Download from http://www.engracetech.com

DATA SHEET

mifare® ultra light

Contactless Single-trip Ticket IC

MF0 IC U1

Functional Specification

Product Specification

March 2003

Revision 3.0

PUBLIC

Philips
Semiconductors

PHILIPS

Download from http://www.engracetech.com

CONTENTS

Download from http://www.engracetech.com

MIFARE® is a registered trademark of Philips Electronics N.V.

Download from http://www.engracetech.com

1 FEATURES

1.1 MIFARE® RF Interface (ISO/IEC 14443 A)

- Contactless transmission of data and supply energy (no battery needed)
- Operating distance: Up to 100mm (depending on 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/IEC14443-3)
- Typical ticketing transaction: < 35 ms
- Fast counter transaction: < 10 ms

1.2 EEPROM

- 512 bit, organised in 16 pages with 4 byte each
- Field programmable read-only locking function per page
- 32 bit user definable One Time Programmable (OTP) area
- 384 bit user r/w area (12 pages)
- Data retention of 5 years
- Write endurance 10000 cycles

1.3 Security

- 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

Download from http://www.engracetech.com

2 GENERAL DESCRIPTION

Philips has developed the MIFARE® MF0 IC U1 to be used with Proximity Coupling Devices (PCD) according to ISO/IEC14443A. The communication layer (MIFARE® RF Interface) complies to parts 2 and 3 of the ISO/IEC14443A standard. The MF0 IC U1 is primarily designed for contactless single trip ticket solutions in transport applications.

2.1 Contactless Energy and Data Transfer

In the MIFARE® system, the MF0 IC U1 is connected to a coil with a few turns. The MF0 IC U1 fits for the TFC.0 (Edmonson) and TFC.1 ticket formats as defined in EN753-2.

TFC.1 ticket formats are supported by the MF0 IC U10 chip featuring an on-chip resonance capacitor of 16.9 pF.

The smaller TFC.0 tickets are supported by the MF0 IC U11 chip holding an on-chip resonance capacitor of 50 pF.

No battery is needed. When the ticket is positioned in the proximity of the coupling device (PCD) antenna, the high speed RF communication interface allows to transmit data with 106 kBit/s.

2.2 Anticollision

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

2.2.1 CASCADED UID

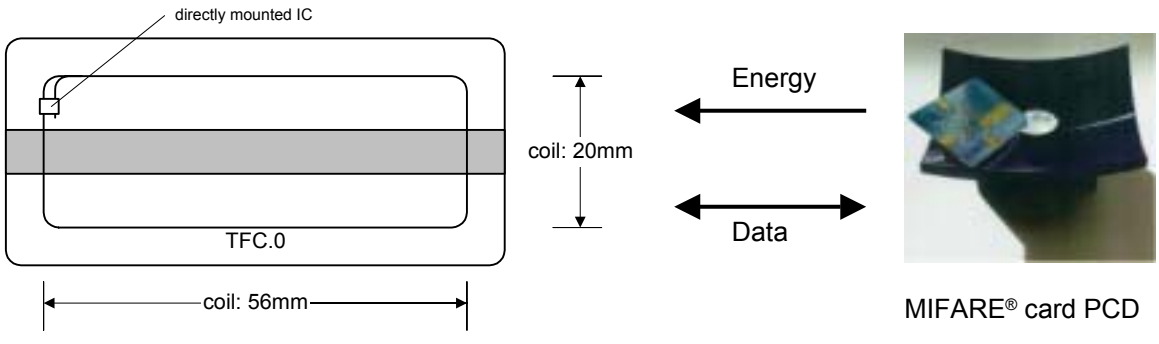
The anticollision function is based on an IC individual serial number called **U**nique **ID**entification. The UID of the MF0 IC U1 is 7 bytes long and supports cascade level 2 according to ISO/IEC14443-3.

2.3 Security

The 7 byte UID is unchangeably programmed into each device during production. It cannot be altered and guarantees the uniqueness of each device. This is an effective anti-cloning mechanism. It may be used for a crypto-graphically secured data storage in the ticket memory. The UID may be used to derive diversified keys per ticket for an appropriate cryptographic system.

The 32 Bit OTP area provides write once operations e.g. for a one-time counter. It may be used for permanent de-validation of a ticket.

The field programmable read-only locking function allows to fix data per page to an unchangeable value. This function may be used to uniquely program the device for a dedicated application.



MIFARE® card PCD

Note: Evaluations show that with the above configuration (6 turn coil) of a ticket about 8cm operation distance can be achieved with a MIFARE® Demo-system.

