

# 目录

1. 链路层通讯数据包定义.....	2
2. 数据单元格式.....	2
2.1. 命令单元格式.....	2
2.2. 应答单元格式.....	2
3. 读写器操作指令.....	3
3.1. 管理操作指令.....	3
3.1.1. 通讯参数设置.....	3
3.1.2. 软复位读写器.....	3
3.1.3. 蜂鸣器控制.....	4
3.1.4. LED 灯控制.....	4
3.1.5. 读版本号.....	4
3.2. 卡操作指令.....	5
3.2.1. 判断接触式卡片状态.....	5
3.2.2. 接触式卡片上电.....	5
3.2.3. 接触式卡片下电.....	5
3.2.4. 激活非接触式卡.....	6
3.2.5. 设置非接触式卡片为halt 状态.....	6
3.2.6. 关闭非接天线.....	7
3.2.7. 应用层命令传输.....	7
3.2.8. 设置接触式存储卡种类.....	8
3.2.9. 识别接触式存储卡种类.....	8
3.2.10. 接触式存储卡密钥初始化.....	8
3.2.11. 接触式存储卡密码校验.....	8
3.2.12. 接触式存储卡读数据.....	8
3.2.13. 接触式存储卡写数据.....	9
3.2.14. 激活非接触式存储卡.....	9
3.2.15. 非接触式存储卡认证扇区.....	9
3.2.16. 非接触式存储卡读块.....	9
3.2.17. 非接触式存储卡写块.....	10
3.2.18. 非接触式存储卡读值块.....	10
3.2.19. 非接触式存储卡写值块.....	10
3.2.20. 非接触式存储卡充值.....	10
3.2.21. 非接触式存储卡减值.....	11
3.2.22. 非接触式存储卡写主密钥.....	11
3.2.23. 设置非接触式存储卡种类.....	11
附录 A（支持的接触式存储卡种类、型号） .....	12
附录 B（支持的非接触式存储卡种类、型号） .....	13

# 1. 链路层通讯数据包定义

序号	内容	长度（字节）	说明
1	数据包头（STX）	1	常量：0x02
2	数据单元长度（Data_len）	2	需传输的数 据单元Data 部分的长度，高字节在前，低字节在后，以16 进制表示。 例如：0x0010 表示Data 部分有16 个字节。
3	需传输的数据单元（Data）	Data_len	数据单元长度由Data_len定义，本数据单元头两个字节是命令码（终端发送命令到读写器）或状态码（读写器返回数据给终端），后面是其它参数
4	冗余检验值（LRC）	1	Data 部分数据各字节异或值
5	数据包尾（ETX）	1	常量：0x03

传输中，数据包中除了数据包头（STX）和数据包尾（ETX），其它部分都要进行字节拆分，每个字节拆分高 4 位、低 4 位两部分，分别加上 0x30，形成两个字节。

## 2. 数据单元格式

### 2.1. 命令单元格式

项目	长度	说明
CommandH	1字节	字节命令类别
CommandL	1字节	字节命令代码
参数	不定长	命令参数

注：

定义命令分类

30H 通讯参数设置命令

31H 读写器功能命令

32H 卡片操作命令

33H 逻辑操作命令

### 2.2. 应答单元格式

项目	长度	说明
----	----	----

StatusH	1字节	状态码高字节
StatusL	1字节	状态码低字节
数据	不定长	回应数据

### 3. 读写器操作指令

#### 3.1. 管理操作指令

##### 3.1.1. 通讯参数设置

命令数据单元		
标识	内容	说明
CommandH	30H	功能命令类别
CommandL	01H	设置串口通讯波特率

功能模块	1 字节	00H: 接触式 01H: 非接触式
串口波特率	1 字节	00H: 9600bps 01H: 19200bps 02H: 38400bps 03H: 57600bps 04H: 115200bps

应答数据单元		
标识	内容	说明
Status	00H, 00H	波特率设置成功
Status	00H, 01H	读写器不支持该串口波特率

**波特率 115200bps 是 JSC280 默认速率**，设备对其它串口通讯速率也支持。

注：波特率设置完成后掉电仍保存。

JSC280 集成非接与接触式，因此 JSC280 设置波特率不区别非接或接触

##### 3.1.2. 软复位读写器

命令数据单元		
31H, 12H		
功能模块	1 字节	00H: 接触式 01H: 非接触式

应答数据单元		
00H,00H 命令执行正确		

说明：操作成功之后，设备整机复位；

对于 JSC280 而言，集成接触式与非接式，因此二者软复位，都同样能使设备整机复位。

指令示例:

**SEND:** 02 30303033 33313132 3030 3233 03

**REC:** 02 30303032 30303030 3030 03

### 3.1.3. 蜂鸣器控制

命令数据单元

31H, 13H

DelayTime 2 字节 蜂鸣器鸣叫时间

Times 1 字节 蜂鸣器鸣叫次数

应答数据单元

00H,00H 命令执行正确

蜂鸣器鸣叫时间单位 100 毫秒。

DelayTime 的 2 个字节中第一字节是一次鸣叫持续时间，第二字节是一次鸣叫停止时间。

指令示例: (蜂鸣 2 次)

