ACGPass e-ID Desktop Reader

Document No.: 1510-USM-01-0-01

Firmware: Version Dual ISO 2.3

User Manual

ASSA ABLOY Identification Technologies GmbH
Am Klingenweg 6A
65396 Walluf
Germany
Phone +49 (0) 6123 791 0
Fax +49 (0) 6123 791 199
www.aaitg.com

Edition One - October 2006

ASSA ABLOY Identification Technologies GmbH (ASSA ABLOY ITG) reserves the right to make changes to its products or services or to discontinue any product or service at any time without notice. ASSA ABLOY ITG provides customer assistance in various technical areas, but does not have full access to data concerning the use and applications of customer's products.

Therefore, ASSA ABLOY ITG assumes no liability and is not responsible for customer applications or product or software design or performance relating to systems or applications incorporating ASSA ABLOY ITG products. In addition, ASSA ABLOY ITG assumes no liability and is not responsible for infringement of patents and/or any other intellectual or industrial property rights of third parties, which may result from assistance provided by ASSA ABLOY ITG.

ASSA ABLOY ITG products are not designed, intended, authorized or warranted to be suitable for life support applications or any other life critical applications that could involve potential risk of death, personal injury or severe property or environmental damage.

With the edition of this document, all previous editions become void. Indications made in this manual may be changed without previous notice.

Composition of the information in this manual has been done to the best of our knowledge. ASSA ABLOY ITG does not guarantee the correctness and completeness of the details given in this manual and may not be held liable for damages ensuing from incorrect or incomplete information. Since, despite all our efforts, errors may not be completely avoided, we are always grateful for your useful tips.

The installation instructions given in this manual are based on advantageous boundary conditions. ASSA ABLOY ITG does not give any guarantee promise for perfect function in cross environments.

The ACG logo is a registered trademark of ASSA ABLOY Identification Technologies GmbH.

Microsoft®, Microsoft Windows 98SE®, Microsoft Windows ME®, Microsoft Windows NT®, Microsoft Windows 2000® and Microsoft Windows XP® are registered trademarks of the Microsoft Corporation USA.

Pentium® is a registered trademark of the Intel Corporation USA

mifare® is a registered trademark of NXP Semiconductor N.V.

All other products mentioned in this document might be brands or brand names of the different suppliers.

Safety Instructions / Warning - Read before start-up!

- The device may only be used for the intended purpose designed by for the manufacturer. The operation manual should be conveniently kept available at all times for each user.
- Unauthorized changes and the use of spare parts and additional devices that have not been sold or recommended by the manufacturer may cause fire, electric shocks or injuries. Such unauthorized measures shall exclude any liability by the manufacturer.
- The liability-prescriptions of the manufacturer in the issue valid at the time of purchase are valid for the device. The manufacturer shall not be held legally responsible for inaccuracies, errors, or omissions in the manual or automatically set parameters for a device or for an incorrect application of a device.
- Repairs may be executed by the manufacturer only.
- Only qualified personnel should carry out installation, operation, and maintenance procedures.
- Use of the device and its installation must be in accordance with national legal requirements and local electrical codes.
- When working on devices the valid safety regulations must be observed.

Preface

Read This First

About This Guide

This manual describes the ACGPass e-ID Desktop Reader. Its goal is to describe the reader, how it works, how to integrate it and how to use it.

If You Need Assistance

Our application center is located in Europe to provide direct support. For more information, please contact your nearest ASSA ABLOY ITG Sales Center. The contact addresses can be found on our home page:

http://www.aaitg.com/

Table of contents

1 Scope

The ACGPass e-ID Desktop Reader supports a broad range of tags compliant with ISO 14443 type A and B standards, including SR176 tags and tags which belong to the Philips mifare® family. An open command structure allows the device to communicate with tags that use an operating system. The read/write unit supports automatic chaining, 256 byte buffer and frame length, extended time framing and up to 848kBaud transmission rates over the air interface.

Additionally this unit implements a DES cipher which enables to use mifare® DESFire tags. These tags are designed for use in high security algorithms.

An internal SAM socket is also available.

Major applications are:

- e-Passport
- e-National ID Cards
- e-Drivers Licenses
- e-Government
- e-Health Cards
- e-Document Authentication
- e-Document Issuing

2 Extended Documentation

Please note that all confidential material is excluded from this documentation in order to comply with NDA requirements of our suppliers as well as prevention from unauthorized copies of the reader modules for increasing the security in the applications.

You can obtain the extended documentation containing the confidential information after signing a NDA.

3 Definitions and Abbreviations

3.1 Definitions

3.1.1 Anti-collision loop

An algorithm used to identify and handle a dialogue between a reader and one or more tags in its antenna field.

3.1.2 Hex notation

A hexadecimal value is marked with the suffix ‘h’, i.e. A1h has the value A1 hexadecimal.

3.1.3 ASCII notation

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

3.2 Abbreviations

Abbreviation	Description
AID	Application ID
ASCII	American Standard Code for Information Interchange
ATR	Answer to Reset
ATS	Answer to Select
Block	For the mifare® Standard one block contains 16 bytes
CID	Card Identifier (logical card address, ISO 14443-4)
CRC	Cyclic Redundancy Check
DES	Data Encryption Standard, for more details about DES refer to [3].
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
OTP	One time programmable
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 the mifare® Standard one sector contains 4 blocks
SID	Station ID
SFGT	Guard time after RATS
SN	Serial Number of a tag (a 32 bit number)
SOF	Start of frame

Abbreviation	Description
TDES	Triple DES
Value block	32 bit data block format. Used in ticketing application
<CR>	Carriage return (0Dh)
<LF>	Line feed (0Ah)

Figure 3-1: Abbreviations

4 Supported tags

	Manufacturer	Serial number	Read block	Write block	Transfer command	Comments
ISO 14443 A						
mifare® Standard	Philips	√	√	√	√	Encryption included
mifare® 4k	Philips	√	√	√	√	Encryption not included
mifare® Ultralight	Philips	√	√	√	√	Encryption not included
mifare® ProX	Philips	√	√	√	√	
mifare® DESFire	Philips	√	-	-	√	
SLE66CLX320P	Infineon	√	-	-	√	
SLE 55R04/ 08	Infineon	√	-	-	√	
Smart MX	Philips	√	-	-	√	
Jewel Tag	Innovision	-	-	-	√	Works only with 't' command
ISO 14443 B						
SLE6666CL160S	Infineon	√	-	-	√	
SR176	STM	√	√	√	√	
SLIX 4K	STM	√	√	√	√	
ASK GTML2 ISO	ASK	√	-	-	√	
ASK GTML	ASK	√	-	-	√	Extended setup needed
Sharp B	Sharp	√	-	-	√	
TOSMART P032/064	Toshiba	√	-	-	√	
Dual Interface						
ISO 14443 A compliant (1)	Various	√	-	-	√	
ISO 14443 B compliant()	Various	√	-	-	√	

Figure 4-1: Supported labels

[1] Performance varies

5 The mifare® Transponder Family

The mifare® transponder family consists of various 13.56 MHz transponder ICs, all compliant to the ISO 14443 standard.

5.1 mifare® Standard

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

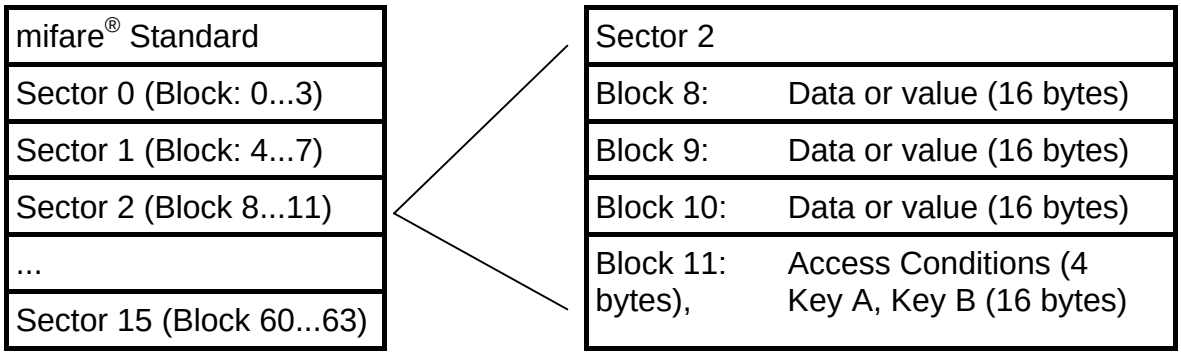


Figure 5-1: mifare® Standard: sector diagram

5.1.1 Sector 0 / Block 0

Block 0 is read only.

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

Figure 5-2: mifare® Standard: sector 0 / block 0

5.1.2 Blocks 3, 7, 11, 15, …

Transport keys are set on delivery:

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

Figure 5-3: 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 is used to read or write; key A itself is not readable; key B is data only). For further information refer to the mifare® card manual.

Remarks

Enabled keys are always read as 00 00 00 00 00 00

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

5.2 State Diagram

All mifare® cards use the following state diagram.

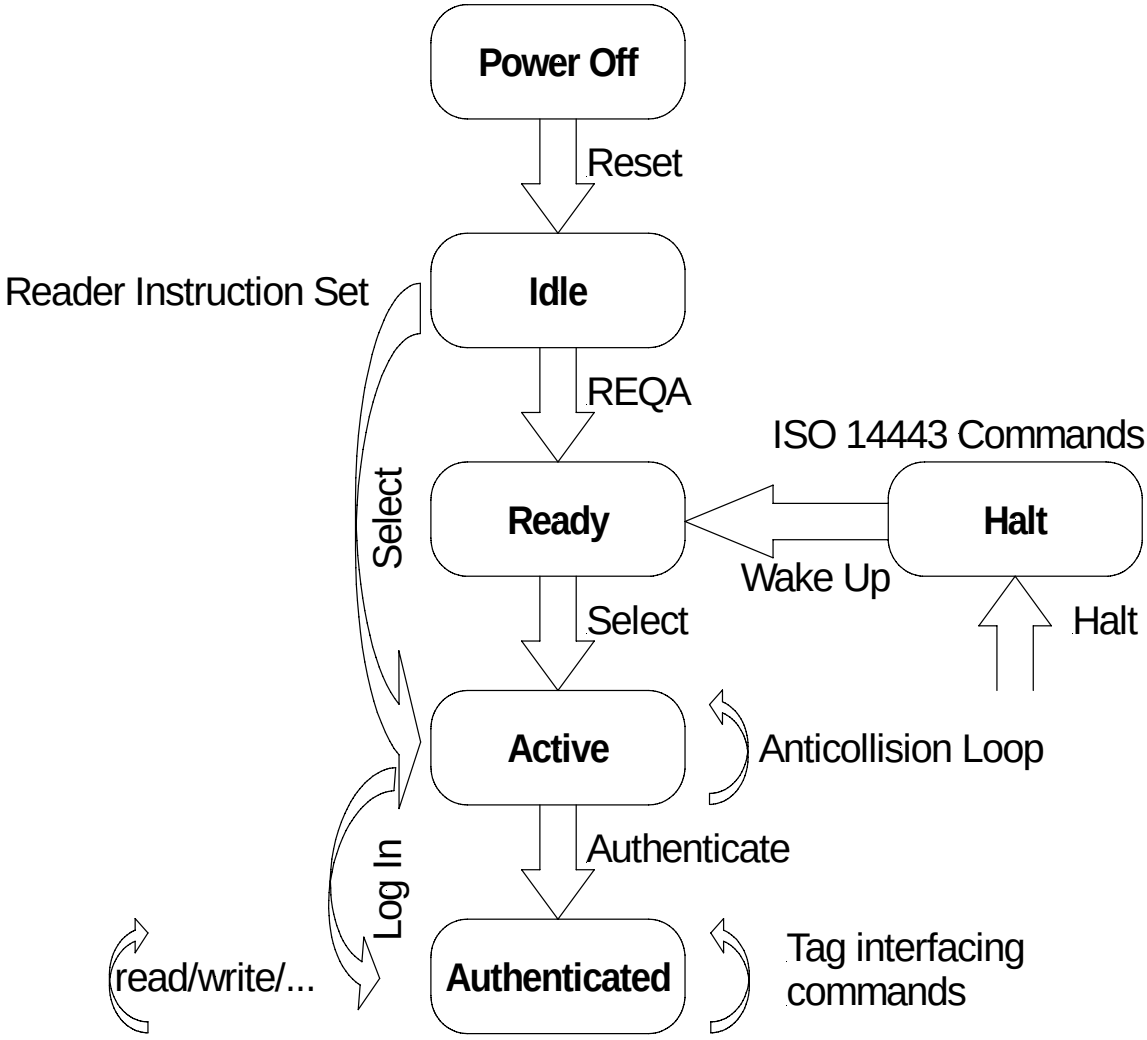


Figure 5-4: State diagram

5.3 mifare® Ultralight

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

mifare® Ultralight only supports 4 bytes per sector, but the command set uses 16 bytes per sector. Only the 4 least significant bytes are valid when using mifare® Ultralight.

Ensure that the other bytes match with the tag content when using the write command; otherwise the read back will fail.

