User Manual

IDENTIVE Technologies AG

Multi-ISO HF Reader – RS232

Contact:
www.identive-technologies.com
www.identive-group.com
support@identive-technologies.com

Document History

Version	Date	Description	Compatibility
1.0	Mar 31, 2009	First Draft	Firmware version 1.02 and above
1.1	Apr 13, 2009	First Release	Firmware version 1.02 and above
1.2	Apr 15, 2009	APDU samples section is removed	Firmware version 1.02 and above
1.3	Apr 17, 2009	APDU samples section is added	Firmware version 1.02 and above
1.4	Jun 29, 2009	DESFire EV1 commands are explained, modified ChangeKey command of DESFire as per spec.	Firmware version 1.02 and above
1.5	Jul 22, 2009	Updated with OS supported in Section 1	Firmware version 1.02 and above
1.6	Sep 01, 2009	- Pin Connection diagram has been updated - MIFARE Restore command description added - Change Key command description for DESFire cards added - Response length of GetCardUID command is corrected in the DESFire-EV1 examples - Removed the Traverse commands for MIFARE - LoadKey command described for AES Keys - Reader LoadKeys added in the APDU examples - “Firmware Upgrade” term is followed - Table numbers corrected - Document Header modified - Value in the command description of MIFARE value blocks have been modified under section 6 - e-PC/SC term is followed	Firmware version 1.02 and above
1.7	Jul 22, 2010	- Details regarding accessing of MIFARE-ULC, My-d move , MIFARE-Plus have been added - SDU samples for MIFARE-Plus have been added - Terms and Abbreviations have been update	Firmware version 1.05 and above
1.8	Feb 02, 2011	- EasyDESFire & Transparent mode explained	Firmware version 1.10 and above
1.9	Jun 13, 2011	- Control TOM mode command has been added	Firmware version 1.14 and above
1.10	Sep 29, 2011	- LED behaviors added	Firmware version 1.15 and above
1.11	May 10, 2012	- Updated the firmware versions in the LED behavior - Insignficant (Logo and headers changed)	Firmware version 1.15 and above
1.12	Mar 06, 2013	- Updated onboard connector part numbers - Added part numbers for cable assembly - Added pre-assembled RS232 cable info - Added Table and Figure descriptions & numbers	Firmware version 1.15 and above
1.13	Apr 08, 2013	- Updated “Getting Started” (section 1)	Firmware version 1.15 and above
1.14	Aug 14, 2013	- Added reader firmware info (section 8)	Firmware version 1.15 and above

CONTENTS

1 Getting Started

The Multi-ISO HF USB Reader/Writer is a contactless smart card/tag reader and writer for accessing ISO14443-4 Type A, ISO14443-4 Type B, MIFARE (Classic, Ultralight C, DESFire, DESFire EV1, Plus), my-d move, NFC (Type 1, 2, 4) tags, ISO15693, and ICODE SLI tags. This document is intended for application developers who want to access contactless cards using the Multi-ISO HF USB Reader/Writer.

This document is intended for smart card application developers who want to access contactless cards using the Multi-ISO HF RS232 Reader/Writer. It explains in detail the Application Programming Interface provided by the reader/writer.

Unlike conventional readers, the interface is maintained quite simple and easy to use for the application developers. Commands are developed to be equivalent to PC/SC compatible WinSCard API that is widely used for smart card application development. Since the commands imitate PC/SC standard, it's given the name "e-PC/SC Commands" (e-PC/SC meaning that the PC/SC standard is embedded inside the device). The card/tag communication protocols are handled within the device firmware itself.

The reader does not require any driver and can be used under the following operating systems

- Windows (2000, XP, 2003, Vista, 2008, 7, 8)
- Linux (any version with serial host support)
- Mac OS (any version with serial host support)
- Any other desktop OS with serial host support
- Any embedded OS with serial host support

1.1 HOST Interface

The following are the characteristics of the HOST interface

- RS232 based UART interface to connect to the host
- Embedded PC/SC like proprietary command support through proprietary serial protocol
- Protocol level handshake and error detection

1.1.1 RS232 Settings

The RS232 interface can be configured to support a variety of baud rates and frame settings. The settings supported by the reader/writer are listed in the following table

UART port parameters	*Values*
Baud rate	110, 300, 600, 1200, 2400, 4800, 9600, 14400, 19200, 38400, 57600, 115200, 128000, 256000, 460800
Data bits	8
Parity	None, Even, Odd, Mark & Space
Stop bits	1 & 2

Table 1- List of supported UART parameters

1.1.2 Host Interface Connector

The onboard connector for host communication is a male 8-pin connector (Molex 53261-0871). For cable assembly you need the connector housing (Molex 51021-0800) and the crimp terminals (Molex 50079-8000).

Identive provides the fully assembled serial communication cable as an accessory when the reader is ordered as an OEM module (PN: KAB_RS232). The power supply for the reader is provided via a separate USB connector (no data lines are connected).

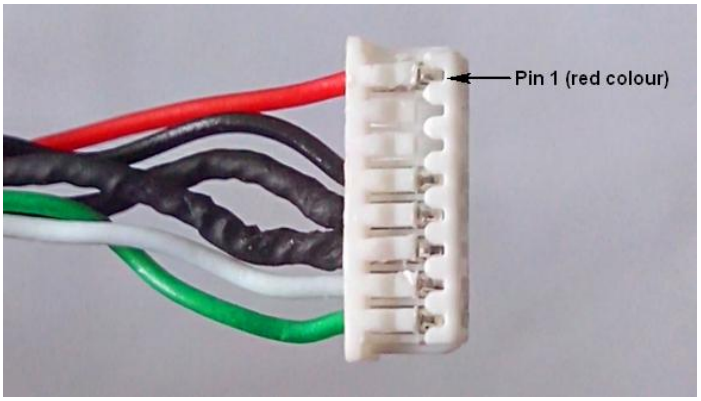

Figure 1 - Molex 8-pin connector of a pre-assembled cable

Connector Pin	*Cable Wire*	*Signal Description*
1	1	+5V ±5% Regulated DC Power input to Multi-ISO Reader
2	-	No Connection
3	-	No Connection
4	2	Ground
5	3	Ground
6	4	Ground
7	5	RXD input to the Multi-ISO Reader at RS232 signal level
8	6	TXD output from the Multi-ISO reader at RS232 signal level

Table 2 - Pin Layout

Note: All three ground wires must be connected to GROUND for the device to operate

2 LED Behaviors

The following tables describe the LED behavior of the reader during possible reader states.

Firmware version ≤ 1.14

Reader States	Green LED	Red LED	Blink-rate (s)
DFU F/W is active	OFF	ON	-
Functional F/W active & Unconfigured	ON	OFF	-
Functional F/W active & Configured			
Waiting for card to be detected			
Card detected			
Host communicating with the card	ON	ON	Red LED will be ON until the reader responds to the host command
Error in card detection*	ON	OFF	-

Table 3 - LED behavior for firmware version ≤1.14

Firmware version ≥ 1.15

Reader States	Green LED	Red LED	Blink-rate (s)
DFU F/W is active	OFF	ON	-
Functional F/W active & Unconfigured	ON	OFF	-
Functional F/W active & Configured	OFF	ON	-
Waiting for card to be detected	OFF	ON	-
Card detected	Blinking	OFF	0.25
Host communicating with the card	ON	Blinking	0.05
Error in card detection*	ON	ON	-

Table 4 - LED behavior for firmware version ≥1.15

* For contactless cards, the card has not fully entered the reader's RF field or the card is not responding.

3 Card Reader Suite – Test Application

This is a test application that is provided along with Multi-ISO HF RS232 Reader/Writer for customer use. CardRdrSuite consists of several sub-applications covering the following functionalities

3.1 Firmware Upgrade

Reader firmware can be upgraded using this sub-application. Salient features are

- Auto reader detection
- User friendly GUI
- Provision to view device's current firmware version and the version of the firmware to be downloaded

Refer to section "Firmware Upgrade" of Card Reader Suite help file for detailed description. Help file can be launched using the "Help" button in the main window of the Card Reader Suite application.

3.2 e-PC/SC Diagnostics

Any reader SDU (Serial Data Unit), Card APDU or Pseudo APDU can be issued and tested using this sub-application.

Its salient features are

- SDU/APDU execution from script file (.SDU)
- Easy to edit script files
- Error status logging in a file
- Working samples scripts for each card type supported

Refer to section "e-PC/SC Diagnostics" of the Card Reader Suite help file for detailed description

3.3 Binary configuration

All configurable parameters of the reader can be modified using these sub-applications. These applications will configure the firmware binary file only.

Configure Binary

- Configures
  - UART parameters
  - Firmware Version parameters
  - Hardware Version parameters
  - Other firmware configurations
- Provides option to make the parameters non-modifiable after configuring

Refer to section "Configure binary" of Card Reader Suite help file for detailed description

Edit Binary

- Configures
  - RF parameters
  - MIFARE keys stored in the non-volatile memory of the reader
  - DESFire keys stored in the non-volatile memory of the reader
- Provides option to make the parameters non-modifiable after configuring

Refer to section "Edit Binary" of Card Reader Suite help file for detailed description

3.4 Serial Diagnostics

This sub-application can be used to detect the reader/writer and to temporarily change the UART settings of the reader/writer. This sub-application provides list box options to choose the desired UART settings

Manual Detection
This option is used to check for presence of a reader/writer using the user selected UART settings

Automatic Detection
This option is used to check for the presence of a reader/writer using all possible UART settings and in all the available COM ports in the HOST

Change UART Settings
This option is used to configure the UART parameters temporarily for one session with the reader/writer i.e. these parameters will be valid until the reader/writer is powered off.
After the next power on, the reader/writer will use the default UART parameters.

Refer to section “Serial Diagnostics” of Card Reader Suite help file for detailed description of all these options

4 Serial embedded PC/SC Protocol [e-PC/SC]

PC/SC (as per reference [R2]) is a de-facto standard to interface Personal Computers with Smart Cards (and smartcard readers of course). Multi-ISO HF RS232 Reader/Writer provides a proprietary command set equivalent to the PC/SC API for communication between the host and the reader/writer, called the e-PC/SC commands. The e-PC/SC commands are transmitted using a proprietary serial protocol which is explained in detail in this section. We call this serial protocol as e-PC/SC serial protocol.

There are 3 different packets used in the e-PC/SC serial protocol for communication between the HOST and the reader/writer. All packet data are sent and received as hexadecimal values

Command Packet Structure:
This packet is used to send commands from the HOST to the reader/writer

Header		***Length***		***Packet Data***		
0D	0A	No of bytes in Packet Data Field excluding DCS (2 bytes)	Length Checksum (1 byte)	Command Opcode (any of the values described in later sections) (1 byte)	Command Data (if any as described in the later sections) (Maximum 270 bytes)	Data Checksum (1 byte)

Response Packet Structure:
The reader/writer uses this packet to send responses to the HOST

Header		***Length***		***Packet Data***		
0D	0A	No of bytes in Packet Data Field Excluding DCS (2 bytes)	Length Checksum (1 byte)	Status byte (any of the values described in Table 3) (1 byte)	Response Data (if any as described in the later sections) (Maximum 270 bytes)	Data Checksum (1 byte)

ACK Packet Structure:
For every set of 16 or less data bytes received from the HOST, the reader/writer sends this packet to the HOST to acknowledge successful reception

Header		***Length***		***Packet Data***	
0D	0A	No of bytes in Packet Data Field excluding DCS (2 bytes) [Value = 0001]	Length Checksum (1 byte) [Value = FF]	ACK byte (1 byte) [Value = FF]	Data Checksum (1 byte) [Value = 01]

Check Sum calculation:
The 1 byte Length Check sum satisfies the relation

$LEN_M + LEN_L + LCS = 00$

Where,
LEN_M - Most significant byte of length
LEN_L - Least significant byte of length

The 1 byte Data Check sum satisfies the relation,

$PD_0 + PD_1 \ldots + PD_n + DCS = 00$

Where,
PD_n - n^{th} Packet data

Status Byte:

Status Byte (HEX)	*Description*
00	Command Successful
01	Length parameter of the received Command is wrong
05	Slot no specified is invalid
80	Command parameter invalid
81	SCardConnect not done
83	Unsupported command Opcode
84	No data from the HOST
87	Error in Serial Framing
88	CRC of Serial data received was wrong
89	Smartcard controller FIFO overflow
8A	Access denied
8B	Invalid Key
8C	Authentication to MIFARE or DESFire card was unsuccessful
8D	Retry the command
92	Functional firmware is invalid
93	The command received is not framed as per the e-PC/SC protocol
94	Operation Timed out
FB	Hardware Error
FD	Parity error in the Serial data received
FE	Smartcard not present in the field

Table 5 - Status Byte

4.1 e-PC/SC Serial Protocol Dialog

- The HOST sends the command packet to the Reader/Writer. As long as the data in the command packet is more than 16 bytes, it is sent in multiples of 16 bytes. When the data in the command packet is less than 16 bytes it is sent completely
- For every set of 16 or less data bytes received, the reader/writer sends an ACK Packet to the HOST
- The Reader/Writer executes the command after receiving the entire command packet successfully
- After command execution, the Reader/Writer sends the response packet to the HOST
- The Status byte in the response indicates successful execution or error status, if any
- In case of any reception error, the Reader/Writer responds with an appropriate Status byte, as described in Table 5

The flow diagram in Figure 2 explains how a host application has to send and receive data:

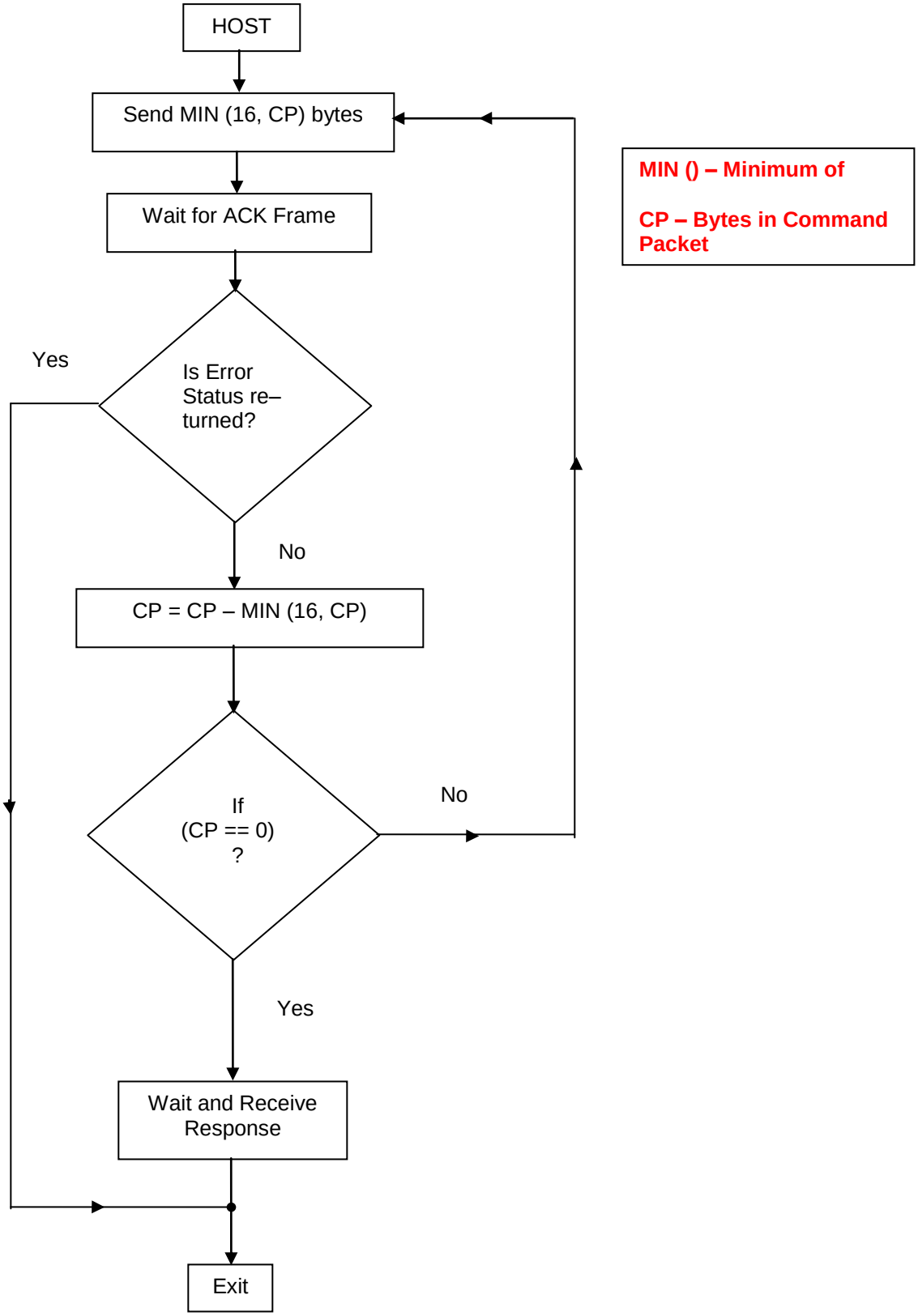

Figure 2 - Serial Data Flow

4.2 How to Access Contactless Cards via e-PC/SC?

The following steps provide a guideline to create your first contactless smart card application using the proprietary commands using the e-PC/SC protocol. The commands and their functionality are also described in detail in this section

4.2.1 RDR Parameters

As the first step, detect the presence of Multi-ISO HF RS232 Reader/Writer. This step also ensures proper communication with the reader/writer, through the RS232 interface. The RDR Parameters command returns information about the reader/writer as in the following structure table.

