# 中国电信集团公司部门文件

中国电信公客〔2010〕39 号

## 关于印发 2.4G 多应用 RF-UIM 卡相关规范的通知

集团公司各省级分公司，股份公司并转各省级分公司:

为了进一步支撑各省公司移动支付业务和翼机通行业应用的顺利开展，在《关于印发移动支付 UIM 卡需求规范的通知》（中国电信〔2009〕1045 号）文件基础上，集团公司组织制定了《中国电信 2.4GRF-UIM 卡需求规范（暂行）》和《中国电信 2.4GRF-UIM 卡射频协议接口方案（暂行）》，作为 RFIDUIM 卡系列规范的补充;制定《中国电信 2.4GRF-UIM 卡空间规划（暂行）》，对 2.4GRFIDUIM 卡空间进行统一规划，规定了各种应用的分布区域和规划空间。

现将相关文件下发你们，请在开展 UIM 卡多应用业务时认真遵守。在实施过程中，如发现问题，请及时向集团公司反馈。

联系人:

公众客户事业部，纪成军 010－58505248，

jicj@chinatelecom.com.cn。


二〇一〇年五月十二日

保密等级：公开发放

# 中国电信集团公司技术标准

Q/CT XXXX-2010

# 中国电信 2.4G RF-UIM 卡需求规范

（暂行）

中国电信集团公司

# 前　言

本规范是根据中国电信近距离非接触应用的业务需求对2.4G RF-UIM卡定制提出的全面要求，是2.4G RF-UIM卡所需要遵循的纲领性技术文件。

本规范主要包括以下几方面内容：业务需求、RF-UIM卡方案描述、卡功能需求、物理特性、电气特性和技术指标等。

本需求规范起草单位：中国电信股份有限公司上海研究院
中国电信股份有限公司广州研究院
本需求规范归口单位：中国电信集团公司公众客户事业部

本需求规范主要起草人：彭昭、王勇、张柳成、谢云、赵欣

# 目　录

# 1. 范围

本规范规定了中国电信RF-UIM卡片定制中需要规范的功能、物理特性、电气特性和技术指标等方面的内容，可作为各级公司在业务开展、卡片采购、工程建设时的技术依据。

# 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。

| | |
|---|---|
| [1] | 《中国电信RFID 技术应用规范（暂行）》 |
| [2] | 《中国电信CDMA卡需求规范-UIM卡分册》 |
| [3] | 《中国电信CDMA卡需求规范-UIM卡（1x增强型）分册》 |
| [4] | 《中国电信CDMA卡需求规范-OTA分册》 |
| [5] | 《中国电信CDMA 卡需求规范-UTK 应用分册》 |
| [6] | 《中国电信2.4G RF-UIM卡射频协议接口方案》 |
| [7] | 《中国电信2.4G RF-UIM卡读写器应用规范》 |
| [8] | 《中国电信2.4G RF-UIM卡空间规划》 |

# 3. 定义和缩略语

| *缩略语* | *英文全名* | *中文全名* |
|---|---|---|
| OTA | Over The Air | 空中下载 |
| UIM | User Identify Module | 用户标识模块 |
| UTK | UIM Toolkit | UIM 卡应用工具包 |
| NVM | Non-Volatile Memory | 非易失性存储器 |
| RF | Radio Frequency | 无线电射频技术 |
| DES | Data Encryption Standard | 一种数据加密算法标准 |
| RF-UIM | RFID－User Identify Module | 带有 RF 射频功能的 UIM 卡 |

# 4. 业务需求

基于RF-UIM卡的解决方案应能满足开展以下业务的功能需求：

- 翼机通校企应用：实现校园和企事业单位手机 RFID 应用。主要场景包括校园食堂、超市、餐厅等地的消费，以及考勤、门禁、图书馆等地的身份识别应用。
- 翼支付应用：满足使用电信翼支付账户在联盟商户刷卡消费。用户可以通过 UTK 等方式查询翼支付账户信息等。
- 积分消费应用：通过 UIM 卡身份识别功能实现的积分应用，通过联机的方式消费积分，包括电信积分和电信联盟商户积分等。
- 电子钱包：实现在中国电信合作商户等场合的现场支付功能，电子钱包应用相关要求参考 PBOC2.0 规范。支持 POS 终端及电信 OTA 方式实现电子钱包账户圈存等远程应用操作，用户也可以通过 UTK 方式查询交易记录及余额。
- 优惠券功能：实现以电子信息的方式存储优惠券信息。用户从下载当前所需的优惠券至 UIM 卡中，通过脱机的方式在商家使用优惠券。实现功能包括：优惠券空中下载等远程应用操作、UTK 查询和删除、脱机消费等功能。

在满足以上应用需求基础上，RF-UIM 卡还应具备扩展支持电信其他新增应用的能力。

# 5. RF-UIM 卡方案描述

中国电信RF-UIM卡方案，将非接触RF功能集成于UIM卡上，通过和手机的配合使用，在完成普通UIM应用的基础上，实现非接触刷卡应用的功能。

RF-UIM卡是指集成了2.4G射频功能的UIM卡，将安全控制芯片、存储器、RF芯片和天线等模块以IC工艺全部嵌入到UIM卡中，RF模块由手机供电工作，实现接触和非接触两种应用功能。RF-UIM卡可以直接置入普通手机，在用户身份鉴权的基础上实现安全可靠的非接触应用。

本方案中的RF-UIM卡遵循中国电信CDMA和UTK相关规范；UIM卡接触通信协议要求符合ISO/IEC 7816规范；2.4G RF非接触通信协议要求符合《中国电信2.4G RF-UIM卡射频接口协议方案》。

# 6. RF-UIM 卡功能需求

## 6.1. 中国电信 UIM 卡功能要求

2.4G RF-UIM卡应支持基于CPU卡的各类非接触应用和UIM卡通信应用。必须满足EVDO、OTA、国际双模等通信功能。

RF-UIM卡的通信功能应遵循《中国电信CDMA卡需求规范-UIM卡分册》和《中国电信CDMA卡需求规范-UIM卡（1x增强型）分册》相关章节的定义。

## 6.2. 通讯速率

RF-UIM卡接触式通讯速率，必须支持1 ETU = 372Clock （9600bit/s，4MHz）和1 ETU = 64 Clock （57600bit/s，4MHz）两种模式，同时也可以遵照ISO7816-3的规定支持其他通讯速率。

RF-UIM卡非接触通讯速率至少支持1Mbps。

## 6.3. 断电处理功能

RF-UIM卡必须能够在交易处理中的任何情况下，甚至是在更新EEPROM过程中掉电的情况下，保持数据的完整性。

RF-UIM卡应支持对卡内数据的断电保护；支持卡上断电时处理的数据在断电后能够恢复；支持卡上文件的访问权限应保证和断电前一致。

## 6.4. UTK 功能要求

遵循《中国电信CDMA卡需求规范-UTK应用分册》。

## 6.5. 远程 OTA 管理安全要求

采用双向CDMA SMS PP DOWNLOAD安全短信的方式。手机支持ENVELOPE（SMS-DOWNLOAD），可识别数据短信并使用ENVELOPE（SMS-PPDOWNLOAD）透传给UIM卡，UIM卡需支持ENVELOPE（SMS-DOWNLOAD）。

安全短信格式参考《中国电信CDMA 卡需求规范-UTK 应用分册》和《中国电信CDMA卡需求规范-OTA分册》、《中国电信SMGP协议(V3.0)》。

RF-UIM卡对于BIP功能暂不要求，在手机终端和平台支持BIP功能后，RF-UIM卡应提供BIP功能。

## 6.6. 卡片应用要求

RF-UIM卡必须支持一卡多应用。在保证安全性的前提下，支持发卡后应用的动态调整，包括旧应用的删除（用以释放空间）和更新、新应用的加载、安装和个人化等。需要支持手机端对UIM卡内存储的钱包、优惠券、积分等应用数据的实时查询。

可采用Java模式或Native应用插件模式实现上述应用动态扩展，建议用JAVA模式实现。

## 6.7. 卡片安全要求

芯片需满足以下安全特性：

卡片芯片要求通过eal4+安全认证；

卡片支持线路加密、线路保护功能，防止通讯数据被非法窃取或篡改；

卡片必须至少支持DES/3DES算法、RSA算法。

## 6.8. 工作模式

### 6.8.1.两种移动工作模式

RF-UIM卡支持两种工作模式：RF关闭模式和RF开启模式。

RF关闭模式：要求可以通过操作手机菜单，选择将RF功能关闭。在RF功能关闭情况下，手机通信功能正常运行。

RF开启模式：要求在移动终端开机给卡供电的正常工作情况下，卡片RF非接触功能和通讯功能正常运行，按照6.8.2小节的描述，处理两个接口的应用请求。

### 6.8.2.接触式和非接触式工作模式切换

卡处于等待应用请求命令的状态时，有能力处理接触式或非接触式端口的命令。当卡接收到某一方的命令，即切换到相应的工作模式下，直到该命令处理完成。

卡需要保障正在处理的应用请求命令不受另一工作模式应用请求命令的干扰，直到卡完成当前的命令处理流程。

非接触式应用，应具备使用事务（Transaction）方式保护由多命令组成的流程和规范的功能。

接触式和非接触式命令同时触发时优先处理接触式命令。

## 6.9. 无线传输距离控制要求

- 支持UTK功率设置传输距离方式；
- 支持校正仪设置传输距离方式；

传输距离控制详见《中国电信RF-UIM卡射频协议接口方案》。

## 6.10. 卡片空间要求

### 6.10.1. 通用要求

RF-UIM卡空间包ROM、RAM、EPPROM空间，ROM空间不小于320K，RAM不少于8K，EPPROM空间不少于288K，其中EPPROM提供基础电信应用和集团标准非接触应用外，提供给其他应用（含数据）下载和扩展空间不少于30K。RF-UIM卡空间详见《中国电信2.4G RF-UIM卡空间规划》。

### 6.10.2. 存储管理要求

下载应用时，RF-UIM卡应该可以管理所有剩余NVM空间，并分配可用空间给当前应用。

如果在下载应用过程中，发现卡上剩余空间不够，RF-UIM卡应放弃当前应用下载，返回状态值通知命令发起方。同时RF-UIM卡应该有能力删除已下载的部分，恢复到未下载前的卡片状态。

# 7. 物理特性

RF-UIM卡的物理特性应遵循《中国电信CDMA卡需求规范-UIM卡分册(v1.0 RC)》相关章节的要求。

| *特性* | *性能* |
|---|---|
| 抗紫外线 | 卡的任何一面在接受总能量为15Ws/cm2的紫外线光照后，不会引起 |

| | |
|---|---|
| | 卡内数据失效 |
| X射线 | 卡的任何一面每边在受到0.1Gy剂量，相当于70～140KV中等能量X射线照射时（一年的累计剂量），不会引起卡的失效 |
| 触点与卡基表面的偏差 | 触点的最高点不高于卡的邻近表面0.1mm |
| （卡和触点的）机械强度 | 在每个触点表面和触点区域（整个导电表面）在相当于对1.5mm直径的钢球施加1.5N的工作压力下，卡不受到破坏 |
| 触点电阻 | 在两个串联的触点间，施加50μA～300mA的直流电流，其触点之间的接触电阻都小于0.5Ω。在施加4MHz、10mA的交流电时，其触点之间的阻抗的压降都小于10mV |
| 抗磁场干扰 | 卡暴露在稳定的79500A/m（1000Qe）磁场下，不会使芯片丧失功能 |
| 抗静电能力 | 在卡的任何触点与地之间通过1000PF的电容，1500Ω电阻，在1500V静电放电时，卡的性能不应受到影响 |
| 卡的翘曲 | 整卡的最大翘曲小于0.1mm |
| 模块附着力 | 卡接受60N的拉力并持续1分钟，模块不会从卡基上分离和出现裂纹、微模块变形等现象 |
| 剥离 | 卡任何一层所能承受的最小剥离强度为6N/cm，并且无任何断裂 |
| 温度和湿度条件下卡尺寸的稳定性和翘曲： | 当卡暴露在环境温度为－35℃～＋50℃之间和相对湿度5%～95%之间、最大湿球温度25℃时：<br>整卡最大翘曲值小于0.5mm，整卡的几何尺寸仍然满足ISO-7816规定 |
| 工作温度： | -25°～+80° |
| 热耗 | 卡中集成电路的热功耗小于0.05W。卡的表面温度不超过50oC |
| 耐化学性 | 卡可以经受正常处理和使用时出现的化学影响 |
| 卡的粘连和并块 | 成品卡堆积在一起时，很容易用手分开，并且外观不会损伤 |
| 卡的可燃性 | 符合GB/T 17554中定义的指标 |
| 卡的阻光度 | 卡具有大于1.5的光透射密度 |
| 振动影响 | 卡在运输或使用中受到振动后，卡的使用特性不受到影响 |
| 静电影响 | 在正常使用时，带静电的人对集成电路不应造成破坏。在任意触点和地之间施加4000V静电（电容器放电形成），卡暴露在其中时，不会影响其功能 |

## 7.1. UIM 卡非接接口触点要求

(1) 触点分配：

C1（VCC）： 提供UIM卡工作电压输入端

C2（RST）： 复位信号输入端

C3（CLK）： 时钟信号输入端

C4（RFU）： 为将来扩展使用

C5（GND）： 参考地电压

C6（VPP）： 为将来扩展使用（SWP）

C7（I/O）： 数据输入或输出端

C8（RFU）： 为将来扩展使用

(2) 触点压力

RF-UIM卡触点压力满足 GSM11.11 中4.3.4 Contact pressure 的规定。

## 7.2. 格式与布局

RF-UIM 卡的布局和格式符合《中国电信CDMA卡需求规范－UIM卡分册》4.1章节要求。

# 8. 电气特性

## 8.1. 工作电压

卡片必须支持CLASS A和CLASS B，可选支持CLASS C。

当Vcc（触点C1）供电电压在表1所规定的范围内时，卡片应该能在CDMA环境中正常工作。

表1 供电电压 $V_{cc}$

| *卡类型* | *最小电压 $V_{min}$（单位：V）* | *最大电压 $V_{max}$（单位：V）* |
|---|---|---|
| CLASS A | 4.5 | 5.5 |
| CLASS B | 2.7 | 3.3 |
| CLASS C | 1.62 | 1.98 |

