山东明华澳汉智能科技有限公司
Shandong Mingwah Aohan Smart Technology Co.,Ltd
地址：山东省济南市高新区新泺大街2008号银荷大厦C座9层　邮编：250101
9/F, Block C, Yinhe Building, No. 2008 Xinluo St., High-Tech District, Ji'nan, Shandong 250101, China
电话: +86-531-88118022/21/20　传真: +86-531-88118020-802　网址: www.sdmwcard.com

UHF 电子标签读写器
用户手册 v2.0

物联天下 · 感知中国

目录

一、通讯接口规格

读写器通过 RS232 或者 RS485 接口与上位机串行通讯，按上位机的命令要求完成相应操作。串行通讯接口的数据帧为一个起始位，8 个数据位，一个停止位，无奇偶校验位，缺省波特率 57600。在串行通讯过程中，每个字节的最低有效位最先传输。

二、协议描述

通讯过程由上位机发送命令及参数给读写器，然后读写器将命令执行结果状态和数据返回给上位机。读写器接收一条命令执行一条命令，只有在读写器执行完一条命令后，才能接收下一条命令。在读写器执行命令期间，如果向读写器发送命令，命令将丢失。

上位机发送过程如下：

上位机	数据传递方向	读写器
命令数据块	→	

说明：上位机发送的数据流中，每两个相邻字节之间的发送时间间隔必须小于 15ms。在上位机的命令数据流发送过程中，如果相邻字符间隔大于 15ms，则之前接收到的数据均被当作无效数据丢弃，然后从下一个字节开始，重新接收。

读写器接收到正确命令后，在不超过询查时间的范围内 (不包括数据发送过程，仅仅是读写器执行命令的时间)，会返回给读写器一个响应。

读写器发送过程如下：

读写器	数据传递方向	上位机
响应数据块	→	

说明：读写器发送响应数据期间，相邻字节之间的发送时间间隔小于 15ms

完整的一次通讯过程是：上位机发送命令给读写器，并等待读写器返回响应；读写器接收命令后，开始执行命令，然后返回响应；之后上位机接收读写器的响应。一次通讯结束。

三、数据的格式

1. 上位机命令数据块

Len	Adr	Cmd	Data[]	LSB-CRC16	MSB-CRC16

数据各部分说明如下：

	长度(字节)	说明
Len	1	命令数据块的长度，但不包括 Len 本身。即数据块的长度等于 4 加 Data[]的长度。Len 允许的最大值为 96，最小值为 4。
Adr	1	读写器地址。地址范围：0x00~0xFE，0xFF 为广播地址，读写器只响应和自身地址相同及地址为 0xFF 的命令。读写器出厂时地址为 0x00。
Cmd	1	命令代码。
Data[]	不定	参数域。在实际命令中，可以不存在。
LSB-CRC16	1	CRC16 低字节。CRC16 是从 Len 到 Data[]的 CRC16 值
MSB-CRC16	1	CRC16 高字节。

2. 读写器响应数据块

Len	Adr	reCmd	Status	Data[]	LSB-CRC16	MSB-CRC16

数据各部分说明如下：

	长度(字节)	说明
Len	1	响应数据块的长度，但不包括 Len 本身。即数据块的长度等于 5 加 Data[]的长度。
Adr	1	读写器地址。
reCmd	1	指示该响应数据块是哪个命令的应答。如果是对不可识别的命令的应答，则 reCmd 为 0x00。
Status	1	命令执行结果状态值。
Data[]	不定	数据域，可以不存在。
LSB-CRC16	1	CRC16 低字节。CRC16 是从 Len 到 Data[]的 CRC16 值。
MSB-CRC16	1	CRC16 高字节。

CRC16 的 C 语言算法：

```
#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;
}
```

pucY 是要计算 CRC16 的字符数组的入口，ucX 是字符数组中字符个数。

上位机收到数据的时候，只要把收到的数据按以上算法进行计算 CRC16，结果为 0x0000 表明数据正确。

四、操作命令总汇

1. EPC C1 G2（ISO18000-6C）命令

序号	命令	功能
1	0x01	询查标签
2	0x02	读数据

3	0x03	写数据
4	0x04	写 EPC 号
5	0x05	销毁标签
6	0x06	设定存储区读写保护状态
7	0x07	块擦除
8	0x08	根据 EPC 号设定读保护设置
9	0x09	不需要 EPC 号读保护设定
10	0x0a	解锁读保护
11	0x0b	测试标签是否被设置读保护
12	0x0c	EAS 报警设置
13	0x0d	EAS 报警探测
14	0x0e	user 区块锁
15	0x0f	询查单标签
16	0x10	块写

2. 18000-6B 命令

序号	命令	功能
1	0x50	询查命令(单张)。这个命令每次只能询查一张电子标签。不带条件询查。
2	0x51	条件询查命令(多张)。这个命令根据给定的条件进行询查标签，返回符合条件的电子标签的 UID。可以同时询查多张电子标签。
3	0x52	读数据命令。这个命令读取电子标签的数据，一次最多可以读 32 个字节。
4	0x53	写数据命令。写入数据到电子标签中，一次最多可以写 32 个字节。
5	0x54	检测锁定命令。检测某个存储单元是否已经被锁定。
6	0x55	锁定命令。锁定某个尚未被锁定的电子标签。

3. 读写器自定义命令

序号	命令	功能
1	0x21	读取读写器信息
2	0x22	设置读写器工作频率
3	0x24	设置读写器地址
4	0x25	设置读写器询查时间
5	0x28	设置读写器的波特率
6	0x2F	调整读写器输出功率
7	0x33	声光控制命令
8	0x34	韦根参数设置命令
9	0x35	工作模式设置命令

10	0x36	读取工作模式参数命令
11	0x37	EAS 测试精度设置命令
12	0x38	设置 Syris485 响应偏执时间
13	0x3b	设置触发有效时间

五、命令执行结果状态值

响应数据块						Status 含义	说明
Len	Adr	reCmd	Status	Data[]	CRC16		
5+Data[]部分的长度	0xXX	0xXX	0x00	……..	LSB+MSB	操作成功	当成功执行命令后返回给上位机的状态值。Data[]包含了所要信息
5+Data[]部分的长度	0xXX	0x01	0x01	……..	LSB+MSB	询查时间结束前返回	上位机发出询查 G2 标签命令时，读写器询查电子标签时，如果在设定的询查时间内返回信息给上位机，则返回此状态值
5+Data[]部分的长度	0xXX	0x01	0x02	……..	LSB+MSB	指定的询查时间溢出	上位机发出询查 G2 标签命令时，当询查时间溢出时，读写器还没有完成询查操作时返回给上位机的状态值
5+Data[]部分的长度	0xXX	0x01	0x03	……..	LSB+MSB	本条消息之后，还有消息	上位机发出询查 G2 标签命令时，如果询查命令读到的标签数量无法在一条消息内传送完，将分多次发送。
5+Data[]部分的长度	0xXX	0x01	0x04	……..	LSB+MSB	读写器存储空间已满	上位机发出询查 G2 标签命令时，如果询查到的电子标签太多，超过了读写器的存储容量，则读写器返回读到的电子标签 EPC 号，同时，也将返回此状态值

