中国电信移动支付业务 RFID 卡片空间规划

（初稿）

中国电信移动支付项目组

二〇一〇年二月

修改过程

版本号	日期	负责人	概述
	2010/2/9	谢云	1、修改了支付卡号编码规则；2、修正部分笔误
	2010/2/25	谢云	1、增加卡号校验位 Luhn 算法；2、增加对发卡方标识及省标识的编码说明。

目　　录

1、卡片规划设计

1.1设计原则

- ✧ 一卡多用原则：整合用户用于日常生活的有关卡证，发行一套用户用于享受电信积分服务和增值商业服务的卡片。
- ✧ 统一名称、统一标识、统一平台、统一标准：卡片覆盖范围广、应用行业多，超出了行业专用卡的管理和使用，便于卡片的使用和推广，电信公司要对卡片进行统一的规划、采用统一的名称、统一的标识、统一的卡片应用平台以及统一的技术标准。
- ✧ 先进与成熟并重：卡覆盖人群广，影响范围大，必须注重所采用技术的成熟性。卡使用时间跨度大，同时也要考虑技术的一定前瞻性。
- ✧ 可扩展性：卡应用规划中将分阶段逐步实施，卡设计必须考虑在使用过程中的新增应用的扩充能力。
- ✧ 安全性高：能抵抗多种芯片攻击手段；持国家标准的加密算法；建立严密的密钥管理体系；应用之间严格隔离，互不干扰。
- ✧ 标准化与开放性：设计与国际、国内有关技术标准和信息标准一致。

1.2选型中考虑的相关因素

1.2.1卡片要求相关技术要求

- ✧ 符合《中国金融集成电路(IC)卡应用规范（V2.0 电子钱包应用）》、《社会保障(个人)卡规范》等其他专属行业制定的应用规范；
- ✧ 接触式界面符合 ISO/IEC7816 规范；
- ✧ 非接触式界面支持 ISO/IEC 14443 中 TYPE-A 或 TYPE-B 通信协议规范；
- ✧ 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；
- ✧ 支持一个保密模块上实现多个不同应用，各应用之间相互独立（多应用、防火墙功能）；
- ✧ 兼容支持国际主流密码算法和国产有关算法；
- ✧ 支持多种文件类型，包括二进制、定长记录、变长记录、循环、钱包文件；

- ✧ 支持 ISO7816－3 T=0（字符传送）和 T=1（块传送）通讯协议；
- ✧ 行业对卡片交易速度的不同，希望支持多种通讯速率，接触方式可支持 9600bps、38400bps、56000bps 等不同的通讯速率；非接触方式支持 106Kbps 通讯速率。

1.2.2卡片受理环境的要求

全国投资的 POS 机，必须能够支持磁条卡、接触式卡片以及非接触式卡的支持（现阶段可以支撑其中一项或多项）；

1.2.3密钥算法

卡片除需支持 DES/3DES 算法外，还需支持其他应用算法（例如 SSF33 算法，应用于社保系统）。DES 经历了较长时间的广泛应用，从安全性抗攻击的角度，需要逐步考虑升级换代，因此各国都在加紧研制推出新的安全算法。

不同算法需要 COS 相应功能支持因此，要考虑未来基于其他应用算法的密钥体系，同时选用支持的智能卡芯片和 COS。

1.2.4卡片容量要求

- ✧ PBOC2.0 规定了电子钱包存折应用功能，实际上规定了电子钱包/存折应用近 1K 字节的存储内容及相适应的安全架构；
- ✧ 卡片规范圈定的内容相对而言，直接规定了近 6K 字节左右的存储内容及相适应的安全架构；
- ✧ 预留一定的卡片空间进行相关应用的扩展使用。

1.2.5其它相关因素

- ✧ 目前国内公司非接触 CPU 卡主要采用 TypeA/TypeB 类型，符合 TypeA 的非接触式 CPU 卡主要以飞利浦公司的产品为主，但是不支持国产的 SSF33 算法；而国产非接触式 CPU 卡主要采用 TypeB 的规范，在芯片设计中支持国产 SSF33 算法；
- ✧ 金融 PBOC2.0 规范中规定卡片可以采用接触式和非接触式的界面，非接触界面采用 TypeA/TypeB 信号均可；

- ✧ 考虑卡片的发行、终端的改造、持卡人使用卡片的方便程序上，卡公司规划的卡片采用相同的技术标准和卡片规范，只是在相关功能、密钥体系的选择上对于不同卡片采用不同的设置。

2、RF-UIM 卡

2.1RF-UIM 整体空间规划

2.4G 的 RF-UIM 卡，目前商用的 RF-UIM 卡的硬件版本为 V5B 版本。V5B 版本在卡片初始化时由厂商按照应用类型对卡片的空间进行了划分，并将卡内相关区域预先格式化好，运营商不能再调整各应用的空间大小。

V5B 版 EPPROM 总空间为 288k，通信部分占用 188K 空间，RFID 部分占用 100K 空间。其中通信部分包含代码段空间（约占 120K）和数据段空间（约 64K）；RFID 部分的 100K 空间中也包括代码段空间（约 64K）和数据段空间（约 32K）。

RFID 部分数据段的空间即 RFID 应用的存储空间，RF-SIM 在生产时，对这 32K 空间进行了预先格式化，将 32K 空间格式化为若干应用空间，提供给运营商使用，对各应用的整体规划如下：