## 8.2. 工作电流

### 8.2.1.RF 功能正常工作电流限制

在正常的操作条件下UIM卡的电流消耗不得超过规定限度，参见表2。

表2 Vcc 上的电流消耗

| *卡类型* | *正常条件下的 $I_{max}$ (平均值，见注) (单位：mA）* | *正常条件下的最大CLK频率 $f_{max}$(单位：MHz)* | *试验时$V_{cc}$上的电压 $V_{cc\ max}$(单位：V)* |
|---|---|---|---|
| CLASS A | 60 | 5 | 5.5 |
| CLASS B | 50 | 4 | 3.3 |
| CLASS C | 30 | 4 | 1.98 |
| *注: 参考ETSI TS 102 221 V8.0.0 6.2.3 table 6.3* | | | |

在RF-UIM卡的RF功能开启的条件下，正常工作情况下电流消耗的最大平均值参考为25-30mA以内。

### 8.2.2.休眠状态（RF 功能开启）电流限制

在休眠状态下（RF功能开启）UIM卡的电流消耗不得超过规定限度，参见表3。

表3　休眠状态下（RF 功能开启）的电流消耗

| *卡类型* | *最大电流Imax(平均值)，时钟频率 1Mhz*<br>*（单位：mA）* | *试验期间Vcc上的最大电压*<br>$V_{cc\ max}$<br>*（单位：V）* |
|---|---|---|
| CLASS A | 1 | 5.5 |
| CLASS B | 1 | 3.3 |
| CLASS C | 1 | 1.98 |

## 8.2.3.RF 功能关闭电流限制

在RF功能关闭时UIM卡的电流消耗不得超过规定限度，参见表4

表4　RF 功能关闭时的电流消耗

| *卡类型* | *最大电流Imax(平均值)，时钟频率 1Mhz*<br>*（单位：uA）* | *试验期间Vcc上的最大电压*<br>$V_{cc\ max}$<br>*（单位：V）* |
|---|---|---|
| CLASS A | 800 | 5.5 |
| CLASS B | 800 | 3.3 |
| CLASS C | 800 | 1.98 |

## 8.2.4.时钟停止模式下电流的限制

在卡7816接口时钟停止模式下（RF关闭）UIM卡的电流消耗不得超过规定限度，参见表5。

表5　时钟停止模式下（RF 关闭）的电流消耗

| *卡类型* | *最大电流* $I_{max}$*（平均值）（单位：uA）* | *试验期间* $V_{cc}$*上的最大电压*<br>$V_{cc\ max}$*（单位：V）* |
|---|---|---|
| CLASS A | 500 | 5.5 |
| CLASS B | 500 | 3.3 |
| CLASS C | 500 | 1.98 |

## 8.3. RST

应符合ETSI TS 102.221 V8.0.0第5章相关要求。

## 8.4. CLK

应符合ETSI TS 102.221 V8.0.0第5章相关要求。

## 8.5. I/O

应符合ETSI TS 102.221 V8.0.0第5章相关要求。

# 9. 技术指标

| *基本参数* | *指标* |
|---|---|
| 数据保存 | 不小于10年 |
| 擦写次数 | 不小于10万次(EEPROM产品)<br>不小于10万次(FLASH产品) |
| 工作电压 | 至少支持CLASS A和CLASS B |
| 外部时钟 | 1～4MHz@3V<br>1～5MHz@5V |
| I/O特性 | 采用T=0协议,支持增强速率F=512，D=8 |
| RF频段 | 2.400 – 2.4835GHz |
| 频率容限 | 75kHz |
| 杂散辐射发射限值 | 最大功率发射状态，不大于-30dbm；<br>空闲状态，不大于-47dbm。 |
| RF功率 | 最大发射功率不大于0dbm。 |
| 接收灵敏度 | 大于-75dbm |
| RF速率 | 至少支持1Mbps，其它可选。 |
| RF有效距离 | 对于近距离非接触应用，卡和读写器之间的交易距离控制在10厘米以内。 |
| RF ID | 唯一ID, ID为16位BCD码 |
| 安全加密 | 支持DES/3DES算法、RSA加密算法 |
| 自身抗干扰 | 为保证刷卡成功率，RF-UIM和读写器距离WiFi AP系统间隔应在1米以上 |

保密等级：公开发放

# 中国电信集团公司技术标准

Q/CT XXXX-2010

# 中国电信 2.4G RF-UIM 卡射频协议接口方案

（暂行）

发布 实施

中国电信集团公司 发布

# 前　言

本规范对中国电信2.4G RF-UIM卡和读写器之间射频接口协议的进行了规定，是中国电信RF－UIM卡开发需循循的技术规范。

本规范主要包括以下几方面内容：RF-UIM卡和读卡器之间的物理层、链路层、传输层、会话层的协议接口、调频机制等。

本规范起草单位：中国电信股份有限公司上海研究院

中国电信股份有限公司广州研究院

本规范归口单位：中国电信集团公司公众客户事业部

本规范主要起草人：　李峰、彭昭、王勇、张柳成、谢云、赵欣

目　　录

# 1. 范围

本标准作为2.4G RF-UIM卡和读写器之间的射频协议技术依据，详细规范了RF-UIM卡于读写器间射频通信的物理层、链路层、传输层、会话层的协议接口。

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] | | 《中国电信2.4G RF-UIM卡需求规范》 | 中国电信 |

# 2. 术语、定义和缩略语

## 2.1. 缩略语

| | |
|---|---|
| ACK | 确认 |
| APDU | 应用协议数据单元 |
| ATR | 复位响应 |
| BCCH | 广播控制信道 |
| BCD | 十进制数的二进制编码 |
| CCP | 性能配置参数 |
| CHV | 卡持有人校验信息；用来校验用户身份的存取条件 |
| CLA | 命令类 |
| CLK | 时钟 |
| CRC | 循环冗余校验 |
| DCS | 数字蜂窝系统 |
| IC | 集成电路 |

| | |
|---|---|
| ICC | 集成电路卡 |
| ID-1 | 插拔式（UIM 卡） |
| IEC | 国际电子技术委员会 |
| INS | 命令报文的指令字节 |
| IMSI | 国际移动用户识别号 |
| ISO | 国际标准化组织 |
| IUT | 经测试实现 |
| LGTH | 数据单元的长度 |
| ME | 移动设备 |
| MSB | 最高有效位 |
| RST | 复位 |
| UIM | 用户识别模块 |
| TP | 传输层协议 |
| TPDU | 传输协议数据单元 |

### 2.2. 符号

| | |
|---|---|
| ACK | 自动应答 |
| PLEN | 帧数据有效长度 |
| PID | 帧标识 |
| ACKID | 应答标识 |

## 3. 协议层次

### 3.1. 协议划分

本协议根据 OSI 参考模型的原理压条法设计，需特别注意穿越边界的交互作用的最小限度。四层定义如下：

——对实现数据包传输载体的物理层。

——对数据包处理的数据链路层。

——为使系统开销最小而与数据链路层结合的传输层。

——与应用层接口的处理应用数据的会话层。

本规范规定的协议层次关系如图 1 协议层次划分。

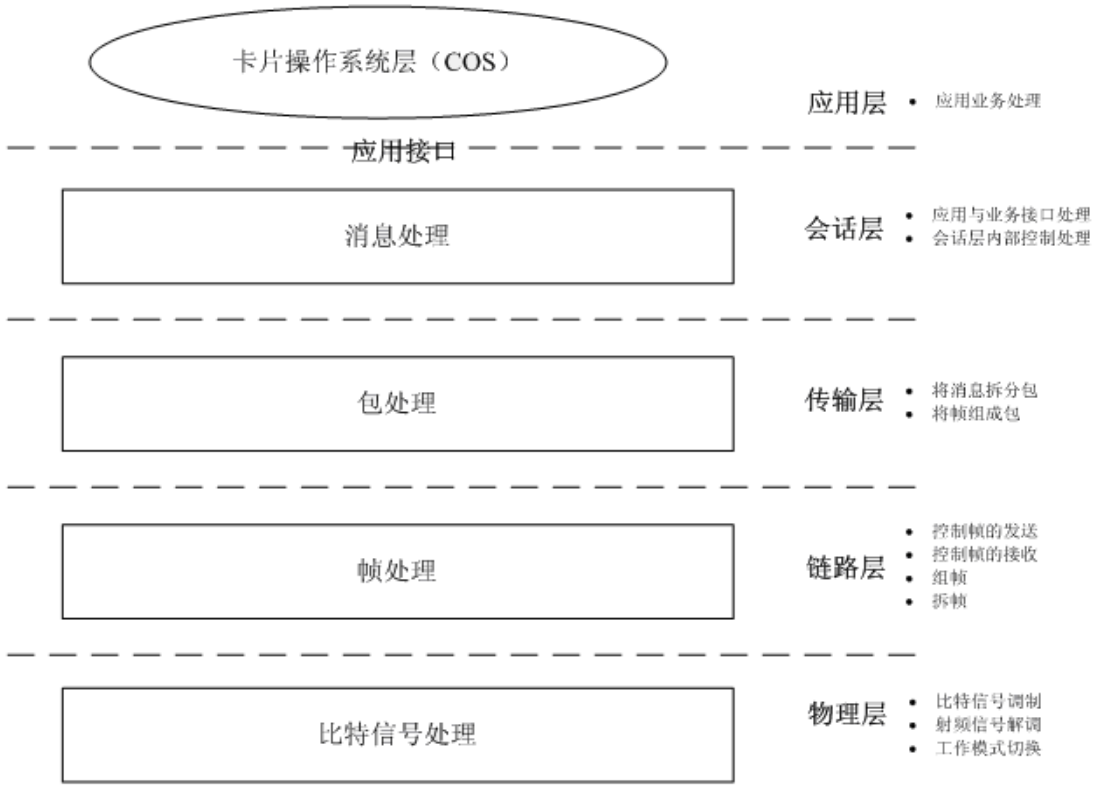



图 1 协议层次划分

3.2. 协议关系

本规范定义各层事务处理的基本单位，规定如下：

帧： 定义为链路层最小数据处理的单位，链路处理行为均基于帧进行处理，对有效数据进行扩展，形成信道能够稳定传输的机制。

包： 定义为传输层处理的最小数据单位，传输层处理行为均基于包进行处理，对有效帧进行扩展，从而形成批量数据的传输机制。

消息：定义为会话层处理的最小数据单位，会话层处理行为均基于消息进行处理，对包进行扩展，从而能够支持业务与应用层处理相应业务的接口。

帧、包、消息的关系如图 2 所示：

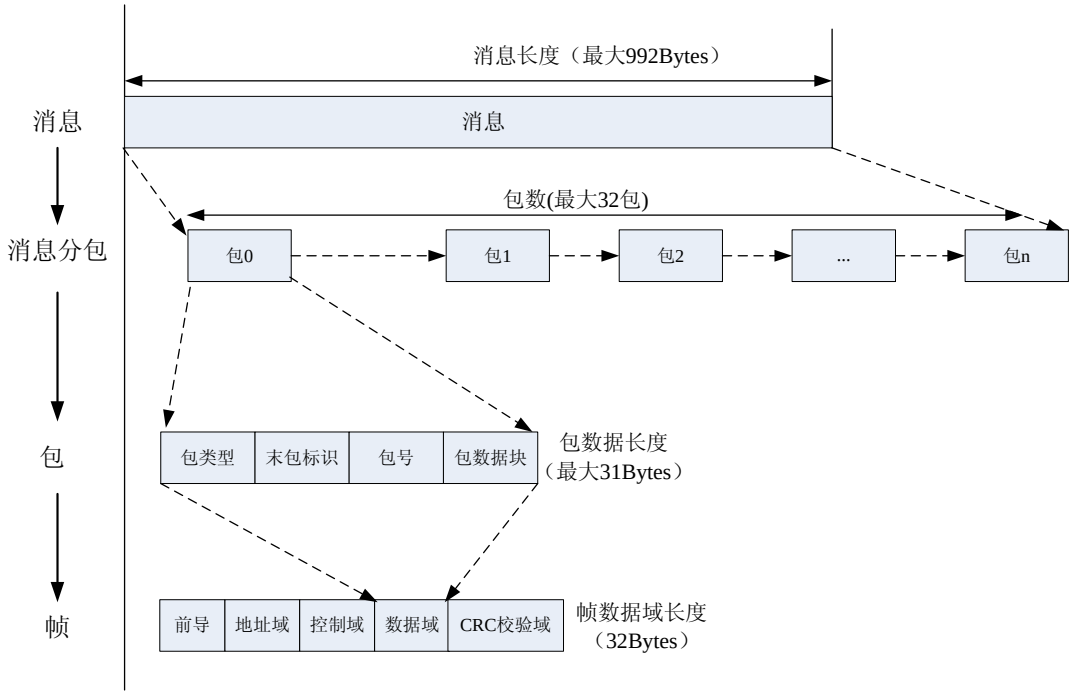



图 2 协议单元关系

## 4. 物理层

物理层提供数据接收与发送的通道。

射频相关部分符合工信部无线电管理局《微功率（短距离）无线电设备的技术要求》相关要求。

### 4.1. 频道

RF-UIM 卡采用 2.4G ISM 频段，分 2 种类型的频道：工作频道和辅助接入频道。工作频道支持 8 个频点，辅助接入频道 1 个频点。

工作频道：用于业务通信。

| 频点 1 | 频点 2 | 频点 3 | 频点 4 | 频点 5 | 频点 6 | 频点 7 | 频点 8 |
|---|---|---|---|---|---|---|---|
| 2478 MHz | 2450 MHz | 2410 MHz | 2442 MHz | 2469 MHz | 2425 MHz | 2460 MHz | 2435 MHz |