Parameter	No of bytes
Hardware Revision No	2
Hardware Customer ID	2
Hardware Product ID	2
Firmware Version No	2
Device Serial No	32
Manufacturer string	32
Product string	32
UART line parameters	1
UART baud rate	4

Table 6 - RDR Parameters structure

Command Format:

Header		Length	LCS	Command Opcode	Command Data	DCS
0D	0A	0001	FF	80	-	80

Response Format:

Header		Length	LCS	Status Byte	Response Data	DCS
0D	0A	0021	DF	00	Reader/Writer Parameters as described in the RDR Parameters structure	xx

4.2.2 ScardStatus

The next step is to detect the presence of a smart card before proceeding with card communication. The SCardStatus command informs the presence or absence of a smart card

Command Format:

Header		Length	LCS	Command Opcode	Command Data	DCS
0D	0A	0002	FE	03	Slot No (1 byte) [Value = 00]	FD

Response Format:

Header		Length	LCS	Status Byte	Response Data	DCS
0D	0A	0002	FE	00	*Card State* 00 – Card Absent 01 – Card Present	xx

4.2.3 SCardConnect

The HOST must then connect to the card before issuing card commands. The SCardConnect command establishes a connection to the smart card, if present, and returns its ATR. [If no card is present an error status is returned]

Command Format:

Header		Length	LCS	Command Opcode	Command Data	DCS
0D	0A	0001	FF	01	Slot No (1 byte) [Value = 00]	FF

Response Format:

Header		Length	LCS	Status Byte	Response Data	DCS
0D	0A	Length of ATR + 01	xx	00	ATR of the Card as defined in reference [R2]	xx

4.2.4 SCardTransmit

The HOST is now ready for active communication with the card. The SCardTransmit command sends APDU/card supported command frame to the card/tag and returns the response data from the Card

A successful execution of SCardConnect command is required before using this command

Command Format:

Header		Length	LCS	Command Opcode	Command Data		DCS
0D	0A	Length of Command Data + 01	xx	04	Slot No (1 byte) [Value = 00]	7816 APDU (as defined in [R7]) / Pseudo APDU (as defined in section Access Cards through ePC/SC) / Card Command	xx

Response Format:

Header		Length	LCS	Status Byte	Response Data	DCS
0D	0A	Length of Response Data + 01	xx	00	Response from card	xx

4.2.5 SCardDisconnect

After the completion of all transactions with the card, the HOST can disconnect the card. It is not absolutely necessary to disconnect the card, but it is recommended. The SCardDisconnect command terminates any previously established connection to the Smart Card

Command Format:

Header		Length	LCS	Command Opcode	Command Data	DCS
0D	0A	0001	FF	02	Slot No (1 byte) [Value = 00]	FE

Response Format:

Header		Length	LCS	Status Byte	Response Data	DCS
0D	0A	0001	FF	00	-	00

4.3 ATR Generation

To make contact less cards available within the PC/SC framework, the Multi-ISO HF RS232 Reader/Writer generates a PC/SC compliant ATR according to PC/SC v2.01.09 “Interoperability Specification for ICCs and Personal Computer Systems” (reference [R2])

4.3.1 CPU Cards

The ATR of Contactless smart cards (i.e. cards with CPU) are composed as described in PC/SC v2.01.09, Part3: Requirements for PC connected Interface Devices, 3.1.3.2.3.1, Table 3.5

4.3.2 Storage Cards

The ATR of storage cards (i.e. cards without CPU) is composed as described in PC/SC v2.01.09, Part3: Requirements for PC connected Interface Devices, 3.1.3.2.3.2, Table 3.6. In order to allow the HOST application to identify a storage card type properly, its standard and card name is mapped according to the Part3: Supplement Document of PC/SC v2.01.04

Note: The registered Application Provider Identifier (RID) returned by the Multi-ISO HF RS232 Reader/Writer for storage cards (cards without CPU) is “A0 00 00 03 06”, which is the RID of the PC/SC workgroup

4.4 Modify Reader parameters

The following commands can be used to modify the reader/writer parameters, to fine tune the reader/writer performance or to suit the end applications requirements.

4.4.1 RDR Change UART Parameters

The RDR Change UART Parameters command is used to change the UART settings of the reader/writer temporarily for one session i.e. until the reader/writer is powered off. After the next power on, the reader/writer will use the default UART settings

Command Format:

Header		Length	LCS	Command Opcode	Command Data		DCS
0D	0A	0006	FA	81	Line Control Parameters (1 byte – See below for definition)	Baud rate (4 bytes)	xx

Response Format:

Header		Length	LCS	Status Byte	Response Data	DCS
0D	0A	0001	FF	00	-	00

Line Control Parameters:

b7	b6	b5	b4	b3	b2	b1	b0
0	0	*Parity Type* 00 – Odd Parity 01 – Even Parity 10 – '1' Stick Parity 11 – '0' Stick Parity		*Parity Enable* 0 – Disable Parity 1 – Enable Parity	*Stop Bits* 0 – 1 Stop bit 1 – 2 Stop bit	*Word Length* 11 – 8 bit character	

Status Conditions:

The following specific status conditions are possible:

- 80 – Baud rate specified is invalid

Example: The following is the command to change the UART settings to Odd Parity, 2 Stop bits, 8 bit character and 115200 kbps

Command: 0D 0A 06 00 FA 81 0F 00 C2 01 00 96

Note: The Baud rate is in units of bits per second (bps). A value of 0xFF for the line control parameters will keep the previous values unchanged. The UART Settings will be changed after sending response to the host for this command.

4.4.2 RDR Control

The RDR Control command is used to modify the configuration settings of the reader/Writer

Command Format:

Header		Length	LCS	Command Opcode	Command Data		DCS
0D	0A	Length of Command Data + 1	xx	85	Reader Control command	Reader Control Data	xx

Response Format:

Header		Length	LCS	Status Byte	Response Data	DCS
0D	0A	Length of response Data + 1	xx	00	Reader Control response (if any as define below)	xx

The following are the Reader/Writer control commands:

4.4.2.1 Get Static RF Parameters

The Get Static RF Parameters command is used to get the RF parameters from the non-volatile area of the reader/writer

Command Data:

Header		Length	LCS	Command Opcode	Command Data			DCS
0D	0A	0004	FC	85	01	00	03	77

Response Data:

Header		Length	LCS	Status Byte	Response Data	DCS
0D	0A	0081	7F	00	RF Parameters as in the Structure shown in Table 7 (128 bytes)	xx

Note:

- The command fails if the reader/writer configuration is invalid
- The command fails if any of the command byte is invalid

4.4.2.2 Set Static RF Parameters

The Set Static RF Parameters command is used to modify the RF parameters in the non-volatile area of the reader/writer. The reader/writer uses these parameters from the next power ON

Command Data:

Header		Length	LCS	Command Opcode	Command Data				DCS
0D	0A	84	7C	85	02	00	03	RF Parameters as in the Structure shown in Table 7 (128 bytes)	xx

Response Data:

Header		Length	LCS	Status Byte	Response Data	DCS
0D	0A	0001	FF	00	-	00

Note:

- In the above command data, modifying the parameter value 00,03 might cause the reader/writer to malfunction
- The command fails if the reader/writer configuration is invalid
- The command fails if any of the command byte is invalid
- The command fails if the length mentioned in the RF parameters structure is not equal to 0x0080
- Modifying the Flag value to anything other than 0x01, might make the reader/writer un-usable

4.4.2.3 Get Dynamic RF Parameters

The Get Dynamic RF Parameters command is used to get the RF parameters from the volatile area of the reader/writer

Command Data:

Header		Length	LCS	Command Opcode	Command Data		DCS
0D	0A	0002	FE	85	03	-	78

Response Data:

Header		Length	LCS	Status Byte	Response Data	DCS
0D	0A	0081	7F	00	RF Parameters as in the Structure shown in Table 7 (128 bytes)	xx

4.4.2.4 Set Dynamic RF Parameters

The Set Dynamic RF Parameters command is used to modify the RF parameters in the volatile area of the reader/writer. Immediately following this control command, the reader/writer restarts its entire activity on the RF interface with the new parameters

Command Data:

Header		Length	LCS	Command Opcode	Command Data		DCS
0D	0A	0082	7E	85	04	RF Parameters as in the Structure shown in Table 7 (128 bytes)	xx

Response Data:

Header		Length	LCS	Status Byte	Response Data	DCS
0D	0A	0001	FF	00	-	00

Note: The command fails if the length mentioned in the RF parameters structure is not equal to 0x0080

4.4.2.5 Get Firmware Configuration

Get Firmware Configuration command is used to the retrieve the Firmware Configuration Record from the reader.

Command Data:

Header		Length	LCS	Command Opcode	Command Data			DCS
0D	0A	0004	FC	85	01	1C	00	5E

Response Data:

Header		Length	LCS	Status Byte	Response Data	DCS
0D	0A	0021	DF	00	Firmware Configuration Record as shown in Table 10 (32 bytes)	xx

Note:

- The command fails if the reader/writer configuration is invalid
- The command fails if any of the command byte is invalid

4.4.2.6 Set Firmware Configuration

Set Firmware Configuration command is used to modify/update the Firmware Configuration Record into the reader.

Command Data:

Header		Length	LCS	Command Opcode	Command Data				DCS
0D	0A	24	DC	85	02	1C	00	Firmware Configuration Record as shown in Table 10 (32 bytes)	xx

Response Data:

Header		Length	LCS	Status Byte	Response Data	DCS
0D	0A	0001	FF	00	-	00

Note:

- In the above command data, modifying the parameter value 1C,00 might cause the reader/writer to malfunction
- The command fails if the reader/writer configuration is invalid
- The command fails if any of the command byte is invalid
- Modifying the Flag value to anything other than 0x01, might make the reader/writer un-usable

4.4.2.7 Control TOM Mode

Control TOM Mode command is used to enable/disable the TOM mode of the reader. By enabling the TOM mode, the reader's RF parameters would be optimally configured to improvise the tag readability for cases where in the reader is placed nearby to a metallic environment. It has to be noted that, this is a dynamic control, and hence would become ineffective, after a power-on cycle.

Command Data:

Header		*Length*	*LCS*	*Command Opcode*	*Command Data*	*DCS*
0D	0A	02	FE	92	01 – Enable TOM Mode (or) 00 – Disable TOM Mode	xx

Response Data:

Header		*Length*	*LCS*	*Status Byte*	*Response Data*	*DCS*
0D	0A	0001	FF	00	-	00

Note:

- The command fails if the reader/writer configuration is invalid
- The command fails if any of the command byte is invalid

4.4.3 RF Parameters Data Structure

Parameter	No of bytes	Offset
Length in bytes	2 [Value = 0x0080]	0
Flag	1 [Value = 0x01]	2
A106 - CWCONDUCTANCE	1	3
A106 – RXTHRESHOLD	1	4
A106 - RXCONTROL1	1	5
A212 - CWCONDUCTANCE	1	6
A212 - RXTHRESHOLD	1	7
A212 - RXCONTROL1	1	8
A424 - CWCONDUCTANCE	1	9
A424 - RXTHRESHOLD	1	10
A424 - RXCONTROL1	1	11
A828 - CWCONDUCTANCE	1	12
A828 - RXTHRESHOLD	1	13
A828 - RXCONTROL1	1	14
B106 - CWCONDUCTANCE	1	15
B106 - RXTHRESHOLD	1	16
B106 - RXCONTROL1	1	17
B106 - MODCONDUCTANCE	1	18
B106 - TYPEBFRAMING	1	19
B212 - CWCONDUCTANCE	1	20
B212 - RXTHRESHOLD	1	21
B212 - RXCONTROL1	1	22
B212 - MODCONDUCTANCE	1	23
B212 - TYPEBFRAMING	1	24
B424 - CWCONDUCTANCE	1	25
B424 - RXTHRESHOLD	1	26
B424 - RXCONTROL1	1	27
B424 - MODCONDUCTANCE	1	28
B424 - TYPEBFRAMING	1	29
B848 - CWCONDUCTANCE	1	30
B848 - RXTHRESHOLD	1	31
B848 - RXCONTROL1	1	32
B848 - MODCONDUCTANCE	1	33
B848 - TYPEBFRAMING	1	34
TESTANASELECT	1	35
TESTDIGISELECT	1	36
Reserved	11	37
RF Reset Width in milliseconds	2	48
Card de-bounce delay in milliseconds	2	50
All Timeout Values Multiplication scale	1	52
All Timeout Values Division scale	1	53
All constant Delay Multiplication scale	1	54
All constant Delay Division scale	1	55
All Loop counts Multiplication scale	1	56
All Loop counts Division scale	1	57
Type-A Max baud limit	1	58
Type-B Max baud limit	1	59
Card Polling scheme	1	60
Reserved	67	61

Table 7 - RF Parameters data structure

Naming Convention

In the above table,

- The parameters starting with 'A' or 'B' refer to the respective ISO 14443 card types
- The number following the alphabet indicates the baud rate at which the card should be operating
- The actual RF parameter follows the '-'. This parameter will take effect for that type of card operating at that baud rate

Example: - *A106 – CWCONDUCTANCE* indicates the CWCONDUCTANCE parameter of ISO 14443 TypeA cards operating at 106 Kbps

Parameter Description

RF Control Parameter:
"CWCONDUCTANCE" parameter controls the strength of RF field when there is no modulation. Its value can vary from 0x00 to 0x3F. The chosen value would get directly programmed into the (Address 0x12) RFID reader silicon. For more details refer to the respective datasheet of RFID reader silicon (reference [R12]).

"RXTHRESHOLD" parameter controls the receiver input threshold levels. The specified value would get directly programmed into the (Address 0x1C) RFID reader silicon. For more details refer to the respective datasheet of RFID reader silicon (reference [R12]).

"RXCONTROL1" parameter controls the receiver input stage gain levels and the low pass filters. The specified value would get directly programmed into the (Address 0x19) RFID reader silicon. For more details refer to the respective datasheet of RFID reader silicon (reference [R12]).

"MODCONDUCTANCE" parameter controls the strength of RF field when there is 10% modulation for Type-B data transmission. Its value can vary from 0x00 to 0x3F. The chosen value would get directly programmed into the (Address 0x13) RFID reader silicon. For more details refer to the respective datasheet of RFID reader silicon (reference [R12]).

"TYPEBFRAMING" parameter controls the framing headers SOF & EOF of type B transmission frames. The specified value would get directly programmed into the (Address 0x17) RFID reader silicon. For more details refer to the respective datasheet of RFID reader silicon (reference [R12]).

"TESTANASELECT" parameter controls the analog debug output pin AUX. The specified value would get directly programmed into the (Address 0x3A) RFID reader silicon. For more details refer to the respective datasheet of RFID reader silicon (reference [R12]).

"TESTDIGISELECT" parameter controls the digital debug output pin MFOUT. The specified value would get directly programmed into the (Address 0x3D) RFID reader silicon. For more details refer to the respective datasheet of RFID reader silicon (reference [R12]).

RF Reset Width in milliseconds:
This parameter defines the width of RF Reset (no RF Power) during the polling sequence. The value entered is in decimal, from 0 to 65535. The RF reset would have a width of this much amount of time in milliseconds.

Card de-bounce delay in milliseconds:
This parameter defines the time in milliseconds for which the card arrival is polled and reconfirmed by repeated RNAK polling, before notifying the arrival of a new card into the RF field, to the host. The value entered is in decimal, from 0 to 65535.

All Timeout values Multiplication scale & All Timeout values Division scale:
These two parameters are used to scale the Timeout values used by the Wait functions. The scaling is done using the following formula:

$$\text{TIMEOUT} = \frac{Timeout * Timeout\ Multiplication\ Scale}{Timeout\ Division\ Scale}$$

All constant Delay Multiplication scale & All constant Delay Division scale:
These two parameters are used to scale the constant Delays used in the Wait functions. The scaling is done using the following formula:

$$\text{CONSTDELAY} = \frac{DefaultRetryCount * Loop\ Count\ Multiplication\ Scale}{Loop\ Count\ Division\ Scale}$$

All Loop counts Multiplication scale & All Loop counts Division scale:
Under ISO 14443 Part 3 & Part 4, on occurrence of any communication errors like CRC, Framing, Parity and Timeout, the command will be re-tried by the reader/writer. The Retry count value is scaled using these two parameters, as per the following formula:

$$\text{RETRYCOUNT} = \frac{DefaultRetryCount * Loop\ Count\ Multiplication\ Scale}{Loop\ Count\ Division\ Scale}$$

Type-A Max baud limit & Type-B Max baud limit:
This parameter is used to limit the maximum baud rate at which the reader/writer can operate with the respective ISO 14443 card types

Value	*Maximum Baud Rate Supported*
0x00	106 Kbps
0x01	212 Kbps
0x02	424 Kbps
0x03	848 Kbps

Table 8 - Max Baud Limit

Card Polling Scheme:
This parameter enables the user to select the card types he wants the reader/writer to detect. The Card types disabled here will not be detected

b7	*B6*	*b5*	*b4*	*b3*	*b2*	*b1*	*b0*	*Polling Scheme*
0	0	0	0	0	0	0	0	No Polling
X	X	X	X	X	X	X	1	Poll for 14443 TypeA cards
X	X	X	X	X	X	1	X	Poll for 14443 TypeB cards
X	X	X	1	X	X	X	X	Poll for ISO 15693 cards
1	X	X	X	X	X	X	X	Reserved

Table 9 - Card Polling Scheme

4.4.4 Firmware Configuration Data Structure

Parameter	No of bytes	Offset
Length in bytes	2 [Value = 0x0020]	0
Flag	1 [Value = 0x01]	2
Reserved – 1	1 [Value = 0x01]	3
Reserved – 2	2 [Value = 0x03E8]	4
Reserved – 3	22 [Value = 0xFF …]	6
Firmware Configuration Option	4 [Value = 0x00000000]	28

Table 10 - Data Structure of the Firmware Configuration Record

Firmware Configuration Option:
Firmware Configuration is a 32 bit value. Each of its bits enables or disables a feature in the firmware. The following is the bit definition for the same.

Bit	Feature Description
0	*Reserved for internal use*
1	*Reserved for internal use*
2	0 – Enables EasyDESFire Mode 1 – Disables EasyDESFire Mode i.e., Enables Transparent Mode
3	0 – Enables Memory Cards 1 – Disables Memory Cards Applicable to ISO14443-3 & ISO15693 cards
4	*Reserved for internal use*
5	*Reserved for internal use*
6	*Reserved for internal use*
7	*Reserved for internal use*
8	*Reserved for internal use*
9	*Reserved for internal use*
10-31	*Reserved for future use*

Table 11 - Bit definition of the Firmware Configuration Option

The default firmware contains a value of 0x00000000.