应用项目编号	应用类型	AID	显示名	空间规划
应用 1	ID 类应用 1		待定义	待定义（电信集团）
应用 2	ID 类应用 2		待定义	预留给省公司应用
应用 3	ID 类应用 3		第三方定义	预留给第三方应用
应用 4	S50 Mifare 卡片 1	MCTGEPAY	翼支付	电信集团应用
应用 5	S50 Mifare 卡片 2		待定义	预留给省公司应用
应用 6	S50 Mifare 卡片 3		第三方定义	预留给第三方应用
应用 7	S50 Mifare 卡片 4		待定义	预留
应用 8	S70 Mifare 卡片 1		待定义	预留
应用 9	S70 Mifare 卡片 2		待定义	预留
应用 10	Bank 磁条卡		待定义	预留
应用 11	Vifare (优惠券)		待定义	预留

应用 12	PBOC 2.0 应用	8888888888100030000000001	待定义	集团离线钱包应用 各省公司可以规划本省的 CPU 应用。 AID 可多个。

RF-UIM 卡为 CPU 卡，可模拟多张 M1 卡，集团层面只定义其中一张模拟 M1 卡的空间，使用“应用 4”空间模拟 M1；另外，使用“应用 12”空间实现标准 PBOC 应用，承载集团离线钱包应用，各省公司可根据本省应用需求在“应用”中规划本省的 CPU 应用。

2.2集团应用（模拟）M1 卡片扇区规划

集团应用模拟 M1 卡片的扇区规划如下（红色为必备区，蓝色为可选区，黑色为预留区）

区号	用途
0	应用标识目录区
1	钱包区
2	明细区 1
3	明细区 2
4	明细区 3
5	全国在线支付应用（联机方式）
6	积分应用（联机方式）
7	发行区 1
8	发行区 2
9	公共信息区
A	个人信息区
B	预留
C	OTA 明细区
D	OTA 明细区
E	OTA 明细区

F	预留

2.2.1 应用标识目录区

块号	数据域	名称	类型	说明
S0B0	0-16	CSN		卡商定义的唯一号
S0B1	0	0x00	HEX	应用标识区
	1	0x10	HEX	钱包区
	2－4	0x03	HEX	明细区
	5	0x08	HEX	全国在线支付应用
	6	0x11 或 0xFF	HEX	全国积分应用
	7-8	0x01 或 0xFF	HEX	发行区
	9	0x06	HEX	公共信息区
	10	0x07 或 0xFF	HEX	个人信息区
	11	0xFF	HEX	预留
	12－14	0x13	HEX	OTA 明细区
	15	0xFF	HEX	预留
S0B2	0－3	发行日期	HEX	CCYYMMDD
	4-7	有效日期	HEX	CCYYMMDD
	8-11	启用日期	HEX	CCYYMMDD
	12	版本	HEX	
	13-14	保留	HEX	
	15	校验码	HEX	CRC8

目录标识区定义如下表所示：

类型	标识
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

2.2.2 钱包区

块号	数据域	名称	类型	说明
S1B0	0－3	钱包正码	HEX	
	4－7	钱包反码	HEX	
	8－11	钱包正码	HEX	
	12	00	HEX	
	13	FF	HEX	
	14	00	HEX	
	15	FF	HEX	
S1B1	0－3	钱包正码备份	HEX	
	4－7	钱包反码备份	HEX	
	8－11	钱包正码备份	HEX	
	12	00	HEX	
	13	FF	HEX	
	14	00	HEX	
	15	FF	HEX	
S1B2	0－3	充值金额正码	HEX	
	4－7	充值金额反码	ASC	

	8-11	累计充值金额	HEX	以元为单位
	12-14	累计充值次数	BCD	
	15	校验码	HEX	CRC8

2.2.3 明细区

块号	数据域	名称	类型	说明
SxB0	0－3	交易时间	BCD	DDHHMMSS
	4－7	交易前余额	HEX	逆序 HEX 码，低字节再前，高字节在后。2C0100h = RMB 3.00 元
	8－10	交易金额	HEX	逆序 HEX 码，低字节再前，高字节在后。2C0100h = RMB 3.00 元
	11	交易类型	HEX	0x01 消费 0x88 充值 0x90 OTA
	12－15	终端机编号	HEX	
SxB1	0－3	交易时间	BCD	DDHHMMSS
	4－7	交易前余额	HEX	逆序 HEX 码，低字节再前，高字节在后。2C0100h = RMB 3.00 元
	8－10	交易金额	HEX	逆序 HEX 码，低字节再前，高字节在后。2C0100h = RMB 3.00 元
	11	交易类型	HEX	0x01 消费 0x88 充值 0x90 OTA
	12－15	终端机编号	HEX	
SxB2	0－3	交易时间	BCD	DDHHMMSS
	4－7	交易前余额	HEX	逆序 HEX 码，低字节再前，高字节在后。2C0100h = RMB 3.00 元
	8－10	交易金额	HEX	逆序 HEX 码，低字节再前，高字节在后。2C0100h = RMB 3.00 元
	11	交易类型	HEX	0x01 消费 0x88 充值 0x90 OTA
	12－15	终端机编号	HEX	

