RFID-SIM卡读写器模块

用户手册

（NMPR0003-1-3）

国民技术股份有限公司

2009年**12**月

目　录

国民技术股份有限公司 Nationz Technologies Inc.
地址：深圳市南山区高新南一道中国科技开发院三号楼塔楼12层
电话：+86-755-86309900　传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

国民技术股份有限公司 Nationz Technologies Inc.
地址: 深圳市南山区高新南一道中国科技开发院三号楼塔楼12层
电话: +86-755-86309900 传真: +86-755-86169100
邮箱: info@nationz.com.cn 邮编: 518057

1. 概述

本文档适用于使用 RFID-SIM 卡标准式读写器模块（以下简称模块）进行终端开发的用户。终端开发者通过发送串口命令的方式操作模块与 RFID-SIM 卡进行数据交换，从而进行增值应用开发。通过阅读本文档，终端开发者可以在无需考虑 RF 通信实现细节情况下，借助模块来迅速创建、或改造现有系统使之适合 RFID-SIM 卡应用。

2. 符合标准

《中国移动手机支付 RFID-SIM 卡读写器技术方案 V1.0.0》

《中国移动手机支付 RFID-SIM 卡读写器认证方案 V1.0.0》

3. 基本特征

模块的基本特征见下表：

射频兼容标准	中国移动手机支付RFID-SIM卡射频协议接口方案 V1.0.0
射频工作频率	2400-2483.5MHz
射频通信速率	1Mbps
射频有效操作距离	<10cm
串口波特率	115200 bps
供电电源	DC（5±10%）V
读写模块消耗电流	<100mA
通讯接口	UART
工作温度	-10℃～60℃
工作湿度	相对湿度0%～95%

国民技术股份有限公司 Nationz Technologies Inc.
地址：深圳市南山区高新南一道中国科技开发院三号楼塔楼12层
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

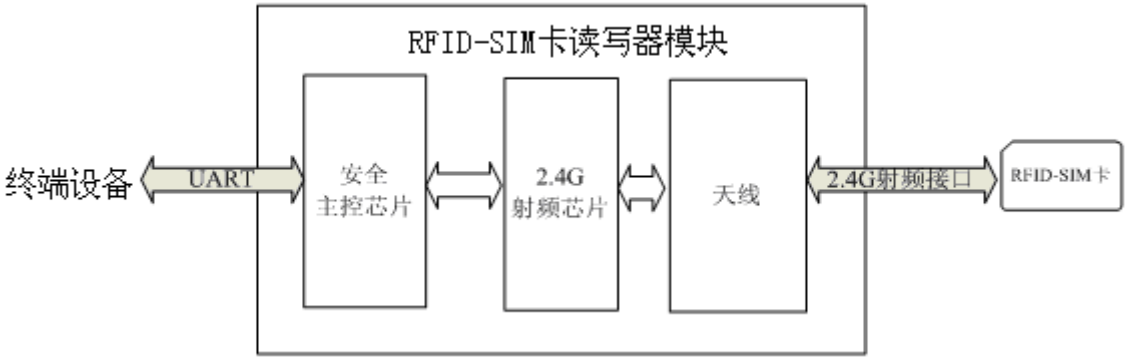
3.1. 硬件构成

1) 安全主控芯片，完成模块内部各接口的控制和安全管理功能；

2) 2.4G 射频芯片，完成与 RFID-SIM 卡的射频通信功能；

3) 点阵天线，是射频通信和距离控制的重要组成部分。

模块内部结构逻辑如下图所示：



模块内部结构逻辑图

3.2. 通信方式

模块与RFID-SIM卡、终端设备的通信方式如下图所示：

模块与外部的通信方式

模块与终端设备之间采用UART接口通讯，由终端设备实现所有业务逻辑。

国民技术股份有限公司 Nationz Technologies Inc.
地址：深圳市南山区高新南一道中国科技开发院三号楼塔楼12层
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

4. 模块使用注意事项

1) 模块上电后需进行自检，故需保持读写器表面无其他物体，如果读写器无法读卡，请重新上电进行尝试。
2) 在模块工作时请勿在其表面摆放任何其他物体。

5. 通信协议

5.1. 物理层

模块采用终端设备串口供电或单独外部供电方式，电压5V。模块串口与POS终端串口相连，采用3.3VCMOS电平，异步全双工通讯，波特率默认为115200bps。数据格式为1位起始位、8位数据位和1位停止位，无校验位。

