Application Note

MicroEngine
13,56MHz Dual Reader Module
ME-H102016xx, ME-H6156

Firmware: 0.15e

4/9/2004

EHAG
ELECTRONIC HARDWARE AG
Industriestr. 8 8618 Oetwil am See
T: +41 43 844 94 00 info@ehag.ch
F: +41 43 844 94 01 www.ehag.ch

Table of Content

1 Scope

The MIFARE® Application Oriented Protocol is a reader Interface to communicate with MIFARE® transponders. The major applications to be supported are:

- Access control, Identification: Reading the serial numbers of all cards in the field.
- Data Storage: Performing encrypted read and write operations.
- Ticketing: Performing read, write, increment and decrement operations in an encrypted environment.
- Multi applications: Performing read, write, increment and decrement operations on various sectors of the MIFARE® Standard tags using different encryption keys.

2 Definitions and abbreviations

2.1 Definitions

2.1.1 Anticollision loop

Algorithm processed to identify and handle a dialogue between VCD and one or more VICCs in its antenna field.

2.1.2 Hex notation

A hexadecimal value is noted with a following h. i.e. A1h has the value A1 hexadecimal.

2.1.3 ASCII notation

ASCII characters are listed within apostrophes, i.e. ‘x’ means a single x.

2.2 Abbreviations

ASCII	American Standard Code for Information Interchange
ATS	Answer to Select
block	For Mifare® Standard one block contains 16 bytes
CID	Card Identifier (logical card adrdess, ISO 14443-4)
CRC	Cyclic Redundancy Check
EDC	Error Detection Code
EOF	End of frame
hex / xxh	value in Hexadecimal notation
I-block	Information block
LSB	Least Significant Bit or Byte
MSB	Most Significant Bit or Byte
NAD	Node Address (ISO 14443-4)
OSI	Open System Interconnection
PCB	Protocol Control Byte (ISO 14443-4)
PCON	Protocol Configuration byte of the reader
PPS	Protocol and Parameter Selection
RATS	Request for Answer to Select
R-block	Receive ready block
REQA	Request ISO Type A
REQB	Request ISO Type B
RFU	Reserved for Future Use
S-block	Supervisory block
sector	For Mifare® Standard one sector contains 4 blocks
SID	Station ID
SN	Serial Number of a tag (a 32 bit number)
SOF	Start of frame
value block	32 bit data block format. Used in ticketing application
<CR>	Carriage return

Figure 2-1: Abbreviations

3 The Mifare® transponder family

The Mifare® transponder family consists of various 13.56 MHz transponders IC, all according to ISO 14443.

3.1 Mifare® Standard

The Mifare® Standard card consists of 16 sectors. A sector includes four blocks 16 bytes each.

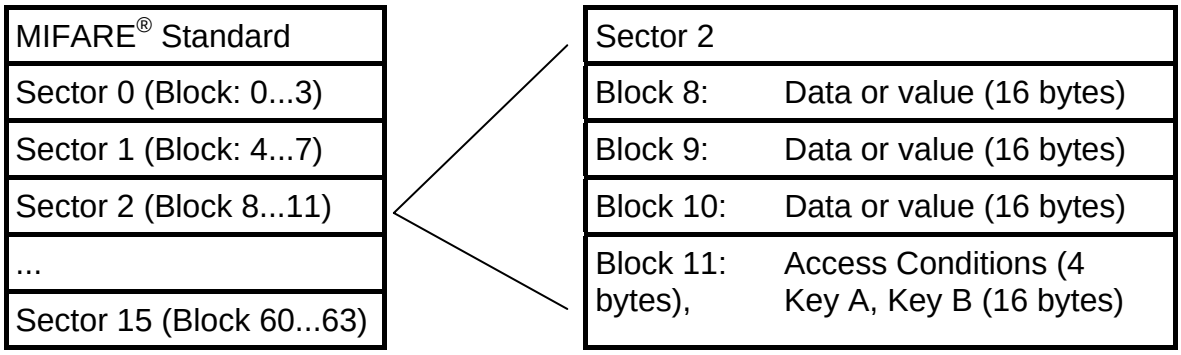


Figure 3-1: MIFARE® Standard: sector diagram

3.1.1 Sector 0 / Block 0

Page 0 is read only.

Serial Number (4 byte)	Check byte (1 byte)	Manufacturer data (11 byte)

Figure 3-2: MIFARE® Standard: sector 0 / block 0

3.1.2 Block 3, 7, 11, 15, …

Transport keys are set on delivery:

Key A (6 byte)	Access Conditions (4 bytes)	Key B (6 byte)

Figure 3-3: MIFARE® Standard: block 3, 7, 11, 15, …

Key A
A0 A1 A2 A3 A4 A5 (Infineon) or FF FF FF FF FF FF (new Philips cards)

Key B
B0 B1 B2 B3 B4 B5 (Infineon) or FF FF FF FF FF FF (new Philips cards)

Access Conditions
FF 07 80 xx (key A used to read or write, the key A itself is not readable; key B is data only). For further information refer to Mifare card manual.

Remarks
Enabled keys are always read as 00 00 00 00 00 00
Using key B as data area will cause a security gap, due to the fact that it is necessary to rewrite key A and access conditions each write process. It is not recommended to use it as data storage.

3.2 State Diagram

All Mifare® cards use following state diagram.