2.2.4 积分应用区

积分应用区数据段规划如下：

块号	数据域	名称	类型	说明
S6B0	0-7	卡号	BCD	见表下文字说明
	8	使用标记	HEX	0x01 未使用
	9-10	扣年费标记	BCD	yyyy
	11	优惠券位置	HEX	0xmn:优惠券在第 m、n 扇区
	12-14	预留	HEX	
	15	校验码	HEX	CRC8
S6B1	0	原始卡类型	HEX	
	1-3	充值有效日期	BCD	yymmdd
	4-7	有效日期	BCD	yyyymmdd
	8-11	启用日期	BCD	yyyymmdd
	12	卡状态标志	HEX	00:未启用 01:已启用 02:已停用 03:已退卡 04:黑名单卡
	13	黑名单次数	HEX	
	14	预留	HEX	
	15	校验码	HEX	CRC8
S6B2	0	卡片主类型	HEX	
	1	应用子类型	HEX	
	2-5	应用卡编号	BCD	
	6-7	城市代码	BCD	
	8-9	行业代码	BCD	
	10-13	卡认证码	HEX	
	14	预留	HEX	
	15	校验码	HEX	CRC8

积分应用卡号编码规则参见现有 E 家俱乐部会员卡号。

2.2.5全国在线支付应用区

支付卡号采用全国统一的 16 位编码规则，区别于积分会员卡号：

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
86		0	0	地区码			顺序号								校验位

（1）预留码 A、B，目前采用国际长途区号，统一为“86”；

（2）客户类别标识：未来可能会区分客户级别，暂时预留，目前取默认值“0”；

（3）卡级别码：D 位用于区别不同的卡级别，目前不区分卡级别，此位预留，暂时定为“0”；

（4）地区码 E-G 位用于区别发卡省份，规则与长途地区区号一致，若不足 3 位，E 位用 0 补足；

（5）顺序编码 H-O 位以省为单位规划，顺序产生；

（6）校验位：最后一位 P 位为校验位；校验算法采用 Luhn 方程计算得出，如下图所示

计算步骤如下：

步骤1：从右边第1个数字（低序）开始每隔一位乘以2。

步骤2：把在步骤1中获得的乘积的各位数字与原号码中未乘2的各位数字相加。

步骤3：从邻近的较高的一个以0结尾的数中减去步骤2中所得到的总和[这相当于求这个总和的低位数字（个位数）的“10的补数”]。如果在步骤2得到的总和是以零结尾的数（如30、40等等），则校验数字就是零。

例：

无校验数的卡号4992 73 9871　　步骤

4　9　9　2　7　3　9　8　7　1　　1

×2　×2　×2　×2　×2

18　4　6　16　2

4 + 1 + 8 + 9 + 4 + 7 + 6 + 9 + 1 + 6 + 7 + 2 = 64　　2

70 − 64 = 6　　3

带有校验数的卡号为：4992 73 9871 6

全国在线支付用区数据段规划如下：

块号	数据域	名称	类型	说明
S5B0	0-7	支付账号	BCD	16 位支付卡号

	8	使用标记	HEX	0x01 未使用
	9-10	扣年费标记	BCD	yyyy
	11-14	预留	HEX	
	15	校验码	HEX	CRC8
S5B1	0	原始卡类型	HEX	
	1-3	充值有效日期	BCD	yymmdd
	4-7	有效日期	BCD	yyyymmdd
	8-11	启用日期	BCD	yyyymmdd
	12	卡状态标志	HEX	00:未启用 01:已启用 02:已停用 03:已退卡 04:黑名单卡
	13	黑名单次数	HEX	
	14	预留	HEX	
	15	校验码	HEX	CRC8
S5B2	0	卡片主类型	HEX	
	1	应用子类型	HEX	
	2-5	应用卡编号	BCD	
	6-7	城市代码	BCD	
	8-9	行业代码	BCD	
	10-13	卡认证码	HEX	
	14	预留	HEX	
	15	校验码	HEX	CRC8

2.2.6 发行区 1 定义

块号	数据域	名称	类型	说明
S7B0	0-1	卡种标识	BCD	8665 全国应用 8667 省应用
	2-3	省代码	BCD	省代码，标识发卡省
	4-7	顺序号	BCD	卡顺序号

	8－11	卡认证码	HEX	由卡号计算出的认证码
	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	发行日期	BCD	CCYYMMDD
	4-7	有效期日期	BCD	CCYYMMDD
	8-11	启用日期	BCD	CCYYMMDD
	12	卡状态标志	HEX	00:未启用 01:已启用 02:已停用 03:已退卡 04:黑名单卡
	13	黑名单次数	HEX	
	14	预留	HEX	
	15	校验码	HEX	CRC8
S7B2	0－14	保留		由集团进行统一定义
	15	校验码	HEX	CRC8

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。

当全国应用相关的 POS 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应用序列号分散后的应用密钥时，POS 机具需根据这 4 位的省代码作为分散因子，以实现对卡的认证。

2.2.7 个人信息区

块号	数据域	名称	类型	说明
SAB0	0	客户类型标识	BCD	01：政企客户，02：家庭客户 03：个人客户，04：号百客户
	1	职工标识	BCD	00：非电信职工

				01：电信职工
	2-11	姓名	HEX	
	12	性别	BCD	00：男 01：女
	13-14	预留		
	15	校验码	HEX	CRC8
SAB1	0	证件类型	HEX	
	1－14	证件号码	ASC	
	15	校验码	HEX	CRC8
SAB2	0-5	证件号码	ASC	继续前块内容
	6－11	手机号码	BCD	
	12-14	保留		
	15	校验码	HEX	CRC8

2.2.8 公共信息区

块号	数据域	名称	类型	说明
S9B0	0	明细指针	HEX	下一条明细的记录位置
	1-2	累计次数	HEX	
	3	状态标志	HEX	01：钱包开始 02：钱包结束
	4-5	月票	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	
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	状态标志备份	HEX	01：钱包开始 02：钱包结束
	4-5	月票备份	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	
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	

