

QR4431 超高频固定式读写器

产品规格

V2.12

2010.1.15



上海坤锐电子科技有限公司

地址：上海市浦东新区张东路 1387 号 10 幢 01 号 2 楼（集电港 2 期）

电话：86-21-68795432

传真：86-21-68795835

网址：www.quanray.com

邮编：201203

版权申明

本文档中包含的信息为上海坤锐电子科技有限公司所有。本文档属于机密信息，事先未经上海坤锐电子科技有限公司书面许可，不得擅自泄漏或复制本文档中的内容。且上海坤锐电子科技有限公司保留不经事先通知而改变本文档信息的权利。

目 录

1.	摘要	1
2.	产品特性	1
2.1.	读写器特性.....	1
3.	读写器驱动安装	2
3.1.	读写器串口连接.....	2
4.	读写器 demo 程序	3
4.1.	demo 程序安装说明	3
4.2.	demo 程序主界面说明	3
4.3.	读写器 demo 程序连接方式.....	4
4.4.	Inventory 方式选择.....	4
4.5.	天线输出功率设值和天线选择.....	5
4.6.	Select 参数设置.....	5
4.7.	Query 参数设置.....	5
4.8.	Access 参数设置.....	6
5.	读写器基本协议架构.....	9
5.1.	协议帧功能及格式.....	9
5.1.1	Get Reader Info(0x0a).....	9
5.1.2	Inventory(0x01).....	10
5.1.3	Read(0x02).....	12
5.1.4	Write(0x03).....	14
5.1.5	Lock (0x04)	15
5.1.6	Kill (0x09)	17
5.1.7	Set Select (0x06)	19
5.1.8	Reset Select(0x07).....	20
5.1.9	Set 6C paramater(0x08).....	21
5.1.10	TagPowerDown(0x32).....	22
5.2	Status Code.....	22

1. 摘要

本手册包括产品特性、硬件安装说明、demo 软件使用说明和 API 开发说明。

2. 产品特性

本读写器通过 pc 的 usb 口供电，通过一个 usb 转 RS232 串口与 pc 通信，读写器天线内置。整个读写器外观，如下图所示：



图 1 一套完整读写器

2.1. 读写器特性

电器特性：

- 使用频率：920-925MHz (CHN)；902-928MHz (FCC)
- 无线电规范：CHN /FCC
- 协议：EPC C1 G2 (ISO18000-6C)
- 读距离：最高到 3 米（依赖于标签）

- 写距离：读距离的 70%
- 天线数量（内置）：1
- 射频功率：15-27dBm
- 频率稳定度：±10%ppm
- 数据接口：串口
- 电源供应：usb 取电
- 电源功耗：5Watts

使用环境：

- 使用温度：-10 至 50° C
- 存储温度：-25 至 65° C
- 湿度：非凝结相对湿度 5 至 95%

机械特性：

- 体积：145*130*30mm
- 总量：350g

3. 读写器驱动安装

由于读写器是通过一个 usb 接口虚拟的串口与主机进行通信，所以第一次连接时需要安装串口驱动。安装 CP210x_VCP_Win2K_XP_S2K3 安装程序。然后将读写器 usb 线插入 pc，pc 将自动安装 usb 转串口驱动，安装完之后进入 pc 的设备管理器找到虚拟出来的串口号。

3.1. 读写器串口连接

读写器有一个 usb 转 RS232 串口。客户端可以通过串口控制读写器。串口设置：波特率 115200，无校验位，8 位字节，1 位停止位。

4. 读写器 demo 程序

4.1. demo 程序安装说明



- 1) 双击 Setup.msi, 安装好 QuanrayReaderDemo 程序, 快捷图标
- 2) 打开 QuanrayReaderDemo, 选择连接端口类型, 连接读写器。
- 3) 需要 NetFramework2.0 或以上版本支持。

4.2. demo 程序主界面说明

demo 程序是读写器功能的应用的演示程序, 其主界面如下所示:

