARE products to have a common way of identifying products across platforms and evolution steps.

The GET_VERSION command has no arguments and replies the version information for the specific MF0ULx1 type. The command structure is shown in Figure 12 and Table 13.

Table 14 shows the required timing.

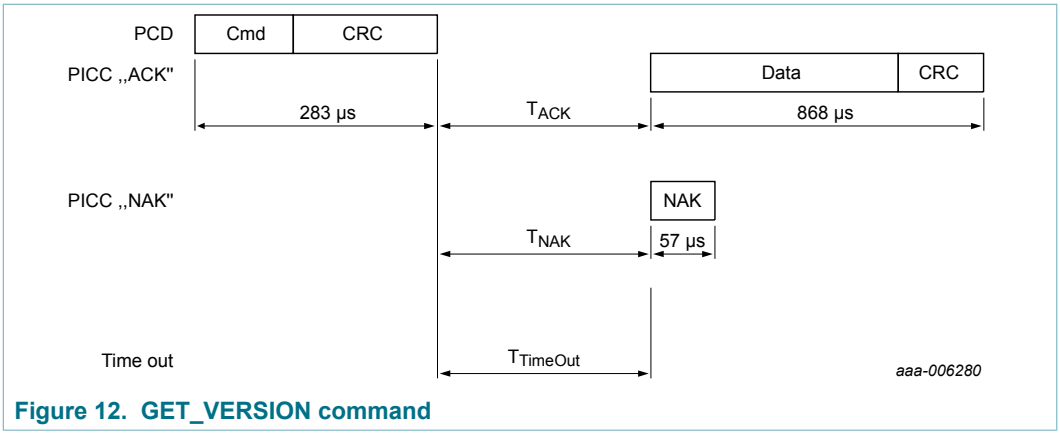


Figure 12. GET_VERSION command

Table 13. GET_VERSION command

Name	Code	Description	Length
Cmd	60h	Get product version	1 byte
CRC	-	CRC according to Ref. 1	2 bytes
Data	-	Product version information	8 bytes
NAK	see Table 10	see Section 9.3	4-bit

Table 14. GET_VERSION timing

These times exclude the end of communication of the PCD.

	T_{ACK} min	T_{ACK} max	T_{NAK} min	T_{NAK} max	$T_{TimeOut}$
GET_VERSION	n=9	$T_{TimeOut}$	n=9	$T_{TimeOut}$	5 ms

Table 15. GET_VERSION response for MF0UL11 and MF0UL21

Byte no.	Description	MF0UL11/ MF0ULH11	MF0UL21/ MF0ULH21	Interpretation
0	fixed header	00h	00h	
1	vendor ID	04h	04h	NXP Semiconductors
2	product type	03h	03h	MIFARE Ultralight
3	product subtype	01h/02h	01h/02h	17 pF / 50pF
4	major product version	01h	01h	EV1
5	minor product version	00h	00h	V0
6	storage size	0Bh	0Eh	see following explanation
7	protocol type	03h	03h	ISO/IEC 14443-3 compliant

The most significant 7 bits of the storage size byte are interpreted as an unsigned integer value n. As a result, it codes the total available user memory size as 2^n. If the least significant bit is 0b, the user memory size is exactly 2^n. If the least significant bit is 1b, the user memory size is between 2^n and 2^{n+1}.

The user memory for the MF0UL11 is 48 bytes. This memory size is between 32d bytes and 64d bytes. Therefore, the most significant 7 bits of the value 0Bh, are interpreted as 5d and the least significant bit is 1b.

The user memory for the MF0UL21 is 128 bytes. This memory size is exactly 128d. Therefore, the most significant 7 bits of the value 0Eh, are interpreted as 7d and the least significant bit is 0b.

10.2 READ

The READ command requires a start page address, and returns the 16 bytes of four MIFARE Ultralight pages. For example if address (Addr) is 03h then pages 03h, 04h, 05h, 06h are returned. A rollover mechanism is implemented if the READ command address is near the end of the accessible memory area. This rollover mechanism is also used when at least part of the addressed pages is within a password protected area. For details on those cases see the description below. The command structure is shown in Figure 13 and Table 16.

Table 17 shows the required timing.