辅助接入频道：用于辅助询卡，频点为 2483MHz。

### 4.2. 传输速率

本规范中在进行数据交互通信期间，近距离应用空中传输的数据波特率应为 1Mbps。

4.3. 调制方式

本规范中射频部分采用 GFSK 调制方式，在载频频点 $f_c$ 基础上迭加调制频率 $f_s$ 。即发送符号“1”的频率为 $f_c+f_s$。发送符号“0”的频率为 $f_c-f_s$。载频频点为本规范中 4.1 节所列频点。调制方式如图 3 所示：

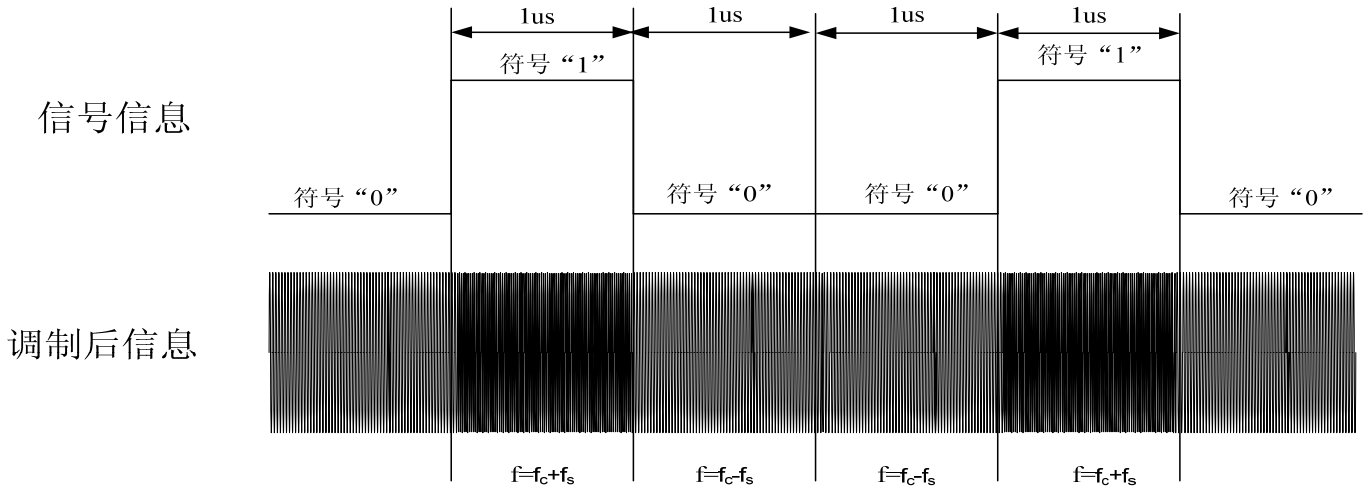



**图 3 调制方式**

4.4. 输出功率

本规范中卡射频部分最大输出功率为 0dBm。

4.5. 无线传输控制

在 ATI 消息中有两字节功率控制参数，一个为卡特性参数，另一个为 pos 辅助参数。Pos 收到 ATI 消息后，根据参数与卡片协同修正功率，然后通过 RCREQ 消息通知卡片，卡片发送 CCRSP 消息，读写器通过 CCRSP 消息对距离进行判断，如在允许范围则接入，否则失败。功率控制参数可通过以下三种设置模式：一、用户通过 UTK 菜单设置，厂家提供各型号手机参考值；二、通过校正仪方式设置。

### 4.5.1. UTK 菜单设置

a.先固定【灵敏度】当前菜单下参数不变，把【校正】菜单距离参数调弱或调强一个级别，然后再测试距离是否满意，否则继续调节校正的参数，直到参数值使用完。

校正：包含0（稍弱），1（弱），2（弱强），3（强），4(很强)五个选项

b.如果【a】的校正参数使用完，还是不理想，就把灵敏度参数调弱或调强一个级别，然后重复【a】的操作步骤，直到刷卡距离理想为止。

灵敏度：0（稍弱），1（弱），2（弱强），3（强）四个选项。

选择其中一项就表示确认。选项前出现“*”,表示此选项功能被开启。

缺省的【近距离】距离参数为【灵敏度：1】，【校正：2】，请谨慎修改近距离参数。

#### 4.5.2. 校正仪设置

校正仪为RF-UIM卡专用定距设备。用户只需将装有RF-UIM卡的手机放在指定的位置，然后按下校正仪上的【启动】按键。此时，校正仪开始对RF-UIM卡进行距离探测，校正仪及RF-UIM卡分别记录各自采集到的数据，最后由校正仪负责对数据进行分析，得出合适的功率控制参数，并回设至RF-UIM卡。整个定距过程大约需要持续1-3分钟。

## 4.6. 距离认证

本规范采用功率控制模式实现对卡片的有效刷卡距离认证。首先确保读写器接收灵敏可动态调节，推荐取值范围为[-52,-20]dbm；其次确保卡片发送功率可调。卡片根据 ATI 消息中的卡片特性调整发送功率，发送距离认证消息；读卡根据收到 ATI 消息中的辅助参数调整接收灵敏度，接收距离认证消息。

卡片收到 INQUIRY 消息后，通过 ATI 消息把距离控制参数发送给读写器，读头根据该卡片的参数调节发射功率和接收灵敏度，通过调节参数后的 RCREQ 和 CCRSP 消息判断卡是否在允许接入范围。

# 5. 链路层

本规范中链路层对发送的数据进行组帧，对接收的数据进行解帧。

## 5.1. 帧格式

### 5.1.1. 帧结构

表 1 帧结构

| 前导 | 地址域 | 控制域 | 数据域 | CRC 校验域 |
|---|---|---|---|---|

#### 5.1.1.1. 前导

本规范中定义前导为 01010101 或 10101010 序列，具体由地址域最高位决定，如果地址域的最高位为 0，则前导为 01010101，如果地址的最高位为 1，则前导为 10101010。

#### 5.1.1.2. 地址域

本规范中定义地址域为接收正确帧的识别地址，定义为 5 字节，各字节取值范围从

0x00 到 0xFF。

5.1.1.3. 控制域

本规范中使用有效帧长度为 6bits，则控制域长度为 9bits。见表 2 所示。

表 2 帧控制域信息

| 有效帧长度<br>PLEN | 帧标识<br>PID | 应答标识<br>ACKID |
|---|---|---|
| 6bits | 2bits | 1bit |

5.1.1.3.1. 有效帧长度

本规范中定义有效帧长度。
有效帧长度为 6bits。
含义如下：

0:0byte
1:1byte
……
32：32bytes

5.1.1.3.2. 帧标识

本规范中定义为接收新帧的识别码，共 2bits，相邻不同帧的帧标识不同。
00 0 号帧
01 0 号帧
。。

5.1.1.3.3. 应答标识

本规范中自动应答标识位为接收方接收到帧后，判断此标识来确定是否发送一个应答帧。如果接收帧中该标志位为高，则接收方将自动发送一个应答帧。如果接收帧中该标志位为低，则接收方将不发送应答帧。

0 无应答
1 有应答

5.1.1.4. 数据域

本规范中定义为所需要的传输数据。
本规范支持长度的数据如下：

有效帧长度为 6bits，可支持最大 32 字节有效长度数据传输。

#### 5.1.1.5. CRC 校验域

本规范定义为帧的 CRC 校验，链路层以此判断该帧的传输是否正确，并规定 CRC 的校验域为可选：

1）0-2 字节宽度的 CRC 校验

2）8 位 CRC 校验的多项式是 $X^8 + X^2 + X + 1$

3）16 位 CRC 校验的多项式是： $X^{16}+ X^{12} + X^5 + 1$.

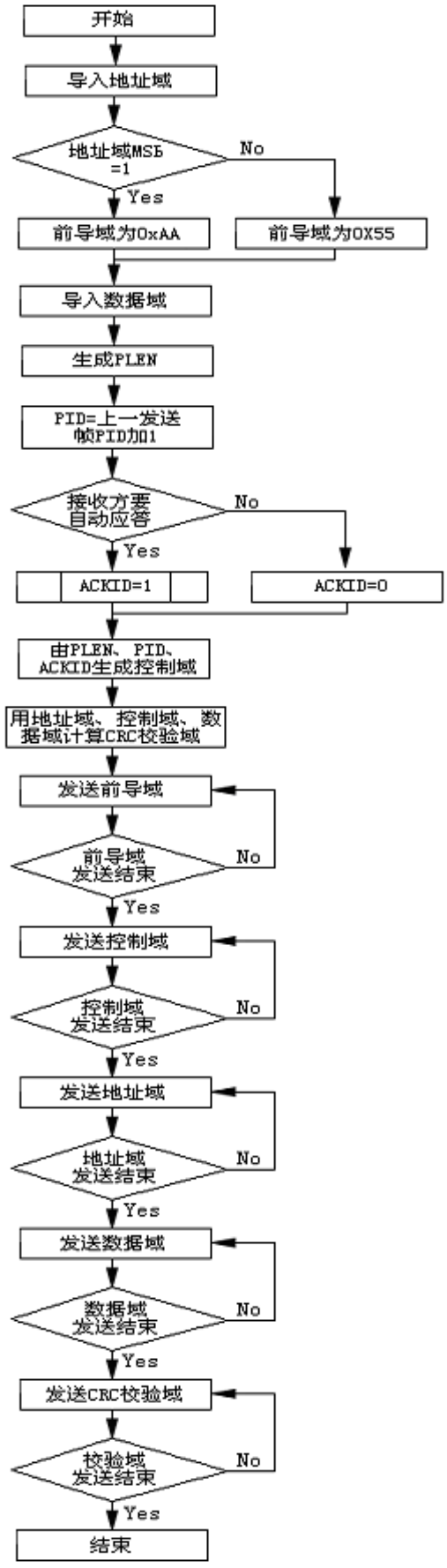
本规范定义 CRC 的计算包含了地址域、控制域、数据域；帧前导和 CRC 域本身不参加计算。

## 5.2. 组帧与解帧

### 5.2.1. 组帧

本规范定义组帧的行为如下：

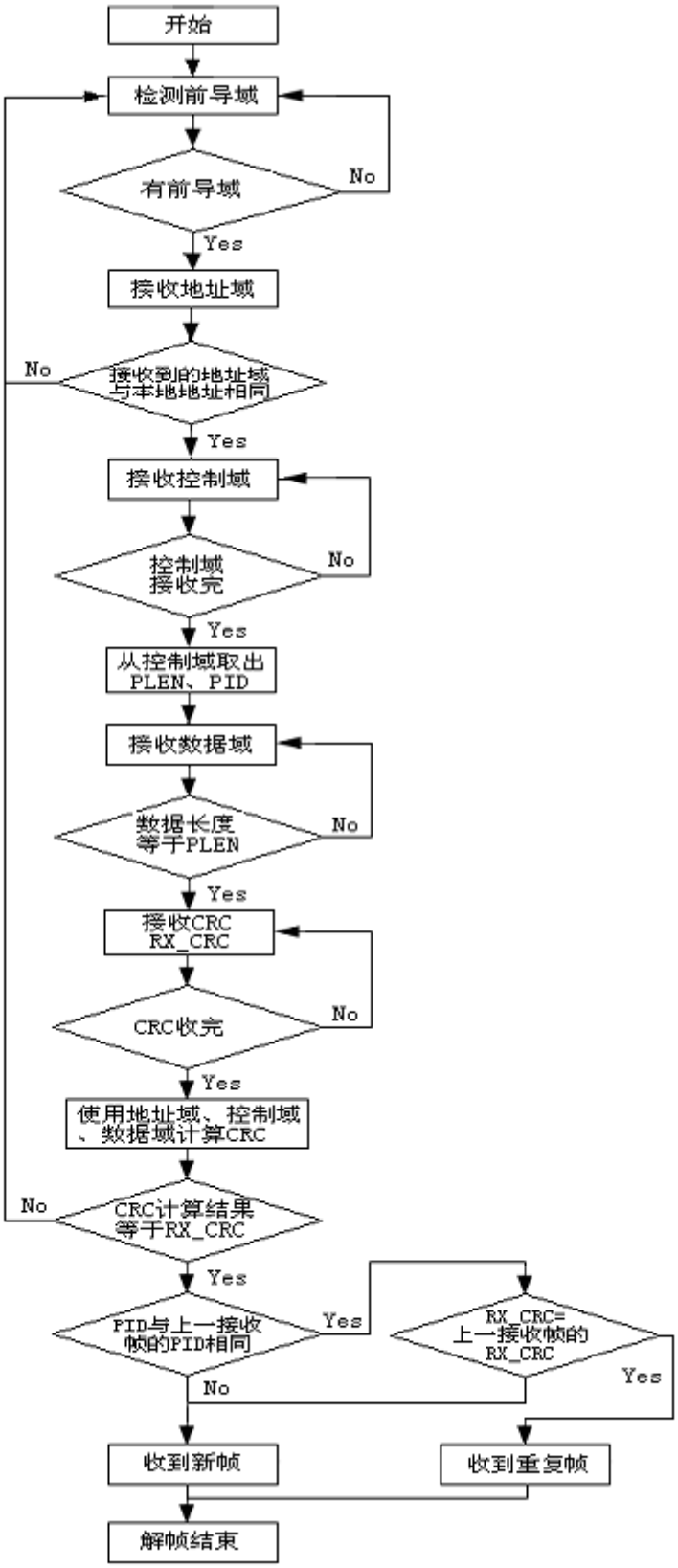
将发送的数据按照帧规定的结构组织在一起形成一个帧，并按照先发送前导域,最后发送 CRC 校验域的方式经过物理层调制成高频信号发送出去。