5 Key Management

The Multi-ISO HF RS232 Reader/Writer provides provision to store card keys in the non-volatile area of the reader/writer. The reader can be customized to store card keys. An authenticated user can later refer to them during card communication using key numbers. This section describes the commands used to achieve this functionality in detail.

5.1 Reader Authentication

The Reader Authenticate command is used to authenticate with the reader/writer. The PIN code specified in the command is verified with the PIN stored in the reader/writer.

Only after a successful Reader Authenticate, the user can use the Load Keys command to store card specific keys or modify the Reader PIN in the non-volatile area of the reader/writer. The default Reader PIN is “00 00 00 00 00 00 00 00”.

The command is used to ensure that a malicious user does not gain access to modify the Card keys or Reader PIN stored in the reader/writer.

Command Format:

Header		*Length*	*LCS*	*Command Opcode*	*Command Data*		*DCS*
0D	0A	000B	F5	83	RFU (2 bytes) [Value = 0000]	Reader PIN (8 bytes)	xx

Response Format:

Header		*Length*	*LCS*	*Status Byte*	*Response Data*	*DCS*
0D	0A	0001	FF	00	-	00

Status Conditions:
The following specific status conditions are possible:

- 01 – Length of command received does not match the expected length
- 8C – Authentication failed. The Reader PIN did not match

Note: The Authentication state will be cleared immediately after the first Load Keys command following the Reader Authenticate command, irrespective of whether the Load Keys command was successful or not. The user will have to authenticate with the reader/writer before issuing each Load Keys command.

5.2 Load Keys

The Load Keys command is used to store MIFARE keys, DESFire keys and Reader PIN into the non-volatile area of the reader/writer.

The User must use Reader Authenticate command (described in section Reader Authentication) to authenticate with the reader/writer before using this command

The reader/writer has provision to store 1 Reader PIN, 80 MIFARE Keys along with Key type and 8 DESFire TDES keys (1 PICC Master key and 7 Application keys) along with AID, PCD Key number and PICC Key number.

When a card specific Authenticate APDU is received from the HOST, the appropriate keys are fetched from the non-volatile and used for Authentication

Command Format:

Header		Length	LCS	Command Opcode	Command Data		DCS
0D	0A	Length of Command Data + 01	xx	82	Card Type (1 byte)	Key Data	xx

Response Format:

Header		Length	LCS	Status Byte	Response Data	DCS
0D	0A	0001	FF	00	-	00

Status Conditions:
The following specific status conditions are possible:

- 8A – Reader Authentication not done
- 80 – Command parameter is invalid

Note: The user must make sure that he uses the Load Keys command to store the appropriate keys (MIFARE or DESFire) in the reader/writer before trying to issue an Authenticate APDU to the respective card.

5.2.1 Load Reader Authentication PIN to Reader

The Following is the Load Keys command format to change the reader PIN. The Reader PIN can be any 8 byte numeric value

Command Data:

Header		Length	LCS	Command Opcode	Command Data		DCS
0D	0A	000A	F6	82	FF	Reader PIN (8 bytes)	xx

Example:
Change Reader PIN in the reader

Command: 0D 0A 0A 00 F6 82 FF 01 02 03 04 05 06 07 08 5B
Response: 0D 0A 01 00 FF 00 00

5.2.2 Load MIFARE Authentication Keys to Reader

The following is the Load Keys command format to load the MIFARE authentication keys into the reader

Command Data:

Header		Length	LCS	Command Opcode	Command Data		DCS
0D	0A	000A	F6	82	00	MIFARE Key data (as shown below)	xx

MIFARE Key Data		
Key Number (1 byte)	Key Type (1 byte)	Key (6 bytes)

Where,

Key Number - any value from 00 to 4F
Key Type - 60 (Key Type A) or 61 (Key Type B)

Example:
Load MIFARE Key with Key Number = 00 & Key Type = 60

Command: 0D 0A 0A 00 F6 82 00 00 60 FF FF FF FF FF FF 24
Response: 0D 0A 01 00 FF 00 00

5.2.3 Load DESFire Authentication Keys to Reader

The following is the Load Keys command format to load DESFire authentication keys into the reader

Command Data:

Header		*Length*	*LCS*	*Command Opcode*	*Command Data*		*DCS*
0D	0A	001F	E1	82	01	DESFire Key data (as shown below)	xx

DESFire Key Data					
PCD Key No (1 byte)	AID (3 bytes)	PICC Key No (1 byte)	Key1 (8 bytes)	Key2 (8 bytes)	Key3 (8 bytes)

Where,

PCD Key No - any value from 00 to 07

- Key no 00 refers to PICC Master Key
- Key no's 01 to 07 refer to Application Keys

AID - Application identifier in the card to which the Key belongs

- Must be 000000 for PICC Master Key

PICC Key No - Key No to be used in the DESFire Authenticate command
Key1-2-3 - It can be a DES/TDES or an AES Key

- DES Key : (Key1 = Key2)
- TDES Key : (Key1 ≠ Key2); (Key1 = Key3)
- AES Key : (Key3 = All zeros)

Note: We do not support 3KTDES as of now.

Example 1:
Loading TDES PICC Master Key with, AID = '000000', PCD Key No = 00, PICC Key No = 00

Command: 0D 0A 1F 00 E1 82 01 00 00 00 00 00 11 22 33 44 55 66 77 88 12 34 56 78 12 34 56 78 11 22 33 44 55 66 77 88 8D
Response: 0D 0A 01 00 FF 00 00

Example 2:
Loading TDES PICC Application Key with, AID = 'C1B1A1', PCD Key No = 01, PICC Key No = 00

Command: 0D 0A 1F 00 E1 82 01 01 A1 B1 C1 00 11 22 33 44 55 66 77 88 12 34 56 78 87 65 43 21 11 22 33 44 55 66 77 88 3D
Response: 0D 0A 01 00 FF 00 00

Example 3:
Loading AES PICC Application Key with, AID = 'C3C2C1', PCD Key No = 02, PICC Key No = 01

Command: 0D 0A 1F 00 E1 82 01 02 C1 C2 C3 01 AA AA AA AA BB BB BB BB CC CC CC CC EE EE EE EE 00 00 00 00 00 00 00 00 34
Response: 0D 0A 01 00 FF 00 00

Note: RdrLoadKeys will fail if any of the command parameters is invalid.

Load MIFARE Plus Authentication Keys in to Reader

The following is the Load Keys command format to load MIFARE Plus AES authentication keys into the reader

Command Data:

CLA	*INS*	*P1*	*P2*	*Lc*	*Data*			*Le*
FF	00	00	00	12	07	03	MIFARE Plus Key data (as shown below)	-

MIFARE Plus Key data:

PCD Key No (1 byte)	*PICC Key Block No (LSB)*	*PICC Key Block No (MSB)*	*KEY Data (16 bytes)*
See PCD Key No. table below	Refer to [R13] fro definition	Refer to [R13] for definition	AES Key

PCD Key Number:

PCD Key number determines the location where the key is being stored in the non-volatile memory of the reader

PCD Key Number	*Key description*
0x00 – 0x0D	SL3 AES Sector Keys
0x00 – 0x09	Special Keys (Refer to [R13] and [R14]for details)

PICC Key block number will be used to identify the type of key being loaded

Up to 14 AES sector keys and all special keys can be stored in the non-volatile memory of the reader using this command. Care should be taken to load keys at different locations by changing the PCD Key number or otherwise the keys will be overwritten and only the last loaded key will be available. AES sector keys and special keys do not share same memory space.

Example 1:

Loading SL3 AES sector key for → Sector 1; Key A; PCD Key No. = 1;
Key = 0x11223344556677881234567812345678

Command: FF 00 00 00 15 07 03 01 02 40 11 22 33 44 55 66 77 88 12 34 56 78 12 34 56 78 00
Response: 90 00

Example 2:

Loading Card Master Key (a special key) → PCD Key No. = 1;
Key = 0x11223344556677888877665544332211

Command: FF 00 00 00 15 07 03 01 00 90 11 22 33 44 55 66 77 88 88 77 66 55 44 33 22 11 00
Response: 90 00

Note: RdrLoadKeys will fail if any of the command parameters is invalid

Load MIFARE ULC Authentication Keys in to Reader

The following is the Load Keys command format to load MIFARE ULC authentication keys into the reader

Command Data:

CLA	*INS*	*P1*	*P2*	*Lc*	*Data*			*Le*
FF	00	00	00	12	07	04	MIFARE ULC Key data (16bytes as shown below)	-

Example:
Loading MIFARE ULC keys in to the reader, Key1 = 49454D4B41455242, Key2 = 214E4143554F5946

Command: FF 00 00 00 12 07 04 49 45 4D 4B 41 45 52 42 21 4E 41 43 55 4F 59 46
Response: 90 00

Note: RdrLoadKeys will fail if any of the command parameters is invalid

6 Accessing Cards through e-PC/SC

The e-PC/SC protocol supports proprietary 7816 wrappers to aid working with “false“ smartcards, i.e., with memory cards or even microprocessor based cards not following the ISO 7816-4 standard (APDU formalism) in their command structure

The proprietary wrapped card commands are called Pseudo APDUs (Refer to [R7] in order to understand the basic structure of APDU). The SCardTransmit command is used to send these Pseudo APDUs to the reader and receive the response from the card in the format described in this section.

MIFARE cards and ISO 15693 cards use proprietary 7816 APDU structures. DESFire cards use the 7816 wrapper as described in the DESFire specifications [R3] & [R11]

All command and response bytes are sent and received as hexadecimal values respectively

Note: In the pseudo APDUs described in this section, specifying a value of 00 in the **Le** field indicates maximum no of available response bytes from the card, as described in reference [R7]

6.1 MIFARE Cards

Pseudo APDUs supported for MIFARE cards are explained in this section.

6.1.1 Authenticate

This APDU performs three pass authentication with the card for the Block No. specified in the data field. It uses the Key at the Key no specified.

***Command APDU*:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Data*	*Le*
FF	86	00	00	05	See Table below (5 bytes)	-

Data:

Byte 1	*Byte 2*	*Byte 3*	*Byte 4*	*Byte 5*
01	Block No (MSB)	Block No (LSB)	00	Key No.

Where,

Block No - Block number in the MIFARE card which is to be authenticated
Key No - Key Number specified in the RDRLoadKeys command to store the corresponding Authentication key in the non-volatile area of the reader/writer

Response:

Data	*Status*	
-	SW1	SW2

For possible values and description of status word, refer Table 16.

6.1.2 Write Binary

This APDU writes data to the Block No. specified.

***Command APDU*:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Data*	*Le*
FF	D6	00	MIFARE Block No	10	Data to Card	-

Response:

Data	*Status*	
-	SW1	SW2

For possible values and description of status word, refer Table 16.

6.1.3 Read Binary

This APDU reads data from the Block No. specified

***Command APDU*:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Data*	*Le*
FF	B0	00	MIFARE Block No	-	-	Expected no of bytes from card

Response:

Data	*Status*	
Data from the specified block in the MIFARE card	SW1	SW2

For possible values and description of status word, refer Table 16.

6.1.4 Value Increment

This APDU increments the data in a Value block, using the 4 byte value specified.

***Command APDU*:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Data*			*Le*
FF	FC	00	00	06	C1	MIFARE Block No	4 bytes of value to be added to the block value (LSB first)	-

Response:

Data	*Status*	
-	SW1	SW2

For possible values and description of status word, refer Table 16.

6.1.5 Value Decrement

This APDU decrements the data in a Value block, using the 4 byte value specified.

***Command APDU*:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Data*			*Le*
FF	FC	00	00	06	C0	MIFARE Block No	4 bytes of value to be subtracted from the block value (LSB first)	-

Response:

Data	*Status*	
-	SW1	SW2

For possible values and description of status word, refer Table 16.

6.1.6 Value Restore

This APDU copies the data present in the data register of the MIFARE card into the Value block. Technically, this command has no significance.

***Command APDU*:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Data*			*Le*
FF	FC	00	00	06	C2	MIFARE Block No	4 bytes of value (no significance)	-

Response:

Data	*Status Word*	
-	SW1	SW2

For possible values and description of status word, refer Table 16.

Note:

1. The Pseudo APDUs for **Authenticate**, **Write Binary** and **Read Binary** described in this section are as defined in the **PC/SC v2.01.09**, Part3: Requirements for PC connected Interface Devices, under section 3.2.2.1
2. For all the value operations in the MIFARE card, Transfer command need not be sent from the application, as the reader implicitly performs it.

6.2 MIFARE ULC Cards

Pseudo APDUs supported for MIFARE ULC cards are explained in this section

6.2.1 Authenticate

This APDU performs three pass authentication with the card. It uses the Key, which is loaded into the reader using RdrLoadKeys command.

***Command* APDU:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Data*	*Le*
FF	86	00	00	05	0x0000000000	-

Response:

Data	*Status Word*	
-	SW1	SW2

For possible values and description of status word, refer Table 16.

6.2.2 Write Binary (16 Bytes)

This APDU writes data to the MIFARE ULC block no. specified

***Command* APDU:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Data*	*Le*
FF	D6	00	MIFARE ULC Block No	10	Data to Card	-

Response:

Data	*Status Word*	
-	SW1	SW2

For possible values and description of status word, refer Table 16.

6.2.3 Write Binary (4 Bytes)

This APDU writes data to the MIFARE ULC block no. specified

***Command* APDU:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Data*	*Le*
FF	D6	00	MIFARE ULC Block No	04	Data to Card	-

Response:

Data	*Status Word*	
-	SW1	SW2

For possible values and description of status word, refer Table 16.

6.2.4 Read Binary

This APDU reads data from the MIFARE ULC block no. specified

***Command* APDU:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Data*	*Le*
FF	B0	00	MIFARE Block No	-	-	00 (or) 10

Response:

Data	*Status Word*	
16 Bytes of data	SW1	SW2

Note:

3. The Pseudo APDUs for **Authenticate**, **Write Binary** and **Read Binary** described in this section are as defined in the **PC/SC v2.01.09**, Part3: Requirements for PC connected Interface Devices, under section 3.2.2.1
4. For all the value operations in the MIFARE card, Transfer command need not be sent from the application, as the reader implicitly performs it.

6.3 my-D Move Cards

Pseudo APDUs supported for My-D Move cards are explained in this section

6.3.1 Access

This APDU performs password verification with the My-D move card,

***Command* APDU:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Command*	*Password*	*Le*
FF	FD	04	01	05	B2	4 Bytes	00

Response:

Data	*Status Word*	
-	SW1	SW2

For possible values and description of status word, refer Table 16.

6.3.2 Set Password

This APDU changes password in My-D move card with the new password value specified in command

***Command* APDU:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Command*	*Password*	*Le*
FF	FD	04	01	05	B1	4 Bytes	00

Response:

Data	*Status Word*	
-	SW1	SW2

For possible values and description of status word, refer Table 16.

6.3.3 Compatibility Write

This APDU writes 4 bytes of data to the My-D Move block no. specified

***Command* APDU:**

CLA	INS	P1	P2	Lc	Command	Block No.	Data	Le
FF	FD	06	01	12	A0	1 Byte	16 Bytes	00

Response:

Data	Status Word	
-	SW1	SW2

For possible values and description of status word, refer Table 16.

6.3.4 Write 2 Blocks (8 Bytes)

This APDU writes 8 bytes of data to the My-D Move block no. specified

***Command* APDU:**

CLA	INS	P1	P2	Lc	Command	Block No.	Data	Le
FF	FD	06	01	0A	A1	1 Byte	8 Bytes	00

Response:

Data	Status Word	
-	SW1	SW2

For possible values and description of status word, refer Table 16.

6.3.5 Write 1 Block (4 Bytes)

This APDU writes 4 bytes of data to the My-D Move block no. specified

***Command* APDU:**

CLA	INS	P1	P2	Lc	Command	Block No.	Data	Le
FF	FD	04	01	06	A2	1 Byte	4 Bytes	00

Response:

Data	Status Word	
-	SW1	SW2

For possible values and description of status word, refer Table 16.

6.3.6 Read 4 Blocks (16 Bytes)

This APDU reads 16 bytes of data from My-D Move block no. specified

***Command* APDU:**

CLA	INS	P1	P2	Lc	Command	Block No.	Le
FF	FD	01	01	02	30	1 Byte	00

Response:

Data	Status Word	
16 Bytes of data	SW1	SW2

For possible values and description of status word, refer Table 16.

6.3.7 Read 2 Blocks (8 Bytes)

This APDU reads 8 bytes of data from My-D Move block no. specified

***Command* APDU:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Command*	*Block No.*	*Le*
FF	FD	01	01	02	31	1 Byte	00

Response:

Data	*Status Word*	
8 Bytes of data	SW1	SW2

6.3.8 Decrement

This APDU decrements counter value of My-D move by the value specified in the command

***Command* APDU:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Command*	*Decrement value*	*Le*
FF	FD	06	01	03	D0	2 Bytes	00

Response:

Data	*Status Word*	
-	SW1	SW2

For possible values and description of status word, refer Table 16.

6.4 ISO 15693 Cards

Pseudo APDUs supported for ISO 15693 cards are explained in this section.

6.4.1 Read Single Block

This APDU reads 4 bytes of data from the Block No. specified.

***Command APDU*:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Data*	*Le*
FF	FC	00	00	No of bytes in Data field	Read single block command as described in reference [R1]	Expected no of bytes from card

Response:

Data	*Status*	
Read single block response as described in reference [R1]	SW1	SW2

For possible values and description of status word, refer Table 16.

6.4.2 Write Single Block

This APDU writes 4 bytes of data to the Block No specified.

***Command APDU*:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Data*	*Le*
FF	FC	00	00	No of bytes in Data field	Write single block command as described in reference [R1]	-

Response:

Data	*Status*	
Write single block response as described in reference [R1]	SW1	SW2

For possible values and description of status word, refer Table 16.

6.4.3 Lock Block

This APDU Locks the specified Block No. Once successfully locked, the block will become read only.

***Command APDU*:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Data*	*Le*
FF	FC	00	00	No of bytes in Data field	Lock block command as described in reference [R1]	-

Response:

Data	*Status*	
Lock block response as described in reference [R1]	SW1	SW2

For possible values and description of status word, refer Table 16.