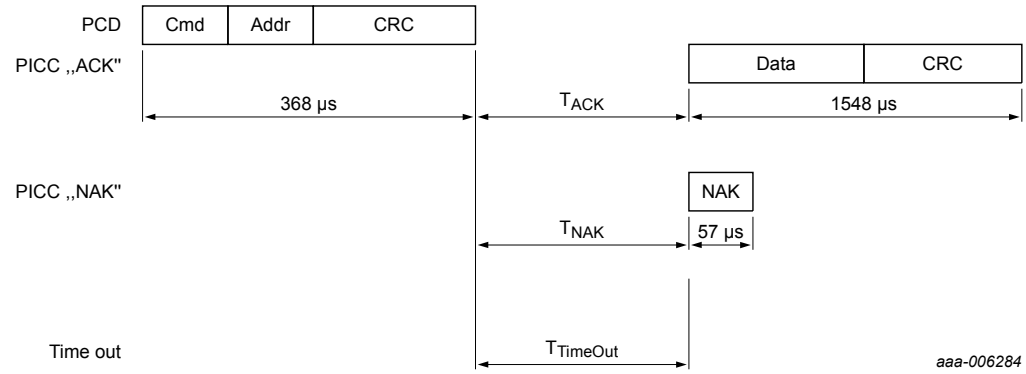


Figure 13. READ command

Table 16. READ command

Name	Code	Description	Length
Cmd	30h	read four pages	1 byte
Addr	-	start page address	1 byte
CRC	-	CRC according to Ref. 1	2 bytes
Data	-	Data content of the addressed pages	16 bytes
NAK	see Table 10	see Section 9.3	4-bit

Table 17. READ timing

These times exclude the end of communication of the PCD.

	T_{ACK} min	T_{ACK} max	T_{NAK} min	T_{NAK} max	$T_{TimeOut}$
READ	n=9	$T_{TimeOut}$	n=9	$T_{TimeOut}$	5 ms

In the initial state of the MF0ULx1, all memory pages are allowed as Addr parameter to the READ command.

- page address 00h to 13h for the MF0UL11
- page address 00h to 28h for the MF0UL21

Addressing a memory page beyond the limits above results in a NAK response from the MF0ULx1.

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 11h on a MF0UL11 results in pages 11h, 12h, 13h and 00h being returned.

The following conditions apply if part of the memory is password protected for read access:

- if the MF0ULx1 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 MF0ULx1 is in the AUTHENTICATED state
  - the READ command behaves like on a MF0ULx1 without access protection

Remark: PWD and PACK values can never be read out of the memory. When reading from the pages holding those two values, all 00h bytes are replied to the PCD instead.

10.3 FAST_READ

The FAST_READ command requires a start page address and an end page address and returns the all n*4 bytes of the addressed pages. For example if the start address is 03h and the end address is 07h then pages 03h, 04h, 05h, 06h and 07h are returned. If the addressed page is outside of accessible area, the MF0ULx1 replies a NAK. For details on those cases and the command structure, refer to Figure 14 and Table 18.

Table 19 shows the required timing.

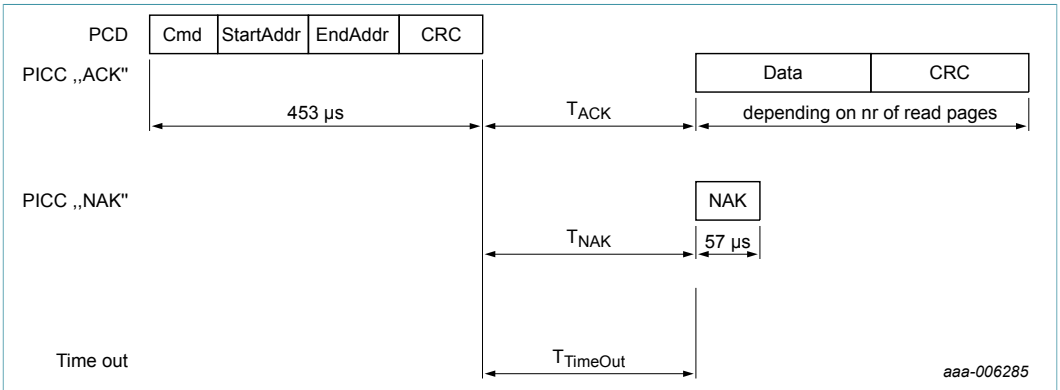


Figure 14. FAST_READ command

Table 18. FAST_READ command

Name	Code	Description	Length
Cmd	3Ah	read multiple pages	1 byte

Name	Code	Description	Length
StartAddr	-	start page address	1 byte
EndAddr	-	end page address	1 byte
CRC	-	CRC according to Ref. 1	2 bytes
Data	-	data content of the addressed pages	n*4 bytes
NAK	see Table 10	see Section 9.3	4-bit

Table 19. FAST_READ timing

These times exclude the end of communication of the PCD.

