CR09 刷卡器

产品手册

版本 v1.0

免责声明

使用产品前请务必认真阅读本《CR09 刷卡器产品手册》中的所有内容，以保障产品安全有效的使用。请勿自行拆卸产品或撕毁设备上的封标，否则我司不承担保修或更换产品的责任。

本手册中的图片仅供参考，如有个别图片与实际产品不符，请以实际产品为准。对于本产品的升级和更新，我司保留随时修改文档而不另行通知的权利。

使用本产品的风险由用户自行承担，在适用法律允许的最大范围内，对因使用或不能使用本产品所产生的损害及风险，包括但不限于直接或间接的个人损害、商业赢利的丧失、贸易中断、商业信息的丢失或任何其它经济损失，我司不承担任何责任。

本手册的一切解释权与修改权归我司所有。

修订记录

变 更 日 期	版 本	版 本 描 述	责 任 人
2022.9.21	V1.0	初始版本	

目录

1. 前言 6
1.1. 产品简介 6
1.2. 产品特点 6
2. 产品外观 7
2.1.1. 外观图 7
2.1.2. 产品尺寸图 8
3. 商品参数 9
3.1. 常规参数 9
3.2. 识读参数 9
3.3. 电气参数 10
3.4. 工作环境 10
4. 连接器 11
4.1. 韦根连接器 11
4.2. 485 连接器 11
4.3. 韦根+485 连接器 12
4.4. 引脚说明 12
5. 安装方法 13
6. 配置指令 14
6.1. 数据传输协议 14
6.1.1. 请求数据格式 14
6.1.2. 应答数据格式 14

6.2. 配置项说明 15
6.3. 配置指令示例 16
6.3.1. 重新配置设备 16
6.3.2. 获取设备配置 16
7. 通信协议 17
7.1. 数据传输协议 17
7.1.1. 请求数据格式 17
7.1.2. 应答数据格式 17
7.2. 协议模式下卡号上报格式 18
7.2.1. 不区分卡类型 18
7.2.2. 区分卡类型 19
7.3. 指令 0x01 设备状态查询 20
7.4. 指令 0x02 获取设备 ID 20
7.5. 指令 0x04 蜂鸣器和 LED 控制 21
7.6. NFC 模块操作 22
7.6.1. 指令 0x53 卡号上报开关 22
7.6.2. 读 M1 卡一块数据 23
7.6.3. 写 M1 卡一块数据 24
7.6.4. 读 M1 卡扇区内多个块 25
7.6.5. 写 M1 卡扇区内多个块 26
7.6.6. 指令 0xA6 发送 APDU 指令 27