开始
导入地址域
地址域MSB =1
No
Yes
前导域为0xAA
前导域为0X55
导入数据域
生成PLEN
PID=上一发送帧PID加1
接收方要自动应答
No
Yes
ACKID=1
ACKID=0
由PLEN、PID、ACKID生成控制域
用地址域、控制域、数据域计算CRC校验域
发送前导域
前导域发送结束
No
Yes
发送控制域
控制域发送结束
No
Yes
发送地址域
地址域发送结束
No
Yes
发送数据域
数据域发送结束
No
Yes
发送CRC校验域
校验域发送结束
No
Yes
结束

图表 4 组帧过程

#### 5.2.2. 解帧

将物理层接收到射频信号解调成数字单比特信号后按照帧结构解帧，解出有效的数据信号。


开始
检测前导域
有前导域
No
Yes
接收地址域
No
接收到的地址域
与本地地址相同
Yes
接收控制域
控制域
接收完
No
Yes
从控制域取出
PLEN、PID
接收数据域
数据长度
等于PLEN
No
Yes
接收CRC
RX_CRC
CRC收完
No
Yes
使用地址域、控制域
、数据域计算CRC
No
CRC计算结果
等于RX_CRC
Yes
PID与上一接收
帧的PID相同
Yes
RX_CRC=
上一接收帧的
RX_CRC
Yes
No
收到新帧
收到重复帧
解帧结束

图表 5 解帧过程

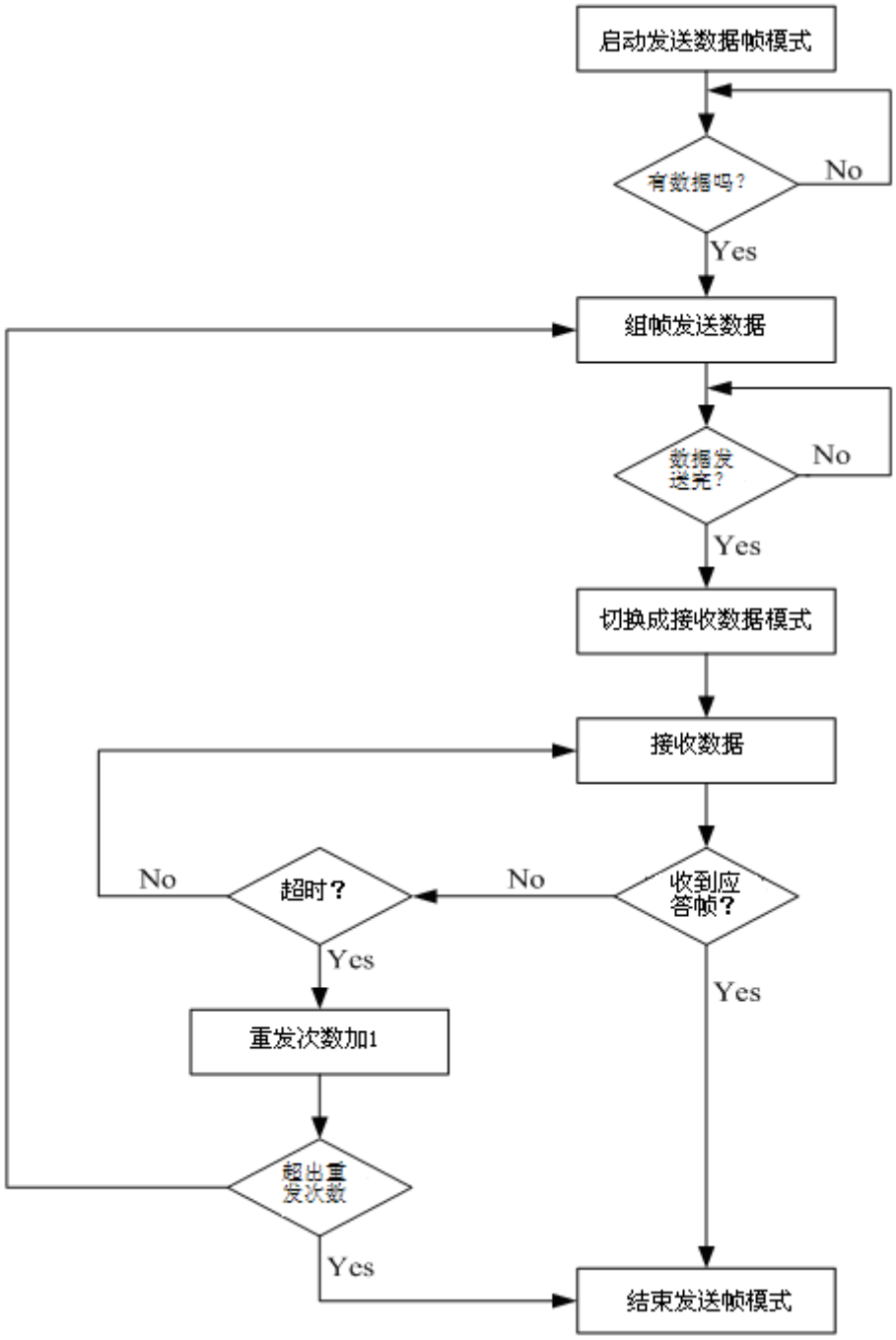
## 5.3. 帧处理协议

### 5.3.1. 发送处理过程

本规范中发送处理帧协议为处理 5.1 节所规定的帧结构，主要分 2 部分：

1） 组帧发送当前数据。

2） 发送数据完毕后，接收对此帧发送数据的应答帧。




图表 6 发送帧处理

若收不到当前发送帧的应答帧，则按照预设的重发次数重新发送当前数据，在预设的重发次数内没有接收到应答帧，则规定此次发送的数据失败。

本规范定义重发次数不超过 15 次。

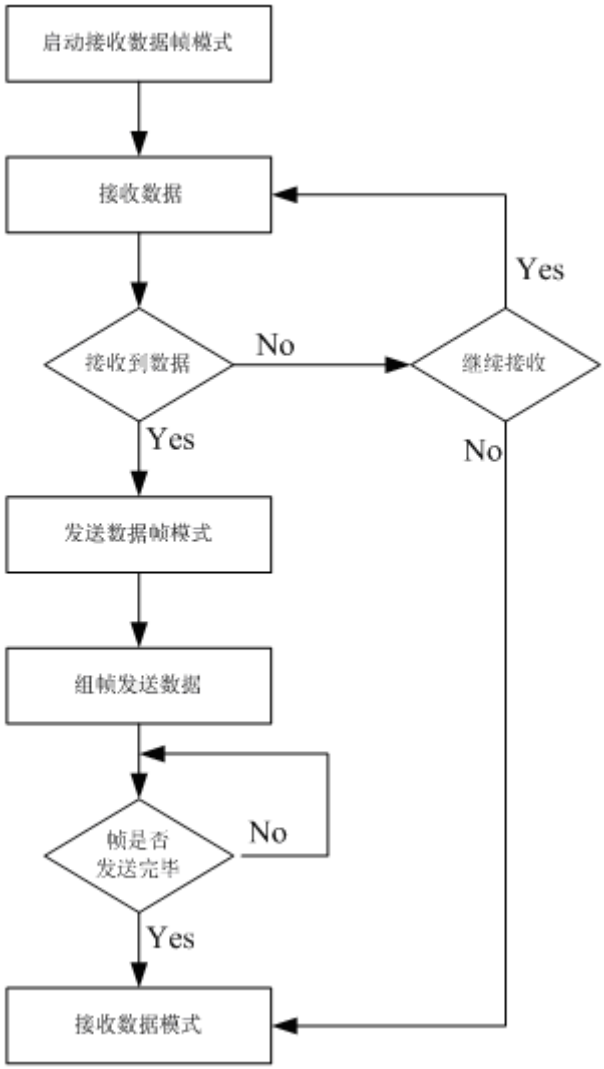
本规范定义发送新帧的 Timeout 时间最大 5ms。

### 5.3.2. 接收处理过程

本规范中接收处理协议为处理 5.1 节所规定的帧结构，主要分 2 部分：

1） 接收当前数据。

2） 发送接收到当前数据的应答帧。




图表 7 接收帧处理

本规范中发送当前接收到数据的应答帧，应答帧的帧结构同本规范中 5.1 节所规定的帧结构。

# 6. 传输层

本规范中传输层处理与会话层的接口协议。由包组成消息。

## 6.1. 包

包分成控制包和数据包，控制包单包（一帧）组成消息，数据包一般由多包（多帧）组成消息。

### 6.1.1. 包协议格式

本规范中消息由多个连续的包组成，包之间按照特定的协议格式组成一个完整的消息。
本规范中规定包协议格式如下：

图表 8 包协议格式

| 包头(1Byte) | 包数据块(最大 31Bytes) |
|---|---|

### 6.1.2. 包头

| | 包类型 | 包头值 |
|---|---|---|
| 控制包 | INQUIRY | 0XC0 |
| | ATI | 0XC1 |
| | RCREQ | 0XC2 |
| | CCRSP | 0XC3 |
| | CLOSE | 0XC4 |
| 数据包 | APDU_REQ | 0XD0 |
| | APDU_RESP | 0XD8 |
| | | |
| | | |

### 6.1.3. 控制包

RF 通信握手或通信控制包，控制包的格式请见后面的详细说明。

### 6.1.4. 数据包

控制包的包数据是通信开始的握手包/消息；数据包的包数据一般由多包组成的消息。

6.1.4.1. 数据包的格式

| 字段 | 长度(字节) | 值 | 注释 | 方向 |
|---|---|---|---|---|
| MsgType | 1 | XX | 消息类型 | 读写器<----->卡片 |
| BatchNo | 1 | XX | 批次号。 | |
| PatchNo | 1 | XX | 分包编号 | |
| DataLen | 1 | XX | 数据长度 | |
| Data | 28 | XX | 数据 | |

**MsgType 字段编码：**

从读写器到卡片，值为 APDU_REQ；从卡片到读写器，值为 APDU_RESP。

**BatchNo 字段编码：**

连接初始值为 0，每发送或接收一次指令加一。

**PatchNo 字段编码：**

| PatchNo 数据（1 字节） | | | | | | | |
|---|---|---|---|---|---|---|---|
| b7 | b6 | b5 | b4 | b3 | b2 | b1 | b0 |
| 1：末包 | 保留为 0 | 包号，取值范围 0～9 | | | | | |