2.2.9 扇区控制位

序号	扇区名称	KA	Access Bit	KB
0	应用标识目录区	A0A1A2A3A4A5	08778f69	发行密钥
1	钱包区	消费密钥	08778f69	充值密钥
2	明细区 1	消费密钥	7F0788	充值密钥
3	明细区 2	消费密钥	7F0788	充值密钥
4	明细区 3	消费密钥	7F0788	充值密钥
5	全国在线支付应用（联机）	A0A1A2A3A4A5	7F078869	发行密钥
6	全国积分应用（联机）	A0A1A2A3A4A5	7F078869	发行密钥
7	发行区 1	A0A1A2A3A4A5	08778f69	充值密钥
8	发行区 2（预留）	消费密钥	7F0788	充值密钥
9	公共信息区	消费密钥	7F0788	充值密钥
A	预留	扇区消费密钥	08778f69	扇区充值密钥
B	预留	扇区消费密钥	08778f69	扇区充值密钥
C	预留	扇区消费密钥	7F0788	扇区充值密钥
D	预留	扇区消费密钥	7F0788	扇区充值密钥
E	预留	扇区消费密钥	7F0788	扇区充值密钥
F	预留	扇区消费密钥	7F0788	扇区充值密钥

2.3 CPU 应用规划

电信全国统一的离线钱包应用利用 RFID 卡片上的 CPU 空间（“应用 12”）实现，

文件结构与双界面卡的 CPU 应用一致,参见 3.2 以及 3.3.4 节内容。各省可根据本省需求规划本省的 CPU 应用。

各省公司可根据本省应用需求规划使用 RF-UIM 的应用空间。

3、双界面卡

3.1双界面卡整体应用空间规划

双界面卡集成一块 M1 卡片，同时支持 CPU 应用，对双界面卡的应用规划如下：

应用空间	支付应用	AID	显示名	应用说明
M1 空间	行业合作应用	无	第三方定义	电信不使用，预留给第三应用
CPU 空间	全国在线支付应用	RID+1000200000000 1	翼支付	电信集团应用
	全国积分应用	RID+1000200000000 2	我的积分	电信集团应用
	全国离线钱包应用	RID+1000300000000 1	待定义	预留
	省公司预留应用		待定义	预留
	省公司预留应用		待定义	预留
	合作预留应用		待定义	预留

其中，M1 空间预留给行业合作应用，电信自己不使用。电信应用都放在 CPU 空间，其中全国本期规划了 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。