1. 前言

感谢使用我司提供的 CR09 刷卡设备。认真阅读本文档，可以帮助您了解此设备功能、特点、以及快速掌握设备的使用、安装方法。

1.1. 产品简介

CR09 刷卡设备是专为门禁刷卡领域研发的一款产品，具备韦根\RS485 两种输出接口，支持韦根 26/34 协议切换。

1.2. 产品特点

1，支持韦根/RS485 两种输出方式

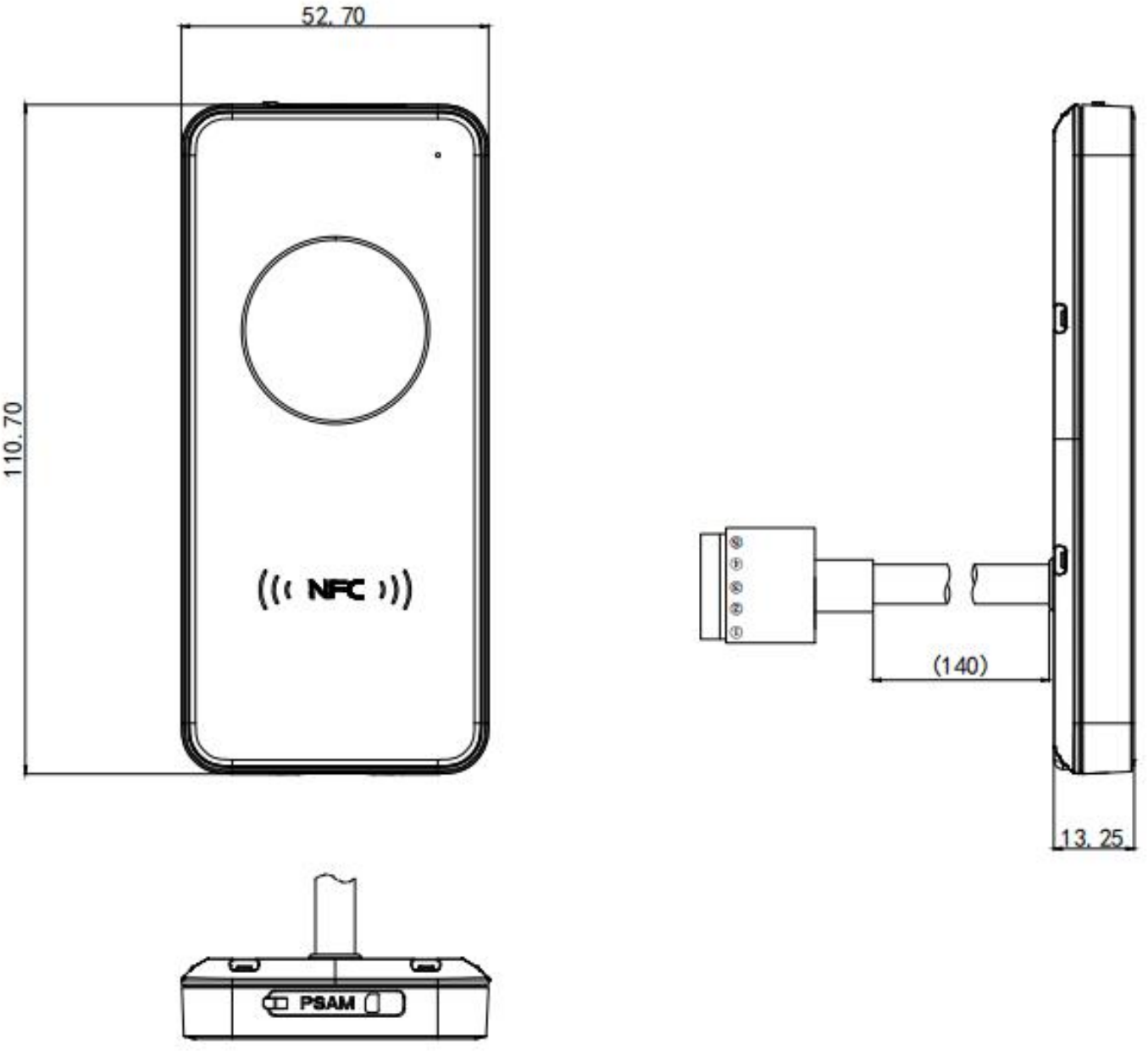
2，支持 PSAM 卡验证

3，86 盒方式安装

2. 产品外观

2.1.1. 外观图

2.1.2. 产品尺寸图



3. 商品参数

3.1. 常规参数

常规参数	
支持接口	RS485、韦根
指示方式	红光、绿光、白光，蓝灯，蜂鸣器
安装方式	壁挂式安装
产品尺寸	110.70mm*52.70mm*13.25mm

3.2. 识读参数

射频卡识读参数	
识别卡类型	ISO 14443A 协议卡、ISO 14443B 协议卡、身份证（仅读取物理卡号）
操作卡方式	读取 UID/读写 M1 卡扇区/PSAM 认证
射频工作频率	13.56MHz
识读有效距离	＜5cm　实际距离与卡片规格有关

3.3. 电气参数

须在连接好设备之后，才允许提供电源输入。如果在线缆带电时接插或拔离设备（带电热插拔），将会损坏其电子部件，请确保在进行线缆插拔时已切断电源。

不良的电源连接、或过短间隔的电源关闭开启操作、或过大的压降脉冲都可能导致设备不能处于稳定正常的工作状态，需保持电源输入的稳定。在关闭电源输入后，需间隔 2 秒以上才可以再次开启电源输入。

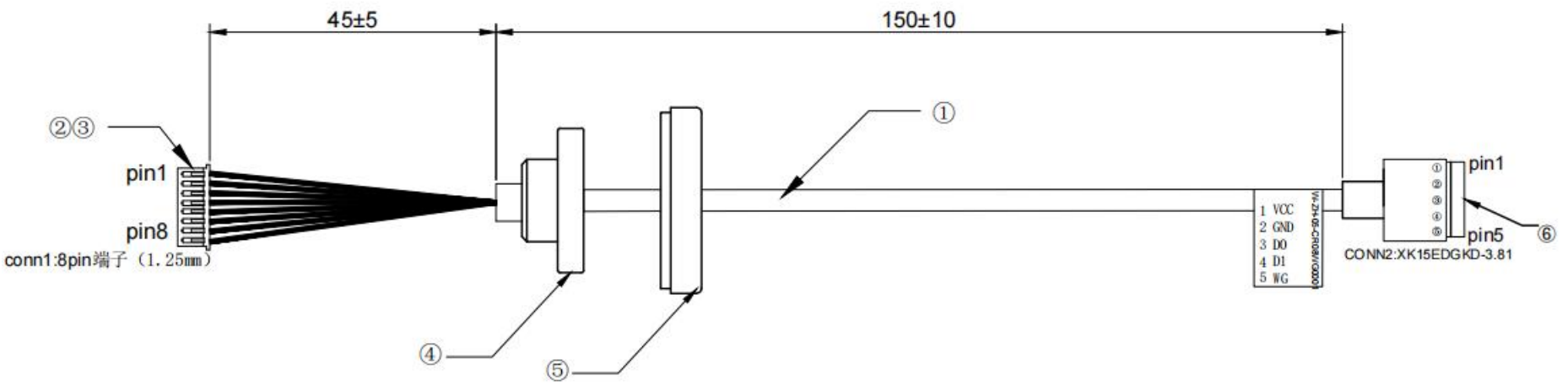
电气参数	
工作电压	DC 5V-15V
工作电流	150mA（典型值 12V供电）
额定功耗	1800mW（典型值 5V 供电）

3.4. 工作环境

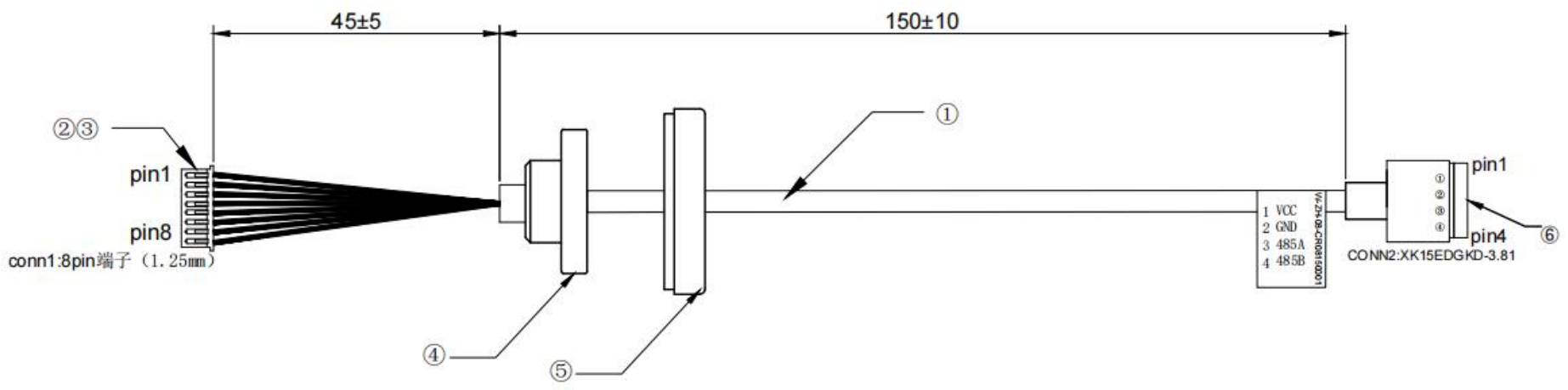
工作环境参数	
静电防护	±15kV（空气放电），±6kV（接触放电）
工作温度	-20° C-70° C
存储温度	-20° C-80° C
相对湿度	5%-95%（无凝结）