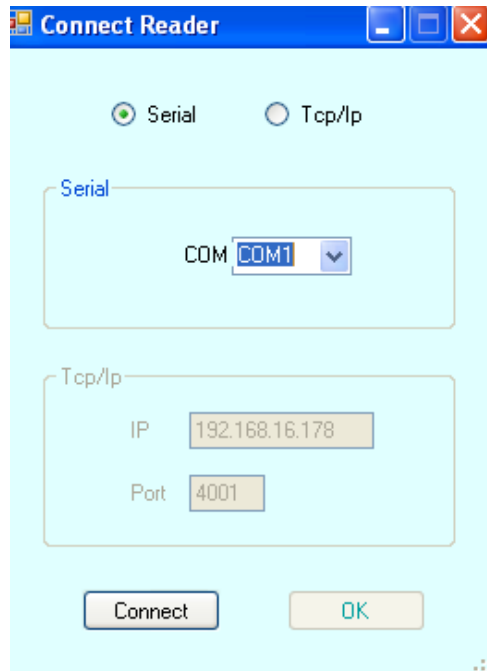


左侧显示窗口主要显示 Inventory 指令获取的 EPC 相关数据。

右侧显示窗口主要记录 Inventory 状态过程, 读取标签数目, 通讯时间等。

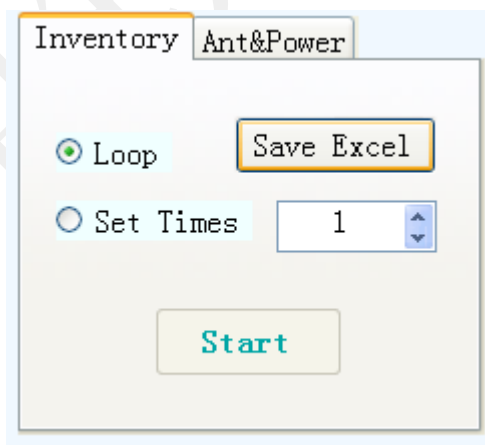
4.3. 读写器 demo 程序连接方式

当打开 demo 程序时，将弹出如下图显示的窗口，可以在连接方式中选择实际与 reader 建立的物理连接方式。



按下 Connect 按钮后如果连接建立成功将弹出主界面窗口。

4.4. Inventory 方式选择



demo 程序提供二种快速获取 epc 的 inventory 方式：

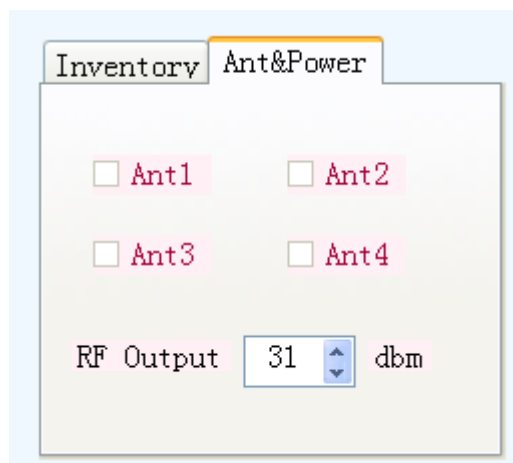
Loop：按一次 start 按钮获进行不间断的循环 inventory 操作，

Set Times：可以设置 inventory 操作周期，时间为秒。

缺省操作为 Loop。

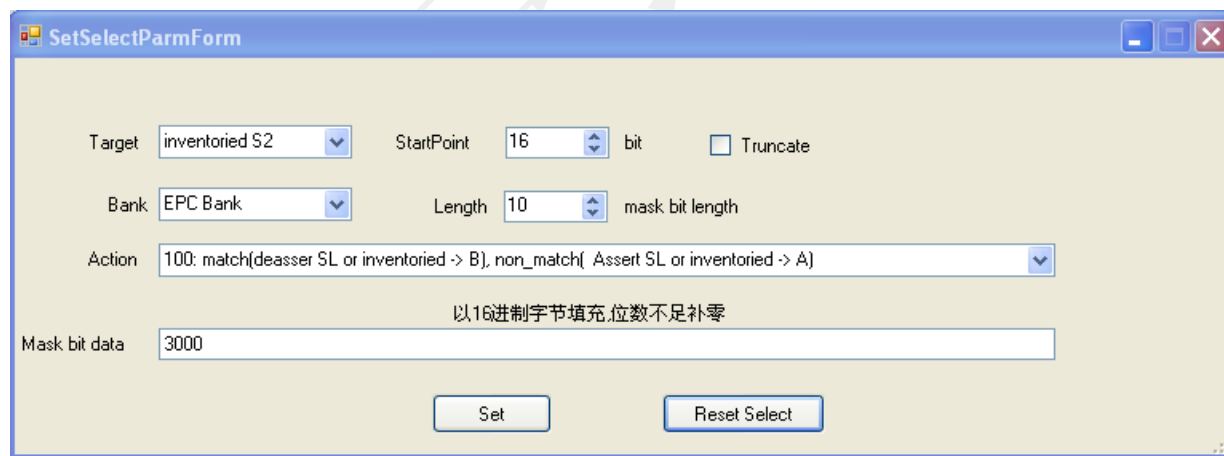
Save excel 按钮可以将按表格显示的 epc 码保存成 csv 的 excel 表格格式。

4.5. 天线输出功率设值和天线选择



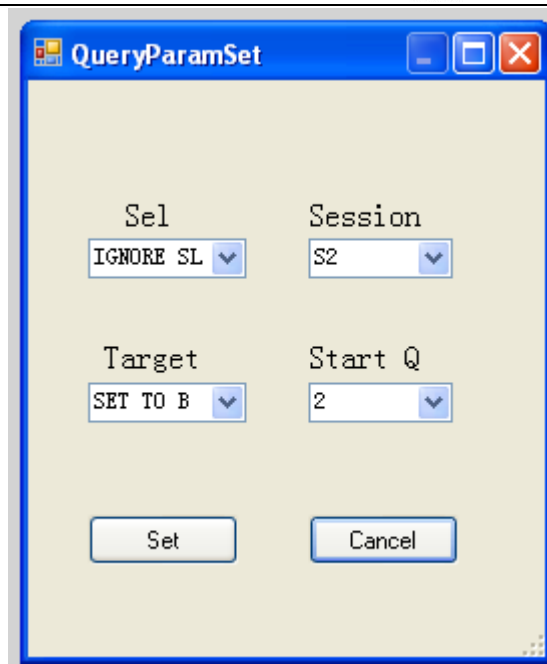
当与读写器连接正常建立后，程序将获得读写器连接天线的状态，如果读写器检测到连接天线将使能对应的天线选择，天线输出功率设置范围为 15~31db. 默认 31db. 当前模块只支持一个天线选择。

