SLR5104 蓝牙读写器数据手册

名称：SLR5104 蓝牙读写器数据手册

型号： SLR5104

版本： V1.01

编号： 2016093001

日期： 20160930

北京芯联创展电子技术股份有限公司

www.silion.com.cn

修订记录

日期	修订版本	修改章节	修改描述	作者
160930	V1.01		优化、完善	

V1.01 16.09.30

目录：

一.简要参数介绍：

标签/传输协议

通信协议：EPC Class 1 Gen 2 （ISO 18000-6C）

蓝牙标准：Bluetooth 4.0(BLE)（可选配兼容 2.0、4.0 的双模蓝牙模块）

射频接口

天线连接：内置 2dBi PCB 天线（线极化）

R F 输出：5dBm 到 30dBm 可调，+/-1.0dBm

频　　率：FCC（美国）902-928MHz

SRRC-MII（中国）920MHz-925MHz、840MHz-845MHz

欧洲：865MHz-867MHz

电源

直流供电：Micro-USB 5pin 充电

充电时间：约 5.5 小时(使用配套适配器)

电　　池：3.7V/3000mAh 可充电锂聚合物电池（非可更换）

硬件结构

R F 架构：RFID ASIC

状态提示：运行状态提示灯、电源指示灯、充电提示灯

智能终端：IOS、Android 4.3 以上

性能

识读距离：约 3 米(alien 9654 标签,27dbm)

写入距离：约 1 米(alien 9654 标签,27dbm)

蓝牙连接距离： 10 米

通信波特率：115200

RF 持续工作时间：约 6 小时(主动模式)

待机时间： 约 30 小时

标签识读率：≥50tags/s

环境特性

工作温度： -5℃ 到 +50℃

贮藏温度：-10℃ 到 +45℃

尺寸

130mm x 65mm x16mm

二.通信协议格式与 CRC16 校验算法：

1.主机到读写器的通信格式：

Header + Data Length + Command + Data + CRC-16

Header: 一字节 固定 0XFF

DataLength: 一字节，Data 数据块的字节数

Command：一字节，命令码

Data：数据块，高字节在前面。

CRC-16: 二字节循环冗余码，高字节在前，从 DataLength 到 Data 结束的所有数据参与计算所得。

备注：整个通信数据串的字节数不得大于 255 个字节。

2. 读写器到主机的通信格式：

Header + DataLength + Command + Status + Data + CRC-16

Header: 一字节 固定 0XFF

DataLength: 一字节，Data 数据块的字节数

Status: 二字节，状态位，为 0 时表示操作成功，非 0 值为操作失败具体请看后面返回状态码解释，如非 0 且非后面解释的错误状态码则仅表示操作失败。

Command：一字节，命令码，同上一条 主机发来的命令码

Data：数据块，高字节在前面。

CRC-16: 二字节循环冗余码，高字节在前，从 DataLength 到 Data 结束的所有数据参与计算所得。

备注：整个通信数据串的字节数不得大于 255 个字节。

3. CRC-16 的计算方法：

```
#define MSG_CRC_INIT                0xFFFF
#define MSG_CCITT_CRC_POLY          0x1021
void CRC_calcCrc8(uint16 *crcReg, uint16 poly, uint16 u8Data)
{
 uint16 i;
 uint16 xorFlag;
 uint16 bit;
 uint16 dcdBitMask = 0x80;
 for(i=0; i<8; i++)
 {
      xorFlag = *crcReg & 0x8000;
      *crcReg <<= 1;
      bit = ((u8Data & dcdBitMask) == dcdBitMask);
      *crcReg |= bit;
      if(xorFlag)
      {
          *crcReg = *crcReg ^ poly;
      }
      dcdBitMask >>= 1;
 }
}
```

```
uint16 CalcCRC(uint8 *msgbuf,uint8 msglen)
{
   uint16 calcCrc = MSG_CRC_INIT;
   uint8   i;
   for (i = 1; i < msglen; ++i)
        CRC_calcCrc8(&calcCrc, MSG_CCITT_CRC_POLY, msgbuf[i]);
   return calcCrc;
}
```

调用函数 uint16 CalcCRC(uint8 *msgbuf,uint8 msglen)所得的返回数据就是 CRC-16,其中参数 *msgbuf 为除了 CRC-16 之外的通信协议串数据，msglen 为除了 CRC-16 之外的所有通信协议串数据的总字节数。（因函数内是从 msgbuf[1]开始取数据的，所以*msgbuf 是包含帧头的除了 CRC-16 之外的通信协议串数据）

三.通信协议命令码简介：

1. BOOTLOADER 层命令：

（1）0X01:写 FLASH 命令；
（2）0X02:读 FLASH 命令；
（3）0X03:获取 BOOTLOADER/FIRMWARE 版本信息；（APP 应用层也可用）
（4）0X04:BOOT FIRMWARE 命令，作用目前同 0X03；（APP 应用层也可用）
（5）0X06:设置波特率命令；（APP 应用层也可用）
（6）0X08:校验烧录固件；
（7）0X09:运行到 BOOTLOADER 层；（APP 应用层也可用）
（8）0X0C:获取目前是运行在 BOOTLOADER 层还是 APP 应用层。（APP 应用层也可用）
（9）0X10:获取读写器序列号；（APP 应用层也可用）
（10）0XAA:该命令中的子命令格式化 OEM 命令与读写 OEM 命令，见附录 1；

2.APP 层标签操作命令：

（1）0X21:单标签盘存命令；
（2）0X22:多标签盘存命令；
（3）0X23:写标签 EPC 命令；
（4）0X24:写标签存储区命令；
（5）0X25:LOCK 标签命令;
（6）0X26:KILL 标签命令；
（7）0X28：读标签存储区命令；
（8）0X29: 获取盘存到标签信息命令；
（9）0X2A:清除标签缓存区命令；

3.APP 层设置命令：

（1）0X91:天线口设置命令；
（2）0X92:设置读发射功率；目前该命令设置的值读写器会忽略；
（3）0X93:设置当前工作标签协议；
（4）0X94:设置写发射功率；目前该命令设置的值读写器会忽略；
（5）0X95:跳频设置；
（6）0X96:GPIO 输出设置；

（7）0X97:设置当前工作频率区域；
（8）0X98:设置功率模式；目前该命令设置的值读写器会忽略；
（9）0X99:设置用户模式；目前该命令设置的值读写器会忽略；
（10）0X9A:设置阅读器配置；
（11）0X9B:设置协议配置；

4.获取 APP 层设置信息命令：

（1）0X61:获取天线口配置信息；
（2）0X62:获取读发射功率信息；
（3）0X63:获取当前工作标签协议；
（4）0X64:获取写发射功率信息；
（5）0X65:获取跳频表；
（6）0X66:获取输入 GPIO 的值；
（7）0X67:获取当前工作频率区域；
（8）0X68:获取功率模式；
（9）0X69:获取用户模式；
（10）0X6A:获取读写器配置；
（11）0X6B:获取协议配置；
（12）0X70:获取可用标签协议；
（13）0X71:获取可用的工作频率区域；
（14）0X72：获取当前读写器温度；

6.备注：

（1）在 BOOTLOADER 层只有 BOOTLOADER 层的命令可使用，到 APP 层后只有 APP 层的命令可使用，当读写器收到不可识别命令时或者是运行在 BOOTLOADER 层或 APP 层收到不属于该层的命令时将会报不可使用操作命令错误 0X101。

（2）上位机发送任何命令后，请上位机等待读写器回复的超时时间设置为 5S+指定命令执行时间，也即是有的命令中包括执行的时间的比如 0X22 盘存命令，则等待读写器回复的超时时间为 5S+该命令中指定盘存的时间。这 5S 时间是为了在读写器突发异常的情况下给予的自恢复时间。

四.通信协议命令码详解：

1.B OOTLOADER 层命令：

读写器一上电是运行在 BOOTLOADER 层的，在 BOOTLOADER 层只有 BOOTLOADER 层的命令可使用，当读写器上电运行在 BOOTLOADER 层时，读取 OEM 寄存器 0X0400 的值，如果该寄存器值高 16 位值为 0XA5A5(已烧录过 APP 标志)，则读写器运行到 APP 层程序，否则停留在 BOOTLOADER 层。

（1）0X01:写 FLASH 命令:

主机到读写器：

0XFF+DATALENGTH+0X01+FINFLAG+WRITEADDR+WRITELEN+WRITEDATA+CRC

读写器到主机：

0XFF+0X00+0X01+STATUS+CRC

FINFLAG：1 个字节；为 0 时表示后续还有烧录数据要写入 FLASH，为 0XFF 时表示此次写 FLASH 是最后一次写入。

WRITEADDR: 4 个字节，高字节在前；烧录初始地址为 0x08003000,每写成功一次后，下次的写地址将为本次的 WRITEADDR+ WRITELEN*4。

WRITELEN：1 字节；定义 WRITEDATA 数据串的长度，后面的 WRITEDATA 的长度为 WRITELEN*4 个字节。

WRITELEN 的值固定为 32，只有当最后一次写 FLASH 的数据长度不足 128 个字节时才为实际的要写入的字节数除于 4；

WRITEDATA：要写入 FLASH 数据串，字节数为 4 的倍数。

STATUS:2 字节状态码:

0X0000:操作成功；

0X0105:不可用参数值，参数错误；

0X0302:FLASH 写入过程中失败；

其他非 0 为操作失败，见后面错误码解释，未有解释仅表示操作失败。

备注：此命令作为升级 APP 应用程序段专用，切勿当其他用。

（2）0X02:读 FLASH 命令：

主机到读写器：

0XFF+DATALENGTH+0X02 +READADDR+READLEN +CRC

读写器到主机：

0XFF+DATALENGTH+0X02+STATUS+READDATA+CRC

READADDR:4 个字节，读地址，高字节在前，读最低地址为 0x08003000；

READLEN：1 字节；值为 0—32；读取的字节数为 READLEN*4；

READDATA: 读取到的数据串，长度为 READLEN*4 个字节；

STATUS：2 字节:

0X0000:读操作成功；

0X0105:不可用参数值，参数错误；

其他非 0 为操作失败，见后面错误码解释，未有解释仅表示操作失败。

备注：此命令作为烧录 APP 应用程序段辅助命令用，切勿当其他用；

（3）0X03:获取 BOOTLOADER/FIRMWARE 版本信息（APP 应用层也可用）：

主机到读写器：

FF	00	03	1D 0C
SOH	Length	OpCode	CRC

读写器到主机格式如下例：

FF	14	03	00 00	13 04 15 00	A3 00 00 01
SOH	Length	OpCode	STATUS	BootLoader Ver	Hardware Ver

20 13 05 22	13 05 23 00	00 00 00 10	CRC
Firmware data	Firmware Version	Supported Protocol	CRC

Bootloader ver：4字节，表示Bootloader版本是 13.04.15.00。

Hardware Ver：4字节，表示硬件版本是A3.00.00.01，最高字节目前固定为A3。

Firmware data：4字节，表示APP应用层固件第一次编译时间2013.05.22。

Firmware Version：4字节，表示目前APP应用层固件版本为2013.5.23。

Supported Protocol：目前固定为00 00 00 10。

STATUS：2字节：

0X0000：操作成功；

其他非0为操作失败，见后面错误码解释，未有解释仅表示操作失败。

（4）0X04:BOOT FIRMWARE 命令，作用目前同 0X03；（APP 应用层也可用）：

命令格式同 0X03:获取 BOOTLOADER/FIRMWARE 命令，只是命令码为 0X04。

（5）0X06:设置波特率命令（APP 应用层也可用）：

读写器上电默认波特率为 115200BPS。命令格式如下例，设置波特率为 115200：

FF	04	06	00	01	C2	00	A4	60
SOH	Length	OpCode	Baud Rate				CRC	

Baud Rate 的值与各个波特率的对应表如下：

Baud Rate (decimal)	Baud Rate (hex)
9600	0x00002580
19200	0x00004B00
38400	0x00009600
57600	0x0000E100
115200	0x0001C200
230400	0x00038400

460800[1]	0x00070800
921600[1]	0x000E1000

备注：该命令预留用，目前读写器波特率仅可用 115200，用户不需使用该命令。

（6）0X08:校验烧录固件：

主机到读写器：

0XFF+DATALENGTH+0X08 +CHECKADDR+CHECKDATALEN +CHECKCRC+CRC

读写器到主机：

0XFF+0X00+0X03+STATUS +CRC

CHECKADDR:4 字节，高字节在前；值为 0x08003000；

CHECKDATALEN：4 字节，高字节在前；值为 0X01 命令所写入 FLASH 的所有字节数除于 4；

CHECKCRC：4 字节，校验码；

计算方法：以 4 个字节为一个单位，把 0X01 命令所写入 FLASH 的所有字节数从一开始到结束分成 N 个 4 个字节的数；

N 个数的最高字节分别相加记为 DATA1;

N 个数的次高字节分别相加记为 DATA2;

N 个数的次低字节分别相加记为 DATA3;

N 个数的最低字节分别相加记为 DATA4;

DATA1，DATA2,DATA3,DATA4 也都是为 32 位的数；

DATA1 的最低 8 位作为 CHECKCRC 的最高字节，

DATA2 的最低 8 位作为 CHECKCRC 的次高字节，

DATA3 的最低 8 位作为 CHECKCRC 的次低字节，

DATA4 的最低 8 位作为 CHECKCRC 的最低字节，

STATUS：2 字节：

0X0000:校验正确。校验正确后读写器会将 0XA5A5 已烧录标志写入 OEM 寄存器 0X0400 的高 16 位，并且跳转到 APP 层程序；

0X0105:不可用参数值，参数错误；

0X0200:校验码错误，校验失败；

其他非 0 为操作失败，见后面错误码解释，未有解释仅表示操作失败。

备注：此命令作为烧录应用程序段后校验烧录是否正确所用，切勿当其他用；

（7）0X09:运行到 BOOTLOADER 层（APP 应用层也可用）：

读写器收到该命令后，会检测 OEM 寄存器 0X0400 的高 2 字节值是否为 0XA5A5，如果是则返回操作失败，如果不是则报操作成功并返回 BOOTLOADER 层。发送该命令收到操作成功回复后，要等待 500MS 再发送其他命令，因为从 APP 层返回到 BOOTLOADER 层需要一些时间处理。

主机到读写器：

0XFF+0X00+0X09 +CRC

读写器到主机：

0XFF+0X00+0X09+STATUS +CRC

STATUS:2 字节:

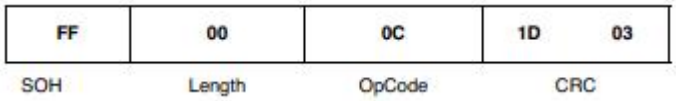
0X0000：操作成功。

其他非 0 为操作失败，见后面错误码解释，未有解释仅表示操作失败。

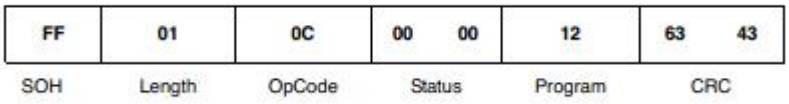
（8）0X0C:获取目前是运行在 BOOTLOADER 层还是 APP 应用层（APP 应用层也可用）：

示例如下：

主机到读写器：



读写器到主机：



Program：1 字节；0X11==BOOTLOADER 层；0X12==APP 应用层。

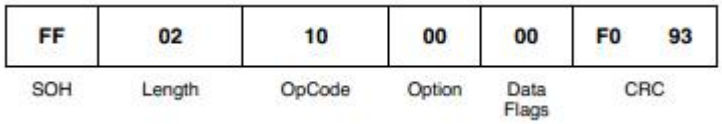
Status：2 字节：

0X0000：操作成功；

其他非 0 为操作失败，见后面错误码解释，未有解释仅表示操作失败。

（9）0X10:获取读写器序列号；（APP 应用层也可用）：

主机到**读写器**示例如下：



读写器到主机示例如下：

FF+DataLength+0X10+Status+DATA+CRC

Option:1 字节，预留参数，目前该值无意义。

Data flags:1 字节，预留参数，目前该值无意义。

Status: 2 字节：

0X0000：操作成功。操作成功时，读写器返回 12 个字节的序列号数据，最高 4 个字节表示年份，低 8 个字节表示序号，例如 02 00 01 03 09 09 09 09 09 09 09 09，表示该读写器的序列号为 201399999999。

其他非 0 为操作失败，见后面错误码解释，未有解释仅表示操作失败。

2.APP 层标签操作命令：

使用标签操作命令时启用不启用选择匹配过滤的时候会用到以下的一些参数协议规则:

Tag Singulation Fields

Field		Values	Description
Select Options	[1]Select Contents (Bits 0,1, 2)	0x00	Select functionality is disabled. First tag found will be the tag operated on. No other Tag Singulation Fields should be specified. Option field must **always** be specified. Note: When Select is disabled commands do not support an access password. Use Select Option=0x05 to send a password without Select.
		0x01	Select on the value of the EPC. Requires all fields except the *Select Address* field.
		0x02	Select on contents of TID memory bank (Gen2 bank 0x02). Requires all fields.
		0x03	Select on contents of User Memory memory bank (Gen2 bank 0x03). Requires all fields.
		0x04	Select on contents of the EPC memory bank (Gen2 bank 0x01). Requires all fields.
		0x05	Use this option when you need to specify an access password to operation on locked data but don't want to perform a Select. When this option is used do not pass any Select Criteria.
	[1]Select Invert (Bit 3)	0x08	Sets Invert Flag. This results in tags NOT matching the specified Tag Singulation Fields will be returned, as defined in Select Algorithm and Parameters.
	[1]Extended Select Data (Bit 5)	0x20	Changes *Select Data Length* to 2 bytes, allowing *Select Data* to be greater than 255 bits.

Field	Values	Description
The Select Options field is typically followed by command specific fields. After the command specific fields the following Tag Singulation fields should be specified as appropriate for the Select Contents specified.		
Select Address	4 bytes	Contains the offset, in bits, within the memory bank, specified by the *Option* value, at which the comparison is to start. NOTE: specifying *Option=0x04* and *Select Address=0x20* is the equivalent, for Gen2 v1 tags, of specifying *Option=0x01*, both specify a comparison against the tag EPC ID data. Note: Addresses are always zero-based. Specifying 0x00 indicates starting at the first address location.
Select Data Length	1 byte (*2 bytes if Extended Data enabled*)	Contains the length of the data (*Select Data*) to be compared, in bits, to the EPC when *Option*=0x01, or to the data beginning at *Select Address* for other options.
Select Data	M bytes	Contains the data to be compared against the specified tag data (memory bank and address, or EPC as specified by the *Option* value) The bit values used start at address 0. So if *Select Data Length* = 2, i.e. matching 2 bits, then the bits used for comparision will be the 2 most significant bits of the *Select Data* value. Examples: Select Data = 0x00 the bits to match will be 0, 0 Select Data = 0x8F the bits to match will be 1, 0 This is independent of the *Select Data Address* field.
Note: 1- The Select Options field contains multiple sub fields which must be combined into a single Select Options value. This means the final Select Options value is a result of Select Invert + Select Contents.		

Example:

The following EPC IDs (first 3 bits) are in the field:

0xAAAA (101)
0xCCCC (110)
0x4444 (010)
0x3000 (001)

Select Option = 0x04 (EPC Mem Bank)
Select Data Length = 0x01 (1 bit)
Select Data = 0x80
Select Data Address = 0x00000022 (third bit in the EPC ID)

In this case the third bit of the EPC ID is matched against the first bit of the *Select Data* value, 1. This would result in the following IDs being returned:

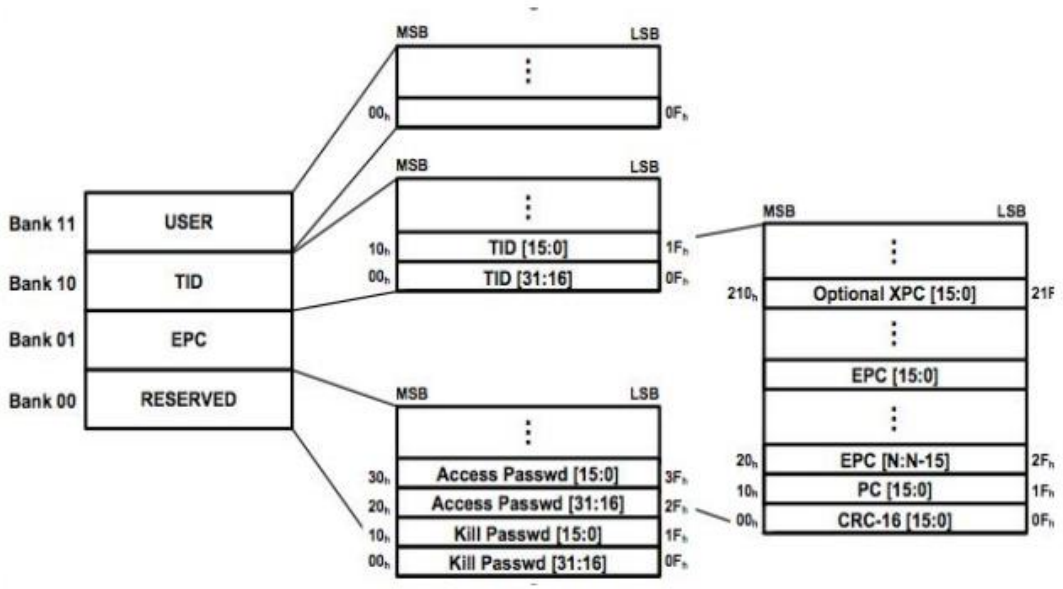
0xAAAA
0x3000

备注：启用选择匹配过滤功能时，目前 Select Data Length 匹配过滤数据的长度最多只能到255bits。

Gen2 Memory Map

When performing a Tag Singulation/Select most of the criteria specifies values of data in certain locations in a Gen2 tag's memory map. The following is a logical view of the Gen2 memory map from the Generation2 Protocol v1.2 that can be used for reference when trying to determine the memory address you are trying to match on:

Gen2 Tag Memory Map



Note

The address values specified in the memory map are hexidecimal, zero-based bit offset within each memory bank (i.e. the PC section of the EPC memory bank starts at bit 0x10, decimal 16, and runs to bit 0x1F, decimal 31). It is important to note the units used in various command fields for address locations. In some cases the address is specified in words (16 bit chunks), sometimes bytes (8 bit chunks) and sometimes bits.

（1）0X21:单标签盘存命令：

该命令为在指定的时间内盘存一个标签 EPC 号，也即是在指定时间内盘存到一个标签后就返回，盘存时间由两个字节组成，单位为 毫秒。

如果 SELECT OPTION=0 则返回第一个盘存到的标签，如果为其他值则返回第一个盘存到的符合选择匹配过滤条件的标签。

该命令能够设置只返回标签的 EPC 号（ Get Tag EPC.）或者是返回 EPC 号加 TAG READ META DATA（ Get Tag EPC and Meta Data）。

备注：当使用该命令时如果选择的盘存算法为 Dynamic Q 则读写器内部将使用 Q=0 去盘存标签，如果选择的是 Static Q 算法则按设置的 Q 值去盘存标签（当 Q>3 时将取用 Q=3 去盘存）。

① 只返回 EPC 号（ Get Tag EPC.）：

下面例子是在 1000MS 内使用选择匹配过滤功能去盘存所要的标签。参照 Tag Singulation/Select Functionality，设置Select Option=0x03，也即是选择匹配的区为USER区。

Memory Bank = User Memory.

Starting Address = bit 32

Select Data = 0x1234

主机到读写器示例：

FF	0A	21	03 E8	03	00 00 00 20	10	12	34	E5 AC
SOH	Length	Opcode	Timeout(ms)	Option	Select Address	Select data length	Select data		CRC

读写器到主机示例：

FF	M+3	21	00 00	03	M bytes	TagCRC	CRC
SOH	Length	Opcode	Status	Option	EPC	TagCRC	CRC

如果 OPTION=0X00 或 0X01 的时候， Tag Singulation Fields 中指明不包括的参数要去掉，该命令不支持 OPTION=0X05。

② 返回 EPC 号加 TAG READ META DATA（Get Tag EPC and Meta Data）

返回 EPC 号的同时获取相关的一些标签相关参数，如果 Option 的 BIT4 位设置为 1 的话，这时主机到读写器的命令中也要加入 2 字节的 Metadata Flags，指示要返回哪些相关标签参数，具体如下。

Read Tag Single Get EPC and Metadata Request Fields

Field	Value	Description
Option	Bit 4=0(0x0X)	该位为 0 时即是只返回 EPC 号（ Get Tag EPC.），这时主机到读写器命令是没有 2 字节的 Metadata Flags

		的。见①只返回 EPC 号（Get Tag EPC.）
	Bit 4=1(0x1X)	该位为 1 时即是返回 EPC 号加 TAG READ META DATA，这时主机到读写器命令中加入 2 字节的 Metadata Flags，Metadata Flags 每个位定义要返回的内容如下：
Metadata Flags：可以多个位置 1 以返回相关数据或者所有相关位都置 1 返回所有相关标签参数。	0X0000	不返回任何相关标签参数。只是返回标签 EPC 号(包括标签 CRC)。
	0X0001	Bit0 置位即标签在盘存时间内被盘存到的次数将会返回
	0X0002	BIT1 置位即标签的 RSSI 信号值将会被返回
	0X0004	BIT2 置位即标签 被盘存到时所用的天线 ID 号将会被返回。（天线逻辑号）
	0X0008	BIT3 置位即标签被盘存到时所用的频率值将会被返回
	0X0010	BIT4 置位即标签被盘存到时读写器的时间值将会被返回，
	0X0020	BIT5 置位即 RFU 预留值将会被返回
	0X0040	BIT6 置位则目前读写器使用的标签协议值将会被返回
	0X0080	BIT7 置位即数据长度将会被返回（在单标签读 0X21 命令该值是返回 0X0000）

使用 Metadata Flags 获取相关标签参数时读写器到主机的回复可包括下面信息：

Read Tag Single Get EPC and Metadata Response Fields

Field	Length	Value
SOH	1byte	0xFF
Length	1byte	取决于返回数据
OpCode	1byte	0X21
Status	2byte	命令操作状态码，0X0000 为操作成功。
Options	1byte	同主机发给读写器命令中的
Metadata Flags	2byte	指示哪些 Metadata 需要返回的
Read Count$_1$	1byte	标签被盘存到的次数
RSSI$_1$	1byte	标签信号强度,单位 DBM，

		该值是有符号字符字节
Antenna ID$_1$	1byte	盘存到标签的天线 ID，高 4 位为发射天线，低 4 位为接收天线。（天线逻辑号）
Frequency$_1$	3byte	盘存到标签时的频率，单位 KHZ
Timestamp$_1$	4byte	读写器的系统时间，单位毫秒。目前时间值无效
RFU$_1$	2byte	预留数据
Protocol ID	1byte	标签协议（0X05 表示 GENT2）
Tag Data Length	2byte	标签数据长度（在单标签读 0X21 命令该值是 0X0000）
EPC ID	N byte	标签 EPC 号
Tag CRC	2byte	标签 CRC
CRC	2byte	命令串 CRC

例子 1：

获取 EPC 号的同时获取天线 ID 号与读写器系统时间信息

Metadata Flags = 0x0004 OR 0x0010 = 0x0014

不启用选择匹配过滤，返回第一个盘存到的标签：

主机到读写器：

FF	05	21	01	E8	10	00	14	2F 6D
SOH	Length	Opcode	Timeout		Option	Metadata Flags		CRC

读写器到主机：

FF	16	21	00 00	10	00	14
SOH	Length	Opcode	Status	Option	Metadat Flags	

11	00 BB 5F 04	01 23 45 67 89 AB CD EF 01 23 45 67	E6 C8	37 C4
Ant ID	Timestamp	Tag EPC	Tag CRC	CRC

例子 2：

获取 EPC 号的同时获取天线 ID 号与读写器系统时间信息

Metadata Flags = 0x0004 OR 0x0010 = 0x0014

启用选择匹配过滤，EPC=0x111122223333444455556666 的标签才返回，主机到读写器：

FF	12	21	01	E8	11	00	14
SOH	Length	Opcode	Timeout		Option	Metadata Flags	

60	11 11 22 22 33 33 44 44 55 55 66 66	9F CE
Select data length	Select Data(EPC)	CRC

读写器到主机：

FF	16	21	00 00	11	00 14
SOH	Length	Opcode	Status	Option	Metadata Flags

11	0F C8 C0 B7	11 11 22 22 33 33 44 44 55 55 66 66	18 35	？？？？
Ant ID	Timestamp	Tag EPC	Tag CRC	CRC