**DataLen 字段编码：**

取值范围从 1 到 28。

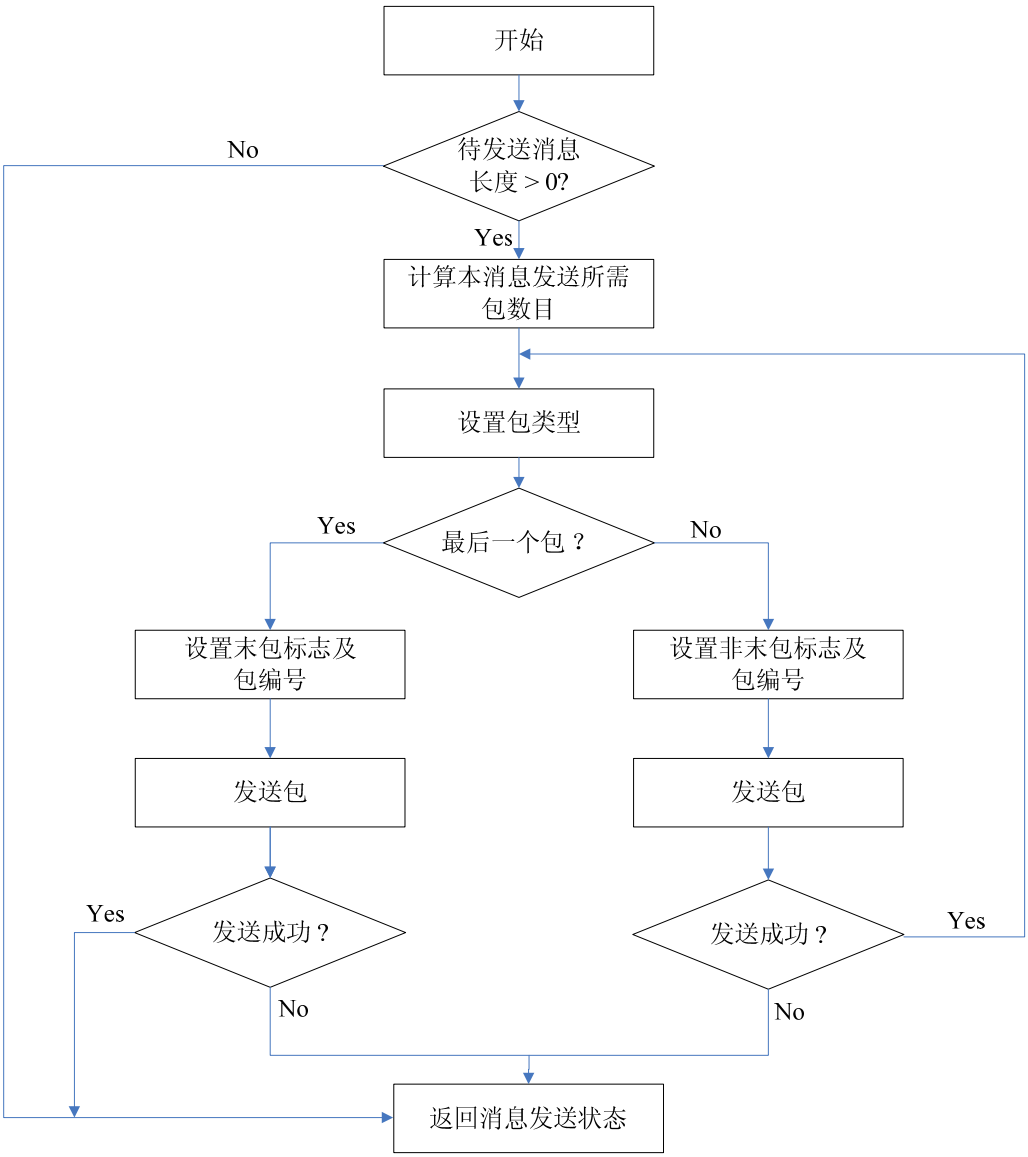
**Data 字段编码：**

数据内容，有效长度由 DataLen 字段决定。

## 6.2. 分包与组包

### 6.2.1. 分包发送

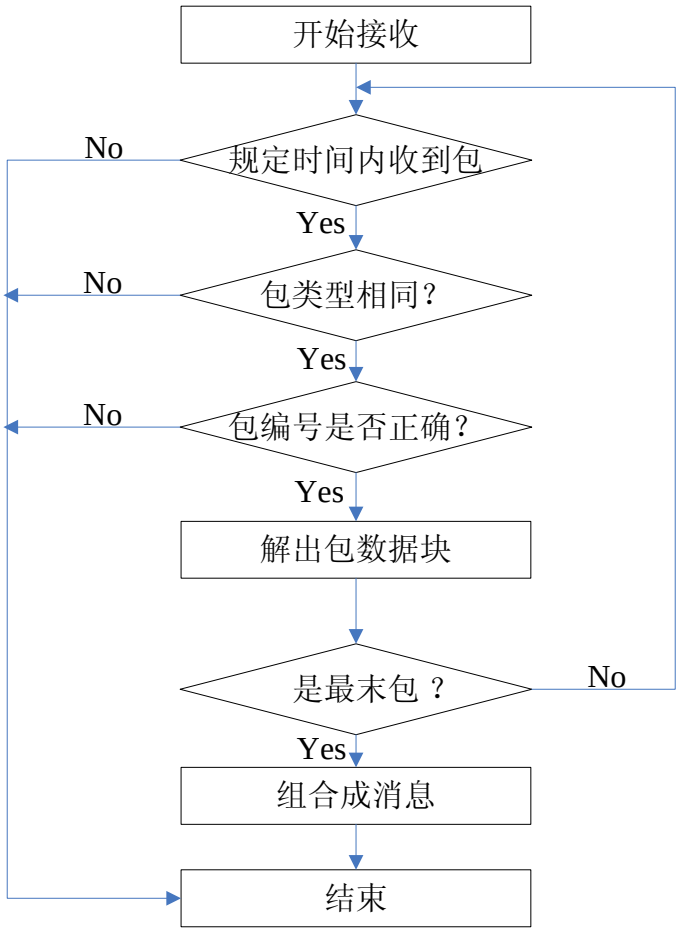
本规范中定义的分包是将消息划分多个包，然后将相应包分片依次发送出去。发送端在发送消息的时候，会将消息拆分成规定的包，然后按照包定义的格式，包编号从0开始，依次递增，逐次地发送出去，每一包都检查是否发送成功，如果成功，就继续发送，直到发送完成；如果在此过程中，有任意一包没有发送成功，则认为整个消息发送失败。




图表8 分包发送流程

6.2.2. 接收组包

本规范中定义的接收组包是将链路层收到的包还原成相应的消息。

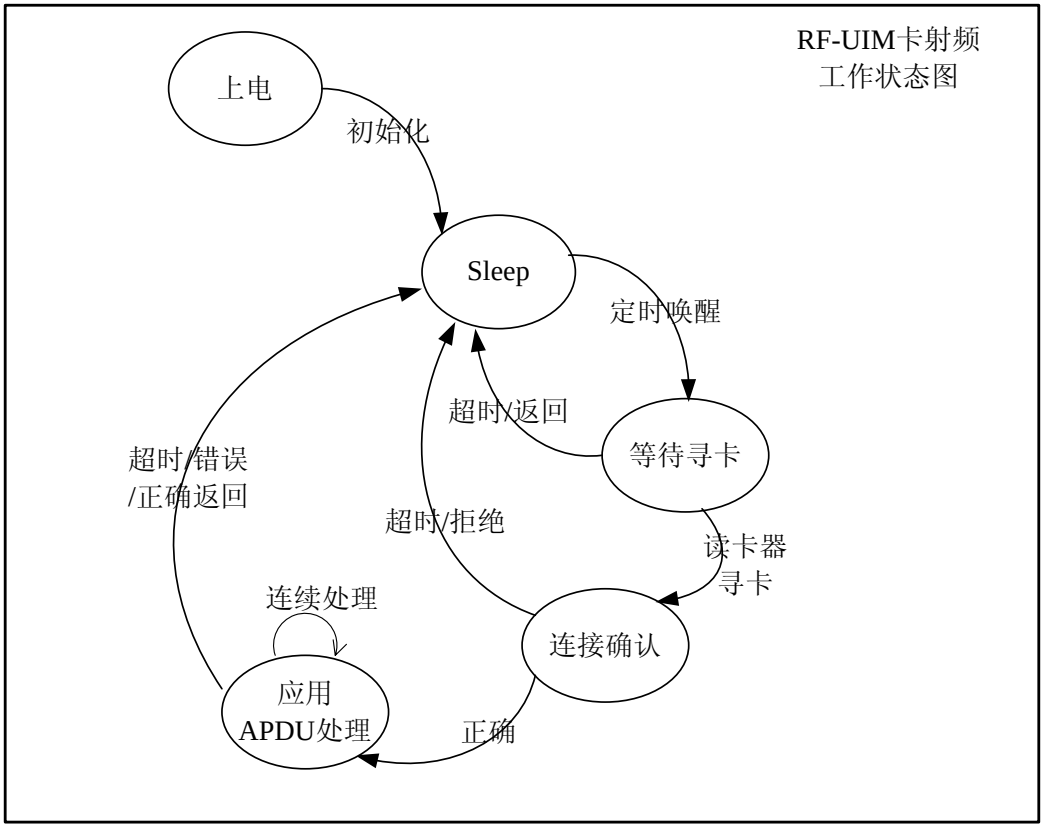



图表 9 接收组包流程

## 7. 会话层

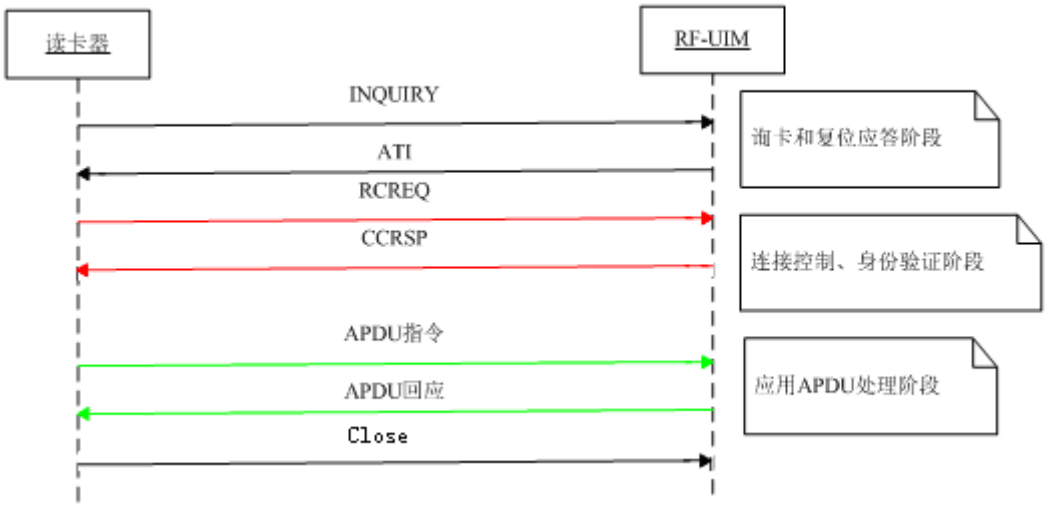
本规范定义了会话层消息类型、消息格式、消息交互流程。会话层主要功能是为应用层提供信息交换的可靠手段，为话层为应用层提供会话的建立，维护与断开功能，并可以对应用层数据进行进行加密，以保证会话的安全性。

RF-UIM 卡射频工作状态描述如下：




7. 1. 消息序列

读写器与 RF-UIM 卡通信消息序列




图表 9－1 被动询卡消息序列

## 7.2. 消息格式

### 7.2.1. 握手消息

本规范定义在层内定义 5 种层内消息，以支持层内事务处理：

1) INQUIRY 消息
2) ATI 消息
3) RCREQ 消息
4) CCRSP 消息
5) Close 消息

#### 7.2.1.1. INQUIRY 消息

本规范定义 INQUIRY 消息为读写器向 RF-UIM 卡发送的询卡命令。

| 字段 | 长度(字节) | 值 | 注释 | 方向 |
|---|---|---|---|---|
| MsgType | 1 | 0xc0 | 消息类型 | 读写器----->卡片 |
| Channel | 1 | XX | 下一步通信频道 | |
| Flag | 1 | XX | 特性值 | |
| Collision | 1 | XX | 防冲突数值 | |
| Read | 1 | XX | 读写器厂家编号 | |
| Power | 1 | XX | 读写器功率 | |
| CollisionBound | 1 | XX | 防冲突范围 | |
| Addr | 5 | XX | 下一步通信地址 | |
| Fam | 4 | XX | 认证参数 | |

**MsgType 字段编码：**

值为 0xC0，表示寻卡消息，由单包组成。

**Channel 字段编码:**

下一步通信频道(要加 2400MHz),例如目标通信频道为:2450MHz,则为 2450-2400 = 50。该频点必须是规范 4.1 所规定的 8 个工作频点之一。

**Flag 字段编码：**

| Flag 数据（1 字节） | | | | | | | |
|---|---|---|---|---|---|---|---|
| b7 | b6 | b5 | b4 | b3 | b2 | b1 | b0 |
| 保留为 0 | 保留为 0 | 保留为 0 | 保留为 0 | 1：近距离 | 保留为 0 | 保留为 0 | 保留为 0 |

**Collision 字段编码：**

取值范围必须小于 CollisionBound 值。CollisionBound 为读头可同时支持的卡总数，Collision 为当前卡的随机值，例：CollisionBound 值为 16，则该字段取值范围为 0～15。

**Read 字段编码：**

读写器厂家编号。

**Power 字段编码：**

读写器发射功率，取值范围 0x00～0x03。

0：读写器发射功率-18dbm

1：读写器发射功率-12dbm

2：读写器发射功率-6dbm

3：读写器发射功率 0dbm

**CollisionBound 字段编码：**

防冲突范围，取值范围从 0x00～0xFF，为 0 表示不使能防冲突。例：为 10 表示该读头同时支持 10 张卡进行防冲突刷卡。

**Addr 字段编码：**

下一步通信地址，取值范围从 0x00～0xFF。由读头随机产生。

**Fam 字段编码:**

认证参数，卡需要判断 INQUIRY 消息和 RCREQ 消息的 Fam 参数是否一致，取值范围 0x00～0xFF。由读头随机产生。

7.2.1.2. ATI 消息

本规范定义 ATI 消息为 RF-UIM 卡收到 INQUIRY 消息后，利用广播地址向读写器发送的应答消息。

| 字段 | 长度(字节) | 值 | 注释 | 方向 |
|---|---|---|---|---|
| MsgType | 1 | XX | 消息类型 | 卡片---->读写器 |

| | | | | |
|---|---|---|---|---|
| AutoFill | 7 | XX | 填充字节 | |
| CardID | 8 | XX | 卡片 ICID | |
| Addr | 5 | XX | 下一步通信地址 | |
| Cstatus | 3 | XX | 卡状态 | |
| Random | 4 | XX | 随机数 | |
| PowerControl | 4 | XX | 功率控制参数 | |

**MsgType 字段编码：**

值为 0xC1，表示 Ati 消息，由单包组成。

**AutoFill 字段编码:**

填充字节，取值范围从 0x00 到 0xFF。消息长度会影响接收灵敏度，所以 Ati 消息必须为 32 字节。

**CardID 字段编码：**

卡片 ICID，卡片唯一识别号（使用卡片硬件唯一 ID)。

16 位 BCD 码，MXXXXXXXXXXXXXXX

M 为：厂商编号（0 为盛华、1 为直通，其他待定)。

**Addr 字段编码：**

下一步通信地址，取值范围从 0x00～0xFF。由卡随机产生。

**Cstatus 字节编码：**

卡状态字节，目前用到第二字节，值 0x01 为 rf 开启。其余两字节值为 0x00。

**PowerControl 字节编码：**

| PowerControl 数据（4 字节） | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | b7 | b6 | b5 | b4 | b3 | b2 | b1 | b0 |
| 1 | 近距离 UIM 卡射频功率（0～3） | | | | 近距离读写器射频功率（0～3） | | | |
| 2 | 近距离读写器微调参数（0～32） | | | | | | | |
| 3 | 中远距离 UIM 卡射频功率（0～3） | | | | 中远距离读写器射频功率（0～3） | | | |
| 4 | 中远距离读写器微调参数（0～32） | | | | | | | |