终端设备向模块发送命令时，在同一个命令内，相连两个发送字符之间的间隔不应大于10个字符时间，否则模块可能会认为命令超时导致无任何响应。

5.2. 链路层

5.2.1. 通讯数据包定义

通信数据包如下图所示：

STX(0x02)	Len_Hi	Len_Low	Data	LRC	ETX(0x03)

通讯数据包项目、长度、含义说明对应见下表：

通讯数据包项目含义一览表

国民技术股份有限公司 Nationz Technologies Inc.
地址：深圳市南山区高新南一道中国科技开发院三号楼塔楼12层
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

序号	项 目	长度（字节）	说明
1	数据包头（STX）	1	常量：0x02
2	数据单元长度（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。 例如：0x0010 表示 Data 部分有 16 个字节。
3	需传输的数据单元(Data)	不定	长度由 Data_len 指出，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

数据包总长度为： Data_len + 5 字节，最长不能超过 512 字节。

5.2.2. 协议描述

终端设备首先发送一个命令数据包，发送完成后等待来自模块的应答数据包。

RIID-SIM卡读写器模块正确收到命令数据包后，便执行命令，然后回应应答数据包。

如果终端设备在规定的最长时间内未能收到正确的应答数据包， 便结束本次数据通讯，并提示出错信息。

除了特定指令指定了响应时间外，各命令缺省的允许最大超时时间设定为500毫秒。

5.3. 数据单元格式

5.3.1. 命令单元格式

终端设备向模块发送的数据包称为命令数据包，命令数据包的格式如下图所示：

命令单元格式见下表：

命令单元格式一览表

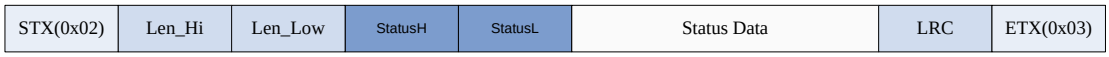
项目	长度	说明
CommandH	1 字节	命令类别

国民技术股份有限公司 Nationz Technologies Inc.
地址：深圳市南山区高新南一道中国科技开发院三号楼塔楼12层
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

CommandL	1 字节	命令代码
【参数】	不定长	命令参数，不是所有命令都有

5.3.2. 应答单元格式

模块向POS机发送的数据包称为应答数据包，如下图所示：



应答单元格式见下表：

应答单元格式一览表

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	应答数据，不是所有应答都有

6. 模块操作指令

6.1. 管理操作指令

6.1.1. 通讯参数设置

通过本命令可重新设置模块的串口通讯波特率，初始缺省串口通讯波率为115200bps。

命令数据单元：

命令数据单元含义一览表

标识	内容	说明
CommandH	A0H	功能命令类别
CommandL	01H	设置串口通讯波特率
串口波特率	1 字节	0： 9600bps(暂不支持)
		1： 19200bps(暂不支持)
		2： 38400bps(暂不支持)

国民技术股份有限公司 Nationz Technologies Inc.
地址：深圳市南山区高新南一道中国科技开发院三号楼塔楼12层
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

		3： 57600bps(暂不支持)
		4： 115200bps

应答数据单元：

应答数据单元含义一览表

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

6.1.2. 查看版本信息

此命令用于查看中国移动定义的接口版本、受理方定义的版本和厂家自定义信息。

命令数据单元：

命令数据单元含义一览表

标识	内容	说明
CommandH	A1H	功能命令类别
CommandL	11H	查看版本命令代码

应答数据单元：

正常应答数据单元含义一览表

标识	内容	说明
Status	00H，00H	命令执行正确
	00H，02H	命令参数错误，此时无后续数据。
CMCC_Interface	8 字节	由中国移动定义的接口版本信息
THIRD_Interface	8 字节	由第三方定义的版本信息
Len	1 字节	厂家自定义信息长度
ProInfomation	Len 字节	厂家自定义信息

6.1.3. 软复位读写器

通过该命令，模块将初始化除波特率以外的所有参数。

国民技术股份有限公司 Nationz Technologies Inc.
地址：深圳市南山区高新南一道中国科技开发院三号楼塔楼12层
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