4. 连接器

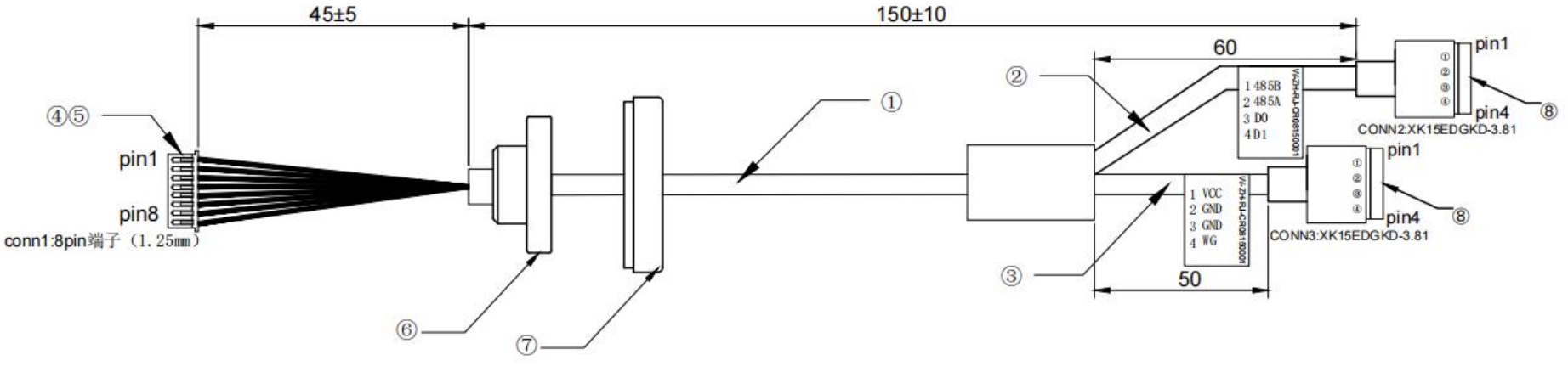
4.1. 韦根连接器



4.2. 485 连接器



4.3. 韦根+485 连接器

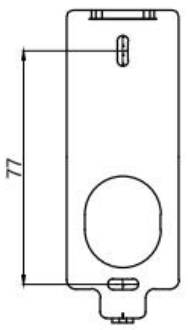
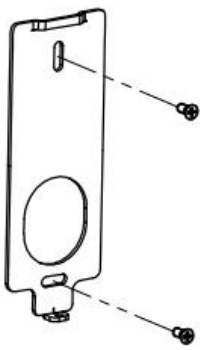
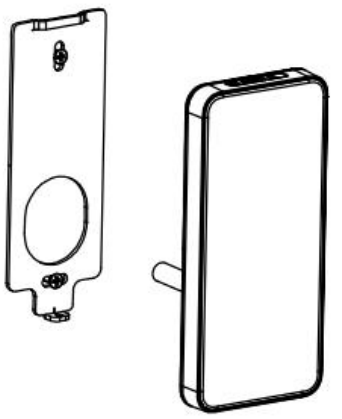
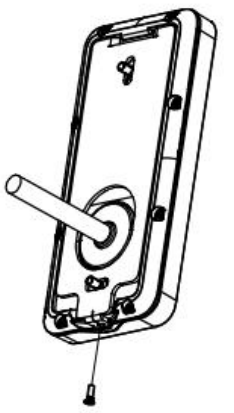


4.4. 引脚说明

引脚定义	引脚说明
VCC	电源正极
GND	电源地
D0	韦根0
D1	韦根1
485A	485A线
485B	485B线
WG	韦根协议设置引脚 悬空：韦根 26 低电平：韦根34

5. 安装方法

射频卡识读天线位于面板下侧，在安装时应避免 10cm 以内无金属和磁性物质，否则会严重降低刷卡性能。

			
第一步：在安装面打孔，放入M3的膨胀管。	第二步：将金属支架用M3螺丝固定在安装面。	第三步：将产品装在支架上。	第四步：使用M2螺丝将设备固定在支架上。

6. 配置指令

6.1. 数据传输协议

6.1.1. 请求数据格式

命令头+ 命令字 + 标识字 + 长度字+ 数据域+ 校验字

命令头：两字节，默认为 0x55，0xAA，可更改

命令字：一字节

长度字：两字节，指明本条命令从长度字后面开始到校验字的字节数（不含效验字），低位在前

数据域：此项可以为空（数据域内容可参考 6.2 表格编写）

校验字：一字节，从命令头到数据域最后一字节的逐字节异或值

6.1.2. 应答数据格式

命令头+ 命令字 + 标识字 + 长度字+ 数据域+ 校验字

命令头：两字节，默认为 0x55，0xAA

命令字：一字节

标识字：一字节， 0x00 则代表成功应答，其它失败或错误

长度字：两字节，指明本条命令从长度字后面开始到校验字的字节数（不含效验字），低位在前

数据域：此项可以为空

校验字：一字节，从命令头到数据域最后一字节的逐字节异或值

6.2. 配置项说明

表格自上而下，即为配置项内容排序，即：指令类型、波特率（默认 115200-8-n-1）、设备号（默认为 1）、灯光配置（包括背光灯、刷卡动作灯）、其他配置、修改包头、前缀、后缀、命令模式获取间隔、输出配置。