5	0xXX	0xXX	0x05	无此项	LSB+MSB	访问密码错误	当读写器执行需要密码才能执行的操作，而命令中给出的密码是错误的密码时返回给上位机的状态值
5	0xXX	0x05	0x09	无此项	LSB+MSB	销毁标签失败	当向 G2 标签进行销毁操作时，如果销毁密码错误，或是读写器与标签通讯不畅，则将返回此状态值
5	0xXX	0x05	0x0a	无此项	LSB+MSB	销毁密码不能为全 0	销毁标签时，销毁密码为 0 的标签是无法销毁的
5	0xXX	0xXX	0x0b	无此项	LSB+MSB	电子标签不支持该命令	G2 协议中的某些**可选命令**，及一些厂商的特定命令，可能某些标签不支持这些命令，此时返回此状态值
5	0xXX	0xXX	0x0c	无此项	LSB+MSB	对该命令访问密码不能为全 0	对 **NXP UCODE EPC G2X** 标签设置读保护及设置 EAS 报警时，访问密码不能为全 0，若为全 0，将返回此状态值
5	0xXX	0x0a	0x0d	无此项	LSB+MSB	电子标签已经被设置了读保护，不能再次设置	对已经被设置了读保护的 **NXP UCODE EPC G2X** 标签，在解除读保护之前，不能再次设置。此情况下返回这个状态值
5	0xXX	0x0a	0x0e	无此项	LSB+MSB	电子标签没有被设置读保护，不需要解锁	对 **NXP UCODE EPC G2X** 标签解锁，如果标签没有被锁定，将返回此状态值，对不支持读保护设定命令的标签发送此命令，也将返回此状态值

5	0xXX	0x53	0x10	无此项	LSB+MSB	有字节空间被锁定，写入失败	在向 6B 标签写入数据时，因为有字节空间被锁定，使得写入数据失败时，返回此状态值
5	0xXX	0x55	0x11	无此项	LSB+MSB	不能锁定	当 6B 标签出现不能被锁定的情况，返回此状态值
5	0xXX	0x55	0x12	无此项	LSB+MSB	已经锁定，不能再次锁定	对已经锁定的 6B 标签进行再次锁定时，返回此状态值
5	0xXX	0xXX	0x13	无此项	LSB+MSB	参数保存失败，但设置的值在读写器断电前有效	对于某些需要保存的参数，如果保存失败，则返回此状态值
5	0xXX	0xXX	0x14	无此项	LSB+MSB	无法调整	调整功率的时候，在某些情况下，如果出现功率无法调整的错误，则返回此状态值
5+Data[]的长度	0xXX	0x51	0X15	……..	LSB+MSB	询查时间结束前返回	上位机发出询查 6B 标签命令时，读写器询查电子标签时，如果在设定的询查时间内返回信息给上位机，则返回此状态值
5+Data[]的长度	0xXX	0x51	0x16	……..	LSB+MSB	指定的询查时间溢出	上位机发出询查 6B 标签命令时，当询查时间溢出时，读写器还没有完成询查操作时返回给上位机的状态值
5+Data[]的长度	0xXX	0x51	0x17	……..	LSB+MSB	本条消息之后，还有消息	上位机发出询查 6B 标签命令时，如果询查命令读到的标签数量无法在一条消息内传送完，将分多次发送。

5+Data[]的长度	0xXX	0x51	0x18	……..	LSB+MSB	读写器存储空间已满	上位机发出询查 6B 标签命令时，如果询查到的电子标签太多，超过了读写器的存储容量，则读写器返回读到的电子标签 UID 号，同时，也将返回此状态值
5	0xXX	0xXX	0x19	无此项	LSB+MSB	电子标签不支持该命令或者访问密码不能为 0	当设置电子标签的 EAS 报警时，在通信正常的情况下，如果标签无法设置，则可能是电子标签不支持该命令，也可能是电子标签的访问密码不能为 0
5	0xXX	0xXX	0xF9	无此项	LSB+MSB	命令执行出错	命令执行出错
5	0xXX	0xXX	0xFA	无此项	LSB+MSB	有电子标签，但通信不畅，操作失败	当检测到有效范围内存在可操作的电子标签，但读写器与电子标签之间的通讯质量不好，而无法完成整个通讯过程时返回给上位机的信息
5	0xXX	0xXX	0xFB	无此项	LSB+MSB	无电子标签可操作	当读写器对电子标签进行操作时，有效范围内没有可操作的电子标签时返回给上位机的状态值
6	0xXX	0xXX	0xFC	Err_code	LSB+MSB	电子标签返回错误代码	电子标签返回错误代码时，错误代码由 Err_code 返回给上位机
5	0xXX	0xXX	0xFD	无此项	LSB+MSB	命令长度错误	当上位机输入的命令的实际长度和它应当具有的长度不同时，返回该状态

5	0xXX	0x00	0xFE	无此项	LSB+MSB	不合法的命令	当上位机输入的命令是不可识别的命令，如不存在的命令、或是 CRC 错误的命令
5	0xXX	0xXX	0xFF	无此项	LSB+MSB	参数错误	上位机发送的命令中的参数不符合要求时，返回此状态

六、电子标签返回错误代码

EPC C1G2（ISO18000 -6C）电子标签错误代码：

错误代码支持	错误代码	错误代码名称	错误描述
特定错误代码	0x00	其它错误	全部捕捉未被其它代码覆盖的错误
	0x03	存储器超限或不被支持的 PC 值	存储位置不存在或标签不支持的 PC 值
	0x04	存储器锁定	存储位置锁定或永久锁定，且不可写入
	0x0b	电源不足	标签电源不足，无法执行存储写入操作
非特定错误代码	0x0f	非特定错误	标签不支持特定错误代码

七、标签存储区及需要注意的问题

A. EPC C1G2 标签（简称 G2 标签）

G2 标签分 4 个区：保留区（又称密码区），EPC 区，TID 区和 User 区。
保留区：保留区 4 个字。前两个字是销毁密码，后两个字是访问密码。可读可写，保留区的两个密码区的读写保护特性可以分别设置。
EPC 区：标签 EPC 号存储在该区，其中第 **0** 个字是 PC 值和标签 EPC 号的 CRC16。第 **1** 个字是 PC 值，该值指示标签 EPC 号长度，从第 **2** 个字开始才是标签的 EPC 号数据。可读可写。
TIC 区：该区存储的数据是由标签生产商设定的 ID 号。可读不可写。
User 区：是用户数据区。可读可写。

G2 命令中很多地方要求给出数据长度，这里要注意字与字节的区别。1 个字等于 2 个字节。
有些命令需要访问密码，如果没有密码设置，则用 0 填充密码区，而不能为空。

B．18000-6B 标签

6B 标签只有一个存储空间，最低 8 个字节是标签的 UID，并且不能被改写。后面的字节都是可改写的，也可以被锁定，但是一旦锁定后，则不能再次改写，也不能解锁。

八、操作命令详细描述

8.1 命令概述

操作命令有三大类，一类是协议相关的；另一类是读写器相关的；还有一类是标签自定义命令。

如果上位机输入的命令是不可识别的命令，如不存在的命令、或是 CRC 错误的命令，则返回值如下：

Len	Adr	reCmd	Status	CRC-16	
0x05	0xXX	0x00	0xFE	LSB	MSB

如果命令的长度不对，则返回信息如下：

Len	Adr	reCmd	Status	CRC-16	
0x05	0xXX	0xXX	0xFD	LSB	MSB

有两种命令读写器不会响应：

1. 如果输入的命令的地址出错(地址不是 0xFF，也不是读写器地址)，读写器不会有任何响应。

2. 如果输入的命令是不完整的，即命令的 Len 域指示的命令长度大于实际的命令长度，则读写器将不会做出任何响应。

8.2 EPC C1G2 命令

8.2.1 询查标签

询查命令的作用是检查有效范围内是否有符合协议的电子标签存在。想要对未知 EPC 的新标签进行别的操作，应先通过询查命令来得到标签的 EPC 号。

在运行询查命令之前，用户可以根据需要先设定好该命令的最大运行时间(询查时间)。读写器在询查时间规定的范围内必须给上位机一个结果，如果读写器尚未读完有效范围内的所有标签，而询查时间已到，则读写器不再询查其它标签，而是直接把已经询查到得标签返回给上位机，并提示上位机还有标签未读完。然后等待下一个命令。