**SEND:** 02 30303035 33313133 303130313032 3230 03

**REC:** 02 30303032 30303030 3030 03

### 3.1.4. LED 灯控制

命令数据单元

31H, 14H

LED 选择 1 字节 位 7 对应绿灯; 位 6 对应红灯;

控制选择 1 字节 0 开; 1 灭

应答数据单元

00H,00H 命令执行正确

指令示例: (红灯亮)

**SEND:** 02 30303034 33313134 34303030 3635 03

**REC:** 02 30303032 30303030 3030 03

说明: 此处提到的红灯指的是 JSC280 板载指示灯, 当操作卡片时, 会有自动指示作用  
(操作前亮, 操作结束后灭)

### 3.1.5. 读版本号

命令数据单元

F1H, 00H

应答数据单元

00H,00H 命令执行正确

数据 (2 字节)

指令示例:

**SEND:** 02 30303032 3F313030 3F31 03

**REC:** 02 30303034 30303030 30313031 3030 03

说明: 数据域为: 01 01

## 3.2. 卡操作指令

### 3.2.1. 判断接触式卡片状态

命令数据单元		
32H, 21H		
CardNo	1 字节	接触式用户卡: 00H, PSAM 卡: 10H-12H
应答数据单元		
10H,01H	不支持接触式用户卡	
10H,02H	接触式用户卡未插到位	
10H,03H	接触式用户卡已上电	
10H,04H	接触式用户卡未上电	
20H,01H	不支持 PSAM 卡	
20H,03H	PSAM 卡已上电	
20H,04H	PSAM 卡未上电	

### 3.2.2. 接触式卡片上电

命令数据单元		
32H, 22H		
DelayTime	2 字节	等待插卡时间（单位：20 毫秒），0:无需等待，无卡直接返回，低位字节有效，高位字节保留
CardNo	1 字节	接触式用户卡：00H， PSAM 卡：10H-12H
成功应答数据单元		
00H,00H		
ATR	卡上电成功，返回 ATR	
其它应答数据单元		
10H,01H	不支持接触式用户卡	
10H,02H	接触式用户卡未插到位	
10H,05H	接触式用户卡上电失败	
20H,01H	不支持 PSAM 卡	
20H,05H	PSAM 卡上电失败	

指令示例: (2000MS 内)

SEND: 02 30303035 33323232 303036343030 3734 03

REC: 02 30 30 30 32 31 30 30 32 31 32 03 (10H,02H 接触式用户卡未插到位)

### 3.2.3. 接触式卡片下电

命令数据单元		
32H, 23H		
CardNo	1 字节	接触式用户卡: 00H, PSAM 卡: 10H-12H
成功应答数据单元		
00H,00H		
其它应答		

---

10H,01H	不支持接触式用户卡
20H,01H	不支持 PSAM 卡

### 3.2.4. 激活非接触式卡

命令数据单元

32H, 24H

DelayTime	2 字节	等待卡进入感应区时间（单位：毫秒），高位字节在前
		0:无需等待，无卡直接返回

成功应答数据单元

00H,00H

Type	1 字节	0AH A 类卡; 0BH B 类卡
UIDLen	1 字节	卡 UID 长度
UID	4 字节	卡 UID
AtrLen	1 字节	ATR 长度
ATR		卡上电成功，返回 ATR

其它应答

30H,01H	不支持非接触用户卡
30H,05H	非接触用户卡激活失败
30H,06H	等待卡进入感应区超时
30H,09H	有多张卡在感应区

指令示例: (15S 内)

SEND: 02 30303034 33323234 333A3938 3B34 03

REC:

02 3030313C 30303030

303A3034383F323B3B35313B3133331333738383038303032383033331383036363B303834303C3  
031363E30313833303039303030 363C 03

解析: 数据域 0000 0A048F2BB51B13137880800280318066B0840C016E0183009000

0000 状态

0A: 代表 A 卡

04 : UID 长度

8F2BB51B: UID 数据

13 : ATR 长度

137880800280318066B0840C016E0183009000 : ATR 数据

### 3.2.5. 设置非接触式卡片为 halt 状态

命令数据单元

32H, 25H

DelayTime	2 字节	等待卡离开感应区时间（单位：毫秒），高位字节在前
		0:无需等待
		0xffff:一直等待

成功应答数据单元

00H,00H

其它应答

30H,01H      不支持非接触用户卡

30H,06H      等待卡离开感应区超时

30H,08H      设置卡 Halt 状态失败

**说明：**此设置只是检测卡片是否离开感应区，直到离开感应区才返回成功状态

### 3.2.6. 关闭非接天线

关闭非接的天线。

命令数据单元

C0H, 03H

成功应答数据单元

00H,00H

### 3.2.7. 应用层命令传输

命令数据单元

32H, 26H

CardNo      1 字节      非接触式卡：FFH，接触式卡：00H，PSAM 卡：  
10H-12H

C-APDU      APDU 数据域

成功应答数据单元

00H,00H

R-APDU

其它应答

10H,01H      不支持接触式用户卡

10H,02H      接触式用户卡未插到位

10H,04H      接触式用户卡未上电

10H,06H      操作接触式用户卡数据无回应

10H,07H      操作接触式用户卡数据出现错误

20H,01H      不支持 PSAM 卡

20H,04H      PSAM 卡未上电

20H,06H      操作 PSAM 卡数据无回应

20H,07H      操作 PSAM 卡数据出现错误

30H,01H      不支持非接触式用户卡

30H,04H      非接触式用户卡未激活

30H,06H      操作非接触式用户卡数据无回应

30H,07H      操作非接触式用户卡数据出现错误

**指令示例：(非接 CPU 卡 APDU 取随机数 0084000008)**

**SEND:** 02 30303038 33323236 3F3F30303834303030303038 3637 03

**REC:**

02 30303034 30303030 363D3030 363D 03

返回 6D00

3.2.8. 设置接触式存储卡种类

命令数据单元		
32H, 31H		
CardNo	1 字节	接触式卡: 00H, PSAM 卡: 10H-12H
CardType	1 字节	接触式卡种类, 见附录 A
成功应答数据单元		
00H,00H		

3.2.9. 识别接触式存储卡种类

命令数据单元		
32H, 32H		
CardNo	1 字节	接触式卡: 00H, PSAM 卡: 10H-12H
成功应答数据单元		
00H,00H		
CardType	1 字节	接触式卡种类, 见附录 A

3.2.10. 接触式存储卡密钥初始化

命令数据单元		
32H, 33H		
CardNo	1 字节	接触式卡: 00H, PSAM 卡: 10H-12H
Len	1 字节	密码长度
Pin		长度为 Len 字节的密钥
成功应答数据单元		
00H,00H		

3.2.11. 接触式存储卡密码校验

命令数据单元		
32H, 34H		
CardNo	1 字节	接触式卡: 00H, PSAM 卡: 10H-12H
Len	1 字节	密码长度
Pin		长度为 Len 字节的密码
成功应答数据单元		
00H,00H		

3.2.12. 接触式存储卡读数据

命令数据单元



---

32H, 35H		
CardNo	1 字节	接触式卡: 00H, PSAM 卡: 10H-12H
Address	2 字节	低字节在前
Len	2 字节	读数据长度
成功应答数据单元		
00H,00H		
Data		

3.2.13. 接触式存储卡写数据

命令数据单元		
32H, 36H		
CardNo	1 字节	接触式卡: 00H, PSAM 卡: 10H-12H
Address	2 字节	低字节在前
Len	2 字节	写数据长度
Data		长度为 Len 字节的数据
成功应答数据单元		
00H,00H		

3.2.14. 激活非接触式存储卡

命令数据单元		
32H, 41H		
DelayTime	2 字节	等待卡进入感应区时间（单位：毫秒），高位字节在前
		0:无需等待，无卡直接返回
		0xffff:一直等待
成功应答数据单元		
00H,00H		
Type	1 字节	0AH A 卡
UID	4 字节	卡 UID

3.2.15. 非接触式存储卡认证扇区

命令数据单元	
32H, 42H	
扇区号	1 字节
密钥类型	1 字节
密钥	6 字节
成功应答数据单元	
00H,00H	

3.2.16. 非接触式存储卡读块

---

命令数据单元  
32H, 43H  
块号           1 字节

成功应答数据单元  
00H,00H  
数据

### 3.2.17. 非接触式存储卡写块

命令数据单元  
32H, 44H  
块号           1 字节  
数据           16 字节  
成功应答数据单元  
00H,00H

### 3.2.18. 非接触式存储卡读值块

命令数据单元  
32H, 45H  
块号           1 字节  
  
成功应答数据单元  
00H,00H  
数据           (高位在前) 4 字节

### 3.2.19. 非接触式存储卡写值块

命令数据单元  
32H, 46H  
块号           1 字节  
数据           4 字节   (低位在前)  
成功应答数据单元  
00H,00H

### 3.2.20. 非接触式存储卡充值

命令数据单元  
32H, 47H  
块号           1 字节  
数据           4 字节   (高位在前)  
成功应答数据单元  
00H,00H

3.2.21. 非接触式存储卡减值

命令数据单元  
32H, 48H  
块号           1 字节  
数据           4 字节   (高位在前)  
成功应答数据单元  
00H,00H

3.2.22. 非接触式存储卡写主密钥

命令数据单元  
32H, 49H  
密钥模式       1 字节  
扇区号         1 字节  
密钥           6 字节  
成功应答数据单元  
00H,00H

3.2.23. 设置非接触式存储卡种类

命令数据单元  
32H, 4AH  
CardType       1 字节       非接触式卡种类，见附录 B  
成功应答数据单元  
00H,00H

---

附录 A（支持的接触式存储卡种类、型号）

种类代码	卡型号
01H	AT24C02
03H	SLE4428
04H	SLE4442
05H	AT24C64

---

## 附录 B（支持的非接触式存储卡种类、型号）

种类代码	卡型号
0AH	Mifare S50、Mifare S70