Download from http://www.engracetech.com

2.4 Delivery Options

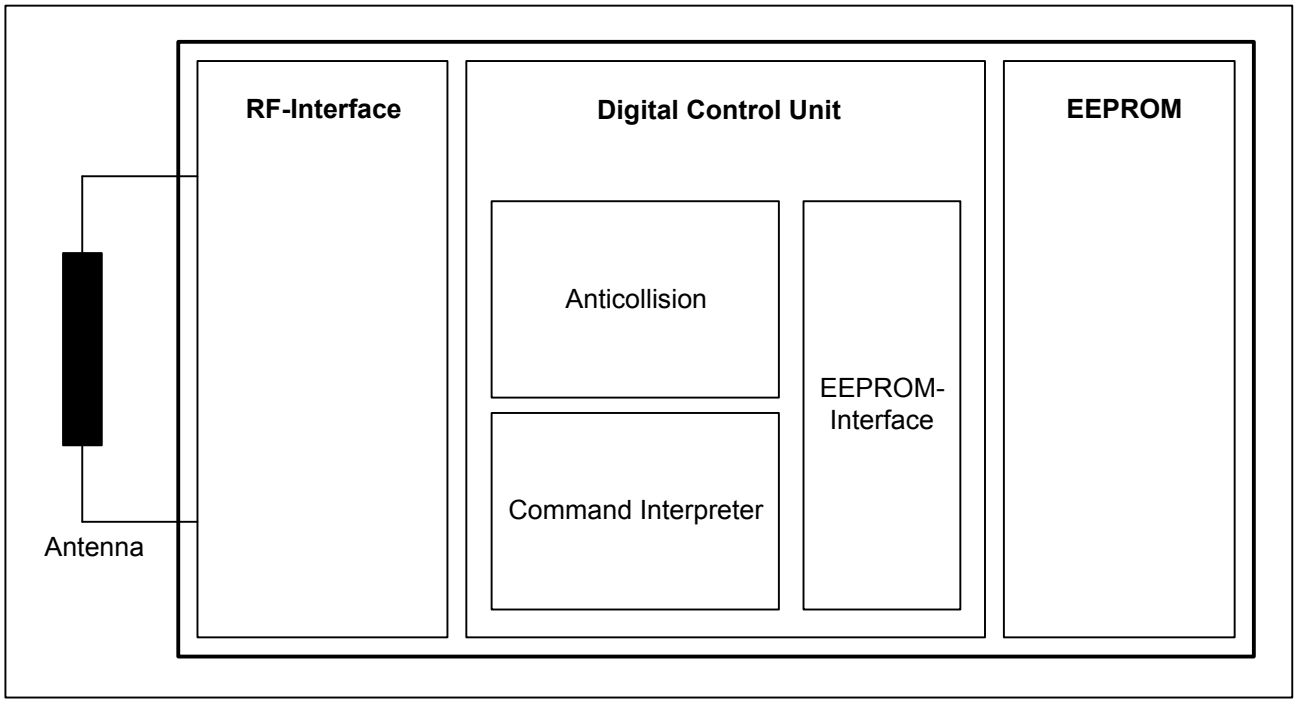
- Au - Bumped die on sawn 8” wafer, FFC, 150µm thickness
- Philips Flip Chip Package FCP2

3 FUNCTIONAL DESCRIPTION

3.1 Block Description

The MF0 IC U1 chip consists of the 512 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 MF0 IC U1. No further external components are necessary. (For details on antenna design please refer to the document *MIFARE® (Card) IC Coil Design Guide*.)

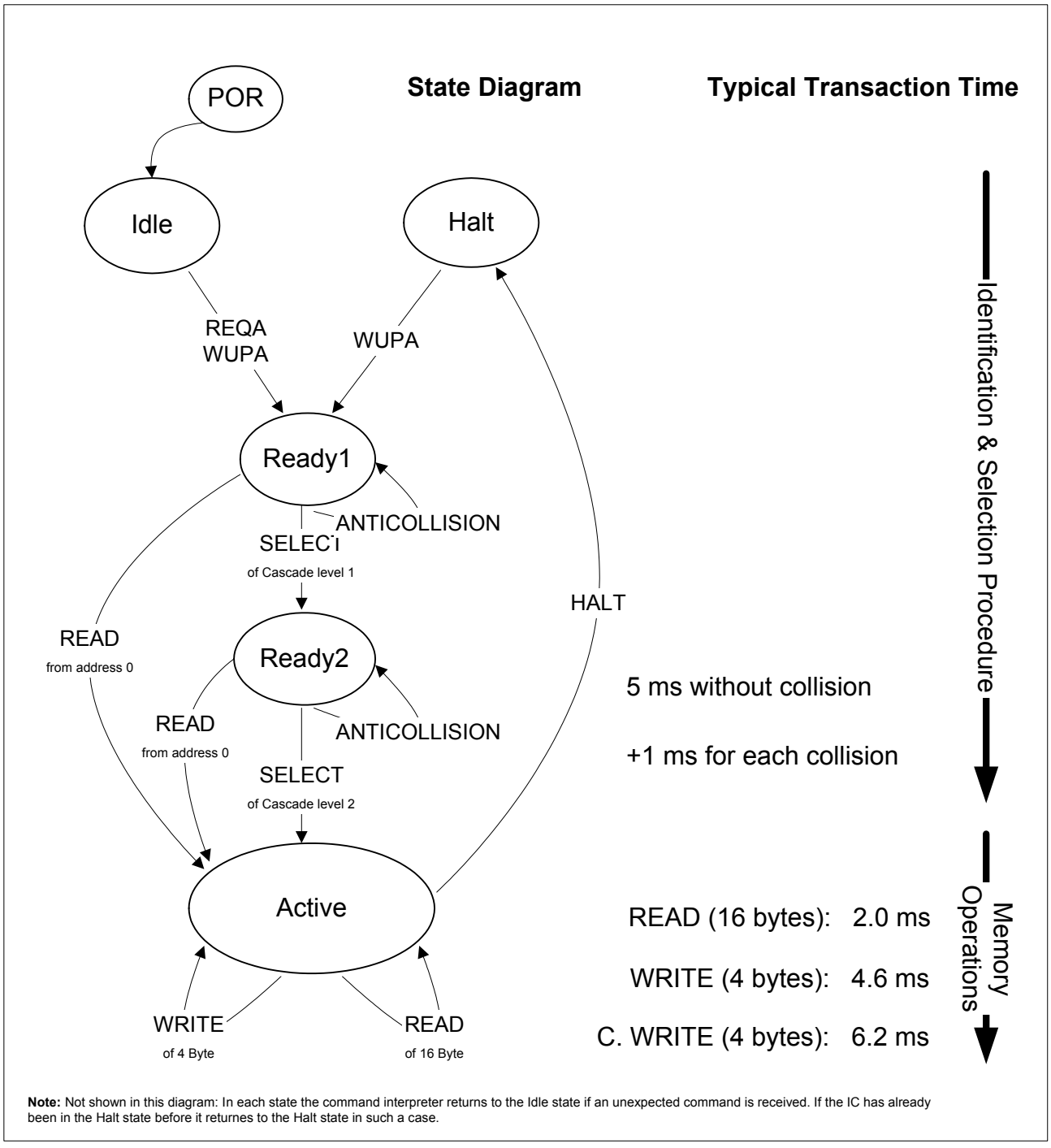
- RF-Interface:
  – Modulator/Demodulator
  – Rectifier
  – Clock Regenerator
  – Power On Reset
  – Voltage Regulator
- Anticollision: Several cards in the field may be selected and operated in sequence
- Command Interpreter: Handles the commands supported by the MF0 IC U1 in order to access the memory
- EEPROM-Interface
- EEPROM: 512 bits are organised in 16 pages with 4 bytes each. 80 bits are reserved for manufacturer data. 16 bits are used for the read-only locking mechanism. 32 bits are available as OTP area. 384 bits are user programmable read / write memory.



