东莞新莞人金融服务 IC 卡的规格文档

一、 IC 卡所需遵循的规范

IC 卡需遵循以下国际标准：

- ISO/IEC7816 智能卡标准
- ISO/IEC14443 非接触标准

需遵循我国的行业规范的要求：

- 《中国金融集成电路（IC）卡规范》 第 1 部分：电子钱包/电子存折应用卡片规范（编号：JR/T 0025.1—2010）
- 《中国金融集成电路（IC）卡规范》 第 2 部分：电子钱包/电子存折应用规范（编号：JR/T 0025.2—2010）
- 《中国金融集成电路（IC）卡规范》第 9 部分：电子钱包扩展应用指南（编号：JR/T 0025.2—2010）

同时，需遵循《手机通宝 PKI 卡非接触面接口规范 V1.0》

如有需要，卡片的背面贴有磁条，其功能和使用方法与现有银行卡完全相同，具有银行卡的全部功能，集定活期、借记、信用多功能于一体；能够很好地支持银行相关的各种应用。磁道的数据格式严格按照银联相关标准：

- 《银联卡卡片规范》
- 《银行卡磁条信息格式和使用规范》

二、 IC 卡文件结构

2.1 文件结构：

IC卡上的文件是一种树形结构。树的每一个分支是一个应用定义文件（ADF）或一个目录定义文件（DDF）。一个ADF是一个或者多个应用基本文件（AEF）

的入口点。一个ADF及其相关的数据文件处于树的同一分支上。一个DDF是其他ADF或者DDF的入口点。

2.2 文件引用

根据其类型，文件可以通过文件名或SFI引用。

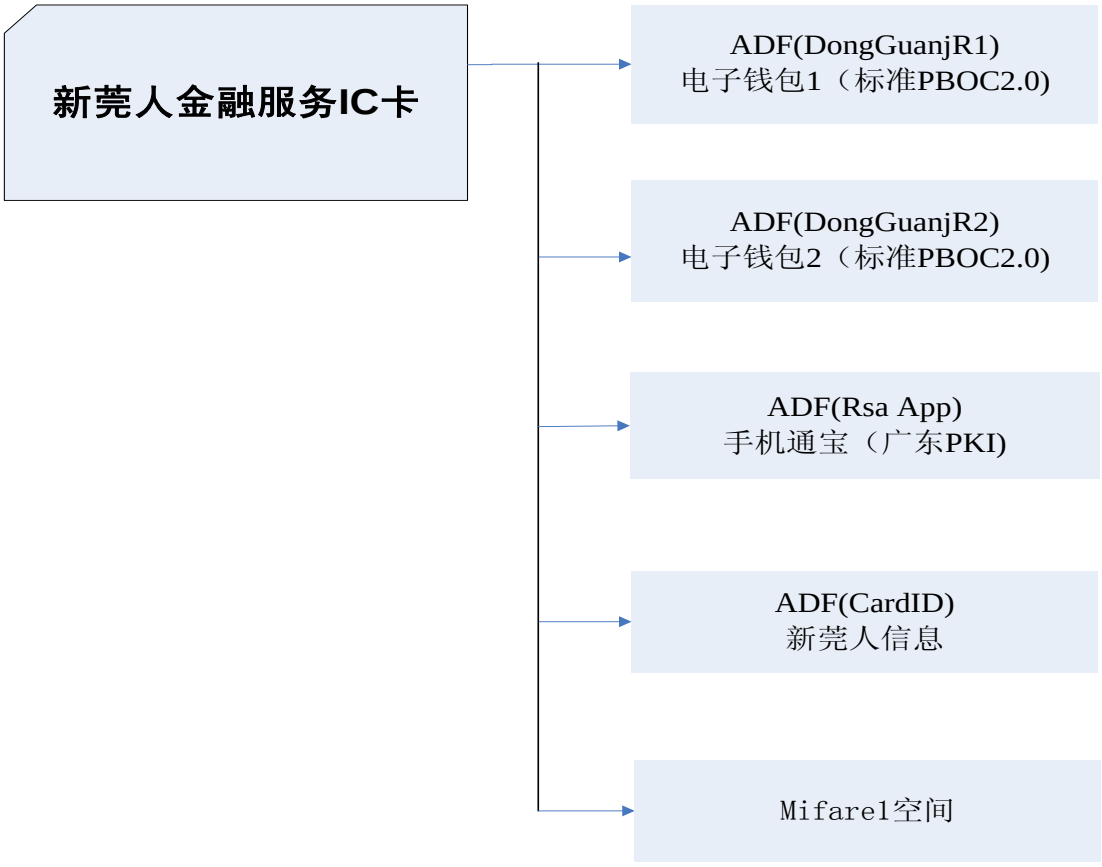
2.2.1 通过文件名引用

卡片中的任何ADF或DDF都可以通过其DF名引用。ADF的DF名与其AID对应或包含AID作为DF的开始字符。在一张给定的卡片内，每个DF名必须唯一。

2.2.2 通过短文件标识符（SFI）引用

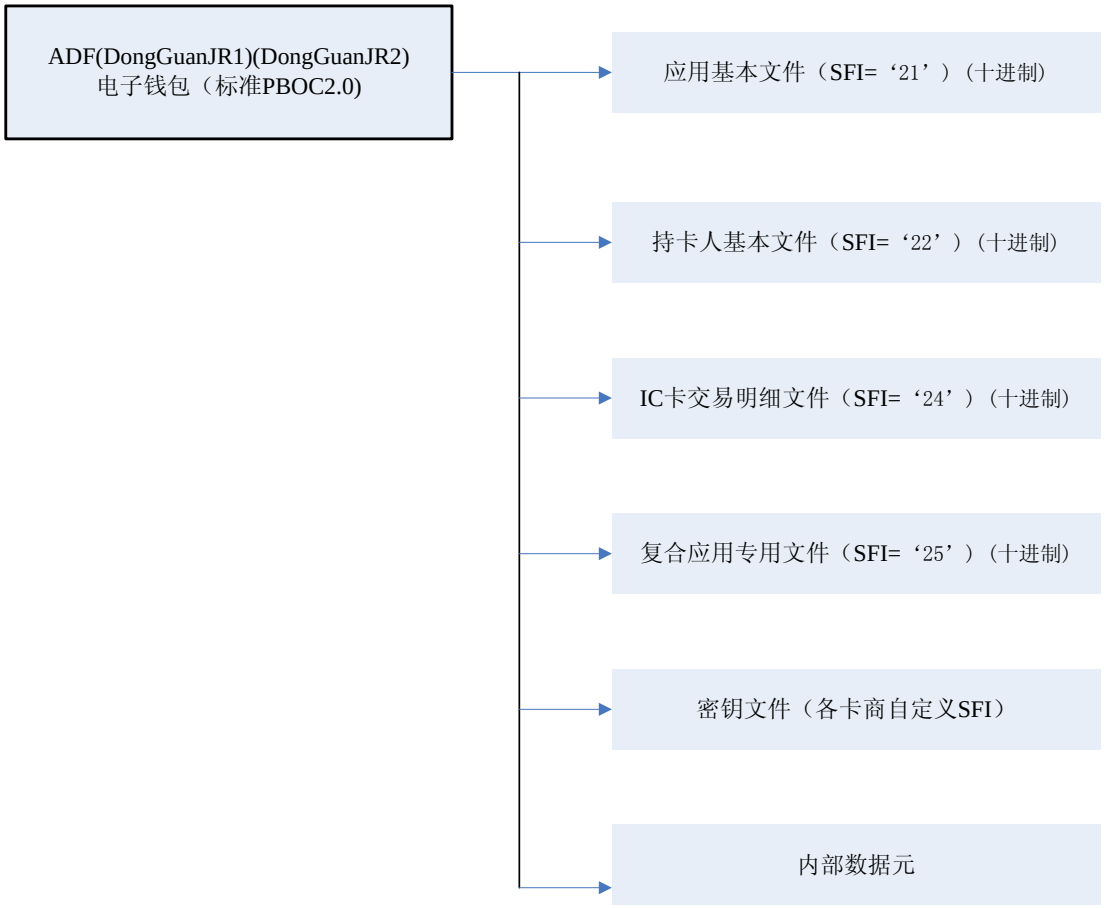
SFI用于选择AEF。在给定应用中的任何AEF都可以通过SFI（5位编码，取值范围从1到30）引用。SFI的编码在每一个用到它的命令中进行描述。在一个应用中SFI必须是唯一的。