5.4 mifare® 4k

mifare® 4k cards have an increased memory. Beginning from sector 32 (20h), sectors have 16 blocks. Due to compatibility reasons, the sector indices have changed according to the following table. The login sector has to be used to access the corresponding sector on the card.

Sector	Block	Login sector
00h	00h – 03h	00h
01h	04h – 07h	01h
…	…	…
1Fh	7Ch – 7Fh	1Fh
20h	80h – 8Fh	20h
21h	90h – 9Fh	24h
22h	A0h – AFh	28h
23h	B0h – BFh	2Ch
24h	C0h – CFh	30h
25h	D0h – DFh	34h
26h	E0h – EFh	38h
27h	F0h – FFh	3Ch

Figure 5-5: mifare® 4k sector index table

5.5 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 a proprietary encipher algorithm.

Before accessing the operating system, the card must be selected. Customized commands are issued using the transfer command.

5.6 mifare® DESFire

This tag supports additional security algorithms (DES, Triple-DES, MAC) for security sensitive applications.

DESFire tags are addressed using a specific command set (see DESFire command set).

5.6.1 Memory organization

The memory of a DESFire card can be personalized to specific requirements. The card can be seen as data storage device like a hard disk in a PC. The memory is divided into a maximum of 28 different applications (directories) with 16 files each. An application has up to 14 keys. Depending on keys and access conditions a file can be accessed in four different ways. Plain data is never secured. Data is secured using a MAC, single DES or triple DES enciphers.

The following figure describes the memory organization of a DESFire card.

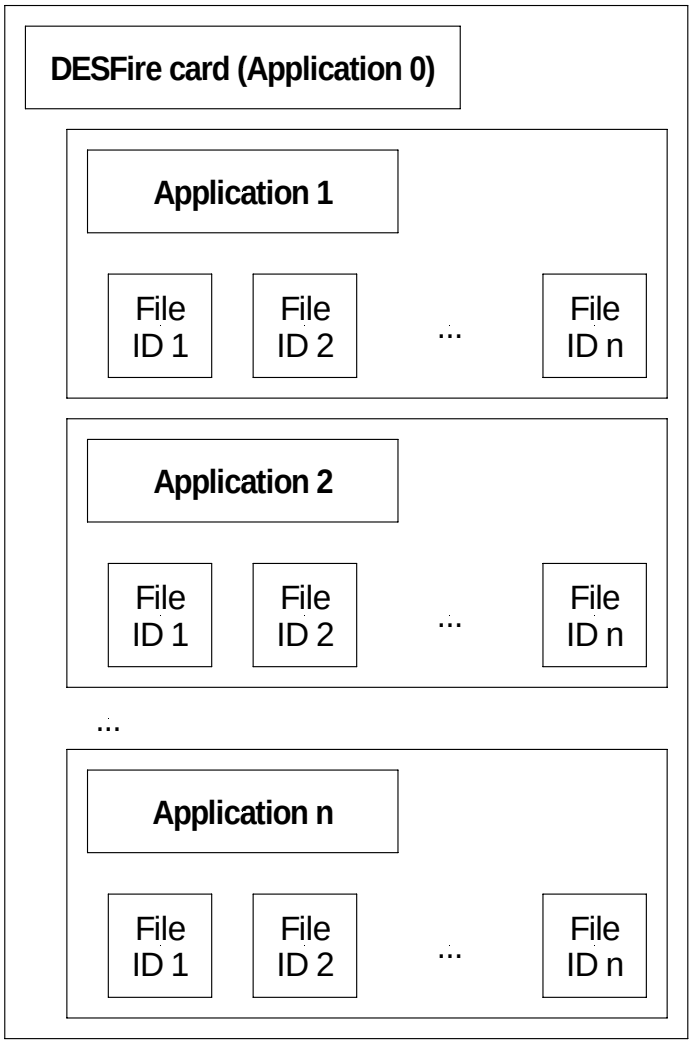


Figure 5-6: DESFire memory organization

5.6.2 State diagram of mifare® DESFire

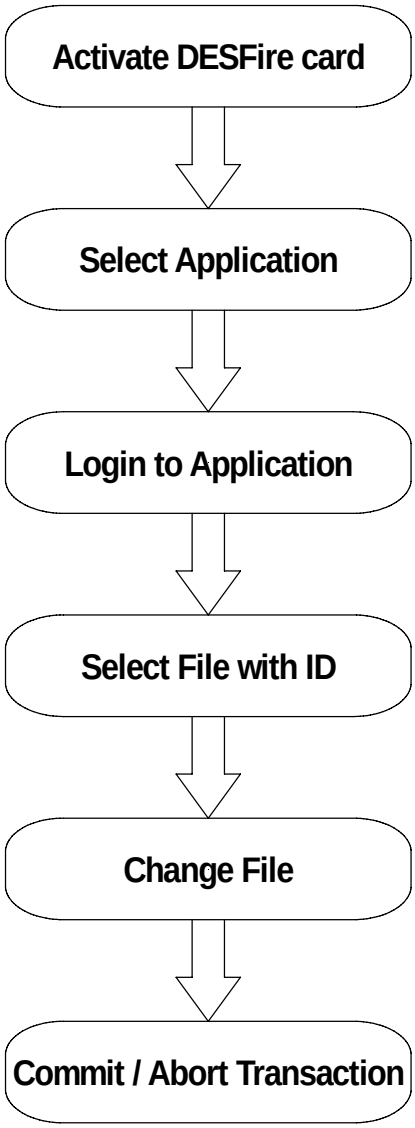


Figure 5-7: mifare® DESFire state diagram

5.6.2.1 Activate PICC

Before accessing a DESFire card, the card must be selected. A mifare® DESFire card has a 7 byte UID. After activation, the card is powered up and ready to accept a mifare® DESFire command. Application 0 is selected automatically.

5.6.2.2 Select application

To jump into another application, the application has to be selected. An application can be seen as a directory, which contains up to 16 files. The size of the application depends on the stored files.

5.6.2.3 Login to application

Specific access rights can be set for each application. Login to an application allows to change the organization of the application. Login to a file opens a secured file for access. A file can be accessed in four different ways: without any security or secured with MAC, single DES or triple DES.

5.6.2.4 Select file

Before accessing a file, the file must be selected

5.6.2.5 Change file

A selected file can be changed according its access rights. If a file is secured, a login is required before changes can be made.

5.6.2.6 Commit / Abort transaction

Value files, backup files, linear record files and cyclic record files only adapt their values after the commit transaction command is given. Several files can be changed within an application at the same time. The abort transactions command annuls all changes within an application. Power loss will cancel all modifications too.

For more details about application settings and access rights refer to [2].

6 ISO 14443 Type B

ISO 14443 type B cards are supported.

6.1 SR176

The SR176 label contains only 30 bytes of data organized in two bytes per page.

6.1.1 Memory organization

block address	Byte 1	Byte 0	
0Fh	Lock byte	RFU	Chip ID
0Eh	User data		
…	…		
04h	User data		
03h	Serial number		
02h	Serial number		
01h	Serial number		
00h	Serial number		

Figure 6-1: SR176 memory organization

6.1.2 Serial number UID

The UID is stored in the first 4 pages. Page 00h contains the LSB of the UID.

Page 03h		Page 02h		Page 01h		Page 00h	
Byte 1h	Byte 0	Byte 1	Byte 0	Byte 1	Byte 0	Byte 1	Byte 0

Figure 6-2: SR176 Serial number

6.1.3 Lock byte

The lock byte defines the write access condition of a pair of pages. Each bit can only be set once. This procedure is irreversible. This byte is implemented as an OTP.

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Page 0Eh Page 0Fh	Page 0Ch Page 0Dh	Page 0Ah Page 0Bh	Page 08h Page 09h	Page 06h Page 07h	Page 04h Page 05h	Page 02h Page 03h	Page 00h Page 01h

Figure 6-3: Lock byte

6.1.4 Chip ID

The Chip ID is defined in the low nibble of page 0Fh. It is manufacturer set and is used internally to select and separate single tags.

6.2 SRIX4K

The SRIX4K label contains 512 bytes of data organized into four-byte pages.

6.2.1 Memory organization

Block address	Byte 3	Byte 2	Byte 1	Byte 0
FFh	OTP Lock Reg	ST Reserved	ST Reserved	Fixed Chip ID
7Fh	User data			
…	…			
07h	User data			
06h	32 bits binary counter			
05h	32 bits binary counter			
04h	32 bits Boolean Area			
03h	32 bits Boolean Area			
02h	32 bits Boolean Area			
01h	32 bits Boolean Area			
00h	32 bits Boolean Area			

Figure 6-4: SRIX4K memory organization

6.2.2 Lock block

Locking of blocks is not supported with this tag.

7 Hardware

Figure 7-1: Picture of the complete reader

7.1 Mechanical dimensions

All Dimensions are in mm

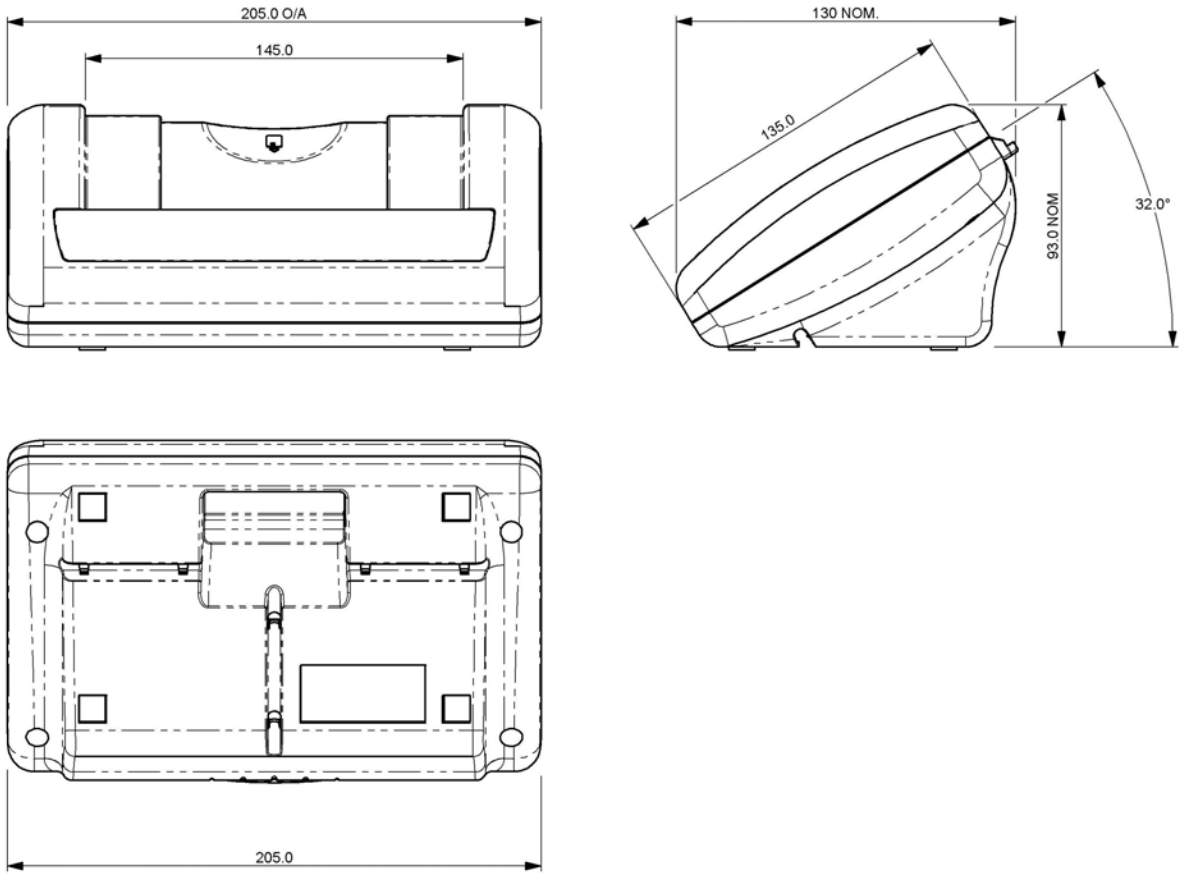


Figure 7-2: Mechanical drawing with dimensions

7.1.1 Features

- Interface type: USB 2.0
- Dimensions: 205x130x93 (LxWxH), all in mm
- Reading Distance: up to 90mm, depending on tag type
- SAM: supported[2]
- Boot loader: supported[3]
- Drivers: virtual COM port driver, DLL driver available
- Antenna: on board
- Signaling: RFID activity indicator LED
  Power LED
  Contact Interface activity indicator LED
  USB Online indicator LED
- Power Supply: via USB

[2] The integrated SAM socket is accessible by opening the housing

[3] The boot loader makes it easy to download a firmware to the unit without replacing/dismantling the hardware.

7.1.2 External Connections

7.1.2.1 USB Cable

The USB connector is located on the bottom side of the housing. Depending on the users preferences the cable can be put and easily fixed within one of three cable guides. Each cable guide leads the cable to one of three possible sides of the housing.