Download from http://www.engracetech.com

3.2 Communication Principle

The commands are initiated by the PCD and controlled by the Command Interpeter of the MF0 IC U1. It handles the internal states and generates the approriate responses.



Note: 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 returnes to the Halt state in such a case.

Download from http://www.engracetech.com

3.2.1 IDLE

After Power On Reset (POR) the MF0 IC U1 jumps directly into the Idle state. 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 MF0 IC U1 remains waiting in the Idle state.
After a correctly executed HALT command, the Halt state becomes the waiting state, which can be left via a WUPA command.

3.2.2 READY1

In this state the MF0 IC U1 supports the PCD in resolving the first part of its UID (3 bytes) with the ANTICOLLISION or a SELECT command of cascade level 1. This state is left correctly with either of two commands:

- With the SELECT command of cascade level 1 the PCD brings the MF0 IC U1 into state Ready2 where the second part of the UID has to be resolved.
- With the READ (from address 0) command the complete anticollision mechanism may be skipped and the MF0 IC U1 jumps directly into the Active state.

Note: If more than one MF0 IC U1 is in the field of the PCD, a read from address 0 will cause a collision because of the different serial numbers, but all MF0 IC U1 devices will be selected!
Any other data received in state Ready1 state is interpreted as an error and the MF0 IC U1 jumps back to its waiting state (IDLE or HALT, depending on it's previous state).

3.2.3 READY2

In this state, which is similar to state Ready1, the MF0 IC U1 supports the PCD in resolving the second part of its UID (4 bytes) with the ANTICOLLISION command of cascade level 2. This state is usually left with the SELECT command of cascade level 2.
Alternatively, state Ready2 may be skipped via a READ (from address 0) command as described in state Ready1.
Note: If more than one MF0 IC U1 is in the field of the PCD, a read from address 0 will cause a collision because of the different serial numbers, but all MF0 IC U1 devices will be selected!
The response of the MF0 IC U1 to the SELECT of cascade level 2 command is the SAK (Select Acknowledge) byte. According to ISO/IEC14443 this byte indicates whether the anticollision cascade procedure is finished. In addition it defines for the MIFARE® architecture platform the type of the selected device.
Now the MF0 IC U1 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 data received in this state is interpreted as an error and the MF0 IC U1 jumps back to its waiting state (IDLE or HALT, depending on it's previous state).

3.2.4 ACTIVE

In the Active state either a READ (16 bytes) or a WRITE (4 bytes) command may be performed. The correct way to leave this state is to send a HALT command. Any other data received in this state is interpreted as an error and the MF0 IC U1 jumps back to its waiting state (IDLE or HALT, depending on it's previous state).

3.2.5 HALT

Besides the Idle state the Halt state constitutes the second waiting state implemented in the MF0 IC U1. A MF0 IC U1 that has already been processed can be set into this state via the HALT command. This state helps the PCD in the anticollision phase to distinguish between already processed cards and cards that have not been selected yet. The only way to get the MF0 IC U1 out of this state is the WUPA command. Any other data received in this state is interpreted as an error and the MF0 IC U1 remains in this state. For an correct implementation of an anticollision procedure based on the usage of the Idle and Halt states and the REQA and WUPA commands please refer to the document *MIFARE® Collection of currently available Application Notes*.

Download from http://www.engracetech.com

3.3 Data Integrity

The following mechanisms are implemented in the contactless communication link between PCD and MF0 IC U1 to ensure a 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)

3.4 RF Interface

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

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

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

Download from http://www.engracetech.com

3.5 Memory Organisation

The 512 bit EEPROM memory is organised in 16 pages with 4 bytes each.

In the erased state the EEPROM cells are read as a logical “0”, in the written state as a logical “1”