<table>
<tr><th>配置项</th><th>数据长度</th><th>说明</th></tr>
<tr><td>指令类型</td><td>1 字节</td><td>0x00：获取设备配置；0x01：按照指令内容重新配置设备</td></tr>
<tr><td>波特率</td><td>4 字节</td><td>波特率 115200 → 00 01 C2 00</td></tr>
<tr><td>设备号</td><td>4 字节</td><td>设备号（目前不生效）</td></tr>
<tr><td>灯光配置</td><td>1 字节</td><td>
<table>
<tr><td colspan="4">背光灯</td><td colspan="4">刷卡动作灯</td></tr>
<tr><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td></tr>
<tr><td>蓝</td><td>绿</td><td>红</td><td>白</td><td>蓝</td><td>绿</td><td>红</td><td>白</td></tr>
</table>
</td></tr>
<tr><td>其他配置</td><td>1 字节</td><td>
<table>
<tr><td>Bit7</td><td>Bit6</td><td>Bit5</td><td>Bit4</td><td>Bit3</td><td>Bit2</td><td>Bit1</td><td>Bit0</td></tr>
<tr><td>区分卡类型</td><td>0x01:主动上报卡号
0x00:命令模式</td><td colspan="4">空</td><td>继电器</td><td>蜂鸣器</td></tr>
</table>
</td></tr>
<tr><td>更改包头</td><td>2 字节</td><td>包头（默认是 0x55 0xaa）
注意：如果修改包头，那以后发送的所有协议，都需要使用修改后的包头</td></tr>
<tr><td>前缀</td><td>3 字节</td><td>
<table>
<tr><td>字节 1</td><td>字节 2</td><td>字节 3</td></tr>
<tr><td>有效长度</td><td>前缀 1</td><td>前缀 2</td></tr>
</table>
</td></tr>
<tr><td>后缀</td><td>3 字节</td><td>
<table>
<tr><td>字节 1</td><td>字节 2</td><td>字节 3</td></tr>
<tr><td>有效长度</td><td>后缀 1</td><td>后缀 2</td></tr>
</table>
</td></tr>
<tr><td>命令模式获取间隔时间</td><td>1 字节</td><td>单位 25 毫秒</td></tr>
<tr><td>输出配置</td><td>1 字节</td><td>
<table>
<tr><td>Bit 7</td><td>Bit 6</td><td>Bit 5</td><td>Bit 4</td></tr>
<tr><td colspan="2">置 0</td><td>以协议模式输出卡号</td><td>输出卡号</td></tr>
<tr><td>Bit 3</td><td>Bit 2</td><td>Bit 1</td><td>Bit 0</td></tr>
<tr><td>反序输出</td><td>字符串输出</td><td>十进制输出</td><td>十六进制 hex 输出</td></tr>
</table>
Bit 7 Bit6 必须置 0；
Bit 5 以通信协议格式输出卡号，参考通信协议说明；
Bit 4 只上传卡号数据；
Bit 2 ~ Bit0 有且仅有一个可以置 1，其他必须置 0；
</td></tr>
</table>

6.3. 配置指令示例

6.3.1. 重新配置设备

设置内容如下：

指令类型 重新配置设备：01

波特率 115200：00 01 C2 00

设备号 1：00 00 00 01

灯光配置 （背光灯）蓝灯常亮，（刷卡动作）闪绿灯：84

其他配置 刷卡响蜂鸣器 主动上报卡号 不区分类型：41

包头 0x55 0xaa：55 AA

无前后缀：00 00 00 00 00 00

命令模式获取间隔 2 秒：50

输出配置 输出卡号（非协议模式） 以十六进制 hex 输出（正序）：11

PC->Reader：55 AA B0 15 00 01 00 01 C2 00 00 00 00 01 84 41 55 AA 00 00 00 00 00 00 50 11 E2

（数据长度为 21，十六进制位 0x15，长度字为两个字节，低位在前，则为 15 00）

Reader->PC：55 AA B0 00 00 00 4F （第四字节 00 代表设置成功，其他值代表失败）

6.3.2. 获取设备配置

PC->Reader：55 AA B0 01 00 00 4E

（当指令类型为 00 时，数据长度只有 1，所以长度字为 01 00）

Reader->PC：55 AA B0 00 15 00 01 00 01 C2 00 00 00 00 01 84 41 55 AA 00 00 00 00 00 00 50 11 E2

（第四字节 00 代表获取成功，其他值代表失败）

7. 通信协议

7.1. 数据传输协议

7.1.1. 请求数据格式

命令头+ 命令字 + 标识字 + 长度字+ 数据域+ 校验字

命令头：两字节，默认为 0x55，0xAA

命令字：一字节

长度字：两字节，指明本条命令从长度字后面开始到校验字的字节数（不含效验字），低位在前

数据域：此项可以为空

校验字：一字节，从命令头到数据域最后一字节的逐字节异或值

7.1.2. 应答数据格式

命令头+ 命令字 + 标识字 + 长度字+ 数据域+ 校验字

命令头：两字节，默认为 0x55，0xAA

命令字：一字节

标识字：一字节， 0x00 则代表成功应答，其它失败或错误

长度字：两字节，指明本条命令从长度字后面开始到校验字的字节数（不含效验字），低位在前

数据域：此项可以为空

校验字：一字节，从命令头到数据域最后一字节的逐字节异或值

7.2. 协议模式下卡号上报格式

7.2.1. 不区分卡类型

指令 0x30 获取结果不区分数据来源

指令： 0x30		上位机端主动轮询或设备端主动上报结果使用此指令			
说明：此指令返回的数据不区分卡类型					
PC->Reader(Send)			Reader->PC(Receive)		
项目	字节	说明	项目	字节	说明
包头	2Byte	Default： 0x55 0xAA	包头	1Byte	Default： 0x55 0xAA
命令字	1Byte	0x30	命令字	1Byte	0x30
数据域长度	2Byte	0x00 0x00	标识字	1Byte	0x00 ： 成功 非 0 ： 失败
数据域	0 Byte	没有此项	数据域长度	2Byte	N
			数据域	N Byte	数据 N = 0 时没有此项
校验字	1Byte		校验字	1Byte	

例：
命令模式下上位机轮询发送该指令获取数据

```
PC-->Reader :55 AA 30 00 00 CF
Reader-->PC :55 AA 30 00 00 00 CF 无数据
Reader-->PC :55 AA 30 00 08 00 37 36 64 30 33 34 39 31 9D 反馈数据
```

