Module Protocol

1.Communication protocols:

1.1 The data format

1.1.1 Host Package Format (host to reader)

STX	SEQ	DADD	CMD	DATA LENGTH	TIME	DATA[0..N]	BCC	ETX

(BCC) = SEQ ⊕ DADD⊕ CMD ⊕ DATALENGTH⊕ TIME ⊕DATA [0] ⊕ … ⊕ DATA [n], where ⊕ is the “EOR”.（RXOR）

1.1.2 Return Package Format (reader to host)

STX	SEQ	DADD	CMD	DATA LENGTH	STATUS	DATA[0..N]	BCC	ETX

(BCC) = SEQ ⊕ DADD⊕ CMD ⊕DATA LENGTH⊕ STATUS⊕ DATA [0] ⊕ … ⊕ DATA [n], where ⊕ is the “EOR”.

1.2 Description of bytes in the data packet:

Field	Length	Description	Remark
STX	1	0xa8 - ‘Start Byte’ – Standard control bytes. Indicates the start of a data packet	
SEQ[1]	1	Random Code	Address bits are reserved for handling device addresses over 255.
DADD	1	Device address is used for multiple machine communication, only address matching can be used for data communication, 0x00 and 0xFF addresses are broadcast addresses.	
CMD	1	Command Code One byte of the command sent by the upper unit to the lower unit.	
DATA LENGTH	2	Data length includes TIME/STATUS +DATA field	The high byte comes first, the low byte comes second
STATUS	1	Lower computer return status, one byte	00 means the command is executed correctly and the others are error codes
TIME	1	Used for specific command time control, timeout processing, other commands (most) the parameter is 0	

DATA [0-N]	2000	It is used as command parameters when sent by the upper computer and as return data when sent by the lower computer with variable length. The maximum length is 512, and it will not be processed when it is out of range. It will reply directly/show that the command is too long and wait for the next command.	
BCC	1	Xor check bit, which verifies data but does not contain STX and ETX	
ETX	1	0xa9 - 'Terminating byte' – Standard control byte. Indicates the end of a data packet	

1.3 Command Code Summary Table

Command Code List			
CMD	**Name**	Description:	**Remark**
System Commands (0x00-0x1F)			
0x01	CMD_GetAddress	Obtain device communication address	
0x02	CMD_GetSoftware_Version	Obtain the device software version	
0x03	CMD_SetBaudRate	Set the baud rate for device communication	
0x04	CMD_SetAddress	Set the communication address of the device	
0x05	CMD_SetReader_SerialNum	Set the factory serial number of the device	
0x06	CMD_GetReader_SerialNum	Obtain the factory serial number of the device	
0x09	CMD_SetWorkmode	Set working mode	
0x0A	CMD_GetWorkmode	Get working mode	
0x0C	CMD_GetCardUID	Get the physical UID of the read card	
0x0D	CMD_OpenRFAntenna	Turn on RF antenna [注1]	
0x0E	CMD_CloseRFAntenna	Turn off RF antenna	
High Level MIFARE and TypeA Basics Commands(0x20-0x2F)			
0x20	CMD_MF_ Halt	Card Halt	
0x21	CMD_TYPEA_Request	TypeA search card	
0x22	CMD_TYPEA_ Anticollision	TypeA Anti-rush	
0x23	CMD_TYPEA_Select	TypeA select card	
0x24	CMD_MF_Read	MIFARE S50/S70 read	
0x25	CMD_MF_Write	MIFARE S50/S70 write	

0x26	CMD_GetTypeAUID	Get TYPEA card UID 注3	
0x27	CMD_MF_Initvalue	Initialize value blocks	
0x28	CMD_MF_ Increment	MIFARE S50/S70 Block Value Added	
0x29	CMD_MF_ Decrement	MIFARE S50/S70 Block impairment	

