UHF Hand Reader Reader Writer

User Manual V1.2

Table of contents

[1. Docking communication protocol 2](#_Toc1086)

[1.1 Communication parameters 2](#_Toc24821)

[1.2 Data frame format 2](#_Toc8968)

[2 . Command frame set 3](#_Toc27759)

[2.1 command list 3](#_Toc8149)

[2.2 Module general control commands 5](#_Toc26172)

[2.2.1 RFM\_MODULE\_INT（Initialize device） 5](#_Toc751)

[2.2.2 RFM\_REBOOT（Restore device to factory settings） 5](#_Toc26644)

[2.2.3 RFM\_SET\_PWR (Set RF output power) 5](#_Toc9753)

[2.2.4 RFM\_SET\_GET\_RFID (Set/read the RF protocol standard supported by the module) 6](#_Toc1562)

[2.2.5 RFM\_SET\_ALL\_PARAM (Set all configurable parameters) 7](#_Toc12444)

[2.2.6 RFM\_GET\_ALL\_PARAM (Read all configurable parameters) 13](#_Toc18296)

[2.2.7 RFM\_GET\_BATTERY\_CAPACITY (Get battery level) 13](#_Toc7661)

[2.2.8 RFM\_SET\_GET\_BLUETOOTH\_NAME（Set/get Bluetooth device name） 14](#_Toc28383)

[2.2.9 RFM\_SET\_GET\_OTUPUTMODE（Set Bluetooth output mode） 15](#_Toc20168)

[2.2.10 RFM\_REPORT\_KEYSTA（Report button start and end status） 16](#_Toc1984)

[2.2.11 RFM\_SET\_GET\_READMODE (Set/get read mode) 17](#_Toc8179)

[2.3 International standard (ISO 18000-6C) protocol related commands 18](#_Toc26231)

[2.3.1 RFM\_INVENTORYISO\_CONTINUE (Label inventory) 18](#_Toc7234)

[2.3.2 RFM\_INVENTORY\_STOP (stop inventory) 20](#_Toc31437)

[2.3.3 RFM\_SETISO\_SELECTMASK (Select the tag you want to operate) 20](#_Toc19350)

[2.3.4 RFM\_READISO\_TAG (Read tag data) 22](#_Toc3955)

[2.3.5 RFM\_WRITEISO\_TAG (Write tag data) 24](#_Toc28389)

[2.3.6 RFM\_LOCKISO\_TAG (Lock tag data) 26](#_Toc9827)

[2.3.7 RFM\_KLENLISO\_TAG (Kill Tags) 28](#_Toc14747)

[Appendix A. Operational status returned by tags 30](#_Toc24912)

[Appendix B. CRC16 checksum reference C code 31](#_Toc23240)

[Appendix C. Definition of STATUS. 32](#_Toc7818)

# Docking communication protocol

This module can communicate with external applications via USB or BLE.

## Communication parameters

## USB 2.0 full speed. BLE 4.2.

## **1.2** Data frame format

The data packets sent by the upper-layer application are hereinafter referred to as "commands", and the data packets returned by the module to the upper-layer application are hereinafter referred to as "responses". The length units of all the following data segments are in bytes.

Data transmission order: For each data item consisting of multiple bytes, the most significant byte is sent first, and the least significant bit within the byte is sent first.

The data frame format of the command is shown in Table A-2.：

Table A-2 Command data frame format

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **MSB** |  |  |  |  | **LSB** |
|  | Control Field | | | Information Field | EpLENogue Field |
| HEAD | ADDR | CMD | LEN | Data[] | CHECK |
| 1Byte | 1Byte | 2Bytes | 1Byte | 0~255Byte | 2Byte |

The response data frame format is shown in Table A-3.：

Table A-3 Response data frame format

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **MSB** |  |  | |  | | **LSB** |
|  | Control Field | | | Information Field | | EpLENogue Field |
| HEAD | ADDR | CMD | LEN | STATUS | Data[] | CHECK |
| 1Byte | 1Byte | 2Bytes | 1Byte | 1Byte | 0~254Byte | 2Byte |

The data frame structure includes the following three parts: frame control field (Control Field), information data field (Information Field) and frame tail field (EpLENogue Field).

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | Length  (byte) | Illustrate |
| Control Field | HEAD | 1 | HEAD is fixed to the hexadecimal number 0xCF, and this byte is used for data frame synchronization. |
| ADDR | 1 | Reader address. Address range: 0x00~0xFE, 0xFF is the broadcast address, the reader only responds to commands that are the same as its own address and whose address is 0xFF. The address of the reader/writer is 0x00 when it leaves the factory. |
| CMD | 2 | Command code, command word definition is shown in Table A-7. |
| LEN | 1 | The length is the data length of all bytes of the actual Information Field, and the maximum data length is 255Bytes (0xFF). |
| Information Field | STATUS | 1 | STATUS is the execution status of the host computer command contained in the module's response. STATUS only exists in the response data frame returned by the module, and there is no STATUS part in the command frame issued by the upper-layer application. STATUS is 0 indicating that the command execution is successful. Successful execution here only means that the module successfully receives the tag response. If the tag response contains the tag execution status, you should further determine whether the tag execution status is correct. The definition of STATUS is shown in Table A-6. |
| Data[] | indefinite | parameter domain. In the actual command, it may not exist. Data[] is the actual data that needs to be transferred, and the valid bytes of Data[] will be specifically defined in each command format. |
| EpLENogue Field | MSB-CRC16 | 1 | CRC16 high byte. CRC16 is the CRC16 value from HEAD to Data[] |
| LSB-CRC16 | 1 | CRC16 low byte. |

See Appendix B for the CRC16 reference code.