集团公客部正在向国家IC卡注册中心申请RID编码，在申请完成前，各省可先使用“8888888888”作为临时RID进行发卡。

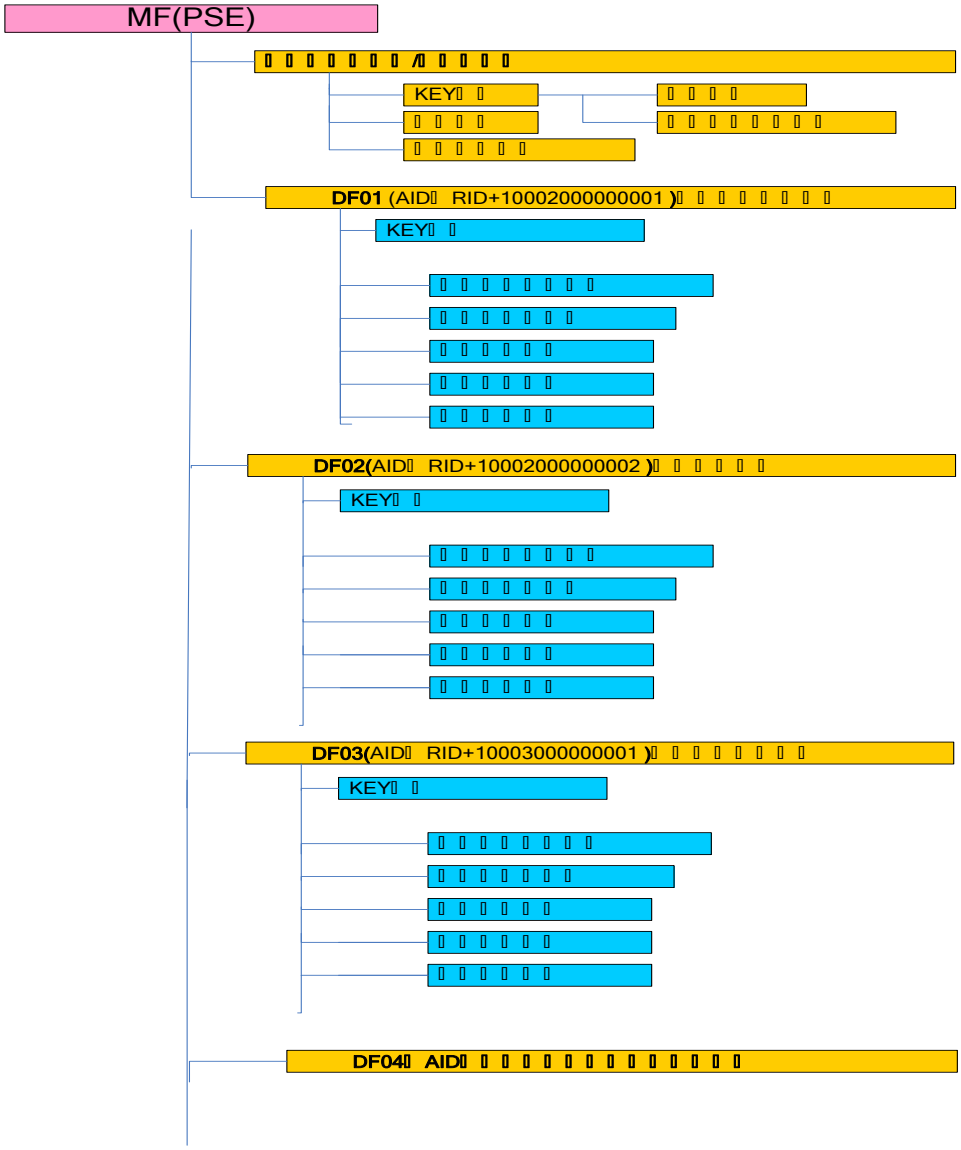
CPU 文件结构及全国应用文件定义如下：

3.2CPU 卡文件结构定义

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 命名应用文件一应用文件。

CPU 卡文件设置示意图如下：



3.3全国应用文件定义

3.3.1卡主控信息数据区文件定义

密钥文件
主控密钥
维护密钥
……

2）持卡人基本信息文件定义如下：

文件标识（SFI）		‘22’（十进制）	
文件类型		透明	
文件大小		72	
文件存取控制	读=自由	更新＝安全保护	
字节	数据元	长度	说明
1	客户类型标识	1	01：政企客户 02：家庭客户 03：个人客户 04：号百客户
2	本系统职工标识	1	00：非电信系统职工 01：电信系统职工
3～22	持卡人姓名	20	
23～38	持卡人证件号码	16	
39	持卡人证件类型	1	
40－48	持卡人手机号码	8	BCD 格式，不足补 F，默认全 0
48－56	持卡人固话号码	8	BCD 格式，不足补 F，默认全 0
57－72	持卡人宽带号码	16	ASC 格式，默认是 0x20（空格）

3.3.2全国在线支付应用文件定义

1）基本信息文件定义如下：

文件标识（SFI）		‘21’（十进制）	
文件类型		透明	
文件大小		30	
文件存取控制	读=自由	更新＝安全保护	
字节	数据元	长度	说明
1～8	发卡方标识	8	4 位机构标识（两字节）＋6 字节全 0
9	应用类型标识	1	01：在线支付账户
10	应用版本	1	01
11～20	应用序列号	10	在线支付账号：16 位卡号（8 字节）＋2 字节全 0
21～24	应用启用日期	4	
25～28	应用有效日期	4	
29－30	发卡方自定义 FCI 数据	2	

其中发卡方标识中的 4 位机构标识为省代码，标识发卡省，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。

当全国应用相关的 POS 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应用序列号分散后的应用密钥时，POS 机具需根据 4 位的机构标识获取省代码分散因子，以实现对卡的认证。

3.3.3全国积分应用文件定义

1）基本信息文件定义如下：

文件标识（SFI）		‘21’（十进制）
文件类型		透明
文件大小		32
文件存取控制	读=自由	更新＝安全保护

字节	数据元	长度	说明
1～8	发卡方标识	8	4 位机构标识（两字节）＋6 字节全 0
9	应用类型标识	1	02：积分应用
10	应用版本	1	01
11～20	应用序列号	10	16 位卡号（8 字节）＋2 字节全 0
21～24	应用启用日期	4	
25～28	应用有效日期	4	
29－32	积分充值有效日期	4	

其中发卡方标识中的 4 位机构标识为省代码，标识发卡省，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。

当全国应用相关的 POS 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应用序列号分散后的应用密钥时，POS 机具需根据 4 位的机构标识获取省代码分散因子，以实现对卡的认证。

3.3.4全国离线钱包文件

1）基本信息文件定义如下：

文件标识（SFI）		‘21’（十进制）	
文件类型		透明	
文件大小		32	
文件存取控制	读=自由	更新＝安全保护	
字节	数据元	长度	说明
1～8	发卡方标识	8	4 位机构标识（两字节）＋6 字节全 0
9	应用类型标识	1	03：离线钱包应用

10	应用版本	1	01
11～20	应用序列号	10	16 位卡号（8 字节）＋2 字节全 0
21～24	应用启用日期	4	
25～28	应用有效日期	4	
29－32	积分充值有效日期	4	

其中发卡方标识中的 4 位机构标识为省代码，标识发卡省，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。

当全国应用相关的 POS 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应用序列号分散后的应用密钥时，POS 机具需根据 4 位的机构标识获取省代码分散因子，以实现对卡的认证。

2）交易明细文件定义如下：

文件标识(SFI)		‘18’ （十六进制）
文件类型		循环记录文件
文件大小		32
记录长度		‘17
记录个数		‘0A’
读权限		‘F1’（口令认证后读）
写权限		‘EF’（有 IC 卡自己维护）
字节	数据元	长度
1-2	脱机交易序号	2
3-5	透支限额	3
6-9	交易金额	4
10	交易类型标志	1
11-16	终端机编号	6
17-20	交易日期	4
21-24	交易时间	4

3）应用密钥文件：

文件标识(SFI)	‘01’ （十六进制）
文件类型	密钥文件（变长记录文件）
文件大小	13*23+6
记录个数	‘0A’
读权限	‘EF’（不能读）
写权限	满足使用权限后，在控制密钥的控制下更新