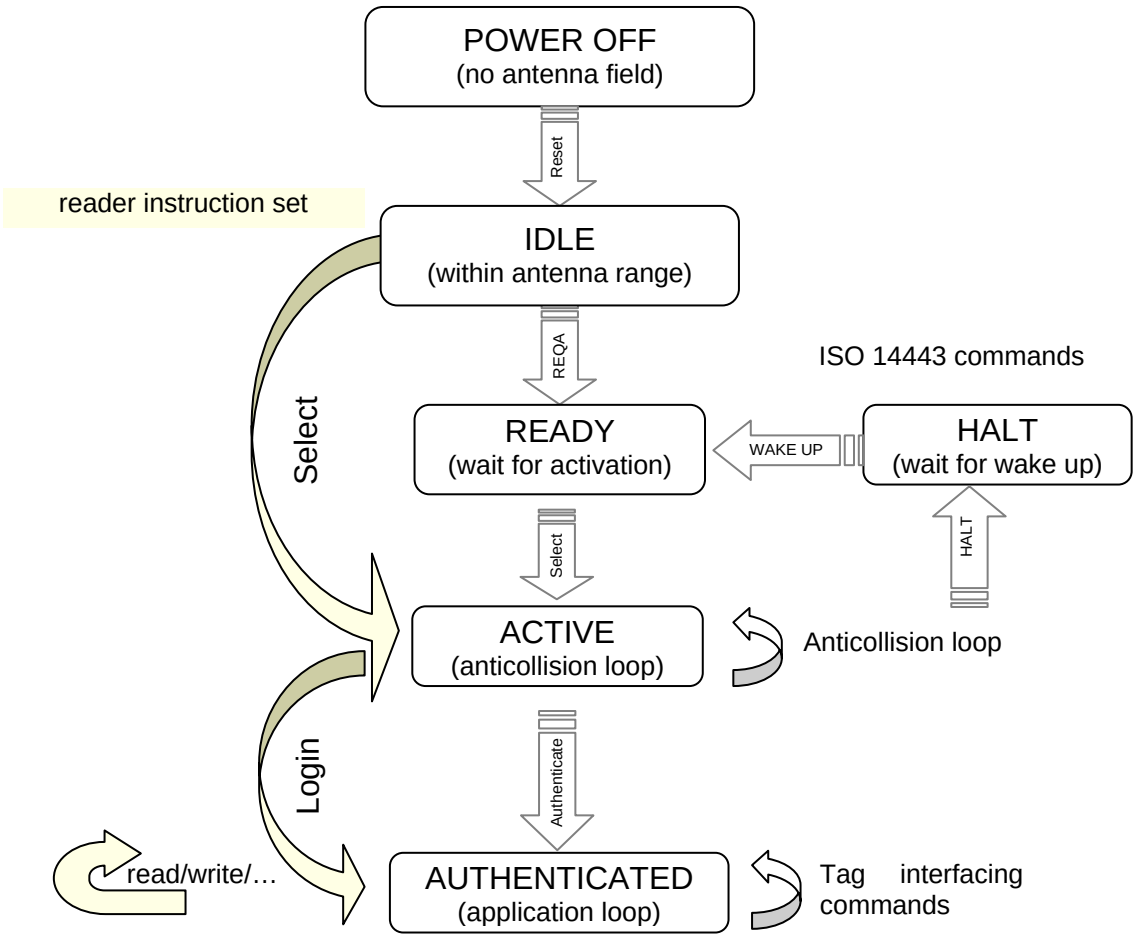


Figure 3-4: State diagram

3.3 Mifare Ultralight

Mifare Ultralight cards have no encryption included. They only support plain text data transmission.

3.4 Mifare ProX

Mifare ProX tags have an operating system onboard. Data organization depends on the operating system installed on the card. These cards can include additional functionalities such as DES or proprietary encipher algorithm.

Prior to any access of the operating system the card must be selected. Customized commands are issued using the transfer command.

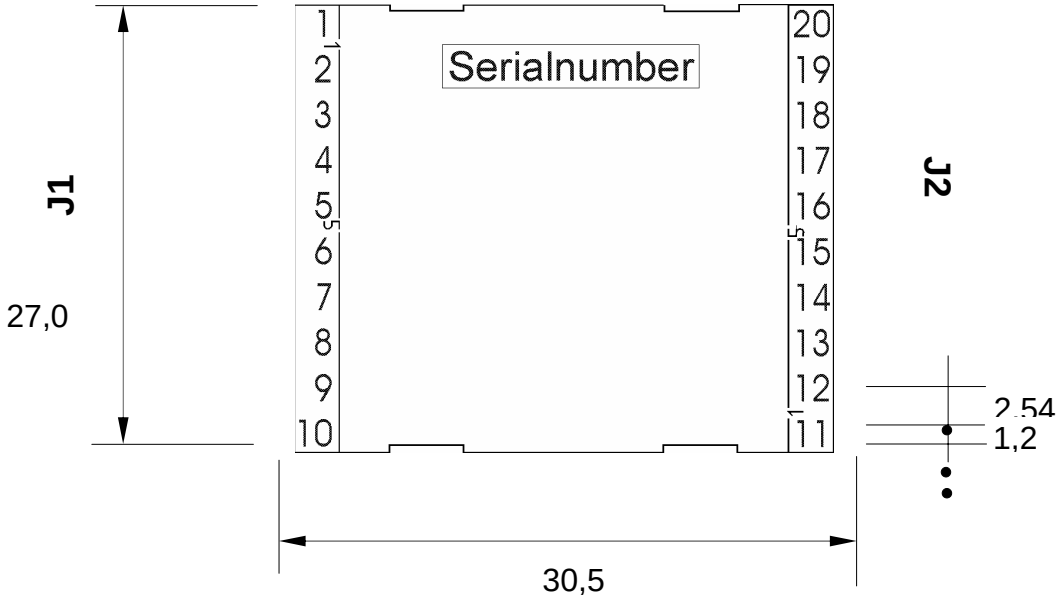
3.5 ISO 14443 Type B

ISO 14443 type B cards are supported. Multiple instances and selection is implemented in high-level command set.

All other commands must be issued using the transfer command.

4 Hardware

4.1 Pin out of OEM Module



4.1.1 Pin out of J1

PIN	PIN Nr	Description
ARX	1	Antenna RX
ATX1	2	Antenna TX1
VDD	3	+5 V DC
GND	4	Ground
ATX2	5	Antenna TX2
TGND	6	Antenna Ground
RFU	7	Reserved for future use
RFU	8	Reserved for future use
RFU	9	Reserved for future use
RFU	10	Reserved for future use

Figure 4-1: Pin out of jumper 1

4.1.2 Pin out of J2

PIN	PIN Nr	Description
VDD	20	+5 V DC
GND	19	Ground
LEDg	18	LED green (reading LED)
LEDr	17	LED red
EN	16	Enable reader, open or logic high
RFU	15	Reserved for future use
USER	14	User Port
DIR	13	Direction of RS 485
TX	12	TX to PC
RX	11	RX from PC

Figure 4-2: Pin out of jumper 2

4.1.3 Electrical characteristics of PINs

PIN	PIN Nr	Voltage	Current (max)	Description
RX TX	11 12	USART[1]	-	To RS232, RS485 device driver
USER	14	TTL[2]	25 mA	User sets logic state
EN	16	ST[3]	25 mA	Low will disable the reader device
LEDr	17	GND	25 mA	Logic Low, used for LED
LEDg	18	LED	25 mA	With 330 Ω (internal)
ARX ATX1 ATX2 TGND	1 2 5 6	(depends on antenna tuning)	200 mA_{PP}	Antenna input Antenna output Antenna output (GND)
RFU	7,8,9, 10,15	-	-	Not connected
GND	4,19	GND	-	Supply Ground
VDD	3,20	+5 V DC	150 mA	Supply Voltage
DIR	13	TTL	25 mA	RS485 direction

Figure 4-3: Electrical characteristics of pins

[1] Universal Synchronous Asynchronous Receiver Transmitter
[2] TTL buffer output / input
[3] Schmitt trigger buffer output

5 Software

As default data is transmitted at 9600,n, 8,1, no handshaking. Two protocol modes are supported. The protocol mode is configured in the reader EEPROM. As factory default, the ASCII protocol is used.

5.1 ASCII Protocol

This protocol is designed for easy handling. The commands are issued using a terminal program. Data is transmitted as ASCII hexadecimal that can be displayed on any terminal program (i.e. HyperTerminal).

Command	Data
Various length	Various length

Figure 5-1: ASCII protocol frame

5.2 Binary Protocol

This protocol is designed for industrial applications with synchronization and frame checking. Also an addressing byte for party line (master slave, multi drop) is included. The protocol usually requires a device driver. Data is transmitted binary. The reader uses a binary watchdog timer internally to ensure correct framing.

STX	Station ID	Length	Data	BCC	ETX
1 byte	1 byte	1 byte	Various length	1 byte	1 byte

Figure 5-2: Binary protocol frame

5.2.1 STX

Start of transmission (02h)

5.2.2 Station ID

Unique ID of the station
00h: reserved for the bus master. Readers send response to this device ID
FFh: Broadcast message. All devices will execute the command and send its response.

5.2.3 Length

Length of the data block

5.2.4 Data

This part contains the command and data. The command values are the same as in ASCII protocol mode (‘x’, ‘s’, …) whereas data is transmitted binary.
The length of the command block depends on the instruction.