4.6. Select 参数设置



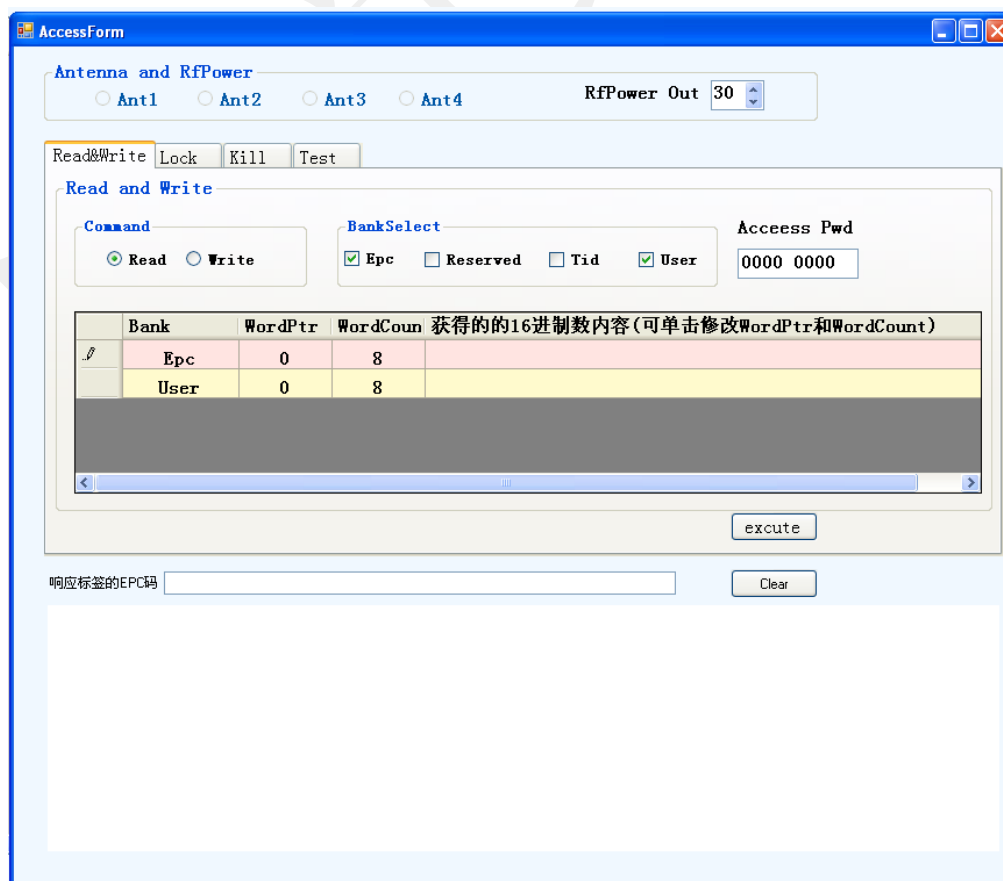
选择 18000-6c (C1G2) → Select Parameter，根据需求可以对读写器 select 参数进行设置，每一组参数组合保存在读写器的缓存中，在读写器发出 query 指令之前自动发出，按 RstSelect 按钮可以恢复读写器的缺省 select 参数。注意：读写器只支持 5 组 select 参数的组合。

4.7. Query 参数设置



选择 18000-6c (C1G2) → Query Parameter, 根据需求可以对 Query 参数进行设置。Query 参数和 select 参数配合可以指定符合条件的标签参与响应。