	T_{ACK} min	T_{ACK} max	T_{NAK} min	T_{NAK} max	$T_{TimeOut}$
FAST_READ	n=9	$T_{TimeOut}$	n=9	$T_{TimeOut}$	5 ms

In the initial state of the MF0ULx1, all memory pages are allowed as StartAddr parameter to the FAST_READ command.

- page address 00h to 13h for the MF0UL11
- page address 00h to 28h for the MF0UL21

Addressing a memory page beyond the limits above results in a NAK response from the MF0ULx1.

The EndAddr parameter must be equal to or higher than the StartAddr.

The following conditions apply if part of the memory is password protected for read access:

- if the MF0ULx1 is in the ACTIVE state
  - if any requested page address is equal or higher than AUTH0 a NAK is replied
- if the MF0ULx1 is in the AUTHENTICATED state
  - the FAST_READ command behaves like on a MF0ULx1 without access protection

Remark: PWD and PACK values can never be read out of the memory. When reading from the pages holding those two values, all 00h bytes are replied to the PCD instead.

Remark: The FAST_READ command is able to read out the whole memory with one command. Nevertheless, receive buffer of the PCD must be able to handle the requested amount of data as there is no chaining possibility.

10.4 WRITE

The WRITE command requires a block address, and writes 4 bytes of data into the addressed MIFARE Ultralight EV1 page. The WRITE command is shown in Figure 15 and Table 20.

Table 21 shows the required timing.

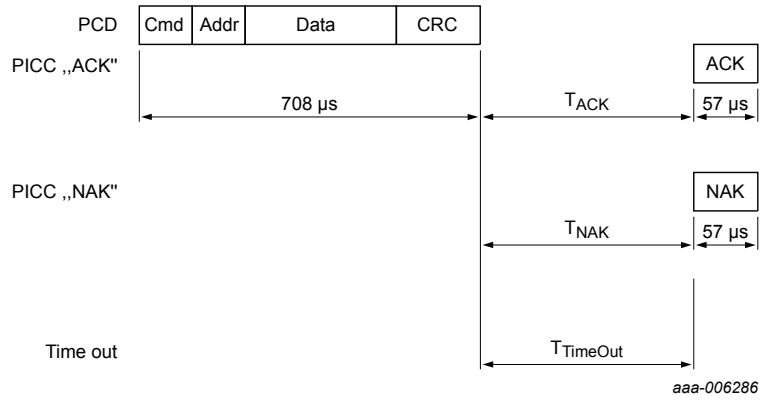


Figure 15. WRITE command

Table 20. WRITE command

Name	Code	Description	Length
Cmd	A2h	write one page	1 byte
Addr	-	page address	1 byte
CRC	-	CRC according to Ref. 1	2 bytes
Data	-	data	4 bytes
NAK	see Table 10	see Section 9.3	4-bit

Table 21. WRITE timing

These times exclude the end of communication of the PCD.

	T_{ACK} min	T_{ACK} max	T_{NAK} min	T_{NAK} max	$T_{TimeOut}$
WRITE	n=9	$T_{TimeOut}$	n=9	$T_{TimeOut}$	5 ms

In the initial state of the MF0ULx1, the following memory pages are valid Addr parameters to the WRITE command.

- page address 02h to 13h for the MF0UL11
- page address 02h to 28h for the MF0UL21

Addressing a memory page beyond the limits above results in a NAK response from the MF0ULx1.

Pages which are locked against writing cannot be reprogrammed using any write command. The locking mechanisms include lock bits as well as the locking of the configuration pages.

The following conditions apply if part of the memory is password protected for write access:

- if the MF0ULx1 is in the ACTIVE state
  - writing to a page which address is equal or higher than AUTH0 results in a NAK response
- if the MF0ULx1 is in the AUTHENTICATED state
  - the WRITE command behaves like on a MF0ULx1 without access protection