6.4.4 Read Multiple Blocks

This APDU reads 4 bytes of data from each of the requested no of blocks, starting from the block no specified.

***Command APDU*:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Data*	*Le*
FF	FC	00	00	No of bytes in Data field	Read multiple block command as described in reference [R1]	Expected no of bytes from card

Response:

Data	*Status*	
Read multiple block response as described in reference [R1]	SW1	SW2

For possible values and description of status word, refer Table 16

6.4.5 Write AFI

This APDU writes the AFI value specified into the card's memory.

***Command APDU*:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Data*	*Le*
FF	FC	00	00	No of bytes in Data field	Write AFI command as described in reference [R1]	-

Response:

Data	*Status*	
Write AFI response as described in reference [R1]	SW1	SW2

For possible values and description of status word, refer Table 16.

6.4.6 Write DSFID

This APDU writes the DSFID value specified into the card's memory.

***Command APDU*:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Data*	*Le*
FF	FC	00	00	No of bytes in Data field	Write DSFID command as described in reference [R1]	-

Response:

Data	*Status*	
Write DSFID response as described in reference [R1]	SW1	SW2

For possible values and description of status word, refer Table 16.

6.4.7 Get System Information

This APDU retrieves system information, like UID; DSFID; AFI; Memory information; IC Manufacturer code, from the card.

***Command APDU*:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Data*	*Le*
FF	FC	00	00	No of bytes in Data field	Get system information command as described in reference [R1]	Expected no of bytes from card

Response:

Data	*Status*	
Get system information response as described in reference [R1]	SW1	SW2

For possible values and description of status word, refer Table 16.

6.4.8 Get Multiple Block Security Status

This APDU retrieves the block security status of each of the requested no of blocks, starting from the block no specified.

***Command APDU*:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Data*	*Le*
FF	FC	00	00	No of bytes in Data field	Get multiple block security status command as described in reference [R1]	00

Response:

Data	*Status*	
Get multiple block security status response as described in reference [R1]	SW1	SW2

For possible values and description of status word, refer Table 16.

Note: In all the above 15693 card commands, the optional the **Flags** byte and optional **UID** field must be omitted. In all the above 15693 card responses, **Flags** byte will be omitted and **Error Code** (if any) will be sent as SW2

6.5 Crypto RF Cards

Pseudo APDUs supported for Atmel CryptoRF cards are explained in this section.

6.5.1 Set User Zone

This APDU selects the specified user Zone. All further user zone operations will be done in the selected user zone. The command is also used to enable anti-tearing mode, following which all writes to this user zone will use anti-tearing.

***Command APDU*:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Data*	*Le*
FF	FC	00	00	No of bytes in Data field	Set User Zone Command as per reference [R10]	-

Response:

Data	*Status*	
Set User Zone responseas per reference [R10]	SW1	SW2

For possible values and description of status word, refer Table 16.

6.5.2 Read User Zone

This APDU reads data from the currently selected user zone.

***Command APDU*:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Data*	*Le*
FF	FC	00	00	No of bytes in Data field	Read User Zone Command as per reference [R10]	Expected no of bytes from card

Response:

Data	*Status*	
Read User Zone response as per reference [R10]	SW1	SW2

For possible values and description of status word, refer Table 16.

6.5.3 Write User Zone

This APDU writes data to the currently selected user zone. In anti-tearing mode the maximum no of bytes that can be written is 8 bytes.

***Command APDU*:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Data*	*Le*
FF	FC	00	00	No of bytes in Data field	Write User Zone Command as per reference [R10]	-

Response:

Data	*Status*	
Write User Zone response as per reference [R10]	SW1	SW2

For possible values and description of status word, refer Table 16.

6.5.4 Read System Zone

This APDU reads system data from the configuration memory of the card. Depending on the value of the PARAM byte (part of the command), this command may read data from the configuration zone, the fuses or a checksum.

***Command APDU*:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Data*	*Le*
FF	FC	00	00	No of bytes in Data field	Read System Zone Command as per reference [R10]	Expected no of bytes from card

Response:

Data	*Status*	
Read System Zone response as per reference [R10]	SW1	SW2

For possible values and description of status word, refer Table 16.

6.5.5 Write System Zone

This APDU writes data to the configuration memory. Depending on the value of the PARAM byte (part of the command), this command may write data to the configuration zone or program fuses. The anti-tearing mode can also be enabled using the PARAM byte. The maximum number of bytes that can be written in anti-tearing mode is 8 bytes.

***Command APDU*:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Data*	*Le*
FF	FC	00	00	No of bytes in Data field	Write System Zone Command as per reference [R10]	-

Response:

Data	*Status*	
Write System Zone response as per reference [R10]	SW1	SW2

For possible values and description of status word, refer Table 16.

6.5.6 Check Password

This APDU is used to send the password for validation against the password selected with the Password index byte (part of the command). This command is used to gain access, to read or write in user zones that require password validation.

***Command APDU*:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Data*	*Le*
FF	FC	00	00	No of bytes in Data field	Check Password Command as per reference [R10]	-

Response:

Data	*Status*	
Check Password response as per reference [R10]	SW1	SW2

For possible values and description of status word, refer Table 16.

Note: In all the above CryptoRF card commands, the **CID** field (higher nibble of the command byte), must be set to 0. In all the above CryptoRF card responses, the **Command** byte and **ACK/NACK** byte will be omitted. **Status** byte will be sent as SW2.

6.6 DESFire Cards

In the Multi-ISO reader there are two modes in which one could communication with a DESFire card. They are:

a) EasyDESFire Mode
b) Transparent Mode

In both of the above modes, knowledge on DESFire specification (as per reference [R3]) is a mandate.

EasyDESFire Mode

In the EasyDESFire mode, the application has to just follow the 7816-4 APDU wrapper command set as described in the DESFire specification. The reader would internally take care of all the necessary cryptographic operations and key management.

In order to activate this mode, bit-2 of Firmware Configuration Option (described in section Firmware Configuration Data Structure) has to be cleared using the Set Firmware Configuration command.

Note:

1. "Change Key" commands need special data formatting for DES/TDES, 3KTDES, AES keys.

   If you need to modify a DES/TDES or 3KTDES key in the card, the following is the command format.

CLA	INS	P1	P2	Lc	Data	Le
FF	C4	00	00	19	24 Byte Key Data	00

   If you need to modify an AES key in the card, the following is the command format.

CLA	INS	P1	P2	Lc	Data	Le
FF	C4	00	00	12	16 Byte Key Data + 1 Byte Key Version	00

2. In order to perform an authentication with the changed key, one has to load the changed Key in the reader's non volatile memory using the Load Key command.

3. The following are the reader specific DESFire error codes,

Status Word (HEX)		Description
SW1	SW2	
91	7C	Specified Key does not exist in the PCD
91	7D	Buffer size exceeds PCD limit

Table 12 - DESFire custom error codes

Transparant Mode

In this mode, the application has to perform all the necessary cryptographic operations as required by the DESFire card.

In order to activate this mode, bit-2 of Firmware Configuration Option (described in section Firmware Configuration Data Structure) has to be set using the Set Firmware Configuration command.

6.7 MIFARE Plus Cards

At security level 1, MIFARE plus cards behave just like MIFARE cards and hence all the commands supported for MIFARE cards will work as is when card is in this mode.

Commands listed here are supported for both MIFARE Plus S and X cards based on the applicability.

6.7.1 AES Authenticate

This APDU is used to authenticate with the card in order to obtain access to secured data sectors. Based on the key block number, authentication effect would be different. For details refer to [R13]. This is common to all security levels

***Command* APDU:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Opcode*	*Key block number (LSB)*	*Key block number (MSB)*	*Le*
FF	FB	00	00	03	0x76	Refer to [R13] and [R14] for definition	Refer to [R13] and [R14] for definition	0

Response:

Status Word	
SW1	SW2

This command can be issued when the card is in any security level. Based on the security level and the key block number, the authentication will be done. Find in the below table possible authentications that can be done using this command

Security Level	*Key Block No.*	*Authentication purpose*
SL0/SL1/SL2/SL3	Originality Key Block No.	To check the originality of the card chip
SL1	SL1 AES Authentication Key	To perform additional AES authentication when the card is in SL1 mode
SL2/SL3	AES Sector Key	To perform AES authentication when the card is in SL2/SL3 mode
SL1	Security Level 2 switch Key	To switch to security level 2
SL1/SL2	Security Level 3 switch Key	To switch to security level 3
SL2/SL3	Card Master Key	To perform authentication in order to modify the card master key, card configuration key, Installation Identifier or ATS
SL2/SL3	Card Configuration Key	To perform authentication in order to modify the Field configuration block, card configuration key and Virtual Card keys
SL2/SL3	Virtual Card Polling Enc Key	Refer to [R13] & [R14] for details
SL2/SL3	Virtual Card Polling MAC Key	
SL2/SL3	Select Virtual Card Key	
SL2SL3	Proximity Check Key	

Table 13 – Possible MIFARE Plus authentications

For possible values and description of status word, refer Table 16.

6.7.2 SL1 Commands

SL1 communication is same as that of standard MIFARE classic, as described in section MIFARE Cards.

Optionally SL1 AES authentication can also be done as described in section AES Authenticate of MIFARE Plus Cards.

6.7.3 SL2 Commands

Below are the APDUs that PCD supports for MIFARE plus SL2 cards.

Authenticate

SL2 authentication is same as that of standard MIFARE classic authentication procedure as described in section Authenticate of MIFARE Cards. Before doing this authentication both AES sector key and the MIFARE classic sector key should be loaded into PCD. PCD will internally do both the authentications.

Optionally AES authentication can also be done separately as described in section AES Authenticate of MIFARE Plus Cards.

Read

SL2 read is same as that of standard MIFARE classic read procedure as described in section Read Binary of MIFARE Cards. For Multiblock read, following command/response pair is used.

***Command* APDU:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Opcode*	*Block number*	*No. of Blks to read*	*Le*
FF	FD	01	02	03	38	00 to FF	1 to FF (sector trailers not counted)	0

Response:

Data read from the card	*Status Word*	
(No. of blks * 16) bytes	SW1	SW2

For possible values and description of status word, refer Table 16.

Write

SL2 write is same as that of standard MIFARE classic read procedure as described in section Write Binary of MIFARE Cards. For Multiblock write, following command/response pair is used.

***Command* APDU:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Opcode*	*Block number*	*Number of blocks*	*Data to write*	*Le*
FF	FB	00	00	3 + (Length of data bytes to be written)	A9	00 to FF	01 to 03	16 * number of blocks	0

Response:

Status Word	
SW1	SW2

6.7.4 SL3 Generic Commands

Below are the APDUs that PCD supports for MIFARE plus SL3 cards.

Authentication

SL3 AES authentication is done as described in section AES Authenticate of MIFARE Cards.

Reset Authentication

This APDU is used to reset the authenticated status obtained by a successful authenticate command. For details refer to [R13]

***Command* APDU:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Opcode*	*Le*
FF	FB	00	00	03	0x78	0

Response:

Status Word	
SW1	SW2

For possible values and description of status word, refer Table 16.

Read

This APDU is used to read data from the card in SL3.

***Command* APDU:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Opcode*	*Block number (LSB)*	*Block number (MSB)*	*No. of Blks to read*	*Le*
FF	FB	00	00	04	Refer to [R13] and [R14] for definition	Refer to [R13] and [R14] for definition	Refer to [R13] and [R14] for definition	1 to 216 (sector trailers not counter)	0

Response:

Data read from the card	*Status Word*	
(No. of blks * 16) bytes	SW1	SW2

For possible values and description of status word, refer Table 16.

Write

This APDU is used to write data to the card in SL3.

***Command* APDU:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Opcode*	*Block number (LSB)*	*Block number (MSB)*	*Data to write*	*Le*
FF	FB	00	00	3 + (Length of data bytes to be written)	Refer to [R13] and [R14] for definition	Refer to [R13] and [R14] for definition	Refer to [R13] and [R14] for definition	16/32/48 bytes	0

Response:

Status Word	
SW1	SW2

For possible values and description of status word, refer Table 16.

6.7.5 SL3 Value Operation commands

These APDUs are used to do value operations on MIFARE plus SL3 card,

Increment and decrement operations

This APDU is used to increment or decrement the value in the value block. Transfer command must be sent for the increment/decrement operation to be permanent in card. If restore is used after increment/decrement operation will be temporary.

***Command* APDU:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Opcode*	*Block number (LSB)*	*Block number (MSB)*	*Increment or decrement Data*	*Le*
FF	FB	00	00	07	Refer to [R13] and [R14] for definition	Refer to [R13] and [R14] for definition	Refer to [R13] and [R14] for definition	4 Bytes (LSB first)	0

Response:

Status Word	
SW1	SW2

For possible values and description of status word, refer Table 16.

Increment transfer and decrement transfer operations

This APDU is used to increment/decrement value in value block. As the command name indicates no external transfer command is needed for the transaction to be permanent.

***Command* APDU:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Opcode*	*Source Block number (LSB)*	*Source Block number (MSB)*	*Destination Block number (LSB)*	*Destination Block number (MSB)*	*Increment or decrement Data*	*Le*
FF	FB	00	00	09	Refer to [R13] and [R14] for definition	Refer to [R13] and [R14] for definition	Refer to [R13] and [R14] for definition	Refer to [R13] and [R14] for definition	Refer to [R13] and [R14] for definition	4 Bytes (LSB first)	0

Response:

Status Word	
SW1	SW2

For possible values and description of status word, refer Table 16.

Transfer and restore operations

This APDU is used to make increment/decrement operations to be permanent in the card

***Command* APDU:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Opcode*	*Block number (LSB)*	*Block number (MSB)*	*Le*
FF	FB	00	00	03	Refer to [R13] and [R14] for definition	Refer to [R13] and [R14] for definition	Refer to [R13] and [R14] for definition	0

Response:

Status Word	
SW1	SW2

For possible values and description of status word, refer Table 16.

6.7.6 SL3 Virtual Card commands

These APDUs are used to do virtual card related operations on MIFARE plus SL3 card.

Write IID

This APDU is used to write card specific IID to the card.

***Command* APDU:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Opcode*	*IID Block number (LSB)*	*IID Block number (MSB)*	*Card IID*	*Le*
FF	FB	00	00	13	A1	01	B0	16 Bytes	0

Response:

Status Word	
SW1	SW2

For possible values and description of status word, refer Table 16.

Virtual card support

This APDU is used to check if the IID is registered in the card or not.

***Command* APDU:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Opcode*	*Card IID*	*Le*
FF	FB	00	00	11	42	16 Bytes	0

Response:

Status Word	
SW1	SW2

For possible values and description of status word, refer Table 16.

Virtual card support last

This APDU is used to get UID and PICC capabilities from the card.

***Command* APDU:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Opcode*	*Card IID*	*Le*
FF	FB	00	00	11	4B	16 Bytes	0

Response:

Status Word	
SW1	SW2

For possible values and description of status word, refer Table 16.

Select virtual card

This APDU is used to select the card with the UID retrieved in the previous command.

***Command* APDU:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Opcode*	*PICC capabilities*	*Card UID*	*Le*
FF	FB	00	00	07 (or) 0A depends on UID size	40	2 Bytes	4 (or) 7 Bytes	0

Response:

Status Word	
SW1	SW2

For possible values and description of status word, refer Table 16.

Deselect virtual card

This APDU is used to deselect the card which is selected in the previous command.

***Command* APDU:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Opcode*	*Le*
FF	FB	00	00	01	48	0

Response:

Status Word	
SW1	SW2

For possible values and description of status word, refer Table 16.

6.7.7 SL3 Proximity check commands

These APDUs are used to do proximity checks with the card.

Proximity check enable

This APDU is used to make proximity check mandatory for all the transactions in the card.

***Command* APDU:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Opcode*	*Proximity check config Block Number(LSB)*	*Proximity check config Block Number(MSB)*	*Data To enable Proximity Check*	*Le*
FF	FB	00	00	13	A1	03	B0	0055AA00000000000000000000000000000	0

Response:

Status Word	
SW1	SW2

For possible values and description of status word, refer Table 16.

Proximity check

This APDU is used to do proximity chek in the proximity check enabled cards.

***Command* APDU:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Opcode*	*Le*
FF	FB	00	00	01	F0	0

Response:

Status Word	
SW1	SW2

For possible values and description of status word, refer Table 16.

Proximity check disable

This APDU is used to disable mandatory proximity check for card communication.

***Command* APDU:**

CLA	*INS*	*P1*	*P2*	*Lc*	*Opcode*	*Proximity check config Block Number(LSB)*	*Proximity check config Block Number(MSB)*	*Data To disable Proximity Check*	*Le*
FF	FB	00	00	13	A1	03	B0	005555000000 000000000000 00000000	0

Response:

Status Word	
SW1	SW2

For possible values and description of status word, refer Table 16.

6.8 Generic APDUs

This section describes the generic Pseudo APDUs used with different type of cards.

6.8.1 Get UID

This APDU retrieves the card Unique ID (UID). Length of the UID varies depending on the card.

***Command APDU*:**

CLA	INS	P1	P2	Lc	Data	Le
FF	CA	00	00	-	-	00

Response:

Data	Status	
UID of the Card	SW1	SW2

For possible values and description of status word, refer Table 16.

6.8.2 Traverse

This APDU is used to send the “Raw Card Command“ in the data field to the card, without any command specific processing by the reader/writer and returns the response data from the Card. The reader/writer only takes care of the protocol specific processing (CRC, Prologue field etc ...). This command is mainly used for sending ISO15693 custom commands. For more details, refer Section 6.

The reader/writer uses the Frame type specified in the P2 parameter field and the Frame waiting time specified in the P1 parameter field, while sending the command and receiving the response, respectively.