7.2.1.3. RCREQ 消息

本规范定义 RCREQ 消息为读写器向 RF-UIM 卡通过私有地址发送的连接请求。

| 字段 | 长度(字节) | 值 | 注释 | 方向 |
|---|---|---|---|---|
| MsgType | 1 | XX | 消息类型 | |

| | | | | |
|---|---|---|---|---|
| Flag | 1 | XX | 通讯标志 | 卡片----->读写器 |
| Result | 1 | XX | 读写器返回参数 | |
| Delay | 1 | XX | 延时时间 | |
| Fam | 4 | XX | 认证参数 | |
| Random | 4 | XX | 读写器随机数 | |
| TermID | 8 | XX | 读写器唯一 ID | |
| Date | 4 | XX | 读写器时间 | |
| AutoFill | 4 | XX | 填充字节 | |

**MsgType 字段编码：**

值为 0xC2，表示 RCREQ 消息，由单包组成。

**Flag 字段编码:**

和 INQUIRY 消息中 Flag 字段同一值。

**Delay 字段编码：**

卡下次刷卡延时时间，单位为 100 毫秒，例：delay=10，表示同张卡同个读写器两次刷卡间隔为 1000 毫秒。

**Fam 字段编码:**

认证参数，卡需要判断 INQUIRY 消息和 RCREQ 消息的 Fam 参数一致，取值范围 0x00～0xFF。

**TermID 字节编码：**

读写器 ID，读写器唯一识别号（使用读写器硬件唯一 ID)。

16 位 BCD 码，MXXXXXXXXXXXXXXX

M 为：厂商编号（0 为盛华、1 为直通，其他待定)。

**Date 字段编码：**

读写器时间戳（公元 1970 年 1 月 1 日的 UTC 时间从 0 时 0 分 0 秒算起到现在所经过的秒数)，为 int 类型。

**AutoFill 字段编码：**

填充字节，取值范围 0x00～0xFF。

7.2.1.4. CCRSP 消息

本规范定义 CCRSP 消息为 RF-UIM 卡对读写器连接请求的回应。

| 字段 | 长度（字节） | 值 | 注释 | 方向 |
|---|---|---|---|---|
| MsgType | 1 | XX | 消息类型 | 卡片----->读写器 |
| AutoFill | 27 | XX | 填充字节 | |

**MsgType 字段编码：**

值为 0xC3，表示 CCRSP 消息，由单包组成。

**AutoFill 字段编码：**

填充字节，取值范围 0x00～0xFF。

7.2.1.5. CLOSE 消息

本规范定义 CLOSE 消息为 RF-UIM 卡对读写器断开连接消息。

| 字段 | 长度（字节） | 值 | 注释 | 方向 |
|---|---|---|---|---|
| MsgType | 1 | XX | 消息类型 | 卡片----->读写器 |
| Disconnec | 1 | XX | 断开标志 | |
| TermID | 8 | XX | 读写器唯一 ID | |

**MsgType 字段编码：**

值为 0xC5，表示 CLOSE 消息，由单包组成。

**Disconnec 字段编码：**

值为 0x01，连接断开。

**TermID 字段编码：**

读写器 ID。卡需和 RCREQ 消息 TermID 比较是否一致。

7.2.2. 应用消息

本规范定义层外消息为应用层接口的消息类型，为处理应用层相关事务的接口，如下：
APDATA 应用数据消息

7.2.2.1. APDATA 消息

本规范定义 APDATA 应用数据消息包含应用层之间传递的数据。

在发送 RF 指令前，和 RF 应用数据解包之后就是 APDU 的下发指令和卡的响应数据。数据格式在本规范 6.1.4 数据包。

## 8. 跳频接入机制

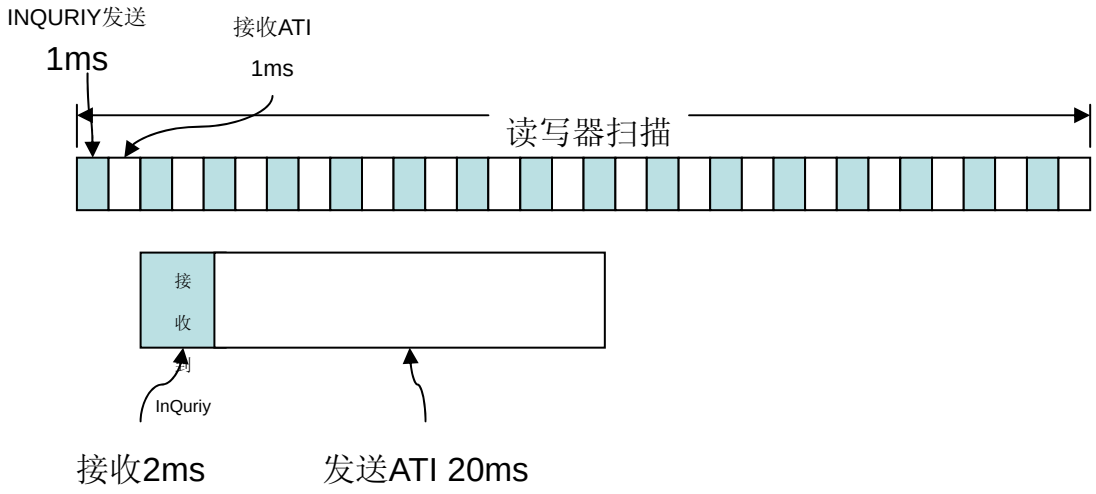
RF-UIM 卡采用跳频技术实现防干扰和抗冲突功能。卡片和读写器共使用到 9 个工作频点，其中 1 个为辅助接入频点，其它 8 个为工作频点。具体值在本规范 4.1 频道。

8.1.1.1. 第一阶段

A、 卡片定时唤醒检测到辅助接入频点有信号后进入第二阶段
B、 卡片定时唤醒时间最快为 200ms
C、 辅助接入频点频点为 2483MHz

8.1.1.2. 第二阶段

A、 读写器在辅助接入频点发送 INQUIRY（1ms）
B、 卡片每次唤醒后在监听辅助接入频点等待读写器 INQUIRY，如果接收到载波则在 8 个工作频道轮流回应 ATI，如果收到 INQUIRY 后即在 INQUIRY 指定的频道回应 ATI，开始会话连接过程;



## 9. 射频特征参数指标要求

根据《微功率（短距离）无线电设备的技术要求》规定，RF-UIM 卡为 F 类设备。

### 9.1. F 类设备

本类设备是指工作于2400－2483.5MHz频段，除数字无绳电话、蓝牙设备和无线局域网设备以外的其它短距离无线电设备。

1. 使用频率:2400-2483.50MHz
2. 发射功率限值：10mW(e.i.r.p)
3. 频率容限：75kHz

### 9.2. 杂散辐射发射测量频率指标

#### 9.2.1. 杂散辐射发射测量频率范围：

| 工作频率范围 | 杂散辐射测量频率范围 | |
|---|---|---|
| | 下限 | 上限 |
| 9kHz～100MHz | 9kHz | 1GHz |
| 100MHz～600MHz | 30MHz | 10 次谐波 |
| 600MHz～2.5GHz | 30MHz | 12.75GHz |
| 2.5～13GHz | 30MHz | 26GHz |
| 13GHz 以上 | 30MHz | 2 次谐波 |

#### 9.2.2. 杂散辐射发射限值(杂散辐射与带外辐射的分界点为载波频率±2.5 倍的信道带宽)；

#### 9.2.3. 发射机以最大功率发射状态

| 频率范围 | 测试带宽 | 限值 | 检波方式 |
|---|---|---|---|
| 9kHz～150kHz | 200Hz(6dB) | 27dBμA/m(10 米处)(每倍频程/下降 3dB) | 准峰值 |
| 150kHz～10MHz | 9kHz(6dB) | | 准峰值 |
| 10MHz～30MHz | 9kHz(6dB) | -3.5dBμA/m(10 | 准峰值 |

| | | 米处) | |
|---|---|---|---|
| 30MHz～1GHz | 100kHz(3dB) | -36dBm | 有效值 |
| 1GHz～40GHz | 1MHz(3dB) | -30dBm | 有效值 |
| >40GHz | 1MHz(3dB) | -20dBm | 有效值 |

对于30MHz以上频段在规定的使用频率范围的上下限处的辐射功率不大于-80dBm/Hz(e.i.r.p)。30MHz以下频段，任何工作信道的占用带宽（99%能量）对应的上下限不能超过所规定的使用频率范围。

中国电信集团公司标准

Q/CT XXXX-2010

# 中国电信 2.4G RF-UIM 卡空间规划

（暂行）

中国电信集团公司

# 前　言

本规范是对中国电信移动支付RF-UIM卡在开展移动支付业务时的空间规划提出全面要求，是移动支付RF-UIM卡方案所需要遵循的纲领性技术文件。

本规范主要包括以下几方面内容：RF-UIM卡整体空间规划、RF-UIM卡模拟M1应用区规划、RF-UIM卡CPU应用区规划、翼支付UTK菜单、密钥和密码计算方法等。

本规范起草单位：中国电信股份有限公司广州研究院
中国电信股份有限公司上海研究院

本规范归口单位：中国电信集团公司公众客户事业部

本规范主要起草人：谢云 俞海宏 王勇

# 目　　录

# 1、名词和术语

本文档中使用的相关名词和术语统一说明如下：

| 名词 | 说明 |
|---|---|
| AID | 应用标识（Application Identification） |
| CID | Card ID，模拟 Mifare 应用的卡片 ID，用于 2.4G RF-UIM 卡标识其中的模拟 Mifare 应用。 |
| RID | 注册机构标识（Registry Identification） |
| FID | 文件标识（File Identification） |
| RF | 无线电射频技术（Radio Frequency） |
| UIM | 用户识别模块（User Identity Model） |
| RF-UIM | 将 RF 技术集成到 UIM 卡上，支持支付、积分应用和身份识别应用的卡片，这里特指使用 2.4G 频率实现的 RFID UIM 卡。 |
| CRC | 循环冗余编码（Cyclic Redundancy Code） |
| OTA | 空中下载、圈存（Over To Air） |
| Mifare | NXP 公司的一种非接触式感应 IC 卡 |

# 2、RF-UIM 卡整体规划

## 2.1 RF-UIM 卡空间定义

RF-UIM 卡可用的 ROM 空间为 320K，目前已使用 160K，剩余 160K 空间；可用的 RAM 空间为 8K，其中系统使用 2.25K，基础射频功能使用 3.25K，电信功能及 RFID 应用功能合用 2.5K；EEPROM 总空间为 288K，是承载电信通信功能和 RFID 应用功能的空间。

RF-UIM 卡的总体空间分配如下表：

| | ROM | RAM | EEPROM |
|---|---|---|---|
| 基础射频空间 | 160K | 3.25K | 64K |
| 预置的模拟 M1 应用空间 | | | 24K（6 张模拟 M1 卡片应用） |
| 电信通信应用空间 | 无 | 2.50K | 133K |
| 集团定义的 CPU 应用空间 | | | 33.4K |
| 预留给省公司及第三方的 CPU 应用空间 | | | 33.6K |
| 总容量： | 320K | 8K(系统占用 2.25K) | 288K |

其中，ROM 是卡内的只读内存，用来保存不会被修改的代码；RAM 是随机存储器，用来存放在交易过程中产生的过程数据；EEPROM 是电可擦可编程只读存储器，用来写入应用代码以及应用数据。目前，2.4G RF-UIM 卡的应用代码和应用数据都使用 EEPROM 空间，对 EEPROM 的详细空间分配情况如下表：

中国电信 2.4G RF-UIM 卡空间规划

| 应用类型 | | 代码空间(k) | 数据空间(k) | 小计 | 备注 |
|---|---|---|---|---|---|
| 基础射频功能 | | 64 | 0 | 64 | |
| 电信通信应用 | 通信应用底层 COS | 40 | 0 | 40 | |
| | EVDO | 7 | 1 | 8 | |
| | OTA 及 UTK 菜单 | 30 | 8 | 38 | 支持数据短信通信能力和菜单动态更新 |
| | ESN 上报 | 1 | 0 | 1 | |
| | PRL 更新 | 4 | 1 | 5 | |
| | 单项全能读 | 1 | 0 | 1 | |
| | 短信 | 8 | 10 | 18 | 40 条 CDMA 短信 |
| | 通信录 | 0 | 7 | 7 | 250 个号码 |
| 模拟 M1 应用 | M1 应用 1 | 20 | 1 | 24 | |
| | M1 应用 2 | | 1 | | |
| | M1 应用 3 | | 1 | | |
| | M1 应用 4 | | 1 | | |
| CPU 应用 | 全国在线支付应用 | 30 | 0.2 | 33.4 | |
| | 全国积分应用 | | 0.2 | | |
| | 全国离线钱包应用 | | 1 | | |
| | 省公司预留应用 | | 1 | | |
| | 省公司预留应用 | | 1 | | |
| | 预留的应用空间 | 25 | 25.6 | 48.6 | |
| 总容量： | | 228 | 60 | 288 | |
| 可选应用 | 超级号薄 | 25 | 15<br>(500 条 AND) | 40 | 本应用可根据空间剩余程度可选加载 |
| | 国际双模 | 8 | 7 | 15 | 对于国际双模卡，本应用必选；<br>对于非国际双模卡，本应用不实现。 |

由于各卡商实现电信通信应用占用的代码空间并不一致，以上电信通信应用占用的 EEPROM 空间尽量按照较大值估算，空间分配较紧张，为保障 RFID 应用的实现以及预留足够空间给省公司及第三方合作方，本空间规划文档将超级号薄应用和国际双模应用作为可选应用。各卡商应尽量优化代码，以尽量保障在 288K 的 EEPROM 空间中实现上述的全部应用，包括可选的超级号薄应用。对于国际双模卡，国际双模功能必选实现，对于非国际双模卡，国际双模功能不实现。

## 2.2RF-UIM 卡整体空间规划

除电信通信应用外，RF-UIM 卡可提供模拟 Mifare 类应用（4 张 S50 的 M1 卡片）和标准 CPU 应用模式。

标准 CPU 应用使用 AID 标识应用，模拟 Mifare 应用使用 CID 标识不同 M1 的应用。基于实际应用场景，根据集团、省公司、合作方等不同管理机构，对 RF-UIM 卡进行了卡空间整体规划。