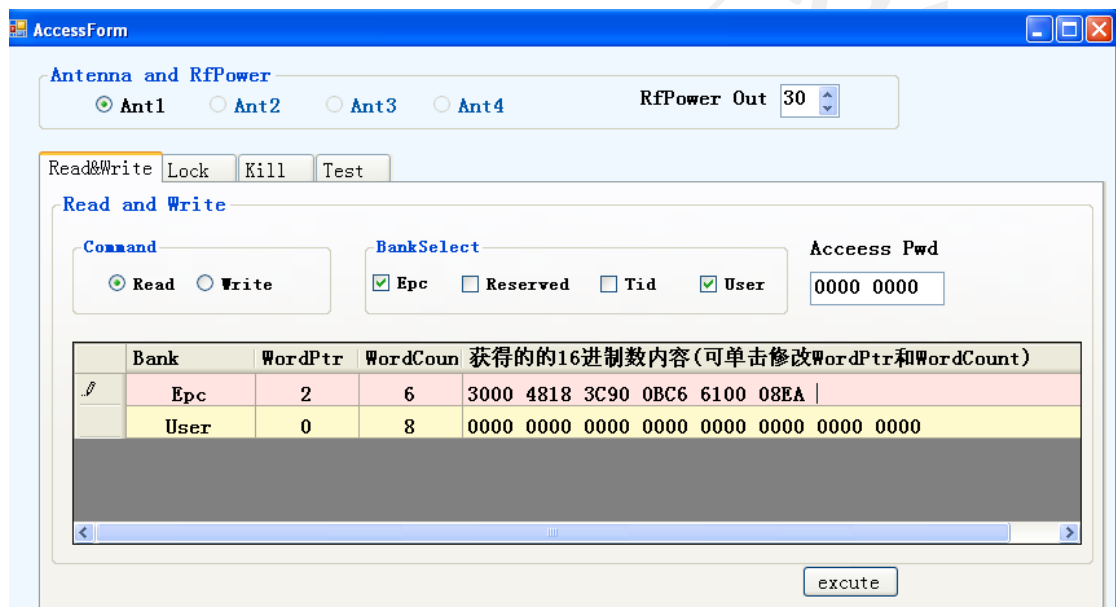
4.8. Access 参数设置



选择 18000-6c (C1G2) → Access, 勾选好天线, 设置发射功率。可以对 tag 各 bank 执行 read, write, kill, lock 等操作。

执行 read&write 操作, Command 栏中选择 read, BankSelect 栏选取要读取的区域。然后按 excute 按钮执行。选择 write, 选择要写入的区域, 下面的区域可以输入要写入的内容。如, 写 EPC 和 User, 勾选好对应区域, WordPtr 为写入的起始地址块, WordCount 为写入的地址块数, 通过单击可进行更改数值。

写 EPC, 从第 2 字开始写入 6 个 Word, 值为 3000 4818 3C90 0BC6 6100 08EA , User 区, 从第 0 字开始写入 8 个 Word, 值为 0000 0000 0000 0000 0000 0000 0000 0000, 如下图所示,



按 excute 按钮执行, 执行成功后, 显示如下

AccessForm

Antenna and RfPower

☒ Ant1 ☐ Ant2 ☐ Ant3 ☐ Ant4 RfPower Out 30

Read&Write Lock Kill Test

Read and Write

Command ☒ Read ☐ Write

BankSelect ☒ Epc ☐ Reserved ☐ Tid ☒ User

Access Pwd 0000 0000

Bank	WordPtr	WordCoun	获得的16进制数内容(可单击修改WordPtr和WordCount)
Epc	2	6	3000 4818 3C90 0BC6 6100 08EA
User	0	8	0000 0000 0000 0000 0000 0000 0000 0000

excute

响应标签的EPC码 3000 4818 3C90 0BC6 6100 Clear

Epc bank Read success
User bank Read success

不成功，则显示如下

AccessForm

Antenna and RfPower

☒ Ant1 ☐ Ant2 ☐ Ant3 ☐ Ant4 RfPower Out 30

Read&Write Lock Kill Test

Read and Write

Command ☒ Read ☐ Write

BankSelect ☒ Epc ☐ Reserved ☐ Tid ☒ User

Access Pwd 0000 0000

Bank	WordPtr	WordCoun	获得的16进制数内容(可单击修改WordPtr和WordCount)
Epc	2	6	3000 4818 3C90 0BC6 6100 08EA
User	0	8	0000 0000 0000 0000 0000 0000 0000 0000

excute

响应标签的EPC码 Clear

Epc bank read fail
tag没响应或者发送超时
User bank read fail
tag没响应或者发送超时

其他区域执行情况类似。

5. 读写器基本协议架构

本协议基本采用主（host）从（reader）应答格式（不排除从机主动上报格式，但格式与应答格式一致）。

协议基本格式：

数据区	描述	长度 (byte)
0xEE	帧头	1
帧长度	命令帧长度，不包括帧头和校验字节	2
	帧类型	1
Payload	帧内容	
Crc 校验	2 字节的 crc 校验字节	2

应答格式：

数据区	描述	长度 (Byte)
0xEE	帧头	1
帧长度	命令帧长度，不包括帧头和校验字节	2
	帧类型, Get Reader Status COMMAND	1
Payload	帧内容	
Crc 校验	2 字节的 crc 校验字节	2

5.1. 协议帧功能及格式

5.1.1 Get Reader Info (0x0a)

得到 reader 的基本信息，Antenna status 显示当前连接的 reader 所能使用的天线。如当前连接的 reader 有一个或多个天线状态改变，reader 主动发送 Response 给 Host。Host 启动时应主动发送此帧获得 reader 的基本信息（主要是天线连接信息）。

COMMAND format:

数据区	描述	长度 (byte)
0xEE	帧头	1
帧长度	命令帧长度，不包括帧头和校验字节	2
0x0a	帧类型, Get Reader Status COMMAND	1
Crc 校验	2 字节的 crc 校验字节	2

Response format:

数据区	描述	长度 (Byte)
0xEE	帧头	1
帧长度	命令帧长度, 不包括帧头和校验字节	2
0x0a	帧类型, Get Reader Status COMMAND	1
Reader status	0x00: 自检通过。 0xFF: reader 初始化失败	1
Software version	Reader 软件版本号	2
Hardware version	Reader 硬件版本号	2
Antenna status	0b0000 0001 Antenna1 connected 0b0000 0010 Antenna2 connected 0b0000 0100 Antenna3 connected 0b0000 1000 Antenna4 connected	1
Status code	0x01 0x00 CRC 校验错	2
Crc 校验	2 字节的 crc 校验字节	2