2.1 System Commands

2.1.1 CMD_GetAddress (0x01)

Description: Get the device communication address

Sending data：0x01

Return Data：

STATUS 0x00 – OK
DATA[0] Device Address

2.1.2 CMD_GetSoftware_Version (0x02)

Description: Get the device software version number

Sending data： 0x02

Return Data：

STATUS: 0x00 – OK
DATA[0..N]: Software Version Information

2.1.3 CMD_SetBaudRate (0x03)

Description: Set the serial port baud rate

Sending data：0x03

DATA[0]

0x00 – 9600 bps
0x01 – 19200 bps
0x02 – 38400 bps
0x03 – 57600 bps
0x04 – 76800 bps
0x05 – 115200 bps

Return Data：

STATUS 0x00 - OK

2.1.4 CMD_SetAddress (0x04)

Description: Set the device address

Sending data： 0x04

DATA[0] Device Address

Return Data：

STATUS: 0x00 – OK

2.1.5 CMD_SetReader_SerialNum (0x05)

Description: Set the factory serial number of the device

Sending data： 0x05

DATA[0-8] 8-byte serial number

Return Data：

STATUS: 0x00 – OK

2.1.6 CMD_GetReader_SerialNum (0x06)

Description: Get the factory serial number of the device

Sending data： 0x06

Return Data：

STATUS: 0x00 – OK

DATA[0-8] 8-byte serial number

2.1.9 CMD_SetWorkmode (0x09)

Description: Set the working mode

Sending data： 0x09

DATA[0] :0x00-Passive action mode 0x01-Active working mode

Return Data：

STATUS: 0x00 – OK

2.1.10 CMD_GetWorkmode (0x0A)

Description: Get working mode

Sending data： 0x0A

Return Data：

STATUS: 0x00 – OK

DATA[0] :0x00-Passive action mode 0x01-Active working mode

2.1.12 CMD_GetCardUID (0x0C)

Description：Get the physical UID of the card read, as long as the card is supported by the device will be returned, this command does not need to do to prevent repeated swipes

Sending data： 0x0C

Return Data：

STATUS: 0x00 – OK

DATA[0]: Card Type // 14443A Return Sak value as per actual。0x00, SFZ,0x01 15693 0x02 Felica 0x03 HID Iclass

DATA[0-N] : Card Physical UID

2.1.13 CMD_OpenRFAntenna (0x0D)

Description: Turn on the RF antenna

Sending data： 0x0D

Return Data：

STATUS: 0x00 – OK

2.1.14 CMD_CloseRFAntenna (0x0E)

Description: Turn off the RF antenna

Sending data： 0x0E

Return Data：

STATUS: 0x00 – OK

2.1.16 CMD_Control_Buzzer (0x11)

Description: Buzzer operation

Sending data：N/A

DATA [0]: The number of cycles of BUZZER chirping in one cycle (one cycle is 100ms)

DATA [1]: Number of buzzer status cycles (one cycle of one second)

Return Data：
STATUS: 0x00 – OK

2.2 High Level MIFARE and TypeA Basics Commands

2.2.1 CMD_TYPEA_Halt (0x20)

Description: Set the card to halt status
Sending data:0x20
Return Data:
STATUS 0x00 – OK

2.2.2 CMD_TYPEA_Request (0x21)

Description: TypeA search card
Sending data:0x20
DATA[0]: Card Search Mode 0x26 –Idle Mode
0x52 –All Mode
Return Data:
STATUS 0x00 – OK

2.2.3 CMD_TYPEA_ Anticollision (0x22)

Description: TypeA anti-punch
Sending data：0x21
DATA[0]: 0x00 First time 0x01 Second time 0x02 Third time
Return Data:
STATUS 0x00 – OK
DATA[0]: 0x00 – A card is detected. Default is 0
DATA[1..4]: UID – Card Chip Number

2.2.4 CMD_TYPEA_Select (0x23)

Description: TypeA card selection
Sending data：
DATA[0]: 0x00 First time 0x01 Second time 0x02 Third time
DATA[1..4]: UID – Card chip number of the card to be selected
Return correctly：
STATUS: 0x00 – OK
DATA[0..3]: UID – Card Chip Number