5.2.5 Block Check Character (BCC)

The BCC is used to detect transmission errors. The BCC is calculated XORing each byte of the transmission frame excluding the STX/BCC and ETX character.

$$BCC = (StatID)\,xor\,(Length)\,xor\,(Command/Data_0)\,xor\,...\,xor\,(Command/Data_N)$$

5.2.6 ETX

End of transmission. (03h)

5.2.7 Remarks

If the reader device receives an invalid instruction frame (i.e. BCC wrong) or the requested station ID does not match the internal ID of the reader, the command is not executed. The reader waits for the next valid frame.
The automatic binary timeout (see protocol configuration register) is used to detect incomplete binary frames.

5.2.8 Examples:

02h	64h	01h	78h	1Dh	03h
STX	Station ID	Length	‘x’	BCC	ETX

This instruction frame will reset the reader module with the station ID 64h.

5.3 Register Set

The reader provides a wide range of system flags, which allow customizing its behavior.
This flags are mapped into a non-volatile register set.
Unless otherwise noted the reader has to be reset to take over changes in the register set.
It is recommended to clear all bits marked as RFU to ensure compatibility with further firmware versions.

Additional to this common register set the reader provides master key memory. The master key memory is able to save 32 authentication keys (for use with Mifare® Standard card authentication).

These keys are also stored non-volatile and are write only. They are only accessed by the write master key instruction.

5.3.1 EEPROM memory organization

Register	Description
00h … 03h	Unique device ID; read only
04h	Station ID
05h	Protocol configuration
06h	Baud rate
07h	Binary watchdog timer
08h	Operation Mode
09h … 0Fh	RFU
10h … 1Fh	User data

Figure 5-3: EEPROM memory

5.3.2 Unique device ID (00h – 03h)

The unique device ID identifies a reader module. It is factory programmed and cannot be changed.

5.3.3 StationID (04h)

The station ID is used in binary mode to address a device in party line set up. The station ID has the range of 01h to FEh and can be set freely. The value 00h is reserved for the bus master. All readers send their response to this device.
The broadcast message (FFh) forces all readers to response to the command.
Default value is 01h.

5.3.4 Protocol configuration (0Bh)

The PCON register specifies general behavior of the reader device.
Default value is 01h.

Protocol configuration register							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
RFU	OP Mode	OP Mode	Multitag list	Bin WDT	Extend-ed ID	Protocol	Auto-start

Figure 5-4: Protocol configuration register

5.3.4.1 Autostart (default 1)

If set the reader device will start up in continuous read mode automatically. Auto start has only effect in ASCII protocol mode.

5.3.4.2 Protocol (default 0)

If set the reader uses binary protocol mode. As default ASCII protocol is used. Refer to binary protocol for further information on the binary protocol format.
Continuous read command decreases its detection speed.

5.3.4.3 Extend ID (default 0)

If set the reader extends the serial number of tags with additional bytes.

ISO 14443 A tags (5 bytes transmitted)

Tag type	**Serial number**
1 byte	4 bytes

Figure 5-5: ISO 14443 A Extended Serial number

The tag type byte indicates the type of cascade level.

Tag type	**Description**
01h	Mifare Light
02h	Mifare Standard
03h	Mifare ProX
04h	ISO 14443B
FFh	Unknown tag type

Figure 5-6: ISO 14443 A Tag type

ISO 14443 B tags (12 bytes transmitted)

Extended byte	Serial number	Application data	Protocol info	CID
1 byte	4 bytes	4 bytes	3 bytes	1 byte

Figure 5-7: ISO 14443 B Extended Serial number

For detailed description of Application Data, Protocol Info and CID refer to ISO 14443 documentation [1].

5.3.4.4 Binary watchdog timer (default 0)

If set the binary watchdog timer is enabled. It enables to detect incomplete or corrupted frames. It should be always enabled in binary protocol mode.

5.3.4.5 Multitag (default 0)

The Multitag flag will enable multi tag recognition in continuous read mode. All tags are detected and displayed. Due to the more complex search algorithm the continuous read command decreases its detection speed.

5.3.4.6 OP Mode (default 00h (ISO-A))

This 2 bit defines the operation mode used at start up.

00b (0h)	ISO-A mode
01b (1h)	ISO-B mode
10b (2h)	ISO-AB (toggle) mode
11b (3h)	RFU

Figure 5-8: OP Modes

The set tag type command switches the operation mode at runtime.

5.3.5 BAUD, Baud rate control register (06h)

The baud rate register defines the communication speed of the reader device.
Default value is 00h.

Baud rate register							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
RFU	RFU	RFU	RFU	RFU	RFU	BS1	BS0

Figure 5-9: Baud rate register

This register defines the baud rate of the device.

BS1	**BS0**	**Baud rate**
0	0	9600 baud (default)
0	1	19200 baud
1	0	38400 baud
1	1	57600 baud

Figure 5-10: Baud rate settings

Following figure describes the communication settings

Description
8 data bits
\No parity bit
1 stop bit
No flow control

Figure 5-11: Communication settings

5.3.6 TMR, RF time out control register (07h, 08h)

The RF time out is used as reader card communication timeout. One time slice is around 300us. Shortest timeout is 164ms, the longest timeout value is 16,3 seconds (FFFFh).
Value 0000h is not allowed and internally set to 0001h.
Default value is 000Fh.

5.3.7 User memory (10h – 1Fh)

User memory is free for use.

5.4 Instruction Set

Following table describes all commands of the reader device. Each command returns an answer to the host. Exceptions are mentioned explicitly.

5.4.1 Overview

Common commands	
‘c’	Continuous read
‘g’	Get ID
‘m’	MultiTag select / tag list
‘oX’	Set tag type
‘poff’ / ’pon’	Antenna power off/on
‘pr’ / ’pw’	Read / write user port
‘rp’	Read EEPROM register
‘s’	Select
‘t’	Transfer data telegram
‘v’	Get version
'wm'	Write master key
‘wp’	Write EEPROM register
‘x’	Reset
ISO 14443 Type A only commands	
'+'	Increment value block (credit)
'-'	Decrement value block (debit)
'='	Copy value block (backup)
'l'	Login (authenticate tag)
‘r’	Read page
'rv'	Read value block
‘w’	Write page
'wv'	Write value block

Figure 5-12: Command overview (Part 1)

5.4.2 Error Codes

Following figure shows an overview of all error messages of the reader device.

Error Code	Description
‘?’	Unknown command
'C'	Collision or CRC Error
‘F’	General failure
‘I’	Invalid value format, specified block does not match the value format
‘N’	No tag in the field
'O'	Operation mode failure or file not selected

Figure 5-13: Error codes

5.4.3 Common commands

5.4.3.1 Continuous Read

The reader device reads and displays serial numbers continuously while one or more tags remain in the field. This command stops if any character is sent to the reader module.
The reader supports different tag types at the same time. To increase the reading performance switch to a single tag mode. If more than one tag of the same tag type should be detected at the same time the Multitag flag must be activated. The response data length depends on the tag type.
This command is not supported in binary protocol mode.

Command

Command	Data
‘c’	none

Answer

Answer	Description
data	serial number (n bytes)

5.4.3.1.1 Multitag continuous read mode

If the Multitag flag is set in the Protocol Configuration (PCON) register the reader reads multiple tags continuously.

5.4.3.1.2 Auto start

The continuous read mode is started automatically. The auto start flag must be set in the PCON register.

5.4.3.1.3 Binary mode

Continuous read is only supported in ASCII protocol. Since the binary protocol is strictly master slave the continuous read mode is not supported.