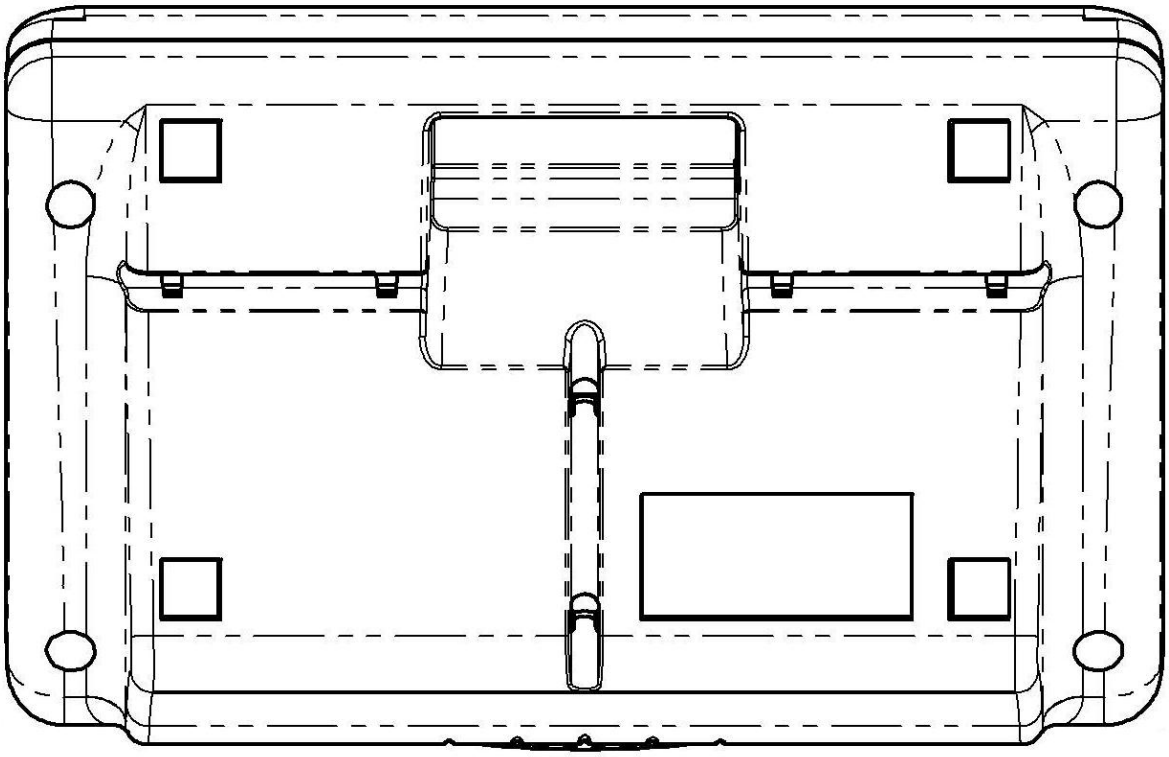


Figure 7-3: mechanical drawing, bottom view

7.1.2.2 Power Supply

The power supply is automatically provided via the USB connection. Therefore the unit can only be connected to a powered USB hub.

Non-powered USB hubs like often used in USB splitter units are not able to supply the reader with enough power. Depending on the internal protection of these units, they even may be damaged.

7.1.2.3 SAM Socket

The integrated SAM socket is accessible only by opening the housing.

- Before opening the housing an ESD protection has to be used.
- The reader has to be unpowered and unpluged from the host system. It's recommended to remove the USB cable on the reader side.
- Open the four screws on the bottom side with an appropriate screwdriver.
- Carefully remove the bottom part of the housing. Install the SAM.
- Close the bottom part of the housing and make sure both housing parts fit together.
- Carefully tighten the four screws again. If the screws are tightened too much, then housing might break.

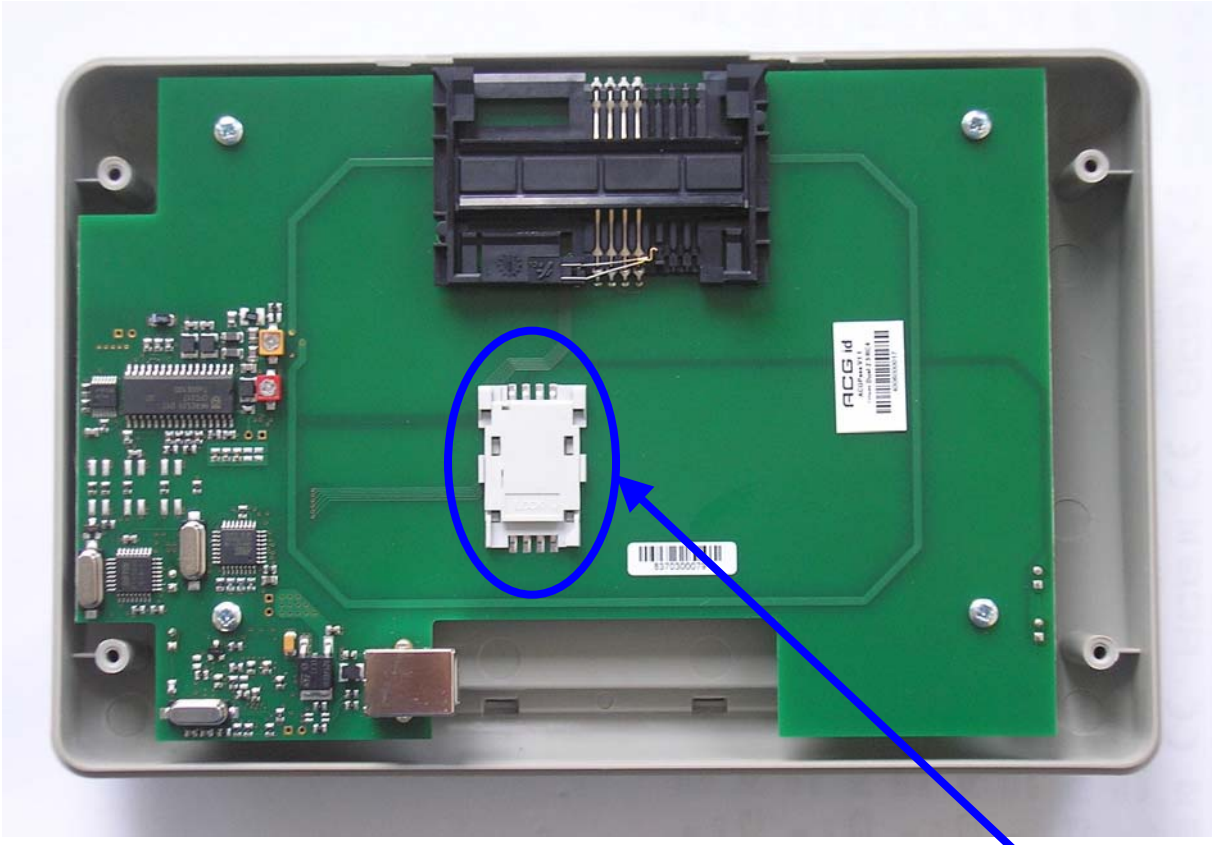


Figure 7-4: position of internal SAM Socket

7.1.3 Function Control Indicator LEDs

The reader comes with four integrated indicator LEDs.

Figure 7-5: Reader with activated indicator LEDs

7.1.3.1 Power LED

This LED shows the status of the power supply. If on, then enough power is provided by the USB hub to run the reader.

Figure 7-6: position and design of Power LED

7.1.3.2 RFID activity indicator LED

This LED shows any activities on the reader's contactless RFID interface. LED On means data is being sent to or received from the card.

Figure 7-7: position and design of RFID activity indicator LED

7.1.3.3 USB Online indicator LED

This LED shows the status of the USB connection. If on, then the reader is connected with the host system.

Figure 7-8: position and design of USB Online indicator LED

7.1.3.4 Contact Interface activity indicator LED

This LED shows any activities on the reader's contact interface. LED On means data is being sent to or received from the card.

Figure 7-9: position and design of contact interface activity indicator LED

8 Software for contactless interface functions

By 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.

If the PC/SC driver has been installed on the host PC, then the commands of this chapter can't be used as such. Only the PC/SC specification is valid in this case. The reader also can be installed with the standard USB driver. The driver can be downloaded from http://www.aaitg.com. This driver enables the usage of a virtual COM port on the host PC. Then all commands mentioned below can be used.

8.1 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
Variable length	Variable length

Figure 8-1: ASCII protocol frame

8.2 Binary Protocol

This protocol is designed for industrial applications with synchronization and frame checking. An addressing byte for party line (master/slave, multi-drop) is also included.

The protocol usually requires a device driver. Data is transmitted in binary mode. The reader uses an internal binary watchdog timer to ensure correct framing.

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

Figure 8-2: Binary Frame Version 1

The binary frame version 2 is only sent to the host. It is implemented to give extended information to the host.

Version 2 must be enabled in the Protocol configuration 2 register.

STX	Station ID	Length	Flags	Data	BCC	ETX
1 byte	1 byte	1 byte	1 byte	Variable length	1 byte	1 byte

Figure 8-3: Binary Frame Version 2

8.2.1 STX

Start of transmission (02h)

8.2.2 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 their response.

8.2.3 Length

Length of the data block, including the flag byte, if binary protocol version 2 is activated.

If length is set to zero, 256 data bytes are transmitted. The reader module only can send 256 data bytes, but can not receive commands with 256 bytes.

8.2.4 Flags

The flag byte gives additional information to the host.

Bit 3 – Bit 7	Bit 1 – Bit 2	Bit 0
RFU	Leading Character Info	Error State

Error State

If cleared, the command was processed successfully.

If set, an error occurred.

Leading Character Info

Bit 1 & 2 defines how to interpret the data in the binary frame.

Bit 2	Bit 1	Description
0	0	No leading character available, all values are hexadecimal.
0	1	The data contains one leading character.
1	0	All data bytes are characters.
1	1	RFU

8.2.5 Data

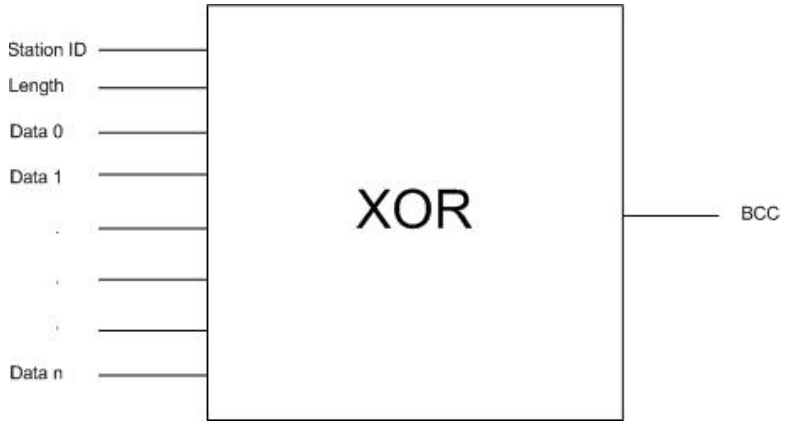
This part contains the command and the data. The command values are the same as in ASCII protocol mode (‘x’, ‘s’, …) whereas data is transmitted in binary mode.

The length of the command block depends on the instruction.

8.2.6 Block Check Character (BCC)

The BCC is used to detect transmission errors. The BCC is calculated XOR-ing each byte of the transmission frame excluding the STX/BCC and ETX characters. The flags are part of the data.

$$BCC = (StatID)\ XOR\ (Length)\ XOR\ (Command / Data_0)\ XOR \ldots XOR\ (Command / Data_N)$$



8.2.7 ETX

End of transmission. (03h)

8.2.8 Remarks

If the reader device receives an invalid instruction frame (i.e. wrong BCC) 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 time-out (see protocol configuration register) is used to detect incomplete binary frames.

8.2.9 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.

8.3 Register Set

The reader has several system flags used for customization purposes. The flags are stored in its non-volatile EEPROM. The reader accepts changes to these settings only during the start-up phase. Clearing all RFU bits is recommended in order to guarantee compatibility with future releases.

The reader can store up to 32 authentication keys internally to login standard mifare® cards. An additional 32 keys can be stored for DESFire authentication. All keys are read only and cannot be accessed via the interface lines.

8.3.1 EEPROM memory organization

Register	Description
00h … 04h	Unique device ID; read only
05h … 09h	Administrative data; read only
0Ah	Station ID
0Bh	Protocol configuration
0Ch	Baud rate
0Dh	Command Guard Time
0Eh	Operation Mode
0Fh	Single shot time-out value
10h	Internal use / Do not change
11h	Internal use / Do not change
12h	Internal use / Do not change
13h	Protocol configuration 2
14h	Reset Off Time
15h	Reset Recovery Time
16h	Application Family Identifier
17h	ISO 14443A Selection Time-out
18h	ISO 14443B Selection Time-out
19h	SR176 Selection Time-out
1Ah	RFU
1Bh	Protocol configuration 3
1Ch	Page Start
1Dh	Internal use / Do not change
1Eh	Internal use / Do not change
1Fh	Page number
20h - 7Fh	RFU
80h … EFh	User data

Figure 8-4: EEPROM memory

8.3.2 Unique device ID (00h – 04h)

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

8.3.3 Station ID (0Ah)

The station ID is used in binary mode to address a device in party line set up. The station ID can range from 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.

