中 国 移 动 通 信 企 业 标 准

QB-XX-XXX-XXXX

中 国 移 动 手 机 支 付
RFID-SIM 卡 读 写 器 技 术 方 案

版 本 号： 1.0.0

XXXX-XX-XX 发 布　　XXXX-XX-XX 实 施

中国移动通信有限公司　　发布

目　　录

1. 范围

本标准规定了手机支付系统中RFID-SIM读写器的规范要求，供中国移动内容和RFID-SIM卡读写器及POS厂商共同使用。

2. 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

序号	标准编号	标准名称	发布单位
[1]		《微功率（短距离）无线电设备的技术要求》	中华人民共和国工业和信息化部
[2]		《中国移动手机支付RFID-SIM卡系统射频协议与接口规范》	中国移动通信集团公司

3. 术语、定义和缩略语

下列术语、定义和缩略语适用于本标准：

词语	解释
(U)SIM	(Universal) Subscriber Identity Module
AID	Application Identifier，由注册的应用提供商标识（RID）以及专用应用标识符扩展（PIX）组成
GPRS	General Packet Radio Service
STK	(U)SIM Tool Kit
UE	User Equipment
MAC	报文鉴别代码(Message Authentication Code)
PSAM	销售点终端安全存取模块(Purchase Secure Access Module)

4. 概述

RFID-SIM卡读写器是业务处理终端和RFID-SIM卡的通信桥梁。RFID-SIM卡读写器主要由以下几部分组成：

1、 安全主控芯片，完成读写器各部分接口的控制和安全管理功能；
2、 2.4G射频芯片，与RFID-SIM卡的射频通信通道；
3、 点阵天线，用于射频通信和距离控制的重要组成部分。