命令数据单元：

命令数据单元含义一览表

标识	内容	说明
CommandH	A1H	功能命令类别
CommandL	12H	软复位读写器命令代码

应答数据单元：

应答数据单元含义一览表

标识	内容	说明
Status	00H，00H	命令执行正确
Status	00H, 02H	命令格式不对

模块收到命令后，先回应命令执行正确应答码，然后在接下来的500ms内重新启动，此时模块无法响应外部命令，因此终端在收到命令执行正确的应答后500ms内不要对模块发送命令。

6.1.4. 读写器认证报文

此命令用于执行PSAM卡对模块的认证，PSAM通过验证MAC决定是否允许交易。

命令数据单元：

命令数据单元含义一览表

标识	内容	说明
CommandH	A1H	功能命令类别
CommandL	13H	计算 MAC 命令
KeyIndex	1	密钥索引
RAND-PSAM	4	RAND-PSAM

应答数据单元：

应答数据单元含义一览表

标识	内容		说明
Status	00H	00H	回应正确
	00H	02H	命令参数错误，此时无后续数据。

国民技术股份有限公司 Nationz Technologies Inc.
地址：深圳市南山区高新南一道中国科技开发院三号楼塔楼12层
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

RID	8	读写器物理 ID
MAC-RP	4	利用 KeyIndex 认证密钥对 RAND-PSAM 进行计算得出会话密钥 采用会话密钥对 RAND-PSAM 和 RID 计算 MAC。 会话密钥和 MAC 计算算法参考《中国移动手机支付 RFID-SIM 卡读写器认证方案 V1.0.0》

6.1.5. 密钥更新（密钥管理用）

对模块的密钥更新分为两个步骤：

1）获取随机数：

命令数据单元含义一览表

标识	内容	说明
CommandH	A1H	功能命令类别
CommandL	14H	获取随机数

应答数据单元：

应答数据单元含义一览表

标识	内容		说明
Status	00H	00H	正确
	00H	02H	命令参数错误，此时无后续数据。
RAND_R	4		读写器返回 4 字节随机数

国民技术股份有限公司 Nationz Technologies Inc.
地址：深圳市南山区高新南一道中国科技开发院三号楼塔楼12层
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

2）更新密钥命令：

命令数据单元含义一览表

标识	内容	说明
CommandH	A1H	功能命令类别
CommandL	15H	密钥更新命令代码
KeyIndex	1	待更新的密钥索引
KeyEnc	16	（利用初始密钥加密的）新密钥密文，密钥算法见《中国移动手机支付 RFID-SIM 卡读写器认证方案 V1.0.0》
MAC	4	采用会话密钥（CommandH||CommandL||KeyIndex||KeyEnc）计算的 MAC 会话密钥由原密钥采用（RAND_R）分散而成，会话密钥的计算方法及 MAC 算法参考《中国移动手机支付 RFID-SIM 卡读写器认证方案 V1.0.0》

应答数据单元：

应答数据单元含义一览表

标识	内容		说明
Status	00H	00H	更新正确
	00H	02H	索引无效
	00H	03H	更新错误（初始密钥错误）

6.2. 卡片操作指令

模块从国民技术出厂时为未激活状态，此状态下的模块只能读写国民技术生产检测卡。在模块嵌入的终端生产完毕出厂前，需要用专用工具进行模块激活操作（参考文档《POS设备RFID-SIM功能检测、激活生产流程说明》，成功激活后的模块方可操作正式应用的RFID-SIM卡。

国民技术股份有限公司 Nationz Technologies Inc.
地址：深圳市南山区高新南一道中国科技开发院三号楼塔楼12层
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

6.2.1. 连接卡片

本命令用于要求模块在DelayTime时间内查寻卡是否进入感应区，并连接进入感应区的卡片。

命令数据单元：

命令数据单元含义一览表

标识	内容	说明
CommandH	A2H	卡片操作命令类别
CommandL	31H	连接 RFID-SIM 卡命令代码
DelayTime	2 字节	等待卡进入感应区时间，高位在前，低位在后。 为 0 时：感应区无卡直接返回失败； 为 0xffff 时,一直寻卡，直到卡进入感应区； 其它值时：在 DelayTime 毫秒时间内一直判断卡是否进入感应区。