RF-UIM 卡的应用类型，CID/AID、空间、显示名称定义如下图所示：

| 编号 | 应用类型 | 电信 CID/AID | 初始 CID | 空间 | 显示名 |
|---|---|---|---|---|---|
| **模拟 Mifare 应用** | | | | | |
| **M1 应用 1** | **全国翼支付应用** | **MCTGEPAY** | **MCTGEPAY** | **1168Byte** | **翼支付** |
| M1 应用 2 | 集团级合作应用 | MCTGEUNN | MCTGEUNN | 1168Byte | 第三方（集团预留） |
| M1 应用 3 | 省内翼机通应用 | MCT+2 位省编码+3 位业务描述 | Mifare13 App | 1168Byte | 翼机通 |
| M1 应用 4 | 省内预留应用 1 | MCT+2 位省编码+3 位业务描述 | Mifare14 App | 1168Byte | 省应用 |
| **标准 CPU 应用** | | | | | |
| CPU 应用 1 | 全国翼支付应用 | D156000040100020 0000000100000000 | 翼支付 | 电信集团应用 | |
| CPU 应用 2 | 全国积分应用 | D156000040100020 0000000200000000 | 我的积分 | 电信集团应用 | |
| CPU 应用 3 | 全国电子钱包应用 | D156000040100030 0000000100000000 | 待定义 | 预留 | |
| CPU 应用 4 | 省公司预留 | 待定义 | 待定义 | 预留 | |
| CPU 应用 5 | 省公司预留 | 待定义 | 待定义 | 预留 | |
| CPU 应用 6 | 金融合作 | 待定义 | 待定义 | 预留给金融合作应用 | |

其中，集团定义的全国性应用使用 M1 应用 1、M1 应用 2 和 CPU 应用 1、CPU 应

用 2 以及 CPU 应用 3。各省可根据本省业务需要自定义 M1 应用 3、M1 应用 4 和 CPU 应用 4、CPU 应用 5、CPU 应用 6。同时，在 CPU 应用区还为省公司及合作伙伴预留了最大 48.6K 应用空间。

RF-UIM 卡上的 M1 应用 1 空间，规划为电信模拟 M1 应用的入口和 M1 应用的应用目录区，使用模拟 M1 应用时，接收端机具使用此应用区 CID 进行“寻卡”，并通过此应用空间中信息，获得整张 RF-UIM 上可使用的 M1 应用 CID 信息、卡片版本信息以及卡片应用特性，进行后续处理。CPU 应用使用 CPU 区的 DIR 目录文件获取 CPU 应用目录。

## 2.3 CID 定义

CID 用于标识 2.4G RF-UIM 卡内的 M1 应用，其定义规则如下：

1. M1 应用的 CID 采用以 M 开头的 8 位字节 ASCII 码；
2. 为保障集团应用的跨地区使用和受理，“M1 应用 1”的 CID 默认设置为“MCTGEPAY”，“M1 应用 2” CID 默认设置为“MCTGEUNN”；
3. “M1 应用 3”、“M1 应用 4”由各省进行规划，这两个 M1 应用的 CID 的命名由各省定义，各省的自定义的 CID 命名规则如下：
   a) M1 应用 3 和 M1 应用 4 的 CID 前 3 位以“MCT”开头，
   b) 第 4、5 位为各省的省编码，省编码的编码规则是取各省名称前两个汉字的中文拼音的前两个字母，并对拼音首字母有冲突的省份进行约定。各省的省编码见下表：

| 省份 | 编码 | 省份 | 编码 | 省份 | 编码 |
|---|---|---|---|---|---|
| 北京 | BJ | 广东 | GD | 上海 | SH |
| 天津 | TJ | 重庆 | CQ | 辽宁 | LN |
| 江苏 | JS | 湖北 | HB | 四川 | SC |
| 陕西 | SX | 河北 | HE | 山西 | SY |
| 河南 | HN | 吉林 | JL | 黑龙江 | HL |
| 内蒙古 | NM | 山东 | SD | 安徽 | AH |
| 浙江 | ZJ | 福建 | FJ | 湖南 | HU |

| | | | | | |
|---|---|---|---|---|---|
| 广西 | GX | 江西 | JX | 贵州 | GZ |
| 云南 | YN | 西藏 | XZ | 甘肃 | GS |
| 宁夏 | NX | 青海 | QH | 海南 | HI |
| 新疆 | XJ | 澳门 | AM | 香港 | XG |

c) 第 6、7、8 字节为各省自定义的业务描述。

省 CID 命名举例：北京翼机通应用可命名为：“MCTBJYJT”。

# 3、M1 应用 1 扇区规划

M1 应用 1 有两个主要功能：

1、 使用 M1 应用 1 承载集团定义的全国在线支付应用（翼支付）、全国离线电子钱包和全国积分应用。

2、 M1 应用 1 规划为电信模拟 M1 应用的入口和 M1 应用的应用目录区，使用模拟 M1 应用时，接收端机具使用此应用区 CID 进行“寻卡”，并通过此应用空间中信息，获得整张 RF-UIM 上可使用的 M1 应用 CID 信息、卡片版本信息以及卡片应用特性，进行后续处理。

本章节定义 M1 应用 1 的扇区规划，其他 M1 应用可根据应用需求参照本章节进行定义。

M1 应用 1 扇区规划如下图所示：

| 扇区号 | 用途 | 可选条件 |
|---|---|---|
| 0 | 应用标识目录区（必备） | |
| 1 | 全国离线钱包区（有条件可选） | 未启用标准 CPU 模式电子钱包时必须 |
| 2 | 钱包明细区 1（有条件可选） | 未启用标准 CPU 模式电子钱包时必须 |
| 3 | 钱包明细区 2（有条件可选） | 未启用标准 CPU 模式电子钱包时必须 |
| 4 | 钱包明细区 3（有条件可选） | 未启用标准 CPU 模式电子钱包时必须 |
| 5 | 全国在线支付应用（必备） | |
| 6 | 全国积分应用（必备） | |
| 7 | 发行区 1（必备） | |
| 8 | 发行区 2（必备） | |
| 9 | 公共信息区（有条件可选） | 未启用标准 CPU 模式电子钱包时必须 |
| 10 | 个人信息区（必备） | |
| 11 | 预留 | |
| 12 | OTA 明细区（有条件可选） | 未启用标准 CPU 模式电子钱包时必须 |
| 13 | OTA 明细区（有条件可选） | 未启用标准 CPU 模式电子钱包时必须 |
| 14 | OTA 明细区（有条件可选） | 未启用标准 CPU 模式电子钱包时必须 |

| | | |
|---|---|---|
| 15 | 预留 | |

注：每个 M1 应用相当于一张 1K 的 S50 卡片，共有 16 个扇区，每个扇区有 4 个数据块，每个数据块有 16 个字节。对第 m 扇区的第 n 块数据，标识为 SmBn。

其中，使用第 5 扇区作为全国在线支付应用区；使用第 1、2、3、4 扇区作为全国离线钱包应用区；使用第 6 扇区作为全国积分应用区。这三个区与应用相关，具体扇区规划在具体应用数据写入的规范文件中说明。

第 0 扇区为应用标识目录区；第 7、8 扇区为发行区；第 9 扇区为公共信息区；第 A 扇区为个人信息区，这几个扇区存放卡片基本信息，对其扇区的定义分章节描述如下。

### 3.1应用标识目录区扇区定义

应用标识区用于存放 RFID 卡片序列号、标识 M1 应用的各扇区承载的应用类型、RFID 卡片的芯片及卡商标识。

| 块号 | 数据域 | 名称 | 类型 | 说明 |
|---|---|---|---|---|
| S0B0（芯片商预置） | 0-16 | 卡片 CSN | | 卡片序列号，写入 RFID 卡号的后 4 字节，加 12 位全 0 |
| S0B1（芯片商预置） | 0 | 0 扇区应用类型 | HEX | 取值 0x00，应用标识区 |
| | 1 | 1 扇区应用类型 | HEX | 未启用为 0xFF，启用钱包时为 0x10，标识为钱包区 |
| | 2－4 | 2－4 扇区应用类型 | HEX | 未启用为 0xFF ，启用钱包为 0x03，标识为明细区 |
| | 5 | 5 扇区应用类型 | HEX | 取值 0x08，全国在线支付应用区 |
| | 6 | 6 扇区类型 | HEX | 取值 0x11，全国积分应用区 |
| | 7-8 | 7－8 扇区应用类型 | HEX | 取值 0x01，发行区 |
| | 9 | 9 扇区应用类型 | HEX | 未启用为 0xFF，启用公共信息 |

| | | | | |
|---|---|---|---|---|
| | | | | 区时为 0x06 |
| | 10 | 10 扇区应用类型 | HEX | 取值 0x07，个人信息区 |
| | 11 | 11 扇区应用类型 | HEX | 预留，默认为 0xFF |
| | 12－14 | 12－14 扇区应用类型 | HEX | 为启用为 0xFF，启用 OTA 明细区时为 0x13 |
| | 15 | 15 扇区应用类型 | HEX | 预留，默认为 0xFF |
| S0B2 | 0－3 | 发行日期 | HEX | YYYYMMDD，暂不使用，在发行区定义 |
| | 4-7 | 有效日期 | HEX | YYYYMMDD，YYYYMMDD，暂不使用，在发行区定义 |
| | 8-11 | 启用日期 | HEX | YYYYMMDDYYYYMMDD，暂不使用，在发行区定义 |
| | 12 | 应用版本号 | HEX | 0x01 |
| | 13 | 芯片商、卡商标识 | HEX | 详见说明 |
| | 14 | 芯片版本、COS 版本号 | HEX | 高 4 位为芯片版本，第 4 位为 COS 版本，当前值 0x11 |
| | 15 | 校验码 | HEX | CRC8 |
| S0B3 | | | | 见扇区控制块定义 |

### 3.1.1 扇区应用类型定义

扇区应用类型定义如下表所示：

| 扇区应用类型 | 取值 |
|---|---|
| 目录区 | 0x00 |
| 发行区 | 0x01 |
| 交易记录区（非 OTA） | 0x03 |
| 公共信息区 | 0x06 |
| 个人信息区 | 0x07 |
| 在线支付应用区 | 0x08 |

| | |
|---|---|
| 钱包应用区 | 0x10 |
| 积分应用区 | 0x11 |
| OTA 交易记录区 | 0x13 |
| 未使用扇区 | 0xFF |

### 3.1.2 芯片商、卡商编码定义

此标志的高 3 位为芯片商编码（0x00 至 0x07），低 5 位表示卡商标识（0x00 至 0x31），定义如下表所示：

| 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | |
|---|---|---|---|---|---|---|---|---|
| A | B | C | | | | | | 芯片商编码 |
| | | | D | E | F | G | H | 卡商编码 |

芯片提供商编码如下表所示：

| 编码 | 取值 | 含义（表示芯片提供商） |
|---|---|---|
| ABC | 000 | 直通电讯 |
| | 其他 | 备用 |

卡片提供商代码如下表所示：

| 编码 | 取值 | 含义（表示卡片提供商） |
|---|---|---|
| DEFGH | 00000 | 恒宝 |
| DEFGH | 00001 | 捷德 |
| DEFGH | 00010 | 东信和平 |
| DEFGH | 00011 | 柯斯 |
| DEFGH | 00100 | 雅斯拓 |
| DEFGH | 00101 | 握奇 |
| DEFGH | 00110 | 大唐 |
| DEFGH | 00111 | 天喻 |
| DEFGH | 01000 | 华虹 |

| | | |
|---|---|---|
| DEFGH | 01001 | 南方全球通 |
| DEFGH | 01010 | 楚天龙 |
| DEFGH | 01011 | 欧贝特 |
| DEFGH | 01100 | 精工科技 |
| DEFGH | 01101 | 杰普 |
| DEFGH | 其他 | 备用 |

举例说明：

1、直通电讯芯片、恒宝卡片的编码为 0x00；

2、直通电讯芯片、捷德卡片的编码为 0x01。

### 3.2发行区 1 扇区定义

发行区 1 由卡片发行方（省公司）在卡片发行时写入卡的基本信息，包括卡号、启用标志、发行日期、启用日期；此外，M1 应用 1 作为整张 RF-UIM 卡片的 M1 应用入口，M1 应用 1 的发行区 1 用于存放其他 M1 应用的启用标志和版本号。

| 块号 | 数据域 | 名称 | 代码类型 | 说明 |
|---|---|---|---|---|
| S7B0 | 0-1 | 卡类别标识 | BCD | 目前使用 8600 |
| | 2-3 | 发行省代码 | BCD | 省代码，标识发卡省 |
| | 4-7 | 卡顺序号 | BCD | 卡顺序号 |
| | 8－11 | 卡认证码 | HEX | 由省代码、卡顺序号等数据计算出的认证码。 |
| | 12 | 启用标志 | HEX | 0：未启用 1：已启用 |
| | 13-14 | 押金 | HEX | 以分为单位 |
| | 15 | 校验码 | HEX | CRC8 |
| S7B1 | 0－3 | 卡发行日期 | BCD | YYYYMMDD |
| | 4-7 | 卡有效期日期 | BCD | YYYYMMDD |
| | 8-11 | 卡启用日期 | BCD | YYYYMMDD |
| | 12 | 卡状态标志 | HEX | 取值参考翼支付业务系统对卡 |

| | | | | |
|---|---|---|---|---|
| | | | | 片状态标志的定义 |
| | 13 | 黑名单次数 | HEX | |
| | 14 | 预留 | HEX | 目前未使用，0x00 |
| | 15 | 校验码 | HEX | CRC8 |
| S7B2 | 0 | CID 启用标志 | HEX | 按位定义卡片各 CID 启用标志，1 代表已启用，0 代表未启用，详见说明 |
| | 1 | CID 应用 1 版本号 | HEX | 0x01 |
| | 2 | CID 应用 2 版本号 | HEX | 版本号，未启用则为 0x00 |
| | 3 | CID 应用 3 版本号 | HEX | 版本号，未启用则为 0x00 |
| | 4 | CID 应用 4 版本号 | HEX | 版本号，未启用则为 0x00 |
| | 5 | 保留 | HEX | 目前未使用，0x00 |
| | 6 | 保留 | HEX | 目前未使用，0x00 |
| | 7 | 保留 | HEX | 目前未使用，0x00 |
| | 8 | 保留 | HEX | 目前未使用，0x00 |
| | 9 | 保留 | HEX | 目前未使用，0x00 |
| | 10 | 保留 | HEX | 目前未使用，0x00 |
| | 11 | 保留 | HEX | 目前未使用，0x00 |
| | 12 | 保留 | HEX | 目前未使用，0x00 |
| | 13-14 | 保留 | HEX | 目前未使用，0x00 |
| | 15 | 校验码 | HEX | CRC8 |
| S7B3 | | | | 见扇区控制块定义 |