# 2 . Command frame set

The UHF RFID reader module is referred to as "module" in the following description.

## **2.1 command list**

Table A-7 Control command example list

|  |  |  |  |
| --- | --- | --- | --- |
| **Command Name** | **CMD control byte** | **Functional Description** | **Remark** |
| **EPC command** | | | |
| RFM\_INVENTORYISO\_CONTINUE | 0x0001 | Tag inventory (process) |  |
| RFM\_INVENTORYISO\_STOP | 0x0002 | Stop tag inventory |  |
| RFM\_READISO\_TAG | 0x0003 | Read tag data |  |
| RFM\_WRITEISO\_TAG | 0x0004 | Write tag data (process) |  |
| RFM\_LOCKISO\_TAG | 0x0005 | Lock tag data (process) |  |
| RFM\_KLENLISO\_TAG | 0x0006 | Kill tag (process) |  |
| RFM\_SETISO\_SELECTMASK | 0x0007 | Set the tag EPC number |  |
| **Module custom command** | | | |
| RFM\_MODULE\_INT | 0X0050 | Initialize the device | Stop all actions |
| RFM\_GET\_DEVICEINFO | 0x0051 | Bluetooth obtains all module version numbers and sn codes |  |
| RFM\_REBOOT | 0x0052 | Restore factory settings | Restore Defaults |
| RFM\_GET\_BATTERY\_CAPACITY | 0x0083 | Get battery level |  |
| RFM\_SET\_ALL\_PARAM | 0x0071 | Set all basic parameters | Package all basic parameters and set them all at once |
| RFM\_GET\_ALL\_PARAM | 0x0072 | Read all basic parameters | Package all basic parameters and read them all at once |
| RFM\_SET\_GET\_S-PERMISSION\_PARAM | 0X0076 | Specific read permission settings | H103 |
| RFM\_SET\_GET\_BLUETOOTH\_NAME | 0x0086 | Set the Bluetooth device name |  |
| RFM\_SET\_BLU\_HID\_SEND | 0x0087 | Bluetooth keyboard output |  |
| RFM\_SET\_GET\_OUTPUTMODE | 0x0088 | Set/get the selected output mode |  |
| RFM \_REPORT\_KEYSTA | 0x0089 | Report key start and end status |  |
| RFM\_SET\_GET\_READMODE | 0x008E | Set/get the code reading mode | H103,H104 |

## 2.2 Module general control commands

### 2.2.1 RFM\_MODULE\_INT（Initialize device）

* The device performs initial configuration according to the stored parameters.
* Command format

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | CHECK |
| 0xCF | 0xFF | 0x0050 | 0x00 | 2Byte |

* Response format and status bytes

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | STATUS | CHECK |
| 0xCF | 0x00 | 0x0050 | 0x01 | 1Byte | 2Byte |

 STATUS：This command will only return successful execution (value is 0x00), other values are invalid;

### 2.2.2 RFM\_REBOOT（Restore device to factory settings）

Restore factory settings command. When the command is successfully executed, the module will restore factory settings (does a restart be required?）。

* Command format

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | CHECK |
| 0xCF | 0xFF | 0x0052 | 0x00 | 2Byte |

* Response format and status bytes

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | STATUS | CHECK |
| 0xCF | 0x00 | 0x0052 | 0x01 | 1Byte | 2Byte |

 STATUS：This command will only return successful execution (value is 0x00), other values are invalid;

### 2.2.3 RFM\_SET\_PWR (Set RF output power)

This command is used to set the RF output power of the module. The user needs to use this command to set the RF output power of the module before using the module to operate the tag. If the user does not set the RF output power of the module, the module will use the default settings when working.

* Command format

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | PAYLOAD | | CHECK |
| Power | Resv |
| 0xCF | 0xFF | 0x0053 | 0x02 | 1Byte | 1Byte | 2Byte |

* + Power：Output power, unit: dBm.

H100 The value range of this parameter of the device is: [1, 20]dBm

The value range of this parameter for H102 reader is：[1, 26]dBm。

The value range of this parameter for H103 reader is：[1, 33]dBm。

* + Resv：System reserved field, default 0x00;
  + Response format and status bytes

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | STATUS | CHECK |
| 0xCF | 0x00 | 0x0053 | 0x01 | 1Byte | 2Byte |

* + STATUS：
  1. 0x00：Command execution successful；
  2. 0x01：The module does not support this output power value；
  3. Other values: invalid；

### 2.2.4 RFM\_SET\_GET\_RFID (Set/read the RF protocol standard supported by the module)

This command sets/reads the RFID protocol standard specification of the module (by issuing this command, you can set the protocol standard to determine whether the module is successfully connected)

* Command format

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | PAYLOAD | | CHECK |
| Option | RFIDPRO |
| 0xCF | 0xFF | 0x0059 | 1Byte | 1Byte | NC or 1Byte | 2Byte |