应答数据单元：

应答数据单元含义一览表

标识	内容		说明
Status	00H	00H	连接成功
	A0H	01H	RFID-SIM 卡未连接，此时无后续数据。
	A0H	06H	等待卡进入感应区超时，此时无后续数据。
	A0H	09H	读写器自检未通过
	A0H	0AH	卡片校准参数异常
	A0H	0BH	刷卡环境受到异物的干扰和影响
UIDLen	1 字节		卡序列号长度
Card UID	UIDLen 字节		卡序列号（连接成功才返回）

如果DelayTime参数为0，在无卡处于模块感应区时，模块不用等待直接返回“连接失败”；如果DelayTime参数为0Xffff时,一直寻卡，直到卡进入感应区；如果DelayTime参数为其它值时，模块可在DelayTime时间内一直寻卡，直到超时了才返回“连接失败”。任意DelayTime内，如果有卡在感应区但连接失败，那么模块不用继续寻卡就直接返回“连接失败”。

国民技术股份有限公司 Nationz Technologies Inc.
地址：深圳市南山区高新南一道中国科技开发院三号楼塔楼12层
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

不建议使用DelayTime为0xFFFF这种方式，因为当终端发送该命令后，如果模块由于某种原因工作异常导致复位，重启后的模块不会主动发送响应，但此时终端还会一直等待，导致系统异常。

由于速度响应速度的问题，模块的响应精度为100ms，也就是说响应收到的时间在【Delaytime, Delaytime+100】ms之间。

当模块成功连接卡片后，除非1）执行断开连接命令；2）卡片已经离开模块工作范围；3）模块重新上电，否则模块对终端再次发送的链接卡片命令均会返回连接失败响应。

6.2.2. 断开连接

该命令要求模块断开与卡的连接。

命令数据单元：

命令数据单元含义一览表

标识	内容	说明
CommandH	A2H	卡片操作命令类别
CommandL	32H	断开连接命令代码
DelayTime	2 字节	等待卡拿离感应区时间，高位在前，低位在后。此版本不支持该参数，请将该参数设置为 0。

应答数据单元：

应答数据单元含义一览表

标识	内容		说明
Status	00H	00H	命令执行正确

由于速度响应速度的问题，模块的响应精度为100ms，也就是说响应收到的时间在【Delaytime, Delaytime+100】ms之间。

6.2.3. 操作卡片数据

传输通讯链路建成后，终端设备和模块通过该命令开始应用层的APDU命令的传送。

命令数据单元：

国民技术股份有限公司 Nationz Technologies Inc.
地址：深圳市南山区高新南一道中国科技开发院三号楼塔楼12层
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

命令数据单元含义一览表

标识	内容	说明
CommandH	A2H	卡片操作命令类别
CommandL	33H	操作卡片数据命令代码
C-APDU	不定长	命令应用协议数据单元。（按照 ISO/IEC 7816 规范格式）

应答数据单元：

应答数据单元含义一览表

标识	内容		说明
Status	00H	00H	卡片正常传回数据
	A0H	02H	卡片连接失败。
		06H	操作卡片数据无回应，此时无后续数据。
		07H	操作卡片数据出现错误，此时无后续数据。
R-APDU	不定长		响应应用协议数据单元（按照 ISO/IEC 7816 规范格式）

关于C-APDU和R-APDU数据格式请参考ISO/IEC 7816规范。

6.3. 厂商私有指令

为了更好的实现行业的应用，定义了以下私有指令作为对标准指令的补充：

6.3.1. 卡片连接状态查询

通过本指令，可以查询已经与模块建立起连接的卡片状态。

命令数据单元：

命令数据单元含义一览表

标识	内容	说明
CommandH	E0H	功能命令类别
CommandL	02H	查看卡片状态命令代码

应答数据单元：

国民技术股份有限公司 Nationz Technologies Inc.
地址：深圳市南山区高新南一道中国科技开发院三号楼塔楼12层
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

应答数据单元含义一览表

标识	内容	说明
Status	00H，00H	命令执行正确
Link_State	1 字节	卡片连接状态: 0：读写器未连接卡片，即手机已经远离读写器的读卡范围。 1：读写器处于连接卡片状态，即手机还处于读写器的读卡范围中。