注: 当 reader 工作时检测到某路天线异常, 将主动上报此帧通知客户端天线异常。

5.1.2 Inventory(0x01)

Reader 获取标签 EPC 段盘点命令。一个或一个以上的标签可以应答。Reader 检查某个标签应答, 获得该标签发出 PC、EPC。如设置了 select 参数, 应配合 select 参数选取该命令中的参数, 应答帧中可以包括多个标签的 pc、epc 数据。如果没有预先设置 select 参数, 将使用 reader 缺省的 select 参数。

此命令可能返回多个数据帧(command status = 0)直至 inventory(command status = 0xff) 结束。

COMMAND format:

数据区	描述	长度 (byte)
0xEE	帧头	1
帧长度	命令帧长度, 不包括帧头和校验字节	2
0x01	帧类型, Inventory command	1
RF POWER	15~30	1
Sel	0x00: All tag can be inventoried ; ignore SL(default) 0x01: Only inventory tags with SL NOT set 0x02: Only inventory tags with SL SET	1

session	0x00:Use session S0 for inventory 0x01:Use session S1 for inventory 0x02:Use session S2 for inventory (default) 0x03:Use session S3 for inventory	1
Target	0x00:Only inventory Tags with inventoried flag set to A for session 0x01:Only inventory Tags with inventoried flag set to B for session (default)	1
Starting Q	由在天线覆盖范围内的 tag 数定	1
Antenna select	0b0000 0001 Antenna1 0b0000 0010 Antenna2 0b0000 0100 Antenna3 0b0000 1000 Antenna4	1
Crc 校验	2 字节的 crc 校验字节	2

Response format:

数据区	描述	长度 (Byte)
0xEE	帧头	1
帧长度	命令帧长度, 不包括帧头和校验字节	2
0x01	帧类型, Inventory command	1
Command status	0x00: 有标签数据返回 Inventory not complete 0xFF: 没有标签数据返回, inventory complete	1
Tag response num	获得 EPC 码的 tag 个数	1
Tag response1	读到 tag 的天线序号	01: Antenna1 02: Antenna2 03: Antenna3 04: Antenna4
	Epc id1 长度 n	第一个 tag id 长度 (按 word 计算长度)
	Pc 码	
	Epc	第一个 tag id 数据区
Tag response2		
...		
Tag response n		
Status code	0x01 0x00 CRC 校验错 0x02 0x00 设置 Tx/Rx 参数错误 0x03 0x00 tag 没响应或者发送超时 0x05 0x00 天线选择错误 0x07 0x00 RFpower 设置超限	2

Crc 校验	2 字节的 crc 校验字节	2
--------	----------------	---

注：如果 Command status = 0xff，tag response 区忽略。

5.1.3 Read(0x02)

Read 命令允许 reader 读取标签的整个或部分保留存储区、EPC 存储区、TID 存储区或用户存储区。Read 命令包含以下字段：

Memory Bank 规定了 Read 命令是否访问 Reserve bank、EPC bank、TID bank 及 user bank。Read 命令应用于单个 bank。

WordPtr 规定指定的 bank 读取的起始字地址，字的长度为 16 位。例如，字指针=00h 规定第一个 16 位存储字，字指针=01h 规定第二个 16 位存储字等。

Access password：当 Access password 不等于零时如果匹配标签存储的 Access password 则标签进入 Secured 状态执行此命令。

COMMAND format:

数据区	描述	长度 (byte)
0xEE	帧头	1
帧长度	命令帧长度，不包括帧头和校验字节	2
0x02	帧类型，read command	1
RF POWER	15~30	1
Sel	0x00:All tag can be inventoried ;ignore SL(default) 0x01:Only inventory tags with SL NOT set 0x02:Only inventory tags with SL SET	1
session	0x00:Use session S0 for inventory 0x01:Use session S1 for inventory 0x02:Use session S2 for inventory (default) 0x03:Use session S3 for inventory	1
Target	0x00:Only inventory Tags with inventoried flag set to A for session 0x01:Only inventory Tags with inventoried flag set to B for session (default)	1
Starting Q	由在天线覆盖范围内的 tag 数定	1

Access password	0x00000000 if not application	4
Memory bank	0x00: reserve bank 0x01: epc bank 0x02: Tid bank 0x03: user bank	1
WordPtr	Start address point	2
WordCount	Number word to read	2
Antenna select	0b0000 0001 Antenna1 0b0000 0010 Antenna2 0b0000 0100 Antenna3 0b0000 1000 Antenna4	1
Crc 校验	2 字节的 crc 校验字节	2

Response format:

数据区	描述		长度 (Byte)
0xEE	帧头		1
帧长度	命令帧长度, 不包括帧头和校验字节		2
0x02	帧类型, read command		1
Command status	0x00: 命令执行成功 0xFF: 命令执行失败		1
Tag response num	Read tag 个数 (当前设置为 1)		1
Tag response 被 read 到的标签	被 read 到标签 EPC id 长度 n	按 word 计算长度	1
	Pc		2
	Epc	EPC 数据区	N*2
Read data	Length n	Read data 长度 (按 word 计算长度)	2
	Data	Read data 内容	N*2
Status code	0x01 0x00 CRC 校验错 0x02 0x00 设置 Tx/Rx 参数错误 0x03 0x00 tag 没响应或者发送超时 0x04 error_code (tag 返回的 error code) 0x05 0x00 天线选择错误 0x06 0x00 Access password 错误 0x07 0x00 Rfpower 设置超限		2
Crc 校验	2 字节的 crc 校验字节		2