* + Option：Command control options

0x01: Setting, followed by RFID of 1Byte length；

0x02: Read, no RFID is connected thereafter；

Other values: invalid；

* + RFIDP：Protocol options, see the table below for details.
* Response format and status bytes

Set response：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | STATUS | Option | CHECK |
| 0xCF | 0x00 | 0x0059 | 1Byte | 1Byte | 1Byte | 2Byte |

Get response：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | STATUS | PAYLOAD | | CHECK |
| Option | RFIDPRO |
| 0xCF | 0x00 | 0x0059 | 1Byte | 1Byte | 1Byte | 1Byte | 2Byte |

|  |  |  |
| --- | --- | --- |
| Field | byte | describe |
| STATUS | 1 | 0x00: Command execution successful; 0x01: Parameter error. |
| Option | 1 | 0x01: Set; 0x02: Get |
| RFID | 1 | 0x00: ISO 18000-6C; 0x01: GB/T 29768; 0x02: GJB 7377.1; currently only ISO 18000-6C is supported. |

### 2.2.5 RFM\_SET\_ALL\_PARAM (Set all configurable parameters)

This command is used to set all configurable parameters of the device. Users need to use this command to set all configurable parameters of the device before using the module to operate tags. If the user does not make this setting, the device will use the default settings when working.。

* Command format

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | PAYLOAD | | | | | | | |
| Addr | RFIDPRO | Work  Mode | Interface | Baudrate | WGSet | Ant | RfidFreq |
| 0xCF | 0xFF | 0x0071 | 0x19 | 1Byte | 1Byte | 1Byte | 1Byte | 1Byte | 1Byte | 1Byte | 8Bytes |
|  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| PAYLOAD | | | | | | | | | | CHECK |
| RfidPower | InquiryArea | QValue | Session | AcsAddr | AcsDataLen | FilterTime | TriggerTime | BuzzerTime | Polling  Interval |
| 1Byte | 1Byte | 1Byte | 1Byte | 1Byte | 1Byte | 1Byte | 1Byte | 1Byte | 1Byte | 2Bytes |

* + Addr：The communication address of the device, the default is 0x00. This address cannot be 0xFF. If set to 0xFF, the read-write module will return parameter error information
  + RFIDPRO：Device radio frequency RFID protocol standard specification, 0x00: ISO 18000-6C; 0x01: GB/T 29768; 0x02: GJB 7377.1; currently only supports ISO 18000-6C
  + WorkMode：The working mode of the device, default value 0。

|  |  |
| --- | --- |
| WorkMode | Operating mode |
| 0 | answer mode |
| 1 | Active mode |
| 2 | trigger mode |

* + Interface：The communication interface of the device, the default value is 0x80, the specific explanation is as follows:

|  |  |
| --- | --- |
| Interface | Interface Type |
| 0x80 | RS232 |
| 0x40 | RS485 |
| 0x20 | RJ45 |
| 0x10 | WiFi |
| 0x01 | USB |
| 0x02 | keyboard |
| 0x04 | CDC\_COM |

* + Baudrate：Serial port baud rate, the default value is 4, the specific explanation is as follows：

|  |  |
| --- | --- |
| baudrate | Actual baud rate |
| 0 | 9600bps |
| 1 | 19200 bps |
| 2 | 38400 bps |
| 3 | 57600 bps |
| 4 | 115200 bps |

* + WGSet：Configuration parameters of the Wiegand data output interface, the default value is 0x00, the specific explanation is as follows：

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| WGSet | Bit7 | Bit6 | Bit5 | Bit4 | Bit3 | Bit2 | Bit1 | Bit0 |
| Bit definition | 0: Turn off Wiegand output  1: Turn on Wiegand output | 0：wg26  1：wg34 | 0: Low bit first  1: High position first | spare | spare | spare | spare | spare |

* + Ant：All the antenna numbers of the device represent the selected antenna bit by bit. A corresponding bit value of 1 indicates that the antenna is used, and a value of 0 indicates that the antenna is not used. Starting from the low bit, bit 0 indicates antenna No. 1, and bit 0 indicates antenna No. 1. Bit 1 represents antenna No. 2, and so on, which can represent up to 8 antennas; different modules support different antennas, depending on the specific situation; the default value 0x01 represents antenna No. 1.
  + RfidFreq：The RFID frequency related parameters of the device are used to select the frequency band and the upper limit frequency point and lower limit frequency point in each frequency band. The length is 8 Bytes. The specific parameters are as follows:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| RfidFreq | | | | |
| REGION | STRATFREI | STRATFRED | STEPFRE | CN |
| 1 Byte | 2Byte | 2Byte | 2Byte | 1Byte |

Definition of each byte：

To set the frequency, first determine the frequency range according to REGION, and then refer to STRATFREI, STRATFRED, STEPFRE, and CN to calculate the specific frequency range.