7.2.2. 区分卡类型

指令 0x33 获取结果区分卡类型

例：

<table>
<tr><td colspan="3">指令:　0x33</td><td colspan="6">上位机端主动轮询或设备端主动上报结果使用此指令</td></tr>
<tr><td colspan="9">说明: 此指令返回的数据区分卡类型</td></tr>
<tr><td colspan="3">PC->Reader(Send)</td><td colspan="6">Reader->PC(Receive)</td></tr>
<tr><td>项目</td><td>字节</td><td>说明</td><td>项目</td><td>字节</td><td colspan="4">说明</td></tr>
<tr><td>包头</td><td>2Byte</td><td>Default:　0x55 0xAA</td><td>包头</td><td>1Byte</td><td colspan="4">Default:　0x55 0xAA</td></tr>
<tr><td>命令字</td><td>1Byte</td><td>0x33</td><td>命令字</td><td>1Byte</td><td colspan="4">0x33</td></tr>
<tr><td>数据域长度</td><td>2Byte</td><td>0x00 0x00</td><td>标识字</td><td>1Byte</td><td colspan="4">0x00 : 成功
非 0 :　失败</td></tr>
<tr><td rowspan="3">数据域</td><td rowspan="3">0 Byte</td><td rowspan="3">没有此项</td><td>数据域长度</td><td>2 Byte</td><td colspan="4">数据 N = 0 时没有此项</td></tr>
<tr><td rowspan="2">数据域</td><td rowspan="2">N Byte
(数 据　N = 0 时没有此项)</td><td>数据区分标志</td><td>1 Byte</td><td colspan="2">0x40:　NFC 卡</td></tr>
<tr><td>结果</td><td>X Byte</td><td colspan="2">结果</td></tr>
<tr><td>校验字</td><td>1Byte</td><td></td><td>校验字</td><td>1Byte</td><td colspan="4"></td></tr>
</table>

例：

命令模式下上位机轮询发送该指令获取数据（蓝色--卡类型，红色--数据）

PC-->Reader :55 AA 33 00 00 CC

Reader-->PC :55 AA 33 00 00 00 CC 无数据

Reader-->PC :55 AA 33 00 09 00 40 37 64 39 30 64 61 36 31 DD 刷卡数据

7.3. 指令 0x01 设备状态查询

指令： 0x01					
说明：标识字 00 表示设备正常；非 0 不正常					
PC->Reader(Send)			Reader->PC(Receive)		
项目	字节	说明	项目	字节	说明
包头	2Byte	Default: 0x55 0xAA	包头	1Byte	Default: 0x55 0xAA
命令字	1Byte	0x01	命令字	1Byte	0x01
数据域长度	2Byte	0x00 0x00	标识字	1Byte	0x00 : 成功； 非 0 : 失败
数据域	0Byte	无此项	数据域长度	2Byte	N
			数据域	N Byte	数据 N = 0 时没有此项
校验字	1Byte		校验字	1Byte	

例：

PC-->Reader :55 AA 01 00 00 FE
Reader-->PC :55 AA 01 00 02 00 55 AA 03

7.4. 指令 0x02 获取设备 ID

指令： 0x02					
说明：第六章设置指令设置的 ID					
PC->Reader(Send)			Reader->PC(Receive)		
项目	字节	说明	项目	字节	说明
包头	2Byte	Default: 0x55 0xAA	包头	1Byte	Default: 0x55 0xAA
命令字	1Byte	0x02	命令字	1Byte	0x02
数据域长度	2Byte	0x00 0x00	标识字	1Byte	0x00 : 成功；非 0 : 失败
数据域	0Byte	无此项	数据域长度	2Byte	N
			数据域	N Byte	N > 0 设备 ID, 低位在前
校验字	1Byte		校验字	1Byte	

例：

PC-->Reader :55 AA 02 00 00 FD
Reader-->PC :55 AA 02 00 04 00 80 00 00 00 79
红色部分代表设备 ID, 低位在前，80000000 代表设备 id 为 128

7.5. 指令 0x04 蜂鸣器和 LED 控制

<table>
<tr><td colspan="3">指令： 0x04</td><td colspan="3"></td></tr>
<tr><td colspan="6">说明：确认设备有相应颜色的灯</td></tr>
<tr><td colspan="3">PC->Reader(Send)</td><td colspan="3">Reader->PC(Receive)</td></tr>
<tr><td>项目</td><td>字节</td><td colspan="2">说明</td><td>项目</td><td>字节</td><td>说明</td></tr>
<tr><td>包头</td><td>2Byte</td><td colspan="2">Default： 0x55 0xAA</td><td>包头</td><td>1Byte</td><td>Default： 0x55 0xAA</td></tr>
<tr><td>命令字</td><td>1Byte</td><td colspan="2">0x04</td><td>命令字</td><td>1Byte</td><td>0x04</td></tr>
<tr><td>数据域长度</td><td>2Byte</td><td colspan="2">0x05 0x00</td><td>标识字</td><td>1Byte</td><td>0x00 ： 成功
非 0 ： 失败</td></tr>
<tr><td rowspan="5">数据域</td><td rowspan="5">5Byte</td><td>1 Byte</td><td>开关：0 关闭，1 使能
bit0： 保留
bit1： 红灯控制位
bit2： 绿灯控制位
bit3： 蜂鸣器控制位
bit4： 蓝灯控制位</td><td>数据域长度</td><td>2Byte</td><td>N</td></tr>
<tr><td>1 Byte</td><td>次数</td><td rowspan="4">数据域</td><td rowspan="4">NByte</td><td rowspan="4">数据 N = 0 时没有此项</td></tr>
<tr><td>1 Byte</td><td>每次持续时间(单位 50MS)</td></tr>
<tr><td>1 Byte</td><td>每次间隔时间(单位 50MS)</td></tr>
<tr><td>1 Byte</td><td>保留</td></tr>
<tr><td>校验字</td><td>1Byte</td><td colspan="2"></td><td>校验字</td><td>1Byte</td><td></td></tr>
</table>