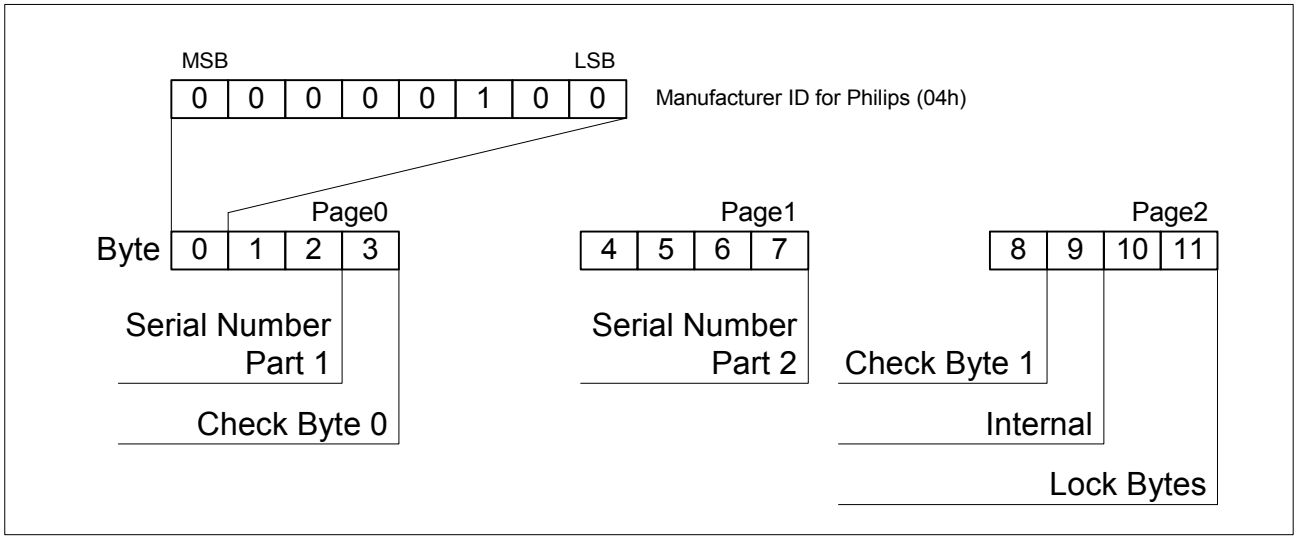
Byte Number	0	1	2	3	Page
Serial Number	SN0	SN1	SN2	BCC0	0
Serial Number	SN3	SN4	SN5	SN6	1
Internal / Lock	BCC1	Internal	Lock0	Lock1	2
OTP	OTP0	OTP1	OTP2	OTP3	3
Data read/write	Data0	Data1	Data2	Data3	4
Data read/write	Data4	Data5	Data6	Data7	5
Data read/write	Data8	Data9	Data10	Data11	6
Data read/write	Data12	Data13	Data14	Data15	7
Data read/write	Data16	Data17	Data18	Data19	8
Data read/write	Data20	Data21	Data22	Data23	9
Data read/write	Data24	Data25	Data26	Data27	10
Data read/write	Data28	Data29	Data30	Data31	11
Data read/write	Data32	Data33	Data34	Data35	12
Data read/write	Data36	Data37	Data38	Data39	13
Data read/write	Data40	Data41	Data42	Data43	14
Data read/write	Data44	Data45	Data46	Data47	15

Note: Bold frame indicates user area

Download from http://www.engracetech.com

3.5.1 UID / SERIAL NUMBER

The unique 7 byte serial number (UID) and its two Check Bytes are programmed into the first 9 bytes of the memory. It therefore covers page 0, page 1 and the first byte of page 2. The second byte of page2 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.

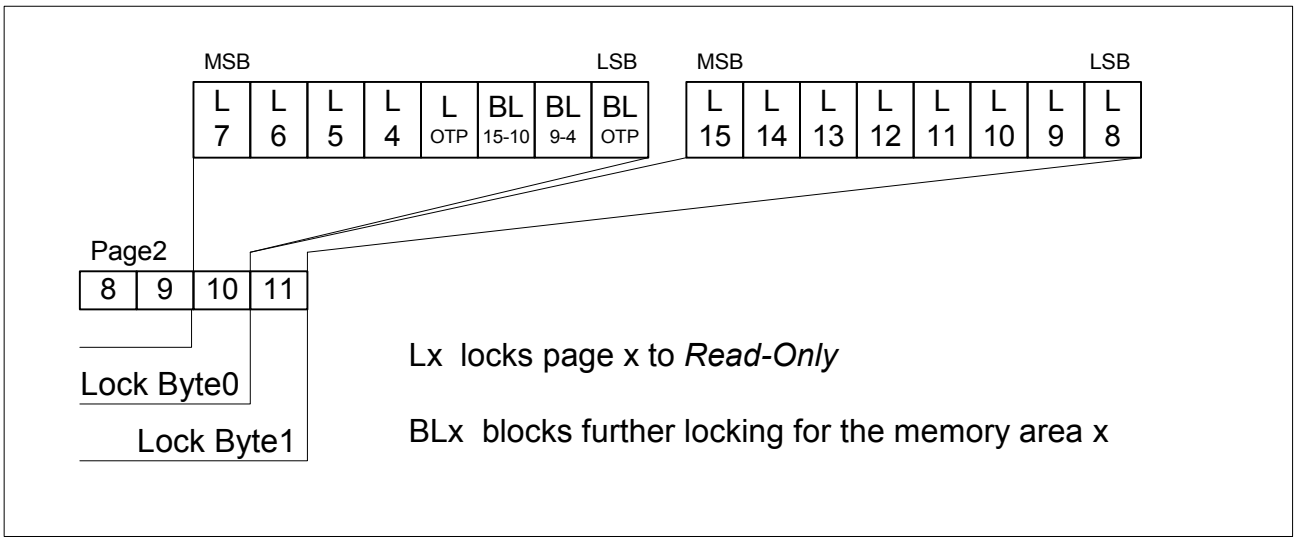


According to ISO/IEC14443-3 Check Byte0 (BCC0) is defined as CT ⊕ SN0 ⊕ SN1 ⊕ SN2 and Check Byte 1 (BCC1) is defined as SN3 ⊕ SN4 ⊕ SN5 ⊕ SN6.
SN0 holds the Manufacturer ID for Philips (04h) according to ISO/IEC14443-3 and ISO/IEC.7816-6 AMD.1.

3.5.2 LOCK BYTES

The bits of Byte 2 and 3 of page 2 represent the field-programmable read-only locking mechanism. Each page x from 3 (OTP) to 15 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 are the block-locking bits. Bit 2 handles pages 15 to 10, bit 1 pages



Download from http://www.engracetech.com

9 to 4 and bit 0 page 3 (OTP). Once the block-locking bits are set the locking configuration for the corresponding memory area is frozen.

Note: If e.g. BL15-10 is set to '1', L15 to L10 (bit 7 to bit 2 of lock byte 2) cannot be changed any more.