注: 如果 Command status 执行失败, tag response, Read data 区忽略。

5.1.4 Write(0x03)

Write 命令允许 reader 写入标签的保留存储区、EPC 存储区、TID 存储区或用户存储区一个字或多个字（16 比特）。Write 命令包含以下字段：

Memory Bank 规定了 Write 命令是否访问 Reserve bank、EPC bank、TID bank 及 user bank。Write 命令应用于单个 bank。

WordPtr 规定指定的 bank 写入的起始字地址，字的长度为 16 位。例如，字指针=00h 规定第一个 16 位存储字，字指针=01h 规定第二个 16 位存储字等。

WordCount 规定写入的 16 位字数。

Access password：当 Access password 不等于零时如果匹配标签存储的 Access password 则标签进入 Secured 状态执行此命令。

COMMAND format:

数据区	描述	长度 (byte)
0xEE	帧头	1
帧长度	命令帧长度，不包括帧头和校验字节	2
0x03	帧类型，Write command	1
RF POWER	15~30	1
Sel	0x00:All tag can be inventoried ;ignore SL(default) 0x01:Only inventory tags with SL NOT set 0x02:Only inventory tags with SL SET	1
session	0x00:Use session S0 for inventory 0x01:Use session S1 for inventory 0x02:Use session S2 for inventory (default) 0x03:Use session S3 for inventory	1
Target	0x00:Only inventory Tags with inventoried flag set to A for session 0x01:Only inventory Tags with inventoried flag set to B for session (default)	1
Starting Q	由在天线覆盖范围内的 tag 数定	1
Access password	0x00000000 if not application	4
Memory bank	0x00: reserve bank	1

	0x01: epc bank 0x02: Tid bank 0x03: user bank	
WordPtr	Start address point	2
WordCount	Number word to write	2
Write option (option)	0b0000 0001 block write 0b0000 0010 blockerase first	1
data	Write data	WordCount * 2
Antenna select	0b0000 0001 Antenna1 0b0000 0010 Antenna2 0b0000 0100 Antenna3 0b0000 1000 Antenna4	1
Crc 校验	2 字节的 crc 校验字节	2

Response format:

数据区	描述	长度 (Byte)
0xEE	帧头	1
帧长度	命令帧长度, 不包括帧头和校验字节	2
0x03	帧类型, Write command	1
Command status	0x00: 命令执行成功 0xFF: 命令执行失败	1
Tag response num	写入 tag 个数 (当前设置为 1)	1
Tag response	EPC 长度 n	长度按 word 计算
	Pc	2
	Epc	EPC 数据区
Status code	0x01 0x00 CRC 校验错 0x02 0x00 设置 Tx/Rx 参数错误 0x03 0x00 tag 没响应或者发送超时 0x04 error_code (tag 返回的 error code) 0x05 0x00 天线选择错误 0x06 0x00 Access password 错误 0x07 0x00 Rfpower 设置超限	2
Crc 校验	2 字节的 crc 校验字节	2

注: 如果 Command status 执行失败, tag response 区忽略。

5.1.5 Lock (0x04)

Lock 命令允许 reader 锁定标签的整个保留存储区、EPC 存储区、TID 存储区或用户存储区。只有处于保护状态 (Secure) 的标签才可执行 Lock 命令。Lock

命令适用于单个段的操作：

锁定口令，由此阻止或允许读取和/或写入该口令。

锁定个别存储区，由此阻止或允许写入该存储区。

永久锁定（永久保持不变）口令或存储区的锁定状态。

COMMAND format:

数据区	描述	长度 (byte)
0xEE	帧头	1
帧长度	命令帧长度，不包括帧头和校验字节	2
帧类型	0x04, lock command	1
RF POWER	15~30	1
Sel	0x00:All tag can be inventoried ;ignore SL (default) 0x01:Only inventory tags with SL NOT set 0x02:Only inventory tags with SL SET	1
session	0x00:Use session S0 for inventory 0x01:Use session S1 for inventory 0x02:Use session S2for inventory (default) 0x03:Use session S3 for inventory	1
Target	0x00:Only inventory Tags with inventoried flag set to A for session 0x01:Only inventory Tags with inventoried flag set to B for session (default)	1
Starting Q	由在天线覆盖范围内的 tag 数定	1
Access password	0x00000000 if not application	4
Lock Mask	0b0000 0000 0000 0001 user memory perma lock mask bit 0b0000 0000 0000 0010 user memory pwd/write lock mask bit 0b0000 0000 0000 0100 TID memory perma lock mask bit 0b0000 0000 0000 1000 TID memory pwd/write lock mask bit 0b0000 0000 0001 0000 EPC memory perma lock mask bit 0b0000 0000 0010 0000 EPC memory pwd/write lock mask bit 0b0000 0000 0100 0000 Access pwd memory perma lock mask bit 0b0000 0000 1000 0000 Access pwd memory pwd read/write lock mask bit 0b0000 0001 0000 0000 Kill pwd memory perma lock mask bit 0b0000 0010 0000 0000 Kill pwd memory pwd read/write lock mask bit	2
Lock action	0b0000 0000 0000 0001 user memory perma lock bit 0b0000 0000 0000 0010 user memory pwd/write lock bit 0b0000 0000 0000 0100 TID memory perma lock bit 0b0000 0000 0000 1000 TID memory pwd/write lock bit 0b0000 0000 0001 0000 EPC memory perma lock bit 0b0000 0000 0010 0000 EPC memory pwd/write lock bit	2