该命令可能返回的状态码如下：
0X0000：操作成功；
0X0100：数据长度出错
0X0105：不可用参数值，参数错误
0X0400：盘存不到标签，没有标签
0X0504：温度超限
0X0505：驻波比过大，反射过大。
其他非 0 为操作失败，见后面错误码解释，未有解释仅表示操作失败。

（2）0X22:多标签盘存命令，READ TAG MULTIPLE:

该命令区别于 0X21 的地方是该命令为在设置的时间里盘存所有在射频场内的标签，直到设置的盘存时间到后，才把盘存到的标签的数量返回。发送该命令后，如果有盘存到标签，则在后面再发送 0X29(GET TAG BUFFER)命令取盘存到的标签信息。目前标签缓存区为最多保存 100 个标签信息，所以发送该命令后，在设定盘存时间内最多一次可盘存保存 100 个标签，当盘存到 100 个标签后，读写器则停止盘存，返回盘存结果。

备注：当使用该命令时如果选择的盘存算法为 Dynamic Q 则读写器内部将自动调节 Q 值去盘存标签，如果选择的是 Static Q 算法则按设置的 Q 值去盘存。（当 Q>6 时将取用 Q=6 去盘存）。

0X22 命令启用不启用选择匹配过滤的格式如下：

Read Tag Multiple with Select Fields

Field	Value	Description
Select Options	[1 byte]	Tag Singulation Fields中的Select Options
Search Flags	[2 bytes]	预留用，请设置为0；
Timeout	[2 bytes]	盘存时间，单位毫秒
Access Password	[4 bytes]	访问密码，预留用，设置为0。 注意：如果Select Options=0，命令中不包含该4字节访问密码。
Tag Singulation Fields		由Select Options的值决定，如果启用选择匹配过滤，则相关的数据接在Access Password数据后面

例子1：

启用选择匹配过滤进行盘存，匹配区域为EPC区。

主机到读写器：

FF	0F	22	04	00 00	03 E8
SOH	Length	Opcode	Option	Search Flags	Timeout

00 00 00 00	00 00 00 78	08	66	DE C0
AccessPassword	Select Address(bits)	Select data length(bits)	Select data	CRC

备注：命令中数据排序是先OPTION，再SEARCH FLAGS，再TIMEOUT，再ACCESSPASSWORD，再Tag Singulation Fields域的相关数据的，跟典型的选择匹配

过滤格式有点不同。另外仅当OPTION=0时ACCESSPASSWORD必须去掉，不包含在命令串中，此时Select Address(bits)，Select data length(bits)，Select data，也将不存在。而当OPTION=0X05时，只有ACCESSPASSWORD,没有Select Address(bits)，Select data length(bits)，Select data。
OPTION=1时Select Address(bits)也不存在，具体看Tag Singulation Fields介绍。

读写器到主机：
读写器到主机的回复中包含盘存到的标签数，如果要取标签具体信息，发送0X29(Get Tag Buffer)命令。

FF	04	22	00 00	04	00 00	02	B7 6E
SOH	Length	Opcode	Status	Option	Search Flags	Tag Found	CRC

如果盘存到的标签数多于255个，则Tag Found为4个字节长度，且Search Flags的BIT 4位会置1，假如盘存到257个标签则返回的命令格式如下：

FF	07	22	00 00	04	00 10	00 00 01 01	??
SOH	Length	Opcode	Status	Option	Search Flags	Tag Found	CRC

例子2：
不启用选择匹配过滤。
主机到读写器：

FF	05	22	00	00 00	00 C8	? ?
SOH	Length Opcode		Option	Search Flags	Timeout	CRC

读写器到主机;

FF	04	22	00 00	00	00 00	00	??
SOH	Length Opcode		Status	Option	Search Flags	Tag Found	CRC

备注：当option=0x05时，只有access password,没有select address/data length/data。
该命令可能返回的状态码如下：
0X0000：操作成功；
0X0100：数据长度出错
0X0105：不可用参数值，参数错误
0X0400: 未盘存到标签。
0X040A：一般标签错误
0X0504：温度超限
0X0505：驻波比过大，反射过大。
其他非 0 为操作失败，见后面错误码解释，未有解释仅表示操作失败。

（3）0X23:写标签 EPC 命令（Write Tag EPC）：

更新标签 EPC 命令，该命令与 0X24 不同的地方是该命令会根据用户写入 EPC 的数据长度自动更改 PC 中的表示 EPC 长度的位的值，该命令是把 EPC ID 写入 EPC 区 0X20（BITS）开始的地址中。

备注：当使用该命令时如果选择的盘存算法为 Dynamic Q 则读写器内部将使用 Q=0 去盘存要更改 EPC 的标签，如果选择的是 Static Q 算法则按设置的 Q 值去盘存。（当 Q>3 时将取用 Q=3 去盘存）。

该命令格式如下：

Write Tag EPC Command Fields

Field	Value	Description
Length	[1 byte]	命令串数据长度
Opcode	0x23	命令码
Timeout	[2 bytes]	写处理时间，单位毫秒
Select Option	[1 byte]	Tag Singulation Fields 中的 Select Options
Access Password	[4 bytes]	访问密码，如果标签EPC域未锁定，则为0X00000000；如果EPC域锁定，则只有访问密码正确时才能够写入。注意：如果 Select Options=0，命令中不包含该 4 字节访问密码。
Tag Singulation Fields		由 Select Options 的值决定，如果启用选择匹配过滤，则相关的数据接在 Access Password 数据后面
Tag EPC ID	[M bytes]	最多 496 位标签 EPC ID（取决于标签）

例子1：

不启用选择匹配过滤。

主机到读写器：

FF	0C	23	03 E8	00	00
SOH	Length	Opcode	Timeout	Option	RFU

11 11 22 22 33 33 44 44	63 2C
Tag EPC ID	CRC

备注：当Option=0时，Option后要带一个字节的RFU=0，预留用。

读写器到主机，写成功：

FF	00	23	00 00	90 C1
SOH	Length	Opcode	Status	CRC

例子2：

启用选择匹配过滤功能，，匹配过滤区域为EPC区，匹配地址为0X00000020（bits），匹配数据长度为0X08位，匹配数据为0X11，反向匹配，也即是标签的EPC区0X00000020（bits）地址开始的8个位数据不是0X11的时候才回应盘存，执行写EPC操作。

主机到读写器：

FF	19	23	03 E8	0C	00 00 00 00	00 00 00 20
SOH	Length	Opcode	Timeout	Option	Access Password	Select Address(bits)

08	11	11 11 22 22 33 33 44 44 55 55 66 66	57 3E
Select data length(bits)	Select data	Tag EPC ID	CRC

读写器到主机，操作失败，没有符合条件的标签：

FF	00	23	04 00	94 C1
SOH	Length	Opcode	Status	CRC

例子3：

启用选择匹配过滤功能，，匹配过滤区域为EPC区，匹配地址为0X00000020（bits），匹配数据长度为0X08位，匹配数据为0X11，即是标签的EPC区0X00000020（bits）地址开始的8个位数据为0X11的时候才回应盘存，执行写EPC操作。

主机到读写器：

FF	19	23	03 E8	04	00 00 00 00	00 00 00 20
SOH	Length	Opcode	Timeout	Option	Access Password	Select Address(bits)

08	11	11 11 22 22 33 33 44 44 55 55 66 66	98 48
Select data length(bits)	Select data	Tag EPC ID	CRC

读写器到主机，操作成功：

FF	00	23	00 00	90 C1
SOH	Length	Opcode	Status	CRC

备注：当 option=0x05 时，只有 access password,没有 select address/data length/data。

该命令可能返回的状态码如下：

0X0000：操作成功；

0X0100：数据长度出错

0X0105：不可用参数值，参数错误

0X0400：盘存不到标签，没有标签

0X040A：一般标签错误

0X0424：存储区锁定

0X0504：温度超限

0X0505：驻波比过大，反射过大。

其他非 0 为操作失败，见后面错误码解释，未有解释仅表示操作失败。

（4）0X24:写标签存储区命令（Write Tag Data）；

该命令为把数据写入指定的标签存储区中指定的地址。第一个被盘存到的标签将会被写入。该命令除了启用不启用选择匹配过滤功能（ Tag Singulation Fields）中的相关数据外，还包括下面数据。

Write Tag Data Fields

Field	Value	Description
Write Address	4 bytes	写起始地址，为指定写入的存储区的写入起始地址，该地址为字地址（16BITS）。地址是从 0 开始的，地址为 0 表示从首地址开始。
Write MemBank	1 byte	写入存储区： 0x00 = Reserved 0x01 = EPC 0x02= TID 0x03 = User Memory
Write Data	N bytes	写入数据。写入数据字节长度必须为 2 的倍数。一次最多只能写 32 个字，即 64 个字节。

Access PassWord	4 byes	访问密码。如果写入的存储区未锁定，则密码 AccessPwd=0x00000000 即可，如果写入的存储区锁定，则密码必须为正确的密码才行。 备注：当 Option=0x00 时，命令串中不包括访问密码。

例子 1：

不启用选择匹配过滤功能。向 USER 区起始地址 1 写入 0XAAAABBBBCCCCDDDD。

Write Address=0X00000001（（16BITS）字地址不是位地址）

Write MemBank=0X03

Write Data=0XAAAABBBBCCCCDDDD

主机到读写器：

FF	10	24	03 E8	00	00 00 00 01	03
SOH	Length	Opcode	Timeout	Option	**Write Address**	**Write MemBank**

AA AA BB BB CC CC DD DD	C7 B3
Write Data	**CRC**

读写器到主机，写失败，存储区锁定：

FF	00	24	04 24	E4 02
SOH	Length	Opcode	Status	CRC

例子2：

不启用选择匹配过滤功能，向Reserved（密码）区0X00000000地址写入 0XAAAABBBBCCCCDDDD。

Write Address=0X00000000

Write MemBank=0X00

Write Data=0XAAAABBBBCCCCDDDD

主机到读写器：

FF	10	24	03 E8	00	00 00 00 00	00
SOH	Length	Opcode	Timeout	Option	**Write Address**	**Write MemBank**

AA AA BB BB CC CC DD DD	58 E2
Write Data	**CRC**

读写器到主机，写成功：

FF	00	24	00 00	E0 26
SOH	Length	Opcode	Status	CRC

例子3：

启用选择匹配过滤功能。

Write MemBank=0X00(Reserved（密码）区)

Write Address=0X00000000

Write Data=0XAAAABBBBCCCCDDDD

Access Password=0XCCCCDDDD

Select **MemBank=EPC区**

Select Address(bits)=0X00000020

Select data length(bits)=0X0C

Select data=0X1110

主机到读写器：

FF	1B	24	03 E8	04	00 00 00 00	00

SOH	Length	Opcode	Timeout	Option	**Write Address**	**Write MemBank**
CC CC DD DD		00 00 00 20		0C		11 10
Access Password		Select Address(bits)		Select data length(bits)		Select data
AA AA BB BB CC CC DD DD		26		AA		
Write Data		**CRC**				

读写器到主机，写成功：

FF	00	24	00 00	E0 26
SOH	Length	Opcode	Status	CRC

例子4：

启用选择匹配过滤功能，标签的EPC ID= 0x0123456789ABCDEF01234567。

Write MemBank=0X03(USER区)

Write Address=0X00000002

Write Data=0X1111222200000000

Access Password=0X00000000

Select **MemBank=0X01（EPC区）**

Select data length(bits)=0X60

Select data=0x0123456789ABCDEF01234567

主机到读写器：

FF	21	24	03 E8	01	00 00 00 02	03
SOH	Length	Opcode	Timeout	Option	Write Address	Write Membank
00 00 00 00		60		01 23 45 67 89 AB CD EF 01 23 45 67		
Access Password		Select data length(bits)		Select data		
11 11 22 22 00 00 00 00		81 E7				
Write Data		**CRC**				

备注1：当option=0x05时，只有access password,没有select address/data length/data。

备注2：当Option=0x00或0X01时， Tag Singulation Fields中指定的不需要的数据部分不应该出现在命令串中，Option=0x00时访问密码也不应该出现在命令串中。

备注3：当使用该命令时如果选择的盘存算法为Dynamic Q则读写器内部将使用Q=0去盘存要写入的标签，如果选择的是Static Q算法则按设置的Q值去盘存（当Q>3时将取用Q=3去盘存）。

该命令可能返回的状态码如下：

0X0000：操作成功；

0X0100：数据长度出错

0X0105：不可用参数值，参数错误

0X0400：盘存不到标签，没有标签

0X040A：一般标签错误

0X0420：其他错误

0X0424：存储区锁定

0X0504：温度超限

0X0505：驻波比过大，反射过大。

其他非 0 为操作失败，见后面错误码解释，未有解释仅表示操作失败。

（5）0X25:LOCK 标签命令：

该命令为锁定或者解锁指定的存储区，Option=0x05 不能用在该命令。

该命令除了启用不启用选择匹配过滤功能（ Tag Singulation Fields）中的相关数据外，还包括下面数据。

Lock Tag Fields

Field	Value	Description
AccessPwd	4 byes	**访问密码**
Mask Bits1	2 bytes	见下表，对应的位为 1 时表示执行对应的 ACTIONBIT 位的操作。
Action Bits1	2 bytes	ACTIONBIT 中的位只有当对应的 MASKBIT 位为 1 时才起作用。0 为解锁，1 为锁定。

1- Mask 和 Action 位为对应 EPC 协议中规定的，具体请看 EPC 协议。

	First Byte								Second Byte							
Bit	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
	Unused						Kill Pwd		Access Pwd		EPC Mem		TID Mem		User Mem	
Mask	X	X	X	X	X	X	Set?	Set?	Set?	Set?	Set?	Set?	Set?	Set?	Set?	Set?
Action	X	X	X	X	X	X	R/W	Perm	R/W	Perm	W	Perm	W	Perm	W	Perm

例子 1：EPC ID=0x111122223333444455556666, access password=0x11223344,
启用选择匹配过滤，锁住 EPC 区：
主机到读写器：

FF	18	25	03 E8	01	11 22 33 44	00 20	00 20
SOH	Length	Opcode	Timeout	Option	Access Password	Mask Bits	Action Bits

60	11 11 22 22 33 33 44 44 55 55 66 66	9E 7A
Select data length(bits)	Select data(EPC ID)	CRC

例子 2：EPC ID=0x111122223333444455556666, access password=0x11223344,
启用选择匹配过滤，锁住 EPC 区：
主机到读写器：

FF	11	25	03 E8	04	11 22 33 44	00 20	00 20
SOH	Length	Opcode	Timeout	Option	Access Password	Mask Bits	Action Bits