8.3.4 Protocol configuration (0Bh)

The protocol configuration register (PCON) specifies general behavior of the reader device.

Default value is 41h.

Protocol configuration register							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Extend-ed ID	Extend-ed Protocol	Single-shot	LED	New serial mode	Multitag	Protocol	Auto-start

Figure 8-5: Protocol configuration register

8.3.4.1 Auto start (default 1)

If set, the reader device will start up in continuous read mode automatically.

8.3.4.2 Protocol (default 0)

If set, the reader uses binary protocol mode. Refer to binary protocol for further information on the binary protocol format.

Default setting = ASCII protocol (0).

8.3.4.3 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.

8.3.4.4 New serial mode (default 0)

If set, new serial mode is enabled. The leading character ‘M’ is added to the serial number of ISO 14443 type A tags, a leading 'Z' character is added to ISO 14443 type B tags and a leading 'S' character for SR176 tags.

8.3.4.5 LED (default 0)

If set the reader suppresses any LED activity. The user manages the state of the LEDs.

8.3.4.6 Single shot (default 0)

If set, the reader displays the serial number of a tag in continuous read mode once within a specified time-out. The time-out is defined at EEPROM register 0Fh.

The delay time can be adjusted stepwise in 100ms steps. 00h indicates no delay and FFh indicates infinite delay.

8.3.4.7 Extended Protocol (default 1)

If set, the transfer data telegram command supports ISO14443-4.

The transfer data telegram command is only supported in normal mode, not in transmit / receive mode.

8.3.4.8 Extend ID (default 0)

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

ISO 14443 A tags (5/8/11 bytes transmitted)

Tag type	Serial number
1 byte	4 / 7 / 10 bytes

Figure 8-6: ISO 14443 A Extended Serial number

The tag type byte indicates the type of cascade level.

Tag type	Description
01h	Cascade level 1 transponder
02h	Cascade level 2 transponder
03h	Cascade level 3 transponder

Figure 8-7: ISO 14443 A tag type

ISO 14443 B tags (12 bytes transmitted)

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

Figure 8-8: ISO 14443 B Extended Serial number

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

8.3.5 BAUD, Baud rate control register (0Ch)

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	BS2	BS1	BS0

Figure 8-9: Baud rate register

This register defines the baud rate of the device.

BS2	**BS1**	**BS0**	**Baud rate**
0	0	0	9600 baud (default)
0	0	1	19200 baud
0	1	0	38400 baud
0	1	1	57600 baud
1	0	0	115200 baud
1	0	1	230400 baud (depends on the used interface chip)
1	1	0	460800 baud (depends on the used interface chip)

Figure 8-10: Baud rate settings

With the high baud rates (230400 and 460800 baud), proper operation depends on the interface chip used. Please note that some of the interface chips available do not support these high baud rates.

The following table describes the exact baud rates used by the reader.

Baud rate	Exact baud rate	Difference
9600 baud	9576 baud	-0.25 %
19200 baud	19261 baud	0.32 %
38400 baud	38523 baud	0.32 %
57600 baud	58448 baud	1.47 %
115200 baud	113000 baud	-1.91 %
230400 baud	241545 baud	4.84 %
460800 baud	483091 baud	4.84 %

Figure 8-11: Exact baud rates

The following table describes the communication settings

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

Figure 8-12: Communication settings

8.3.6 Command Guard Time (0Dh)

The Command Guard Time is used to ensure that commands are not sent to fast consecutively. Following commands are sent after the guard time is elapsed. One time slice is around 37,8us. The longest timeout value is 9,6ms (FFh).

The default value is 20h (1,2ms).

8.3.7 OPMODE, operating mode register (0Eh)

The operation mode register defines which tag types the reader supports. This register enables fast tag recognition because only defined tag types are requested.

Operation mode register							
Bit 7 (MSB)	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0 (LSB)
RFU	RFU	RFU	RFU	RFU	SR176	ISO 14443B	ISO 14443A

Figure 8-13: Operation mode register

8.3.8 Single Shot Time-out (0Fh)

The time-out value defines the delay time between two responses of the reader. It only has effect in continuous read mode. To enable the time-out, the single shot flag has to be set. See the protocol configuration register above. One time-out slice is around 100ms. Exact timing depends on the protocol used.

Value 00h indicates no delay time.

Default value is 0Ah (1 second).

8.3.9 Protocol configuration 2 (13h)

The protocol configuration register 2 (PCON2) further specifies the general behavior of the reader device.

Default value is 00h.

Protocol configuration 2 register							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Disable ISO 14443 -4 Error Handling	Enable ISO 14443B Anti-collision	Reset Recovery Time Multiplier		Noisy Environ-ment	Enable binary frame v2	Disable start-up message	Disable multi-tag reset

Figure 8-14: Protocol configuration register

8.3.9.1 Disable multi-tag reset (default 0)

If set, the reader does not reset before the multi-tag list and multi-select command have been performed.

8.3.9.2 Disable start-up message (default 0)

If set, the reader suppresses the start-up message in ASCII mode. This flag is ignored in binary protocol mode.

8.3.9.3 Enable binary frame v2 (default 0)

If set, the reader sends version 2 binary frames.

The get station ID command always sends version 1 binary frames!

8.3.9.4 Noisy Environment (default 0)

If set, the continuous read mode can only be aborted with the '.' character. When working in a noisy environment, the probability for a reception of an arbitrary/stochastic sign/command is quite high. This implies a high probability of an unintentional command execution. To reduce this probability, only one character (out of 255) is chosen (‘.’) to be interpreted as the continuous read stop command.

8.3.9.5 Reset Recovery Time Multiplier (default 0)

Multiplies the Reset Recovery Time, including the recovery time of the field reset command.

Reset Recovery Time Multiplier	Reset Recovery Time
0	1x
1	2x
2	3x
3	4x

Figure 8-15: Reset Recovery Time Multiplier

8.3.9.6 Enable ISO14443 B Anti-collision (default 0)

If set, the anti-collision algorithm for ISO 14443 B tags is enabled.

8.3.9.7 Disable ISO 14443-4 Error Handling (default 0)

If set, ISO14443-4 Error Handling is disabled. The error handling always uses the TMR time-out.

8.3.10 Reset Off Time (14h)

The Reset Off Time register represents the field off time in ms.

This register is used for the select, continuous read and multi-tag commands.

Default value is 0Ah.

8.3.11 Reset Recovery Time (15h)

The Reset Recovery Time register represents the recovery time in ms after the field is turned on.

This register is used for the select, continuous read and multi-tag commands.

Default value is 25h.

8.3.12 Application Family Identifier (16h)

The AFI (Application Family Identifier) is only supported for ISO14443B tags. If the set value is different from 00h, the AFI is implemented in the ReqB command of ISO14443B. Only transponders with an identical AFI will answer to the reader.

Default value is 00h.

8.3.13 Selection Time-out ISO 14443A (17h)

The Selection Time-out represents the reader card communication time-out for the select, high speed select, continuous read, multilist, multiselect and mifare® login command with ISO 14443A tags. For a better reaction time use low values. One time slice is around 300us.

The default value is 10h.

8.3.14 Selection Time-out ISO 14443B (18h)

The Selection Time-out represents the reader card communication time-out for the select, high speed select, continuous read, multilist and multiselect commands with ISO 14443B tags. For a better reaction time, use low values. One time slice is around 300µs.

The default value is 50h.

8.3.15 Selection Time-out SR176 (19h)

The Selection Time-out represents the reader card communication time-out for the select, continuous read, multilist and multiselect command with SR176 tags. For a better reaction time, use low values. One time slice is around 300µs.

The default value is 10h.

8.3.16 Protocol configuration 3 (1Bh)

The protocol configuration register 3 (PCON3) further specifies the general behavior of the reader device.

Default value is 00h.

Protocol configuration 3 register							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
RFU	ReqA Extended ID	Internal use / do not change			Page Read	RFU	Disable automatic ISO 14443-4 timeouts

Figure 8-16: Protocol configuration register

8.3.16.1 Disable automatic ISO 14443-4 timeouts (default 0)

If set the automatic ISO 14443-4 timeouts are disabled. The timeouts specified with TMR registers are used.

8.3.16.2 Page read (default 0)

If set the continuous read mode retrieves the content of the tag instead of the serial number. The register Page Start (1Ch) defines the start block and the Page Number (1Fh) defines the number of blocks to be read.

8.3.16.3 ReqA Extended ID (default 0)

If set the Extended ID information for ISO14443 A tags replaces the cascade level information (1 byte) with Request A answer (2 bytes).

8.3.17 User data (80h - EFh)

These registers are for free use.

8.4 Instruction Set

Following table describes all the commands of the reader device. Each command returns an answer to the host. Exceptions are mentioned explicitly. The RFID activity indicator LED acknowledges a successfully executed command. The RFID activity indicator LED indicates an error by changing its color to red.

8.4.1 Overview

Common commands	
'!'	Test continuous read
'c'	Continuous read
'.'	Abort continuous read, refer to continuous read
'dg' / 'dn' / 'dr'	Set LED
'ds'	DES encryption / decryption of data
'f'	DESFire command set
'g'	Get ID
'h'	High speed select
'm'	MultiTag select / tag list
'o+a' / 'o+b' / 'o+s'	Include tag type
'o-a' / 'o-b' / 'o-s'	Exclude tag type
'oa' / 'ob' / 'ot' / 'os'	Set tag type
'of'	Set configuration flags
'og'	Set configuration register
'poff' / 'pon'	Antenna power off/on
'pr' / 'pw'	Read / write user port
'q'	Quiet
'rp'	Read EEPROM register
'r' / 'rb'	Read block
's'	Select
'v'	Get version
'w' / 'wb'	Write block
'wf'	Write DESFire key
'wm'	Write master key
'wp'	Write EEPROM register
'x'	Reset

Figure 8-17: Command overview (Part 1)

Common commands (Part2)	
'y'	Field reset
ISO 14443 Type A only commands	
'+'	Increment value block (credit)
'-'	Decrement value block (debit)
'='	Copy value block (backup)
'l'	Login (authenticate tag)
'rv'	Read value block
'wv'	Write value block
SR176 only commands	
'k'	Lock block

Figure 8-18: Command overview (Part 2)

DESFire command set	
00h	Authenticate
01h	Change Key Settings
02h	Get Key Settings
03h	Change Key
04h	Get Key Version
05h	Create Application
06h	Delete Application
07h	Get Application IDs
08h	Select Application
09h	Format PICC
0Ah	Get Version
0Bh	Get File IDs
0Ch	Get File Settings
0Dh	Select File
0Eh	Change File Settings
0Fh	Create Standard Data File
10h	Create Backup Data File
11h	Create Value File
12h	Create Linear Record File
13h	Create Cyclic Record File
14h	Delete File
15h	Read Data / Records
16h	Write Data / Record
17h	Get Value
18h	Credit
19h	Debit
1Ah	Limited Credit
1Bh	Clear Record File
1Ch	Commit Transaction
1Dh	Abort Transaction

Figure 8-19: Command overview (Part 3)

8.4.2 Error Codes

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

Error Code	Description
‘?’	Unknown command
'C'	Collision or CRC/MAC 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
‘R’	Command parameter out of range
'X'	Authentication failed
Xxh	DESFire error code

Figure 8-20: Error codes

8.4.3 Common commands

8.4.3.1 Test Continuous Read

This command tests the state of the continuous read command.

This command only works in ASCII mode.

Command

Command	Data
'!'	None

Answer

Answer	Description
'F'	Continuous read mode is not active.
'!'	Continuous read mode is active.

8.4.3.2 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 module returns the character ‘S’ (53h).

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 type should be detected at the same time, the Multitag flag must be activated. The response data length depends on the tag type.

Command

Command	Data
'c'	none

Answer

Answer	Description
data	Serial number (n bytes)
'N'	Error: No Tag in the field (only binary protocol)

8.4.3.2.1 Multitag continuous read mode

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

8.4.3.2.2 Auto start

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

8.4.3.2.3 Noisy Environment

If the Noisy Environment flag is set, the continuous read mode can only be aborted with the '.' character.

8.4.3.2.4 Binary mode

This command is not fully supported in binary protocol mode.

Continuous Read in binary mode does not start-up automatically at boot time, even if the corresponding EEPROM flag is set.

Within the single shot time-out, only one response is sent.

8.4.3.2.5 Simple access control applications

Serial numbers are always sent plain. Data encryption is activated after a successful login.

For simple access control applications the use read-only blocks for the identification of the tag is recommended.

Reading any block (even the manufacturer block) of the transponder will increase your security.

8.4.3.3 Set LED

This command controls the LED activity. If the LED flag is set, the automatic LED function is switched off. The user can set the state of the LED manually.

Command

Command	Data
'dg'	None
'dr'	None
'dn'	None

Answer

Answer	Description
'DG' 'DR' 'DN'	String of LED state

Example

Command	Answer	Description
'dg'	DG	Switch on LED green, LED red off
'dr'	DR	Switch on LED red, LED green off
'dn'	DN	Switch off both LEDs

8.4.3.4 DES encryption / decryption of data

This command returns 8 bytes of encrypted / decrypted data.