密钥属性	数据元	长度
39	应用主控密钥	23
36	应用维护密钥（线路保护密钥、 应用锁定密钥、应用解锁密钥）	23
3C	修改透支限额密钥(不要)	23
37	口令解锁密钥（不要）	23
38	口令重装密钥（不要）	23
34	TAC 密钥（内部密钥）	23
3A	PIN	6 （888888）
3E	消费密钥(1 个版本 3 条密钥)	23*3
3F	圈存密钥（1 个版本 3 条密钥）	23*3
	圈提密钥（不要）	23

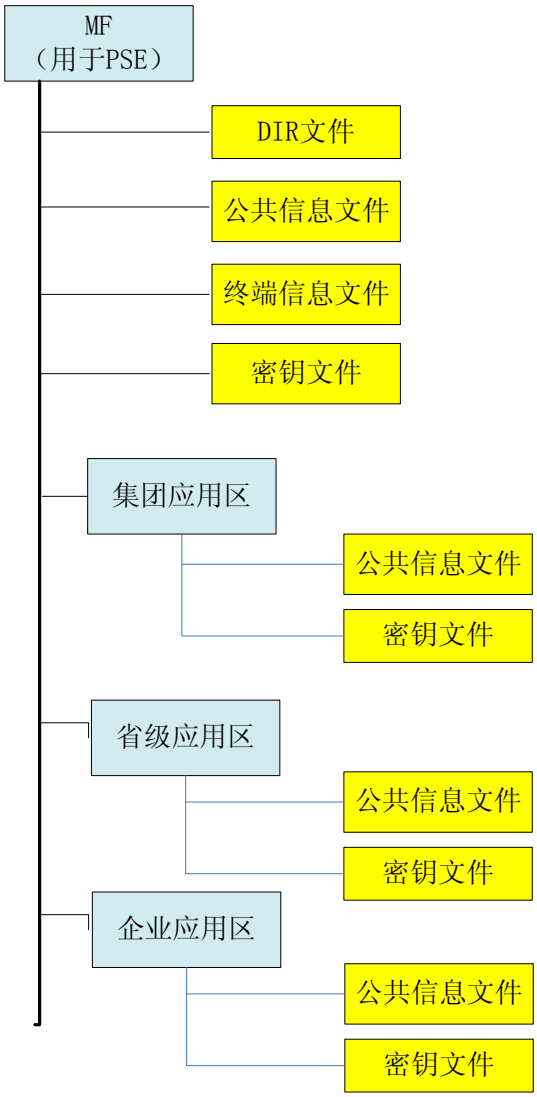
4）钱包文件定义：

字段名	长度（Byte）
余额	4
消费交易序号（次数）	2
充值交易序号（次数）	2

4、PSAM 卡

4.1 PSAM 卡结构设计

用于金融应用环境的 PSAM 则应符合中国人民银行 PSAM 卡规范，用于社会保险（政府）应用环境授权与安全认证的 PSAM 卡设计应符合劳社部 PSAM 卡规范，用于教育应用环境的 PSAM 卡则应符合教育部 PSAM 卡规范，用于扩展应用环境的 PSAM 则采用公司的密钥管理体系。



图表 1 PSAM 卡结构

4.2 PSAM 卡信息文件格式

卡片公共信息文件格式如下：

文件标识（SFI）			'21'（十进制）
文件类型			透明
文件大小			14
文件存取控制		读 = 自由	改写 = 需要 安全信息
字节	数据元		长度
1－10	PSAM 序列号		10
11	PSAM 版本号		1
12	密钥卡类型		1
13－14	发卡方自定义 FCI 数据		2

MF 目录下终端信息文件格式：

文件标识（SFI）			'22'（十进制）
文件类型			透明
文件大小			6
文件存取控制		读 = 自由	改写 = 需要 安全信息
字节	数据元		长度
1－6	终端机编号		6

集团应用区公共信息文件格式：

文件标识（SFI）			'23'（十进制）
文件类型			透明
文件大小			25
文件存取控制		读 = 自由	改写 = 需要 安全信息
字节	数据元		长度
1	全国消费密钥索引号		1

2－9	应用发行者标识	8
10－17	应用接收者标识	8
18－21	应用启用日期	4
22－25	应用有效日期	4

4.3 PSAM 卡密钥定义

4.3.1 集团应用区密钥定义

密钥类型	密钥属性	密钥索引	使用条件
全国 M1 卡消费密钥	0x27	01-05	按照省代码分散后使用
全国 M1 卡 TAC 密钥	0x26	01-05	按照省代码分散后使用
全国 M1 卡充值密钥	0x27	11-15	按照省代码分散后使用

4.3.2 省应用区密钥定义

密钥类型	密钥属性	密钥索引	使用条件
省 M1 钱包消费密钥	0x07	01-02	直接进行加密计算
省 M1 卡 TAC 密钥	0x06	01-02	直接进行 TAC 计算
省 M1 卡充值密钥	0x07	11-12	直接进行加密计算
通讯密钥	0x27	01-02	按照 POS 机编号分散后使用

4.3.3 企业应用区密钥定义

密钥类型	密钥属性	密钥索引	使用条件
企业 M1 钱包消费密钥	0x27	01-02	按照企业代码分散后使用
企业 M1 卡 TAC 密钥	0x26	01-02	按照企业代码分散后使用
企业 M1 卡充值密钥	0x27	11-12	按照企业代码分散后使用