00 00 00 20	08	11	94 32
Select Address(bits)	Select data length(bits)	Select data	CRC

读写器到主机：

FF	00	25	00 00	F0 07
SOH	Length	Opcode	Status	CRC

例子 3：

EPC ID=0x111122223333444455556666, access password=0x11223344,

不启用选择匹配过滤，锁住 USER 区：

主机到读写器：

FF	0B	25	03 E8	00	11 22 33 44	00 02	00 02	0F A9
SOH	Length	Opcode	Timeout	Option	Access Password	Mask Bits	Action Bits	CRC

读写器到主机：

FF	00	25	00 00	F0 07
SOH	Length	Opcode	Status	CRC

备注：当使用该命令时如果选择的盘存算法为 Dynamic Q 则读写器内部将使用 Q=0 去盘存要 LOCK 的标签，如果选择的是 Static Q 算法则按设置的 Q 值去盘存（当 Q>3 时将取用 Q=3 去盘存）。

该命令可能返回的状态码如下：

0X0000：操作成功；

0X0100：数据长度出错

0X0105：不可用参数值，参数错误

0X0400：盘存不到标签，没有标签

0X040A：一般标签错误

0X0420：其他错误

0X0424：存储区锁定，已永久锁定。

0X0504：温度超限

0X0505：驻波比过大，反射过大。

其他非 0 为操作失败，见后面错误码解释，未有解释仅表示操作失败。

（6）0X26:KILL 标签命令：

该命令为杀死标签命令，Option=0x05 不能用在该命令。

例子 1：

不启用选择匹配过滤功能。

主机到读写器：

FF	08	26	03 E8	00	11 22 33 44	00	91 16
SOH	Length	Opcode	Timeout	Option	Kill Password	RFU	CRC

读写器到主机，KILL 失败：

FF	00	26	04 20	C4 44
SOH	Length	Opcode	Status	CRC

例子 2：

使用选择匹配过滤，过滤区域为 USER 区。

主机到读写器：

FF	10	26	03 E8	03	11 22 33 44	00
SOH	Length	Opcode	Timeout	Option	Kill Password	RFU

00 00 00 00	18	11 11 22	BF 40
Select Address(bits)	Select data length(bits)	Select data	CRC

读写器到主机，KILL 成功：

FF	00	26	00 00	C0 64
SOH	Length	Opcode	Status	CRC

例子 3：

使用选择匹配过滤功能，过滤区域为 EPC 区。

FF	13	26	03 E8	01	11 11 22 22	00
SOH	Length	Opcode	Timeout	Option	KILL Password	RFU

50	11 22 33 44 55 66 77 88 99 AA	DD DB
Select data length(bits)	Select data (EPC ID)	CRC

备注 1：KILL Password 不能为 0。RFU 为一个字节，预留用，为 0.

备注 2：当使用该命令时如果选择的盘存算法为 Dynamic Q 则读写器内部将使用 Q=0 去盘存要 KILL 的标签，如果选择的是 Static Q 算法则按设置的 Q 值去盘存（当 Q>3 时将取用 Q=3 去盘存）。

该命令可能返回的状态码如下：

0X0000：操作成功；

0X0100：数据长度出错

0X0105：不可用参数值，参数错误

0X0400：盘存不到标签，没有标签

0X040A：一般标签错误

0X040C：不可用杀死密码

0X0420：其他错误

0X0504：温度超限

0X0505：驻波比过大，反射过大。

其他非 0 为操作失败，见后面错误码解释，未有解释仅表示操作失败。

（7）0X28：读标签存储区命令：

读标签存储区内容，该命令除了启用不启用选择匹配过滤功能（ Tag Singulation Fields）中的相关数据外，还包括下面数据。

Read Tag Data Fields

Field	Value	Description
Read MemBank	1 byte	指定读存储区： 0x00 = Reserved 0x01 = EPC 0x02= TID 0x03 = User Memory
Read Address	4 bytes	读起始字地址，存储区的字地址（16BITS），地址是从 0 开始的，地址为 0 表示从首地址开始。
WordCount	1 byte	读取的字数（16BITS），一次最多只能读 96 个字。
Access Password	4 byes	访问密码,如果存储区未锁读，则 AccessPassword=0X00000000，锁读则需要正确密码。

		备注：Option=0 时访问密码不包括在命令串中。

读标签存储区命令有两种方式，一种是只单单获取存储区数据 （Get Tag Data.），另一种是获取存储区数据的同时把标签相关信息参数也获取（ Get Tag Data and Meta Data）。

1.只单单获取存储区数据 Get Tag Data：

例子 1：

不启用选择匹配过滤功能，读 TID 区字地址 1 开始的 2 个字：

主机到读写器：

FF	09	28	03 E8	00	02	00 00 00 01	02	C1 F3
SOH	Length	Opcode	Timeout	Option	Read Membank	Read address	WordCount	CRC

读写器到主机：

FF	05	28	00 00	00	60 04 01 35	13 04
SOH	Length	Opcode	Status	Option	Data Read	CRC

例子 2：

启用选择匹配过滤功能，读 TID 区地址 1 开始的 3 个字，密码=0，匹配区域为 TID 区，匹配起始地址为 0X10(BITS),匹配长度为 4 位，匹配数据为 0X60：

主机到读写器：

FF	13	28	03 E8	02	02	00 00 00 01	03
SOH	Length	Opcode	Timeout(ms)	Option	Read membank	Read address	Word count

00 00 00 00	00 00 00 10	04	60	7C 91
Access password	Select Address(bits)	Select data length(bits)	Select data	CRC

读写器**到主机：**

FF	07	28	00 00	02	60 04 01 35 F8 69	6C 29
SOH	Length	Opcode	Status	Option	Data Read	CRC

例子 3：

EPC ID=0x0123456789ABCDEF01234567，读 USER 区，启用选择匹配过滤：

主机到读写器：

FF	**1A**	**28**	**03 E8**	**01**	**03**	**00 00 00 02**	**04**
SOH	Length	Opcode	Timeout(ms)	Option	Read membank	Read address	Word count

00 00 00 00	60	01 23 45 67 89 AB CD EF 01 23 45 67	7A C1
Access password	Select data length(bits)	Select data	CRC

读写器**到主机：**

FF	09	28	00 00	01	AA BB CC DD 00 00 00 00	E7 54
SOH	Length	Opcode	Status	Option	Data Read	CRC

2. 获取存储区数据的同时把标签相关信息参数也获取（ Get Tag Data and Meta Data）。

Option 的 BIT4 位设置为 1，主机到读写器的命令中也要加入 2 字节的 Metadata Flags，指示要返回哪些相关标签参数，具体如下。

Read Tag Data Get Data and Metadata Request Fields

Field	Value	Description
Option	Bit 4=0(0x0X)	该位为 0 时即是**只单单获取**

		存储区数据 Get Tag Data，这时主机到读写器命令是没有 2 字节的 Metadata Flags 的。见 1 中**只单单获取存储区数据 Get Tag Data**
	Bit 4=1(0x1X)	该位为 1 时即是**获取存储区数据的同时把标签相关信息参数也获取**，这时主机到读写器命令中加入 2 字节的 Metadata Flags，Metadata Flags 每个位定义要返回的内容如下：
Metadata Flags：可以多个位置 1 以返回相关数据或者所有相关位都置 1 返回所有相关标签参数。	0X0000	不返回任何相关标签参数。只是返回读取的存储区数据。
	0X0001	Bit0 置位即标签在盘存时间内被盘存到的次数将会返回
	0X0002	BIT1 置位即标签的 RSSI 信号值将会被返回。
	0X0004	BIT2 置位即标签 被盘存到时所用的天线 ID 号将会被返回。（天线逻辑号）
	0X0008	BIT3 置位即标签被盘存到时所用的频率值将会被返回
	0X0010	BIT4 置位即标签被盘存到时读写器的时间值将会被返回
	0X0020	BIT5 置位即 RFU 预留值将会被返回
	0X0040	BIT6 置位则目前读写器使用的标签协议值将会被返回
	0X0080	BIT7 置位即数据长度将会被返回（该命令该值是返回 0X0000）

使用 Metadata Flags 获取相关标签参数时读写器到主机的回复可包括下面信息：

Read Tag Data Get Data and Metadata Response Fields

Field	Length	Value
SOH	1byte	0xFF
Length	1byte	取决于返回数据
OpCode	1byte	0X28
Status	2byte	命令操作状态码，0X0000 为操作成功。
Options	1byte	同主机发给读写器命令中的
Metadata Flags	2byte	指示哪些 Metadata 需要返

		回的
Read Count$_1$	1byte	标签被盘存到的次数
RSSI$_1$	1byte	标签信号强度,单位 DBM，目前该值无效。
Antenna ID$_1$	1byte	盘存到标签的天线 ID，高 4 位为发射天线，低 4 位为接收天线。（天线逻辑号）
Frequency$_1$	3byte	盘存到标签时的频率，单位 KHZ
Timestamp$_1$	4byte	读写器的系统时间，单位毫秒，目前时间值无效。
RFU$_1$	2byte	预留数据
Protocol ID	1byte	标签协议（0X05 表示 GENT2）
Tag Data Length	2byte	该值固定是 0X0000
Tag Data	N byte	读取的数据
CRC	2byte	命令串 CRC

例子 1：

主机到读写器：

FF	15	28	03 E8	14	00 14	00	00 00 00 02
SOH	Length	Opcode	Timeout	Option	Metadata Flags	Read Membank	Read address

02	00 00 00 00	00 00 00 78	08
Word count	Access Password	Select Address(bits)	Select data length(bits)

34	9C 0E
Select data	CRC

读写器**到主机**：

FF	0C	28	00 00	14	00 14
SOH	Length	Opcode	Status	Option	Metadata Flags

11	00 00 00 15	12 34 56 78	? ? ? ?
Antenna ID	Timestamp	Tag Data	CRC

备注 1：当使用该命令时如果选择的盘存算法为 Dynamic Q 则读写器内部将使用 Q=0 去盘存要读取存储区的标签，如果选择的是 Static Q 算法则按设置的 Q 值去盘存（当 Q>3 时将取用 Q=3 去盘存）。

备注 2：当 option=0x05 时，只有 access password,没有 select address/data length/data.

该命令可能返回的状态码如下：

0X0000：操作成功；

0X0100：数据长度出错

0X0105：不可用参数值，参数错误

0X0400：盘存不到标签，没有标签

0X040A：一般标签错误

0X0420：其他错误

0X0424：存储区锁定

0X0504：温度超限

0X0505：驻波比过大，反射过大。
其他非 0 为操作失败，见后面错误码解释，未有解释仅表示操作失败。

（8）0X29: 获取盘存到的标签信息命令:

该命令为 0X22 命令后，获取 0X22 命令盘存到的标签信息。可获取的信息包括标签的 EPC 内容与相关标签参数。

该命令主机到读写器的命令串中包括下面信息：

Get EPC and Metadata Request Fields

Field	Value	Description
Metadata Flags：可以多个位置 1 以返回相关数据或者所有相关位都置 1 返回所有相关标签参数。	0X0000	不返回任何相关标签参数。只是返回标签 EPC 号(包括标签 PC，CRC)。
	0X0001	Bit0 置位即标签在盘存时间内被盘存到的次数将会返回
	0X0002	BIT1 置位即标签的 RSSI 信号值将会被返回
	0X0004	BIT2 置位即标签 被盘存到时所用的天线 ID 号将会被返回。（天线逻辑号）
	0X0008	BIT3 置位即标签被盘存到时所用的频率值将会被返回
	0X0010	BIT4 置位即标签被盘存到时读写器的时间值将会被返回
	0X0020	BIT5 置位即 RFU 预留值将会被返回
	0X0040	BIT6 置位则目前读写器使用的标签协议值将会被返回
	0X0080	BIT7 置位即数据长度与内存数据将会被返回（只有 0X22 命令嵌入 0X28 命令时读到内存数据了，置该位将返回读取到的数据位长度与数据，否则只返回 0X0000）
Read Option	0x00	返回还未被获取的标签信息
	0x01	返回上一条 0X29 命令所获取的标签信息

备注：0X22 命令嵌入 0X28 命令暂时不支持。

该命令读写器到主机的回复可包括下面信息：

Get EPC and Metadata Response Fields

Field	Length	Value
SOH	1byte	0xFF
Length	1byte	取决于返回数据

OpCode	1byte	0X29
Status	2byte	命令操作状态码，0X0000 为操作成功。
Metadata Flags	2byte	指示哪些 Metadata 需要返回的，同主机发给模块命令中的
Read Options	1byte	同主机发给读写器命令中的
Tag Count	1byte	本次返回信息中包含的标签数。
Read Count$_1$	1byte	标签被盘存到的次数
RSSI$_1$	1byte	标签信号强度,单位 DBM，该值是有符号字符字节
Antenna ID$_1$	1byte	盘存到标签的天线 ID，高 4 位为发射天线，低 4 位为接收天线。（天线逻辑号）
Frequency$_1$	3byte	盘存到标签时的频率，单位 KHZ
Timestamp$_1$	4byte	读写器的系统时间，单位毫秒，目前时间值无效
RFU$_1$	2byte	预留数据
Protocol ID	1byte	标签协议（0X05 表示 GENT2）
Tag Data Length	2byte	标签数据位长度。0X22 命令嵌入 0X28 命令时读到的标签内存数据位长度，如果 0X22 命令未嵌入 0X28 命令或者嵌入了 0X28 命令但是对该标签进行 0X28 命令操作失败，则该值为 0X0000。
Tag Data	N bytes	标签内存数据，长度为 Tag Data Length/8。
EPC Length	2byte	EPC 区内容的位长度，包括 PC 跟 CRC。
PC Word	2byte	EPC 区的 PC 值
EPC ID	N byte	标签 EPC 号
Tag CRC	2byte	标签 CRC
重复从 Read Count 到 Tag CRC 的内容为其他的标签，重复次数由 Tag Count 决定。		
CRC	2byte	命令串 CRC

备注：0X22 命令嵌入 0X28 命令暂时不支持。

例子 1：

返回盘存次数 Read Count，盘存天线 AntennaID 和被盘存到时的时间。

Metadata Flags = 0x0001 OR 0x0004 OR 0x0010 = 0x0015

主机到读写器：

FF	03	29	00 15	00	97 55
SOH	Length	Opcode	Metadata Flags	Read Options	CRC

读写器到主机：

FF	34	29	00 00	00 15	00	02
SOH	Length	Opcode	Status	Metadata Flags	Read Options	Tag Count