Command

Command	Data
'ds'	Options (1 byte) Key (8/16 bytes) / Key Number (1 byte) Data (8 byte)

Answer

Answer	Description
Data	Encrypted / Decrypted data (8 bytes)

Option byte

Option byte							
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
RFU	RFU	RFU	RFU	RFU	Encode	Key Length	Key Index

Key Index

If set, the command only needs the key number (1 byte) instead of the key (8/16 bytes).

The key number corresponds to the key number used in the "wf" command

Key Length

If set, the command uses the TDES algorithm with 16-byte key.

If cleared, the command uses the DES algorithm with 8-byte key.

Encode

Setting this flag encodes the data.

Clearing this flag decodes the data.

8.4.3.5 Get ID

This command returns the station ID of the reader device. The answer is time slotted to enable the detection of all devices in party line mode.

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)

8.4.3.5.1 Binary Protocol Version 2

This command never sends version 2 binary frames.

8.4.3.5.2 High speed select

This command selects a card in the antenna field (according to the selection criteria) or prepares a multiselect command, switches to high baud rates and enables 256-byte frames. If execution is successful, the command returns the UID of the selected card and the used baud rate. The reader automatically detects the maximum frame size of the card. The reader also tries to communicate to the transponder with the specified baud rate. If no communication is possible, the reader will automatically decrease the speed to the next lower value.

This command can also force the reader to the communication speed and frame size of the tag to the specified values. This is only needed if the high speed select is done manually with the transfer command.

Command

Command	Data
'h'	option byte (1 byte) 00h … select a single card with 106kBaud 02h … select a single card with 212kBaud 04h … select a single card with 424kBaud 08h … select a single card with 848kBaud 10h … prepare next multiselect for 106kbaud 12h … prepare next multiselect for 212kbaud 14h … prepare next multiselect for 424kbaud 18h … prepare next multiselect for 848kbaud 20h … forces reader to 106kBaud 22h … forces reader to 212kBaud 24h … forces reader to 424kBaud 28h … forces reader to 848kBaud 30h – 38h … force tag frame size

Answer

Answer	Description
Data (n bytes) + frame size and baud rate (1byte)	serial number + frame size used and baud rate
'F'	Error: General failure
‘N’	Error: No Tag in the field

Example

Command	Description
h08	1234567890ABCD84 Select the card with UID 1234567890SABCD. The card supports a 256-byte frame size and 424kBaud on the air interface.

8.4.3.5.3 Answer from 0xh and 1xh

The lower nibble contains the baud rate used for the air interface.

Baud Rate	Description
x0	106kBaud
x2	212kBaud
x4	424kBaud
x8	848kBaud

Figure 8-21: Baud Rate values

The higher nibble contains the frame size used for the air interface.

Frame Size	Description
0x	16 Bytes
1x	24 Bytes
2x	32 Bytes
3x	40 Bytes
4x	48 Bytes
5x	64 Bytes
6x	96 Bytes
7x	128 Bytes
8x	256 Bytes

Figure 8-22: Frame Size

8.4.3.5.4 Answer from 2xh and 3xh

The option byte is returned as the answer.

8.4.3.5.5 Select a single tag

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

8.4.3.5.6 Extended ID

See above for more information on Extended ID.

The RATS answer is inserted between the serial number and baud rate / frame size byte for ISO14443 A tags.

8.4.3.5.7 Multiple tags

This command with parameter 1xh prepares the next multiselect command as a high-speed select. Any other command will disable the preparation.

8.4.3.5.8 RATS Guard Time SFGT

A high-speed select with parameters 0xh and 1xh automatically waits the SFGT guard time gotten from the tag before sending the PPS command.

8.4.3.6 Multi-Tag Selection / List

This command detects several 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 their 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 (n bytes) <CR> (1 byte)

Answer

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

Example

Command	Description
m<CR>	04E9E700000000 → first card 34030F07 → second card 02 → number of detected tags
m04E9E700000000<CR>	Select card with its serial number

8.4.3.6.1 Multi-tag list

Sending a <CR> as the first parameter, the reader returns a list of all tags present in the antenna field. In the end the total number of tags detected is returned.

8.4.3.6.2 Reading distance

Each card needs a specific amount of power. The reader always provides the same amount of power. Therefore, the reading distance will decrease if more tags are present. Basically, the reading distance depends on the tag, the antenna and the tuning of the antenna.

8.4.3.6.3 Multi-tag select

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

8.4.3.6.4 Multi-tag reset

The antenna field reset can be deactivated with the Protocol configuration 2 register.

By suppressing the antenna field reset, it is possible to detect only new tags in the antenna field.

8.4.3.6.5 Maximum number of tags

The maximum number of tags in the antenna field is limited to 30 and by the physical characteristics of the antenna.

8.4.3.7 Include tag type

This command includes a specific tag type to those addressed by the reader device.

Command

Command	Data
‘o+’	tag type (1 byte)

Answer

Answer	Description
'O+' + tag type (1 byte)	Command code + String of tag type

Tag type character

Refer to Set tag type.

Example

Command	Description
o+a	Include ISO14443-A to the tag types addressed by the reader device.

8.4.3.8 Exclude tag type

This command excludes a specific tag type from being addressed by the reader device.

Command

Command	Data
‘o-’	Tag type (1 byte)

Answer

Answer	Description
'O-' + tag type (1 byte)	Command code + String of tag type

Tag type character

Refer to Set tag type.

Example

Command	Description
o-a	Exclude ISO14443-A from the tag types addressed by the reader device.

8.4.3.9 Set tag type

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

Command

Command	Data
'o'	ISO type (1 byte) 'a' … ISO 14443 Type A 'b' … ISO 14443 Type B 's' … SR176 't' … activate all tags

Answer

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

Example

Command	Description
oa	Sets the reader device to address ISO14443-A type tags.

8.4.3.10 Set Configuration Flags

This command allows setting some configuration flags just in time; no reset is needed. The values are not stored in the EEPROM, therefore the changed values are not available after a reset.

Command

Command	Data
of	flag type (1 byte) data (1 byte)

Answer

Answer	Description
Data (1 byte)	Current state of changed flag.
'R'	Error: Out of range

Example

Command	Description
of0101	Answer: 01 Enables the New Serial Mode flag.

Flag Types

The following table shows the Flag Type with its corresponding flag from the specified Protocol Configuration Register.

Flag Type	Corresponding Flag	Protocol Configuration Register	Valid values
00h	Multitag	1	00 / 01
01h	New Serial Mode	1	00 / 01
02h	LED	1	00 / 01
03h	Single Shot	1	00 / 01
04h	Extended Protocol	1	00 / 01
05h	Extended ID	1	00 / 01
06h	Disable Multitag Reset	2	00 / 01
07h	Noisy Environment	2	00 / 01
08h	Reset Recovery Time Multiplier	2	00 … 03
09h	Enable ISO14443 B Anti-collision	2	00 / 01
0Ah	Disable ISO14443-4 Error Handling	2	00 / 01
0Bh	Disable automatic ISO14443-4 timeouts	3	00 / 01
0Dh	Page Read	3	00 / 01
11h	ReqA Extended ID	3	00 / 01

Figure 8-23: Flag Type with corresponding flag

8.4.3.10.1 Out of range failure 'R'

The entered flag type is out of range.

8.4.3.11 Set Configuration Register

This command allows setting some configuration registers just in time; no reset is needed. The values are not stored in the EEPROM; therefore the changed values are not available after a reset.

Command

Command	Data
og	Register type (1 byte) data (1 byte)

Answer

Answer	Description
Data (1 byte)	Current state of changed register.
'R'	Error: Out of range

Example

Command	Description
og0450	Answer: 50 Sets the Reset Recovery Time to 50h.

Register Types

The following table shows the Register Type with its corresponding register.

Register Type	Corresponding Register
00h	Single shot time-out value
01h	Internal use / Do not change
02h	Internal use / Do not change
03h	Reset Off Time
04h	Reset Recovery Time
05h	ISO 14443A Selection Time-out
06h	ISO 14443B Selection Time-out
07h	SR176 Selection Time-out
08h	AFI
0Ch	Page Read Start
0Dh	Page Read Number
0Eh	Command Guard Time

Figure 8-24: Register Type with corresponding register

8.4.3.11.1 Out of range failure 'R'

The entered register type is out of range.

8.4.3.12 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 reader on
'poff'	Put reader in standby mode

Answer

Answer	Description
'P'	Positive acknowledge

Example

Command	Description
poff	Put reader in standby mode

8.4.3.12.1 Power off

The reader enters standby mode. Power consumption is decreased. All tags in the antenna field are powered off and reset. Standby mode is only entered manually.

To switch off the whole unit, pin 16 (Enable) has to be set to logic low.

8.4.3.12.2 Power on

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

8.4.3.13 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)
'C'	Error: Error correction fails
'F'	Error: Transmission Error / No answer received

Example

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

8.4.3.13.1 Read port

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

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

Figure 8-25: Read USER port return values

8.4.3.13.2 Write port

If user port is used as an output, a 1kΩ resistor has to be integrated into the wire. Otherwise the reader device can be damaged.

Port state	Description
00h	Sets USER port to low
01h	Sets USER port to high
02h – 7Fh	RFU
80h - FFh	Sends a serial data frame and checks the received frame

Figure 8-26: Write User port settings

Sending a Data Frame

If the highest bit (MSB) is set in the State of the User Port, the command sends a serial data frame out the USER port.

The frame includes a start bit, 8 data bits, parity bit and a stop bit.

Transmit Frame	Description
Low	Start bit
Low	RFU
Data Bit 6	State of the User Port Bit 6
Data Bit 5	State of the User Port Bit 5
Data Bit 4	State of the User Port Bit 4
Data Bit 3	State of the User Port Bit 3
Data Bit 2	State of the User Port Bit 2
Data Bit 1	State of the User Port Bit 1
Data Bit 0	State of the User Port Bit 0
Parity Bit	Even Parity Bit
High	Stop Bit

Figure 8-27: Sending Serial Data Frame

After 2ms Guard Time the answer should be received on the User Port otherwise an error is returned.

Receive Frame	Description
Low	Start bit
Error Bit	If set, an error was detected.
Data Bit 6	State of the User Port Bit 6
Data Bit 5	State of the User Port Bit 5
Data Bit 4	State of the User Port Bit 4
Data Bit 3	State of the User Port Bit 3
Data Bit 2	State of the User Port Bit 2
Data Bit 1	State of the User Port Bit 1
Data Bit 0	State of the User Port Bit 0
Parity Bit	Even Parity Bit
High	Stop Bit

Figure 8-28: Receiving Serial Data Frame

If the Error bit is set or the Parity Bit is not correct, the Write User Port command returns an error code.

8.4.3.14 Quiet

This command sets a selected tag into halt state.

Command

Command	Data
'q'	none

Answer

Answer	Description
'Q'	Halt state successfully set.
'N'	Error: No Tag in the field

8.4.3.14.1 ISO 14443 Type A

With ISO14443 Type A tags, the Quiet command always answers with 'Q' because the halt command does not send any acknowledge.

8.4.3.14.2 ISO 14443 Type B

Some ISO14443 Type B tags do not support this command or do not respond. ‘Quiet’ is an ISO 14443-4 command, so it will work only if the ‘Deselect’ command is supported by the corresponding transponder.

8.4.3.14.3 SR176

With SR176 tags the Quiet command always answer with 'Q' because the completion command does not send any acknowledge.

8.4.3.15 Read block

This command reads a data block on a card. The size of the returned data depends on the tag used. The block address range depends on the tag as well.

Command

Command	Data
'r'	Block address (1 byte), valid range 00h – 40h
'rb'	Block address (1 byte)

Answer

Answer	Description
Data	data block (depends on tag type)
'F'	Error: read failure
'N'	Error: No tag in field
'O'	Error: Operation mode failure
'R'	Error: Out of range

Example

Command	Description
rb05	Reads block 05.

8.4.3.15.1 Read failure 'F'

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

8.4.3.15.2 No tag in field 'N'

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

8.4.3.15.3 Operation mode failure 'O'

The presented tag is not ISO14443 type A compliant.

8.4.3.15.4 Out of range failure 'R'

The block address of the 'r' command is higher than 40h.

The block address of the 'r' command conflicts with other commands, therefore the block address has to be limited to 40h.

Use the 'rb' command instead.

8.4.3.16 Read reader EEPROM

This command reads the internal reader EEPROM. It contains all start-up parameters and the device ID. Changes in the start-up settings will only go into effect after a reset of the device.

Command

Command	Data
'rp'	EEPROM address (1 byte) 00h … EFh

Answer

Answer	Description
Data	EEPROM data (1 byte)
'R'	Error: Out of range failure

Example

Command	Description
rp0B	Reads protocol configuration register.

8.4.3.16.1 Out of range failure 'R'

The entered EEPROM address is not valid.

8.4.3.17 Select

This command selects a single card in the antenna field. It can only be used in single tag mode. If successfully executed, the command returns the UID of the selected card. The reader detects the length of the UID 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 UID 1234567890SABCD.