***Command APDU*:**

CLA	INS	P1	P2	Lc	Data	Le
FF	FD	FWT (as defined in the table 9)	Frame Type (as defined in the table 10)	No of data bytes sent to the card	Raw Card Command	00

FWT Code	FWT (in microseconds)
00	500
01	1000
02	2000
03	5000
04	10000
05	25000
06	50000
07	75000
08	100000
09	250000
0A	500000
0B	750000
0C	1000000
0D	1250000
0E	1500000
0F	1750000
10	2000000
11	2500000
12	3000000
13	4000000
14	5000000

Table 14 - List of FWT codes

Frame Type	Description
00	FRAMETYPE_SHORT
01	FRAMETYPE_STD
01	FRAMETYPE_ACBITORIENTED

Table 15 - Frame Type

Response:
The response from the card is returned as such without any processing. Reception of any response from the card is considered as success irrespective of the content of the response

Data	***Status***	
Response from Card	SW1	SW2

For possible values and description of status word, refer Table 16.

6.9 Status Word

Status Word (HEX)		Description
SW1	SW2	
90	00	Command Successful
63	00	Reason for error unknown
69	83	Authentication is required to access the block in the card
69	82	Block's security status prevents access
69	88	Wrong key no. was specified to authenticate with the block
67	00	Length parameter in the APDU is wrong
68	00	Class byte in the APDU is wrong
6B	00	Invalid parameter in the APDU
6A	81	Command requested is not supported
6C	xx	Wrong Le field. Actual Le is mentioned in place of xx
6F	00	No Precise diagnosis
6D	00	Instruction code not supported or invalid

Table 16 - Status word definitions

7 SDU Samples to Access Cards

The basic card access sequence using would be:

- Connect to the card using **SCardConnect** API
- Send commands to the card using **SCardTransmit** API
- Use **SCardDisconnect** API to disconnect from the card

7.1 How to access MIFARE classic cards?

SCardStatus
Command: 0D 0A 02 00 FE 03 00 FD
Response: 0D 0A 02 00 FE 00 01 xx

SCardConnect
Command: 0D 0A 02 00 FE 01 00 FF
Response: 0D 0A 07 00 F9 00 xx xx xx xx xx xx xx

ReaderAuthenticate (PIN : '0000000000000000')
Command: 0D 0A 0B 00 F5 83 00 00 00 00 00 00 00 00 00 00 7D
Response: 0D 0A 01 00 FF 00 xx

MIFARE Load Keys (PCD Key No. : 24, Key Type : Key A)
Command: 0D 0A 0A 00 F6 82 00 24 60 FF FF FF FF FF FF 00
Response: 0D 0A 01 00 FF 00 xx

Authenticate (Block No. : 001E, PCD Key No. : 00)
Command: 0D 0A 0C 00 F4 04 00 FF 86 00 00 05 01 00 1E 00 24 2F
Response: 0D 0A 03 00 FD 00 90 00 xx

Read Binary (Block No. : 1E)
Command: 0D 0A 07 00 F9 04 00 FF B0 00 1E 00 2F
Response: 0D 0A 13 00 ED 00 xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx 90 00 xx

Read Binary (Block No. : 1E)
Command: 0D 0A 07 00 F9 04 00 FF B0 00 1E 10 1F
Response: 0D 0A 13 00 ED 00 xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx 90 00 xx

Write Binary (Block No. : 1E)
Command: 0D 0A 17 00 E9 04 00 FF D6 00 1E 10 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 47
Response: 0D 0A 03 00 FD 00 90 00 xx

Read Binary (Block No. : 1E)
Command: 0D 0A 07 00 F9 04 00 FF B0 00 1E 00 2F
Response: 0D 0A 13 00 ED 00 xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx 90 00 xx

Write Binary (Block No. : 1E)
Command: 0D 0A 17 00 E9 04 00 FF D6 00 1E 10 A1 B2 C3 D4 E5 F6 1F 2E 3D 4C 5B 6A BB CC DD EE 47
Response: 0D 0A 03 00 FD 00 90 00 xx

Read Binary (Block No. : 1E)
Command: 0D 0A 07 00 F9 04 00 FF B0 00 1E 00 2F
Response: 0D 0A 13 00 ED 00 xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx 90 00 xx

Prepare Block as value block (Block No. : 1E, Value : 00000064)
Command: 0D 0A 17 00 E9 04 00 FF D6 00 1E 10 64 00 00 00 9B FF FF FF 64 00 00 00 00 FF 00 FF 9B

Response: 0D 0A 03 00 FD 00 90 00 xx

Value Increment (Block No. : 1E)
Command: 0D 0A 0D 00 F3 04 00 FF FC 00 00 06 C1 1E 01 00 00 00 1B
Response: 0D 0A 03 00 FD 00 90 00 xx

Value Decrement (Block No. : 1E)
Command: 0D 0A 0D 00 F3 04 00 FF FC 00 00 06 C0 1E 01 00 00 00 1C
Response: 0D 0A 03 00 FD 00 90 00 xx

SCardDisconnect
Command: 0D 0A 02 00 FE 02 00 FE
Response: 0D 0A 01 00 FF 00 xx

7.2 How to access MIFARE UL cards?

SCardStatus
Command: 0D 0A 02 00 FE 03 00 FD
Response: 0D 0A 02 00 FE 00 01 xx

SCardConnect
Command: 0D 0A 02 00 FE 01 00 FF
Response: 0D 0A 07 00 F9 00 xx xx xx xx xx xx xx

Get Uid
Command: 0D 0A 07 00 F9 04 00 FF CA 00 00 00 33
Response: 0D 0A 0A 00 F6 00 xx xx xx xx xx xx xx 90 00 xx

Read Binary (Block No. : 09)
Command: 0D 0A 07 00 F9 04 00 FF B0 00 09 00 44
Response: 0D 0A 07 00 F9 00 xx xx xx xx 90 00 xx

Write Binary (Block No. : 09)
Command: 0D 0A 0B 00 F5 04 00 FF D6 00 09 04 01 02 03 04 10
Response: 0D 0A 03 00 FD 00 90 00 xx

Read Binary (Block No. : 09)
Command: 0D 0A 07 00 F9 04 00 FF B0 00 09 00 44
Response: 0D 0A 07 00 F9 00 xx xx xx xx 90 00 xx

Write Binary (Block No. : 09)
Command: 0D 0A 17 00 E9 04 00 FF D6 00 09 10 A1 B2 C3 D4 01 01 01 01 01 01 01 01 01 01 01 01 18
Response: 0D 0A 03 00 FD 00 90 00 xx

SCardDisconnect
Command: 0D 0A 02 00 FE 02 00 FE
Response: 0D 0A 01 00 FF 00 xx

7.3 How to access MIFARE ULC cards?

SCardStatus
Command: 0D 0A 02 00 FE 03 00 FD
Response: 0D 0A 02 00 FE 00 01 xx

SCardConnect
Command: 0D 0A 02 00 FE 01 00 FF
Response: 0D 0A 07 00 F9 00 xx xx xx xx xx xx xx

Get Uid
Command: 0D 0A 07 00 F9 04 00 FF CA 00 00 00 33
Response: 0D 0A 06 00 XX 00 XX XX XX XX 90 00 XX

Following four write commands to blocks 2C, 2D, 2E, 2F, changes the key value in card to Key1 = 49454D4B41455242, Key2 = 214E4143554F5946.

Write Binary (Block No. : 2C)
Command: 0D 0A 0B 00 F5 04 00 FF D6 00 2C 04 42 52 45 41 DD
Response: 0D 0A 01 00 FF 00 xx

Write Binary (Block No. : 2D)
Command: 0D 0A 0B 00 F5 04 00 FF D6 00 2D 04 4B 4D 45 49 D0
Response: 0D 0A 01 00 FF 00 xx

Write Binary (Block No. : 2E)
Command: 0D 0A 0B 00 F5 04 00 FF D6 00 2E 04 46 59 4F 55 B2
Response: 0D 0A 01 00 FF 00 xx

Write Binary (Block No. : 2F)
Command: 0D 0A 0B 00 F5 04 00 FF D6 00 2F 04 43 41 4E 21 01
Response: 0D 0A 01 00 FF 00 xx

Reader Authenticate (PIN : '0000000000000000')
Command: 0D 0A 0B 00 F5 83 00 00 00 00 00 00 00 00 00 00 7D
Response: 0D 0A 01 00 FF 00 xx

MIFARE ULC Load Keys
Command: 0D 0A 12 00 EE 82 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7A
Response: 0D 0A 01 00 FF 00 xx

MFUL-C Auth
Command: 0D 0A 0C 00 F4 04 00 FF 86 00 00 05 00 00 00 00 00 72
Response: 0D 0A 03 00 XX 00 90 00 XX

Write Binary (Block No. : 15)
Command: 0D 0A 0B 00 F5 04 00 FF D6 00 15 04 AA BB CC DD 00
Response: 0D 0A 03 00 XX 00 90 00 XX

Write Binary (Block No. : 16)
Command: 0D 0A 17 00 E9 04 00 FF D6 00 16 10 EE FF AB CD 00 00 00 00 00 00 00 00 00 00 00 00 9C
Response: 0D 0A 03 00 XX 00 90 00 XX

Read Binary (Block No. : 15)
Command: 0D 0A 07 00 F9 04 00 FF B0 00 15 00 38
Response: 0D 0A 13 00 XX 00 XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX 90 00 XX

SCardDisconnect
Command: 0D 0A 02 00 FE 02 00 FE
Response: 0D 0A 01 00 FF 00 xx

7.4 How to access My-D Move cards?

SCardStatus
Command: 0D 0A 02 00 FE 03 00 FD
Response: 0D 0A 02 00 FE 00 01 xx

SCardConnect
Command: 0D 0A 02 00 FE 01 00 FF
Response: 0D 0A 07 00 F9 00 xx xx xx xx xx xx xx

Get Uid
Command: 0D 0A 07 00 F9 04 00 FF CA 00 00 00 33
Response: 0D 0A 0A 00 F6 00 XX XX XX XX XX XX XX 90 00 XX

Access (Pass. : 00000000)
Command: 0D 0A 0D 00 F3 04 00 FF FD 04 01 05 B2 00 00 00 00 00 44
Response: 0D 0A 03 00 FD 00 90 00 XX

Set Password (Pass. : 0x12345678)
Command: 0D 0A 0D 00 F3 04 00 FF FD 04 01 05 B1 12 34 56 78 00 31
Response: 0D 0A 07 00 F9 00 XX XX XX XX 90 00 XX

Access (Pass. : 0x12345678)
Command: 0D 0A 0D 00 F3 04 00 FF FD 04 01 05 B2 12 34 56 78 00 30
Response: 0D 0A 03 00 FD 00 90 00 XX

Write 1 Block (Block No. : 11)
Command: 0D 0A 0E 00 F2 04 00 FF FD 04 01 06 A2 11 11 22 33 44 00 98
Response: 0D 0A 03 00 FD 00 90 00 XX

Write 2 Blocks (Block No. : 12, 13)
Command: 0D 0A 12 00 EE 04 00 FF FD 06 01 0A A1 12 55 66 77 88 99 AA BB CC 00 B8
Response: 0D 0A 03 00 FD 00 90 00 XX

Write 4 Block (Block No. : 14)
Command: 0D 0A 1A 00 E6 04 00 FF FD 06 01 12 A0 14 DD EE FF 00 10 20 30 40 50 60 70 80 90 A0 B0 C0 00 89
Response: 0D 0A 03 00 FD 00 90 00 XX

Read 2 Blocks (Block No. : 11, 12)
Command: 0D 0A 0A 00 F6 04 00 FF FD 01 01 02 31 11 00 BA
Response: 0D 0A 0B 00 F5 00 XX XX XX XX XX XX XX XX 90 00 XX

Read 4 Blocks (Block No. : 11, 12, 13, 14)
Command: 0D 0A 0A 00 F6 04 00 FF FD 01 01 02 30 11 00 BB
Response: 0D 0A 13 00 ED 00 XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX 90 00 XX

Access (Pass. : 12345678)
Command: 0D 0A 0D 00 F3 04 00 FF FD 04 01 05 B2 12 34 56 78 00 30
Response: 0D 0A 03 00 FD 00 90 00 XX

Set Password (Pass. : 00000000)
Command: 0D 0A 0D 00 F3 04 00 FF FD 04 01 05 B1 00 00 00 00 00 45
Response: 0D 0A 07 00 F9 00 XX XX XX XX 90 00 XX

Access (Pass. : 00000000)
Command: 0D 0A 0D 00 F3 04 00 FF FD 04 01 05 B2 00 00 00 00 00 44
Response: 0D 0A 03 00 FD 00 90 00 XX

Decrement counter (by value 2)
Command: 0D 0A 0B 00 F5 04 00 FF FD 06 01 03 D0 02 00 00 24
Response: 0D 0A 05 00 FB 00 XX XX 90 00 XX

SCardDisconnect
Command: 0D 0A 02 00 FE 02 00 FE
Response: 0D 0A 01 00 FF 00 xx

7.5 How to access DESFIRE cards?

SCardStatus
Command: 0D 0A 02 00 FE 03 00 FD
Response: 0D 0A 02 00 FE 00 01 xx

SCardConnect
Command: 0D 0A 02 00 FE 01 00 FF
Response: 0D 0A 07 00 F9 00 xx xx xx xx xx xx xx

Select Application (AID : '000000')
Command: 0D 0A 0B 00 F5 04 00 90 5A 00 00 03 00 00 00 00 0F
Response: 0D 0A 03 00 xx 00 91 00 xx

Authenticate (PICC Key No. : 00)
Command: 0D 0A 09 00 F7 04 00 90 0A 00 00 01 00 00 61
Response: 0D 0A 03 00 xx 00 91 00 xx

Format PICC
Command: 0D 0A 07 00 F9 04 00 90 FC 00 00 00 70
Response: 0D 0A 03 00 xx 00 91 00 xx

Create DES/TDES Application (AID : 'C3C2C1')
Command: 0D 0A 0D 00 F3 04 00 90 CA 00 00 05 C1 C2 C3 0F 07 00 41
Response: 0D 0A 03 00 xx 00 91 00 xx

ReaderAuthenticate (PIN : '0000000000000000')
Command: 0D 0A 0B 00 F5 83 00 00 00 00 00 00 00 00 00 00 7D
Response: 0D 0A 01 00 FF 00 xx

DESFire Load keys (PCD Key No. : 01, AID : 'C3C2C1', PICC Key No. : 00)
Command: 0D 0A 1F 00 E1 82 01 01 C1 C2 C3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 36
Response: 0D 0A 01 00 FF 00 xx

ReaderAuthenticate (PIN : '0000000000000000')
Command: 0D 0A 0B 00 F5 83 00 00 00 00 00 00 00 00 00 7D
Response: 0D 0A 01 00 FF 00 xx

DESFire Load keys (PCD Key No. : 02, AID : 'C3C2C1', PICC Key No. : 01)
Command: 0D 0A 1F 00 E1 82 01 02 C1 C2 C3 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 34
Response: 0D 0A 01 00 FF 00 xx

ReaderAuthenticate (PIN : '0000000000000000')
Command: 0D 0A 0B 00 F5 83 00 00 00 00 00 00 00 00 00 7D
Response: 0D 0A 01 00 FF 00 xx

DESFire Load keys (PCD Key No. : 03, AID : 'C3C2C1', PICC Key No. : 02)
Command: 0D 0A 1F 00 E1 82 01 03 C1 C2 C3 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 32
Response: 0D 0A 01 00 FF 00 xx

Select Application (AID : 'C3C2C1')
Command: 0D 0A 0B 00 F5 04 00 90 5A 00 00 03 C1 C2 C3 00 C9
Response: 0D 0A 03 00 xx 00 91 00 xx

Authenticate (PICC Key No. : 00)
Command: 0D 0A 09 00 F7 04 00 90 0A 00 00 01 00 00 61
Response: 0D 0A 03 00 xx 00 91 00 xx

ChangeKeySettings (Free Access)
Command: 0D 0A 09 00 F7 04 00 90 54 00 00 01 0F 00 08
Response: 0D 0A 03 00 xx 00 91 00 xx

Change Key (PICC Key No. : 02)
Command: 0D 0A 21 00 DF 04 00 90 C4 00 00 19 02 FF FF FF FF FF FF FF FF AA AA AA AA AA AA AA AA FF FF FF FF FF FF FF FF 00 4D
Response: 0D 0A 03 00 xx 00 91 00 xx

Change Key (PICC Key No. : 00)
Command: 0D 0A 21 00 DF 04 00 90 C4 00 00 19 00 AA AA BB BB CC CC DD DD EE EE FF FF 11 11 22 22 33 44 55 66 77 88 99 AA 00 BF
Response: 0D 0A 03 00 xx 00 91 00 xx

Authenticate (PICC Key No. : 02)
Command: 0D 0A 09 00 F7 04 00 90 0A 00 00 01 02 00 5F
Response: 0D 0A 03 00 xx 00 91 00 xx

Authenticate (PICC Key No. : 00)
Command: 0D 0A 09 00 F7 04 00 90 0A 00 00 01 00 00 61
Response: 0D 0A 03 00 xx 00 91 00 xx

Create StdData File (File No. : 01)
Command: 0D 0A 0F 00 F1 04 00 90 CD 00 00 07 01 00 EE EE FF 02 00 00 BA
Response: 0D 0A 03 00 xx 00 91 00 xx

Create Value File (File No. : 02)
Command: 0D 0A 19 00 E7 04 00 90 CC 00 00 11 02 00 EE EE 00 00 00 00 FF 00 00 00 00 00 00 00 01 00 B1
Response: 0D 0A 03 00 xx 00 91 00 xx

Create Linear Record File ((File No. : 03))
Command: 0D 0A 12 00 EE 04 00 90 C1 00 00 0A 03 00 EE EE 20 00 00 08 00 00 00 9A
Response: 0D 0A 03 00 xx 00 91 00 xx

Change File Settings (File No. : 01, Comm Mode : Plain)
Command: 0D 0A 0C 00 F4 04 00 90 5F 00 00 04 01 00 00 00 00 08
Response: 0D 0A 03 00 xx 00 91 00 xx

Authenticate (PICC Key No. : 00)
Command: 0D 0A 09 00 F7 04 00 90 0A 00 00 01 00 00 61
Response: 0D 0A 03 00 xx 00 91 00 xx