5.4.3.1.4 Simple access control applications

Serial numbers are always sent plain. Data encryption is activated after a successful log in.
For simple access control applications it is recommended to use read-only blocks for the identification of the tag.
Reading any block (even the manufacturer block) of the transponder will increase your security.

5.4.3.2 Get ID

This command returns the station ID of the reader device. The answer is time slotted to enable that all devices in party line mode are detected.
The station ID has only effect in binary mode.

Command

Command	Data
‘g’	None

Answer

Answer	Description
Data	Station ID of the reader device (1 byte)

5.4.3.2.1 Time slotted answer

In party line mode more than one reader can be used simultaneously. The time slotted answer allows separating all connected devices. The station ID is used to determine the correct time slot.
The reader supports up to 254 unique time slots. Following formula calculates the needed time of one time slot. Only one baud rate on the same party line is supported.

$$T_0[s] = \frac{10}{Baudrate} * 6$$

Figure 5-14: Time slot formula

Following figure shows the timing diagram of time slotted answers.

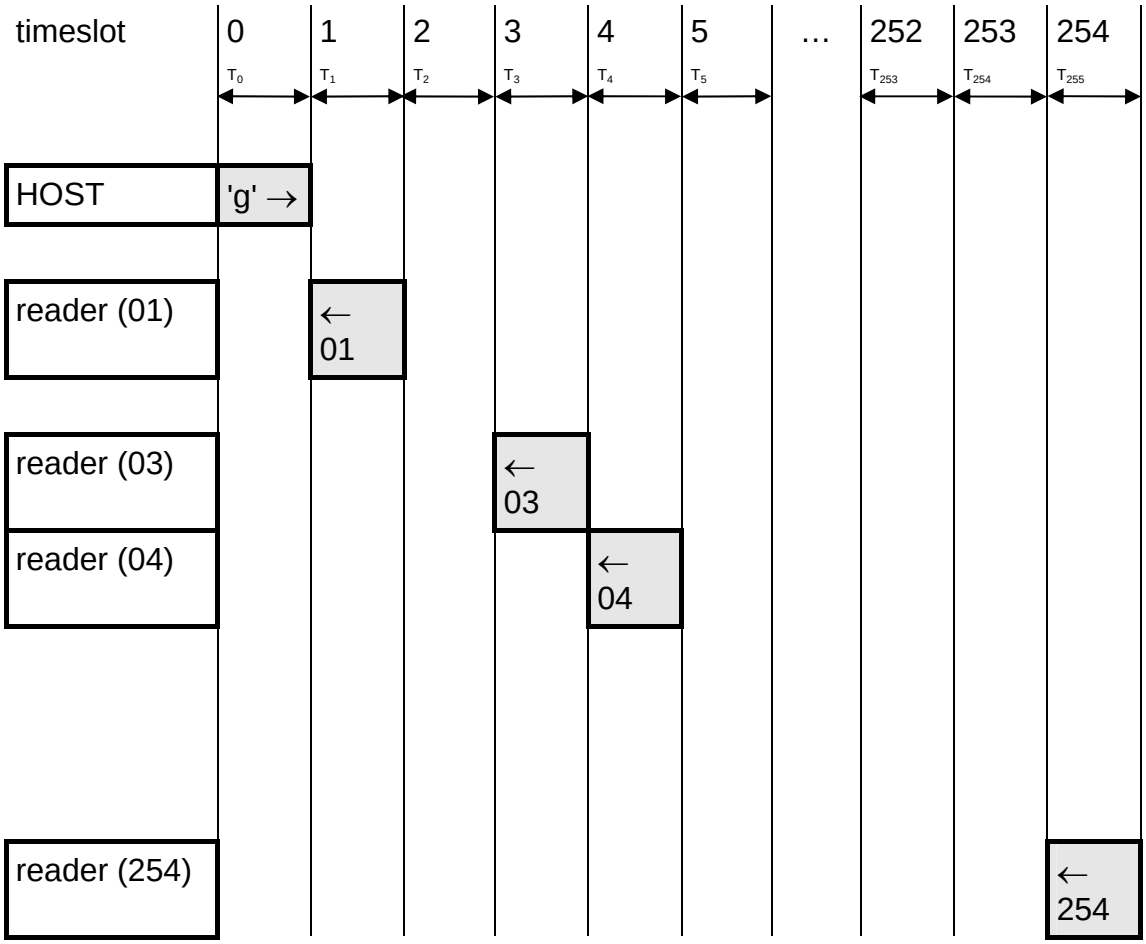


Figure 5-15: Timing diagram of time slotted answers

5.4.3.3 Multi Tag Selection / List

This command detects several ISO 14443 type A and B tags at the same time. It replaces the fast select command (‘s’) in multiple tag surroundings. The Multi Tag list command lists all tags with its serial numbers. Use the Multi Tag Select command to select a single tag. Each tag has to be selected separately

Command

Command	Data
‘m’	Serial number (0/4 bytes) <CR> (1 byte)

Answer

Answer	Description
Data	serial number
‘N’	Error: No Tag in the field

Example

Command	Description
m<CR>	01234556 → first card 34030F07 → second card 02 → number of detected tags
m01234556	Select card with its serial number

5.4.3.3.1 Multi tag list

Sending a <CR> as first parameter the reader returns a list of all present tags in the antenna field. In the end the amount of detected tags are returned. A Multitag list command resets all tags in the antenna field.

5.4.3.3.2 Reading distance

Each card needs a specific amount of power. The reader always provides the same power. Therefore the reading distance will decrease if more tags are present.

5.4.3.3.3 Multi tag select

Using the serial number with <CR> as parameter the according tag will be selected. High-level interactions can be performed addressing only this card. All other tags remain silent.

5.4.3.3.4 Maximum number of tags

The maximum number of tags in the antenna field is limited to the physical characteristics of the antenna. Internally the software can handle up to 40 tags (theoretical maximum).

5.4.3.4 Set tag type

This command sets up the reader to a specific tag type. The continuous read function will speed up because only this tag type is addressed. After a reset the reader starts as defined in its startup configuration.

Command

Command	Data
‘o’	ISO type (1 byte) 'a' … ISO 14443 Type A 'b' … ISO 14443 Type B 't' … ISO 14443 Type A + B

Answer

Answer	Description
'OA' 'OB' 'OT'	String of tag type

Example

Command	Description
Oa	Sets the reader device to ISO14443-A tags

5.4.3.5 Antenna power on/off

This command controls the antenna power. It can be used to decrease the power consumption of the reader.

Command

Command	Data
‘pon’	Switch on reader
‘poff’	Reader enters the stand by mode

Answer

Answer	Description
‘P’	Positive acknowledge

Example

Command	Description
Poff	Reader enters stand by mode

5.4.3.5.1 Power off

The reader enters the stand by mode. Power consumption is decreases. All tags in the antenna field are powered off and reset. The stand by mode is only entered manually.
To switch off the whole unit pin 16 (Enable) has to be set to logic low.

5.4.3.5.2 Power on

The reader leaves the stand by mode and is ready for the next command. Sending a tag command (i.e. select, continuous read) the reader is powered up.

5.4.3.6 Read/Write user port

This command sets or reads the state of the user port (pin 14) of the OEM reader device. The port is set either as output or as input.