由于 RFID-SIM 卡模块除了被动响应终端发送的命令外，还负责了卡片的检测、距离判断等操作，在优先级上，模块会优先处理终端的命令。因此终端在使用本命令查询卡片是否还在有效读卡范围内时，建议每隔 50-60ms 左右发送一次该指令，不宜频繁发送该指令，以免模块忙于处理终端的命令而减缓对卡片连接状态的判断，从而导致响应结果的时效性。

6.3.2. 获取上电自检结果

模块在上电或软复位后会立即启动对周边环境的自动检测，如果自检时周围有金属等可能会干扰刷卡的物质存在并且影响超过一定范围时，模块会自检失败，此时需要将干扰物清除并且重新上电或发送软复位命令让模块重新启动，模块需要自检通过才能正常工作。

本指令用来读取模块上电自检的结果。

命令数据单元：

命令数据单元含义一览表

标识	内容	说明
CommandH	A1H	功能命令类别
CommandL	16H	获取自检结果

应答数据单元：

应答数据单元含义一览表

标识	内容		说明
Status	00H	00H	正确
RES	1		自检结果（0 成功，1 失败）
RFU	4		自检项内容

国民技术股份有限公司 Nationz Technologies Inc.
地址：深圳市南山区高新南一道中国科技开发院三号楼塔楼12层
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

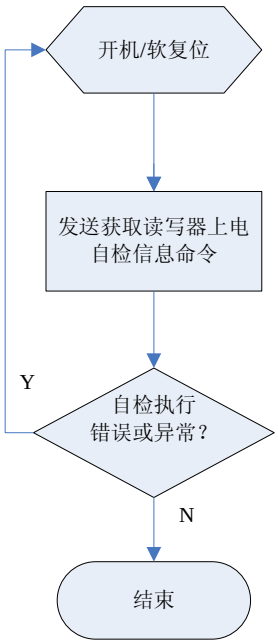
7. 操作流程

本节描述常见操作的建议流程，用户可参照本节来设计通过模块和RFID-SIM卡的数据交换。

一个基于模块的完整操作包括两个过程：终端对模块发送命令的过程和模块对终端发送命令的应答过程。每一次的操作都必须顺序的完成这一个来回。终端对模块发送命令后，如果在规定时间内（500ms）没有收到模块的响应，则表明系统发生了错误。在这种情况下，终端可以发送软复位命令，使模块重新回到初始状态。

7.1. 开机后对自检状态进行检查

模块自检成功后才能正常工作，为确保后续业务的正常操作，建议终端设备在对模块进行上电或软复位操作后对模块的自检情况进行检查，以及时排除自检异常。



7.2. 有人操作的终端(如普通商户 POS)

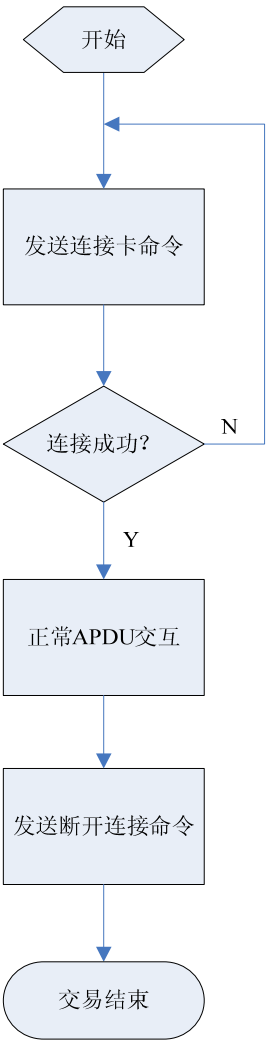
操作行为特点：

国民技术股份有限公司 Nationz Technologies Inc.
地址：深圳市南山区高新南一道中国科技开发院三号楼塔楼12层
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

每一次交易都由操作员手动发起，完成一次交易后不会自动进行下次交易，因此不会出现多次重复刷卡的问题。

操作流程：

对于此类终端设备，建议使用如下的操作流程：



有人操作终端的建议操作流程

操作示例：

以下是普通商户POS机操作读写器的示例片段（P: POS机, R: 读写器）。

P: 02 00 04 A2 31 00 00 93 03 //连接卡片命令， DelayTime=0

R: 02 00 02 A0 01 A1 03 //连接不到卡片

P: 02 00 04 A2 31 00 00 93 03 //连接卡片命令， DelayTime=0

R: 02 00 0B 00 00 08 FF FF FF FF FF FF FF FF 08 03 //连接上卡片，UID长度8字节，内容为全FF

P: 02 00 18 A2 33 00 A4 04 00 10 D1 56 00 01 01 80 03 80 00 00 00 01 00 00 10 02 3B 8D 03

国民技术股份有限公司 Nationz Technologies Inc.
地址：深圳市南山区高新南一道中国科技开发院三号楼塔楼12层
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