|  |  |  |
| --- | --- | --- |
| Field | byte | describe |
| REGION | 1 | Frequency band range of each country：  0x00: User customized according to needs；  0x01：US [902.75~927.25]  0x02：Korea [917.1~923.5]  0x03：EU [865.1~868.1]  0x04：JAPAN [952.2~953.6]  0x05：MALAYSIA [919.5~922.5]  0x06：EU3 [865.7~867,5]  0x07：CHINA\_BAND1 [840.125~844.875]  0x08：CHINA\_BAND2 [920.125~924.875] |
| STRATFREI | 2 | Megahertz The integer part of the starting frequency; such as 920.125MHz, STRATFREI = 920 = 0x0398, high byte = 0x03, low byte = 0x98; |
| STRATFRED | 2 | Megahertz The decimal part of the starting frequency; such as 920.125MHz, STRATFRED =125, high byte = 0x00, low byte = 0x7D |
| STEPFRE | 2 | Frequency step (KHz), please refer to the calculation formula of each frequency band; such as 125KHz, STEPFRE =125, high byte = 0x00, low byte = 0x7D; |
| CN | 1 | Number of channels； |

Frequency calculation formula： Minimum frequency point：Fmin = STRATFREI + STRATFRED/1000 （unit：MHz）

Maximum frequency point：Fmax = Fmin + STEPFRE\*CN/1000 （单位：MHz）

Calculation formula for each frequency band：(The set frequency range must be within the standards of each country)

Chinese band2： Fs = 920.125 + CN \* 0.25 (MHz) where CN∈[0, 19]。

US band： Fs = 902.75 + CN \* 0.5 (MHz) where CN∈[0,49]。

Korean band： Fs = 917.1 + CN \* 0.2 (MHz) where CN∈[0, 31]。

EU band: Fs = 865.1 + CN\*0.2(MHz) where CN∈[0, 14]。

Ukraine band: Fs = 868.0 + CN\*0.1(MHz) where CN∈[0, 6]。

Peru band： Fs = 916.2 + CN\*0.9(MHz) where CN∈[0, 11]。

Chinese band1： Fs = 840.125 + CN \* 0.25 (MHz) where CN∈[0, 19]。

EU3 band： Fs = 865.7 + CN \* 0.6(MHz) where CN∈[0, 3]。

US band3： Fs = 902 + CN \* 0.5 (MHz) where CN∈[0,52]。

Taiwan band： Fs = 922.25 + CN \* 0.5 (MHz) where CN∈[0,11]。

* + RfidPower：The RFID output power of the device, the unit is: dBm, the value range is: [0, 30]dBm, others are invalid.
  + InquiryArea：The storage area of the tag that the device wants to access. 0x00: Reserved area; 0x01 (default): EPC storage area; 0x02: TID storage area; 0x03: USER storage area; 0x04: EPC+TID; 0x05: EPC+USER; 0x06: EPC+TID+USER; other values are reserved. If other values appear in the command, a parameter error message will be returned.
  + QValue：The initial Q value used when querying EPC tags. The Q value should be set so that the number of tags in the field is approximately equal to 2Q. The default value of Q value is 4, and the range of Q value is 0~15. If other values appear in the command, a parameter error message will be returned.
  + Session: Session value used when querying EPC tags, the default is 0, the value range is [0, 3], other values will return a parameter error message

|  |  |
| --- | --- |
| Session | Comment |
| 0 | Session uses S0 |
| 1 | Session uses S1 |
| 2 | Session uses S2 |
| 3 | Session uses S3 |

* + AcsAddr：The starting address of the tag storage area that the device wants to access, unit: Byte, default value: 0x00: When accessing the EPC area, 0x00 indicates the starting address of the EPC number segment except the CRC and PC segments of the EPC area; when accessing other storage areas, 0x00 Indicates the starting address of the storage area
  + AcsDataLen：The data length of the tag storage area that the device needs to access, unit: Byte, default value: 0x00.
  + FilterTime：Filtering time, within this value after successfully reading a tag data, tags with the same data are filtered out. The unit is: S, the value range is: [0, 255], others are invalid; the default value is 0, and there is no filtering.
  + TriggerTime：The query time after the device receives the trigger signal, unit: S, the default value is 1, the value range is: [0, 255], others are invalid.
  + BuzzerTime：he duration of the buzzer beeping after the device is successfully executed, the unit is: 10ms, the value range is: [0, 255], others are invalid; the default is 1, when it is 0, it means the buzzer does not sound.
  + PollingInterval：Query interval, unit: 10ms, value range: [0, 255], others are invalid, default is 1.
* Response format and status bytes

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | STATUS | CHECK |
| 0xCF | 0xXX | 0x0071 | 0x01 | 1Byte | 2Byte |

* + STATUS：
  1. 0x00：Command execution successful；
  2. 0x01：Parameter error；
  3. Other values: invalid；

### 2.2.6 RFM\_GET\_ALL\_PARAM (Read all configurable parameters)

This command is used to read the currently set RF power of the module. Users can use this command to view the power settings of the module before using the module to operate the tag.