Command

Command	Data
‘pr’	none
‘pw’	State of user port (1 Byte)

Answer

Answer	Description
Data	State of user port (1 Byte)

Example

Command	Description
pr	Reads user port
pw01	Sets user port state to high

5.4.3.6.1 Read port

The port read command returns the actually state of the USER port.

Port state	Description
00	USER port is low
01	USER port is high

Figure 5-16: Read USER port return values

5.4.3.6.2 Write port

If user port is used as an output a 1kΩ resistor has to be integrated into the wire. Otherwise the reader device may cause damage.

Port state	Description
00	Sets USER port to low
01	Sets USER port to high

Figure 5-17: Write User port settings

5.4.3.7 Read reader EEPROM

This command reads the internal reader EEPROM. It contains all startup parameters and the device ID. Changes of the startup settings will only be taken into effect after a reset of the device.

Command

Command	**Data**
‘re’	EEPROM address (1 byte) 00h … 1Fh

Answer

Answer	**Description**
Data	EEPROM data (1 byte)
'?’	Error: register address exceeds range.

Example

Command	**Description**
rp05	01 Reads protocol configuration register.

5.4.3.8 Select

This command selects a single card in the antenna field. It can only be used in single tag mode. In the case of success the command returns the UID of the selected card. The reader detects the length of the card automatically.

Command

Command	Data
‘s’	None

Answer

Answer	Description
Data	serial number
‘N’	Error: No Tag in the field

Example

Command	Description
S	1234567890ABCD Select the card with its UID 1234567890SABCD.

5.4.3.8.1 Select a single tag

No previous continuous read is required. The command executes an automatic field reset.

5.4.3.8.2 Extended ID (default)

See above for more information of the Extended ID.

5.4.3.8.3 Multiple tags

This command is designed for fast access of a single tag in the field. If multiple cards are used the ‘m’ instruction has to be used instead.

5.4.3.9 Transfer data telegram

This command sends a custom data block to a card. First the proper tag type has to be specified using the set tag type command. The command shows a specific command frame for each tag type.

Command

Command	Data
‘t’	Downlink length (1 byte) Option byte (1 byte) Data (n bytes)

Answer

Answer	Description
Data	Response of card
'C'	Error: Collision
‘F’	Error: General failure
'N'	Error: No Tag in the field

5.4.3.9.1 Downlink length

The downlink length includes the data length. The CRC is computed automatically and is not included (optional).

5.4.3.9.2 Option Byte

This byte contains the transfer options. For ISO 14443 type B tags only bits 2 and 3 are interpreted. The crypto unit is only activated after a successfully log in.

Bit	Description
0	If set parity generation is enabled
1	If set parity is even, otherwise parity is odd
2	If set CRC generation for transmission is enabled
3	If set CRC checking for receiving is enabled
4	If set the crypto unit is deactivated prior transmission start. Only the log in sequence switches on the crypto unit correctly.
5, 6, 7	Bit framing. Number of bits of the last byte to transmit.

Figure 5-18: Option byte of the transfer command

5.4.3.9.3 Collision 'C'

If a collision is detected the anticollision sequence is required before accessing the tags. Thus anticollision is a complex procedure it is recommended to use Multitag List and Multitag select.

5.4.3.9.4 CRC generation

CRC generation described in ISO 14443-3 Appendix B.

5.4.3.9.5 Receiving answer

The reader switches to receiving mode automatically after data is sent. If no data is detect the reader returns the error 'N' no tag in field. If the time out value (register 07h and 08h) is too short the reader aborts detecting the answer before it is sent. Increase the time out value and the communication will work.

Examples for ISO-A tags (in ASCII mode)

Select sequence for a single tag in the field

Command	**Answer**	**Description**
t01E326	020400	REQA
t02039320	05**81635640F4**	Get serial number
t070F9370**81635640F4**	0188	Select card with UID81635640F4
t020F**30**04	10010203...	Read block 4: (after login) command code is 0x30

5.4.3.10 Get Version

This command returns the current version of the reader module.

Command

Command	Data
‘v’	None

Answer

Answer	Description
'Mifare 0.15e + <CR> + <LF>	ASCII Mode
02 00 0C 4D 69 66 61 72 65 20 30 2E 31 35 65 97 03	Binary Mode

Example

Command	Description
V	‘Mifare 0.15e’ Version of the reader module

5.4.3.11 Write master key

This command stores a MIFARE Standard key into the master key memory of the reader.

Command

Command	Data
‘wm’	Key number (1 byte) Key (6 bytes)

Answer

Answer	Description
Data	written key (6 bytes)
‘F’	Error: Write failure

Example

Command	Description
wm00112233445566	Store key 112233445566h in EEPROM (key number 0).
wm02A0A1A2A3A4A5	Store transport key 1 in EEPROM key 2.

5.4.3.11.1 Writing master keys

Keys are write only. The read after write operation fails. Nevertheless the reader returns correct error messages if the writing process fails.
A verification of the master key can only be done using an appropriate card and a successful login.

5.4.3.11.2 Using master keys for authentication

Master keys may be used for ISO-A tag authentication. It is possible to use every stored for key A as well as key B authentication.
Each key is 6 bytes long and stored redundantly for data security.

5.4.3.12 Write EEPROM

Writes to the internal reader EEPROM. It contains all startup parameters and the device ID. Changes of the startup settings will only be taken into effect after a reset of the device.

Command

Command	Data
‘wp’	Page address (1 byte) 04h … 1Fh Data (1 byte)

Answer

Answer	Description
Data	EEPROM data (1 byte)
'F'	Error: Read after write failure
'?'	Error: register address exceeds range

Example

Command	Description
Wp0401	Set EEPROM address 0A (Station ID) to 01h

5.4.3.12.1 Out of range failure 'R'

The entered page address exceeds the address range.

5.4.3.13 Reset

This command executes a power on (software) reset. New configuration settings will be loaded. It resets all tags in the antenna field.

Command

Command	Data
‘x’	None

Answer

Answer	Description
'Mifare 0.15e’ + <CR> + <LF>	ASCII Mode
None	Binary Mode

5.4.3.13.1 Reset Timing

The power up timing depends on environmental conditions such as voltage ramp up. For handheld devices the timing can change on the charging state of the battery.

5.4.4 ISO 14443 Type A only commands

5.4.4.1 Increment value block (credit)

Increments a value block with a defined value. A read after write is done automatically to verify data integrity. The command fails if the source block is not in value block format. A previous log in needed to access a page.

Command

Command	Data
'+'	Block (1 byte) Value (4 bytes)

Answer

Answer	Description
Data	Value (4 bytes)
'I'	Error: value block failure
'F'	Error: increment failure
'N'	Error: No tag in field
'O'	Error: Operation mode failure

Example

Command	Description
+0400000001	Adds 1 to value block 4
+0500000100	Adds 256 to value block 5

5.4.4.1.1 No value block 'I'

Specified block does not match the value format. The value block is corrupted. A backup block can be used to restore the correct value.

5.4.4.1.2 Increment failure 'F'

General failure during increment procedure or unable to read after write.

5.4.4.1.3 No tag error 'N'

The reader does not detect a response of the tag. There is either no tag present or the tag does not respond t the request.

5.4.4.1.4 Operation mode failure 'O'

The presented tag is not ISO14443 type A compliant

5.4.4.2 Decrement value block (debit)

Decrements a value block with a defined value. A read after write is done automatically to verify data integrity. The command fails if the source block is not in value block format. A previous log in is needed to access a page.