卡片文件结构如下图所示：



2.3 各 ADF 描述：

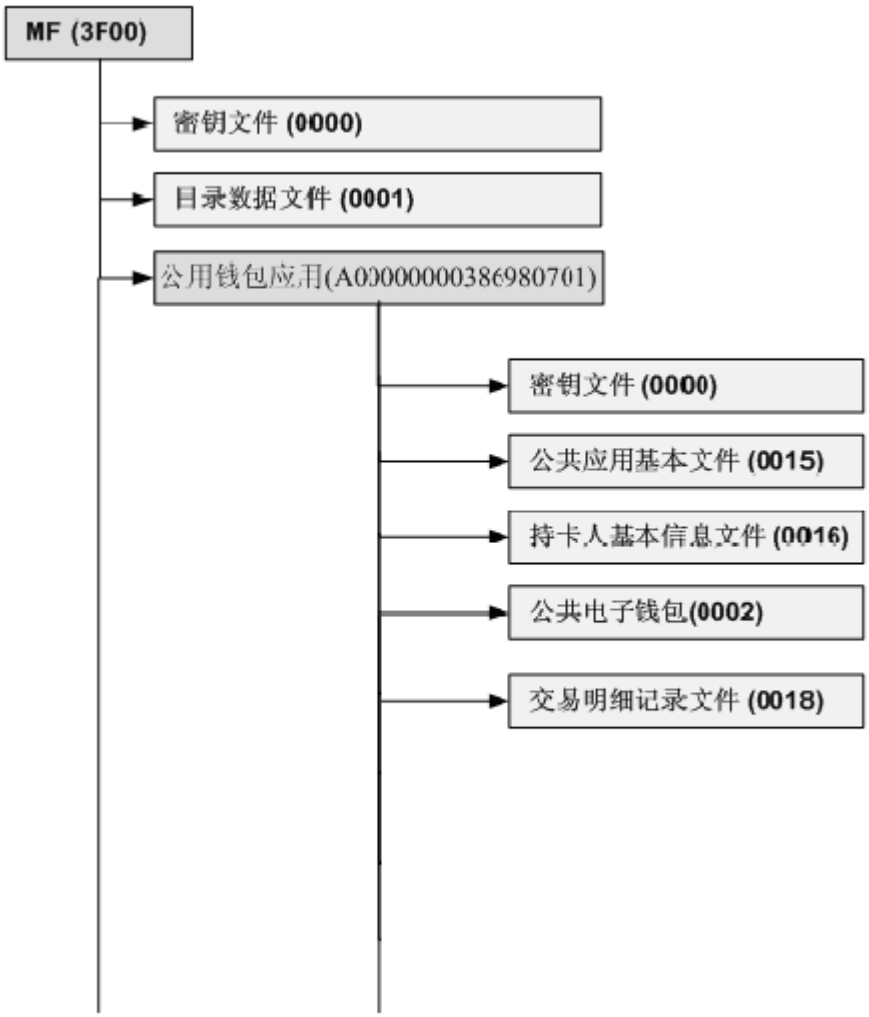
2.3.1 ADF(DongGuanJR1)（(DongGuanJR2)



各文件和内部数据元定义完全按照《中国金融集成电路（IC）卡规范》定义。

/******为与省公司一致，必须有一个应用使用此结构 start**********/**

1.1 卡片结构



1.2 卡结构说明

1.2.1 MF（3F00）

MF 下文件信息：

文件名称	文件类型	标识符	大小	权限设计	
MF	主控文件	3F00	FFFFH	-	-
KEY 文件	密钥文件	0000	10 条	读取：禁止	增权：密文+MAC(DCCK)
目录数据文件	变长记录文件	0001	0050H	读取：自由	更新：禁止
ADF1-ADFn	目录文件	3F01-3Fnn		-	-

KEY 文件（0000）

密钥名称	密钥代码	密钥类型	密钥标识	分散级别	分散因子	密钥作用
卡片主控子密钥	DCCK	主控密钥	00	0		控制 MF 下文件添加

目录数据文件(0001)