22	11	02 50 CE F6	00 80	31 C1	111122223333444455556666	FB15
Read Count	Ant ID	Timestamp	EPC length	PC word	Tag EPC ID	Tag CRC

0E	11	04 1D 3D 3C	00 80	30 00	050000000000000000002354	4AC8
Read Count	Ant ID	Timestamp	EPC length	PC word	Tag EPC ID	Tag CRC

1A B8
CRC

例子 2：

返回除 Protocol ID 标签协议之外的所有能返回的标签参数信息。

Metadata Flags = **0x00BF**

主机到读写器：

FF	03	29	00 BF	00	4B 22
SOH	Length	Opcode	Metadata Flags	Read Options	CRC

读写器到主机：

FF	4A	29	00 00	00 BF	00	02
SOH	Length	Opcode	Status	Metadata Flags	Read Options	Tag Count

07	E3	11	0E 22 2A	00 00 8D 8F	00 00	00 00
Read Count	RSSI	Ant ID	Frequency	Timestamp	RFU	Tag Data Length

00 60	**20 00**	**11 11 22 22 33 33 44 44**	**C2 41**
EPC length	PC word	Tag EPC ID	Tag CRC

07	D0	11	0E 22 2A	00 00 8D 87	00 00	00 00
Read Count	RSSI	Ant ID	Frequency	Timestamp	RFU	Tag Data Length

00 D0	58 00	11 11 22 22 33 33 44 44 55 55 66 66 77 77 88 88 99 99 00 00 AA AA	96 86
EPC length	PC word	Tag EPC ID	Tag CRC

DC 46
CRC

例子 3：备注：0X22 命令嵌入 0X28 命令暂时不支持

0X22 命令嵌入了 0X28 命令，读取 TID 区 0 地址开始 2 个字，返回除 Protocol ID 标签协议之外的所有能返回的标签参数信息。

Metadata Flags = **0x00BF**

主机到读写器：

FF	03	29	00 BF	00	4B 22
SOH	Length	Opcode	Metadata Flags	Read Options	CRC

读写器到主机：

FF	6E	29	00 00	00 BF	00	03
SOH	Length	Opcode	Status	Metadata Flags	Read Options	Tag Count

08	D7	11	**0D F7 32**	**00 00 71 9B**	00 00	00 20	**E2 00 34 12**
Read Count	RSSI	Ant ID	Frequency	Timestamp	RFU	Tag Data Length	Tag Data

00 80	**30 00**	**E2 00 81 81 81 16 02 40 08 20 C7 4C**	**7E 4C**
EPC length	PC word	Tag EPC ID	Tag CRC

08	D5	11	**0D F7 32**	**00 00 71 B5**	00 00	00 20	**E2 00 60 04**
Read Count	RSSI	Ant ID	Frequency	Timestamp	RFU	Tag Data Length	Tag Data

00 D0	58 00	11 11 22 22 33 33 44 44 55 55 66 66 77 77 88 88 99 99 00 00 AA AA	96 86
EPC length	PC word	Tag EPC ID	Tag CRC

07	D4	11	**0D F7 32**	**00 00 71 8D**	00 00	00 20	**E2 00 60 04**
Read Count	RSSI	Ant ID	Frequency	Timestamp	RFU	Tag Data Length	Tag Data

00 20	**00 00**	**E2 F0**
EPC length	PC word	Tag CRC

03 8A
CRC

该命令可能返回的状态码如下：

0X0000：操作成功；

0X0100：数据长度出错

0X0105：不可用参数值，参数错误

其他非 0 为操作失败，见后面错误码解释，未有解释仅表示操作失败。

（9）0X2A:清除标签缓存区命令（该命令可不用，因每次启动新的盘存缓冲区会自动清 0）：

清除掉上次盘存到的标签信息，清 0 缓冲区。

主机到读写器：

FF	00	2A	1D 25
SOH	Length	Opcode	CRC

该命令可能返回的状态码如下：

0X0000：操作成功；

0X0100：数据长度出错

0X0105：不可用参数值，参数错误

其他非 0 为操作失败，见后面错误码解释，未有解释仅表示操作失败。

3.APP 层设置命令：

APP 层设置命令所有命令可能返回的状态码为：

0X0000：操作成功；

0X0100：数据长度出错

0X0105：不可用参数值，参数错误

其他非 0 为操作失败，见后面错误码解释，未有解释仅表示操作失败。

（1）0X91:天线口设置命令：

目前读写器的发射天线与接收天线为同一个天线，即是收发一体的，所以设置时发射天线逻辑号必须跟接收天线逻辑号一样，且成对出现。读写器共有 1 个天线口，设置天线命令有多种格式，设置命令中的天线逻辑号与实际物理天线口的对应关系如下：

TX ANT NUM（天线逻辑号）	RX ANT NUM（天线逻辑号）	实际物理天线口
01	01	天线口 1

目前读写器上电默认初始发射功率是 20dbm。

各个命令格式的详解如下：

1） 设置单个天线口工作（读写器本身为一个天线口，可不用发送该命令）：

主机到读写器：

FF	02	91	01	01	70 3B
SOH	Length	Opcode	TX Ant Num	RX Ant Num	CRC

或者

FF	03	91	00	01	01	?? ??
SOH	Length	Opcode	Option	TX Ant Num	RX Ant Num	CRC

备注：Option=0;

上例为设置天线口 1 工作，TX Ant Num 与 RX Ant Num 的值必须一样，见上表。该命令为对单一标签进行操作的时候用（如：单标签读 0X21,写 EPC 0X23,写标签内存 0X24,锁标签 LOCK,读标签内存 0X28 等）。

2） 设置单个或多个天线口工作（该命令无效，预留）：

当 Option=2 时为设置单个或多个天线口工作，命令格式见下表：

Field	Value	Description
Length	1 byte	数据长度，取决于实际长度
Opcode	0x91	
Option	0x02	
TX、RX ANT NUM(天线逻辑号对，对应关系见上表)	2 bytes	1 个到 4 个 2 字节的天线逻辑号对设置。根据所使能工作的天线数量确定。读写器默认上电是使能物理天线

		口 1 工作，设置多个天线工作时，天线的工作顺序是按照从物理天线口 1->3>2->4 顺序工作的。

例子 1：

使能逻辑天线 1 与逻辑天线 4 工作：

主机到读写器：

FF	05	91	02	01	01	04	04	2B C6
SOH	Length	Opcode	Option	TX Ant Num	RX Ant Num	TX Ant Num	RX Ant Num	CRC

读写器到主机：

FF	00	91	00 00	17 58
SOH	Length	Opcode	Status	CRC

例子 2：

使能 4 个逻辑天线都工作：

主机到读写器：

FF	09	91	02	01	01	03	03
SOH	Length	Opcode	Option	TX Ant Num	RX Ant Num	TX Ant Num	RX Ant Num

02	02	04	04	9E 8F
TX Ant Num	RX Ant Num	TX Ant Num	RX Ant Num	CRC

备注：天线逻辑号对参数在命令中可以不分顺序。

3）设置天线口的发射功率与天线配置时间。

当 Option=3 或 Option=4 时都可以设置天线发射功率，仅当 Option=4 时可以设置天线配置时间。命令格式如下：

Field	Value	Description
Length	1byte	数据长度，取决于实际长度
Opcode	0x91	
Option	0x03/0x04	Option=0x03 时只是设置发射功率；Option=0x04 时设置发射功率与天线配置时间。
TX ANT NUM	1byte	发射天线逻辑号
READ POWER	2bytes	读时发射功率，单位 0.01dbm，实际有效值以 1dbm 为单位，也即是比如设置 0x0800=20.48dbm，而实际最后只会输出 20dbm。
WRITE POWER	2bytes	写时发射功率，单位 0.01dbm，实际有效值以 1dbm 为单位，也即是比如设置 0x0800=20.48dbm，而实际最后只会输出 20dbm。
SETTING TIME	2bytes	天线设置时间，单位微妙 us，

		当轮到某天线工作时，在该天线开始工作前，对天线进行设置时间，射频开启前停留时间。目前该值不起实际作用。（只当 Option=0x04 时命令中才包含该参数）
读写器只有一个天线口，所以天线逻辑号为 1。		

备注：READ POWER 适用的命令为：单标签盘存命令 0X21，多标签盘存命令 0X22，读标签存储区命令 0X28。
WRITE POWER 适用的命令为：除 READ POWER 适用的命令外的其他标签操作命令，比如写标签存储区命令 0X24，标签锁命令 0X25 等等。

例子 1：
Option=0x04，设置天线发射功率与天线设置时间。设置天线的读发射功率为 20dbm,写发射功率为 30dbm。
主机到读写器：

FF	08	91	04	01	07 D0	0B B8	01 F4
SOH	Length	Opcode	Option	TX ANT NUM	READ POWER	WRITE POWER	SETTING TIME
?? ??							
CRC							

读写器到主机：

FF	00	91	00 00	17 58
SOH	Length	Opcode	Status	CRC

备注：读功率跟写功率的值可以设置不同。
当 Option=0x03 时，命令格式为 Option=0x04 的命令中去掉 SETTING TIME 即是。

（2）0X92:设置读发射功率；目前该命令设置的值模块会忽略，设置功率值请用 0X91 命令；
命令格式如下：
主机到读写器：

FF	02	92	09 C4	48 9D
SOH	Length	Opcode	POWER(单位 0.01dbm)	CRC

（3）0X93:设置当前工作标签协议；
设置标签工作协议，目前该读写器只适用于 GEN2，18K-6C 协议。
命令如下：
主机到读写器：

FF	02	93	00 05	51 7D
SOH	Length	Opcode	Current Protocol	CRC

Current Protocol：2 字节，0X0005 表示 GEN2，18K-6C 协议。目前读写器只适用于该协议。所以可不使用该命令，模块默认上电即是使用 6C 协议

（4）0X94:设置写发射功率；目前该命令设置的值模块会忽略，设置功率值请用 0X91 命令；

命令格式如下：

主机到读写器：

FF	02	94	09 C4	28 5B
SOH	Length	Opcode	POWER(单位 0.01dbm)	CRC

（5）0X95:跳频设置；

1）指定设置读写器工作在哪些频点，目前设置在那个频段就只能设置该频段内对应的频点。命令格式如下：

例子 1：设置读写器工作在北美 915250KHZ,903250KHZ,926750KHZ 三个频点，设置之后，读写器发射的载波频率就在这 3 个频点之间轮流切换，切换时间为 400ms，也即是每个频点工作时间为 400MS。(每个频段区域对应的可设置频点见 0X97 命令解释)

主机到读写器：

FF	0C	95	00 0D F7 32	00 0D C8 52	00 0E 24 1E	E5 24
SOH	Length	Opcode	Freq #1	Freq#2	Freq#3	CRC

读写器到主机：

FF	00	95	00 00	57 DC
SOH	Length	Opcode	Status	CRC

2）设置跳频时间，即是每个频点工作时间。目前读写器默认北美频段的跳频时间是 400MS，中国频段是 1000MS，欧洲频段是 4000MS。用户如无特别需求请勿更改该时间。

命令格式如下：

Field	Value	Description
Length	0x05	命令数据长度
Opcode	0x95	
Option	0x01	
Hop time	4 bytes	跳频时间，单位毫秒。

例子 1：设置跳频时间为 256ms。

主机到读写器

FF	**05**	**95**	**01**	**00 00 01 00**	**?? ??**
SOH	**Length**	**Opcode**	**Option**	**Hop time**	**CRC**

（6）0X96:GPIO 输出设置；目前该功能无效，请勿使用。

读写器有两路输出 GPIO 口，设置 GPIO 口输出命令格式如下：

例子 1：

设置输出 GPIO 口 1 输出为 1（高）；

主机到读写器

FF	02	96	01	01	28 E0
SOH	Length	Opcode	GPIO 1	Output Value	CRC

读写器到主机：

FF	00	96	00 00	?? ??
SOH	Length	Opcode	Status	CRC

例子 2：

设置输出 GPIO 口 1 输出为 1（高），设置输出 GPIO 口 2 输出为 0（低）：

主机到读写器：

FF	04	96	01	01	02	00	?? ??
SOH	Length	Opcode	GPIO 1	Output val	GPIO 2	Output val	CRC

读写器到主机：

FF	00	96	00 00	?? ??
SOH	Length	Opcode	Status	CRC

如果要获取输出 GPIO 口输出状态，则发送下面命令：

主机到读写器：

FF	00	96	1D 99
SOH	Length	Opcode	CRC

读写器到主机：

FF	02	96	00 00	01	00	28 E1
SOH	Length	Opcode	Status	output #1	output #2	

读写器回复表示输出 GPIO 口 1 的输出状态为 1，输出 GPIO 口 2 的输出状态为 0；

读写器上电默认两输出口都为 0；

（7）0X97:设置当前工作频率区域；

设置值与对应频率区域关系如下：

区域 region	设置值 code
北美（902-928）	0x01
中国 1（920-925）	0x06
欧频（865-867）	0x08
中国 2（840-845）	0x0a

北美跳频表：

NAfrelist[50]= {915750,915250,903250,926750,926250,904250,927250,920250,919250,909250,
918750,917750,905250,904750,925250,921750,914750,906750,913750,922250,
911250,911750,903750,908750,905750,912250,906250,917250,914250,907250,
918250,916250,910250,910750,907750,924750,909750,919750,916750,913250,

923750,908250,925750,912750,924250,921250,920750,922750,902750,923250};

中国 1 跳频表：

Chinafrelist1[16]={921375,922625,920875,923625,921125,920625,923125,921625,
922125,923875,921875,922875,924125,923375,924375,922375};

欧频跳频表：

Eu3frelist[4]={865700,866300,866900,867500};

中国 2 跳频表：

Chinafrelist2[16]={841375,842625,840875,843625,841125,840625,843125,841625,
842125,843875,841875,842875,844125,843375,844375,842375};

备注：1.当使用 0X95 命令设置频点时，当前设置读写器工作在哪个频段区域，就只能设置该区域对应的跳频表里面的频点。2.设置读写器工作在那个频段读写器就自动按照跳频表里频点顺序跳频工作，读写器上电默认工作在北美频段，如无使用 0X95 命令设置工作频点，则读写器在北美频段内按照上面跳频表顺序跳频工作。

例子 1：

设置工作频率区域为北美频段。

主机到读写器:

FF	01	97	01	?? ??
SOH	Length	Opcode	code	CRC

读写器到主机：

FF	00	97	00 00	?? ??
SOH	Length	Opcode	Status	CRC

例子 2：

设置工作频率区域为中国 1 频段.