* Command format

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | CHECK |
| 0xCF | 0xFF | 0x0072 | 0x00 | 2Byte |

* Response format and status bytes

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | PAYLOAD | | | | | | | | |
| STATUS | Addr | RFIDPRO | Work  Mode | Interface | Baudrate | WGSet | Ant | RfidFreq |
| 0xCF | 0xFF | 0x0071 | 0x1A | 1Byte | 1Byte | 1Byte | 1Byte | 1Byte | 1Byte | 1Byte | 1Byte | 8Bytes |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| PAYLOAD | | | | | | | | | | CHECK |
| RfidPower | InquiryArea | QValue | Session | AcsAddr | AcsDataLen | FilterTime | TriggerTime | BuzzerTime | Polling  Interval |
| 1Byte | 1Byte | 1Byte | 1Byte | 1Byte | 1Byte | 1Byte | 1Byte | 1Byte | 1Byte | 2Bytes |

* + STATUS：
  1. 0x00：Command execution successful；
  2. Other values: invalid；
  + Refer to other parameters RFM\_SET\_ALL\_PARAM。

### 2.2.7 RFM\_GET\_BATTERY\_CAPACITY (Get battery level)

* This command gets the battery level
* Command format

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | CHECK |
| 0xCF | 0xFF | 0x0083 | 0x00 | 2Byte |

* Response format and status bytes

* Get response:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | STATUS | Battery | CHECK |
| 0xCF | 0x00 | 0x0083 | 2Byte | 1Byte | 1Byte | 2Byte |

|  |  |  |
| --- | --- | --- |
| Field | byte | describe |
| STATUS | 1 | 0x00: Command execution successful; 0x01: Parameter error. |
| Battery | 1 | If the battery power is 20%, the data is [0x14] |

### 2.2.8 RFM\_SET\_GET\_BLUETOOTH\_NAME（Set/get Bluetooth device name）

* This command sets the Bluetooth device name
* Command format

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | PAYLOAD | | CHECK |
| Option | BleName |
| 0xCF | 0xFF | 0x0086 | 1Byte | 1Byte | NC or 1-20Byte | 2Byte |

* + Option：command control options

0x01：Setting, followed by RFID of 1Byte length;

0x02：Read, then do not connect to RFID;

Other values: invalid;

|  |  |  |
| --- | --- | --- |
| Field | byte | describe |
| Option | 1 | 0x01 set, 0x02 get |
| BleName | 1-20 | If the Bluetooth name is CF-H100, the final data is {0x43,0x46,0x2D,0x48,0x31,0x30,0x30} |

* Response format and status bytes

Set response:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | STATUS | Option | CHECK |
| 0xCF | 0x00 | 0x0086 | 1Byte | 1Byte | 1Byte | 2Byte |

Get response:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | PAYLOAD | | | CHECK |
| STATUS | Opiont | BleName |
| 0xCF | 0xFF | 0x0086 | 1Byte | 1Byte | 1Byte | 1-20Byte | 2Byte |

|  |  |  |
| --- | --- | --- |
| Field | byte | describe |
| Option | 1 | 0x01 set, 0x02 get |
| STATUS | 1 | 0x00: Command execution successful; 0x01: Parameter error. |
| BleName | 1-20 | For example, the data is {0x43,0x46,0x2D,0x48,0x31,0x30,0x30}, then the name is CF-H100 |

### **2.2.9 RFM\_SET\_GET\_OTUPUTMODE（Set Bluetooth output mode）**

This command sets the Bluetooth output mode

* Command format

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | Option | MODE | CHECK |
| 0xCF | 0xFF | 0x0088 | 0x02 | 0x01 | 1Byte | 2Byte |

* + MODE：
  1. 0x00：Bluetooth HID output;
  2. 0x01：Bluetooth transparent transmission;
  3. Other values: invalid.
* Response format and status bytes

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | STATUS | CHECK |
| 0xCF | 0x00 | 0x0088 | 0x01 | 1Byte | 2Byte |

* + STATUS：
  1. 0x00：Command execution successful；
  2. 0x01：Parameter error；
  3. Other values: invalid；

This command gets the Bluetooth output mode

* Command format

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | Option | CHECK |
| 0xCF | 0xFF | 0x0088 | 0x01 | 0x02 | 2Byte |

* Response format and status bytes

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | STATUS | MODE | CHECK |
| 0xCF | 0xFF | 0x0088 | 0x02 | 1Byte | 1Byte | 2Byte |

### 2.2.10 RFM\_REPORT\_KEYSTA（Report button start and end status）

* This command reports the start and end status of keystrokes

Command format

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | KEYSTA | CHECK |
| 0xCF | 0x00 | 0x0089 | 0x01 | 1Byte | 2Byte |

* + KEYSTA：
  1. 0x01：start；
  2. 0x02：end；
  3. Other values: invalid

### 2.2.11 RFM\_SET\_GET\_READMODE (Set/get read mode)

This command sets/gets the working parameters of the scan head

* Set command format

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | OPTION | READMODE | RECEV | CHECK |
| 0xCF | 0xFF | 0x008E | 0x09 | 0x01 | 1Byte | 7Byte | 2Byte |

* Set response

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | STATUS | CHECK |
| 0xCF | 0x00 | 0x008E | 0x01 | 1Byte | 2Byte |

* Get command format

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | OPTION | CHECK |
| 0xCF | 0xFF | 0x008E | 0x01 | 0x02 | 2Byte |

* Get response

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | STATUS | READMODE | RECEV | CHECK |
| 0xCF | 0x00 | 0x008E | 0x09 | 1Byte | 1Byte | 7Byte | 2Byte |

* + Option：command control options，1Byte。

0x01：Settings; when setting, you need to wait for 1 second to completely start the module

0x02：read；

Other values: invalid；

* + STATUS：0x00：The command was executed successfully; 0x01: Parameter error.
  + READMODE：Code reading module parameters, 1Byte.