<table>
<tr><td colspan="2">文件标识（SFI）</td><td colspan="6">0x01</td></tr>
<tr><td colspan="2">文件类型</td><td colspan="6">变长记录文件</td></tr>
<tr><td colspan="2">文件大小</td><td colspan="6">0050H</td></tr>
<tr><td colspan="2">文件存取控制</td><td colspan="3">读=自由</td><td colspan="3">改写=禁止</td></tr>
<tr><td>标志</td><td>长度</td><td colspan="6">值</td></tr>
<tr><td rowspan="4">70</td><td rowspan="4">Var.</td><td colspan="6">结构数据对象标签</td></tr>
<tr><td>61</td><td>Var.</td><td colspan="4">应用模板</td></tr>
<tr><td></td><td></td><td>4F</td><td>0x05-0x10</td><td colspan="2">DDF 名称</td></tr>
<tr><td></td><td></td><td>50</td><td>0x01-0x10</td><td colspan="2">应用标签</td></tr>
</table>

1.2.2 公用钱包应用（A00000000386980701）

A00000000386980701 目录下文件信息：

文件名称	文件类型	标识符	大小	权限设计	
目录文件	主控文件	3F01	07FFH	-	-
KEY 文件	密钥文件	0000	01FFH	读取：禁止	增权：密文+MAC(DCMK)
公共应用基本	二进制文件	0015	001EH	读取：自由	更新：明文+MAC(DAMK)
持卡人基本信息文件	二进制文件	0016	0037H	读取：自由	更新：明文+MAC(DAMK)
电子钱包文件	钱包文件	0002		读取：COS 维护	更新：COS 维护
电子钱包交易明细记录文件	循环记录文件	0018	0A × 17H	读取：自由	更新：COS 维护

KEY 文件（0000）

密钥名称	密钥代码	密钥类型	密钥标识	分散级别	分散因子
应用维护子密钥	DAMK	维护密钥	00	1	L1：应用序列号
消费子密钥	DPK	消费密钥	01	1	L1：应用序列号
圈存子密钥	DLK	圈存密钥	01	1	L1：应用序列号
TAC 子密钥	DTK	TAC 密钥	01	1	L1：应用序列号

公共应用基本信息文件(0015)

文件标识（SFI）	0x15		
文件类型	二进制文件		
文件大小	001EH		
文件存取控制	读=自由	改写=明文+MAC(DAMK)	
字节	数据元	长度	格式
01－02	发卡方代码	2	BCD（8698）
03－04	城市代码	2	BCD
05－06	行业代码	2	BCD
07－08	RFU	2	BCD（FFFF）
09－09	应用类型标识（启用标志）	1	BCD
10－10	应用版本	1	BCD
11－12	互联互通标识（参与互通城市的标识）	2	BCD
13－20	应用序列号	8	HEX
21－24	应用启动日期	4	YYYYMMDD 启用时更新
25－28	应用有效日期	4	YYYYMMDD 启用时更新
29－29	卡主类型	1	
30－30	卡子类型	1	

持卡人基本信息文件（0016）

文件标识（SFI）	0x16	
文件类型	二进制文件	
文件大小	0037H	
文件存取控制	读=自由	改写=明文+MAC(DAMK)

电子钱包文件（0002）

文件标识（SFI）	0x02	
文件类型	电子钱包专用文件	
文件大小	0002×0008H	
文件存取控制	读=COS 内部操作	改写= COS 内部操作

电子钱包交易明细记录文件（0018）

文件标识（SFI）	0x18		
文件类型	循环记录文件		
文件大小	000A×0017H		
文件存取控制	读=自由	改写= COS 内部操作	
字节	数据元	长度	格式
01－02	电子钱包消费、冲资交易序号	2	HEX

03－05	透支限额	3	HEX
06－09	交易金额	4	HEX
10－10	交易类型	1	BCD
11－16	交易终端编号	6	BCD
17－20	交易日期	4	YYYYMMDD
21－23	交易时间	3	HHMMSS