R: 02 00 3F 00 00 6F 39 84 10 D1 56 00 01 01 80 03 80 00 00 00 01 00 00 10 02 A5 04 9F 08 01 02 9F 0C 1E FF FF FF FF FF FF FF FF 02 FF FF FF FF FF FF FF FF FF FF FF 3A 00 00 FF FF FF FF FF FF FF 90 00 45 03

……

P: 02 00 04 A2 32 00 00 90 03//断开与卡片的连接

R: 02 00 02 00 00 00 03//断开连接成功

7.3. 无人操作终端设备(如公交/轨道闸机)

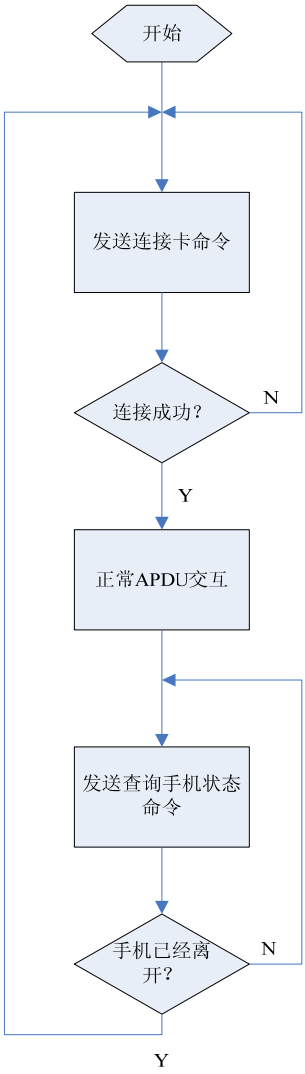
操作行为特点：

此类终端设备由于没有操作人员，需要自动管理每次交易，因此终端应用流程设计时要考虑两个因素：1）不能重复刷卡；2）每次交易结束后，主动查询卡片状态，以免后续卡片等待时间过长。

操作流程：

对于此类操作，建议使用如下的流程：

国民技术股份有限公司 Nationz Technologies Inc.
地址：深圳市南山区高新南一道中国科技开发院三号楼塔楼12层
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057



无人值守终端的操作建议流程

操作示例：

以下是公交POS机操作读写器的示例片段（P: POS机, R: 读写器）。

P: 02 00 04 A2 31 00 00 93 03 //连接卡片命令， DelayTime=0

R: 02 00 02 A0 01 A1 03 //连接不到卡片

P: 02 00 04 A2 31 00 00 93 03 //连接卡片命令， DelayTime=0

R: 02 00 0B 00 00 08 FF FF FF FF FF FF FF FF 08 03 //连接上卡片，UID长度8字节，内容为全FF

P: 02 00 18 A2 33 00 A4 04 00 10 D1 56 00 01 01 80 03 80 00 00 00 01 00 00 10 02 3B 8D 03

R: 02 00 3F 00 00 6F 39 84 10 D1 56 00 01 01 80 03 80 00 00 00 01 00 00 10 02 A5 04 9F 08 01 02 9F 0C 1E FF FF FF FF FF FF FF FF 02 FF FF FF FF FF FF FF FF FF FF FF 3A 00 00 FF FF FF FF FF FF FF 90 00 45 03

……

国民技术股份有限公司 Nationz Technologies Inc.
地址：深圳市南山区高新南一道中国科技开发院三号楼塔楼12层
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

P: 02 00 02 E0 02 E2 03//查询卡片状态

R: 02 00 03 00 00 01 01 03//手机仍在读写器读卡范围内

……

P: 02 00 02 E0 02 E2 03//查询卡片状态

R: 02 00 03 00 00 00 00 03 //手机已经离开读写器读卡范围

8. 防拔机制

一个完整的业务流程一般涉及RFID-SIM卡模块和卡片之间的多次数据交互，在此过程中存在由于异常情况（如断电、RFID-SIM卡突然移走等）导致业务操作的完整性受到破坏，如消费过程中卡片金额扣除了，但是终端扣款却没有成功的现象。因此上层应用设计者必须考虑防拔机制。