0x01：Turn on QR code scanning mode and turn off RFID mode

0x00：Turn on RFID mode and turn off QR code scanning mode.

Other values: invalid;

* + RECEV：reserve，7Bytes。

## 2.3 International standard (ISO 18000-6C) protocol related commands

### 2.3.1 RFM\_INVENTORYISO\_CONTINUE (Label inventory)

This command is to start the international standard multi-label inventory command. The inventory function has an anti-collision algorithm.

This command can specify the inventory counting duration. If the input count count is 0, it means that the inventory tags will continue to be counted until the stop inventory command is received. During the inventory process, every time a tag is successfully counted, the newly counted tag information will be returned through a command response with a "STATUS" value of "0".

When the inventory command is successfully executed, a command response with a "STATUS" value of "0x12" will be returned, which is used to notify that the inventory command has been executed.

* Command format

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | PAYLOAD | | CHECK |
| InvType | InvParam |
| 0xCF | 0xFF | 0x0001 | 0x05 | 1Byte | 4Byte | 2Byte |

* + InvType：Inventory method：

0x00：Inventory label by time, stop the inventory after executing the specified time or stop the inventory after receiving the stop inventory command；

0x01: Count according to the number of cycles, and stop counting after performing a specified number of polls or receiving a stop counting instruction.；

* + InvParam ：Inventory method parameters：

1.If InvType is 0x00：

InvParam represents the inventory time, in seconds. If the value is 0, it means that the inventory tags will continue to be counted until the stop inventory command is received;

2.If InvType is 0x01：

InvParam represents the number of inventory counts, the unit is: times, the value must be greater than 0;

* Response format and status bytes

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | STATUS | PAYLOAD | | | | | CHECK |
| RSSI | Antenna | Channel | EPC LEN | EPC NUM |
| 0xCF | 0x00 | 0x0001 | 1Byte | 1Byte | 2Bytes | 1 Byte | 1 Byte | 1Byte | N Bytes | 2Byte |

Definition of each byte：

|  |  |  |
| --- | --- | --- |
| Field | byte | describe |
| STATUS | 1 | 0x00：The tag was successfully inventoried, and the tag information is included in PAYLOAD;  0x01：Q. The MemBank parameter value is wrong or the Length and Mask data lengths are inconsistent;  0x02：Command execution failed due to internal module error;  0x12：No tags were counted or the entire inventory command was executed;  0x17：The tag data exceeds the maximum transmission length of the serial port;  Other values: invalid; |
| RSSI | 2 | RSSI of tag ACK response, unit is dBm, signed number, negative numbers use complement format; |
| Channel | 1 | From which channel the tag data is received, the value starts from 0, 0 represents channel 0, 1 represents channel 1, and so on; |
| EPC LEN | 1 | Tag’s EPC number length (bytes); |
| EPC NUM | N Byte | The EPC number of the label; |

### 2.3.2 RFM\_INVENTORY\_STOP (stop inventory)

This command allows the user to actively stop the international standard multi-label anti-collision inventory process.

* Command format

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | CHECK |
| 0xCF | 0xFF | 0x0002 | 0x00 | 2Byte |

* Response format and status bytes

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | STATUS | CHECK |
| 0xCF | 0x00 | 0x0002 | 0x01 | 1Byte | 2Byte |

 STATUS：This command will only return successful execution (value is 0x00), other values are invalid；

### 2.3.3 RFM\_SETISO\_SELECTMASK (Select the tag you want to operate)

This command is used to set the tag EPC number required for tag operation (read, write, lock and deactivate).

* Format

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN |  | PAYLOAD | | CHECK |
| Pointer | Length | Mask |
| 0xCF | 0xFF | 0x0007 | 1Byte | 2Bytes | 1Byte | N-Bytes | 2Byte |

* + Pointer：Reserved, default value is 0x0000；
  + Length：The bit length of the EPC number to be matched. The default value is 0x00。
  + Mask：The data to be matched has a valid data length of Length bits. If Length is an odd number, the low bit of the mask needs to be padded with 0.；
* Response format and status byte

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | STATUS | CHECK |
| 0xCF | 0x00 | 0x0007 | 0x01 | 1Byte | 2Byte |

* + STATUS：
  1. 0x00：Command executed successfully；
  2. 0x01：Parameter error；
  3. Other values: invalid；

### 2.3.4 RFM\_READISO\_TAG (Read tag data)

* This command frame is for the module to read the data in the international standard protocol tag storage area.
* Before calling this method, please set the inventory conditions (for selecting tags) through the RFM\_SETISO\_SELECTMASK command. When performing international standard protocol tag data operations (reading tag data, writing tag data, locking tags, and deactivating tags), the tag will return the tag operation status. At this time, the module's response contains a byte of tag operation status. The definition of tag operation status is shown in Appendix A
* Format

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN |  | PAYLOAD | | |  | CHECK |
| Option | AccPwd | MemBank | WordPtr | WordCount |
| 0xCF | 0xFF | 0x0003 | 1Byte | 1Byte | 4 Bytes | 1Byte | 2 Bytes | 1 Bytes | 2Byte |