询查时间的缺省值是 1s，用户可以通过运行读写器自定义命令设定询查时间命令来修改。允许的范围是：3*100ms~255*100ms(实际的响应时间可能会比设定的值大 0~75ms)。

询查时间如果设定的过短，可能会出现在规定时间内询查不到电子标签的情况。

命令：

Len	Adr	Cmd	Data[]		CRC-16	
			AdrTID	LenTID		
0xXX	0xXX	0x01	0xXX	0xXX	LSB	MSB

参数解析：

AdrTID：询查 TID 区的起始字地址。

LenTID：询查 TID 区的数据字数。LenTID 取值为 0~15，若为其它参数将返回参数错误信息。

注：当 AdrTID、LenTID 为空时表示询查标签 EPC，否则询查 TID。TID 询查功能仅当读写器固件 V2.36 及以上版本有效。

应答：

Len	Adr	reCmd	Status	Data[]		CRC-16	
				Num	EPC ID		
0xXX	0xXX	0x01	0xXX	0xXX	EPC-1,EPC-2,EPC-3…	LSB	MSB

参数解析：

Status 是应答的状态，其代表的意义如下表所述：

Status	说明
0x01	命令执行结束，同时返回询查到的电子标签数据
0x02	询查时间结束，命令执行强制退出，同时返回已询查到的标签数据
0x03	如果读到的标签数量无法在一条消息内传送完，将分多次发送。如果 Status 为 0x03，则表示这条数据结束后，还有数据。
0x04	还有电子标签未读取，电子标签数量太多，读写器的存储区已满，返回此状态值，同时返回已询查到得电子标签数据。

Num：本条命令中包含的电子标签的 **EPC/TID** 的个数。

EPC ID：读到的电子标签的 **EPC/TID** 数据，EPC-1 是第一张标签的 **EPC/TID** 长度+第一张标签的 EPC 号或 TID 数据，依此类推。每个电子标签 EPC 号或 TID 数据高字(EPC C1 G2 中数据以字为单位)在前，每一个字的高字节在前。**EPC/TID** 长度以一个字节表示。

8.2.2 读数据

这个命令读取标签的保留区、EPC 存储区、TID 存储区或用户存储区中的数据。从指定的地址开始读，以字为单位。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x02	——	LSB	MSB

Data 参数如下：

Data[]							
ENum	EPC	Mem	WordPtr	Num	Pwd	MaskAdr	MaskLen
0xXX	变长	0xXX	0xXX	0xXX	4Byte	0xXX	0xXX

参数解析：

ENum：EPC 号长度，以字为单位。EPC 的长度在 15 个字以内，不能为 0。超出范围，将返回参数错误信息。

EPC：要读取数据的标签的 EPC 号。长度根据所给的 EPC 号决定，EPC 号以字为单位，且必须是整数个长度。高字在前，每个字的高字节在前。这里要求给出的是完整的 EPC 号。

Mem：一个字节。选择要读取的存储区。0x00：保留区；0x01：EPC 存储区；0x02：TID 存储区；0x03：用户存储区。其他值保留。若命令中出现了其它值，将返回参数出错的消息。

WordPtr：一个字节。指定要读取的字起始地址。0x00 表示从第一个字(第一个 16 位存储区)开始读，0x01 表示从第 2 个字开始读，依次类推。

Num：一个字节。要读取的字的个数。不能设置为 0x00，否则将返回参数错误信息。Num 不能超过 120，即最多读取 120 个字。若 Num 设置为 0 或者超过了 120，将返回参数出错的消息。

Pwd：四个字节，这四个字节是访问密码。32 位的访问密码的最高位在 Pwd 的第一字节(从左往右)的最高位，访问密码最低位在 Pwd 第四字节的最低位，Pwd 的前两个字节放置访问密码的高字。只有当读保留区，并且相应存储区设置为密码锁、且标签的访问密码为非 0 的时候，才需要使用正确的访问密码。在其他情况下，Pwd 为零或正确的访问密码。

MaskAdr：一个字节，掩模 EPC 号的起始字节地址。0x00 表示从 EPC 号的最高字节开始掩模，0x01 表示从 EPC 号的第二字节开始掩模，以此类推。

MaskLen：一个字节，掩模的字节数。掩模起始字节地址+掩模字节数不能大于 EPC 号字节长度，否则返回参数错误信息。

注：当 MaskAdr、MaskLen 为空时表示以完整的 EPC 号掩模。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0xXX	0xXX	0x02	0x00	Word1，Word2,…	LSB	MSB

参数解析：

Word1, Word2….： 以字为单位。每个字都是 2 个字节，高字节在前。Word1 是从起始地址读到的字，Word2 是起始地址后一个字地址上读到的字，以此类推。

8.2.3 写数据

这个命令可以一次性往保留区、TID 存储区或用户存储区中写入若干个字。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x03	——	LSB	MSB

Data 参数如下：

Data[]								
WNum	ENum	EPC	Mem	WordPtr	Wdt	Pwd	MaskAdr	MaskLen
0xXX	0xXX	变长	0xXX	0xXX	变长	4Byte	0xXX	0xXX

参数解析：

WNum：待写入的字个数，一个字为 2 个字节。这里字的个数必须和实际待写入的数据个数相等。WNum 必须大于 0，若上位机给出的 WNum 为 0 或者 WNum 和实际字个数不相等，将返回参数错误的消息。

ENum：EPC 号长度。以字为单位。EPC 的长度在 15 个字以内，可以为 0。否则返回参数错误信息。

EPC：要写入数据的标签的 EPC 号。长度由所给的 EPC 号决定，EPC 号以字为单位，且必须是整数个长度。高字在前，每个字的高字节在前。这里要求给出的是完整的 EPC 号。

Mem：一个字节，选择要写入的存储区。0x00：保留区；0x01：EPC 存储区；0x02：TID 存储区；0x03：用户存储区。其他值保留。若命令中出现了其它值，将返回参数出错的消息。

WordPtr：一个字节，指定要写入数据的起始地址。

Wdt：待写入的字，字的个数必须与 WNum 指定的一致。这是要写入到存储区的数据。每个字的高字节在前。如果给出的数据不是整数个字长度，Data[]中前面的字写在标签的低地址中，后面的字写在标签的高地址中。比如，WordPtr 等于 0x02，则 Data[]中第一个字(从左边起)写在 Mem 指定的存储区的地址 0x02 中，第二个字写在 0x03 中，依次类推。

Pwd：4 个字节的访问密码。32 位的访问密码的最高位在 Pwd 的第一字节(从左往右)的最高位，访问密码最低位在 Pwd 第四字节的最低位，Pwd 的前两个字节放置访问密码的高字。在写操作时，应给出正确的访问密码，当相应存储区未设置成密码锁时 Pwd 可以为零。

MaskAdr：一个字节，掩模 EPC 号的起始字节地址。0x00 表示从 EPC 号的最高字节开始掩模，0x01 表示从 EPC 号的第二字节开始掩模，以此类推。

MaskLen：一个字节，掩模的字节数。掩模起始字节地址+掩模字节数不能大于 EPC 号字节长度，否则返回参数错误信息。

注：当 MaskAdr、MaskLen 为空时表示以完整的 EPC 号掩模。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x03	0x00	——	LSB	MSB

8.2.4 写 EPC 号

这个命令向电子标签写入 EPC 号。写入的时候，天线有效范围内只能有一张电子标签。

命令：

Len	Adr	Cmd	Data[]			CRC-16	
			ENum	Pwd	WEPC		
0xXX	0xXX	0x04	0xXX	4Byte	变长	LSB	MSB