Write Data (File No. : 01)
Command: 0D 0A 8F 00 71 04 00 90 3D 00 00 87 01 00 00 00 80 00 00 AA AA BB BB CC CC DD DD AA AA BB BB CC CC DD DD AA AA BB BB CC CC DD DD AA AA BB BB CC CC DD DD AA AA BB BB CC CC DD DD AA AA BB BB CC CC DD DD AA AA BB BB CC CC DD DD AA AA BB BB CC CC DD DD AA AA BB BB CC CC DD DD AA AA BB BB CC CC DD DD AA AA BB BB CC CC DD DD AA AA BB BB CC CC DD DD AA AA BB BB CC CC DD DD AA AA BB BB CC CC DD DD AA AA BB BB CC CC DD DD AA AA BB BB CC CC DD DD 00 67
Response: 0D 0A 03 00 xx 00 91 00 xx

Read Data (File No. : 01)
Command: 0D 0A 0F 00 F1 04 00 90 BD 00 00 07 01 00 00 00 FF 00 00 00 A8
Response: 0D 0A 02 01 xx 00 xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx
xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx
xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx
xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx
xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx
xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx
xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx
xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx 91 00 xx

Get Value (File No. : 02)
Command: 0D 0A 09 00 F7 04 00 90 6C 00 00 01 02 00 FD
Response: 0D 0A 07 00 xx 00 xx xx xx xx 91 00 xx

Credit (File No. : 02)
Command: 0D 0A 0D 00 F3 04 00 90 0C 00 00 05 02 10 00 00 00 00 49
Response: 0D 0A 03 00 xx 00 91 00 xx

Commit Transaction
Command: 0D 0A 07 00 F9 04 00 90 C7 00 00 00 A5
Response: 0D 0A 03 00 xx 00 91 00 xx

Get Value (File No. : 02)
Command: 0D 0A 09 00 F7 04 00 90 6C 00 00 01 02 00 FD
Response: 0D 0A 07 00 xx 00 xx xx xx xx 91 00 xx

Debit (File No. : 02)
Command: 0D 0A 0D 00 F3 04 00 90 DC 00 00 05 02 08 00 00 00 00 81
Response: 0D 0A 03 00 xx 00 91 00 xx

Commit Transaction
Command: 0D 0A 07 00 F9 04 00 90 C7 00 00 00 A5
Response: 0D 0A 03 00 xx 00 91 00 xx

Get Value (File No. : 02)
Command: 0D 0A 09 00 F7 04 00 90 6C 00 00 01 02 00 FD
Response: 0D 0A 07 00 xx 00 xx xx xx xx 91 00 xx

Debit (File No. : 02)
Command: 0D 0A 0D 00 F3 04 00 90 DC 00 00 05 02 04 00 00 00 00 85
Response: 0D 0A 03 00 xx 00 91 00 xx

Abort Transaction
Command: 0D 0A 07 00 F9 04 00 90 A7 00 00 00 C5
Response: 0D 0A 03 00 xx 00 91 00 xx

Get Value (File No. : 02)
Command: 0D 0A 09 00 F7 04 00 90 6C 00 00 01 02 00 FD
Response: 0D 0A 07 00 xx 00 xx xx xx xx 91 00 xx

Write Records (File No. : 03)
Command: 0D 0A 2F 00 D1 04 00 90 3B 00 00 27 03 00 00 00 20 00 00 AA AA BB BB CC CC DD DD AA AA BB BB CC CC DD DD AA AA BB BB CC CC DD DD AA AA BB BB CC CC DD DD 00 77
Response: 0D 0A 03 00 xx 00 91 00 xx

Commit Transaction
Command: 0D 0A 07 00 F9 04 00 90 C7 00 00 00 A5
Response: 0D 0A 03 00 xx 00 91 00 xx

Read Records (File No. : 03)
Command: 0D 0A 0F 00 F1 04 00 90 BB 00 00 07 03 00 00 00 00 00 00 00 A7
Response: 0D 0A 23 00 xx 00 xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx 91 00 xx

SCardDisconnect
Command: 0D 0A 02 00 FE 02 00 FE
Response: 0D 0A 01 00 FF 00 xx

7.5.1 DESFIRE EV1 Specific commands

SCardStatus
Command: 0D 0A 02 00 FE 03 00 FD
Response: 0D 0A 02 00 FE 00 01 xx

SCardConnect
Command: 0D 0A 02 00 FE 01 00 FF
Response: 0D 0A 07 00 F9 00 xx xx xx xx xx xx xx

Select Application (AID : '000000')
Command: 0D 0A 0B 00 F5 04 00 90 5A 00 00 03 00 00 00 00 0F
Response: 0D 0A 03 00 xx 00 91 00 xx

Authenticate (PICC key No : 00)
Command: 0D 0A 09 00 F7 04 00 90 0A 00 00 01 00 00 61
Response: 0D 0A 03 00 xx 00 91 00 xx

Change Key (Master Level from DES/TDES to AES)
Command: 0D 0A 1A 00 E6 04 00 90 C4 00 00 12 80 12 34 56 78 9A BC DE F1 23 45 67 89 AB CD EF EE AE 00 82
Response: 0D 0A 03 00 xx 00 91 00 xx

ReaderAuthenticate (PIN : '0000000000000000')
Command: 0D 0A 0B 00 F5 83 00 00 00 00 00 00 00 00 00 00 7D
Response: 0D 0A 01 00 FF 00 xx

DESFire Load keys (PCD Key No. : 00, AID : '000000', PICC Key No. : 00)
Command: 0D 0A 1F 00 E1 82 01 00 00 00 00 00 12 34 56 78 9A BC DE F1 23 45 67 89 AB CD EF EE 00 00 00 00 00 00 00 00 97
Response: 0D 0A 01 00 FF 00 xx

Authenticate (Master level AES Authentication)
Command: 0D 0A 09 00 F7 04 00 90 AA 00 00 01 00 00 C1

Response: 0D 0A 03 00 xx 00 91 00 xx

GetVersion
Command: 0D 0A 07 00 F9 04 00 90 60 00 00 00 0C
Response: 0D 0A 1F 00 xx 00 xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx 91 00 xx

Get Card UID
Command: 0D 0A 07 00 F9 04 00 90 51 00 00 00 1B
Response: 0D 0A 13 00 xx 00 xx xx xx xx xx xx xx 91 00 xx

Get FreeMemory
Command: 0D 0A 07 00 F9 04 00 90 6E 00 00 00 FE
Response: 0D 0A 06 00 xx 00 xx xx xx 91 00 xx

Set Configuration
Command: 0D 0A 0A 00 F6 04 00 90 5C 00 00 02 00 00 00 0E
Response: 0D 0A 03 00 xx 00 91 00 xx

Set Configuration
Command: 0D 0A 22 00 DE 04 00 90 5C 00 00 1A 01 11 11 22 22 33 33 44 44 55 55 66 66 77 77 88 88 99 99 AA AA BB BB CC CC FF 00 9A
Response: 0D 0A 03 00 xx 00 91 00 xx

Set Configuration
Command: 0D 0A 0F 00 F1 04 00 90 5C 00 00 07 02 06 75 77 81 02 80 00 12
Response: 0D 0A 03 00 xx 00 91 00 xx

Change Key (Master level from AES to DES/TDES)
Command: 0D 0A 21 00 DF 04 00 90 C4 00 00 19 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 8F
Response: 0D 0A 03 00 xx 00 91 00 xx

ReaderAuthenticate (PIN : '0000000000000000')
Command: 0D 0A 0B 00 F5 83 00 00 00 00 00 00 00 00 00 00 7D
Response: 0D 0A 01 00 FF 00 xx

DESFire Load keys (PCD Key No. : 00, AID : '000000', PICC Key No. : 00)
Command: 0D 0A 1F 00 E1 82 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7D
Response: 0D 0A 01 00 FF 00 xx

Authenticate (PICC Key No. : 00)
Command: 0D 0A 09 00 F7 04 00 90 0A 00 00 01 00 00 61
Response: 0D 0A 03 00 xx 00 91 00 xx

Format PICC
Command: 0D 0A 07 00 F9 04 00 90 FC 00 00 00 70
Response: 0D 0A 03 00 xx 00 91 00 xx

SCardDisconnect
Command: 0D 0A 02 00 FE 02 00 FE
Response: 0D 0A 01 00 FF 00 xx

7.6 How to access ISO15693 cards?

SCardStatus
Command: 0D 0A 02 00 FE 03 00 FD
Response: 0D 0A 02 00 FE 00 01 xx

SCardConnect
Command: 0D 0A 02 00 FE 01 00 FF
Response: 0D 0A 07 00 F9 00 xx xx xx xx xx xx xx

Get Uid
Command: 0D 0A 07 00 F9 04 00 FF CA 00 00 00 33
Response: 0D 0A 0A 00 F6 00 xx xx xx xx xx xx xx 90 00 xx

Write Single Block (Block no: 0F)
Command: 0D 0A 0D 00 F3 04 00 FF FC 00 00 06 21 0F 01 02 03 04 C1
Response: 0D 0A 03 00 FD 00 90 00 xx

Lock Block (Block no: 13)
Command: 0D 0A 09 00 F7 04 00 FF FC 00 00 02 22 13 CA
Response: 0D 0A 03 00 FD 00 90 00 xx

Write Single Block (Block no: 13)
Command: 0D 0A 0D 00 F3 04 00 FF FC 00 00 06 21 13 01 02 03 04 BD
Response: 0D 0A 03 00 FD 00 90 00 xx

Read Single Block (Block no: 13)
Command: 0D 0A 0A 00 F6 04 00 FF FC 00 00 03 20 13 00 CB
Response: 0D 0A 07 00 F9 00 xx xx xx xx 90 00 xx

Write Multiple Block (Start Block no: 10, No of Blocks: 02)
Command: 0D 0A 12 00 EE 04 00 FF FC 00 00 0B 24 10 01 01 01 01 01 01 01 01 B9
Response: 0D 0A 03 00 FD 00 90 00 xx

Read Multiple Block (Start Block no: 10, No of Blocks: 04)
Command: 0D 0A 0B 00 F5 04 00 FF FC 00 00 04 23 10 03 00 C7
Response: 0D 0A 13 00 ED 00 xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx 90 00 xx

Write AFI
Command: 0D0A0900F70400FFFC00000227F0E8
Response: 0D 0A 03 00 FD 00 90 00 xx

Write DSFID
Command: 0D 0A 09 00 F7 04 00 FF FC 00 00 02 29 F0 E6
Response: 0D 0A 03 00 FD 00 90 00 xx

Lock AFI
Command: 0D 0A 08 00 F8 04 00 FF FC 00 00 01 28 D8
Response: 0D 0A 03 00 FD 00 90 00 xx

Lock DSFID
Command: 0D 0A 08 00 F8 04 00 FF FC 00 00 01 2A D6
Response: 0D 0A 03 00 FD 00 90 00 xx

Get Multiple Block Security Status (Start Block no: 00, No of Blocks: 02)
Command: 0D 0A 0B 00 F5 04 00 FF FC 00 00 04 2C 00 01 00 D0
Response: 0D 0A 05 00 FB 00 xx xx 90 00 xx

Get System Info

Command: 0D 0A 09 00 F7 04 00 FF FC 00 00 02 2B 00 D4
Response: 0D 0A 11 00 EF 00 xx xx xx xx xx xx xx xx xx xx xx xx xx xx 90 00 xx

SCardDisconnect
Command: 0D 0A 02 00 FE 02 00 FE
Response: 0D 0A 01 00 FF 00 xx

7.7 How to access Crypto RF cards?

SCardStatus
Command: 0D 0A 02 00 FE 03 00 FD
Response: 0D 0A 02 00 FE 00 01 xx

SCardConnect
Command: 0D 0A 02 00 FE 01 00 FF
Response: 0D 0A 07 00 F9 00 xx xx xx xx xx xx xx

Get Uid
Command: 0D 0A 07 00 F9 04 00 FF CA 00 00 00 33
Response: 0D 0A 0A 00 F6 00 xx xx xx xx xx xx xx 90 00 xx

Set User Zone (User Zone: 00)
Command: 0D 0A 09 00 F7 04 00 FF FC 00 00 02 01 00 FE
Response: 0D 0A 03 00 FD 00 90 00 xx

Write User Zone (Start Address: 0000, Length: 10)
Command: 0D 0A 1B 00 E5 04 00 FF FC 00 00 14 03 00 00 0F 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0E 0E 0F 62
Response: 0D 0A 03 00 FD 00 90 00 xx

Write User Zone - Traverse (Start Address: 0000, Length: 01)
Command: 0D 0A 0D 00 F3 04 00 FF FD 04 01 05 03 00 00 00 0B 00 E8
Response: 0D 0A 06 00 FA 00 xx 00 00 90 00 xx

Read User Zone (Start Address: 0000, Length: 20)
Command: 0D 0A 0C 00 F4 04 00 FF FC 00 00 04 02 00 00 1F 20 BC
Response: 0D 0A 23 00 DF 00 xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx 90 00 xx

Set User Zone with Anti Tearing (User Zone: 00)
Command: 0D 0A 09 00 F7 04 00 FF FC 00 00 02 01 80 7E
Response: 0D 0A 03 00 FD 00 90 00 xx

Write User Zone with Anti Tearing (Start Address: 0000, Length: 08)
Command: 0D 0A 13 00 ED 04 00 FF FC 00 00 0C 03 00 00 07 08 09 0A 0B 0C 0D 0E 0F 8F
Response: 0D 0A 03 00 FD 00 90 00 xx

Read User Zone (Start Address: 0000, Length: 20)
Command: 0D 0A 0C 00 F4 04 00 FF FC 00 00 04 02 00 00 1F 20 BC
Response: 0D 0A 23 00 DF 00 xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx 90 00 xx

Read System Zone Fuse (Length: 01)
Command: 0D0A0C00F40400FFFC0000040601FF0000F7
Response: 0D 0A 04 00 FC 00 xx 90 00 xx

Read System Zone Check Sum (Length: 02)
Command: 0D 0A 0C 00 F4 04 00 FF FC 00 00 04 06 02 FF 01 00 F5
Response: 0D 0A 05 00 FB 00 xx xx 90 00 xx

Check Password
Command: 0D 0A 0C 00 F4 04 00 FF FC 00 00 05 0C 07 10 14 7C 49
Response: 0D 0A 03 00 FD 00 90 00 xx

Write System Zone (Start Address: 0008, Length: 10)
Command: 0D 0A 1B 00 E5 04 00 FF FC 00 00 14 04 00 08 0F 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 5A
Response: 0D 0A 03 00 FD 00 90 00 xx

Read System Zone (Start Address: 0008, Length: 41)
Command: 0D 0A 0C 00 F4 04 00 FF FC 00 00 04 06 00 08 40 41 6E
Response: 0D 0A 44 00 BC 00 xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx

Write System Zone with Anti tearing (Start Address: 0008, Length: 08)
Command: 0D 0A 13 00 ED 04 00 FF FC 00 00 0C 04 80 08 07 08 09 0A 0B 0C 0D 0E 0F 06
Response: 0D 0A 03 00 FD 00 90 00 xx

Read System Zone (Start Address: 0008, Length: 41)
Command: 0D 0A 0C 00 F4 04 00 FF FC 00 00 04 06 00 08 40 41 6E
Response: 0D 0A 44 00 BC 00 xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx

Write System Zone Fuse (Fuse: SEC, Fuse Address: 07)
Command: 0D 0A 0C 00 F4 04 00 FF FC 00 00 05 04 01 07 00 01 EF
Response: 0D 0A 03 00 FD 00 90 00 xx

SCardDisconnect
Command: 0D 0A 02 00 FE 02 00 FE
Response: 0D 0A 01 00 FF 00 xx

7.8 How to access ICODE-SLI cards?

SCardStatus
Command: 0D 0A 02 00 FE 03 00 FD
Response: 0D 0A 02 00 FE 00 01 xx

SCardConnect
Command: 0D 0A 02 00 FE 01 00 FF
Response: 0D 0A 07 00 F9 00 xx xx xx xx xx xx xx

Get UID
Command: 0D 0A 07 00 F9 04 00 FF CA 00 00 00 33
Response: 0D 0A 0B 00 F5 00 BA 4D CC 08 00 01 04 E0 90 00 xx

Traverse - Inventory Read (Start Block no: 10, No of Blocks: 05)
Command: 0D 0A 0E 00 F2 04 00 FF FD 03 01 06 66 A0 04 00 10 04 00 D8
Response: 0D 0A 20 00 E0 00 xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx 90 00 xx

Traverse - Set EAS
Command: 0D 0A 13 00 ED 04 00 FF FD 04 01 0B 22 A2 04 BA 4D CC 08 00 01 04 E0 00 68
Response: 0D 0A 04 00 FC 00 00 90 00 xx

Traverse - EAS Alarm
Command: 0D 0A 13 00 ED 04 00 FF FD 04 01 0B 22 A5 04 BA 4D CC 08 00 01 04 E0 00 65
Response: 0D 0A 24 00 DC 00 00 xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx 90 00 xx

Traverse - Lock EAS
Command: 0D 0A 13 00 ED 04 00 FF FD 04 01 0B 22 A4 04 BA 4D CC 08 00 01 04 E0 00 66
Response: 0D 0A 04 00 FC 00 00 90 00 xx

Traverse - Reset EAS
Command: 0D 0A 13 00 ED 04 00 FF FD 04 01 0B 22 A3 04 BA 4D CC 08 00 01 04 E0 00 67
Response: 0D 0A 04 00 FC 00 00 90 00 xx

Traverse - EAS Alarm
Command: 0D 0A 13 00 ED 04 00 FF FD 04 01 0B 22 A5 04 BA 4D CC 08 00 01 04 E0 00 65
Response: 0D 0A 24 00 DC 00 00 xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx xx 90 00 xx

SCardDisconnect
Command: 0D 0A 02 00 FE 02 00 FE
Response: 0D 0A 01 00 FF 00 xx

7.9 How to access MIFARE Plus cards?

Accessing MIFARE Plus SL2 Cards:

SCardStatus
Command: 0D 0A 02 00 FE 03 00 FD
Response: 0D 0A 02 00 FE 00 01 XX

SCardConnect
Command: 0D 0A 02 00 FE 01 00 FF
Response: 0D 0A 07 00 F9 00 XX XX XX XX XX XX XX