5、密钥和密码计算方法

5.1卡密钥定义

卡交易过程中涉及的密钥如下表所示：

密钥类型	密钥管理机构	密钥使用方法
发行密钥	RF-UIM 卡发行机构维护、管理	存储在加密机中，在发行时进行更新
全国消费密钥	全国密钥管理中心	存储在 PSAM 卡上
全国充值密钥	全国密钥管理中心	存储在加密机中
全国 TAC 密钥	全国密钥管理中心	存储在 PSAM 卡上
省级消费密钥	省级密钥管理中心	建议存储在 PSAM 卡上
省级充值密钥	省级密钥管理中心	存储在加密机中
省级 TAC 密钥	省级密钥管理中心	存储在 PSAM 卡上
PSAM 外部认证密钥	全国密钥管理中心	存储在 POS 安全区
企业消费密钥	省级密钥管理中心	存储在读头或 POS 安全区
企业充值密钥	省级密钥管理中心	存储在读头或 POS 安全区
企业 TAC 密钥	省级密钥管理中心	存储在读头或 POS 安全区

5.2 卡片认证码

卡片认证码计算方法：

1. 3DES（卡片发行密钥，2 字节城市代码＋4 字节 CSN＋发行流水右 2 字节）
2. 取加密结果的前 4 字节为卡片认证码

5.3 扇区密钥计算

全国应用、省应用扇区消费密钥计算方法：

1. 从 PSAM 卡上获得应用序列号，将保存在安全区中的外部认证密钥按照应用序列号分散后，进行外部认证，获得 PSAM 卡密钥计算权限
2. 取 PSAM 卡上的消费密钥，针对（4 字节 CSN＋发行流水右 2 字节＋认证码左

2 字节）进行 3DES 加密

3. 取加密结果前 6 字节作为扇区消费密钥

全国应用、省应用扇区充值密钥计算方法：

1. 从 PSAM 卡上获得应用序列号，将保存在安全区中的外部认证密钥按照应用序列号分散后，进行外部认证，获得 PSAM 卡密钥计算权限
2. 取 PSAM 卡上的充值密钥，针对（4 字节 CSN＋发行流水右 2 字节＋认证码左 2 字节）进行 3DES 加密

取加密结果前 6 字节作为扇区充值密钥

企业应用扇区消费密钥计算方法：

1. 从读头取扇区消费密钥，针对（4 字节 CSN＋发行流水右 2 字节＋认证码左 2 字节）进行 3DES 加密计算
2. 取加密结果前 6 字节作为扇区消费密钥

企业应用扇区充值密钥计算方法：

1. 从读头取扇区充值密钥，针对（4 字节 CSN＋发行流水右 2 字节＋认证码左 2 字节）进行 3DES 加密计算
2. 取加密结果前 6 字节作为扇区充值密钥

5.4 TAC 计算方法

5.4.1 M1 类型卡片 TAC 计算方法

参加 TAC 计算的数据，包括：

- ✧ 交易类型，1 字节（0x01：消费；0x02：充值）
- ✧ 应用类型标识，1 字节（0x01：全国钱包；0x04：省钱包；0x08：企业钱包）
- ✧ SAM 卡应用序列号（不采用 SAM 卡的取终端号）6 字节，不足前补 0
- ✧ 终端交易流水号，4 字节
- ✧ 卡种标识，2 字节
- ✧ 地区代码，2 字节
- ✧ 卡顺序号，4 字节
- ✧ 交易前余额，4 字节
- ✧ 交易金额，4 字节

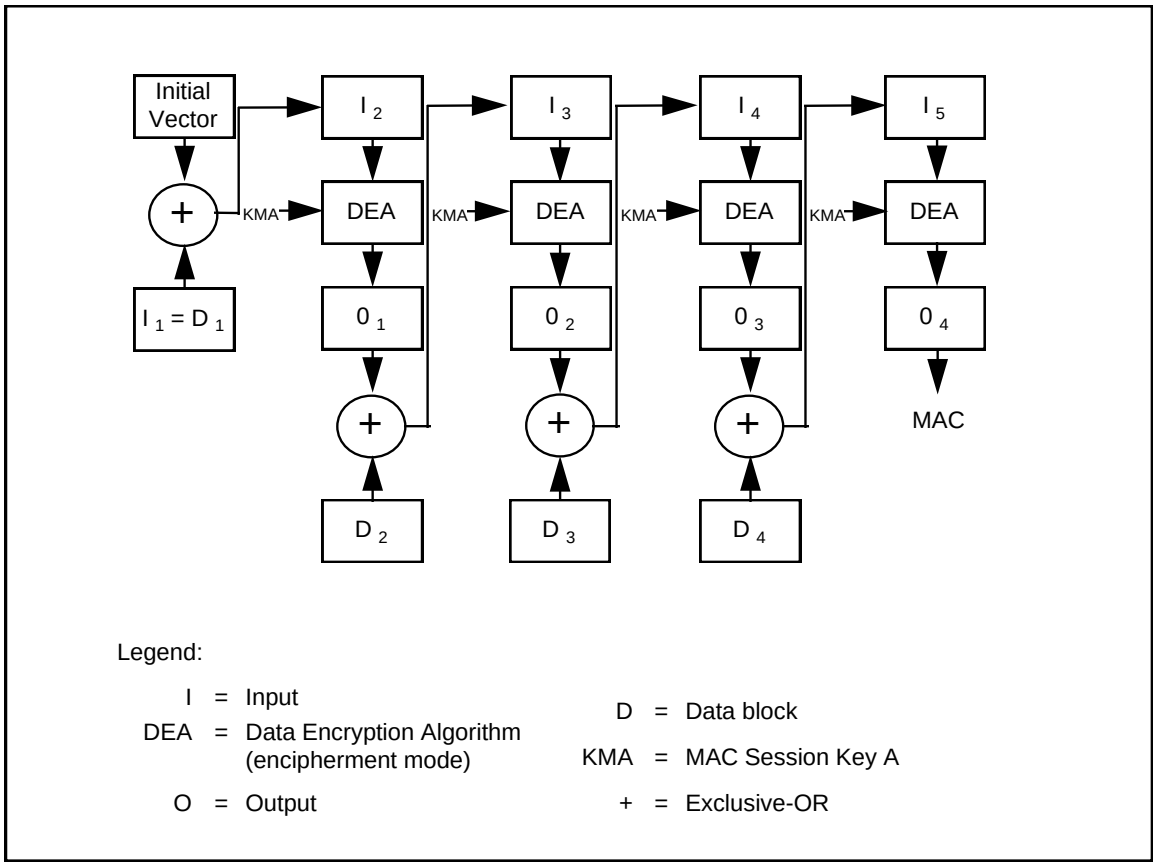
- ✧ 交易日期，4 字节
- ✧ 交易时间，3 字节
- ✧ 卡交易计数器，4 字节