主机到读写器:

FF	01	97	06	?? ??
SOH	Length	Opcode	code	CRC

读写器到主机：

FF	00	97	00 00	?? ??
SOH	Length	Opcode	Status	CRC

（8）0X98:设置功率模式（目前该命令无效）；

命令格式如下：

主机到读写器：

FF	01	98	03	44 BE
SOH	Length	Opcode	Power Mode	CRC

Power Mode：对该值的定义请看 0X68 命令中介绍，没特别需求无需设置或设置为 0。

（9）0X99:设置用户模式；目前该命令设置的值读写器会忽略；

该命令预留未来用，命令格式如下：

主机到读写器：

FF	01	99	00	?? ??
SOH	Length	Opcode	User Mode	CRC

（10）0X9A:设置阅读器配置；

相关配置信息如下：

可用配置选择

Option	key	value	Reader configuration setting
0x01（固定为该值）	**0x00**:盘存到的标签是否以被盘存到时所用的天线口来判断是否跟其他天线口盘存到的同样 EPC 号的标签区别开来。（预留用，目前读写器只有一个天线口，故该设置实际无效）	0x00	不同天线口盘存到的同样 EPC 号的标签当作不同的标签，即如果两个不同天线口盘存到两个 EPC 号一样的标签，则盘存命令（0X22）返回时盘存到的标签数是 2，而不是 1。（读写器上电默认为该设置）
		0x01	不管是哪个天线口，如果盘存到同样 EPC 号的标签，则认为是同一个标签，即认为盘存到的标签数为 1，只是单单给标签被盘存到的次数加 1 而已，而不是当作 2 个标签。
	0x01:射频发射模式（预留未来用，目前的设置不起作用）	0x00	高功耗模式（上电默认设置）
		0x01	低功耗模式
	0x02: 预留未来用，标签 EPC 最大长度，目前的设置不起作用，目前读写器可接收的最大长度 EPC 号为 496bit。	0x00	
		0x01	
	0x03:预留未来使用	0x00	
		0x01	
		0x02	
		0x03	
	0x04: 预留未来用，天线口检测。	0x00	不使用天线口检测（上电默认设置）
		0x01	使能天线口检测功能
	0x06:最大 RSSI 信号强度值保存。	0x00	metadata 中 RSSI 信号值保存标签最后一次被盘存到时的信号强度值。（上电默认设置）
		0x01	metadata 中 RSSI 信号值保存标签被盘存到的所有次数中最大的值。
	0x08: 预留用，附加数据唯一使用与否，0X22 命令嵌入读内存使用。	0x00	当采用盘存嵌入读时，如果 EPC 号一样但读取的内存数据不一样则认为是不一样的标签。
		0x01	EPC 一样的标签都认为是一个标签（默认
	0x09:预留未来使用	0x00	
		0x01	

例子 1：设置不管哪个天线口盘存到同样 EPC 号的标签都认为是同一个标签。

主机到读写器：

FF	03	9A	01	00	01	?? ??

SOH	Length	Opcode	Option	Key	Value	CRC

读写器到主机：

FF	00	9A	00 00	A6 33
SOH	Length	Opcode	Status	CRC

备注：设置命令中 key 值的不同表示本次要设置的是那项的内容，value 值为本次设置该项为那种工作方式。

（11）0X9B:设置协议配置；

相关配置信息如下：

可用配置选择

Protocol Value	**parameter**	**option**	**value**
0x05: (gen2)	**0x00:** 选择盘存标签时使用的 session。	无该项	**0x00**:选择 s0(上电默认)
			0x01:选择 s1
			0x02:选择 s2
			0x03:选择 s3
	0x01: 选择盘存标签时使用的 target。	**0x01**: 静态 target。	**0x00**:使用 target A（上电默认）
			0x01:使用 target B
		0x00: 动态 target，从 A 盘存完后转到 B 或者从 B 盘存完后转到 A。	**0x00**:从 A 开始盘存，直到盘存不到标签后再转到 B。（只适用 0x22 命令，如果使用了该动态 target 进行 0x22 命令操作后，进行其他读写 LOCK 等命令操作时没有重新设置使用静态 Q 则使用 target A 进行其他命令操作）
			0x01: 从 B 开始盘存，直到盘存不到标签后再转到 A。（只适用 0x22 命令，如果使用了该动态 target 进行 0x22 命令操作后，进行其他读写 LOCK 等命令操作时没有重新设置使用静态 Q 则使用 target B 进行其他命令操作）
	0x02: Miller 编码选择，预留	无该项	**0x01**:(M=2)
			0x02:(M=4) 上电默认

	未来使用。		使用 **0x03**:(M=8)
	0x12: Q 值设置	**0x00**: **Dynamic Q，**使用动态 Q 值，读写器根据盘存情况自动更改 Q 值进行盘存（上电默认）	无该项。
		0x01: **Static Q，**使用静态 Q 值	**0x00** 到 **0x0F**(1 字节，Q 值)

例子 1：

设置使用 SESSION 1 进行盘存。

主机到读写器：

FF	03	9B	05	00	01	DC E9
SOH	Length	Opcode	Protocol value	Parameter	Value	CRC

读写器到主机：

FF	00	9B	00 00	B6 12
SOH	Length	Opcode	Status	CRC

例子 2：

设置使用 Static Q 进行盘存，Q=3。

主机到读写器：

FF	04	9B	05	12	01	03	80 AC
SOH	Length	Opcode	Protocol value	Parameter	Option	Value	CRC

读写器到主机：

FF	00	9B	00 00	B6 12
SOH	Length	Opcode	Status	CRC

例子 3：

设置使用静态 Target B 进行盘存。

主机到读写器：

FF	04	9B	05	01	01	01	A2 FC
SOH	Length	Opcode	Protocol value	Parameter	Option	Value	CRC

读写器到主机：

FF	00	9B	00 00	B6 12
SOH	Length	Opcode	Status	CRC

4.获取 APP 层设置信息命令：

获取 APP 层设置信息命令所有命令可能返回的状态码为：

0X0000：操作成功；

0X0100：数据长度出错

0X0105：不可用参数值，参数错误

其他非 0 为操作失败，见后面错误码解释，未有解释仅表示操作失败。

（1）0X61:获取天线口配置信息；

此命令其实为获取 0X91 命令设置的天线口信息。该命令有多种使用方式。

1) 获取设置的单天线口工作信息：当使用过 0X91 命令设置过单天线口工作时，此命令返回设置的那个工作天线口的信息。（由于读写器只有一个天线口，所以返回是天线逻辑号 1）

命令格式如下：

主机到读写器：

FF	01	61	00	BD BD
SOH	Length	Opcode	Option	CRC

读写器到主机：

FF	02	61	00 00	01	01	?? ??
SOH	Length	Opcode	Status	TX ant num	RX ant num	CRC

2)获取天线各方面信息：

获取天线各方面信息命令格式如下：

Get Antenna Port Command Fields

Field	Value	Description
Length	0x01	
Opcode	0x61	
Option	0x02	获取哪些逻辑天线已设置为工作天线的信息
	0x03	获取所有逻辑天线口的读写发射功率。
	0x04	获取所有逻辑天线口的读写发射功率和天线配置时间。
	0x05	获取所有逻辑天线口的连接状态。（目前读写器未有检测天线功能，所以该命令返回的信息无意义）

1) 例子 1：获取目前哪些逻辑天线已设置为工作天线。（由于读写器只有一个天线口，所以返回是天线逻辑号 1）

主机到读写器：

FF	01	61	02	BD BF
SOH	Length	Opcode	Option	CRC

读写器到主机：

FF	03	61	00 00	02
SOH	Length	Opcode	Status	Option
01		01		? ? ? ?
TX ant num		RX ant num		CRC

2）例子 2：获取逻辑天线口的读写发射功率，假设都为 30DBM。

主机到读写器：

FF	01	61	03	BD BE
SOH	Length	Opcode	Option	CRC

读写器到主机：

FF	29	61	00 00	03
SOH	Length	Opcode	Status	Option

01	0B B8	0B B8	02	00 00	00 00
TX ant num	Read Power	Write Power	TX ant num	Read Power	Write Power
03	00 00	00 00	04	00 00	00 00
TX ant num	Read Power	Write Power	TX ant num	Read Power	Write Power
05	00 00	00 00	06	00 00	00 00
TX ant num	Read Power	Write Power	TX ant num	Read Power	Write Power
07	00 00	00 00	08	00 00	00 00
TX ant num	Read Power	Write Power	TX ant num	Read Power	Write Power

? ? ? ?
CRC

3）例子 3：获取逻辑天线口的读写发射功率与配置时间，假设都为 30DBM，配置时间目前无实际意义。

主机到读写器：

FF	01	61	04	BD B9
SOH	Length	Opcode	Option	CRC

读写器到主机：

FF	39	61	00 00	04
SOH	Length	Opcode	Status	Option

01	0B B8	0B B8	01 F4	02	00 00	00 00	00 00
TX ant num	Read Power	Write Power	Setting time	TX ant num	Read Power	Write Power	Setting time
03	00 00	00 00	00 00	04	00 00	00 00	00 00
TX ant num	Read Power	Write Power	Setting time	TX ant num	Read Power	Write Power	Setting time
05	00 00	00 00	00 00	06	00 00	00 00	00 00
TX ant num	Read Power	Write Power	Setting time	TX ant num	Read Power	Write Power	Setting time
07	00 00	00 00	00 00	08	00 00	00 00	00 00
TX ant num	Read Power	Write Power	Setting time	TX ant num	Read Power	Write Power	Setting time

? ? ? ?
CRC

备注：TX ant num 2-8 预留未来使用。

例子 4：获取逻辑天线口的连接状态：

主机到读写器：

FF	01	61	05	BD B8
SOH	Length	Opcode	Option	CRC

读写器到主机：

FF	03	61	00 00	05
SOH	Length	Opcode	Status	Option

01	00	?? ??
TX ant num	connection status	CRC

connection status:

0 为未检测到天线；

1 为检测到天线。

（2）0X62:获取读发射功率信息；

命令格式如下：

主机到读写器：

FF	01	62	01	BE BC
SOH	Length	Opcode	Option	CRC

读写器到主机：

FF	07	62	00 00	01
SOH	Length	Opcode	Status	Option

07 D0	0B B8	07 6C	?? ??
Current TX power(dbm)	Max TX power(dbm)	Min TX power(dbm)	CRC

备注：

Option:目前的值只能设置为 0 跟 1，无论设置哪个值，返回结果都是一样；

Current TX power:目前该值没意义，返回的是读写器上电默认 发射功率；

Max TX power：读写器最大发射功率，目前是 30dbm。

Min TX power：读写器最小发射功率，目前是 5dbm。

（3）0X63:获取当前工作标签协议；

目前读写器只能适应 EPC GEN2，18K-6C 协议。命令格式如下：

主机到读写器：

FF	00	63	1D 6C
SOH	Length	Opcode	CRC

读写器到主机：

FF	02	63	00 00	00 05	21 46
SOH	Length	Opcode	Status	Current procotol	

Current Protocol：2 字节，0X0005 表示 GEN2，18K-6C 协议。目前读写器只适用于该协议。

（4）0X64:获取写发射功率信息；

命令格式如下：

主机到读写器：

FF	01	64	01	B8 BC
SOH	Length	Opcode	Option	CRC

读写器到主机：

FF	07	64	00 00	01
SOH	Length	Opcode	Status	Option

07 D0	0B B8	07 6C	?? ??
Current TX power(dbm)	Max TX power(dbm)	Min TX power(dbm)	CRC

备注：

Option:目前的值只能设置为 0 跟 1，无论设置哪个值，返回结果都是一样；

Current TX power:目前该值没意义，返回的是读写器上电默认 发射功率；

Max TX power：读写器最大发射功率，目前是 30dbm。

Min TX power：读写器最小发射功率，目前是 5dbm。

（5）0X65:获取跳频表；

该命令为获取所设置工作的频率信息与获取跳频间隔。

1） 获取所设置工作的频率信息。

主机到读写器：

FF	00	65	1D 6A
SOH	Length	Opcode	CRC

读写器到主机，假设已设置读写器工作的频点是 915750Khz，903250Khz，926750Khz。

FF	0C	65	00 00	00 0D F9 26
SOH	Lengt	Opcode	Status	Freq #1

00 0D C8 52	00 0E 24 1E	2C B5
Freq #2	Freq #3	CRC

Freq #N：频率值，4 字节，单位是 Khz。

2） 获取跳频间隔。

主机到读写器：

FF	01	65	01	B9 BC
SOH	Length	Opcode	Option	CRC

读写器到主机：

FF	05	65	00 00	01	00 00 01 90	4B 6C
SOH	Length	Opcode	Status	Option	Hop Time(ms)	CRC

（6）0X66:获取输入 GPIO 的值；目前该功能无效，请勿使用。

命令格式如下：

主机到读写器：

FF	00	66	1D 69
SOH	Length	Opcode	CRC

读写器到主机，假设输入 GPIO #1 的输入状态为 0，GPIO # 2 的输入状态为 1：

FF	02	66	00 00	00	01	CA B2
SOH	Length	Opcode	Status	Input #1	Input #2	CRC

（7）0X67:获取当前工作频率区域；

该命令为获取当前工作频率区域，其实也即是获取 0X97 命令所设置的频率工作区域，读写器上电默认工作频率区域为北美。

例子 1：假设读写器工作在北美频段。

主机到读写器：

FF	00	67	1D 68
SOH	Length	Opcode	CRC

读写器到主机：

FF	01	67	00 00	01	B4 80
SOH	Length	Opcode	Status	Region code	CRC

（8）0X68:获取功率模式；

目前该命令获取的信息无实际意义。命令格式如下：

主机到读写器：

FF	00	68	1D 67
SOH	Length	Opcode	CRC

读写器到主机：

FF	01	68	00 00	02	A4 BD
SOH	Length	Opcode	Status	Power mode	CRC

（9）0X69:获取用户模式；

目前该命令获取的信息无实际意义。命令格式如下：

主机到读写器：

FF	00	69	1D 66
SOH	Length	Opcode	CRC

读写器到主机：

FF	01	69	00 00	01	97 8F
SOH	Length	Opcode	Status	User mode	CRC

（10）0X6A:获取配置；

该命令为获取 0X9A 命令所设置的值。命令格式如下：

主机到读写器：

FF	02	6A	01	00	2E 4E
SOH	Length	Opcode	Option	Key	CRC

读写器到主机：

FF	03	6A	00 00	01	00	01	AF 5C
SOH	Length	Opcode	Status	Option	Key	Value	CRC

备注：命令中的 Option，Key，Value 与 0X9A 命令中的是一致的，所以要获取哪方面的信息，就把 Key 设置为相对应的值。

（11）0X6B:获取协议配置；

该命令为获取 0X9B 命令所设置的值。命令格式如下：

例子 1：获取所使用的盘存 session。

主机到读写器：

FF	02	6B	05	00	3A 6F
SOH	Length	Opcode	Procotol Value	Parameter	CRC

读写器到主机，假设采用 S0：

FF	03	6B	00 00	05	00	00	08 74
SOH	Length	Opcode	Status	Procotol Value	Parameter	Value	CRC