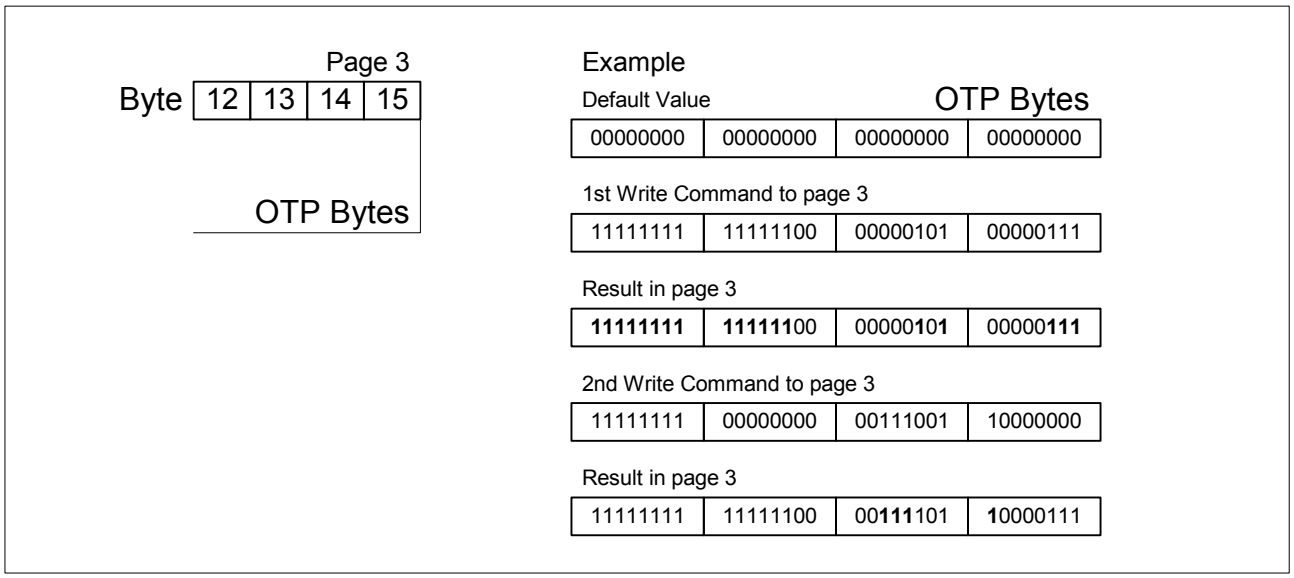
The locking and block-locking bits are set via a standard write command to page 2. Bytes 2 and 3 of the write command, and the actual contents of the lock bytes are bit-wise "or-ed" and the result then becomes the new contents of the lock bytes. This process is irreversible. If a bit is set to "1", it cannot be changed back to "0" again.

Note: The contents of bytes 0 and 1 of page 2 is not affected by the corresponding data bytes of the write command.

Important Security Note: To activate the new locking configuration after a write to the lock bit area, a REQA or WUPA command has to be carried out.

3.5.3 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.



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 contents of the OTP bytes. This process is irreversible. If a bit is set to "1", it cannot be changed back to "0" again.

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

3.5.4 DATA PAGES

Pages 4 to 15 constitute the user read/write area. After production the data pages are initialised to all "0".

Download from http://www.engracetech.com

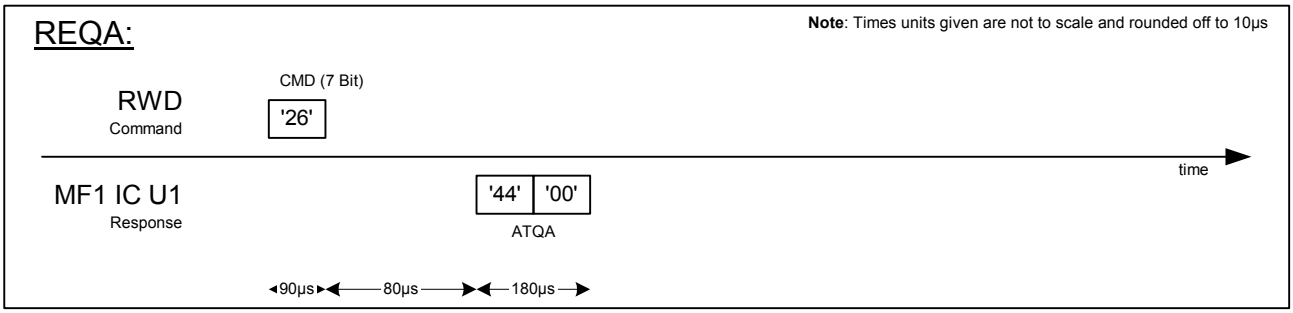
3.6 Command Set

The MF0 IC U1 comprises the following command set:

3.6.1 REQA

Code	Parameter	Data	Integrity mechanism	Response
0x26 (7 Bit)	-	-	Parity	0x0044

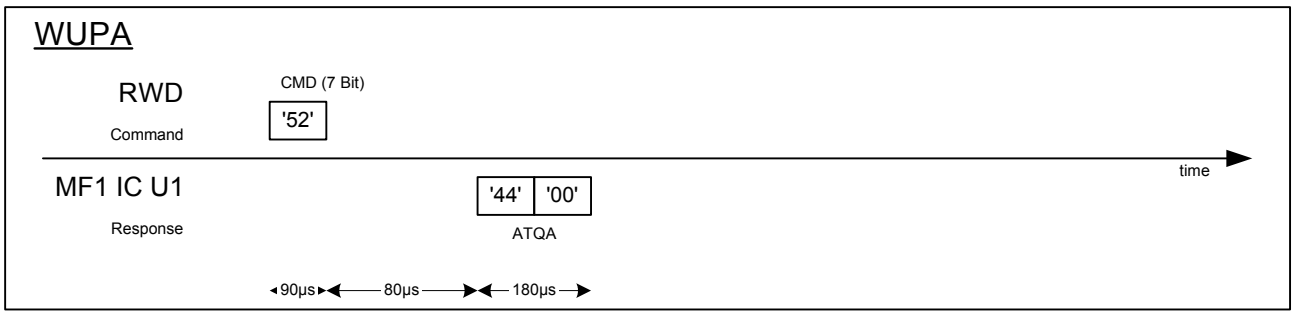
Description: The MF0 IC U1 accepts the REQA command in Idle state only. The response is the 2-byte ATQA (0x0044). REQA and ATQA are implemented fully according to ISO/IEC14443-3.