8.4.3.17.1 Select a single tag

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

8.4.3.17.2 Extended ID

See above for more information on Extended ID.

8.4.3.17.3 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.

8.4.3.18 Get Version

This command returns the current version of the reader module.

Command

Command	Data
'v'	None

Answer

Answer	Description
'Dual 2.2' + <CR> + <LF>	ASCII Mode
02 00 08 44 75 61 6C 20 32 2E 32 32 03	Binary Mode

Example

Command	Description
v	‘Dual 2.2’ Version of the reader module

8.4.3.19 Write DESFire key

This command is used to store a key into the DESFire key memory of the reader. The reader can store up to 32 keys. DESFire keys can be used for fast access to applications on a card.

Command

Command	Data
'wf'	Key number (1 byte) 00h … 1Fh Key (16 bytes)

Answer

Answer	Description
data	Written key (16 bytes)
'F'	Error: Write failure
'R'	Error: Out of range

Example

Command	Description
wf0000112233445566778899AABBCCDDEEFF	Store key 00112233445566778899AABBCCDDEEFFh in EEPROM (key number 0).

8.4.3.19.1 Out of range failure 'R'

The entered key number exceeds the permitted range.

8.4.3.19.2 Writing DESFire Keys

Keys are write only. It is not possible to read the keys. Nevertheless the reader returns correct error messages if the writing process fails.

A verification of the DESFire key can only be done using an appropriate card and following successful login.

8.4.3.19.3 Using DESFire keys for authentication

DESFire keys may be used for DESFire tag authentication or DES/TDES encryption/decryption.

Each key is 16 bytes long and stored redundantly for data security.

8.4.3.20 Write master key

This command stores a mifare® Standard key into the master key memory of the reader. The reader can store up to 32 keys.

Command

Command	Data
'wm'	Key number (1 byte) 00h … 1Fh Key (6 bytes)

Answer

Answer	Description
data	Written key (6 bytes)
'F'	Error: Write failure
'R'	Error: Out of range

Example

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

8.4.3.20.1 Out of range failure 'R'

The entered key index exceeds the address range.

8.4.3.20.2 Writing master keys

Keys are Write-Only. It is not possible to read the keys. 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 following successful login.

8.4.3.20.3 Using master keys for authentication

Master keys may be used for ISO-14443 A tag authentication. It is possible to use every stored key for key A as well as key B authentication.

Each key is 6 bytes long and stored redundantly for data security.

8.4.3.21 Write block

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

Command

Command	Data
'w'	Block address (1 byte), valid range 00h – 40h Data (n bytes)
'wb'	Block address (1 byte) Data (n bytes)

Answer

Answer	Description
Data	Data block (depends on tag type)
'F'	Error: Write failure
'N'	Error: No tag in field
'O'	Error: Operation mode failure
'R'	Error: Out of range

Example

Command	Description
wb0511223344	Writes data 11223344 on block 05.

8.4.3.21.1 Write failure 'F'

This error is displayed if bad transmission conditions are given. If the block address exceeds the physical number of blocks of a tag, this error is shown.

8.4.3.21.2 No tag error 'N'

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

8.4.3.21.3 Operation mode failure 'O'

The tag is not ISO14443 type A compliant.

8.4.3.21.4 Out of range failure 'R'

The block address of the 'w' command is higher than 40h.

The block address of the 'w' command conflicts with other commands, therefore the block address has to be limited to 40h.

Use the 'wb' command instead.

8.4.3.22 Write EEPROM

Writes to the internal reader EEPROM. It contains all start-up parameters and the device ID. Changes to the start-up settings will only go into effect after a reset of the device.

Command

Command	Data
'wp'	Address (1 byte), valid range 0Ah - EFh Data (1 byte)

Answer

Answer	Description
Data	EEPROM data (1 byte)
'F'	Error: Read after write failure
'R'	Error: Out of range failure

Example

Command	Description
wp0A01	Set EEPROM address 0A (Station ID) to 01h

8.4.3.22.1 Out of range failure 'R'

The entered address exceeds the address range.

8.4.3.23 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
'Dual 2.2' + <CR> + <LF>	ASCII Mode
None	Binary Mode

8.4.3.23.1 Disable Start-up Message

If the start-up message is disabled in the protocol configuration register 2, the ASCII mode does not respond with the version of the reader.

8.4.3.23.2 Reset Timing

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

8.4.3.24 Field Reset

The field reset switches off the antenna field for the specified duration. All tags need a certain amount of time to initialize before a command can be processed. The second byte specifies the field recovery time.

Command

Command	Data
'y'	Off time in milliseconds (1 byte) Field recovery time in milliseconds (1 byte)

Answer

Answer	Description
'Y'	After the field reset the reader sends back a ‘Y’ to acknowledge the command.

8.4.4 ISO 14443 Type A only commands

8.4.4.1 Increment value block (credit)

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

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

8.4.4.1.1 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.

8.4.4.1.2 Increment failure 'F'

The Increment failure indicates a general failure during the increment procedure or inability to read after the write process.

8.4.4.1.3 No tag error 'N'

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

8.4.4.1.4 Operation mode failure 'O'

The tag is not ISO14443 type A compliant.

8.4.4.2 Decrement value block (debit)

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

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

8.4.4.2.1 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.

8.4.4.2.2 Decrement failure 'F'

The Decrement failure indicates a general failure during the decrement procedure or inability to read after the write process.

8.4.4.2.3 No tag error 'N'

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

8.4.4.2.4 Operation mode failure 'O'

The tag is not ISO14443 type A compliant.

8.4.4.3 Copy value block (backup)

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

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

8.4.4.3.1 Target block

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

8.4.4.3.2 No value block 'I'

Source value block is not in a valid value block. The value block is corrupted. A backup block can be used to restore the correct value.

8.4.4.3.3 Copy failure 'F'

The Copy failure indicates a general failure during the copy procedure or inability to read after the write process.

8.4.4.3.4 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 to the request.

8.4.4.3.5 Operation mode failure 'O'

The tag is not ISO14443 type A compliant.

8.4.4.4 Login (authenticate tag)

Performs an authentication in order to access one sector of a mifare® card. Only one sector can be accessed at a time.

Optionally, the command can be used to transmit the key data to the reader-stored keys, in the reader EEPROM.

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), valid range 00h - 3Fh 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) / <CR> (1 byte), optional By transmitting <CR> instead of the keydata authentication is done with manufacturer's 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)
l0FAAFFFFFFFFFFF	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

8.4.4.4.1 No tag error 'N'

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

8.4.4.4.2 Operation mode failure 'O'

The tag is not ISO14443 type A compliant.

8.4.4.4.3 Out of range failure 'R'

The entered key type or the sector is out of range.

8.4.4.4.4 <CR>

Three transport keys are implemented to access cards quickly.

By transmitting <CR> instead of the key, the reader module uses the transport keys for the login procedure.

Command	Description
LxxAA<CR>	Authenticate for sector xx, using the transport key 1 (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)

8.4.4.4.5 Login with key data from EEPROM

Each key stored in the reader EEPROM can be used as type A or type B key. 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.

8.4.4.4.6 Usage of key A, key B

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

8.4.4.5 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.

8.4.4.5.1 No value block 'I'

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

8.4.4.5.2 No tag error 'N'

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

8.4.4.5.3 General failure 'F'

In addition to the case of a data read failure caused by bad transmission conditions, this error is returned if a sector is addressed which is not located in the authenticated area.

8.4.4.5.4 Operation mode failure 'O'

The tag is not ISO14443 type A compliant.

8.4.4.6 Write value block

This command formats a block as a value block containing a 32-bit value. A read is performed automatically after the write. 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.

8.4.4.6.1 Invalid value 'I'

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

8.4.4.6.2 Write failure 'F'

In addition to the case of a data read failure caused by bad transmission conditions, this error is returned if a sector is addressed which is not located in the authenticated area.

8.4.4.6.3 No tag error 'N'

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

8.4.4.6.4 Operation mode failure 'O'

The tag is not ISO14443 type A compliant.

8.4.4.6.5 Writing values

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

8.4.5 SR176 only commands

8.4.5.1 Lock block

This command locks a block permanently.

Command

Command	Data
'k'	Block address (1 byte)

Answer

Answer	Description
data	'K' + page address
'F'	Error: Lock failure
'N'	Error: No tag in field
'O'	Error: Operation mode failure (only SR176 tags supported)
'X'	Error: Block already locked

Example

Command	Description
k05	K05 Lock block 05.

8.4.5.1.1 Operation mode failure 'O'

The presented tag is not a SR176 tag.

8.4.5.1.2 Apply settings

After locking a block permanently, the tag needs to be selected for the settings to apply.

8.4.6 DESFire command set

This command set provides easy communication with DESFire tags. The reader handles all encryption and decryption automatically. The length byte includes all data and command bytes.

For more information about DESFire, refer to DESFire documentation [2].

The DESFire command set is only available for ISO 14443 Type A tags; with other tags, the Error Code 'O' is returned.

A DESFire command has the following syntax:

Command	**Data**
'f'	Length byte (1 byte) DESFire Command Code (1 byte) Data (n bytes)

Example

Command	**Description**
f0107	Get Application IDs.
f020D00	Select File 00h.

All the following DESFire commands are listed without length byte.

8.4.6.1 Authenticate

Authenticates to a DESFire card. Authentication depends on access conditions of an application or file. ROM keys can be used to login. The reader can store up to 32 keys internally.

Command

Command	Data
00h	Key number on tag (1 byte) Key number (1 byte) / Key on reader (16 bytes)

Answer

Answer	Description
Data	Authentication status (1 byte)
'L'	Login success
'F'	Error: General failure
'N'	Error: No tag in field
'X'	Error: Authentication failed
Xxh	DESFire status / error code, refer to DESFire documentation

Example

Command	Description
f03000000	Authenticate using key 00h of the tag and key 00h stored in reader ROM.
f12020011223344556677 8899AABBCCDDEEFF	Authenticate using key 02h of the tag and key 00112233445566778899AABBCCDDEEFFh.

8.4.6.2 Change Key Settings

This command changes the key settings of a selected application.

Command

Command	Data
01h	Settings (1 byte)

Answer

Answer	Description
data	Status code (1 byte)
00h	Success
'N'	Error: No tag in field
Xxh	DESFire status / error code, refer DESFire documentation

Example

Command	Description
f0201FF	Answer: 00 change key settings to FFh.

8.4.6.3 Get Key Settings

This command gets the key settings of a selected application. Settings of the currently selected application are returned. Additionally the maximum number of keys that can be stored in the application is displayed.

Command

Command	Data
02h	none

Answer

Answer	Description
00h + Key settings (1 byte) + max. number of keys (1 byte)	Key settings
'N'	Error: No tag in field
Xxh	DESFire status / error code, refer DESFire documentation

Example

Command	Description
f0102	Answer: 000F01 Key settings of the application are 0F and key number 01 is used.

8.4.6.4 Change Key

This command changes the key of a selected application.

Command

Command	Data
03h	Key number on tag (1 byte) New key (16 bytes) Old key (16 bytes)

Answer

Answer	Description
Data	Status code (1 byte)
00h	Success
'F'	Error: General failure
'N'	Error: No tag in field
Xxh	DESFire status / error code, refer to DESFire documentation

Example

Command	Description
f22030000112233445566778899AABBCCDDEEFF00000000000000000000000000000000	Answer: 00 Key 00h is changed to 00112233445566778899AABBCCDDEEFFh.

8.4.6.5 Get Key Version

This command reads the key version of a key of a selected application.

Command

Command	Data
04h	Key number on tag (1 byte)

Answer

Answer	Description
00h + Key version (1 byte)	Key version
'N'	Error: No tag in field
Xxh	DESFire status / error code, refer to DESFire documentation

Example

Command	Description
f020400	Answer: 0000 Key version 00h.

8.4.6.6 Create Application

This command creates an application on a tag. Applications can only be created in the master application (000000h).

Command

Command	Data
05h	Application ID (3 bytes) Key settings (1 byte) Number of keys (1 byte)

Answer

Answer	Description
Data	Status code (1 byte)
00h	Success
'N'	Error: No tag in field
Xxh	DESFire status / error code, refer to DESFire documentation

Example

Command	Description
f06050000100F01	Answer: 00 Create application 000010h with one key.

8.4.6.7 Delete Application

This command deletes an application on a tag.

Command

Command	Data
06h	Application ID (3 bytes)

Answer

Answer	Description
Data	Status code (1 byte)
00h	Success
'N'	Error: No tag in field
Xxh	DESFire status / error code, refer to DESFire documentation

Example

Command	Description
f0406000010	Answer: 00 Delete application 000010h.

8.4.6.8 Get Application IDs

This command returns all application IDs on a tag.

Command

Command	Data
07h	None

Answer

Answer	Description
00h + Application IDs (3 bytes each)	Application IDs
'N'	Error: No tag in field
Xxh	DESFire status / error code, refer to DESFire documentation

Example

Command	Description
f0107	Answer: 00000010 Application 000010h is available on the tag

8.4.6.9 Select Application

This command selects a specific application. An application must be selected to access all files stored in it.