/*****为与省公司一致，必须有一个应用使用此结构 end**********/**

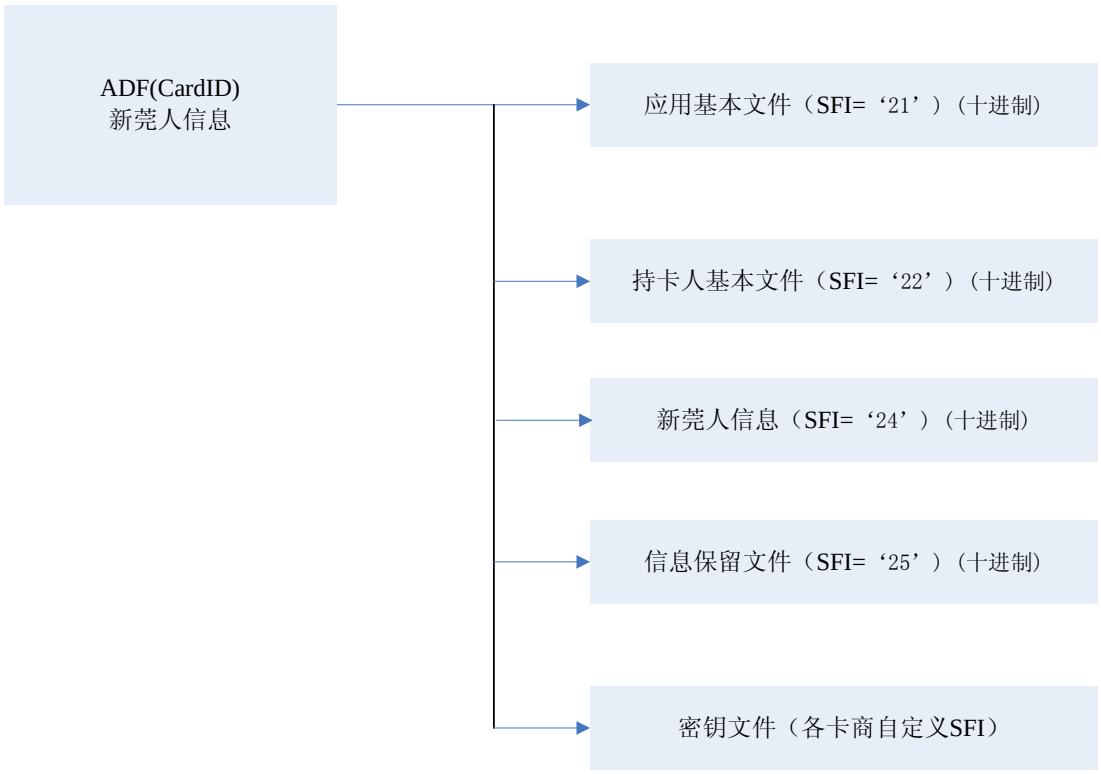
复合交易记录文件（0019）

文件标识（SFI）	0x19		
文件类型	变长记录文件		
文件大小	00xxH(根据客户需求定义长度)		
文件存取控制	读=自由	改写=过程消费改写	
字节	数据元	长度	格式
01	复合消费标志符	1	HEX
02	记录长度	1	HEX
03	应用锁定标志	1	HEX
04-n	复合消费数据	n-3	HEX

2.3.2 ADF(Rsa App)

数据规划见《手机通宝 PKI 卡非接触面接口规范 V1.0》2.2 章节描述。

2.3.3 ADF(CardID)



应用基本文件

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	改写 =明文+MAC(DAMK)
字节	数据元	长度
1-8	发卡方标识	8
9	应用类型标识	1
10	发卡方应用版本	1
11-20	应用序列号	10
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

持卡人基本文件

文件标识(SFI)		‘22’ (十进制)
文件类型		透明
文件大小		55
文件存取控制	读 = 自由	改写 =明文+MAC(DAMK)
字节	数据元	长度
1	卡类型标识	1
2	本行职工标识	1

3-22	持卡人姓名	20
23-54	持卡人证件号码	32
55	持卡人证件类型	1

新莞人信息文件

文件标识(SFI)		‘24’ (十进制)
文件类型		透明
文件大小		738 字节
文件存取控制	读 = 明文+MAC(DAMK)	改写 = 明文 +MAC(DAMK)
字节	数据元	长度
基本情况		
1	基本情况标识位（0F）	1byte
2-31	姓名	30 bytes
32	性别	1byte
33	政治面貌	1byte
34-45	身份证件号码	12bytes
46-49	出生日期	4bytes
50	身高	1byte
51	文化程度	1byte
52	婚姻状态	1byte
53-54	国家/地区	2bytes
55	民族	1byte
56	户口所在地类型	1byte
57-106	户口所在地	50bytes
107-156	户籍所在地（籍贯）	50bytes
157-160	首次来东莞日期	4bytes
161-170	联系电话	10bytes
居住信息		
171	居住信息标识位（04）	1byte
172-175	居住日期	4bytes
176	经济来源	1byte
177-226	现居住地址	50bytes