3.6.2 WUPA

Code	Parameter	Data	Integrity mechanism	Response
0x52 (7Bit)	-	-	Parity	0x0044

Description: The MF0 IC U1 accepts the WUPA command in the Idle and Halt state only. The response is the 2-byte ATQA (0x0044). WUPA is implemented fully according to ISO/IEC14443-3.

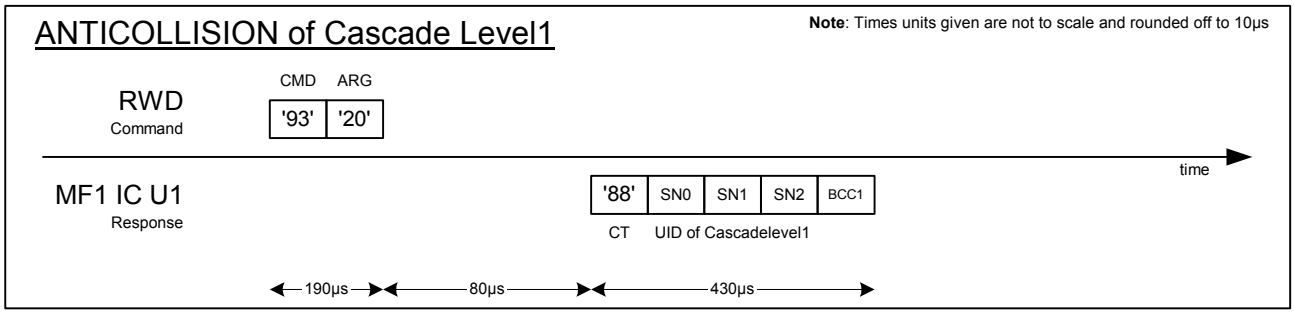


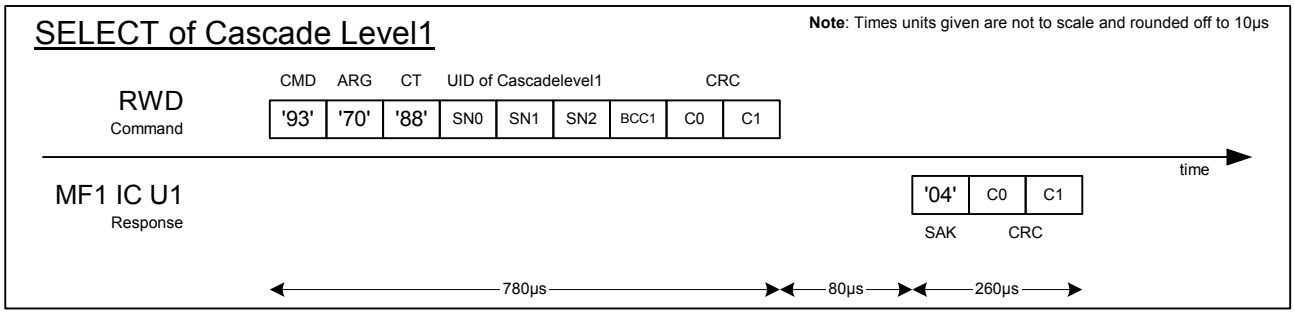
Download from http://www.engracetech.com

3.6.3 ANTICOLLISION AND SELECT OF CASCADE LEVEL 1

Code	Parameter	Data	Integrity mechanism	Response
Anticollision: 0x93	0x20 – 0x67	Part of the UID	Parity	Parts of UID
Select: 0x93	0x70	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 0x70 in case of SELECT. The MF0 IC U1 accepts these commands in the Ready1 state only. The response is part 1 of the UID.



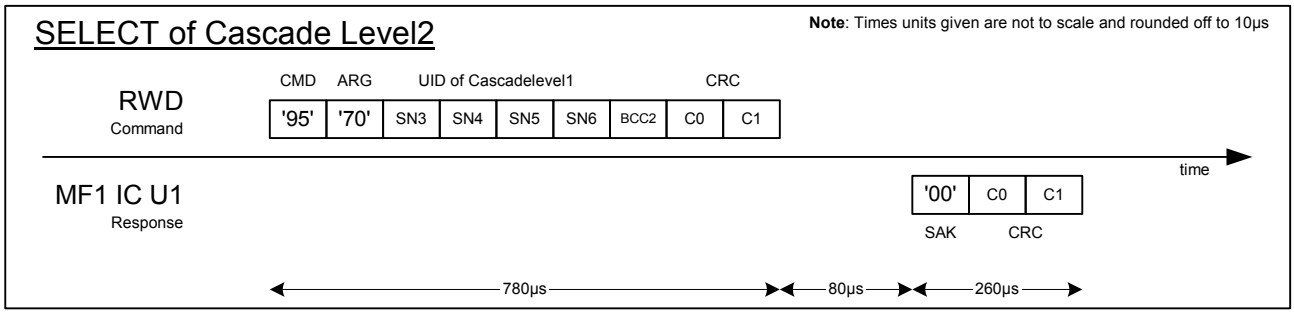


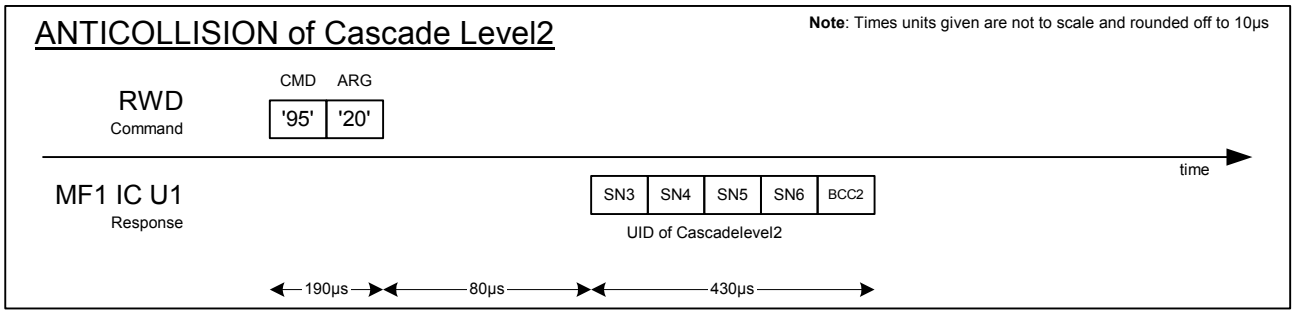
Download from http://www.engracetech.com