Authenticate reader with default PIN (PIN:'0000000000000000') to load MIFARE classic crypto1 Type A key to reader non-volatile memory
Command: 0D 0A 0B 00 F5 83 00 00 00 00 00 00 00 00 00 7D
Response: 0D 0A 01 00 XX 00 XX

Load MIFARE classic crypto1 Type A Key to reader non-volatile memory (PCD Key No.:00; Key Type:Key A; Key:FFFFFFFFFFFF)
Command: 0D 0A 0A 00 F6 82 00 00 60 FF FF FF FF FF FF 24
Response: 0D 0A 01 00 XX 00 XX

Authenticate reader with default PIN (PIN '0000000000000000') to load MIFARE Plus AES Sector Ket for Sector 0 to reader non-volatile memory
Command: 0D 0A 0B 00 F5 83 00 00 00 00 00 00 00 00 00 7D
Response: 0D 0A 01 00 XX 00 XX

Load MIFARE Plus AES Sector Key for sector 0 to reader non-volatile memory (PCD Key No:0x00; Key type:Key A; Key:0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF)
Command: 0D 0A 15 00 EB 82 03 00 00 40 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 4B
Response: 0D 0A 01 00 XX 00 XX

Perform AES authentication with the card to access sector 0 using AES sector key for the sector (Firmware will internally perform AES auth when MF classic auth is done for SL2 cards, so this APDU need not be issued externally)
Command: 0D 0A 0B 00 F5 04 00 FF FB 00 00 03 76 00 40 00 49
Response: 0D 0A 03 00 XX 00 90 00 XX

Perform SL2 AES authentication followed by MIFARE Classic Crypto1 authentication (Sector:0; Block No.:0x00; PCD Key No.:00; Key type:Key A)
Command: 0D 0A 0C 00 F4 04 00 FF 86 00 00 05 01 00 00 00 00 71
Response: 0D 0A 03 00 XX 00 90 00 XX

Write single block (16 bytes) of data to authenticated block 0x01
Command: 0D 0A 17 00 E9 04 00 FF D6 00 01 10 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 64
Response: 0D 0A 03 00 XX 00 90 00 XX

Read back 16 bytes of daya from block 0x01
Command: 0D 0A 07 00 F9 04 00 FF B0 00 01 00 4C
Response: 0D 0A 13 00 XX 00 XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX 90 00 XX

Perform multi block write for block 0x01 and 0x02 (32 bytes are written totally)
Command: 0D 0A 2B 00 D5 04 00 FF FB 00 00 23 A9 01 02 12 34 56 78 9A BC DE F0 0F ED CB A9 87 65 43 21 12 34 56 78 9A BC DE F0 0F ED CB A9 87 65 43 21 00 43
Response: 0D 0A 03 00 XX 00 90 00 XX

Perform multi block read from block 0x00 to 0x02 (48 bytes are read totally)
Command: 0D 0A 0B 00 F5 04 00 FF FD 01 02 03 38 00 03 00 BF
Response: 0D 0A 33 00 XX 00 XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX 90 00 XX

SCardDisconnect
Command: 0D 0A 02 00 FE 02 00 FE
Response: 0D 0A 01 00 FF 00 XX

Accessing MIFARE Plus S SL3 Cards:

SCardStatus
Command: 0D 0A 02 00 FE 03 00 FD
Response: 0D 0A 02 00 FE 00 01 XX

SCardConnect
Command: 0D 0A 02 00 FE 01 00 FF
Response: 0D 0A 07 00 F9 00 XX XX XX XX XX XX XX

Reset authentication already enabled in the card
Command: 0D 0A 09 00 F7 04 00 FF FB 00 00 01 78 00 89
Response: 0D 0A 03 00 XX 00 90 00 XX

Authenticate Reader with default reader PIN (PIN:'0000000000000000') to load the MIFARE Plus AES sector 4 key in to reader non-volatile memory
Command: 0D 0A 0B 00 F5 83 00 00 00 00 00 00 00 00 00 00 7D
Response: 0D 0A 01 00 XX 00 XX

Load MIFARE Plus AES Sector Key for sector 4 with PCD Key No:0x00; Key type:Key A and Key:0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF into reader non-volatile memory
Command: 0D 0A 15 00 EB 82 03 00 08 40 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 43
Response: 0D 0A 01 00 XX 00 XX

Authenticate with card to access sector 4 using the key loaded in to the reader non-volatile memory
Command: 0D 0A 0B 00 F5 04 00 FF FB 00 00 03 76 08 40 00 41
Response: 0D 0A 03 00 XX 00 90 00 XX

Write data to 3 consecutive blocks (16 bytes per block) namely block0 to block2 in sector 4

Command: 0D 0A 3B 00 C5 04 00 FF FB 00 00 33 A3 10 00 0F 0E 0D 0C 0B 0A 09 08 07 06 05 04 03 02 01 00 55 AA 44 BB 33 CC 22 DD 11 EE 00 FF AB CD EF 55 AA 55 BB 44 CC 33 DD 22 EE 11 FF 00 99 66 88 77 00 F6
Response: 0D 0A 03 00 XX 00 90 00 XX

Read data from 3 consecutive blocks - block0 to block2 in sector 4
Command: 0D 0A 0C 00 F4 04 00 FF FB 00 00 04 33 10 00 03 00 B8
Response: 0D 0A 33 00 XX 00 XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX 90 00 XX

Change Sector 4 AES key (Key A) of the card to 0x0F0E0D0C0B0A09080706050403020100
Command: 0D 0A 1B 00 E5 04 00 FF FB 00 00 13 A1 10 40 0F 0E 0D 0C 0B 0A 09 08 07 06 05 04 03 02 01 00 00 86
Response: 0D 0A 03 00 XX 00 90 00 XX

Reset authentication already enabled in the card
Command: 0D 0A 09 00 F7 04 00 FF FB 00 00 01 78 00 89
Response: 0D 0A 03 00 XX 00 90 00 XX

Authenticate with card to access sector 4 using the old key (0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF) already available in the reader memory
Command: 0D 0A 0B 00 F5 04 00 FF FB 00 00 03 76 10 40 00 39
Response: 0D 0A 03 00 XX 00 63 06 XX

Authenticate Reader with default reader PIN (PIN:'0000000000000000') to update the new MIFARE Plus AES sector key in to reader non-volatile memory
Command: 0D 0A 0B 00 F5 83 00 00 00 00 00 00 00 00 00 00 7D
Response: 0D 0A 01 00 XX 00 XX

Overwrite the MIFARE Plus AES Sector Key for sector 4 with Key:0x0F0E0D0C0B0A09080706050403020100 in the reader non-volatile memory
Command: 0D 0A 15 00 EB 82 03 00 10 40 0F 0E 0D 0C 0B 0A 09 08 07 06 05 04 03 02 01 00 B3
Response: 0D 0A 01 00 XX 00 XX

Authenticate with card to access sector 4 using the key loaded into the reader memory
Command: 0D 0A 0B 00 F5 04 00 FF FB 00 00 03 76 10 40 00 39
Response: 0D 0A 03 00 XX 00 90 00 XX

Change Sector 4 AES key (Key A) of the card to 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
Command: 0D 0A 1B 00 E5 04 00 FF FB 00 00 13 A1 10 40 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 00 0E
Response: 0D 0A 03 00 XX 00 90 00 XX

Authenticate Reader with default reader PIN (PIN:'0000000000000000') to overwrite the MIFARE Plus AES sector 4 key in the reader non-volatile memory
Command: 0D 0A 0B 00 F5 83 00 00 00 00 00 00 00 00 00 00 7D
Response: 0D 0A 01 00 XX 00 XX

Overwrite MIFARE Plus AES Sector Key for sector 4 with Key: 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
Command: 0D 0A 15 00 EB 82 03 00 10 40 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 3B
Response: 0D 0A 01 00 XX 00 XX

Authenticate with card to access sector 4 using the new key loaded in to the reader memory
Command: 0D 0A 0B 00 F5 04 00 FF FB 00 00 03 76 10 40 00 39
Response: 0D 0A 03 00 XX 00 90 00 XX

Read block 0 of Sector 4 to check if authentication was successful
Command: 0D 0A 0C 00 F4 04 00 FF FB 00 00 04 33 10 00 01 00 BA

Response: 0D 0A 13 00 XX 00 XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX 90 00 XX

Authenticate Reader with default reader PIN (PIN:'0000000000000000') to load Card Master Key into reader non-volatile memory
Command: 0D 0A 0B 00 F5 83 00 00 00 00 00 00 00 00 00 7D
Response: 0D 0A 01 00 XX 00 XX

Load MIFARE Plus Card Master Key to reader non-volatile memory with PCD Key No:0x00 and Key:0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
Command: 0D 0A 15 00 EB 82 03 00 00 90 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FB
Response: 0D 0A 01 00 XX 00 XX

Authenticate with card using the Card Master Key loaded in to the reader memory
Command: 0D 0A 0B 00 F5 04 00 FF FB 00 00 03 76 00 90 00 F9
Response: 0D 0A 03 00 XX 00 63 06XX

Change Card Master Key of the card to 0x00000000000000000000000000000000
Command: 0D 0A 1B 00 E5 04 00 FF FB 00 00 13 A1 00 90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 BE
Response: 0D 0A 03 00 XX 00 90 00 XX

Authenticate Reader with default reader PIN (PIN:'0000000000000000') to update the new Card Master Key to the reader memory
Command: 0D 0A 0B 00 F5 83 00 00 00 00 00 00 00 00 00 7D
Response: 0D 0A 01 00 XX 00 XX

Overwrite Card Master Key with Key: 0x00000000000000000000000000000000
Command: 0D 0A 15 00 EB 82 03 00 00 90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 EB
Response: 0D 0A 01 00 XX 00 XX

Authenticate with the card using the updated Card Master Key loaded in to the reader memory
Command: 0D 0A 0B 00 F5 04 00 FF FB 00 00 03 76 00 90 00 F9
Response: 0D 0A 03 00 XX 00 63 06 XX

Restore Card Master Key again to0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
Command: 0D 0A 1B 00 E5 04 00 FF FB 00 00 13 A1 00 90 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 00 CE
Response: 0D 0A 03 00 XX 00 90 00 XX

Authenticate Reader with default reader PIN (PIN:'0000000000000000') to load the restored Card Master Key to the reader memory
Command: 0D 0A 0B 00 F5 83 00 00 00 00 00 00 00 00 00 7D
Response: 0D 0A 01 00 XX 00 XX

Load restored Card Master Key with PCD Key No: 0x00 and Key:
0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
Command: 0D 0A 15 00 EB 82 03 00 00 90 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FB
Response: 0D 0A 01 00 XX 00 XX

Authenticate with the card using the restored Card Master Key loaded in to the reader memory
Command: 0D 0A 0B 00 F5 04 00 FF FB 00 00 03 76 00 90 00 F9
Response: 0D 0A 03 00 XX 00 63 06 XX

SCardDisconnect
Command: 0D 0A 02 00 FE 02 00 FE
Response: 0D 0A 01 00 FF 00 XX

Accessing MIFARE Plus X SL3 Cards :

SCardStatus
Command: 0D 0A 02 00 FE 03 00 FD
Response: 0D 0A 02 00 FE 00 01 XX

SCardConnect
Command: 0D 0A 02 00 FE 01 00 FF
Response: 0D 0A 07 00 F9 00 XX XX XX XX XX XX XX

Read the UID of the card
Command: 0D 0A 07 00 F9 04 00 FF CA 00 00 00 33
Response: 0D 0A 0A 00 XX 00 XX XX XX XX XX XX XX 90 00 XX

Reset authentication with the card
Command: 0D 0A 09 00 F7 04 00 FF FB 00 00 01 78 00 89
Response: 0D 0A 03 00 XX 00 90 00 XX

Authenticate Reader with PIN '0000000000000000' to load card master key to reader non-volatile memory
Command: 0D 0A 0B 00 F5 83 00 00 00 00 00 00 00 00 00 7D
Response: 0D 0A 01 00 XX 00 XX

Load MIFARE Plus Card Master Key to reader non-volatile memory (PCD Key No:0x00; Key:0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF)
Command: 0D 0A 15 00 EB 82 03 00 00 90 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FB
Response: 0D 0A 01 00 XX 00 XX

Authenticate with the card using the Card Master Key loaded in the reader non-volatile memory
Command: 0D 0A 0B 00 F5 04 00 FF FB 00 00 03 76 00 90 00 F9
Response: 0D 0A 03 00 XX 00 90 00 XX

Write to Block 0xB000 (MFP Configuration block). Change number of unmaced commands in one session to 0x20
Command: 0D 0A 1B 00 E5 04 00 FF FB 00 00 13 A1 00 B0 20 0F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6F
Response: 0D 0A 03 00 XX 00 90 00 XX

Authenticate Reader with PIN '0000000000000000' to load AES sector key for sector 0x03to reader non-volatile memory
Command: 0D 0A 0B 00 F5 83 00 00 00 00 00 00 00 00 00 7D
Response: 0D 0A 01 00 XX 00 XX

Load MIFARE Plus AES Sector Key (Sector No:0x03; PCD Key No:0x01; Key type:Key A and Key:0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF) to reader non-volatile memory
Command: 0D 0A 15 00 EB 82 03 01 06 40 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 44
Response: 0D 0A 01 00 XX 00 XX

Authenticate with the card using the AES sector key (Sector:0x03; Key type:Key A) loaded in the reader non-volatile memory
Command: 0D 0A 0B 00 F5 04 00 FF FB 00 00 03 76 06 40 00 43
Response: 0D 0A 03 00 XX 00 90 00 XX

Write 16 bytes of data (Sector No:0x03; Block No:0x0C; No of Blocks:0x01; Write Type:Encrypted, MAC on Command & MAC on Response)
Command: 0D 0A 1B 00 E5 04 00 FF FB 00 00 13 A1 0C 00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 00 52

Response: 0D 0A 03 00 XX 00 90 00 XX

Read back 16 bytes of data (Sector No:0x03; Block No:0x0C; No of Blocks:0x01; Read Type:Encrypted, MAC on Command & MAC on Response)
Command: 0D 0A 0C 00 F4 04 00 FF FB 00 00 04 31 0C 00 01 00 C0
Response: 0D 0A 13 00 XX 00 XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX 90 00 XX

Write data to 2 consecutive blocks (32 bytes) (Sector No:0x03; Block No:0x0C & 0x0D; No of Blocks:0x02; Write Type:Plain, MAC on Command & MAC on Response)
Command: 0D 0A 2B 00 D5 04 00 FF FB 00 00 23 A3 0C 00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF EE EE EE EE EE EE EE EE EE EE EE EE EE EE EE EE 00 60
Response: 0D 0A 03 00 XX 00 90 00 XX

Read data from 2 consecutive blocks (Sector No:0x03; Block No:0x0C & 0x0D; No of Blocks:0x02; Read Type:Plain, MAC on Command & MAC on Response)
Command: 0D 0A 0C 00 F4 04 00 FF FB 00 00 04 33 0C 00 02 00 BD
Response: 0D 0A 23 00 XX 00 XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX 90 00 XX

Write data to 3 consecutive blocks (Sector No:0x03; Block No:0x0C, 0x0D & 0x0E; No of Blocks:0x03; Write Type:Encrypted, MAC on Command & MAC on Response)
Command: 0D 0A 3B 00 C5 04 00 FF FB 00 00 33 A1 0C 00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF EE EE EE EE EE EE EE EE EE EE EE EE EE EE EE EE DD DD DD DD DD DD DD DD DD DD DD DD DD DD DD DD 00 82
Response: 0D 0A 03 00 XX 00 90 00 XX

Read data from 3 consecutive blocks (Sector No:0x03; Block No:0x0C, 0x0D & 0x0E; No of Blocks:0x03; Read Type:Encrypted, No MAC on Command & MAC on Response)
Command: 0D 0A 0C 00 F4 04 00 FF FB 00 00 04 35 0C 00 03 00 BA
Response: 0D 0A 33 00 XX 00 XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX 90 00 XX

Authenticate Reader with PIN '0000000000000000' to load MIFARE plus AES sector key for sector 0x05 to reader non-volatile memory
Command: 0D 0A 0B 00 F5 83 00 00 00 00 00 00 00 00 00 00 7D
Response: 0D 0A 01 00 XX 00 XX

Load MIFARE Plus AES Sector Key (Sector No:0x05; PCD Key No:0x01; Key type:Key A and Key:0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF) to reader non-volatile memory
Command: 0D 0A 15 00 EB 82 03 01 0A 40 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 40
Response: 0D 0A 01 00 XX 00 XX

Authenticate with the card using the AES sector key (Sector:0x05; Key type:Key A) loaded in the reader non-volatile memory
Command: 0D 0A 0B 00 F5 04 00 FF FB 00 00 03 76 0A 40 00 3F
Response: 0D 0A 03 00 XX 00 90 00 XX

Prepare Value Block with value 0x000000FF (Sector No:0x05; Block No:0x14; Write Type:Encrypted, MAC on Command & MAC on Response, Value:0x000000FF)
Command: 0D 0A 1B 00 E5 04 00 FF FB 00 00 13 A1 14 00 FF 00 00 00 00 FF FF FF FF 00 00 00 0F F0 0F F0 00 41
Response: 0D 0A 03 00 XX 00 90 00 XX

Read 16 bytes data from the value block (Sector No:0x05; Block No:0x14; No of Blocks:0x01; Read Type:Encrypted, MAC on Command & MAC on Response)
Command: 0D 0A 0C 00 F4 04 00 FF FB 00 00 04 31 14 00 01 00 B8
Response: 0D 0A 13 00 XX 00 XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX 90 00 XX

Decrement value by 0x08 from the value block (Sector No:0x05; Block No:0x14; Decrement Type:Encrypted, MAC on Command & MAC on Response; Value:0x00000008)
Command: 0D 0A 0F 00 F1 04 00 FF FB 00 00 07 B3 14 00 08 00 00 00 00 2C
Response: 0D 0A 03 00 XX 00 90 00 XX

Transfer Decremented value to the block (Sector No:0x05; Block No:0x14; Transfer Type:MAC on Command & MAC on Response)
Command: 0D 0A 0B 00 F5 04 00 FF FB 00 00 03 B5 14 00 00 36
Response: 0D 0A 03 00 XX 00 90 00 XX