防拔机制的实现，可以参考《电子钱包STK技术规范-V0.5》，基于GET TRANSACTION PROVE命令实现。GET TRANSACTION PROVE提供了一种在交易处理过程中拔出并重插卡后的恢复机制。

终端对交易的正常处理流程：

1) 询卡
2) 选择AID
3) 初始化消费
4) 消费
5) 查询余额（可选）

当终端消费命令发送完毕，卡片执行成功后返回，但终端没有收到卡片返回或收到后判断出错而丢弃时，就会影响交易完整性，出现“卡片拔出”问题。

为了解决交易的完整性问题，建议终端实现如下的防拔机制：

1) 当出现交易完整性问题时，终端应该发出相应的交易异常提示，要求用户将卡片重新靠近模块；与此同时，终端应当记录下本次异常交易的卡片UID以及交易MAC等关键数据，以便后面的防拔处理。
2) 当用户将手机靠近模块时，终端通过询卡获取并判断该卡片 UID，如果该 UID 与之前记录的交易异常的 UID 不一致，则表示这是一张新的卡，按照标准的交易流程处理即可；如果该 UID 与之前记录的交易异常的 UID 一致，则发送 GET TRANSACTION PROVE 命

国民技术股份有限公司 Nationz Technologies Inc.
地址：深圳市南山区高新南一道中国科技开发院三号楼塔楼12层
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

令，之后按照防拔处理流程进行，交易完成后将异常交易的 UID 和 MAC 等关键数据记录清除。

9. 常见问题解答

1) 将模块连接到终端后，无论终端发送任何命令，模块均无响应。

请确认一下配置是否正常：

a) 确保终端能给模块提供 5V 100mA 的工作电流。

b) 确保终端的 UART 接口能够兼容 3.3VCMOS 电平。

c) 确保终端的 UART 接口 TX 信号连接到模块的 RX 信号，终端的 UART 接口 RX 信号连接到模块的 TX 信号。

2) 终端发送短的命令时，模块有回应，但是终端发送长的命令时，模块没有回应。

a) 确保发送长命令时，命令的总字节数不超过 512 字节。

b) 确保发送同一个命令的过程中，两个连续的字符之间的间隔不大于 10 个字符时间。

c) 终端采取先发送 STX，LEN，DATA，然后计算 LRC，再发送 LRC 和 ETX 的方式，则有可能在计算 LRC 时时间较长，导致超过上述限制，被模块认为是非法的指令而不作任何响应。

3) 连接卡片的命令发送以后，一直返回连接不成功。

请检查响应的状态字：

a) 如果是 A0 09， 则是模块的上电自检没有通过所致。终端在对模块上电的瞬间，要注意模块附近不能有金属等可能影响 2.4GHz 信号的物质，否则可能会导致模块自检不通过而不能正常工作。

b) 如果是 A0 0B，则表示读写器检测到附近有影响刷卡的干扰物而拒绝工作，请将附近的干扰物清除后再试。

10. 附录

10.1. LRC 计算程序(C 语言)

```
typedef unsigned char       U8;
```


国民技术股份有限公司 Nationz Technologies Inc.
地址：深圳市南山区高新南一道中国科技开发院三号楼塔楼12层
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057

```
U8 LRC(U8 *pBuff, int nLen)
{
    U8 Lrc = 0 ;
    while(nLen--)
    {
        Lrc ^=*pBuff++;
    }
    return Lrc;
}
```

11. 修订记录

编号	修订内容	版本
1	“连接卡片”命令去掉 A005 返回值	NMP0003-1-2
2	“断开连接”命令去掉 A001、A006、 A004 返回值	NMP0003-1-2
3	“操作卡片数据”命令去掉 A001 返回值，增加 A002 返回值	NMP0003-1-2
4	6.2 节增加模块状态描述	NMP0003-1-3

国民技术股份有限公司 Nationz Technologies Inc.
地址：深圳市南山区高新南一道中国科技开发院三号楼塔楼12层
电话：+86-755-86309900 传真：+86-755-86169100
邮箱：info@nationz.com.cn 邮编：518057