例：每次闪亮 0x50*50ms（十进制 80）间隔 0x0A*50 ms（十进制 10）

55 AA 04 05 00 02 03 50 0A 00 A5　控制红灯闪亮三次，时间 4 秒，间隔 0.5s
55 AA 04 05 00 08 03 50 0A 00 AF　蜂鸣器响三次，时间 4 秒，间隔 0.5s
55 AA 04 05 00 04 03 50 0A 00 A3　控制绿灯闪亮 三次，时间 4 秒，间隔 0.5s
55 AA 04 05 00 0A 03 50 0A 00 AD　红灯蜂鸣器动作，时间 4 秒，间隔 0.5s
55 AA 04 05 00 0C 03 50 0A 00 AB　绿灯 蜂鸣器动作，时间 4 秒，间隔 0.5s
55 AA 04 05 00 06 03 50 0A 00 A1　红绿闪三次，时间 4 秒，间隔 0.5s
55 AA 04 05 00 0E 03 50 0A 00 A9　红绿灯蜂鸣器动作三次，时间 4 秒，间隔 0.5s
55 AA 04 05 00 18 03 50 0A 00 BF　蓝灯蜂鸣器动作三次，时间 4 秒，间隔 0.5s

7.6. NFC 模块操作

NFC 模块可支持 Mifare One 卡块读写、CPU 卡发送 APDU 指令，详见具体指令。
名词解释：
任务启动标志位--该标志位用于告知扫码器何时开始卡的操作，何时结束卡的操作，或告知扫码器操作卡的指令是独立的，无指令间依赖关系。
该标志位用来设置卡片的操作环境，标志位的值有以下三种：
0x00->AUTO 告知扫码器该指令可单独执行，无指令间的依赖关系。
0x01->START 告知扫码器开始对卡操作或对卡操作尚未结束，且指令间可能存在依赖关系。
0x02->FINISH 告知扫码器本条指令是操作卡的最后一条指令，将卡片操作环境恢复到默态。
若操作卡的指令是独立的，如读写 M1 卡的某块数据，则该标志位即可设置为 AUTO 也可设置为 FINISH。

1、若使用 START 标识开始操作卡片，则必须使用 FINISH 标识结束操作，否则会导致 NFC 模块工作异常，需重启后才可再次使用。
2、若卡片操作过程中涉及多条卡片操作指令，则过程中所发指令的任务启动标志位均为 START，最后一条指令标记为 FINISH。

7.6.1. 指令 0X53 卡号上报开关

<table>
<tr><td colspan="3">指令： 0x53</td><td colspan="3"></td></tr>
<tr><td colspan="6">说明：数据域的值设置为 0x01 或 0x00 时（即进入或退出命令模式），均为空操作且扫描器回复成功。目的用于兼容 v2.10 版本通讯协议
注：默认卡号上报功能开启，若关闭卡号上报功能，则协议工作在任何模式下均得不到卡号。此时扫码器多用于直接读写 M1 卡或操作 CPU 卡，而无需得到卡号。</td></tr>
<tr><td colspan="3">PC->Reader(Send)</td><td colspan="3">Reader->PC(Receive)</td></tr>
<tr><td>项目</td><td>字节</td><td>说明</td><td>项目</td><td>字节</td><td>说明</td></tr>
<tr><td>包头</td><td>2Byte</td><td>Default: 0x55 0xAA</td><td>包头</td><td>1Byte</td><td>Default: 0x55 0xAA</td></tr>
<tr><td>命令字</td><td>1Byte</td><td>0x53</td><td>命令字</td><td>1Byte</td><td>0x53</td></tr>
<tr><td>数据域长度</td><td>2 Byte</td><td>0x01 0x00</td><td>标识字</td><td>1Byte</td><td>0x00 ： 成功
非 0 ： 失败</td></tr>
<tr><td rowspan="2">数据域</td><td rowspan="2">1 Byte</td><td rowspan="2">0x01：模块进入命令模式
0x00：模块退出命令模式
0x02：刷卡上报
0x03：关闭上报</td><td>数据域长度</td><td>2 Byte</td><td>N</td></tr>
<tr><td>数据域</td><td>N Byte</td><td>数据 N = 0 时没有此项</td></tr>
<tr><td>校验字</td><td>1 Byte</td><td></td><td>校验字</td><td>1 Byte</td><td></td></tr>
</table>

例：
PC-->Reader :55 AA 53 01 00 02 AF 使能卡号上报
PC-->Reader :55 AA 53 01 00 03 AE 关闭卡号上报
Reader-->PC :55 AA 53 00 00 00 AC

7.6.2. 读 M1 卡一块数据

<table>
<tr><td colspan="3">指令: 0x51</td><td colspan="4">读取 M1 卡某块</td></tr>
<tr><td colspan="7">说明: 任务启动标志字段可选，当指令中不包含该标志位时，默认按 AUTO 标识执行</td></tr>
<tr><td colspan="4">PC->Reader(Send)</td><td colspan="3">Reader->PC(Receive)</td></tr>
<tr><td>项目</td><td>字节</td><td colspan="3">说明</td><td>项目</td><td>字节</td><td>说明</td></tr>
<tr><td>包头</td><td>2Byte</td><td colspan="3">Default: 0x55 0xAA</td><td>包头</td><td>1Byte</td><td>Default: 0x55 0xAA</td></tr>
<tr><td>命令字</td><td>1Byte</td><td colspan="3">0x51</td><td>命令字</td><td>1Byte</td><td>0x51</td></tr>
<tr><td>数据域长度</td><td>2 Byte</td><td colspan="3">N</td><td>标识字</td><td>1Byte</td><td>0x00 : 成功
非 0 : 失败</td></tr>
<tr><td rowspan="4">数据域</td><td rowspan="4">N Byte</td><td>密钥类型</td><td>1Byte</td><td>0x60 -> KEY A
0x61 -> KEY B</td><td rowspan="2">数据域长度</td><td rowspan="2">2 Byte</td><td rowspan="2">N</td></tr>
<tr><td>块号</td><td>1 Byte</td><td>0 ~ 0xFF</td></tr>
<tr><td>密钥</td><td>6 Byte</td><td></td><td rowspan="2">数据域</td><td rowspan="2">N Byte</td><td rowspan="2">数据 N = 0 时没有此项</td></tr>
<tr><td>任务启动标志位(可选)</td><td>1 Byte</td><td>0x00 -> AUTO
0x01 -> START
0x02 -> FINISH</td></tr>
<tr><td>校验字</td><td>1 Byte</td><td colspan="3"></td><td>校验字</td><td>1Byte</td><td></td></tr>
</table>