参数解析：

ENum：1 个字节。要写入的 EPC 的长度，以字为单位。不能为 0，也不能超过 15，否则返回参数错误信息。

Pwd：4 个字节的访问密码。32 位的访问密码的最高位在 Pwd 的第一字节(从左往右)的最高位，访问密码最低位在 Pwd 第四字节的最低位，Pwd 的前两个字节放置访问密码的高字。在本命令中，当 EPC 区设置为密码锁、且标签访问密码为非 0 的时候，才需要使用访问密码。在其他情况下，Pwd 为零或正确的访问密码。

WEPC：要写入的 EPC 号，长度必须和 ENum 说明的一样。WEPC 最小 1 个字，最多 15 个字，否则返回参数错误信息。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x04	0x00	——	LSB	MSB

8.2.5 销毁标签

这个命令用来销毁标签。标签销毁后，永远不会再处理读写器的命令。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x05	——	LSB	MSB

Data 参数如下：

Data[]				
ENum	EPC	Killpwd	MaskAdr	MaskLen
0xXX	变长	4Byte	0xXX	0xXX

参数解析：

ENum：EPC 号长度，以字为单位。EPC 的长度在 15 个字以内，不能为 0，否则返回参数错误信息。

EPC：要写入数据的标签的 EPC 号。长度根据所给的 EPC 号决定，EPC 号以字为单位，且必须是整数个长度。高字在前，每个字的高字节在前。这里要求给出的是完整的 EPC 号。

Killpwd：4 个字节的销毁密码。32 位的销毁密码的最高位在 Killpwd 的第一字节(从左往右)的最高位，销毁密码最低位在 Killpwd 第四字节的最低位，Killpwd 的前两个字节放置销毁密码的高字。要销毁标签，则销毁密码必须为非 0，因为密码为 0 的标签是无法销毁的。如果命令中的销毁密码为 0，则返回参数错误的应答。

MaskAdr：一个字节，掩模 EPC 号的起始字节地址。0x00 表示从 EPC 号的最高字节开始掩模，0x01 表示从 EPC 号的第二字节开始掩模，以此类推。

MaskLen：一个字节，掩模的字节数。掩模起始字节地址+掩模字节数不能大于 EPC 号字节长度，否则返回参数错误信息。

注：当 MaskAdr、MaskLen 为空时表示以完整的 EPC 号掩模。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x05	0x00	——	LSB	MSB

8.2.6 设定存储区读写保护状态

这个命令可以设定保留区为无保护下的可读可写、永远可读可写、带密码可读可写、永远不可读不可写；可以分别设定 EPC 存储区、用户存储区为无保护下的可写、永远可写、带

密码可写、永远不可写；TID 存储区是只读的，永远都不可写。EPC 存储区、TID 存储区和用户存储区是永远可读的。

标签的保留区一旦设置为永远可读写或永远不可读写，则以后不能再更改其读写保护设定。标签的 EPC 存储区、TID 存储区或用户存储区若是设置为永远可写或永远不可写，则以后不能再更改其读写保护设定。如果强行发命令欲改变以上几种状态，则电子标签将返回错误代码。

在把某个存储区设置为带密码可读写、带密码可写或把带密码锁状态设置为其它非密码锁状态时，必须给出访问密码，所以，在进行此操作前，必须确保电子标签已设置了访问密码。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x06	——	LSB	MSB

Data 参数如下：

Data[]						
ENum	EPC	Select	SetProtect	Pwd	MaskAdr	MaskLen
0xXX	变长	0xXX	0xXX	4Byte	0xXX	0xXX

参数说明：

ENum：EPC 号长度，以字为单位。EPC 的长度在 15 个字以内，不能为 0，否则返回参数错误信息。

EPC：要写入数据的标签的 EPC 号。长度由所给的 EPC 号决定，EPC 号以字为单位，且必须是整数个长度。高字在前，每个字的高字节在前。这里要求给出的是完整的 EPC 号。

Select：一个字节。定义如下：

Select 为 0x00 时，控制 Kill 密码读写保护设定。
Select 为 0x01 时，控制访问密码读写保护设定。
Select 为 0x02 时，控制 EPC 存储区读写保护设定。
Select 为 0x03 时，控制 TID 存储区读写保护设定。
Select 为 0x04 时，控制用户存储区读写保护设定。

其它值保留，若读写器接收到了其他值，将返回参数出错的消息，并且不执行命令。

SetProtect：SetProtect 的值根据 Select 的值而确定。

当 Select 为 0x00 或 0x01，即当设置 Kill 密码区或访问密码区的时候，SetProtect 的值代表的意义如下：

0x00：设置为无保护下的可读可写
0x01：设置为永远可读可写

0x02：设置为带密码可读可写
0x03：设置为永远不可读不可写

当 Select 为 0x02、0x03、0x04 的时候，即当设置 EPC 区、TID 区及用户区的时候，SetProtect 的值代表的意义如下：

0x00：设置为无保护下的可写
0x01：设置为永远可写
0x02：设置为带密码可写
0x03：设置为永远不可写

当 Select 与 SetProtect 出现了其他值的时候，将返回参数出错的消息，并且不执行命令。

Pwd：4 个字节的访问密码。32 位的访问密码的最高位在 Pwd 的第一字节(从左往右)的最高位，访问密码最低位在 Pwd 第四字节的最低位，Pwd 的前两个字节放置访问密码的高字。必须给出正确的访问密码。

MaskAdr：一个字节，掩模 EPC 号的起始字节地址。0x00 表示从 EPC 号的最高字节开始掩模，0x01 表示从 EPC 号的第二字节开始掩模，以此类推。

MaskLen：一个字节，掩模的字节数。掩模起始字节地址+掩模字节数不能大于 EPC 号字节长度，否则返回参数错误信息。

注：当 MaskAdr、MaskLen 为空时表示以完整的 EPC 号掩模。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x06	0x00	——	LSB	MSB

8.2.7 块擦除

此命令可以擦除标签的保留区、EPC 存储区、TID 存储区或用户存储区的若干字。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x07	——	LSB	MSB

Data 参数如下：

Data[]							
ENum	EPC	Mem	WordPtr	Num	Pwd	MaskAdr	MaskLen

0xXX	变长	0xXX	0xXX	0xXX	4Byte	0xXX	0xXX

参数解析：

ENum：EPC 号长度。以字为单位。EPC 的长度在 15 个字以内，不能为 0，否则返回参数错误信息。

EPC：要写入数据的标签的 EPC 号。长度根据所给的 EPC 号决定，EPC 号以字为单位，且必须是整数个长度。高字在前，每个字的高字节在前。这里要求给出的是完整的 EPC 号。

Mem：1 个字节，选择要读取的存储区。0x00：保留区；0x01：EPC 区；0x02：TID 存储区；0x03：用户存储区。其他值保留，若命令中出现了其它值，则返回参数错误信息。

WordPtr：1 个字节，指定要擦除的字起始地址。0x00 表示从第一个字(第一个 16 位存储体)开始擦除，0x01 表示从第 2 个字开始擦除，依次类推。当擦除 EPC 区时，WordPtr 必须大于等于 0x01，若小于 0x01，则返回参数错误消息。

Num：1 个字节，指定要擦除的字的个数。从 WordPtr 指定的地址开始擦除，擦除 Num 指定个数的字。若 Num 为 0x00，则返回参数错误信息。

Pwd：4 个字节的访问密码。32 位的访问密码的最高位在 Pwd 的第一字节(从左往右)的最高位，访问密码最低位在 Pwd 第四字节的最低位，Pwd 的前两个字节放置访问密码的高字。当进行擦除操作时，并且相应存储区设置为密码锁的时候，才必须使用正确的访问密码。其它情况下，Pwd 为零或正确的访问密码。

MaskAdr：一个字节，掩模 EPC 号的起始字节地址。0x00 表示从 EPC 号的最高字节开始掩模，0x01 表示从 EPC 号的第二字节开始掩模，以此类推。