RFID-SIM卡读写器的主要接口有两部分：
1、 与POS终端通讯的串行接口；
2、 与RFID-SIM卡通讯的2.4G射频接口。

RFID-SIM卡读写器结构图如图1所示：

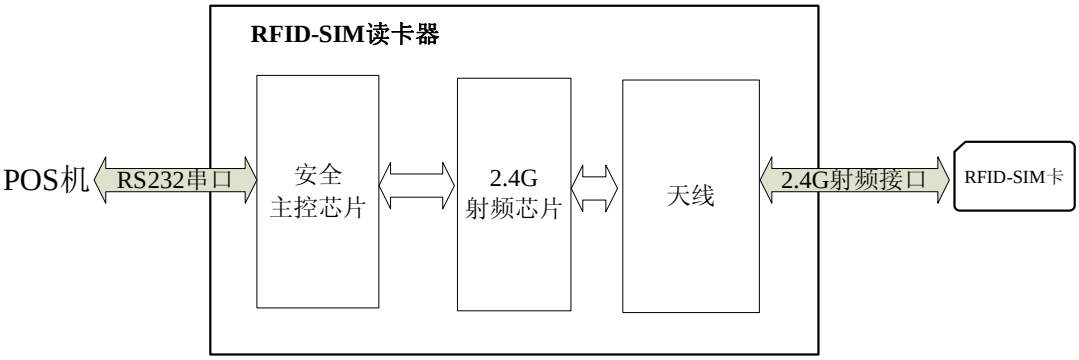

图1　　读写器模块结构图

5. 读写器性能与硬件要求

5.1. 读写器型号说明

中国移动手机支付 RFID-SIM 卡读写器的型号字节定义为：0x00 （近距离读写器）。

5.2. 读写器工作方式

读写器通过RS232串口与POS终端设备连接并进行数据交互。读写器与卡片、POS终端设备的工作示意图如图2所示：

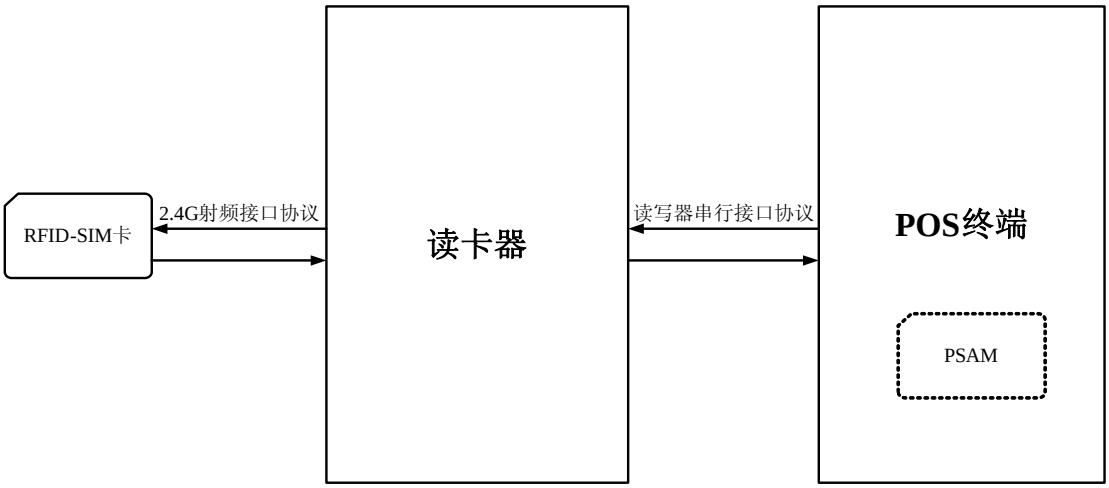

图2　　读写器工作方式

读写器与POS终端之间采用RS232方式通讯，由POS终端实现所有业务逻辑。当需要对读写器进行设置或读写卡片时，POS终端向读写器发送相应指令，由读写器返回操作结果。

读写器与卡片之间交互，应符合中国移动手机支付规范相关部分的要求。

5.3.　基本性能要求

见表1　。

表1　　读写器基本性能要求一览表

射频兼容标准	2.4G射频协议
射频工作频率	2400-2483.5MHz
射频通信速率	1Mbits/s
射频有效操作距离	<4cm
串口波特率	115200 bps
供电电源	DC（5±5%）V
读写模块消耗电流	<100mA
通讯接口	RS232（必备）
操作温度	-10℃～50℃
存储温度	-25℃～50℃
最大工作湿度	相对湿度0%～95%
参考标准天线尺寸	6.5cm X 8.7 cm