Command

Command	Data
08h	Application ID (3 bytes)

Answer

Answer	Description
Data	Status code (1 byte)
00h	Success
'N'	Error: No tag in field
Xxh	DESFire status / error code, refer to DESFire documentation

Example

Command	Description
f0408000010	Answer: 00 Application 000010h is selected.

8.4.6.10 Format PICC

This command formats the tag. All applications are deleted. The format command requires successful authentication.

Command

Command	Data
09h	None

Answer

Answer	Description
Data	Status code (1 byte)
00h	Success
'N'	Error: No tag in field
Xxh	DESFire status / error code, refer to DESFire documentation

Example

Command	Description
f0109	Answer: 00 The tag is formatted successfully. All applications and files have been deleted.

8.4.6.11 Get Version

This command returns the production data of a tag.

Command

Command	Data
0Ah	none

Answer

Answer	Description
Data	Version (28 bytes) For more detailed information refer to DESFire documentation.
'F'	Error: General failure
'N'	Error: No tag in field
Xxh	DESFire status / error code, refer to DESFire documentation.

Example

Command	Description
f010A	Answer: 04010100021805040101000418050445310136 6E108E26515D502003 Version string of DESFire tag.

8.4.6.12 Get File IDs

This command returns all file IDs found for a selected application.

Command

Command	Data
0Bh	none

Answer

Answer	Description
00h + File IDs (1 byte each)	File IDs
'N'	Error: No tag in field
Xxh	DESFire status / error code, refer to DESFire documentation

Example

Command	Description
f010B	Answer: 000005 File with ID 00h and 05h exists.

8.4.6.13 Get File Settings

This command returns additional information of a file.

Command

Command	Data
0Ch	File number (1 byte)

Answer

Answer	Description
00h + File settings (n bytes)	File settings Length depends on file type. For more detailed information refer to DESFire documentation.
'F'	Error: General failure
'N'	Error: No tag in field
xxh	DESFire status / error code, refer to DESFire documentation

Example

Command	Description
f020C00	Answer: 000000EEEE100000 File 00h is a standard data file with access conditions EEEEh and data length 100000h.

8.4.6.14 Select File

This command selects a specific file.

Command

Command	Data
0Dh	File number (1 byte)

Answer

Answer	Description
Data	Status code (1 byte)
00h	Standard Data File selected
01h	Backup Data File selected
02h	Value File selected
03h	Linear Record File selected
04h	Cyclic Record File selected
'N'	Error: No tag in field
Xxh	DESFire status / error code, refer DESFire documentation

Example

Command	Description
f020D00	Answer: 00 File 00h has been successfully selected.

8.4.6.15 Change File Settings

This command changes the access rights of a selected file.

Command

Command	Data
0Eh	Communication settings (1 byte) Access rights (2 bytes)

Answer

Answer	Description
Data	Status code (1 byte)
00h	Standard Data File selected
'N'	Error: No tag in field
'O'	Error: No file selected
Xxh	DESFire status / error code, refer to DESFire documentation

Example

Command	Description
f040E010000	Answer: 00 Sets file to MAC secured with key 0000h.

Note

For further information on communication settings and access rights, refer to the DESFire documentation. [2]

8.4.6.16 Create Standard Data File

This command creates a Standard Data File in a selected application.

Command

Command	Data
0Fh	File number (1 byte) Communication settings (1 byte) Access rights (2 bytes) File size (3 bytes)

Answer

Answer	Description
Data	Status code (1 byte)
00h	Standard Data File created
'N'	Error: No tag in field
Xxh	DESFire status / error code, refer to DESFire documentation

Example

Command	Description
f080F0000EEEE100000	Answer: 00 Create standard data file with ID 00h.

Note

For further information on communication settings and access rights, refer to the DESFire documentation.

8.4.6.17 Create Backup Data File

This command creates a Backup Data File in a selected application. Backup data files use a shadow register for data manipulation operations. The file number must be in the range from 00h to 07h.

Command

Command	Data
10h	File number (1 byte) Communication settings (1 byte) Access rights (2 bytes) File Size (3 bytes)

Answer

Answer	Description
Data	Status code (1 byte)
00h	Backup Data File created
'N'	Error: No tag in field
Xxh	DESFire status / error code, refer to DESFire documentation

Example

Command	Description
f081001000000100000	Answer: 00 Create backup data file with ID 01h. File is only accessible after login with key 00h

Note

For further information on communication settings and access rights, refer to the DESFire documentation.

8.4.6.18 Create Value File

This command creates a Value File in a selected application. Value blocks are signed long numbers, which are stored in Intel format (LSB first). Value files use a shadow register for data manipulation operations. The file number must be in the range from 00h to 07h.

Command

Command	Data
11h	File number (1 byte) Communication settings (1 byte) Access rights (2 bytes) Low Limit (4 bytes) High Limit (4 bytes) Value (4 bytes) Enable Limited Credit (1 byte)

Answer

Answer	Description
Data	Status code (1 byte)
00h	Value File created
'N'	Error: No tag in field
Xxh	DESFire status / error code, refer to DESFire documentation

Example

Command	Description
f12110503000000000000 666666663333333300	Answer: 00 Value file with ID 05h created. Transmission is secured using DES encryption with key 00h. Lower limit is 00000000h and high limit 66666666h. Default value is 33333333h.

Note

For further information on communication settings and access rights, refer to the DESFire documentation.

8.4.6.19 Create Linear Record File

This command creates a Linear Record File in a selected application. Linear record files use a shadow register for data manipulation operations. The file number must be in the range from 00h to 07h.

Command

Command	Data
12h	File number (1 byte) Communication settings (1 byte) Access rights (2 bytes) Record Size (3 bytes) Number of Records (3 bytes)

Answer

Answer	Description
Data	Status code (1 byte)
00h	Linear Record File created.
'N'	Error: No tag in field
Xxh	DESFire status / error code, refer to DESFire documentation

Example

Command	Description
f0B1202010000010000 100000	Answer: 00 Linear record file with ID 02 and MAC security is created. Record size is 000001h and number of records is 000010h.

Note

For further information on communication settings and access rights, refer to the DESFire documentation.

8.4.6.20 Create Cyclic Record File

This command creates a Cyclic Record File in a selected application. Cyclic record files use a shadow register for data manipulation operations. The file number must be in the range from 00h to 07h.

Command

Command	Data
13h	File number (1 byte) Communication settings (1 byte) Access rights (2 bytes) Record Size (3 bytes) Number of Records (3 bytes)

Answer

Answer	Description
Data	Status code (1 byte)
00h	Cyclic Record File created
'N'	Error: No tag in field
Xxh	DESFire status / error code, refer to DESFire documentation

Example

Command	Description
f0B1303010000020000 100000	Answer: 00 Cyclic record file with ID 03 and MAC security is created. Record size is 000001h and number of records is 000010h.

Note

For further information on communication settings and access rights, refer to the DESFire documentation.

8.4.6.21 Delete File

This command deletes a file on tag in a selected application.

Command

Command	Data
14h	File number (1 byte)

Answer

Answer	Description
Data	Status code (1 byte)
00h	File is successfully deleted
'N'	Error: No tag in field
Xxh	DESFire status / error code, refer to DESFire documentation

Example

Command	Description
f021403	Answer: 00 File with ID 03h is deleted.

8.4.6.22 Read Data / Records

This command reads data of a selected Data or Record file.

Command

Command	Data
15h	Offset (3 bytes) Length (1 byte)

Answer

Answer	Description
00h + Data (n bytes)	Data
'C'	Error: CRC or MAC does not match
'N'	Error: No tag in field
'O'	Error: No file selected
'R'	Error: Out of range
Xxh	DESFire status / error code, refer to DESFire documentation

Example

Command	Description
f051500000005	Answer: 000011223344 Read 5 bytes from offset 000000h.
f051500000000	Answer: 0011112222 Read all records of the record file.

8.4.6.22.1 Our of range 'R'

If the data received exceeds the maximum of 232 bytes, the error R ('Out of range') is returned.

Note

If performance is important, 232 bytes should be used for plain data and 224 should be used for enciphered and MACed data, because in this case, the smaller frames from the DESFire tag are filled up completely.

8.4.6.23 Data files

The offset defines the start address of the reading. The length specifies the number of bytes, which are read. The offset and length must not exceed the limits of the file.

8.4.6.24 Record file

Records are always read one at a time. The offset points to the record within the record file from which the reading starts. The length defines the number of records that have to be read. The response always starts with the oldest record. Offset 000000h points to the latest record. Length 00h reads all records of the record file.

8.4.6.25 Write Data / Record

This command writes data to a selected Data or Record file. A write record command will append a new record to a linear record file until all records are filled up. Using cyclic record files, the oldest record is updated when all records are used up. The write record command must be validated with the commit/abort transaction command.

Command

Command	Data
16h	Offset (3 bytes) Data (n bytes)

Answer

Answer	Description
Data	Status code (1 byte)
00h	Success
'C'	Error: CRC or MAC does not match
'N'	Error: No tag in field
'O'	Error: No file selected
'R'	Error: Out of range
Xxh	DESFire status / error code, refer to DESFire documentation

Example

Command	Description
f091601000011223344 55	Answer: 00 Writes data 1122334455 starting at position 000001h to a data file or a new record.

8.4.6.25.1 Our of range 'R'

If sent data exceeds the maximum of 232 bytes, the error R ('Out of range') is returned.

Note

If performance is important 232 bytes should be used for plain data and 224 should be used for enciphered and MACed data, because in this case the smaller frames from the DESFire tag are filled up completely.

8.4.6.26 Get Value

This command reads a value block of a selected value file.

Command

Command	Data
17h	None

Answer

Answer	Description
00h + Value (4 bytes)	Value
'C'	Error: CRC or MAC does not match
'N'	Error: No tag in field
'O'	Error: No file selected
Xxh	DESFire status / error code, refer to DESFire documentation

Example

Command	Description
f0117	Answer: 0022222222 value 22222222h is currently stored in the value file.

8.4.6.27 Credit

This command increases a value in a selected value file. All value manipulation commands are accumulated in a shadow register. This shadow register is only written after a successful commit transaction command.

Command

Command	Data
18h	Data (4 bytes)

Answer

Answer	Description
Data	Status code (1 byte)
00h	Success
'N'	Error: No tag in field
Xxh	DESFire status / error code, to refer DESFire documentation

Example

Command	Description
f051878563412	Answer: 00 The value 12345678h is added to the selected value file.

8.4.6.28 Debit

This command decreases a value in a selected value file. All value manipulation commands are accumulated in a shadow register. This shadow register is only written after a successful commit transaction command.

Command

Command	Data
19h	Data (4 bytes)

Answer

Answer	Description
Data	Status code (1 byte)
00h	Success
'N'	Error: No tag in field
xxh	DESFire status / error code, refer to DESFire documentation

Example

Command	Description
f051944332211	Answer: 00 The value 11223344h is charged from the selected value file.

8.4.6.29 Limited Credit

This command limits the credit to a selected value file. The value depends on all previous debit values. It enables to cancel misattributed debits. All value manipulation commands are accumulated in a shadow register. This shadow register is only written after a successful commit transaction command.

Command

Command	Data
1Ah	Data (4 bytes)

Answer

Answer	Description
Data	Status code (1 byte)
00h	Success
'N'	Error: No tag in field
Xxh	DESFire status / error code, refer to DESFire documentation

Example

Command	Description
f051A11111111	Answer: 00 The value 11111111h is added to the selected value file. A previous debit sum of at least 11111111h is needed.

8.4.6.30 Clear Record File

This command clears the whole content of a selected record file. After a commit / abort transaction command the changes are written.

Command

Command	Data
1Bh	None

Answer

Answer	Description
Data	Status code (1 byte)
00h	Success
'N'	Error: No tag in field
Xxh	DESFire status / error code, refer to DESFire documentation

Example

Command	Description
f011B	Answer: 00 All records of the record file are erased.

8.4.6.31 Commit Transaction

This command validates all previous write operations to backup data or record files and data manipulations on value files in a selected application. All changes are done at the same time.

Command

Command	Data
1Ch	None

Answer

Answer	Description
Data	Status code (1 byte)
00h	Success
'N'	Error: No tag in field
Xxh	DESFire status / error code, refer to DESFire documentation

Example

Command	Description
f011C	Answer: 00 All changes successfully executed.

8.4.6.32 Abort Transaction

This command aborts all previous write operations to backup data or record files and data manipulations on value files of a selected application. No data is changed. Power loss will be interpreted as an abort transaction command.

Command

Command	Data
1Dh	None

Answer

Answer	Description
Data	Status code (1 byte)
00h	Success
'N'	Error: No tag in field
xxh	DESFire status / error code, refer to DESFire documentation

Example

Command	Description
f011D	Answer: 00 All modifications are cancelled.

9 Software for contact interface functions

The contact interface is fully CCID and PC/SC compliant. Therefore there are no own commands available. The PC/SC documentation can be downloaded from PC/SC workgroup web site http://www.pcscworkgroup.com/.

In order to develop own application S/W it's recommended to use the Microsoft SDK, as the reader supports ScardControl commands.

10 Frequently Asked Questions

10.1 Getting Started

To test and interface the ACGPass e-ID Desktop Reader, you just need to connect the reader via the USB cable with a Microsoft Windows 2000® or Microsoft Windows XP® based PC. You do not need a power supply for the reader. Once the reader is connected then please just follow the instruction on the PC screen.