MaskLen：一个字节，掩模的字节数。掩模起始字节地址+掩模字节数不能大于 EPC 号字节长度，否则返回参数错误信息。

注：当 MaskAdr、MaskLen 为空时表示以完整的 EPC 号掩模。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x07	0x00	——	LSB	MSB

8.2.8 读保护设置(根据 EPC 号设定)

这个命令根据电子标签的 EPC 号，对标签设置读保护，使得电子标签不能被任何命令读写，对标签进行询查操作，也无法得到电子标签的 EPC 号。仅对 **NXP UCODE EPC G2X** 标签有效。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x08	——	LSB	MSB

Data 参数如下：

Data[]				
ENum	EPC	Pwd	MaskAdr	MaskLen
0xXX	变长	4Byte	0xXX	0xXX

参数解析：

ENum：EPC 号长度。以字为单位。EPC 的长度在 15 个字以内，不能为 0，否则返回参数错误信息。

EPC：要写入数据的标签的 EPC 号。长度由所给的 EPC 号决定，EPC 号以字为单位，且必须是整数个长度。高字在前，每个字的高字节在前。这里要求给出的是完整的 EPC 号。

Pwd：4 个字节的访问密码。32 位的访问密码的最高位在 Pwd 的第一字节(从左往右)的最高位，访问密码最低位在 Pwd 第四字节的最低位，Pwd 的前两个字节放置访问密码的高字。待设定读保护的电子标签访问密码必须不为 0，访问密码为 0 的电子标签是无法设置读保护的，在命令中，必须给出正确的访问密码。

MaskAdr：一个字节，掩模 EPC 号的起始字节地址。0x00 表示从 EPC 号的最高字节开始掩模，0x01 表示从 EPC 号的第二字节开始掩模，以此类推。

MaskLen：一个字节，掩模的字节数。掩模起始字节地址+掩模字节数不能大于 EPC 号字节长度，否则返回参数错误信息。

注：当 MaskAdr、MaskLen 为空时表示以完整的 EPC 号掩模。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x08	0x00	——	LSB	MSB

8.2.9 读保护设定(不需要 EPC 号)

这个命令可以为有效范围内的电子标签设定读保护。这个命令与前面一个命令的区别是，当有效范围内存在多张标签的时候，无法知道这个命令操作的是哪一张电子标签。如果要同时对多张标签进行操作，则标签的访问密码最好是相同的。仅对 **NXP UCODE EPC G2X** 标签有效。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
			Pwd		
0x08	0xXX	0x09	4Byte	LSB	MSB

参数解析：

Pwd：4 个字节的访问密码。32 位的访问密码的最高位在 Pwd 的第一字节(从左往右)的最高位，访问密码最低位在 Pwd 第四字节的最低位，Pwd 的前两个字节放置访问密码的高字。待设定读保护的电子标签访问密码必须不为 0，访问密码为 0 的电子标签是无法设置读保护的，在命令中，必须给出正确的访问密码。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x09	0x00	——	LSB	MSB

8.2.10 解锁读保护

这个命令用来给设置了读保护的标签解锁。用这个命令时，天线有效范围内只能放置一张要被解锁的电子标签。仅对 **NXP UCODE EPC G2X** 标签有效。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
			Pwd		
0x08	0xXX	0x0a	4Byte	LSB	MSB

参数解析：

Pwd：4 个字节的访问密码。32 位的访问密码的最高位在 Pwd 的第一字节(从左往右)的最高位，访问密码最低位在 Pwd 第四字节的最低位，Pwd 的前两个字节放置访问密码的高字。命令中必须给出正确的访问密码。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x0a	0x00	——	LSB	MSB

说明：对于不支持读保护设定的标签，认为没有被锁定。

8.2.11 测试标签是否被设置读保护

这个命令不能测试标签是否支持读保护锁定命令，只能测试标签是否被读保护锁定。对于不支持读保护锁定的电子标签，一致认为没有被锁定。

这个命令只能对单张电子标签进行操作，确保天线有效范围内只存在一张电子标签。仅对 NXP 的 UCODE EPC G2X 标签有效。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0x04	0xXX	0x0b	——	LSB	MSB

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x06	0xXX	0x0b	0x00	ReadPro	LSB	MSB

参数解析：

ReadPro	说明
0x00	电子标签没有被设置为读保护。
0x01	电子标签被设置读保护。

说明：对于不支持读保护设定的标签，认为没有被设置读保护。

8.2.12 EAS 报警设置

对电子标签的 EAS 状态位进行设置或复位。仅对 NXP UCODE EPC G2 标签有效。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x0c	——	LSB	MSB

Data 参数如下：

Data[]					
ENum	EPC	Pwd	EAS	MaskAdr	MaskLen
0xXX	变长	4Byte	0xXX	0xXX	0xXX

参数解析：

ENum：EPC 号长度。以字为单位。EPC 的长度在 15 个字以内，不能为 0，否则返回参数错误信息。

EPC：要写入数据的标签的 EPC 号。长度由所给的 EPC 号决定，EPC 号以字为单位，且必须是整数个长度。高字在前，每个字的高字节在前。这里要求给出的是完整的 EPC 号。

Pwd：4 个字节的访问密码。32 位的访问密码的最高位在 Pwd 的第一字节(从左往右)的最高位，访问密码最低位在 Pwd 第四字节的最低位，Pwd 的前两个字节放置访问密码的高字。待设置的标签的访问密码必须不为 0，访问密码为 0 的电子标签是无法设置 EAS 报警的。Pwd 必须是正确的访问密码。

EAS：1 个字节。Bit0 位为 0，表示设置为关闭 EAS 报警；为 1，表示设置为打开 EAS 报警。Bit1 – Bit7 位保留，默认为 0。

MaskAdr：一个字节，掩模 EPC 号的起始字节地址。0x00 表示从 EPC 号的最高字节开始掩模，0x01 表示从 EPC 号的第二字节开始掩模，以此类推。

MaskLen：一个字节，掩模的字节数。掩模起始字节地址+掩模字节数不能大于 EPC 号字节长度，否则返回参数错误信息。

注：当 MaskAdr、MaskLen 为空时表示以完整的 EPC 号掩模。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0xXX	0xXX	0x0c	0x00	——	LSB	MSB

8.2.13 EAS 报警检测

该命令检测电子标签的 EAS 报警。仅对 NXP UCODE EPC G2 标签有效。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0x04	0xXX	0x0d	——	LSB	MSB

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x0d	0x00	——	LSB	MSB

无 EAS 报警的时候，返回“无电子标签可操作”消息。

8.2.14 user 区块锁

这个命令每次永久锁定 user 区中的 32bits 数据，锁定后，这 32bits 数据只能读，不能被再次写，也不能被擦除。这个命令仅对 NXP UCODE EPC G2 电子标签有效。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x0e	——	LSB	MSB

Data 参数如下：

Data[]

ENum	EPC	pwd	WrdPointer	MaskAdr	MaskLen
0xXX	变长	4Byte	0xXX	0xXX	0xXX

参数解析：

ENum：EPC 号长度。以字为单位。EPC 的长度在 15 个字以内，不能为 0，否则返回参数错误信息。

EPC：要写入数据的标签的 EPC 号。长度由所给的 EPC 号决定，EPC 号以字为单位，且必须是整数个长度。高字在前，每个字的高字节在前。这里要求给出的是完整的 EPC 号。

Pwd：4 个字节的访问密码。32 位的访问密码的最高位在 Pwd 的第一字节(从左往右)的最高位，访问密码最低位在 Pwd 第四字节的最低位，Pwd 的前两个字节放置访问密码的高字。User 区块锁操作时必须给出正确的访问密码。