227	居住事由	1byte
计生信息		
228	计生信息标识位（02）	1byte
229	计生措施	1byte
230	落实计生措施地点	1byte
图书证信息		
231-237	图书证信息	7bytes
指纹文件信息		
238-737	指纹文件信息	500bytes
卡片生命周期信息		
738	卡片生命周期信息	1bytes

数据定义：
基本情况标识位：0F 代表后面属于基本情况的 LV 格式的数据信息有 15 个。
姓名：预留 30 个字节，可存储 15 个汉字，外国人姓和名之间用“ • ”区分
性别：
01 ——男
02 ——女
政治面貌：指本人政治身份，国标 GB/T 4762-1984 定义
01 ——中国共产党党员
02 ——中国共产党预备党员
03 ——中国共产主义青年团团员
04 ——中国国民党革命委员会会员
05 ——中国民主同盟盟员
06 ——中国民主建国会会员
07 ——中国民主促进会会员
08 ——中国农工民主党党员
09 ——中国致公党党员
0A ——九三学社社员
0B ——台湾民主自治同盟盟员
0C ——无党派民主人士
0D ——群众
身份证件号码：预留 13 字节，第一字节代表长度，后面几个自己存储数据，空缺位补 F。
文化程度：
01 ——研究生
02 ——本科
03 ——专科
04 ——职高
05 ——高中
06 ——初中

07 ——小学
08 ——其他
婚姻状态：
01 ——未婚
02 ——已婚
03 ——丧偶
04 ——离婚
国家/地区： ISO 3166-1 这个标准定义了大部分国际普遍公认的国家和境外领土，这个文件中用两个字节存储采用二位字母代码（ISO 3166-1 alpha-2）编码的国家/地区编码。
民族：

01 汉 族	02 蒙古族	03 回 族	04 藏 族	05 维吾尔族	06 苗 族	07 彝 族
08 壮族	09 布依族	0A 朝鲜族	0B 满族	0C 侗族	0D 瑶族	0E 白族
0F 土家族	10 哈尼族	11 哈萨克族	12 傣族	13 黎族	14 傈僳族	15 佤族
16 畲族	17 高山族	18 拉祜族	19 水族	1A 东乡族	1B 纳西族	1C 景颇族
1D 柯尔克孜族	1E 土族	1F 达斡尔族	20 仫佬族	21 羌族	22 布朗族	23 撒拉族
24 毛南族	25 仡佬族	26 锡伯族	27 阿昌族	28 普米族	29 塔吉克族	2A 怒族
2B 乌孜别克族	2C 俄罗斯族	2D 鄂温克族	2E 德昂族	2F 保安族	30 裕固族	31 京族
32 塔塔尔族	33 独龙族	34 鄂伦春族	35 赫哲族	36 门巴族	37 珞巴族	38 基诺族
40 黑种人	41 白种人	42 棕种人	43 黄种人	44 其他		

户口所在地类型
01 ——非农业户口
02 ——农业户口
03 ——其他
居住信息标识位（04）：04 代表后面属于居住信息的 LV 格式的数据信息有 4 个。
经济来源：
01 ——工资收入
02 ——经营收入
03 ——亲属供给
04 ——租金收入
05 ——其他
居住事由：

01 ——务工
02 ——务农经商
03 ——服务
04 ——因公出差
05 ——借读培训
06 ——治病疗养
07 ——保姆
08 ——投靠亲友
09 ——探亲访友
0A ——旅游观光
0B ——其他
计生信息标识位（02）:02 代表后面属于计生信息的 LV 格式的数据信息有 2 个。
计生措施：
01 ——女扎
02 ——男扎
03 ——上环
04 ——皮下埋植
05 ——药具
06 ——无（待孕、怀孕、哺乳期）
落实计生措施地点：
01 ——省外
02 ——省内
03 ——市内

信息保留文件

文件标识(SFI)		‘25’（十进制）
文件类型		透明
文件大小		100
文件存取控制	读 = 自由	改写 = 明文+MAC(DAMK)
字节	数据元	长度
1-100	自定义数据	100

2.4 Mifare1 空间

新莞人金融服务 IC 卡须预留 Mifare1 空间支持标准的 Mifare1 应用，用户可根据具体应用情况，对不同的扇区选用不同的访问控制条件和不同的密钥，以保证一卡多用的安全性。如果访问控制条件允许修改密钥，则可以在通过授权验证后进行修改，否则密钥将不可更改。