3.6.4 ANTICOLLISION AND SELECT OF CASCADE LEVEL 2

Code	Parameter	Data	Integrity mechanism	Response
Anticollision: 0x95	0x20 – 0x67	Part of the UID	Parity	Parts of UID
Select: 0x95	0x70	Second 4 bytes of UID	Parity, BCC, CRC	SAK (‘00’)

Description: The ANTICOLLISION and SELECT command are based on the same command code. They differ only in the parameter byte. This byte is per definition 0x70 in case of SELECT. The MF0 IC U1 accepts these commands in the Ready2 state only. The response is part 2 of the UID.



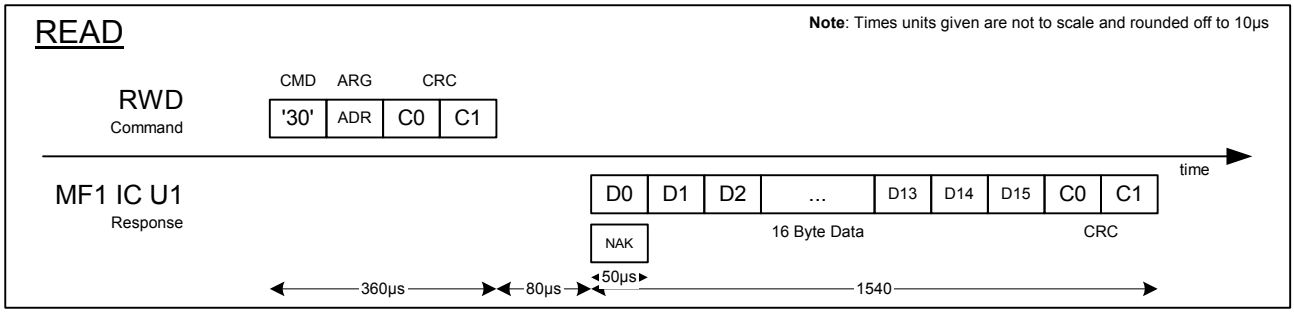


Download from http://www.engracetech.com

3.6.5 READ

Code	Parameter	Data	Integrity mechanism	Response
0x30	ADR: '0'-'7'	-	CRC	16 Byte Date

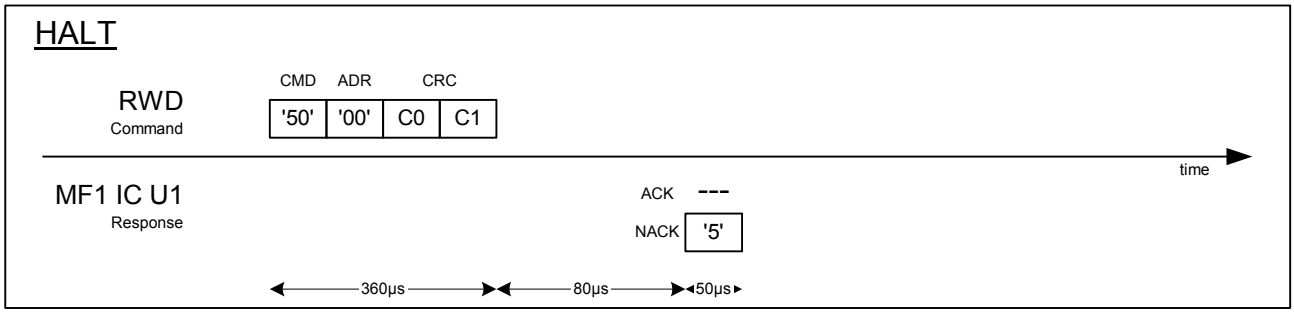
Description: The READ command needs the page address as a parameter. Only addresses 0 to 15 are decoded. For higher addresses the MF0 IC U1 returns a NAK. The MF0 IC U1 responds to the READ command by sending 16 bytes starting from the page address defined in the command (e.g. if ADR is '3' pages 3,4,5,6 are returned). A roll back is implemented; e.g. if ADR is '14', the contents of pages 14, 15, 0 and 1 is returned).



3.6.6 HALT

Code	Parameter	Data	Integrity mechanism	Response
0x50	0x00	-	Parity, CRC	Passive AK, NAK

Description: The HALT command is used to set already processed MF0 IC U1 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.

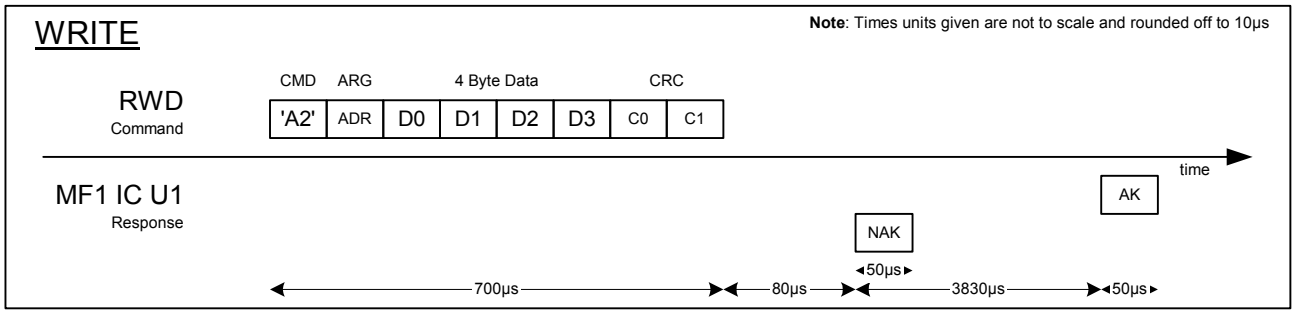


Download from http://www.engracetech.com

3.6.7 WRITE

Code	Parameter	Data	Integrity mechanism	Response
0xA2	ADR: ‘0’ – ‘7’	4 Byte	Parity, CRC	AK or NAK