WrdPointer：要锁定的字地址。由于一次会锁定 2 个字，这里列出 WrdPointer 和实际被锁定的地址的关系：

WrdPointer	被保护的数据块(字地址)
0 或 1	0 和 1
2 或 3	2 和 3
4 或 5	4 和 5
6 或 7	6 和 7
8 或 9	8 和 9
10 或 11	10 和 11
12 或 13	12 和 13

MaskAdr：一个字节，掩模 EPC 号的起始字节地址。0x00 表示从 EPC 号的最高字节开始掩模，0x01 表示从 EPC 号的第二字节开始掩模，以此类推。

MaskLen：一个字节，掩模的字节数。掩模起始字节地址+掩模字节数不能大于 EPC 号字节长度，否则返回参数错误信息。

注：当 MaskAdr、MaskLen 为空时表示以完整的 EPC 号掩模。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x0e	0x00	——	LSB	MSB

8.2.15 询查单张标签

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0x04	0xXX	0x0f	——	LSB	MSB

应答：

Len	Adr	reCmd	Status	Data[]		CRC-16	
				Num	EPC ID		
0xXX	0xXX	0x0f	0x01	0x01	EPC-1	LSB	MSB

Num：本条命令中包含的电子标签的 EPC 的个数。

EPC ID：读到的电子标签的 EPC 数据，EPC-1 是第一张标签的 **EPC 长度**+第一张标签的 EPC 号。电子标签 EPC 号高字(EPC C1 G2 中数据以字为单位)在前，每一个字的高字节在前。**EPC 长度**以一个字节表示。

8.2.16 块写命令

该命令一次能将多个字写入标签的保留区、EPC 区、TID 区或用户区。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0xXX	0xXX	0x10	——	LSB	MSB

Data 参数如下：

Data[]								
WNum	ENum	EPC	Mem	WordPtr	Wdt	Pwd	MaskAdr	MaskLen
0xXX	0xXX	变长	0xXX	0xXX	变长	4Byte	0xXX	0xXX

参数解析：

WNum：待写入的字个数，一个字为 2 个字节。这里字的个数必须和实际待写入的数据个数相等。WNum 必须大于 0，若上位机给出的 WNum 为 0 或者 WNum 和实际字个数不相等，将返回参数错误的消息。

ENum：EPC 号长度。以字为单位。EPC 的长度在 15 个字以内，可以为 0。否则返回参数错误信息。

EPC：要写入数据的标签的 EPC 号。长度由所给的 EPC 号决定，EPC 号以字为单位，且必须是整数个长度。高字在前，每个字的高字节在前。这里要求给出的是完整的 EPC 号。

Mem：一个字节，选择要写入的存储区。0x00：保留区；0x01：EPC 存储区；0x02：TID 存储区；0x03：用户存储区。其他值保留。若命令中出现了其它值，将返回参数出错的消息。

WordPtr：一个字节，指定要写入数据的起始地址。

Wdt：待写入的字，字的个数必须与 WNum 指定的一致。这是要写入到存储区的数据。每个字的高字节在前。如果给出的数据不是整数个字长度，Data[]中前面的字写在标签的低地址中，后面的字写在标签的高地址中。比如，WordPtr 等于 0x02，则 Data[]中第一个字(从左边起)写在 Mem 指定的存储区的地址 0x02 中，第二个字写在 0x03 中，依次类推。

Pwd：4 个字节的访问密码。32 位的访问密码的最高位在 Pwd 的第一字节(从左往右)的最高位，访问密码最低位在 Pwd 第四字节的最低位，Pwd 的前两个字节放置访问密码的高字。在写操作时，应给出正确的访问密码，当相应存储区未设置成密码锁时 Pwd 可以为零。

MaskAdr：一个字节，掩模 EPC 号的起始字节地址。0x00 表示从 EPC 号的最高字节开始掩模，0x01 表示从 EPC 号的第二字节开始掩模，以此类推。

MaskLen：一个字节，掩模的字节数。掩模起始字节地址+掩模字节数不能大于 EPC 号字节长度，否则返回参数错误信息。

注：当 MaskAdr、MaskLen 为空时表示以完整的 EPC 号掩模。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x10	0x00	——	LSB	MSB

8.3 18000-6B 命令

8.3.1 寻查命令(单张)

本命令只能询查单张电子标签。如果多张标签同时处于天线有效范围内，可能无法询查到电子标签。

命令：

Len	Adr	Cmd	CRC-16	
0x04	0xXX	0x50	LSB	MSB

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x0d	0xXX	0x50	0x00	ID	LSB	MSB

参数解析：

ID：标签的 UID 号，8 个字节，低字节在前。

8.3.2 按条件寻查标签

本命令按照给定的条件询查电子标签。

命令：

Len	Adr	Cmd	Data[]				CRC-16	
			Condition	Address	Mask	Word_data		
0x0f	0xXX	0x51	0xXX	0xXX	0xXX	8 Bytes	LSB	MSB

参数解析：

Condition：选择标签的要求。0x00：等于条件；0x01：不等于条件；0x02：大于条件；0x03：小于条件。

Address：比较的起始字节地址。

Mask：掩码。用来指定要比较的数据。

Word_data：比较的条件，用来比较的数据。

Mask 的每一位对应 Word_data 的一个字节。Mask 的最高位(Bit7)对应 Word_data 的最左边的一个字节。Mask 的最低位 (Bit0)对应 Word_data 的最右边一字节。Word_data 是用来与标签中的数据进行比较的。Word_data 的最左边一字节与电子标签的 Address 地址上的数据进行比较，最右边一字节与 Address+7 地址上的数据进行比较。其它依此类推。Mask 相应位为 1，表示要把该位在 Word_data 中对应的字节与标签中对应的字节进行比较；为 0 则不比较。

应答：

Len	Adr	reCmd	Status	Num	Data[]	CRC-16	
0xXX	0xXX	0x51	0xXX	0xXX	UID1, UID2…	LSB	MSB

参数解析：

Status 是应答的状态，其代表的意义如下表所述：

Status	说明
0x15	命令执行结束，同时返回询查到的电子标签数据
0x16	询查时间结束，命令执行强制退出，同时返回已询查到的标签数据
0x17	如果读到的标签数量无法在一条消息内传送完，将分多次发送。如果 Status 为 0x03，则表示这条数据结束后，还有数据。
0x18	还有电子标签未读取，电子标签数量太多，读写器的存储区已满，返回此状态值，同时返回已询查到得电子标签数据。

参数解析：

Num：本条命令中包含的 UID 个数。范围为 1 – 31。

Data[]：电子标签的 UID。每个 UID 是 8 个字节，低字节在前。当无 UID 时(即 Num 为 0 时)，Data[]为空。

8.3.3 读数据

该命令用来从电子标签的某个指定地址开始读若干个字节。

命令：

Len	Adr	Cmd	Data[]			CRC-16	
			Address	ID	Num		
0x0e	0xXX	0x52	0xXX	8 Bytes	0xXX	LSB	MSB

参数解析：

Address：读数据的起始字节地址。地址范围为 0 ~ 223。如果地址超出 223，将返回参数错误信息。

Num：要读的数据个数，以字节为单位。 Num 的范围是 1 ~ 32。如果 Address+Num 大于 224、或是 Num 超过 32、或 Num 为 0，读写器将返回参数错误信息。

ID：要读数据的电子标签的 ID。8 个字节，低字节在前。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0xXX	0xXX	0x52	0x00	Data	LSB	MSB

参数解析：

Data：读到的数据，低字节在前。

8.3.4 写数据

该命令向指定的电子标签写入若干个字节。

命令：

Len	Adr	Cmd	Data[]			CRC-16	
			Address	ID	Wdata		
0xXX	0xXX	0x53	0xXX	8 Bytes	变长	LSB	MSB