Command

Command	Data
'-'	Block (1 byte) Value (4 bytes)

Answer

Answer	Description
Data	Value (4 bytes)
'I'	Error: value block failure
'F'	Error: increment failure
'N'	Error: No tag in field
'O'	Error: Operation mode failure

Example

Command	Description
-0400000001	Subtract 1 to value block 4
-0500000100	Subtract 256 to value block 5

5.4.4.2.1 No value block 'I'

Specified block does not match the value format. The value block is corrupted. A backup block can be used to restore the correct value.

5.4.4.2.2 Decrement failure 'F'

General failure during decrement procedure or unable to read after write.

5.4.4.2.3 No tag error 'N'

The reader does not detect a response of the tag. There is either no tag present or the tag does not respond t the request.

5.4.4.2.4 Operation mode failure 'O'

The presented tag is not ISO14443 type A compliant

5.4.4.3 Copy value block (backup)

Copies a value block to another block of the same sector. A read after write is done automatically to ensure data integrity. Used for backup and error recovery. A previous log in is needed to access a page.

Command

Command	Data
'='	Source block (1 byte) Target block (1 byte)

Answer

Answer	Description
Data	New value of target block (4 bytes).
'I'	Error: value block failure
'F'	Error: increment failure
'N'	Error: No tag in field
'O'	Error: Operation mode failure

Example

Command	Description
=0405	Copy value block 4 to block 5
=0506	Copy value block 5 to block 6

5.4.4.3.1 Target block

The target block needs not to be a valid value block. If source block is not in value format the command fails.

5.4.4.3.2 No value block 'I'

Source value block does not match the value format. The value block is corrupted. A backup block can be used to restore the correct value.

5.4.4.3.3 Copy failure 'F'

General failure during copy procedure or unable to read after write.

5.4.4.3.4 No tag error 'N'

The reader does not detect a response of the tag. There is either no tag present or the tag does not respond t the request.

5.4.4.3.5 Operation mode failure 'O'

The presented tag is not ISO14443 type A compliant

5.4.4.4 Login (authenticate tag)

Performs an authentication to access one sector of a card. Only one sector can be accessed at the same time.
Optionally to transmit the key data to the reader stored keys in the reader EEPROM can be used.
To store keys in the EEPROM the write master key command is used. It is possible to store up to 32 master keys in the reader EEPROM. The login requires a successful select.

Command

Command	Data
'l'	Sector (1 byte) Key type (1 byte) AAh authenticate with key type A FFh authenticate with key type A, transport key FFFFFFFFFFFFh BBh authenticate with key type B 10h … 2Fh authenticate with key type A using stored key (00h … 1Fh) 30h … 4Fh authenticate with key type B using stored key (00h … 1Fh) Key (6 bytes) By transmitting <CR> instead of the keydata authentication is done with manufacturers transport keys (A0A1A2A3A4A5h, B0B1B2B3B4B5h, FFFFFFFFFFFFh).

Answer

Answer	Description
Data	Login status (1 byte)
'L'	Login success
'F'	Error: General failure
'N'	Error: No tag
'O'	Error: Operation mode failure
'R'	Error: Out of range
'X'	Error: Authentication failed

Example

Command	Description
l02AA<CR>	authenticate for sector 2, using the transport key A (A0A1A2A3A4A5h, key type A)
l3FBB<CR>	authenticate for sector 63, using the transport key 2 (B0B1B2B3B4B5h, key type B)
l04FF<CR>	authenticate for sector 4, using the transport key 3 (FFFFFFFFFFFFh, key type A)
l0FAAFFFFFFFFFFFF	Authenticate for sector 15, using key FFFFFFFFFFFFh, key type A
l0E14	Authenticate for sector 14, using EEPROM key 4, key type A
l0530	Authenticate for sector 5, using EEPROM key 0, key type B
l0732	Authenticate for sector 7, using EEPROM key 2, key type B
l0110	Authenticate for sector 1, using EEPROM key 0, key type A
l0ABBFF12FFFFFF35	Authenticate for sector 10, using key FF12FFFFFF35h, key type B

5.4.4.4.1 No tag error 'N'
The reader does not detect a response of the tag. There is either no tag present or the tag does not respond t the request.
5.4.4.4.2 Operation mode failure 'O'
The presented tag is not ISO14443 type A compliant
5.4.4.4.3 Out of range failure 'R'
The entered key type is incorrect.

5.4.4.4.4 <CR>

Three transport keys are implemented to access cards fast.
Transmitting <CR> instead of the key the reader module uses transport keys for the login procedure.

Command	Description
LxxAA<CR>	Authenticate for sector xx, using the transport key A (A0A1A2A3A4A5h, key type A)
LxxBB<CR>	Authenticate for sector xx, using the transport key 2 (B0B1B2B3B4B5h, key type B)
LxxFF<CR>	Authenticate for sector xx, using the transport key 3 (FFFFFFFFFFFFh, key type A)

5.4.4.4.5 Login with keydata from EEPROM

Each key stored in the reader EEPROM can be used as keytype A or keytype B. To use a key as type A the value 10h must be added to the key index. 30h must be added to use a key as type B.

5.4.4.4.6 Usage of key A, key B

Mifare® cards support two different crypto keys for each sector. Each key is 32 bit long and is stored in the sector trailer (last block of the sector) on a card. It is possible to set different access rights for each key.

5.4.4.5 Read page

This command reads a data block on a card. Size of returned data depends on the used tag. The page address range depends on the present tag.

Command

Command	Data
‘r’	page address (1 byte)

Answer

Answer	Description
Data	page data (depends on tag type)
‘F’	Error: read failure
‘N’	Error: No tag in field
'O'	Error: Operation mode failure

Example

Command	Description
r05	Reads page 05.

5.4.4.5.1 Read failure 'F'

This error is returned if the reader receives either bad data or the page address exceeds the page address range of the sector.

5.4.4.5.2 No tag in field 'N'

The tag does not respond. There is either no tag present or not addressed.

5.4.4.5.3 Operation mode failure 'O'

The presented tag is not ISO14443 type A compliant

5.4.4.6 Read value block

Reads a value block. The command checks if data is in value block format. The read value block command needs a successful login.

Command

Command	Data
‘rv’	Value block (1 byte)

Answer

Answer	Description
Data	Read value (4 bytes)
‘F’	Error: General failure
'I'	Error: value block failure
‘N’	Error: No tag in field
'O'	Error: Operation mode failure

Example

Command	Description
rv04	Reads value of block 4.

5.4.4.6.1 No value block 'I'

The value read back after the write value instruction is a not a value block. Data was written corruptly.

5.4.4.6.2 No tag error 'N'

This means that the tag does not respond, because there is either no tag present or none of the tags in the field is authenticated (‘I’ instruction).

5.4.4.6.3 General failure 'F'

Additional to a data read error caused by bad transmission conditions, this error appears if a sector is addressed which is not located in the authenticated sector.

5.4.4.6.4 Operation mode failure 'O'

Write value block is only valid for ISO 14443 A tags.

5.4.4.7 Write page

This command writes data to a page. A read after write is done automatically to ensure correct writing.

Command

Command	Data
‘w’	Page address (1 byte) Data (n bytes)

Answer

Answer	Description
Data	Page data (depends on tag type)
‘F’	Error: Write failure
‘N’	Error: No tag in field

Example

Command	Description
w0511223344	Writes data 11223344 on page 05.

5.4.4.7.1 Write failure 'F'

This error is displayed if bad transmission conditions are given. If the page address exceeds the physical number of pages of a tag this error is thrown.