例：
用 A（0x60）密钥做认证，读取 6 扇区第二块(即绝对块号为 0x19）数据。
认证密钥为 FF FF FF FF FF FF,标志位选配。
PC-->Reader :55 AA 51 09 00 60 19 FF FF FF FF FF FF 00 DE 包含标志位
PC-->Reader :55 AA 51 08 00 60 19 FF FF FF FF FF FF DF 无标志位
Reader-->PC :55 AA 51 00 10 00 12 34 56 78 90 12 34 56 78 90 12 34 56 78 90 12 34 读卡成功
Reader-->PC :55 AA 51 FF 00 00 51 失败或无卡

7.6.3. 写 M1 卡一块数据

<table>
<tr><td colspan="3">指令: 0x52</td><td colspan="4">向 M1 卡某块写数据</td></tr>
<tr><td colspan="7">说明: 任务启动标志字段可选，当指令中不包含该标志位时，默认按 AUTO 标识执行</td></tr>
<tr><td colspan="3">PC->Reader(Send)</td><td colspan="4">Reader->PC(Receive)</td></tr>
<tr><td>项目</td><td>字节</td><td colspan="3">说明</td><td>项目</td><td>字节</td><td>说明</td></tr>
<tr><td>包头</td><td>2 Byte</td><td colspan="3">Default: 0x55 0xAA</td><td>包头</td><td>1Byte</td><td>Default: 0x55 0xAA</td></tr>
<tr><td>命令字</td><td>1 Byte</td><td colspan="3">0x52</td><td>命令字</td><td>1Byte</td><td>0x52</td></tr>
<tr><td>数据域长度</td><td>2 Byte</td><td colspan="3">N</td><td>标识字</td><td>1Byte</td><td>0x00 : 成功
非 0 : 失败</td></tr>
<tr><td rowspan="5">数据域</td><td rowspan="5">N Byte</td><td>密钥类型</td><td>1 Byte</td><td>0x60 -> KEY A
0x61 -> KEY B</td><td rowspan="2">数据域长度</td><td rowspan="2">2Byte</td><td rowspan="2">N</td></tr>
<tr><td>块号</td><td>1 Byte</td><td>0 ~ 0xFF</td></tr>
<tr><td>密钥</td><td>6 Byte</td><td></td><td rowspan="4">数据域</td><td rowspan="4">NByte</td><td rowspan="4">数据 N = 0 时没有此项</td></tr>
<tr><td>数据</td><td>16 Byte</td><td></td></tr>
<tr><td>任务标志位(可选)</td><td>1 Byte</td><td>0x00 -> AUTO
0x01 -> START
0X02 -> FINISH</td></tr>
<tr><td>校验字</td><td>1 Byte</td><td colspan="3"></td><td>校验字</td><td>1Byte</td><td></td></tr>
</table>

例：
用 B（0x61）密钥做认证，向 6 扇区第二块(即绝对块号为 0x19）写数据。
认证密钥为 FF FF FF FF FF FF,标志位选配。
PC-->Reader :55 AA 52 19 00 61 19 FF FF FF FF FF FF 11 11 11 11 11 11 11 11 22 22 22 22 22 22 22 22 00 CC 包含标志位
PC-->Reader :55 AA 52 18 00 61 19 FF FF FF FF FF FF 12 34 56 78 90 12 34 56 12 34 56 78 90 12 34 56 CD 无标志位
Reader-->PC :55 AA 52 00 00 00 AD 写数据成功
Reader-->PC :55 AA 52 FF 00 00 52 失败或无卡

7.6.4. 读 M1 卡扇区内多个块

指令： 0xA0	读 M1 卡扇区内多个块

说明： 可读 S50/S70 卡，扇区号、偏移、块数的取值根据卡片类型而定
偏移--以选取的扇区 0 块为起始地址计算待读块的基地址。
块数--以选定的基地址块为读卡开始块，连续读取选中的块数。
命令解析：
读取一张卡的 2 扇区 1 块和 2 块数据
55 AA A0 0B 00 00 60 02 01 02 FF FF FF FF FF FF 35

55 AA	A0	0B 00	00	60	02	01	02	FF ~FF	35
命令头	指令	数据长度	AUTO	密钥类型	扇区号	待读块基地址	从基地址开始连续读几块	密钥	校验字

注：读取的块数不可为 0，若为 0 视为无效指令；一条指令中不可跨扇区读取块数据

PC->Reader(Send)					Reader->PC(Receive)		
项目	字节	说明			项目	字节	说明
包头	2Byte	Default: 0x55 0xAA			包头	1Byte	Default: 0x55 0xAA
命令字	1Byte	0xA0			命令字	1Byte	0x51
数据域长度	2Byte	N			标识字	1Byte	0x00 : 成功；非 0 : 失败
数据域	11 Byte	任务标志位	1 Byte	0x00 -> AUTO 0x01 -> START 0x02 -> FINISH	数据域长度	2Byte	N
		密钥类型	1 Byte	0x60 -> KEY A 0x61 -> KEY B			
		扇区号	1 Byte	S50 -> 0x00~0x0F S70 -> 0x00~0x27			
		偏移	1 Byte	S50 -> 0x00~0x03 S70 -> 0x00~0x03 或 0x00~0x0F	数据域	NByte	数据 N = 0 时没有此项
		块数	1Byte	S50 -> 0x01~0x04 S70 -> 0x01~0x04 或 0x01~0x10			
		密钥	6 Byte				
校验字	1Byte				校验字	1Byte	

例：
用 A（0x60）密钥做认证，读取 2 扇区 0 块、1 块、2 块数据，即以 0 块为基地址连续读 3 块。
认证密钥为 FF FF FF FF FF FF,标志位设置为 AUTO。
PC-->Reader :55 AA A0 0B 00 00 60 02 00 03 FF FF FF FF FF FF 35
Reader-->PC :55 AA A0 00 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6F 读数据成功
Reader-->PC :55 AA A0 FF 00 00 A0 失败或无卡