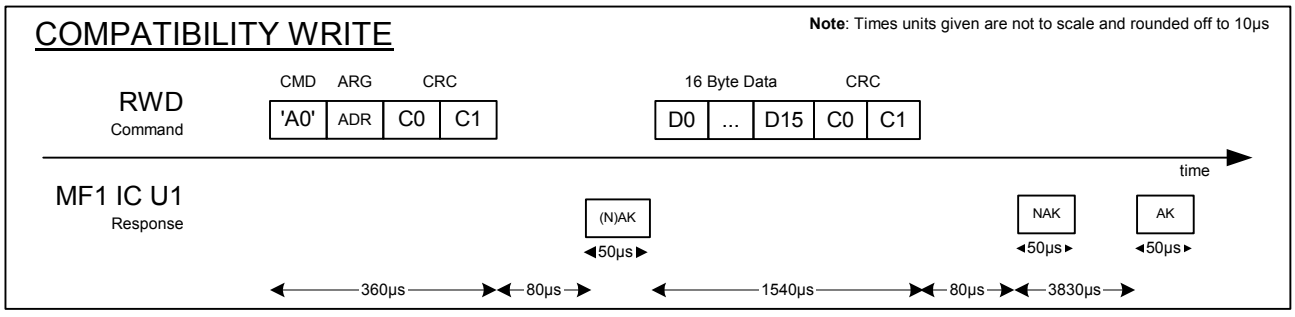
Description: The WRITE command is used to program the lock bytes in page 2, the OTP bytes in page 3 or the data bytes in pages 4 to 15. A WRITE command is performed page-wise, programming 4 bytes in a row.



3.6.8 COMPATIBILITY WRITE

Code	Parameter	Data	Integrity mechanism	Response
0xA0	ADR: ‘0’ – ‘7’	16 Byte	Parity, CRC	AK or NAK

Description: The COMPATIBILITY WRITE command was implemented to accommodate the established mifare® PCD infrastructure. Even though 16 bytes are transferred to the MF0 IC U1, 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’.



Download from http://www.engracetech.com

3.7 Summary of Relevant Data for Device Identification

Code	Type	Value	Binary Format	Remark
ATQA	2 Byte	0x0044	0000 0000 0100 0100 1st '1' indicates cascade level 2 2nd '1' indicates MIFARE family	Hard Coded
CT	1 Byte Cascade Tag	0x88	1000 1000 ensures collision with cascade level 1 products	Hard Coded
SAK (casc. level 1)	1 Byte	0x04	0000 0100 '1' indicates additional cascade level	Hard Coded
SAK (casc. level 2)	1 Byte	0x00	0000 0000 indicates complete UID and MF0 IC U1 functionality	Hard Coded
Manufacturer Byte	1 Byte	0x04	0000 0100 indicates manufacturer Philips	Acc. to ISO/IEC 14443-3 and ISO/IEC 7816-6 AMD.1

Download from http://www.engracetech.com

4 DEFINITIONS

Data sheet status	
Objective specification	This data sheet contains target or goal specifications for product development.
Preliminary specification	This data sheet contains preliminary data; supplementary data may be published later.
Product specification	This data sheet contains final product specifications.
Limiting values	
Limiting values given are in accordance with the Absolute Maximum Rating System (IEC 134). Stress above one or more of the limiting values may cause permanent damage to the device. These are stress ratings only and operation of the device at these or at any other conditions above those given in the Characteristics section of the specification is not implied. Exposure to limiting values for extended periods may affect device reliability.	
Application information	
Where application information is given, it is advisory and does not form part of the specification.	

5 LIFE SUPPORT APPLICATIONS

These products are not designed for use in life support appliances, devices, or systems where malfunction of these products can reasonably be expected to result in personal injury. Philips customers using or selling these products for use in such applications do so on their own risk and agree to fully indemnify Philips for any damages resulting from such improper use or sale.

Download from http://www.engracetech.com

6 REVISION HISTORY

Table 1 Objective Specification MF0 IC U1 Revision History

REVISION	DATE	CPCN	PAGE	DESCRIPTION
3.0	0303			Product Version
2.5	0103	CIN	4	Write Endurance, Data Retention
2.4	0202			Preliminary Version
2.3	1001			Include MF0 IC U11 type
2.2	0801		4	Updated document layout + wording Change of Write endurance to 1000 cycles
2.1	0201			Introduction of read in state Ready2 and Compatibility write command
2.0				Introduction of Lock bytes and increase of memory to 512 bit. Correction of Manufacturer Code
1.0				First official version.

Download from http://www.engracetech.com

NOTES

Download from http://www.engracetech.com

Philips Semiconductors - a worldwide company

Contact Information

For additional information please visit **http://www.semiconductors.philips.com**.Fax: **+31 40 27 24825**
For sales offices addresses send e-mail to: **sales.addresses@www.semiconductors.philips.com**.

© Koninklijke Philips Electronics N.V. 2002 SCA74

All rights are reserved. Reproduction in whole or in part is prohibited without the prior written consent of the copyright owner.

The information presented in this document does not form part of any quotation or contract, is believed to be accurate and reliable and may be changed without any notice. No liability will be accepted by the publisher for any consequence of its use. Publication thereof does not convey nor imply any license under patent- or other industrial or intellectual property rights.

Philips Semiconductors

Let's make things better.

PHILIPS