	0b0000 0000 0100 0000 Access pwd memory perma lock bit 0b0000 0000 1000 0000 Access pwd memory pwd read/write lock bit 0b0000 0001 0000 0000 Kill pwd memory perma lock bit 0b0000 0010 0000 0000 Kill pwd memory pwd read/write lock bit	
Antenna select	0b0000 0001 Antenna1 0b0000 0010 Antenna2 0b0000 0100 Antenna3 0b0000 1000 Antenna4	1
Crc 校验	2 字节的 crc 校验字节	2

Response format:

数据区	描述	长度 (Byte)
0xEE	帧头	1
帧长度	命令帧长度, 不包括帧头和校验字节	2
0x04	帧类型, lock command	1
Command status	0x00: 命令执行成功 0xFF: 命令执行失败	1
Tag response num	Lock tag 个数 (当前设置为 1)	1
Tag response	被锁定标签 EPC 长度 n	按 word 计算 1
	Pc	2
	Epc	EPC 数据区 N*2
Status code	0x01 0x00 CRC 校验错 0x02 0x00 设置 Tx/Rx 参数错误 0x03 0x00 tag 没响应或者发送超时 0x04 error_code (tag 返回的 error code) 0x05 0x00 天线选择错误 0x06 0x00 Access password 错误 0x07 0x00 RFpower 设置超限	2
Crc 校验	2 字节的 crc 校验字节	2

5.1.6 Kill (0x09)

kill 命令允许 reader 永久禁用标签。

COMMAND format:

数据区	描述	长度 (byte)
0xEE	帧头	1
帧长度	命令帧长度, 不包括帧头和校验字节	2
0x09	帧类型, Kill command	1
RF POWER	15~30	1

Sel	0x00:All tag can be inventoried ;ignore SL(default) 0x01:Only inventory tags with SL NOT set 0x02:Only inventory tags with SL SET	1
session	0x00:Use session S0 for inventory 0x01:Use session S1 for inventory 0x02:Use session S2 for inventory (default) 0x03:Use session S3 for inventory	1
Target	0x00:Only inventory Tags with inventoried flag set to A for session 0x01:Only inventory Tags with inventoried flag set to B for session (default)	1
Starting Q	由在天线覆盖范围内的 tag 数定	1
Access password	0x00000000 if not application	4
Kill password	0x00000000 if not application	4
Antenna select	0b0000 0001 Antenna1 0b0000 0010 Antenna2 0b0000 0100 Antenna3 0b0000 1000 Antenna4	1
Crc 校验	2 字节的 crc 校验字节	2

Response format:

数据区	描述	长度 (Byte)
0xEE	帧头	1
帧长度	命令帧长度, 不包括帧头和校验字节	2
0x09	帧类型, Kill command	1
Command status	0x00: 命令执行成功 0xFF: 命令执行失败	1
Tag response num	Kill tag 个数 (当前设置为 1)	1
Tag response	被 Kill 标签的 EPC 长度 n	按 word 计算长度
	Pc	2
	Epc	EPC 数据区
Status code	0x01 0x00 CRC 校验错 0x02 0x00 设置 Tx/Rx 参数错误 0x03 0x00 tag 没响应或者发送超时	2

	0x04 error_code (tag 返回的 error code) 0x05 0x00 天线选择错误 0x06 0x00 Access password 错误或 Kill password 错误 0x07 0x00 RFpower 设置超限	
Crc 校验	2 字节的 crc 校验字节	2

注：如果 Command status 执行失败，tag response 区忽略。

5.1.7 Set Select (0x06)

添加缓存在 reader 缓冲区中以便选择特定标签群以响应 Inventory 和 Access 过程。Reader 可以设置一个 Select 命令在 Inventory 或 Access 之前选择特定的标签群。select command 保存在 reader 的缓冲区中。Reader 有一个缺省的 select command，参数是 Target = 2、Action = 4、MemBank = 1、Pointer = 0、Length = 0、Mask = 0、Truncate = 0，即所有 tag 均匹配且 Session = 2，Inventoried flag = B。

COMMAND format:

数据区	描述			长 度 (byte)
0xEE	帧头			1
帧长度	命令帧长度，不包括帧头和校验字节			2
0x06	帧类型，set select command			1
Target	0x00: Modify Session S0 Inventoried Flag 0x01: Modify Session S1 Inventoried Flag 0x02: Modify Session S2 Inventoried Flag 0x03: Modify Session S3 Inventoried Flag 0x04 Select SL			1
Action	Action	Matching	Non_Matching	1
	0x00	Assert SL or inventoried -> A	deassert SL or inventoried -> B	
	0x01	Assert SL or inventoried -> A	Do nothing	
	0x02	Do nothing	deassert SL or inventoried -> B	
	0x03	Negate SL or A-> B, B-> A	Assert SL or inventoried ->	