The PC/SC driver for the reader should come together with the reader. It is also available via the next ASSA ABLOY ITG sales office, the web site http://www.aaitg.com/

10.2 Personalized ACGPass e-ID Desktop Reader

In applications that are using the binary protocol mode, personalization maybe required. Use the Utility program to set up your reader correctly. Ask the reseller or the ASSA ABLOY ITG sales representative for the Utility software or download it from http://www.aaitg.com/. Minimum requirements are Microsoft Windows 2000®, Microsoft Windows XP® and the reader connected to the PC.

10.3 What type of mifare® card should I use?

The mifare® standard is designed for multi-application environments. It contains 16 sectors each with 2 individual keys, access conditions, and 3 data or value blocks. Some applications use the 1 Kbytes of the mifare® Standard Card Memory only as storage area.

mifare® Ultralight has no crypto unit on chip. It only supports 16 blocks.

mifare® Standard 4k cards have the same features as mifare® Standard cards but increased memory capacity.

10.4 How safe is mifare® Standard for cashless payment?

Security is always a feature 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 identifying possible attacks and then create barriers to block them.

mifare® was specifically designed for cashless payment applications. The mifare® concept provides the following security barriers:

- Anti-collision/-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 based on trying many different keys is limited by the transaction time (several ms) of the card and would last virtually forever.

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 increment the value on the cards. As a general rule, key A is used as a field key, allowing only to read and decrement values, and key B is used to format the card or increment values.
- Diversified keys. To make life even harder for attackers, keys can be modified using the 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 programmed at the time of delivery) for ticketing applications!
- Ciphered and scrambled data storage
- Sabotage alarm
- Even higher security with contact less controller cards like mifare® DESFire, mifare® ProX, mifare® Smart MX etc.

10.5 Using a mifare® card

This example demonstrates the detection of a card in the antenna field with continuous read and the reading of a page.

Command	**Answer**
c	Activate continuous read mode
	B2197B58 a card responds with its serial number
.	S abort continuous read mode
s	B2197B58 select card
l01AAFFFFFFFFFFF	L login into sector 1 with key FFFFFFFFFFFFh key type A
rb04	00112233445566778899AABBCCDDEEFF read block 04
c	Activate continuous read mode to detect a new card

Figure 10-1: Using a mifare® card

10.6 Using a DESFire card

10.6.1 Create a plain standard data file

After activation, application 0 is selected automatically. Default access rights of application 0 require a login to create an application. The following example illustrates the successful creation of a plain standard data file.

Command	Answer
s	04E10E00000000 activate card
f1200000000000000000000000000000000000000	L login to application 0
f06050000100F01	00 create application with ID 000010
f0408000010	00 select application with ID 000010
f080F0000eeee10000000	00 create plain standard data file with ID 00

Figure 10-2: Create plain standard data file of a DESFire card

10.6.2 Use a plain standard data file

The next example demonstrates the use of a plain standard data file, such as that created in the previous example. No login needed since the file is plain.

Command	Answer
s	04E10E00000000 activate card
f0408000010	00 select application with ID 000010
f020D00	00 select file with ID 00
f09160000001122334455	00 write data to standard data file
f051500000010	00112233445500000000000000000000000 read data from standard data file

Figure 10-3: Change data of a plain standard data file

10.6.3 Create a value file

Basically, each application is created in the same way. The access rights of an application can be adjusted to freeze the application organization. In this case, a login to the application is needed to make any changes to the application. Regardless of the application access rights, a file can be selected using its ID. Before accessing a secured file, a login to the application is needed. A successful login allows changing all the files in the application that use the same key.

A value file has a special structure. If a value file is changed the changes are only accepted after a commit transaction command. This feature allows modifying several files of an application and changing all the contents at the same time.

The following example illustrates the creation of a value file using DES encipher.

Command	**Answer**
s	04E10E00000000 activate card
f1200000000000000000000000000000000000000	L login to application 0
f06050000110F01	00 create application with ID 000011
f0408000011	00 select application with ID 000011
f12110003000000000000FFFFFF7Ff5555555500	00 create value file with initial value 55555555 with ID 00. File is secured with DES encipher

Figure 10-4: Create a plain standard data file on a DESFire card

10.6.4 Use a DES secured value file

The next example demonstrates the use of a DES secured value file, such as the one created in the previous example. After the selection of the application, a login with the key of the value file is needed to access the file. Modification of the value file is accepted after the commit transaction command is given.

Command	Answer
s	04E10E00000000 activate card
f0408000011	00 select application with ID 000010
f03000000	L login to application
f020D00	02 select file with ID 00 (value file)
f0117	0055555555 read value file data
f051911111111	00 debit value file with 11111111
f0117	0055555555 read value file, no modification done
f011c	00 commit transaction, modification is done
f0117	0044444444 read value file, verify modification

Figure 10-5: Change data of a plain standard data file

11 References

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

[2] DESFire Documentation, Philips, http://www.semiconductors.philips.com

[3] Data Encryption Standard (DES), FIPS PUB 46-3,
Reaffirmed 1995 October 25

[4] ASSA ABLOY ITG Antenna Design Guide

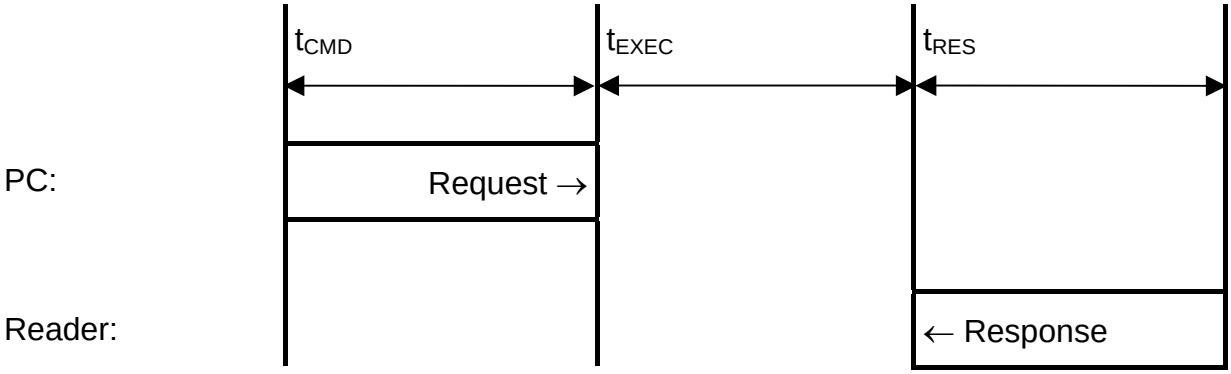
[5] Philips; Application Note, mifare® & I-Code, Micore Reader IC family Directly Matched Antenna Design

12 Appendix A: SAM

Please note that the power supply of the SAM adapter must be turned off during the entire card insertion period, otherwise SAM card damage might occur.

For proper usage of the SAM, a 100nF capacitor between V_{cc} and GND is necessary.

13 Appendix C: Timings



Command	t_{EXEC} [ms]	Comments
Common commands		
Cont. read (locked tag)	2.8 – 22.6	+ Reset Off and Recovery Time
Cont. read (worst case)	54	+ 3x Reset Off and Recovery Time
DES en/decryption	9.6 – 9.7	
TDES en/decryption	28.7 – 28.8	
High-speed select 'h08' (locked tag)	8.9 – 14.4	+ Reset Off and Recovery Time + SFGT
High-speed select 'h08' (no tag)	15	+ 3x Reset Off and Recovery Time
High-speed select 'h08' (worst case)	14.7	+ 3x Reset Off and Recovery Time + SFGT
Multiselect (locked tag)	5.8 – 11.4	+ Reset Off and Recovery Time
Multiselect (no tag)	67	+ Reset Off and Recovery Time
Multiselect (worst case)	67	+ Reset Off and Recovery Time
Antenna on	0.2	+ Reset Recovery Time
Antenna off	0.2	
Port read	0.1	
Port write	0.1	
Read block	1.8 – 2.2	
Write block	8.2 – 11	
Reset	13.2	
Select (locked tag)	5.4 – 22.8	+ Reset Off and Recovery Time
Select (no tag)	38	+ 3x Reset Off and Recovery Time
Select (worst case)	55	+ 3x Reset Off and Recovery Time

Command	t_{EXEC} [ms]	Comments
ISO 14443 Type A only commands		
Increment value block	18.4	
Decrement value block	18.4	
Copy value block	18.5	
Read value block	2.3	
Write value block	7.9 - 10.5	
Mifare Login	4.9	
Power conditions		
Power on	79	Does not include rise time of power supply
Enable on	85	

Figure 13-1: Timings

Default Command Guard Time (20h = 1.2ms) was used.

All timing data is advisory application information and does not form part of the specifications. It may change in future firmware releases. Please also note that all values specified in the above table depend on the tag used and Command Guard Time.

14 Appendix D: Release Notes

14.1 Version History

14.1.1 Dual 2.0

Initial Release.

14.1.2 Dual 2.1

- High-speed select supports anti-collision and the forcing of the air interface transmission rate and the frame size
- Automatic ISO 14443-4 error handling (can be switched on/off)
- RATS answer is returned with high-speed select command for ISO14443 A tags and with Extended ID flag set
- Support for the ISO14443 B anti-collision algorithm
- Extended Protocol flag now switches on/off, complete ISO14443-4 handling
- ISO14443-4 chaining and WTX improved
- 'of' and 'og' commands get new parameters
- Selection time-out for ISO14443-4 A tags is set to 10h

14.1.3 Dual 2.2

- Sending serial data frames over User Port
- Automatic ISO 14443-4 timeouts can be switched on/off
- Request A information within ISO 14443 A Extended ID answer can be switched on / off
- Command Guard Time added
- 'of' and 'og' commands get new parameters
- Chaining of 256 byte frame support
- Support of ASK GTML tag
- Page read functionality added
- Additional protocol register PCON3
- Some bug fixes

14.1.4 Dual 2.3

- Reset To Default via MCLR Pin possible
- Added 'ra' command: Resend last answer
- SAM Command: Option byte modified, Improvements
- Default value of ISO 14443B Selection timout register changed to 10h
- Asynchronous Baudrates possible with Highspeed select
- Added command that returns the version of the bootloader
- Added command "rd"/"wd": read/write multiple blocks
- "DisableReadAfterWrite" Flag added
- Bug fixes

14.2 Revision history

Date	Revision number
02/18/2005	Version 2.1, Rev. 1.0
05/17/2005	Version 2.2, Rev. 1.0
??/??/2006	Version 2.3, Rev. 1.0

15 Appendix F: Approvals / Certificates

15.1 CE Declaration

ASSA ABLOY Identification Technologies GmbH declares that, in conformity with the European CE requirements specified in the EMC Directive 89/336/EEC, ACGPass e-ID Desktop Reader, described in this manual is

CE compliant

The relevant documents are available.

If any of the ACGPass e-ID Desktop Reader is operated from a mains power supply, all power connections and additional components of the final device must also comply with the EMC Directive 89/336/EEC directive.

Customers selling into Europe must themselves make sure that the final device conforms to the EMC Directive 89/336/EEC directive.

For ASSA ABLOY Identification Technologies GmbH, the compliance of important international regulations into business practices are a priority and the implementation of the EMC Directive 89/336/EEC is fully in line with the company's commitment to continuously improve its Quality Management System.

Walluf, January 2006

ASSA ABLOY Identification Technologies GmbH

15.2 FCC Declaration

ASSA ABLOY Identification Technologies GmbH declares that, in conformity with the U.S. Directive FCC part 15, the ACGPass e-ID Desktop Reader described in this manual, is

FCC part15 compliant

The relevant documents are available.

If any of the ACGPass e-ID Desktop Reader is operated from a mains power supply, all power connections and additional components of the final device must also comply with the US FCC Part 15 directive.

Customers selling into the USA must themselves make sure that the final device conforms to the US FCC Part 15 directive.

Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

For ASSA ABLOY Identification Technologies GmbH, the compliance of important international regulations into business practices are a priority and the implementation of the FCC part 15 is fully in line with the company's commitment to continuously improve its Quality Management System.

Walluf, January 2006

ASSA ABLOY Identification Technologies GmbH

15.3 RoHS Compliance

ASSA ABLOY Identification Technologies GmbH declares that, in conformity with the Directive 2002/95/EC about the Restriction of Hazardous Substances (RoHS), its ACGPass e-ID Desktop Reader products, listed in this manual, are

RoHS compliant

The following substances

- Cadmium and cadmium compounds
- Lead and lead compounds
- Mercury and mercury compounds
- Hexavalent chromium compounds
- Polybrominated biphenyls (PBB)
- Polybrominated Diphenylethers (BPDE)

are contained in accordance with the limits required by the Directive.

For ASSA ABLOY Identification Technologies GmbH, the integration of environmental considerations into business practices are a priority and the implementation of RoHS Directive is fully in line with the company's commitment to continuously improve its Quality Management System.

Walluf, January 2006

ASSA ABLOY Identification Technologies GmbH