Definition of each field：

|  |  |  |
| --- | --- | --- |
| Fields | byte | describe |
| Option | 1 | Command options (this field is not used, invalid, default 0x00) ； |
| AccPwd | 4 | Access password, used for the tag to enter the safe state, the default value is 0x00000000； |
| MemBank | 1 | The storage area of ​​the tag to be read, the value list is as follows：  0x00：Reserved； 0x01：EPC； 0x02：TID； 0x03：User； |
| WordPtr | 2 | Points to the read start address of the logical storage area (word)； |
| WordCount | 1 | The number of words to be read cannot be 0. The default value is 4. The value range is[1,120] |

* Response format and status byte

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | STATUS | PAYLOAD | | | | | | | | CHECK |
| TagStatus | Antenna | CRC | PC | EPC LEN | EPC NUM | WordCount | Data |
| 0xCF | 0x00 | 0x0003 | 1Byte | 1Byte | 1Byte | 1Byte | 2Byte | 2Bytes | 1Byte | N  Bytes | 1Bytes | N-Byte | 2Byte |

Definition of each field：

Determine whether the command is executed successfully based on STATUS and TagStatus.

|  |  |  |
| --- | --- | --- |
| Fields | byte | describe |
| STATUS | 1 | Refer to Table A-6 STATUS definition |
| TagStatus | 1 | The operation status returned by the tag, see Appendix A for specific definitions； |
| Antenna | 1 | From which antenna is the reading |
| CRC | 2 | CRC data in the tag response data |
| PC | 2 | PC data in tag response data |
| EPC LEN | 1 | The length of the tag's EPC number (bytes)； |
| EPC NUM | N Byte | The EPC number of the label； |
| WordCount | 1 | The number of tag data words successfully read； |
| Data | N Byte | The tag data successfully read has a length of WordCount×2 bytes； |

### 2.3.5 RFM\_WRITEISO\_TAG (Write tag data)

This command is for the module to write data to the tag storage area.

Before calling this method, please set the inventory condition (for selecting tags) through the RFM\_SETISO\_SELECTMASK command.。

* Format

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | PAYLOAD | | | | | | CHECK |
| Option | AccPwd | MemBank | WordPtr | WordCount | Data |
| 0xCF | 0xFF | 0x0004 | 1Byte | 1Byte | 4Byte | 1Byte | 2Byte | 1Byte | N-Byte | 2Byte |

Definition of each field：

|  |  |  |
| --- | --- | --- |
| Fields | byte | describe |
| Option | 1 | Command options (this field is not used, invalid, default 0x00) ； |
| AccPwd | 4 | Access password, used for the tag to enter the safe state, the default value is 0x00000000； |
| MemBank | 1 | The storage area of ​​the tag to be read, the value list is as follows：  0x00：Reserved； 0x01：EPC； 0x02：TID； 0x03：User； |
| WordPtr | 2 | Points to the read start address of the logical storage area (words)； |
| WordCount | 1 | The number of data words that need to be written to the tag (1 word is two bytes), must be greater than 0； |
| Data | N-Byte | The data to be written to the tag must be an integer multiple of words, with a length of 1 to WordCount words. |

* Response format and status byte

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | STATUS |  | | PAYLOAD | | | | CHECK |
| TagStatus | Antenna | CRC | PC | EPC LEN | EPC NUM |
| 0xCF | 0x00 | 0x0004 | 1Byte | 1Byte | 1Byte | 1Byte | 2Byte | 2Bytes | 1Byte | N  Bytes | 2Byte |

* + TagStatus：The operation status returned by the tag. For specific definitions, see Appendix A. This field is included in the response data only when the value of the STATUS field is 0.；

Definition of each field：

Determine whether the command is executed successfully based on STATUS and TagStatus.

|  |  |  |
| --- | --- | --- |
| Fields | byte | describe |
| STATUS | 1 | Refer to Table A-6 STATUS definition |
| TagStatus | 1 | The operation status returned by the tag, see Appendix A for specific definitions； |
| Antenna | 1 | From which antenna port the tag data is received. The value range is: 1~4, representing antennas 1 to 4 respectively. |
| CRC | 2 | CRC data in the tag response data |
| PC | 2 | PC data in tag response data |
| EPC LEN | 1 | The length of the tag's EPC number (bytes)； |
| EPC NUM | N Byte | The EPC number of the label； |

### 2.3.6 RFM\_LOCKISO\_TAG (Lock tag data)

This command locks the specified data storage area of ​​the specified international standard protocol label.

Before calling this method, please set the inventory condition (for selecting tags) through the RFM\_SETISO\_SELECTMASK command.