2.2.5 CMD_MF_Read (0x24)

Description: Read MF content
Sending data：
DATA[0] Mode Control
Bit0 Request Mode. 0=Request Idle, 1 = Request All
Bit1 Request Mode. 0 = checksum for KEYA, 1 = checksum for KeyB
DATA[1] The length value of the number of blocks to be read, i.e. how many blocks to read. Value range 01-04
DATA[2] The starting address of the block to be read. The range of values: hex 00-3F i.e. 00 blocks to 63 blocks.
DATA[3-8] Key
Return correctly：
STATUS 0x00 – OK
DATA[0-3] Card Serial Number (LL LH HL HH)
DATA[4..N] Data read from the card.

2.2.6 CMD_MF_Write (0x25)

Description: Write MF content

Sending data：
DATA[0] Mode Control
Bit0 Request Mode. 0=Request Idle, 1 = Request All
Bit1 Request Mode. 0 = checksum for KEYA, 1 = checksum for KeyB
DATA[1] The length value of the number of blocks to be written, i.e. how many blocks to read. Value range 01-04
DATA[2] The starting address of the block to be written. The range of values: hex 00-3F i.e. 00 blocks to 63 blocks.
DATA[3-8] Key
DATA[9-N] Data to be written to the memory blocks.
Return correctly：
STATUS 0x00 – OK
DATA[0-3] Card Serial Number (LL LH HL HH)

2.2.7 CMD_GetTypeAUID (0x26)

Description: Get TYPEA card UID

Sending data： 0x26
Return data：
STATUS: 0x00 – OK
DATA[0]: Card Type
DATA[0-N] : Card Physical UID

2.2.8 CMD_MF_Initvalue (0x27)

Description: Initialize the value block

Sending data：
DATA[0] Mode Control
Bit0 Request Mode. 0=Request Idle, 1 = Request All
Bit1 Request Mode. 0 = checksum for KEYA, 1 = checksum for KeyB
DATA[1] The Sector used for Value storage. Sector number to be initialized 00-0F
Block0 –Opened for user use.
Block1 –Value Stored Block
Block2 –Value Backup Block.
DATA[2-7]: KEY（SIX BYTES）
DATA[8-11]: The initial value to be stored to the value block. (Value format : LL LH HL HH)
Return correctly：
STATUS: 0x00 – OK
DATA[0-3]: Card Serial Number (LL LH HL HH)

2.2.9 CMD_HL_Decrement (0x28)

Description: MF Card Value Impairment

Sending data：
DATA[0] Mode Control
Bit0 Request Mode. 0=Request Idle, 1 = Request All
Bit1 Request Mode. 0 = checksum for KEYA, 1 = checksum for KeyB
DATA[1] The area code where the data is stored.
DATA[2-7] KEY（SIX BYTES）
DATA[8-11] Value after decrement. (Data Format : LL LH HL HH)
Return correctly：
STATUS 0x00 – OK
DATA[0-3] Card Chip Number(LL LH HL HH)
DATA[4-7] Value after subtraction (LL LH HL HH)
Error Return：
STATUS: 0x01 –FAIL

2.2.10 CMD_HL_Increment (0x29)

Description: MF Card Value Added

Sending data：

DATA[0] Mode Control

Bit0 Request Mode. 0=Request Idle, 1 = Request All

Bit1 Request Mode. 0 = checksum for KEYA, 1 = checksum for KeyB

DATA[1] The area code where the data is stored.

DATA[2-7] KEY（SIX BYTES）

DATA[8-11] The value to be increased to the value block. (Data Format : LL LH HL HH)

Return correctly：

STATUS: 0x00 – OK

DATA[0-3] Card Chip Number(LL LH HL HH)

DATA[4-7] Value after increase(LL LH HL HH)

Error Return：

STATUS 0x01 –FAIL

3. Wrong instruction

3.1 Instruction execution success return status to 0x00, plus instruction return data

3.2 The instruction execution fails to return a status of 0x01.