参数解析：

Address：写入数据的起始地址。地址范围：8 ~ 223。地址如果超出范围，将返回参数错误信息。

ID：要读数据的电子标签的 ID。8 个字节，低字节在前。

Wdata：要写入的数据。Wdata 的长度限定在 32 个字节以内。Wdata 的高字节写在电子标签的低地址。如果命令中 Wdata 的长度为 0(即 Wdata 部分不存在)或超过 32，将返回参数错误信息。如果 Address 加 Wdata 的长度大于 224，也将返回参数错误信息。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x53	0x00	——	LSB	MSB

8.3.5 锁定检测

该命令用来检测指定的字节是否锁定。

命令：

Len	Adr	Cmd	Data[]		CRC-16	
			Address	ID		
0x0d	0xXX	0x54	0xXX	8 Bytes	LSB	MSB

参数解析：

Address：要检测是否被锁定的字节的地址。范围：0～223。超过这个范围将返回参数错误信息。

ID：要读数据的电子标签的 ID。8 个字节，低字节在前。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x06	0xXX	0x54	0x00	LockState	LSB	MSB

参数解析：

LockState：

0x00：该字节未被锁定

0x01：该字节已经被锁定

8.3.6 锁定

该命令锁定指定的字节。

命令：

Len	Adr	Cmd	Data[]		CRC-16	
			Address	ID		
0x0d	0xXX	0x55	0xXX	8 Bytes	LSB	MSB

参数解析：

Address：要锁定的字节地址。范围：8～223。超过这个范围将返回参数错误信息。

ID：要读数据的电子标签的 ID。8 个字节，低字节在前。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x55	0x00	——	LSB	MSB

8.4 读写器自定义命令

8.4.1 读取读写器信息

当上位机通过发送命令数据块让读写器执行该命令后，将获得读写器的信息，这其中包括读写器地址（Adr）、读写器软件版本（Version）、读写器类型代码、读写器协议支持信息、读写器的频率范围、读写器的功率、询查时间等信息。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0x04	0xXX	0x21	——	LSB	MSB

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x0d	0xXX	0x21	0x00	Version， Type， Tr_Type，dmaxfre，dminfre，Power，Scntm	LSB	MSB

参数解析：

参数	长度(Byte)	说明
Version	2	版本号，高字节代表主版本号，低字节代表子版本号
Type	1	读写器类型代号。0x09 代表 UHFREADER18。
Tr_Type	1	读写器支持的协议信息，Bit1 为 1 表示支持 18000-6c 协议，Bit0 为 1 表示 18000-6B 协议，其它位保留。。
dmaxfre	1	Bit7-Bit6 用于频段设置用；Bit5-Bit0 表示当前读写器工作的最大频率。
dminfre	1	Bit7-Bit6 用于频段设置用；Bit5-Bit0 表示当前读写器工作的最小频率。
Power	1	读写器的输出功率。范围是 0 到 30。
Scntm	1	询查时间。读写器收到询查命令后，在询查时间内，会给上位机应答。

频段设置如下表：

MaxFre(Bit7)	MaxFre(Bit6)	MinFre(Bit7)	MinFre(Bit6)	FreqBand
0	0	0	0	User band
0	0	0	1	Chinese band2
0	0	1	0	US band
0	0	1	1	Korean band
0	1	0	0	保留
0	1	0	1	保留
…	…	…	…	…
1	1	1	1	保留

8.4.2 设置读写器工作频率

这个命令用来选择频段及各频段中的上限频率，下限频率。上限频率必须大于或等于下限频率。

命令：

Len	Adr	Cmd	Data[]		CRC-16	
			MaxFre	MinFre		
0x06	0xXX	0x22	0xXX	0xXX	LSB	MSB

参数解析：

MaxFre：一个字节，Bit7-Bit6 用于频段设置用；Bit5-Bit0 表示读写器工作的最大频率。

MinFre：一个字节，Bit7-Bit6 用于频段设置用；Bit5-Bit0 表示读写器工作的最小频率。最小频率必须小于等于最大频率。

频段设置如下表：

MaxFre(Bit7)	MaxFre(Bit6)	MinFre(Bit7)	MinFre(Bit6)	FreqBand
0	0	0	0	User band
0	0	0	1	Chinese band2
0	0	1	0	US band
0	0	1	1	Korean band
0	1	0	0	保留
0	1	0	1	保留
…	…	…	…	…
1	1	1	1	保留

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x22	0x00	——	LSB	MSB

设置的时候，如果下限频率大于上限频率，则会返回参数出错信息。
各频段计算公式：

User band ： Fs = 902.6 + N * 0.4 (MHz) 其中N∈[0, 62]。
Chinese band2： Fs = 920.125 + N * 0.25 (MHz) 其中N∈[0, 19]。
US band： Fs = 902.75 + N * 0.5 (MHz) 其中N∈[0,49]。
Korean band： Fs = 917.1 + N * 0.2 (MHz) 其中N∈[0, 31]。

8.4.3 设置读写器地址

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0x05	0xXX	0x24	address	LSB	MSB
			0xXX		

参数解析：

Address：要设置的新的读写器地址。本条命令使用原来的地址应答。这个地址不能为0xFF。如果设置为 0xFF，则读写器将返回参数出错信息。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x24	0x00	——	LSB	MSB

8.4.4 设置读写器询查时间

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0x05	0xXX	0x25	Scantime	LSB	MSB
			0xXX		

参数解析：

Scantime：询查时间。读写器将会把询查命令最大响应时间改为用户给定的值（3*100ms~255*100ms），以后将使用此项新的询查命令最大响应时间。出厂时缺省值是 0x0a（对应的时间为 10*100ms）。用户修改范围是 0x03~0xff（对应时间是 3*100ms~255*100ms）。注意，实际的响应时间可能会比设定值大 0~75ms。当用户写入的值是 0x00~0x02 时，读写器将会自动恢复成缺省值 0x0a（对应的时间为 10*100ms）。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x25	0x00	——	LSB	MSB

8.4.5 设置串口波特率

此命令用来更改读写器的串口波特率。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0x05	0xXX	0x28	BaudRate	LSB	MSB
			0xXX		

参数解析：

BaudRate：新的波特率，波特率默认为 57600。BaudRate 值为 0/1/2/5/6/。其它值保留。其对应的波特率为：

BaudRate	实际波特率
0	9600bps
1	19200 bps
2	38400 bps
5	57600 bps
6	115200 bps

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x28	0x00	——	LSB	MSB

需要特别注意的是，本次传送应答数据所用的波特率还是原来的波特率。从下一次发命令开始，使用新的波特率。

8.4.6 调整功率

该命令设置读写器功率。范围是 0~30，取值 30 时约为 1 瓦的输出功率。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0x05	0xXX	0x2F	Pwr	LSB	MSB
			0xXX		

Pwr：要设定的功率参数。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x2F	0x00	——	LSB	MSB

8.4.7 声光控制命令

该命令用来控制 LED 灯和蜂鸣器按一定规律闪烁和鸣叫。

命令：

Len	Adr	Cmd	Data[]			CRC-16	
			ActiveT	SilentT	Times		
0x07	0xXX	0x33	0xXX	0xXX	0xXX	LSB	MSB

参数解析：

ActiveT：LED 灯亮和蜂鸣器鸣叫时间(ActiveT*50ms)，默认值为零。0<=ActiveT<=255。

SilentT： LED 灯和蜂鸣器静默时间(SilentT *50ms)，默认值为零。0<= SilentT <=255。

Times： LED 灯亮和蜂鸣器鸣叫次数(0<=Times<=255) 默认值为零。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x33	0x00	——	LSB	MSB

8.4.8 韦根参数设置命令

这个命令用于设置韦根参数

命令：

Len	Adr	Cmd	Data[]				CRC-16	
			Wg_mode	Wg_Data_Inteval	Wg_Pulse_Width	Wg_Pulse_Inteval		
0x08	0xXX	0x34	0xXX	0xXX	0xXX	0xXX	LSB	MSB