### 3.2.1 省代码、卡认证码说明

S7B0 块中的卡类别标识、发行省代码和卡顺序号三个字段合起来即由发行方定义的卡号。其中省代码标识发卡省，采用 BCD 编码，共 4 位数字，取各发卡省省会城市电话区号，4 位的区号，不足 4 位的，左边补 0。全国应用相关的接收端机具装载的 PSAM 卡中保存的是未经过省代码分散的全国应用根密钥，而各省发卡时写入 UIM 卡的应用密钥是全国应用根密钥经过省代码以及卡片应用序列号分散后的应用密钥，接收端机具需根据这 4 位的省代码＋0001 作为分散因子，以实现对卡的认证。

卡认证码是卡片发行机构根据相关规则计算出来的卡号校验码，类似于银联使用的 CVV，用来防止通过卡号方式伪造卡片。

### 3.2.2 应用启用标志说明

应用启用标志定义如下：

| 7bit | 6bit | 5bit | 4bit | 3bit | 2bit | 1bit | 0bit |
|---|---|---|---|---|---|---|---|
| 保留 | 保留 | 保留 | 保留 | 应用 4 标志 | 应用 3 标志 | 应用 2 标志 | 应用 1 标志 |

注 1：此启用标志定义了 RF-UIM 卡整体规划中相关应用是否已启用。其中 M1 应用 1 为 RF-UIM 卡整个 M1 应用的入口，必须启用。

注 2：取值为 0 时表示应用未启用，取值为 1 时表示应用已启用。

举例说明：如果某张 RF-UIM 卡应用启用关系如下表所示：

| 编号 | 应用类型 | CID | 归属机构 | 启用状态 |
|---|---|---|---|---|
| **应用 1** | **全国翼支付应用** | **MCTGEPAY** | **电信集团** | **必须使用** |
| 应用 2 | 集团级合作应用 | MCTGEUNN | 电信集团 | 未使用 |
| 应用 3 | 省内翼机通应用 | MCT+2 位省编码+3 位业务描述 | 省公司 | 翼机通，已使用 |
| 应用 4 | 省内预留应用 1 | MCT+2 位省编码+3 位业务描述 | 省公司 | 未使用 |

则应用启用状态标志按位表示为：

| 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|---|---|---|---|---|---|---|---|
| 保留 | 保留 | 保留 | 保留 | 应用 4 标志 | 应用 3 标志 | 应用 2 标志 | 应用 1 标志 |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 |

相应的启用状态标志为 0x05

### 3.2.3 应用版本号说明

应用版本号用于接收端机具读取卡内应用的版本号以调用相应的处理程序。

RF-UIM 卡 M1 应用的版本号定义如下：如果未定义此应用，应用版本号为 0x00，如果已定义此应用，则第一个版本号为 0x01，后续版本号依次增加。

## 3.3发行区 2 扇区定义

发行区 2 定义了 RF-UIM 卡上由省公司定义的 M1 应用 3 至 M1 应用 6 的 CID 名称，以及这些 CID 在接收端机具上的显示顺序。

| 块号 | 数据域 | 名称 | 代码类型 | 说明 |
|---|---|---|---|---|
| S8B0 | 0-7 | 优选 CID1 | ASCII | 省公司根据定义填写 |
| | 8-15 | 优选 CID2 | ASCII | 省公司根据定义填写 |
| S8B1 | 0-7 | 优选 CID3 | ASCII | 省公司根据定义填写 |
| | 8-15 | 优选 CID4 | ASCII | 省公司根据定义填写 |
| S8B2 | 0-7 | 保留 | | 目前未使用，0x00 |
| | 8-15 | 保留 | | 目前未使用，0x00 |
| S8B3 | | | | 见扇区控制块定义 |

## 3.4 公共信息区扇区定义

公共信息区用于保存模拟 M1 卡片在交易过程中的过程值。

| 块号 | 数据域 | 名称 | 代码类型 | 说明 |
|---|---|---|---|---|
| S9B0 | 0 | 交易明细指针 | HEX | 下一条明细的记录位置 |
| | 1-2 | 累计次数 | HEX | |
| | 3 | 交易状态标志 | HEX | 01：钱包开始 02：钱包结束 |
| | 4-5 | 保留 | HEX | |

| | | | | |
|---|---|---|---|---|
| | 6 | 黑名单标志 | HEX | 01：正常 04：黑名单 |
| | 7-14 | 保留 | HEX | |
| | 15 | 校验码 | HEX | CRC8 |
| S9B1 | 0 | 明细指针备份 | HEX | 下一条明细的记录位置 |
| | 1-2 | 累计次数备份 | HEX | |
| | 3 | 交易状态标志备份 | HEX | 01：钱包开始 02：钱包结束 |
| | 4-5 | 保留 | HEX | |
| | 6 | 黑名单标志备份 | HEX | 01：正常 04：黑名单 |
| | 7-14 | 保留备份 | HEX | |
| | 15 | 校验码备份 | HEX | CRC8 |
| S9B2 | 0 | OTA 交易指针 | HEX | 由卡片 COS 进行维护 |
| | 1-14 | 保留 | HEX | |
| | 15 | 校验码 | HEX | CRC8 |
| S9B3 | | | | 见扇区控制块定义 |

## 3.5 个人信息区扇区定义

个人信息区用于写入持卡人的基本信息，如客户类型、姓名、证件号码、手机号码等。

| 块号 | 数据域 | 名称 | 代码类型 | 说明 |
|---|---|---|---|---|
| SAB0 | 0 | 客户类型标识 | BCD | |
| | 1-14 | 姓名 | HEX | 最多 7 个汉字 |
| | 15 | 校验码 | HEX | CRC8 |
| SAB1 | 0 | 证件类型 | HEX | 0x00：身份证 0x01：军官证 0x02：学生证 0x04：户口簿 0x05：其他 |
| | 1－14 | 证件号码 | ASCII | |
| | 15 | 校验码 | HEX | CRC8 |

| | | | | |
|---|---|---|---|---|
| SAB2 | 0-5 | 证件号码 | ASCII | 继续前块内容 |
| | 6－11 | 手机号码 | BCD | 不足第一位补 0，默认全 0 |
| | 12-14 | 保留 | | |
| | 15 | 校验码 | HEX | CRC8 |
| SAB3 | | | | 见扇区控制块定义 |

# 4、 CPU 应用空间规划

## 4.1 CPU 应用 AID 命名规则

CPU 应用 AID 的命名规划参见集团下发的《关于规范移动支付 RFID UIM 卡生产发行管理的通知》（中国电信〔2010〕27 号）文件中的 AID 规划附件。集团本期规划了 3 个应用，分别是全国在线支付应用、全国积分应用、全国离线钱包应用；各省可在 CPU 应用空间定义自己的应用。集团统一定义的 AID 如下表所示：

| 应用类别 | AID | 显示名 | FID |
|---|---|---|---|
| 全国在线支付应用 | D156000040100020000000100000000 | 翼支付 | DF01 |
| 全国积分应用 | D156000040100020000000200000000 | 我的积分 | DF02 |
| 全国离线钱包应用 | D156000040100030000000100000000 | 待定义 | DF03 |

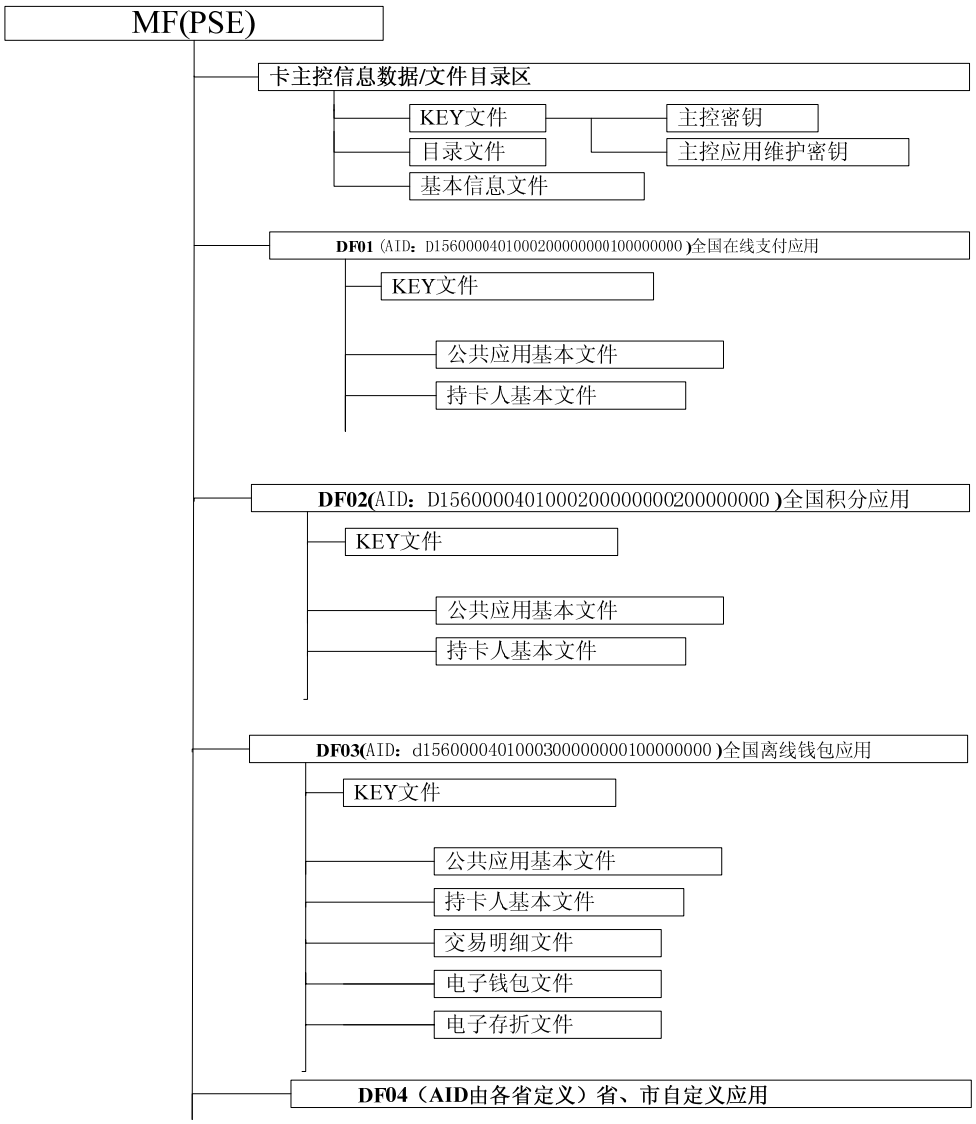
## 4.2 CPU 应用文件结构定义

智能卡文件存储按主控密钥、客户信息和不同应用文件存放于不同 DF 文件，文件存储格式符合 ISO7816 国际标准。各应用文件名称如下：

- ✧ MKF-主密钥文件，控制整个卡片存储结构的建立；
- ✧ AID 命名应用文件－应用文件。

CPU 应用结构如下图所示：

中国电信 2.4G RF-UIM 卡空间规划




## 4.3 卡片级文件定义

MF 下文件信息如下表所示：

| 文件内容 | 文件类型 | 标识 | 文件空间 | 权限 |
|---|---|---|---|---|
| MF | 目录文件 | 3F00 | 32K 左右 | 卡片主控 |
| 密钥文件 | KEY 文件 | | 0x70 | 卡片主控 |
| DIR 文件 | 定长记录 | 0001 | 0x80 | 卡片维护 |
| 全国在线支付应用 | 目录文件 | DF01 | 100 字节左右 | 卡片主控 |
| 全国积分应用 | 目录文件 | DF02 | 100 字节左右 | 卡片主控 |

| | | | | |
|---|---|---|---|---|
| 全国离线钱包应用 | 目录文件 | DF03 | 1K 左右 | 卡片主控 |
| | | | | |

### 4.3.1 密钥文件定义

密钥文件和卡片安全机制有关，不同卡片提供商有不同格式，不进行统一定义。

### 4.3.2 DIR 文件

| | | |
|---|---|---|
| 文件标识（FID） | | 0001 |
| 文件类型 | | 变长纪录 |
| 文件大小 | | 0080 |
| 文件位置 | | MF |
| 文件存取控制 | 读 = 自由 | 改写 = 需要<br>安全信息 |
| TLV 格式存储应用目录名 | | |

全国在线支付应用、积分应用、离线钱包应用的详细文件定义见相关应用规范。

会签部门：市场部

中国电信集团公司综合部　　2010年5月17日印发