5.4.4.7.2 No tag error 'N'

This error is returned if no tag is present or the card does not respond.

5.4.4.8 Write value block

This command formats a block as a value block containing a 32-bit value. A read after write is performed automatically. Value blocks need a complete 16-byte block due to redundant storage. A successful login is required to run the command.

Command

Command	Data
‘wv’	Value block (1 byte) Value (4 bytes)

Answer

Answer	Description
Data	Written value (4 bytes)
'I'	Error: value block failure
‘F’	Error: increment failure
‘N’	Error: No tag in field
'O'	Error: Operation mode failure

Example

Command	Description
Wv05010055EF	Writes value 010055EFh to block 5.

5.4.4.8.1 Invalid value 'I'

The value read back after the write value instruction is a not a value block. Data was written corruptly.

5.4.4.8.2 Write failure 'F'

Additional to a data read error caused by bad transmission conditions, this error appears if a sector is addressed which is not located in the authenticated sector.

5.4.4.8.3 No tag error 'N'

This error is returned if no tag is present or the card does not respond.

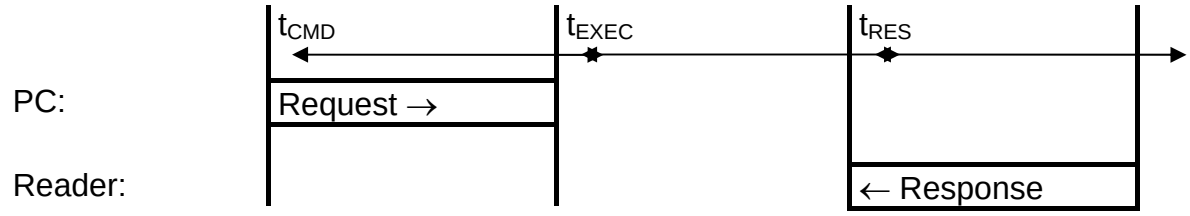
5.4.4.8.4 Operation mode failure 'O'

Write value block is only valid for ISO 14443 A tags.

5.4.4.8.5 Writing values

The write value block command is designed to create blocks, which match the value format. This command requires write access to specified block. It is not recommended to use this instruction for ticketing operations. For ticketing applications special instructions (Increment/Decrement/Copy) are supported.

6 Timing



Command	Command	Execution			Response
		t_{FAIL}	t_{TYP} [4]	t_{NOTAG} [5]	
Reset			94		
Cont. Read		various [6]			
Select		var.			
Multi Tag Select		var.	30	43,2	
Multi Tag List		various			
Login		19	5	34	
Read					
Data [r]		1,5	3,8	16,1	
Value [rv]		4	4	16,1	
EEPROM [re]			1,2		
Write					
Data [w]		18,2	15,6	33	
Value [wv]		18,2	15,6	33	
EEPROM [we]			9,7		
Master Key [m]			116		
Power ON			5,4		
Power OFF			<0,1		
Port					
write [w]			0,2		
read [r]			0,2		
Get ID		various			
Transfer Telegram		various			
Increment		4	15,3	16	
Decrement		4	15,3	16	
Copy		4	15,3	16	
Operation mode					
set ISO A [oa]			2		
set ISO A [ob]			<1		
set ISO AB [ot]			2		

All values are ms. Grey marked cells are fixed values.

[4] Indicates a successful processing of the command
[5] Indicates that no TAG is within reading range, depends on TMR value (register 07/08)
[6] Depends on number of tags within reading range

All timing data is advisory application information and does not form part of the specification. It may change in further firmware releases.
Timing for “Request” and “Response” is fixed by digital processes and depends on the operation speed (Baud rate) used by the RS232 interface.

7 Frequently Ask Questions

7.1 Getting Started

To test and interface the Mifare® OEM Module, you do not need a sophisticated µP development system. All you need is a PC, a connection cable and a power supply for the reader. If you are using Microsoft Windows (95/98/NT/…), take the following steps:

- Make sure, that your reader is RS232-interface type
- Start HyperTerminal
- Create a new connection (FILE/NEW CONNECTION)
- Enter name of connection as you like (i.e. ‘MIFARE’)
- Select connect COM2 (COM1) direct connection
- Connection setup 9600,8,n,1,no handshake
- Connect your reader to COM2 (COM1) of the PC and apply appropriate the supply voltage. The reader transmits a string to the host. This String denotes the firmware provided by your reader module
- Put a tag to your reader. Serial numbers should be displayed properly
- Enter commands via keyboard. They should be transmitted to the reader and the reader should reply

If using an operating system different from Microsoft Windows you may use any other terminal program which is capable of receiving/transmitting via the serial port of your PC.

7.2 How should the MIFARE® reader be personalized?

In ASCII protocol applications, no personalization is necessary.

For bus applications that are using the binary protocol mode a personalization procedure is required.

To configure the reader for binary protocol mode the following instruction flow is recommended.

- Start HyperTerminal
- Connect your reader to the PC and turn on the supply voltage
- The reader transmits the Version String (i.e. “MIFARE 0.15a”) after initialization
- Type ‘we00xx’ (where xx denotes the Station ID for the reader) to set the ID
- Wait until the reader replies with ‘xx’. Now the Station ID is set. You may read it by typing ‘re04’
- To set the reader into binary protocol mode type ‘we0502’. It is stored non-volatile in the binary mode flag (Protocol Configuration Byte).
- Until you reset the reader (turn off the supply voltage or type ‘x’) the reader stays in ASCII protocol mode

- By typing ‘x’ the reader execute a reset. In binary mode the reader does not transmit the version string at start up any more and does not respond to the ASCII command set.

To restore the ASCII protocol mode you have to transmit the write EEPROM command (in binary mode: >02h FFh 04h 77h 65h 01h 01h E8h 03h<) that resets the binary mode flag.

7.3 What type of Mifare® card should I use?

MIFARE® Light was designed as a lean solution for a single application environment. It contains only one sector with 2 keys, access condition, 2 data blocks and one value block.

MIFARE® Standard was designed for a multi application environment. It contains 16 sectors each with 2 individual keys, access conditions, 3 data or value blocks. Some applications use the 1 Kbytes of the MIFARE® Standard Card Memory just as storage.

7.4 We would like to use Mifare® for cashless payment. How safe is it?

Security is always a property of the overall system, not of the components. It requires careful design.
A properly designed system will require **ALL** barriers to be hacked in order to be broken.
For good design start specifying feasible attacks. Then create barriers to block them.
MIFARE® was specifically designed for cashless payment applications. The MIFARE® concept provides following barriers:

- Anticollision/-selection
- Atomic value transaction
- Ciphered communication
- Storage of values and data protected by mutual authentication
- Weak field keys that allow decrement only
- Stored keys in the reader that are not readable
- Keys in the card that are not readable
- A brute force attack by trying different keys is limited by the transaction time (several msec) of the card and would last virtually forever.
- Etc.

The Application can and should provide more barriers:

- Sector access conditions. It is possible, to assign access conditions in a way that only decrementing of values is allowed with the keys used in the field. So even a manipulated field station cannot be used to charge cards with additional values. As a rule, key A is used as a field key, allowing decrement and read only, and key B to format the card or charge values.