		A	
	0x04	deassert SL or inventoried ->B	Assert SL or inventoried ->A
	0x05	deassert SL or inventoried ->B	Do nothing
	0x06	Do nothing	Assert SL or inventoried ->A
	0x07	Do nothing	Negate SL or A-> B, B-> A
Memory bank	0x00: reserve bank 0x01: epc bank 0x02: Tid bank 0x03: user bank		1
Point	The memory bit address at which to start matching Ms Byte first		2
length	Number of bits to use of Mask Note : 0 implies all tags match		1
mask	Bits to match ,MSbit first		注
Truncate	0x00 :disable truncation		1
Crc 校验	2 字节的 crc 校验字节		2

注：如果 $(length\%8)$ 不等于 0, mask 的长度是 $(length/8+1)$;
如果 $(length\%8)$ 等于 0, mask 的长度是 $(length/8)$ 。
Mask 最长为 32Byte。

Response format:

数据区	描述	长度 (Byte)
0xEE	帧头	1
帧长度	命令帧长度, 不包括帧头和校验字节	2
0x06	帧类型, set select command	1
Command status	0x00: 命令执行成功 0xFF: 命令执行失败	1
Status code	0x01 0x00 CRC 校验错 0x11 0x00 select 缓冲区满	2
Crc 校验	2 字节的 crc 校验字节	2

5.1.8 Reset Select(0x07)

清除 reader 缓冲区中的 select 参数并把 reader 中的 select 参数设置为缺省值。

COMMAND format:

数据区	描述	长 度
-----	----	-----

		(byte)
0xEE	帧头	1
帧长度	命令帧长度, 不包括帧头和校验字节	2
0x07	帧类型, reset select command	1
Crc 校验	2 字节的 crc 校验字节	2

Response format:

数据区	描述	长度 (Byte)
0xEE	帧头	1
帧长度	命令帧长度, 不包括帧头和校验字节	2
0x07	帧类型, reset select command	1
Command status	0x00: 命令执行成功 0xFF: 命令执行失败	1
Status code	0x01 0x00 CRC 校验错	2
Crc 校验	2 字节的 crc 校验字节	2

5.1.9 Set 6C paramater(0x08)

6C 读写器参数设置

数据区	描述	长度 (byte)
0xEE	帧头	1
帧长度	命令帧长度, 不包括帧头和校验字节	2
0x8	帧类型, 读写器参数设置	1
频谱规范	CHN: 1; FCC: 0	1
编码方式	MILLER: 1; FM0: 0	1
调制方式	DSB: 1; PRSK 0	1
发送速率	40K: 0; 80K: 1; 160K: 2	
Crc 校验	2 字节的 crc 校验字节	2

Response format

数据区	描述	长度 (Byte)
0xEE	帧头	1
帧长度	命令帧长度, 不包括帧头和校验字节	2
0x8	帧类型, 读写器参数设置	1
Command status	0x00: 命令执行成功 0xFF: 命令执行失败	1
Status code	0x01 0x00 CRC 校验错 0x10 0x00 当前参数设置不可使用	2
Crc 校验	2 字节的 crc 校验字节	2

5.1.10 TagPowerDown(0x32)

标签下电命令

数据区	描述	长度 (byte)
0xEE	帧头	1
帧长度	命令帧长度, 不包括帧头和校验字节	2
0x32	帧类型, 标签下电设置	1
下电时间	时间长度 (ms)	2
Crc 校验	2 字节的 crc 校验字节	2

Response format

数据区	描述	长度 (Byte)
0xEE	帧头	1
帧长度	命令帧长度, 不包括帧头和校验字节	2
0x32	帧类型, 标签下电设置	1
Command status	0x00: 命令执行成功 0xFF: 命令执行失败	1
Status code	0x01 0x00 CRC 校验错 0x10 0x00 当前参数设置不可使用	2
Crc 校验	2 字节的 crc 校验字节	2

5.2 Status Code

Status code 是 Reader 返回给上位机的错误信息, 有以下几种

- 0x01 0x00 CRC 校验错 (2.1、2.2、2.3)
- 0x02 0x00 设置 Tx/Rx 参数错误 (2.2、2.3)
- 0x03 0x00 tag 没响应或者发送超时 (2.2、2.3)
- 0x04 error_code tag 返回的 error code (2.2)
- 0x05 0x00 天线选择错误 (2.2、2.3)
- 0x06 0x00 Access password 错误或 Kill password 错误 (2.2)
- 0x07 0x00 Rfpower 设置超限 (2.2、2.3)
- 0x08 0x00 检测不到天线信息 (2.1.4、2.1.5)
- 0x09 0x00 写 Flash 错误 (2.1.2)
- 0x10 0x00 当前参数设置不可使用 (2.1.6)
- 0x11 0x00 select 缓冲区满 (2.2.6)
- 0x12 0x00 Test Type 错误 (2.2.8)