7.6.5. 写 M1 卡扇区内多个块

指令： 0xA1	写多块数据

说明： 可读 S50/S70 卡，扇区号、偏移、块数的取值根据卡片类型而定
偏移--以选取的扇区 0 块为起始地址计算待写块的基地址。
块数--以选定的基地址块为写卡开始块，连续写数据到选中的块数。
命令解析:
写数据到一张卡的 2 扇区 1 块和 2 块（指令详见示例）
55 AA A1 2B 00 00 60 02 01 02 FF FF FF FF FF FF 36

55 AA	A1	2B 00	00	60	02	01	02	FF ~FF	... ...	36
命令头	指令	数据长度	AUTO	密钥类型	扇区号	待写块基地址	从基地址开始连续写几块	密钥	待写数据	检验字

注：待写入的块数不可为 0，若为 0 视为无效指令；一条指令中不可跨扇区写入数据

PC->Reader(Send)					Reader->PC(Receive)		
项目	字节	说明			项目	字节	说明
包头	2 Byte	Default: 0x55 0xAA			包头	1 Byte	Default: 0x55 0xAA
命令字	1 Byte	0xA1			命令字	1 Byte	0xA1
数据域长度	2 Byte	N			标识字	1 Byte	0x00:成功；非 0:失败
数据域	N Byte	任务标志位	1 Byte	0x00 -> AUTO 0x01 -> START 0X02 -> FINISH	数据域长度	2 Byte	N
		密钥类型	1 Byte	0x60 -> KEY A 0x61 -> KEY B			
		扇区号	1 Byte	S50 -> 0x00~0x0F S70 -> 0x00~0x27			
		偏移	1 Byte	S50 -> 0x00~0x03 S70 -> 0x00~0x03 或 0x00~0x0F	数据域	0 Byte	数据 N = 0 时没有此项
		块数	1Byte	S50 -> 0x01~0x04 S70 -> 0x01~0x04 或 0x01~0x10			
		密钥	6 Byte				
		数据	N Byte	N = 16 * 块数			
校验字	1 Byte				校验字	1 Byte	

例：
用 A（0x60）密钥做认证，向 2 扇区 1 块、2 块写入数据，即以 1 块为基地址连续写 2 块。
认证密钥为 FF FF FF FF FF FF,标志位设置为 AUTO。
PC-->Reader :55 AA A1 2B 00 00 60 02 01 02 FF FF FF FF FF FF 11 11 11 11 11 11 11 11 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 33 33 33 33 33 33 33 33 33 36
例 2：
55 AA A1 2B 00 00 60 02 01 02 FF FF FF FF FF FF 44 44 44 44 44 44 44 44 44 55 55 55 55 55 55 55 55 55 55 55 55 55 55 66 66 66 66 66 66 66 66 66 36
Reader-->PC : 55 AA A1 00 00 00 5E 写数据成功
Reader-->PC :55 AA A1 FF 00 00 A1 失败或无卡

7.6.6. 指令 0XA6 发送 APDU 指令

<table>
<tr><td colspan="3">指令： 0xA6</td><td colspan="4"></td></tr>
<tr><td colspan="7">说明： 用于与 CPU 卡之间进行通信，APDU 指令可参见《FMCOS2.0 用户手册》</td></tr>
<tr><td colspan="4">PC->Reader(Send)</td><td colspan="3">Reader->PC(Receive)</td></tr>
<tr><td>项目</td><td>字节</td><td colspan="3">说明</td><td>项目</td><td>字节</td><td>说明</td></tr>
<tr><td>包头</td><td>2 Byte</td><td colspan="3">Default: 0x55 0xAA</td><td>包头</td><td>1 Byte</td><td>Default: 0x55 0xAA</td></tr>
<tr><td>命令字</td><td>1 Byte</td><td colspan="3">0xA6</td><td>命令字</td><td>1 Byte</td><td>0xA6</td></tr>
<tr><td>数据域长度</td><td>2 Byte</td><td colspan="3">N</td><td>标识字</td><td>1 Byte</td><td>0x00 ： 成功
非 0 ： 失败</td></tr>
<tr><td rowspan="2">数据域</td><td rowspan="2">N Byte</td><td>任务标志位</td><td>1 Byte</td><td>0x01 -> START
0X02 -> FINISH</td><td rowspan="2">数据域长度</td><td rowspan="2">2 Byte</td><td rowspan="2">N</td></tr>
<tr><td>APDU DATA</td><td>N Byte</td><td>符合 ISO7816-4 的数据结构</td></tr>
<tr><td>数据域</td><td>N Byte</td><td>数据 N = 0 时没有此项</td></tr>
<tr><td>校验字</td><td>1 Byte</td><td colspan="3"></td><td>校验字</td><td>1 Byte</td><td></td></tr>
</table>

例：红色字体部分为 APDU 指令
选择应用目录：
PC-->Reader :55 AA A6 08 00 01 00 A4 00 00 02 3F 01 C8
Reader-->PC : 55 AA A6 00 11 00 6F 0D 84 05 41 44 46 30 31 A5 04 9F 08 01 02 90 00 4C

获取 4 位随机数：
Reader-->PC : 55 AA A6 06 00 01 00 84 00 00 04 DE
Reader-->PC :55 AA A6 00 06 00 7C C9 56 38 90 00 14

外部认证:四位随机数用于外部认证，认证方式为 DES 单倍长，默认密钥（1122334455667788）
PC-->Reader :55 AA A6 0E 00 01 00 82 00 00 08 71 7E B1 7D 4C F6 81 17 33
Reader-->PC : 55 AA A6 00 02 00 90 00 CB

选择二进制文件：
PC-->Reader :55 AA A6 06 00 02 00 B0 83 00 00 6E
Reader-->PC : 55 AA A6 00 12 00 11 22 33 44 55 66 77 88 00 00 00 00 00 00 00 00 90 00 53