- Diversified keys. To make life even harder for attackers, keys can be modified using serial number and memory content of the card. So each card uses different keys and a listening attack on the reader interface would be hopeless.
- Limiting cash volume stored on a card
- Do not use the transport keys (keys as programmed after delivery) for ticketing applications!
- Ciphered and scrambled data storage
- Sabotage alarm
- Etc.

7.5 How does ticketing work with Mifare®?

To get a quick impression, connect the reader to a terminal program, take a new card and try the following steps:

Put the card in the field. The terminal program should show continuously the serial numbers of the card, for example “D1635640”.
Enter space. The transmission of serial numbers should stop.
Enter “s” for select. A Mifare® card always has to be selected, before it can be accessed.
If using a Mifare® Standard card you may proceed as following.
Enter “l01<ENTER>” for login to sector 01. This uses key A and the transport key A0A1A2A3A4A5. Alternatively you can type in “L01AAA0A1A2A3A4A5”, specifying that you want to use key A which is A0A1A2A3A4A5 on a new card. A login is always needed before a sector can be accessed. For new Philips cards use “l01FF<ENTER>” since they have FFFFFFFFFF as transport key.
Now you can access block 04, 05, 06, 07, which are on, sector 01. If you enter “w04000123456789AABBCCDDEEFFDDEE0375” then the data 000123456789AABBCCDDEEFFDDEE0375 gets written to block 04. To read it, enter “r04”.
To format block 04 as a value block and store 1500 points (1500dec=000005DChex) enter “wv04000005DC”.
To use up 100 points (100dec=00000064hex) enter “-0400000064”
To backup the value into block 05 enter “=0405”
You also can add to the values on the card. To charge 500 points (500dec=000001F4hex) enter “+04000001F4”.

7.6 What happens, if somebody pulls the card out of the field during a transaction?

Modifying memory content of a MIFARE® card is an EEPROM write operation internally. It requires a sufficient energy supply to execute properly. If a card leaves the field during an EEPROM write, corrupted data may be left. However, a sophisticated transaction scheme inside the MIFARE® tag reduces the chance of this happening significantly, maybe you will never encounter it in your tests. Incrementing or decrementing is safer than doing read-write explicitly. In addition to that the application can be designed in a way, that each value block is mirrored in a backup

block. This allows for automatic recovery of lost data resulting in very reliable systems. However, carefully designing and testing the application is recommended.

7.7 Manual activation sequence for ISO-A tags:

For single tag applications:
t01E326 valid reply: 020400 (send REQA)
t02039320 valid reply: 05**81635640F4** (81635640F4 denotes SN of tag)

For multi tag applications:
m<CR> valid reply: List of accessible tags.

To select a specific tag (after sending REQA):
t070F9370**81635640F4** answer: 0188 (Select card 81635640F4)

After selecting a tag additional parameter selection is done by the RATS sequence.
t020FE020 (send RATS)
valid reply: ATS bytes (refer ISO 14443-4 section 5.2)

7.8 Manual activation sequence for ISO-B tags:

For single tag applications:
t030C050008 (REQB, 1 time slot)
valid reply: 0C50**34030F07**63223344000002

For multi tag applications:
As above, use Multi Tag List.

To select s specific tag (after sending REQB)
t090C1D**34030F07**00020100
valid reply: 0100

Note: The select procedure is called ATTRIB in ISO 14443-3 protocol parameters (max. frame size, …) are defined during the select process. For details refer ISO 14443-3.

After selecting and configuring (ATS/ATTRIB or PPS) a tag, higher-level communication can be initialized.

The half duplex block transmission protocol features special needs of contactless environment.
Communications is designed according to principles of the OSI reference model.
Four layers are defined.

Physical layer (exchange bytes -> ISO 14443-3)
Data link layer (exchange blocks -> this clause)
Session layer (combined with data link layer for minimum overhead)
Application layer (process commands, which involve to exchange at least one block or a chain of blocks)

7.9 Block format

A block consist of following elements:
PCB (Protocol Control Byte, mandatory)
CID (Card Identifier, optional)
NAD (Node Address, optional)
INF (Information field, optional)
EDC (Error Detection code, mandatory)

Prologue field			**Information field**	**Epilogue field**
PCB	[CID]	[NAD]	[INF]	[EDC]
1 byte	1 byte	1 byte	various	2 bytes

7.9.1 PCB

The PCB is used to distinguish between three different block types as well as define if CID/NAD are following.
I-blocks
They are used to convoy information used by the application layer.
Frames, which exceeds the max. frame size set between the reader<>card communication are divided up (chaining ISO 14443-4 section 7.4.2).
R-blocks
They are used to convoy positive or negative acknowledgements.
R-blocks never contain an INF field. The acknowledgement relates to the last received block.
S-blocks
They are used to exchange control information between card and reader.
Tow types of S-block are used.
DESELECT
Deselect contains no INF field. Put a tag into HALT state.
Waiting time extension
WTX contains one byte INF field.

For detailed coding of PCB refer ISO 14443-4 section 7.1.1.1.

7.9.2 CID

4-bit long logical card address in range of 00h to 0Eh, 0F is RFU.

7.9.3 NAD

Should be compliant to NAD defined in ISO 7816-3.

7.9.4 INF

Commands and data mainly used are the application layer.

7.9.5 EDC

Defines as 16-bit CRC, could be automatically generated by the reader module (refer Option byte of Transfer Data Command).

Examples:

Description		**Data stream**
I-Block (no CID, no NAD)	Application level command	02 INF EDC
I-Block (CID=05, no NAD)	Application level command	0A05 INF EDC
R-Block (no CID, no NAD)	Acknowledged	A2 EDC
R-Block (CID=06, no NAD)	Not acknowledged	BA06 EDC

7.10 Application level command (Type A tag)

As an example for application level command we use an imaginary tag.
This tag supports a ”Get Challenge Code” command used to for authentication procedure, which has to be packed into a proper transmission block.

7.10.1 Get Challenge

The “Get Challenge” command does fit following command parameter.
00840000xx
Where xx denotes the length of the challenge code.

A proper block for a 7-byte challenge will look like this.
020084000007
02 indicate an I-block (PCB) without CID and NAD (which are optional).

The instruction to transfer that block will therefore be.
t060F020084000007
The option byte (0Fh) sets the reader to automatically generate CRC and parity data.

If using an ISO-B tag set the option byte to 0Ch in order to pay attention to ISO/IEC 14443-3 Annex B (CRC generation).
Frequently Asked Questions

7.11 How to implement a device driver?

For the implementation of device drivers using the Mifare® OEM module a separated Applications Note is available including source code examples.
Additionally a PC/SC compliant device for the MIFARE Module is already available from United Access GmbH (http://www.united-access.de/). Furthermore, a smart card service provider for MIFARE standard cards and a PC security application (PC logon) is offered.

7.12 Major Differences between Version 0.14d and 0.15

Multiple operation modes to allow handling of ISO B tags
Anticollision procedure for ISO a tags is much faster
Timeout for card-reader communication mapped into registers

Revision History

1.3		Updated layout
1.2		Updated PCB examples Updated RF timeout
1.1	Internal Version	Updated ISO B documentation
1.0	Internal Version	First internal version

8 References:

[1] ISO/IEC 14443 Part 1-4, Identification Cards – Contactless integrated circuit(s) cards – Proximity cards

9 APPENDIX A

9.1 P & P Module (Version 3)

9.1.1 Pin Out

All distances are listed in mm.

RS485 operation:

Connect

Rx A with Tx A to RS485 – A
Rx B with Tx B to RS485 – B
GND to RS485 - GND.