例子 2：获取采用的 target。

主机到读写器：

FF	02	6B	05	01	3A 6E
SOH	Length	Opcode	Procotol Value	Parameter	CRC

读写器到主机，假设采用静态 STATIC TARGET A：

FF	04	6B	00 00	05	01	01	00	2C 68
SOH	Length	Opcode	Status	Procotol Value	Parameter	Option	Value	CRC

备注：命令中的 Procotol Value，Parameter，Option，Value 与 0X9B 命令中的是一致的，在主机发往读写器的命令中只需要包含 Procotol Value，Parameter 两个参数，想要获取哪方面的信息，就把 Parameter 设置为相对应的值。

（12）0X70:获取可用标签协议；

目前只有 GEN2，18K-6C 协议，命令格式如下：

主机到读写器：

FF	00	70	1D 7F
SOH	Length	Opcode	CRC

读写器到主机：

FF	02	70	00 00	00 05	3B 75
SOH	Length	Opcode	Status	Procotol Value	CRC

（13）0X71:获取可用的工作频率区域；

目前可用的有北美频段、中国频段、欧频。命令格式如下：

主机到读写器：

FF	00	71	1D 7E
SOH	Length	Opcode	CRC

读写器到主机：

FF	02	71	00 00	01	06	0D 46
SOH	Length	Opcode	Status	Region #1	Region #2	CRC

（14）0X72：获取当前读写器温度；

目前该命令获取的信息无实际意义。。命令格式如下：

主机到读写器：

FF	00	72	1D 7D
SOH	Length	Opcode	CRC

读写器到主机：

FF	01	72	00 00	27	48 20
SOH	Length	Opcode	Status	Temperature	CRC

Temperature：温度值，1 字节，有符号数。

五.返回状态码详解:

0x0000:操作成功
0X0100:数据实际长度跟长度字节的值不一样
0X0101:不可用命令
0X0105:不可用参数值
0X010A:不可用波特率
0X010B:不可用区域选择（北美，中国，欧洲等）
0X0200:应用层程序 CRC 不正确，校验应用层程序 CRC 错误。
0X0302:FLASH 未定义错误，FLASH 写入失败。
0X0400:未找到标签（盘存读写 LOCK 等 操作失败，没找到标签）
0X0402:协议不可用（GEN2 或 6B 什么的）
0X040A:一般标签错误（读写 LOCK,KILL 命令）
0X040B:读内存的长度值超限。（如只能读 96 个字一次，
0X040C:不可用的 KILL 密码
0X0420:GEN2 OTHER ERR
0X0423:MEMORY OVERRUN BAD PC
0X0424:MEM LOCKED
0X042B:INSUFFICIENT POWER
0X042F:NON SPECIFIC ERR
0X0430:UNKNOWN ERR
0X0500:不可用频率值
0X0504:温度超限
0X0505:反射过大
0X7F00:系统不知道的错误，严重错误。

0XAA2A:OEM 格式化失败
0XAA02:OEM 写失败
0XAA03:OEM 读失败
0XAA04:测试校验命令失败

0XAA1B:GROSS GAIN 校验失败
0XAA24:命令失败
0XAA27:命令失败
0XAA2C:命令失败
0XAA2E:MAC 寄存器写失败
0XAA2F:MAC 寄存器读失败

0XFF01:初始化定时器出错；
0XFF02:OEM 初始化失败；
0XFF03: 失败
0XFF04: 失败
0XFF05: 失败
0XFF06: 失败
0XFF07: 失败
0XFF08: 失败
0XFF09: GPIO 配置出错
0XFF0A: QM100 芯片初始化失败
0XFF0B: 失败
0XFF0C: 失败
0XFF0D: 失败
0XFF0E: 失败

其他非 0 值表示命令执行失败。

附录 1：OEM 寄存器读写命令：

一. 发送命令格式：

0xFF+DATALEN+0xAA+”Moduletech”+SubCmdHighByte+SubCmdLowByte+data+SubCrc+0xbb+CRC

1. SubCrc：1 字节，为 SubCmdHighByte 开始到 data 结束的所有数据相加结果的低 8 位值；
2. SubCmdHighByte：1 字节，为子命令码的高 8 位
3. SubCmdLowByte：1 字节，为子命令码的低 8 位
4. Data:命令的数据段；

二. 返回命令格式：

0xFF+DATALEN+0XAA+STATUS +”Moduletech”+SubCmdHighByte+SubCmdLowByte+data+CRC

1. STATUS：2 字节状态码，高字节在前；0 为操作成功，其他值为操作失败，操作失败时，返回命令格式非全部按照上述返回格式，所以上位机收到返回的操作失败协议帧时只需通过状态码值判断为何种失败原因；
2. Data:返回的数据；

备注 1：”Moduletech”为字符串（发送命令时请转化为对应的 16 进制）；

备注 2：格式与上文介绍的通信协议格式一样。

备注 3：SubCmdHighByte+SubCmdLowByte 为子命令码（主命令码为 0XAA）；

备注 4：整个通信数据串的字节数不得大于 255 个字节；

三．SubCmd 命令码：

1.0XAA2A:OEM 格式化命令

2.0XAA02:写 OEM 寄存器命令

3.0XAA03:读 OEM 寄存器命令

四．SubCmd 命令码详解：

1.0XAA2A:OEM 格式化命令，目前没有 DATA 段（该命令谨慎使用）

2.0XAA02:写 OEM 寄存器命令：

发送命令 DATA 格式为：ADDR_N+DATA_N，N 组地址加数据对，ADDR_N 为 2 字节 OEM 寄存器地址，DATA_N 为 4 字节写入 OEM 寄存器的值，高字节在前。

返回命令格式：

FF+DATALEN+0XAA+STATUS+”Moduletech”+0XAA+0X02+CRC

3.0XAA03:读 OEM 寄存器命令

发送命令 DATA 格式为：ADDR_N,N 个 2 字节长度的需要读取的 OEM 寄存器的地址，最多一次读取 32 个寄存器的值，高字节在前；

正确返回命令格式：

FF+DATALEN+0XAA+STATUS+”Moduletech”+0XAA+0X03+ADDR_N+DATA_N+CRC

ADDR_N 为 OEM 寄存器的地址，2 字节，DATA_N 为对应寄存器地址的值，4 字节，高字节在前；

错误返回命令格式：

FF+DATALEN+0XAA+STATUS+”Moduletech”+0XAA+0X03+CRC

备注：

1.在 BOOTLOADER 层，只可使用 OEM 格式化命令以及读写 OEM 寄存器 0X0400 的命令。

2.在 APP 层可以使用 OEM 格式化命令以及 OEM 寄存器的读写工作，OEM 寄存器请看附录 2。

附录 2：蓝牙读写器工作情况介绍，重点：

一．升级：（此功能最好采用我们公司提供的函数接口，为后续升级更新软件用）

1. 升级界面首先出现提醒“请确认蓝牙读写器是否处于刚上电配置状态”，点击“是”后，进入下 1 步，点击“否”退出。
2. 下 1 步出现提醒“是否清除掉原先对蓝牙读写器的配置”点击“是”的话，上位机发送 OEM 写命令，将 0 写入 0X0400 地址的寄存器，点击“否”的话，上位机发送读 OEM 命令，读出 0X0400 寄存器的值，保留低 2 个字节的值，将高 2 个字节的值清 0 并写入 0X0400 寄存器；操作成功后进入下 1 步；
3. 下 1 步开始进行程序升级，首先上位机发送 0X09 命令给读写器，收到操作成功返回后，等待 500MS，即可进行写 FLASH 的升级操作，如果收到操作失败则应退出。写 FLASH 完成后发送 0X08 校验固件命令，如果读写器返回校验成功，则读写器将自动把已烧录标志写入 0X0400 寄存器，并且跳转到 APP 应用层程序，此时大约需花费 5 秒左右时间进行初始化，所以上位机收到校验成功返回后，需等待 5S 的时间，然后发送 0X0C 命令获取读写器是运行在 APP 层还是 BOOTLOADER 层命令，如收到返回是读写器运行在 APP 层，则升级成功，如返回是读写器运行在 BOOTLOADER 层则报升级失败，如读写器无回复，则再等待 3S，再重新发送 0X0C 命令，如还无回复则报升级失败。

二．蓝牙读写器有 2 种工作模式，一种是主动工作模式（由蓝牙读写器的盘存按钮控制读取标签数据，按下按钮时读取，松开按钮时不读取）；一种是被动工作模式（被动工作模式蓝牙读写器的盘存按钮无效，被动工作模式下由上位机发送指令控制读写器工作，通信协议按照本文上面介绍的通信协议进行通信）。

主动工作模式下有两个工作模式：

1. 配置模式：刚上电时是处于配置模式，此时通信协议按照本文上面介绍的通信协议进行通信，在配置模式下，用户可以对读写器的盘存相关参数进行设置；建议在配置界面，除了正常的读写器工作界面外，还须有：

   （1）增加配置保存蓝牙读写器参数界面，也即是读写器盘存标签的一些相关参数配置；

2. 工作模式：当蓝牙读写器上的盘存按钮被按下时，读写器将处于工作模式，工作模式下读写器不处理上位机发来的命令，读写器处于主动工作状态，当按下读写器盘存按键，读写器即进行盘存，盘存到标签后将以 0X29 命令的格式主动上传盘存到的标签的数据，当读写器返回的 0X29 命令中的状态码为非 0 时则表示读写器异常，上位机可报错，可采用重启读写器的方式看是否能回复正常。所以处于工作模式下，上位机只须做 1 件事，就是监控接收读写器发来的标签数据。

三．蓝牙读写器处于主动工作模式的工作模式下时，也即是蓝牙读写器的盘存按键被按下时，读写器将读取以下寄存器所保存的配置参数，进行相关盘存工作，这些寄存器的读写需在配置模式下进行，读写器出厂时会初始化出厂配置参数，客户如需进行修改，可在配置模式下采用 OEM 读写命令进行修改：

1.OEM 寄存器从 0X0400 开始存储蓝牙读写器相关配置参数，各个寄存器以及相关内容如下：

（1）0X0400：高 2 字节表示是否已烧录 APP 程序标志，值为 0XA5A5 时标志已烧录过 APP 程序，其他值表示未烧录过 APP 程序；低 2 字节表示是否已配置过读写器参数标志，值为 0X5A5A 表示已配置过读写器参数，其他值表示未配置过读写器参数。

当读写器上电运行在 BOOTLOADER 里时，首先读取该寄存器的值，如果表明已经烧录过 APP，则直接跳转到 APP 程序，如果表明未烧录过 APP，则停留在 BOOTLOADER 层。当要给读写器进行升级时，上位机首先需要先发送写 OEM 寄存器命令更改该寄存器的值，如不需要保存原先配置的读写器参数，可将该寄存器设置为 0，如要保存先前配置的读写器参数值，则只需更改高 2 字节为非 0XA5A5 即可。更改完毕后则发送运行到 BOOTLOADER 命令 0X09，然后再对读写器 进行升级。读写器收到 0X09 命令后会先读取该寄存器的值，如果表示已烧录过 APP 则会返回失败，只有该标志为未烧录 APP 才会返回操作成功，返回成功则需要等待 500MS，再对读写器进行升级。升级完毕后必须发送 0X08 检验烧录 CRC 命令，如果校验成功，读写器自己将会写入已烧录 APP 标志到该寄存器且运行至 APP 层，此时读写器执行到 APP 层后大约需 5S 的时间完成初始化。

备注：

1.读写器程序结构为每次从 BOOTLOADER 运行到 APP 时都会检测 OEM 是否已初始化过，第一次烧录 BOOTLOADER 底层后完成 APP 程序升级后读写器自己会初始化 OEM，初始化完后会重新写入已烧录 APP 标志，且写入读写器初始参数配置并赋值读写器参数配置标志。即是出厂读写器已完成读写器的初始化参数配置。

2.如果在 APP 程序中上位机发送初始化 OEM 命令给读写器的话，读写器初始化 OEM 后会重新赋值已烧录 APP 标志且写入读写器初始参数配置并赋值读写器参数配置标志。初始化 OEM 功能慎用。

3.如果在 BOOTLOADER 里面读写器收到初始化 OEM 命令则不会赋值已烧录 APP 标志，且会将整个 OEM 区的寄存器值初始为 0。初始化 OEM 功能慎用。

4.读写器程序结构为每次从 BOOTLOADER 运行到 APP 时都会检测 OEM 是否已初始化，检查完毕后会再检测读写器参数配置标志，如读写器参数配置标志未赋值，则会写入读写器初始参数配置并赋值读写器参数配置标志。

5.如用户无进行升级更新软件操作，请勿对该寄存器进行设置。

（2）0X0401：最高字节存放读写器工作模式下是采用单标签盘存还是多标签盘存还是读标签存储区标志，0XA5 为多标签盘存，0XB5 为读标签存储区，其他为单标签盘存。低 2 个字节为 METADATA FLAG 值，每个位对应读写器读到标签后返回的标签参数，详情请看备注介绍。当使用单标签盘存时会按照 0X21 命令的方式去盘存标签，也即是在设定的时间内读到一个标签就返回，适用于只读一个标签的，盘存到标签后会按照 0X29 命令返回的格式发送给上位机；当使用多标签盘存时会按照 0X22 命令的方式去盘存标签，然后在设定的盘存时间内把盘存到的一个或多个标签以 0X29 命令返回的格式发送给上位机；当使用读标签存储区时会按照 0X28 命令的方式去盘存标签，盘存到的标签数据会以 0X29 命令的格式上传给上位机，见备注介绍。如果读写器未读到标签则无任何数据发送给上位机。如果盘存到的标签量无法一次发送完毕时，则会分几次发送，每次发送的时间间隔默认为 10ms（可由 0X0448 寄存器修改该时间）。如果读写器返回的 0X29 命令中的状态码为非 0 时则表示读写器异常，上位机可报错，可采用重启读写器的方式看是否能回复正常。

备注：1.默认为单标签盘存方式；METADATA FLAG 默认值为 0.