5.4. 硬件要求

5.4.1. 非接触处理芯片

非接触处理芯片符合《中国移动手机支付RFID-SIM卡射频协议接口规范》相关要求。

5.4.2. 天线

天线应采用点阵天线，标准参考天线尺寸为6.5cmX8.7cm。

5.4.3. 电源

读写器由POS机提供电源，应为(5±5%) V直流供电。

5.4.4. 通讯接口

读写器必须支持RS232通讯方式。RS232需支持115200bps通讯速率。

6. 读写器状态与软件要求

6.1. 读写器状态描述

RFID-SIM卡读写器共有关机、空闲、寻卡、操作处理等4种固定状态以及各状态之间转换时的过渡状态。

读写器各种状态的转换以及相应操作如图3所示：

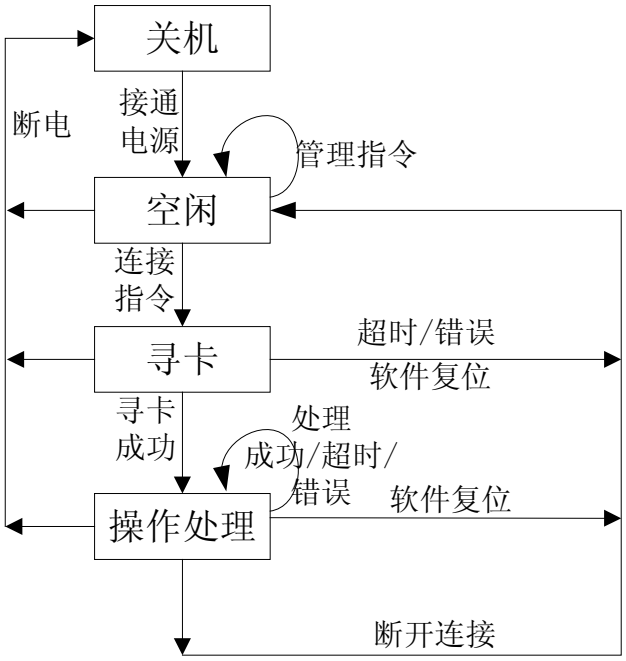

图3　　读写器状态转换图

6.2.　读写器软件要求

6.2.1.　读写器软件

读写器应具有设备初始化，对硬件的自检及报警功能，可以由生产商重新写入软件。读写器应具备受理RFID-SIM卡片的能力。

6.2.2.　协议兼容性

读写器应兼容《中国移动手机支付RFID-SIM卡射频协议接口规范》。
读写器若需增加其它非强制通讯协议时，不能影响原有通讯协议的处理。

7. 安全要求

7.1. 读头认证要求

PSAM对读头的认证过程，及读头、PSAM卡和POS机需要遵循的相关技术要求，请参考《中国移动手机支付RFID-SIM卡读写器认证方案》相关定义。

7.2. 密钥存储

读写器中必须预留读写器认证密钥的安全存储区。

7.3. 安全报文传送

具体业务中对卡操作采用安全报文传送，安全报文传送的目的是保证数据的可靠性、完整性和对发送方的认证。数据完整性和对发送方的认证通过使用MAC/TAC来实现。数据的可靠性通过对数据域的加密来得到保证。

安全报文的传送格式、报文完整性和验证方法、数据可靠性的保证和过程密钥的产生方法和流程遵循中国移动手机支付相关规范规定。

7.4. 设备的安全性

一个防入侵的设备必须保证在它的正常的运行环境中，设备或它的接口不会泄露或改变任何输入或输出设备的、存储在设备中的或者在设备中处理的敏感数据（关于对防入侵的设备的要求请参阅ISO 13491）。

8. 通讯协议

8.1. 物理层

读写器采用POS终端设备串口供电或单独外部供电方式，电压5V。读写器串口与POS终端串口相连，电信号符合RS_232C要求，异步全双工通讯，波特率默认为115200bps。数据由1位起始位、8位数据位和1位停止位组成，无校验位。

8.2. 链路层

8.2.1. 通讯数据包定义

通讯数据包项目、长度、含义说明对应见表2。

表2 通讯数据包项目含义一览表

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（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。 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。

8.2.2. 协议描述

POS终端首先发送一个命令数据包，发送完成后等待来自读写器的应答数据包。

读写器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POS终端在规定的最长时间内未能收到正确的应答数据包，那么POS终端便结束本次数据通讯，并提示出错信息。

各命令缺省的允许最大超时时间设定为0.5秒。

8.2.3. 数据单元格式

8.2.3.1. 命令单元格式

命令单元格式见表3 。

表3 命令单元格式一览表

项目	长度	说明
CommandH	1 字节	命令类别
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

8.2.3.2. 应答单元格式

应答单元格式见表4 。

表4　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

8.3. 应用层

应用层主要介绍命令和应答数据单元的详细内容。

8.3.1. 命令码定义

命令码定义及编码规则见表5 、表6 。

表5　命令码定义一览表

CommandH	CommandL	说明
00H－8F	*	第三方专用命令
90－BF	*	中国移动专用命令
C0h~F0h	*	开发商保留可自定义命令

表6　命令码编码规则

CommandH	CommandL	说明
A0H	*	通讯参数设置命令
A1H	*	读写器功能命令
A2H	*	卡片操作命令

8.3.2. 状态码定义

状态码定义及编码规则见表7 、表8 。

表7　状态码定义一览表

StatusH	StatusL	说明
00H－8FH	*	第三方专用状态码
90H－BFH	*	中国移动专用状态码
C0H~F0H	*	开发商保留可自定义状态码

表8　状态码编码规则

StatusH	StatusL	说明
00H	00H	命令执行正确回应
00H	01H	串口设置参数不支持
00H	02H	与 POS 双向认证失败
A0H	01H	RFID-SIM 卡未连接
A0H	02H	RFID-SIM 卡连接失败
A0H	03H	不支持的操作
A0H	04H	关闭操作失败
A0H	05H	操作数据格式错误

A0H	06H	操作 RFID-SIM 卡无回应（等待超时）
A0H	07H	操作 RFID-SIM 卡数据出现错误
A0H	08H	未知错误

9. 读写器操作指令

9.1. 管理操作指令

9.1.1. 通讯参数设置

通过设置通讯参数，可以调整串口通讯波特率，初始缺省串口通讯波率为115200bps。

a) 命令数据单元（见表 9）：

表9 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
		1： 19200bps
		2： 38400bps
		3： 57600bps
		4： 115200bps

b) 应答数据单元（见表 10）：

表10 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

9.1.2. 查看版本信息

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（见表 11）：

表11 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（见表 12）：

表12 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

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

其中，受理方和厂家版本信息格式自行定义。

中国移动接口版本信息存放在读写器版本信息中，共8个字节，版本号信息主要使用前2个字节。8个字节分配与用途见表13：

表13　中国移动接口版本信息分配与使用一览表

字节数	1 字节	2 字节	3 字节	4 字节	5 字节	6 字节	7 字节	8 字节
用途	2 字节版本号，十六进制，当前版本“0304”		功能位字节	保留使用	保留使用	保留使用	保留使用	保留使用