TAC 计算流程：

1. 取保存在安全区或 PSAM 卡上的 TAC 密钥，针对（4 字节 CSN＋发行流水右 2 字节＋认证码左 2 字节）进行密钥分散
2. 根据子密钥针对 TAC 计算数据进行 3DES CBC MAC 计算，随机因子为 8 字节全 0
3. 取计算结果的前 4 字节为 TAC

MAC 计算流程如下：

- ✧ 第一步：将一个 8 个字节长的初始值（Initial Vector）设定为 16 进制的’0x 00 00 00 00 00 00 00 00’。
- ✧ 第二步：将所有的输入数据按指定顺序连接成一个数据块。
- ✧ 第三步：将连接成的数据块分割为 8 字节长的数据块组，标识为 D1, D2, D3, D4 等等。分割到最后，余下的字节组成一个长度小于等于 8 字节的最后一块数据块。
- ✧ 第四步：如果最后一个数据块长度为 8 字节，则在此数据块后附加一个 8 字节长的数据块，附加的数据块为：16 进制的’0x 80 00 00 00 00 00 00 00’。如果最后一个数据块长度小于 8 字节，则该数据块的最后填补一个值为 16 进制 ’0x80’ 的字节。如果填补之后的数据块长度等于 8 字节，则跳至第五步。如果填补之后的数据块长度仍小于 8 字节，则在数据块后填补 16 进制’0x00’的字节至数据块长度为 8 字节。
- ✧ 第五步：MAC 的产生是通过上述方法产生的数据块组，由 TAC 密钥进行加密运算， MAC 或 TAC 的算法如下图描述。
- ✧ 第六步：最终值的左 4 字节为 MAC 或 TAC。



5.4.2 CPU 类型卡片 TAC 计算方法(完全遵循 PBOC 标准规范)

1) TAC 计算方法：

PBOC 中 TAC 的计算如下：

TAC 的计算不采用过程密钥方式，它用 DTK 左右 8 位字节异或运算的结果对以下数据进行加密运算来产生（按所列顺序）：

——电子存折余额（交易后）或电子钱包余额（交易后）；

——电子存折联机交易序号（加 1 前）或电子钱包联机交易序号（加 1 前）；

——交易金额；

——交易类型标识；

——终端机编号

——交易日期（主机）；

——交易时间（主机）。

2) MAC 计算：

MAC 的计算如下：

SESLK：伪随机数（ICC）||电子存折联机交易序号或电子钱包联机交易序号||“8000”

MAC1 的计算如下:

用 SESLK 对数据加密产生 MAC1；

主机产生一个报文签别码（MAC2），用于 IC 卡对主机进行合法性检查。用 SESLK 对数据加密产生 MAC2

5.5校验位 Luhn 算法

Luhn 计算模 10“隔位 2 倍加”校验数的公式 计算步骤如下：

1. 步骤 1：从右边第 1 个数字（低序）开始每隔一位乘以 2。
2. 步骤 2：把在步骤 1 中获得的乘积的各位数字与原号码中未乘 2 的各位数字相加。
3. 步骤 3：从邻近的较高的一个以 0 结尾的数中减去步骤 2 中所得到的总和[这相当于求这个总和的低位数字（个位数）的“10 的补数”]。如果在步骤 2 得到的总和是以零结尾的数（如 30、40 等等），则校验数字就是零。

计算步骤如下：

步骤1：从右边第1个数字（低序）开始每隔一位乘以2。

步骤2：把在步骤1中获得的乘积的各位数字与原号码中未乘2的各位数字相加。

步骤3：从邻近的较高的一个以0结尾的数中减去步骤2中所得到的总和[这相当于求这个总和的低位数字（个位数）的“10的补数”]。如果在步骤2得到的总和是以零结尾的数（如30、40等等），则校验数字就是零。

例：

无校验数的卡号4992 73 9871										步骤
4	9	9	2	7	3	9	8	7	1	1
	×2		×2		×2		×2		×2	
	18		4		6		16		2	
4 + 1 + 8 + 9 + 4 + 7 + 6 + 9 + 1 + 6 + 7 + 2 = 64										2
70 − 64 = 6										3

带有校验数的卡号为：4992 73 9871 6