2.当使用读标签存储区时请正确设置 0X44A,0X44B,0X44C,0X44D 寄存器。

3.返回的 0X29 命令格式：

MEDADATA FLAG 值与返回的 0X29 命令中 READ OPTION 值代表的意义如下：

Field	Value	Description
Metadata Flags：可以多个位置 1 以返回相关数据或者所有相关位都置 1 返回所有相关标签参数。	0X0000	不返回任何相关标签参数。只是返回盘存到的标签 EPC 号或读到的标签存储区数据。
	0X0001	Bit0 置位即标签在盘存时间内被盘存到的次数将会返回。
	0X0002	BIT1 置位即标签的 RSSI 信号值将会被返回。读标签存储区时该值无效。
	0X0004	BIT2 置位即标签 被盘存到时所用的天线 ID 号将会被返回。（天线逻辑号）
	0X0008	BIT3 置位即标签被盘存到时所用的频率值将会被返回
	0X0010	BIT4 置位即标签被盘存到时读写器的时间值将会被返回。目前时间值无效。
	0X0020	BIT5 置位即 RFU 预留值将会被返回。
	0X0040	BIT6 置位则目前读写器使用的标签协议值将会被返回
	0X0080	BIT7 置位即 Tag Data Length 将会被返回，目前该参数无意义，目前返回为 0X0000。
Read Option	0x00	返回的是标签 EPC 号，也即是采用单标签或多标签盘存时为该值。
	0x01	返回的是读标签存储区 EPC 区的数据。使用读标签存储区时。
	0x02	返回的是读标签存储区 TID 区的数据。使用读标签存储区时。
	0x03	返回的是读标签存储区 USER 区的数据。使用读标签存储区时。
	0x04	返回的是读标签存储区 RESERVED 区的数据（密码区）。使用读标签存储区时。

① 当采用的是单标签或多标签盘存时：

读写器到主机的回复可包括下面信息：

Field	Length	Value
SOH	1byte	0xFF
Length	1byte	取决于返回数据
OpCode	1byte	0X29
Status	2byte	命令操作状态码，0X0000 为操作成功。其他为失败。
Metadata Flags	2byte	0X401 OEM 寄存器中的 Metadata Flags 值。
Read Options	1byte	0X00
Tag Count	1byte	本次返回信息中包含的标签数。
Read Count$_1$	1byte	标签被盘存到的次数
RSSI$_1$	1byte	标签信号强度,单位 DBM，该值是有符号字符字节。
Antenna ID$_1$	1byte	盘存到标签的天线 ID，高 4 位为发射天线，低 4 位为接收天线。（天线逻辑号）
Frequency$_1$	3byte	盘存到标签时的频率，单位 KHZ
Timestamp$_1$	4byte	读写器的系统时间，单位毫秒。目前时间值无效。
RFU$_1$	2byte	预留数据
Protocol ID	1byte	标签协议（0X05 表示 GENT2）
Tag Data Length	2byte	该值为 0X0000。目前该参数无意义。
EPC Length	2byte	EPC 区内容的位长度，包括 PC 跟 CRC。
PC Word	2byte	EPC 区的 PC 值
EPC ID	N byte	标签 EPC 号
Tag CRC	2byte	标签 CRC
重复从 Read Count 到 Tag CRC 的内容为其他的标签，重复次数由 Tag Count 决定。		
CRC	2byte	命令串 CRC

例子 1：

返回盘存次数 Read Count，盘存天线 AntennaID 和被盘存到时的时间。

Metadata Flags = 0x0001 OR 0x0004 OR 0x0010 = 0x0015

读写器到主机：

FF	34	29	00 00	00 15	00	02
SOH	Length	Opcode	Status	Metadata Flags	Read Options	Tag Count

22	11	02 50 CE F6	00 80	31 C1	111122223333444455556666	FB15
Read Count	Ant ID	Timestamp	EPC length	PC word	Tag EPC ID	Tag CRC

0E	11	04 1D 3D 3C	00 80	30 00	050000000000000000002354	4AC8
Read Count	Ant ID	Timestamp	EPC length	PC word	Tag EPC ID	Tag CRC

1A B8
CRC

例子 2：

返回除 Protocol ID 标签协议之外的所有能返回的标签参数信息。

Metadata Flags = **0x00BF**

读写器到主机：

FF	4A	29	00 00	00 BF	00	02
SOH	Length	Opcode	Status	Metadata Flags	Read Options	Tag Count

07	E3	11	0E 22 2A	00 00 8D 8F	00 00	00 00
Read Count	RSSI	Ant ID	Frequency	Timestamp	RFU	Tag Data Length

00 60	**20 00**	**11 11 22 22 33 33 44 44**	**C2 41**
EPC length	PC word	Tag EPC ID	Tag CRC

07	D0	11	0E 22 2A	00 00 8D 87	00 00	00 00
Read Count	RSSI	Ant ID	Frequency	Timestamp	RFU	Tag Data Length

00 D0	58 00	11 11 22 22 33 33 44 44 55 55 66 66 77 77 88 88 99 99 00 00 AA AA	96 86
EPC length	PC word	Tag EPC ID	Tag CRC

DC 46
CRC

例子 3：

METADATA FLAG=0;

读写器到主机：

FF	**16**	**29**	**00 00**	**00 00**	**00**	**01**
SOH	**LENGTH**	**OPCODE**	**STATUS**	**METEDATA FLAG**	**READ OPTION**	**TAG COUNT**

00 80	**30 00**	00 00 00 00 00 00 00 00 00 00 00 86	FC E3	CD AE
Epc length	**PC word**	**Tag EPC ID**	**Tag CRC**	**CRC**

② 当采用的是读标签存储区时：

读写器到主机的回复可包括下面信息：

Field	Length	Value
SOH	1byte	0xFF
Length	1byte	取决于返回数据
OpCode	1byte	0X29
Status	2byte	命令操作状态码，0X0000 为操作成功。其他为失败。
Metadata Flags	2byte	0X401 OEM 寄存器中的 Metadata Flags 值。
Read Options	1byte	0X01 或 0X02 或 0X03 或 0X04，具体看设置的是读那个存储区。
READ ADDR	4byte	读取的存储区的起始字地址。
READ LEN	1byte	读取的字长度
Tag Count	1byte	该值目前为 1，即每次返回的是读到的一个标签的存储区内容。
Read Count$_1$	1byte	标签被盘存到的次数
RSSI$_1$	1byte	标签信号强度,单位 DBM，该值是有符号字符字节。目前该值无效。
Antenna ID$_1$	1byte	盘存到标签的天线 ID，高 4 位为发射天线，低 4 位为接收天线。（天线逻辑号）
Frequency$_1$	3byte	盘存到标签时的频率，单位 KHZ
Timestamp$_1$	4byte	读写器的系统时间，单位毫秒。目前时间值无效。
RFU$_1$	2byte	预留数据
Protocol ID	1byte	标签协议（0X05 表示 GENT2）
Tag Data Length	2byte	该值为 0X0000。目前该参数无意义。
PC+EPC LENGTH	1byte	标签 PC+EPC 的字节长度。
PC	2byte	标签的 PC 值
EPC	Nbyte((PC+EPC LENGTH)-2)	标签的 EPC 号
READ DATAS	N byte	读取到的存储区的数据，READ LEN *2 个字节。
CRC	2byte	命令串 CRC

例子 1.读取 TID 起始地址为 0 的 4 个字。

返回盘存次数 Read Count，盘存天线 AntennaID 和被盘存到时的时间。

Metadata Flags = 0x0001 OR 0x0004 OR 0x0010 = 0x0015；

读写器到主机：

FF	26	29	00 00	00 15	02	00 00 00 00	04
SOH	Length	Opcode	Status	Metadata Flags	Read Options	read addr	read len

01	01	11	00 00 00 00	0E	30 00	666655554444333322221111
Tag Count	Read Count	Ant ID Timestamp		pc+epc length	PC	EPC

1111222233334444	?? ??
READ DATAS	CRC

例子 2：读取 EPC 区起始地址为 2 的 6 个字。METADATA FLAG=0;

读写器到主机：

FF	24	29	00 00	00 00	01	00 00 00 02	06
SOH	Length	Opcode	Status	Metadata Flags	Read Options	read addr	read len

01	0E	30 00	6666 5555 4444 3333 2222 1111
Tag Count	pc+epc length	PC	EPC

1111 2222 3333 4444 5555 6666	?? ??
READ DATAS	CRC

（3）0X0402：低 2 个字节存放盘存时间 TIMEOUT，默认 100 毫秒；当使用读标签存储区时，推荐将该值设置为 1000 毫秒，以避免时间不够读取较长的数据。

（4）0X0403：低两个字节存放 SELECT OPTION。如果 SELECT OPTION 设置值有误则按照 0 处理。默认为 0 不采用匹配过滤；该值为是否采用匹配过滤去盘存标签，工作模式下有效位只有最低 4 位。该值为在 0X0401 寄存器中提到的使用 0X21 或 0X22 或 0X28 方式去盘存标签时是否采用匹配过滤去盘存，详情请看这几个命令对 SELECT OPTION 的介绍。如果采用匹配过滤，则应正确设置 0X404—0X040D 寄存器的值。

（5）0X0404: SELECT ADDRESS；匹配过滤位地址，默认为 0；

（6）0X0405: SELECTDATAS LENGTH；匹配数据位长度，最多 255 位；默认为 0；

（7）0X0406—0X040D：存放匹配过滤数据；高字节在前。默认为 0；

（8）0X040E—0X040F：预留用。

（9）0X0410：设置发射功率，单位 0.01DBM，范围为 500-3000；如果存储的值不为该范围，则按默认 2700.

（10）0X0411：工作频段;0X01=北美（902-928），0x06=中国 1（920-925），0X08=欧频（865-867），0X0A=中国 2（840-845）。如存储的值不为这些值，则按默认 0X01 北美处理。

（11）0X0412：预留。

（12）0X0413—0X0444：共可设 50 个频点，设置读写器工作在哪个频段即只能设置对应的频段内的频点。默认是设置北美频段内的 50 个频点。

设置读写器工作频点时，首先要先设置 0X0411 寄存器，指明是工作在哪个频段，然后把相关频段内的想要设置的工作频点写入 0X0413—0X0444 寄存器中，寄存器的最高字节存放是否使用该寄存器设置频点标志，低 3 个字节表示频点值，单位 KHZ，最高字节为 0XA5 表示使用该频点。设置的频率值应该按照每个频段所

允许设置的频率值设置，且当设置频率时，由于每个频段的可允许工作频率数量不一样，只有北美频段有 50 个频点可设置，所以对于未使用的寄存器值应清 0，且设置频率的时候应从 0X413 开始存起；

设置值与对应频率区域关系如下：

区域 region	设置值 code
北美（902-928）	0x01
中国 1（920-925）	0x06
欧频（865-867）	0x08
中国 2（840-845）	0x0a

北美跳频表：

```
NAfrelist[50]= {915750,915250,903250,926750,926250,904250,927250,920250,919250,909250,
                918750,917750,905250,904750,925250,921750,914750,906750,913750,922250,
                911250,911750,903750,908750,905750,912250,906250,917250,914250,907250,
                918250,916250,910250,910750,907750,924750,909750,919750,916750,913250,
                923750,908250,925750,912750,924250,921250,920750,922750,902750,923250};
```

中国 1 跳频表：

```
Chinafrelist1[16]={921375,922625,920875,923625,921125,920625,923125,921625,
                   922125,923875,921875,922875,924125,923375,924375,922375};
```

欧频跳频表：

```
Eu3frelist[4]={865700,866300,866900,867500};
```

中国 2 跳频表：

```
Chinafrelist2[16]={841375,842625,840875,843625,841125,840625,843125,841625,
                   842125,843875,841875,842875,844125,843375,844375,842375};
```

（13）0X0445：目前该值只有最低位有效，为 0 时，METADATA 中的 RSSI 值保存标签最后一次被盘存到时的信号强度值，上电默认为 0；为 1 时保存标签被盘存到的最大信号强度值。

（14）0X0446：盘存使用的 SESSION 设置，0=S0，1=S1，2=S2，3=S3；默认为 0=S0;

（15）0X0447：盘存使用的 TARGET 选择；高 16 位表示选择静态或动态 TARGET，高 16 位为 0=选择动态 TARGET，此时低 16 位表示从 A 到 B 还是从 B 到 A，0=从 A 到 B，1=从 B 到 A；高 16 位为 1=选择静态 TARGET，此时低 16 位=0 表示使用 TARGET A（上电默认），低 16 位=1 表示使用 TARGET B。默认为 0X00010000 选用静态 TARGET A；

（16）0X0448：蓝牙读写器盘存到标签后向上位机发送盘存数据流时每帧数据流之间的时间间隔，也即是按下读写器盘存按键读写器开始盘存后，每盘存到标签后向上发送标签数据流帧的时间间隔，默认是 10MS，即是读写器向上位机发送一帧数据流后，至少会在 10MS 后再发送下一帧。该寄存器取值范围为 0-1000；如无特别需求可不更改该寄存器。

（17）0X0449：高 16 位为 0 表示使用动态 Q 值，选择动态 Q 值则读写器根据读取标签状况自动更改 Q 值；高 16 位为 1 表示使用静态 Q 值，此时最低 4 位表示 Q 值。默认使用静态 Q 值，Q=2；

（18）0X044A：当使用读标签存储区时指定读取的标签存储区，有效位为最低 2 位：

0x00 = Reserved

0x01 = EPC

0x02= TID

0x03 = User Memory

备注：默认 0X00。

（19）0X44B：当使用读标签存储区时指定读取的起始字地址；默认为 0；

（20）0X44C：当使用读标签存储区时指定读取的字长度，最多为 64 个字，如果该值大于 64 将按 64 处理，如果该值为 0 将按 0X04 处理；默认为 0；

（21）0X44D：当使用读标签存储区时指定的访问密码，默认为 0X00000000;

（22）0x0450:主动被动模式选择寄存器，当值为 0XA5A55A5A 时为被动工作模式，也即是只接受上位机发下来的命令工作；其他值为主动工作 模式，也即是按键有效，按键按下即盘存。对该寄存器进行设置后，只有重启设备后才生效。