Read current value from value block (Sector No:0x05; Block No:0x14; No of Blocks:0x01; Read Type:Encrypted, No MAC on Command & MAC on Response)
Command: 0D 0A 0C 00 F4 04 00 FF FB 00 00 04 31 14 00 01 00 B8
Response: 0D 0A 13 00 XX 00 XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX 90 00 XX

Increment value by 0x02 in the value block (Sector No:0x05; Block No:0x14; Increment Type:Encrypted, MAC on Command & MAC on Response; Value:0x00000002)
Command: 0D 0A 0F 00 F1 04 00 FF FB 00 00 07 B1 14 00 02 00 00 00 00 34
Response: 0D 0A 03 00 XX 00 90 00 XX

Transfer Incremented value to the block (Sector No:0x05; Block No:0x14; Transfer Type:MAC on Command & MAC on Response)
Command: 0D 0A 0B 00 F5 04 00 FF FB 00 00 03 B5 14 00 00 36
Response: 0D 0A 03 00 XX 00 90 00 XX

Read current value from value block (Sector No:0x05; Block No:0x14; No of Blocks:0x01; Read Type:Plain, MAC on Command & MAC on Response)
Command: 0D 0A 0C 00 F4 04 00 FF FB 00 00 04 33 14 00 01 00 B6
Response: 0D 0A 12 00 XX 00 XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX 90 00 XX

Decrement value by 0x08 from value block and transfer the decremented value to the block(Sector No:0x05; Block No:0x14; Decrement Type:Encrypted, MAC on Command & MAC on Response; Value:0x00000008)
Command: 0D 0A 11 00 EF 04 00 FF FB 00 00 09 B9 14 00 14 00 08 00 00 00 00 10
Response: 0D 0A 03 00 XX 00 90 00XX

Read current value from value block (Sector No:0x05; Block No:0x14; No of Blocks:0x01; Read Type:Plain, No MAC on Command & MAC on Response)
Command: 0D 0A 0C 00 F4 04 00 FF FB 00 00 04 37 14 00 01 00 B2
Response: 0D 0A 12 00 XX 00 XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX 90 00 XX

Increment value by 0x02 from value block and transfer the inccremented value to the block
Command: 0D 0A 11 00 EF 04 00 FF FB 00 00 09 B7 14 00 14 00 02 00 00 00 00 18
Response: 0D 0A 03 00 XX 00 90 00XX

Read current value from value block (Sector No:0x05; Block No:0x14; No of Blocks:0x01; Read Type:Plain, MAC on Command & MAC on Response)
Command: 0D 0A 0C 00 F4 04 00 FF FB 00 00 04 33 14 00 01 00 B6
Response: 0D 0A 12 00 XX 00 XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX 90 00 XX

Decrement value by 0x08 from value block (Sector No:0x05; Block No:0x14; Decrement Type:Encrypted, MAC on Command & MAC on Response; Value:0x00000008)
Command: 0D 0A 0F 00 F1 04 00 FF FB 00 00 07 B3 14 00 08 00 00 00 00 2C
Response: 0D 0A 03 00 XX 00 90 00 XX

Restore previous contents of the block (Sector No:0x05; Block No:0x14; Transfer Type:MAC on Command & MAC on Response)
Command: 0D 0A 0B 00 F5 04 00 FF FB 00 00 03 C3 14 00 00 28
Response: 0D 0A 03 00 XX 00 90 00 XX

Read current value from value block (Sector No:0x05; Block No:0x14; No of Blocks:0x01; Read Type:Plain, No MAC on Command & MAC on Response)
Command: 0D 0A 0C 00 F4 04 00 FF FB 00 00 04 37 14 00 01 00 B2
Response: 0D 0A 12 00 XX 00 XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX 90 00 XX

Authenticate with the card using the Card Master key
Command: 0D 0A 0B 00 F5 04 00 FF FB 00 00 03 76 00 90 00 F9
Response: 0D 0A 03 00 XX 00 90 00 XX

Write to Block 0xB000 (MFP Configuration block). Change number of unmaced commands in one session to 0x00
Command: 0D 0A 1B 00 E5 04 00 FF FB 00 00 13 A1 00 B0 00 0F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 8F
Response: 0D 0A 03 00 XX 00 90 00 XX

SCardDisconnect
Command: 0D 0A 02 00 FE 02 00 FE
Response: 0D 0A 01 00 FF 00 XX

SL1 Switching from SL0

SCardStatus
Command: 0D 0A 02 00 FE 03 00 FD
Response: 0D 0A 02 00 FE 00 01 XX

SCardConnect
Command: 0D 0A 02 00 FE 01 00 FF
Response: 0D 0A 07 00 F9 00 XX XX XX XX XX XX XX

Initialize Card Master Key
Command: 0D 0A 1B 00 E5 04 00 FF FB 00 00 13 A8 00 90 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 00 C7
0D 0A 03 00 XX 00 90 00 XX

Initialize Card Configuration Key
Command: 0D 0A 1B 00 E5 04 00 FF FB 00 00 13 A8 01 90 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 00 C6
Response: 0D 0A 03 00 XX 00 90 00 XX

Initialize SL2 Switch Key
Command: 0D 0A 1B 00 E5 04 00 FF FB 00 00 13 A8 02 90 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 00 C5
Response: 0D 0A 03 00 XX 00 90 00 XX

Initialize SL3 Switch Key
Command: 0D 0A 1B 00 E5 04 00 FF FB 00 00 13 A8 03 90 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 00 C4
Response: 0D 0A 03 00 XX 00 90 00 XX

CommitPerso - Change the keys in the card to the above initialized values
Command: 0D 0A 09 00 F7 04 00 FF FB 00 00 01 AA 00 57
Response: 0D 0A 03 00 XX 00 90 00 XX

SCardDisconnect

Command: 0D 0A 02 00 FE 02 00 FE
Response: 0D 0A 01 00 FF 00 XX

SL2 Switching from SL1

SCardStatus
Command: 0D 0A 02 00 FE 03 00 FD
Response: 0D 0A 02 00 FE 00 01 XX

SCardConnect
Command: 0D 0A 02 00 FE 01 00 FF
Response: 0D 0A 07 00 F9 00 XX XX XX XX XX XX XX

Authenticate reader with default reader PIN (PIN:'0000000000000000') to load the SL2 switch key in to reader non-volatile memory
Command: 0D 0A 0B 00 F5 83 00 00 00 00 00 00 00 00 00 7D
Response: 0D 0A 01 00 XX 00 XX

Load MIFARE Plus SL2 Switch Key into reader non-volatile memory (PCD Key No.:0x03; Key:0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF)
Command: 0D 0A 15 00 EB 82 03 03 02 90 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF F6
Response: 0D 0A 01 00 XX 00 XX

Authenticate with card using the SL2 switch key loaded in the reader non-volatile memory (Hereafter card will enumerate in SL2 mode)
Command: 0D 0A 0B 00 F5 04 00 FF FB 00 00 03 76 02 90 00 F7
Response: 0D 0A 03 00 XX 00 90 00 XX

SCardDisconnect
Command: 0D 0A 02 00 FE 02 00 FE
Response: 0D 0A 01 00 FF 00 XX

SL3 Switching from SL1 or from SL2

SCardStatus
Command: 0D 0A 02 00 FE 03 00 FD
Response: 0D 0A 02 00 FE 00 01 XX

SCardConnect
Command: 0D 0A 02 00 FE 01 00 FF
Response: 0D 0A 07 00 F9 00 XX XX XX XX XX XX XX

Authenticate reader with default PIN (PIN:'0000000000000000') to load SL3 switch key in to reader non-volatile memory
Command: 0D 0A 0B 00 F5 83 00 00 00 00 00 00 00 00 00 7D
Response: 0D 0A 01 00 XX 00 XX

Load MIFARE Plus SL3 switch key into reader non-volatile memory (Pcd Key No.:0x03, Key:0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF)
Command: 0D 0A 15 00 EB 82 03 04 03 90 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF F4
Response: 0D 0A 01 00 XX 00 XX

Authenticate with card using the SL3 siwtch key loaded in the reader non-volatile memory (SL1 to SL3 Switching or SL2 to SL3 Switching)
Command: 0D 0A 0B 00 F5 04 00 FF FB 00 00 03 76 03 90 00 F6
Response: 0D 0A 03 00 XX 00 90 00 XX

SCardDisconnect
Command: 0D 0A 02 00 FE 02 00 FE
Response: 0D 0A 01 00 FF 00 XX

SL3 Virtual Card commands

SCardStatus
Command: 0D 0A 02 00 FE 03 00 FD
Response: 0D 0A 02 00 FE 00 01 XX

SCardConnect
Command: 0D 0A 02 00 FE 01 00 FF
Response: 0D 0A 07 00 F9 00 XX XX XX XX XX XX XX

Authenticate Reader with PIN '0000000000000000'
Command: 0D 0A 0B 00 F5 83 00 00 00 00 00 00 00 00 00 7D
Response: 0D 0A 01 00 XX 00 XX

Load card master key in to reader non-volatile memory with PCD Key No:0x00 and Key:0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
Command: 0D 0A 1F 00 E1 82 03 02 00 90 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF F9
Response: 0D 0A 01 00 XX 00 XX

Authenticate with the card using the card master key loaded in to the reader memory FFFB00000376009000
Command: 0D 0A 0B 00 F5 04 00 FF FB 00 00 03 76 00 90 00 F9
Response: 0D 0A 01 00 FF 00 XX

Write to IID block (IID: 0x00000000000000000000000000000000)
Command: 0D 0A 1B 00 E5 04 00 FF FB 00 00 13 A1 01 B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9D
Response: 0D 0A 03 00 XX 00 90 00 XX

Authenticate Reader with PIN '0000000000000000' to load VC Polling Mac key to reader non-volatile memory
Command: 0D 0A 0B 00 F5 83 00 00 00 00 00 00 00 00 00 7D
Response: 0D 0A 01 00 XX 00 XX

Load MIFARE Plus VC Polling Mac Key to reader non volatile memory (PCD Key No:0x00 and Key:0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF)
Command: 0D 0A 15 00 EB 82 03 00 81 A0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 6A
Response: 0D 0A 01 00 XX 00 XX

Authenticate Reader with PIN '0000000000000000' to load VC Polling Enc key to reader non-volatile memory
Command: 0D 0A 0B 00 F5 83 00 00 00 00 00 00 00 00 00 7D
Response: 0D 0A 01 00 XX 00 XX

Load MIFARE Plus VC Polling Enc Key to reader non volatile memory (PCD Key No: 0x01 and Key: 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF)
Command: 0D 0A 15 00 EB 82 03 01 80 A0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 6A
Response: 0D 0A 01 00 XX 00 XX

Authenticate Reader with PIN '0000000000000000' to load VC Select Mac key to reader non-volatile memory
Command: 0D 0A 0B 00 F5 83 00 00 00 00 00 00 00 00 00 7D
Response: 0D 0A 01 00 XX 00 XX

Load MIFARE Plus VC Select Mac Key to reader non volatile memory (PCD Key No:0x02 and Key:0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF)
Command: 0D 0A 15 00 EB 82 03 02 00 A0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF E9
Response: 0D 0A 01 00 XX 00 XX

Issue Virtual Card Support command (This is an optional command - refer spec for further details)
Command: 0D 0A 19 00 E7 04 00 FF FB 00 00 11 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 AF
Response: 0D 0A 03 00 XX 00 90 00XX

Issue Virtual Card Support Last command
Command: 0D 0A 19 00 E7 04 00 FF FB 00 00 11 4B 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 A6
Response: 0D 0A 13 00 XX 00 XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX 90 00 XX

Issue Select Virtual Card command
Command: 0D 0A 19 00 E7 04 00 FF FB 00 00 11 40 00 0B 04 81 53 A9 61 28 80 00 00 00 00 00 00 00 00 1C
Response: 0D 0A 03 00 XX 00 90 00 XX

Issue Deselect Virtual Card command
Command: 0D 0A 09 00 F7 04 00 FF FB 00 00 01 48 00 B9
Response: 0D 0A 03 00 XX 00 90 00 XX

SCardDisconnect
Command: 0D 0A 02 00 FE 02 00 FE
Response: 0D 0A 01 00 FF 00 XX

SL3 proximity check commands

SCardStatus
Command: 0D 0A 02 00 FE 03 00 FD
Response: 0D 0A 02 00 FE 00 01 XX

SCardConnect
Command: 0D 0A 02 00 FE 01 00 FF
Response: 0D 0A 07 00 F9 00 XX XX XX XX XX XX XX

Authenticate Reader with PIN '0000000000000000' to load Card Configuration key to the reader non-volatile memory
Command: 0D 0A 0B 00 F5 83 00 00 00 00 00 00 00 00 00 00 7D
Response: 0D 0A 01 00 XX 00 XX

Load MIFARE Plus Card Configuration Key to reader non-volatile memory (PCD Key No:0x01 and Key:0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF)
Command: 0D 0A 15 00 EB 82 03 01 01 90 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF F9
Response: 0D 0A 01 00 XX 00 XX

Authenticate with card using the card configuration key loaded in to the reader memory
Command: 0D 0A 0B 00 F5 04 00 FF FB 00 00 03 76 01 90 00 F8
Response: 0D 0A 03 00 XX 00 90 00XX

Set the PC mandatory byte in the Field Configuration Block
Command: 0D 0A 1B 00 E5 04 00 FF FB 00 00 13 A1 03 B0 00 55 AA 00 00 00 00 00 00 00 00 00 00 00 00 00 9C
Response: 0D 0A 03 00 XX 00 90 00 XX

Authenticate Reader with PIN '0000000000000000' to load Proximity Check key to reader non-volatile memory
Command: 0D 0A 0B 00 F5 83 00 00 00 00 00 00 00 00 00 00 7D
Response: 0D 0A 01 00 XX 00 XX

Load the Proximity Check key to reader non-volatile memory (PCD Key No:0x08 and Key:0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF)
Command: 0D 0A 15 00 EB 82 03 08 01 A0 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF E2
Response: 0D 0A 01 00 XX 00 XX

Issue Proximity check command to the card
Command: 0D 0A 09 00 F7 04 00 FF FB 00 00 01 F0 00 11
Response: 0D 0A 03 00 XX 00 90 00 XX

Authenticate Reader with PIN '0000000000000000' to load Card Configuration key to the reader non-volatile memory
Command: 0D 0A 0B 00 F5 83 00 00 00 00 00 00 00 00 00 00 7D
Response: 0D 0A 01 00 XX 00 XX

Clear the Proximity Check mandatory byte in the Field Configuration Block
Command: 0D 0A 1B 00 E5 04 00 FF FB 00 00 13 A1 03 B0 00 55 55 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F1
Response: 0D 0A 03 00 XX 00 90 00 XX

SCardDisconnect
Command: 0D 0A 02 00 FE 02 00 FE
Response: 0D 0A 01 00 FF 00 XX

8 Reader Firmware

8.1 Flavors

The below provided information shows the available firmware flavors for Multi-ISO RS232 readers:

ePC/SC	Proprietary PC/SC stack (similar to standard PC/SC) embedded inside the reader firmware.

8.2 Upgrade

The steps to update the reader firmware using the Identive Card Reader Suite application are shown in the following document:

Identive_Multi-X_Firmware_Update_Manual_xx.pdf

If you want to embed the reader firmware update functionality into your own application you can use the “DFU Console” application. See the following document for details:

Identive_DFU_Console_UM_xx.pdf

Appendix A Terms and Abbreviations

Terms / Abbreviations	*Description*
3KTDES	3-Key Triple Data Encryption Standard
ACK	Acknowledgement
AES	Advanced Encryption Standard
AFI	Application Family Identifier
APDU	Application Protocol Data Unit
API	Application Programming Interface
ATR	Answer to Reset
CID	Card ID Number
CRC	Cyclic Redundancy Check
DCS	Data Checksum
DES	Data Encryption Standard
DFU	Device Firmware Upgrade
DSFID	Data Storage Format Identifier
EAS	Electronic Article surveillance
e-PC/SC	Embedded-PC/SC
FWT	Frame Waiting Time
GUI	Graphical User Interface
HF	High Frequency
ICC	Integrated Circuit Card
ISO	International Standard Organization
LCS	Length Checksum
LSB	Least Significant Byte
MIFARE UL	MIFARE Ultralight
MIFARE ULC	MIFARE Ultralight with cryptographic engine
MSB	Most Significant Byte
NACK	Negative Acknowledgement
NFC	Near Field Communication
PC	Personal Computer
PC/SC	Personal Computer/Smart Card
PCD	Proximity Coupling Device
PICC	Proximity integrated circuit card
PIN	Personal Identification Number
RF	Radio Frequency
RFID	Radio Frequency Identification
RoHS	Restriction of Hazardous Substance
SLx	Security Level – x
TDES	Triple Data Encryption Standard
TOM	Tag On Metal
UART	Universal Asynchronous Receiver Transmitter
UID	Unique Identifier

Table 17 - Terms and Abbreviations

Appendix B References

[R1] ISO/IEC 15693 Part 3, Identification cards – Contactless integrated circuit(s) cards – Vicinity card(s)
[R2] Interoperability Specification for ICCs and Personal Computer Systems Part 3
[R3] NXP MIFARE® DESFire Datasheet (M075031.pdf)
[R4] Microsoft's PC/SC reference documentation is included in most Visual Studio help systems and available online at http://msdn.microsoft.com. Enter "WinSCard" or "SCardTransmit" keywords in the search box.
[R5] PC/SC workgroup: http://www.pcscworkgroup.com/
[R6] ISO/IEC 7816-3 Third Edition 2006-11-01
[R7] ISO/IEC 7816-4 Second Edition 2005-01-15
[R8] ISO/IEC 14443-4 First Edition 2001-02-01
[R9] ISO/IEC 14443-4 Amendment-1 2006-03-15
[R10] Atmel CryptoRF Specification (AT88SCxxxxCRF) Rev 2.0 2007-04-13
[R11] NXP MIFARE® DESFire EV1 Functional Specification (MF3ICD81)
[R12] Philips CL RC632 Multiple Protocol Contactless Reader IC Datasheet Rev 3.0 May 2003