功能位字节表示见表14：

表14　中国移动接口功能位字节含义一览表

位数	BIT7	BIT6	BIT5	BIT4	BIT3	BIT2	BIT1	BIT0
用途	保留使用	保留使用	RFID-SIM 卡标识	保留使用	保留使用	保留使用	保留使用	保留使用

9.1.3. 软复位读写器

软复位读写器，读写器将初始化除了波特率以外的所有参数。

命令数据单元（见表 15）：

表15　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（见表 16）：

表16　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

软复位成功后，读写器将回应正确确认码，所以波特率参数不能被初始化。

9.1.4. 读写器认证报文

此命令用于交易启动前PSAM卡对读写器的认证，PSAM通过验证MAC决定是否允许交易。

命令数据单元：

表17　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：

表18　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	索引无效（如果索引无效，MAC-RP 无效）
RID	8		读卡器物理 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》附录-1、附录-2

9.1.5. 密钥更新（密钥管理用）

获取随机数：

表19　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：

表20　应答数据单元含义一览表

标识	内容		说明
Status	00H	00H	正确
	00H	02H	产生随机数错误
RAND_R	4		读头返回 4 字节随机数

更新密钥命令：

表21　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》附录-3
MAC	4	采用会话密钥对

		（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》附录-1、附录-2

应答数据单元：

表22　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）

9.2. 卡片操作指令

9.2.1. 连接卡片

要求读写器在DelayTime传递的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（见表 17）：

表23　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（见表 18）：

表24　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
	A0H	05H	RFID-SIM 卡连接失败
	A0H	06H	等待卡进入感应区超时
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）

由于发送该命令时，不一定有卡在感应区，很有可能需要较长的时间才能等到卡进感应区。一种方法是由主机一直发该命令；另一种方法是设定较长的时间给读写器，完全由读写器在这段时间等待对卡连接，如果超时了便返回“连接失败”。此命令的DelayTime参数就是为了传递上述时间给读写器。如果DelayTime参数为0，在无卡进感应区时读写器不用等待直接返回“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，读写器可在DelayTime时间内一直寻卡，直到超时了读写器才返回“连接失败”，此时主机端也是采用DelayTime作为超时退出时间。如果有卡在感应区但连接失败，那么读写器不用继续寻卡就直接返回“连接失败”。

9.2.2. 断开连接

该命令要求读写器断开与卡的连接。

命令数据单元（见表 19）：

表25 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。参数说明见备注。

应答数据单元（见表 20）：

表26 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
	A0H	01H	RFID-SIM 卡未连接
		06H	等待卡拿离感应区超时
		04H	断开连接失败

完成对卡的断开连接操作后,要求用户将卡离开射频操作区域，否则将一直循环判断。如果DelayTime参数为0时，则不用等待，将直接返回断开操作结果；若DelayTime为0xffff时，将无限等待，直至卡离开感应区；若为其它值时，将在规定时间判断卡是否还在感应区直至定时时间到或者卡离开感应区。

9.2.3. 操作卡片数据

传输通讯链路建成后，终端和读写器通过该命令开始应用层的APDU命令的传送。

命令数据单元（见表 21）：

表27 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（见表 22）：

表28　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	01H	卡片未连接
		06H	操作卡片数据无回应
		07H	操作卡片数据出现错误
R-APDU	不定长		响应应用协议数据单元（按照 ISO/IEC 7816 规范格式）

只有在STATUS为00H 00H的情况下才会有R-APDU数据单元，其他情况是由于卡片无法正常返回数据，所以无R-APDU数据单元。关于C-APDU和R-APDU数据格式请参考ISO/IEC 7816规范。

读写器自己有超时退出机制，退出时间是按照卡片规范来确定的，单一命令的超时时间不得超过0.5秒。

10. 编制历史

版本号	更新时间	主要内容或重大修改
V1.0.0	2009-6-12	V1.0.0版本