当对区尾的访问控制条件、密钥进行写操作时，需要良好的操作环境（将卡置于可靠的

读写区域中），以防止发生写操作非正常中断，造成该扇区被自锁而无效。

三、 APDU

3.1 APDU(电子钱包和新莞人信息)

——APPLICATION UNBLOCK（应用解锁）
——CARD BLOCK（卡片锁定）
——EXTERNAL AUTHENTICATION（外部认证）
——GET RESPONSE（取响应）
——GET CHALLENGE（产生随机数）
——INTERNAL AUTHENTICATION（内部认证）
——PIN CHANGE/UNBLOCK（个人识别码修改/解锁）
——READ BINARY（读二进制）
——READ RECORD（读记录）
——SELECT（选择）
——UPDATE BINARY（修改二进制）
——UPDATE RECORD（修改记录）
——CREDIT FOR LOAD（圈存）
——DEBIT FOR PURCHASE/CASH WITHDRAW（消费/取现）
——DEBIT FOR UNLOAD（圈提）
——GET BALANCE（读余额）
——GET TRANSACTION PROVE（取交易认证）
——NITIALIZE FOR CAPP PURCHASE（复合应用消费初始化）；
——UPDATE CAPP DATA CACHE（更新复合应用数据缓存）；
——DEBIT FOR CAPP PURCHASE（复合应用消费）。
——等等
（详见《中国金融集成电路（IC）卡规范》）

3.2 APDU(手机通宝)

——Generate RSA KEY（生成 RSA 密钥对）
——Select File（选择文件）
——Read Data（读数据）
——Write Data（写数据）
——Data Compress（数据压缩）
——Digital Signatures（数字签名）
——Signatures Verify（签名验证）
——Data Encrypt（数据加密）
——Data Decrypt（数据解密）
——Create Random Num（产生随机数）
——Operation Verify（操作认证）
——等等

（详见《手机通宝 PKI 卡非接触面接口规范 V1.0》规范）

四、 指令与交易流程

电子钱包和新莞人信息应用指令与交易流程符合《中国金融集成电路（IC）卡规范》，手机通宝应用符合《手机通宝 PKI 卡非接触面接口规范 V1.0》。

五、 密钥

密钥	发卡方	IC 卡	POS (PSAM)
用于消费交易的密钥	消费主密钥(MPK)	消费子密钥（DPK），由 MPK 用应用序列号推导获得。	消费主密钥(MPK)
用于圈存交易的密钥	圈存主密钥(MLK)	圈存子密钥（DLK），由 MLK 用应用序列号推导获得。	N/A
消费交易中用于产生 TAC 的密钥	TAC 主密钥(MTK)	TAC 子密钥（DTK），由 MTK 用应用序列号推导获得。	N/A
用于解锁 PIN 的密钥	PIN 解锁主密钥（MPUK）	PIN 解锁子密钥（DPUK），由 MPUK 用应用序列号推导获得。	由发卡方考虑决定
用于重装 PIN 的密钥	PIN 重装主密钥（MRPK）	PIN 重装子密钥（DRPK），由 MRPK 用应用序列号推导获得。	N/A
用于应用维护功能的密钥	应用主控密钥（MAMK）	应用主控子密钥（DAMK），由 MAMK 用应用序列号推导获得。	N/A

电子钱包应用的密钥

密钥的推导方法和过程密钥的产生方法见《中国金融集成电路（IC）卡规范》

密钥	发卡方	IC 卡	POS (PSAM)
用于应用维护功能的密钥	应用主控密钥（MAMK）	应用主控子密钥（DAMK），由 MAMK 用应用序列号推导获得。	N/A

新莞人信息应用的密钥

手机通宝应用密钥管理符合《手机通宝 PKI 卡非接触面接口规范 V1.0》。

六、 个人化

预个人化卡片需要分别为三个应用写密钥数据和个人化初始数据。

手机钱包应用和新莞人信息应用的密钥数据，由省公司提供加密机和端口，卡商在生产工厂连接省公司加密机灌装。

手机通宝应用密钥和初始数据遵循卓望公司提供的数据，在生产工厂个人化，并将返回数据提交给卓望公司导入 PKI 系统。

如果卡片的背面贴有磁条，个性化数据后期在银行或其他安全渠道写入。

七、 补充说明

电子钱包应用支持复合应用但不需要灰锁应用。