参数解析：

Wg_mode：Bit0：韦根 26、34 选择位。Bit0=0 时选择韦根 26，Bit0=1 时选择韦根 34。
Bit1：Bit1=0 时韦根输出高字节在前，Bit1=1 是韦根输出低字节在前。
其它位保留，默认为 0。

Wg_Data_Inteval：输出数据间隔时间(0 ~255)*10ms，默认值为 30。

Wg_Pulse_Width：数据脉冲宽度(1 ~255)*10us，默认值为 10。

Wg_Pulse_Inteval：数据脉冲间隔(1 ~255)*100us，默认值为 15。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x34	0x00	——	LSB	MSB

8.4.9 工作模式设置命令

该命令用于设置读写器工作模式。进入主动模式后，读写器仍然可以接收上位机的命令，但是读写器只允许运行读写器自定义命令，当要读写器运行其它命令时，读写器将返回命令结果状态值为 0xFE 的应答而不执行该命令。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
			Parameter		
0x0a	0xXX	0x35	6Bytes	LSB	MSB

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x35	0x00	——	LSB	MSB

Parameter 这个参数共 6 个字节，该组参数将写入 EEPROM 内，所以，除非再次使用这条命令来修改配置的内容，否则读写器将一直保持这样的设置运行。具体内容如下：

Byte1	Byte2	Byte3	Byte4	Byte5	Byte6
Read_mode	Mode_state	Mem_Inven	First_Adr	Word_Num	Tag_Time

参数解析：

Read_mode：工作模式选择。

Bit1	Bit0	工作模式
0	0	应答模式
0	1	主动模式
1	0	触发模式(低电平有效)
1	1	触发模式(高电平有效)

Mode_state：Bit0：协议选择位。Bit0=0 时读写器支持 18000-6C 协议；Bit0=1 时读写器支持 18000-6B 协议。

Bit1：输出方式选择位。Bit1=0 时韦根输出，Bit1=1 时 RS232/RS485 输出。

Bit2：蜂鸣器提示选择位。Bit2=0 时开蜂鸣器提示，Bit2=1 时关蜂鸣器提示，默认值为 0。

Bit3：韦根输出模式下 First_Adr 参数为字地址或字节地址选择位。Bit3=0 时 First_Adr 为字地址；Bit3=1 时 First_Adr 为字节地址。

Bit4：玺瑞 485 选择位，Bit1=0 时该位无效。Bit4=0 时是普通 485 输出方式，Bit4=1 时是玺瑞 485 模式。玺瑞 485 模式下只支持单标签操作（18000-6C、18000-6B 均有效）（读保留 区、EPC 区、TID 区、用户区，单张查询）。玺瑞 485 模式下 First_Adr 为字节地址。

其它位保留，默认为 0。

Mem_Inven：当读写器工作在 18000-6C 协议时才有效，选择要读取的存储区或询查标签。0x00：保留区；0x01：EPC 存储器；0x02：TID 存储器；0x03：用户存储器；0x04：多张查询；0x05：单张查询；0x06 ：EAS 检测。其他值保留，若命令中出现了其它值，将返回参数出错的消息。玺瑞模式下多张查询、EAS 检测无效。

First_Adr：指定要读取的起始地址。18000-6C 协议中：0x00 表示从第一个字(第一个 16 位存储区)开始读，0x01 表示从第 2 个字开始读，依次类推；18000-6B 中：0x00 表示从第一个字节开始读，0x01 表示从第 2 个字节开始读，依次类推。

Word_Num：要读取的字的个数，RS232 输出方式下才有效。不能设置为 0x00，否则将返回参数错误信息。Word_Num 不能超过 32，若 Word_Num 设置为 0 或者超过了 32，将返回参数出错的消息。玺瑞模式下，Word_Num 范围为 0x01~0x04。

Tag_Time：主动模式下单张标签操作（18000-6C，18000-6B 均有效）(读保留区、EPC 区、TID 区、用户区，单张查询)间隔时间(0~255)*1s，对同一张标签在间隔时间内只操作一次。默认值为零，即对标签操作不用等待时间。玺瑞模式下该参数无效。

主动模式下端口输出格式说明：

RS232/RS485 输出方式下，串口输出格式如下：

注：RS232/RS485 输出方式下，当要重新设置读写器参数时要保证射频场内无卡。

1、当读写器支持 18000-6C 协议，Mem_Inven 为 0x00~0x03 时：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0xXX	0xXX	0xee	0x00	Word1，Word2,…	LSB	MSB

参数解析：

Word1, Word2… 以字为单位。每个字都是 2 个字节，高字节在前。Word1 是从起始地址读到的字，Word2 是起始地址后一个字地址上读到的字，以此类推。

2、当读写器支持 18000-6C 协议，Mem_Inven 为 0x04、0x05 时：

Len	Adr	reCmd	Status	Data[]	CRC-16

0xXX	0xXX	0xee	0x00	EPC ID	LSB	MSB

参数解析:

EPC ID: 读到的电子标签的 EPC 数据，EPC 号高字(EPC C1 G2 中数据以字为单位)在前，每一个字的最高字节在前。

3、当读写器支持 18000-6C 协议，Mem_Inven 为 0x06 时：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0xee	0xee	——	LSB	MSB

4、当读写器支持 18000-6B 协议时：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0xXX	0xXX	0xee	0x00	Word1，Word2,…	LSB	MSB

参数解析：

Word1, Word2… 以字为单位。每个字都是 2 个字节，高字节在前。Word1 是从起始地址读到的字，Word2 是起始地址后一个字地址上读到的字，以此类推。

8.4.10 读取工作模式参数

该命令可以读取工作模式参数。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
0x04	0xXX	0x36	——	LSB	MSB

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x11	0xXX	0x36	0x00	Wg_mode，Wg_Data_Inteval，Wg_Pulse_Width，Wg_Pulse_Inteval，Read_mode，Mode_state，Mem_Inven，First_Adr，Word_Num，Tag_Time，Accuracy，OffsetTime	LSB	MSB

参数解析：

Wg_mode、Wg_Data_Inteval、Wg_Pulse_Width、Wg_Pulse_Inteval：韦根参数

Read_mode、Mode_state、Mem_Inven、First_Adr、Word_Num、Tag_Time：工作模式参数

Accuracy：EAS 测试精度参数

OffsetTime：Syris485 命令响应偏置时间

8.4.11 EAS 检测精度设置

该命令用于设置主动模式下 EAS 检测精度。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
			Accuracy		
0x05	0xXX	0x37	0xXX	LSB	MSB

Accuracy：范围为 0~8，数值越大精度越高。默认值为 8。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x37	0x00	——	LSB	MSB

8.4.12 Syris 响应偏置时间设置

该命令用于设置 Syris485 模式下的 Syris 命令响应偏置时间。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
			OffsetTime		
0x05	0xXX	0x38	0xXX	LSB	MSB

OffsetTime：Syris485 命令响应偏置时间（0~100）*1ms，默认值为 5。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x05	0xXX	0x38	0x00	——	LSB	MSB

8.4.13 触发延时设置

本命令用于设置触发模式下触发有效时间。此项功能仅对读写器固件 V2.36 及以上版本有效。

命令：

Len	Adr	Cmd	Data[]	CRC-16	
			TriggerTime		
0x05	0xXX	0x3b	0xXX	LSB	MSB

TriggerTime：触发有效时间(0~254)*1s，默认值为 0。当触发有效时间设置为 255 时，为获取当前的触发有效时间设置值。

应答：

Len	Adr	reCmd	Status	Data[]	CRC-16	
0x06	0xXX	0x3b	0x00	TriggerTime	LSB	MSB

TriggerTime：当前触发有效时间(0~254)*1s。