* Format

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN |  | PAYLOAD | | CHECK |
| AccPwd | Area | Action |
| 0xCF | 0xFF | 0x0005 | 0x06 | 4Byte | 1Byte | 1Byte | 1Byte |

Definition of each field：

|  |  |  |
| --- | --- | --- |
| Fields | byte | describe |
| AccPwd | 4 | Access password, used for the tag to enter the safe state, the default value is 0x00000000 |
| Area | 1 | The area that needs to be locked, the value list is as follows：  0x00: deactivate password area; 0x01: access password area； 0x02：EPC； 0x03：TID； 0x04：User； |
| Action | 1 | Lock operation type, the value list is as follows：  0x00: open; 0x01: permanently open; 0x02: locked; 0x03: permanently locked; |

* Response format and status byte

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | STATUS |  | PAYLOAD | | | | | CHECK |
| TagStatus | Antenna | CRC | PC | EPC LEN | EPC NUM |
| 0xCF | 0x00 | 0x0005 | 1Byte | 1Byte | 1Byte | 1Byte | 2Bytes | 2Bytes | 1Byte | N  Bytes | 1Byte |

Definition of each field：

Determine whether the command is executed successfully based on STATUS and TagStatus.

|  |  |  |
| --- | --- | --- |
| Fields | byte | describe |
| STATUS | 1 | Refer to Table A-6 STATUS definition |
| TagStatus | 1 | The operation status returned by the tag, see Appendix A for specific definitions； |
| Antenna | 1 | From which antenna port the tag data is received. The value range is: 1~4, representing antennas 1 to 4 respectively. |
| CRC | 2 | CRC data in the tag response data |
| PC | 2 | PC data in tag response data |
| EPC LEN | 1 | The length of the tag's EPC number (bytes)； |
| EPC NUM | N Byte | The EPC number of the label； |

### 2.3.7 RFM\_KLENLISO\_TAG (Kill Tags)

This command is to deactivate the module tag.

Before calling this method, please set the inventory conditions (for selecting tags) through the RFM\_SETISO\_SELECTMASK command.

Deactivation, only non-zero deactivation passwords are supported.

* Format

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | PAYLOAD | CHECK |
| KLENlPwd |
| 0xCF | 0xFF | 0x0006 | 0x04 | 4Byte | 1Byte |

* + KLENlPwd：KLENlCommand password；
* Response format and status byte

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| HEAD | ADDR | CMD | LEN | STATUS |  | | PAYLOAD | | | | CHECK |
| TagStatus | Antenna | CRC | PC | EPC LEN | EPC NUM |
| 0xCF | 0x00 | 0x0006 | 1Byte | 1Byte | 1Byte | 1Byte | 2Byte | 2Byte | 1Byte | N  Bytes | 1Byte |

Definition of each field：

Determine whether the command is executed successfully based on STATUS and TagStatus.

|  |  |  |
| --- | --- | --- |
| Fields | byte | describe |
| STATUS | 1 | Refer to Table A-6 STATUS definition |
| TagStatus | 1 | The operation status returned by the tag, see Appendix A for specific definitions； |
| Antenna | 1 | From which antenna port the tag data is received. The value range is: 1~4, representing antennas 1 to 4 respectively. |
| CRC | 2 | CRC data in the tag response data |
| PC | 2 | PC data in tag response data |
| EPC LEN | 1 | The length of the tag's EPC number (bytes)； |
| EPC NUM | N Byte | The EPC number of the label； |

# Appendix A. Operational status returned by tags

The operation status code returned by the tag is 8 bits in total, see Table A-1.

Table A-1 Operation status returned by the tag

|  |  |  |  |
| --- | --- | --- | --- |
| Operation status code | Operational Status | describe | Error Priority |
| 0x81 | Other Errors | Unknown error returned by tag |  |
| 0x82 | Storage area overflow | The target storage area does not exist |  |
| 0x83 | Storage Area Lock | Write or erase the storage area that is locked as unwritable, and read the storage area that is locked as unreadable. |  |
| 0x84 | Insufficient power | The tag does not have enough energy to complete the operation |  |
| 0x85 | Non-specific error | Unknown error returned by tag |  |
|  |  |  |  |

# Appendix B. CRC16 checksum reference C code

as follows：

#define PRESET\_VALUE 0xFFFF

#define POLYNOMIAL 0x8408

unsigned int uiCrc16Cal(unsigned char const \* pucY, unsigned char ucX)

{

unsigned char ucI,ucJ;

unsigned short int uiCrcValue = PRESET\_VALUE;

for(ucI = 0; ucI < ucX; ucI++)

{

uiCrcValue = uiCrcValue ^ \*(pucY + ucI);

for(ucJ = 0; ucJ < 8; ucJ++)

{

if(uiCrcValue & 0x0001)

{

uiCrcValue = (uiCrcValue >> 1) ^ POLYNOMIAL;

}

else

{

uiCrcValue = (uiCrcValue >> 1);

}

}

}

return uiCrcValue;

}

# Appendix C. Definition of STATUS.

Table A-6 STATUS definition

|  |  |
| --- | --- |
| STATUS | wrong description |
| 0x00 | Execution successful (this only means that the module successfully received the tag response data. If there is a tag execution status in the tag response, it should be further determined whether the tag execution status is correct) |
| 0x01 | The parameter value is incorrect or out of range, or the module does not support the parameter value. |
| 0x02 | Command execution failed due to an internal module error |
| 0x03 | reserve |
| 0x12 | No inventory was taken to the tag or the entire inventory command was executed. |
| 0x14 | Tag response timeout |
| 0x15 | Demodulation tag response error |
| 0x16 | Protocol authentication failed |
| 0x17 | Wrong password |
| 0xFF | No more data |