中 国 移 动 通 信 企 业 标 准

QB-XX-XXX-XXXX

中国移动一卡通业务设备规范
—RFID-SIM卡应用部分

RFID-SIM Card Application

Specification Supporting E-card Pass

版本号： 1.0.0

XXXX-XX-XX **发布** XXXX-XX-XX **实施**

中国移动通信集团公司 发布

目　　录

附录 B．基本数据文件

当为数据定义的长度超过实际数据长度，而位数没有占满时，补位规则如下：

- 格式n的数据元右靠齐并且左补十六进制'0'。
- 格式cn的数据元左靠齐并且右补十六进制'F'。
- 格式an的数据元左靠齐并且右补十六进制'0'。
- 格式ans的数据元左靠齐并且右补十六进制'0'。

当数据从一个实体移动到另一个时（例如：卡到终端），不管其内部如何存放，都是按照由高到低的顺序传送。数据的连接也同样符合这个原则。

一卡通应用的公共应用基本数据文件参见表B-1：

表B-1 一卡通应用的公共应用基本数据文件

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 = 需要 安全信息

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
11-18	应用序列号	8
19-22	应用启用日期	4
23-26	应用有效日期	4
27	卡类型标识	1
28-30	发卡方自定义FCI数据	3

一卡通应用下所有消费子应用的交易明细保存在同一个交易文件中，该文件必须能够容纳20条消费、圈存交易记录。

交易明细必须允许卡对其循环修改，循环文件的结构应符合ISO/IEC CD7816-4。

对明细中所有数据元的修改必须考虑数据完整性和安全要求。

文件标识（SFI）		'24'（十进制）
文件类型		循环
文件存取控制		读 = 自由 改写 = 不允许[1)]
记录大小		57（十进制）

字节	数据元	长度
1-16	企业名称	16

注：[1)] 交易明细由(U)SIM卡或普通IC卡维护，不允许外部对其修改。

17-32	钱包（脱机或联机）名称	16
33-35	联机或脱机交易序号（仅对脱机电子钱包有效） 或POS机流水号（仅对联机消费有效）	3
36-38	透支限额(仅对脱机电子钱包有效，不显示）	3
39	交易金额类型 （值：0x01—次数，0x02—金额）	
40-43	交易金额	4
44	交易类型标识	1
45-50	终端机编号	6
51-54	交易日期（终端）	4
55-57	交易时间（终端）	3

附录 C．基本数据元

一卡通应用涉及的数据元参见表C-1：

表C-1 一卡通应用数据元

数据域	说明	来源	类型	长度（字节）	取值
应用AID	标识一卡通应用	RFID-SIM 卡或普通IC卡终端	an	16	参见附录D
发卡方标识	唯一标识发卡方的数字	RFID-SIM 卡或普通IC卡	cn	8	D156000101
应用类型标识	代表卡上存在的应用类型的标识	RFID-SIM 卡或普通IC卡	cn	1	值： 00：一卡通应用（支持门禁、考勤、消费功能） 所有其他值保留为将来使用
发卡方应用版本	代表卡当前使用应用版本的一个数字	RFID-SIM 卡或普通IC卡	b	1	参见《中国移动一卡通业务接口规范--RFID-SIM 卡与一卡通平台接口分册》
应用序列号	发卡方分配的一个数字	RFID-SIM 卡	cn	8	参见

		或普通IC卡			
应用启用日期	指示应用生效日期	RFID-SIM卡或普通IC卡	cn	4	格式：YYYYMMDD（4位年、2位月、2位日）
应用有效日期	该日期后卡应用终止	RFID-SIM卡或普通IC卡	cn	4	格式：YYYYMMDD（4位年、2位月、2位日）
卡类型标识	卡的类型	RFID-SIM卡或普通IC卡	cn	1	值： 00：普通IC卡 01：RFID-SIM卡 所有其他值保留为将来使用
发卡方自定义FCI数据	发卡方在其自己的终端上用于特殊处理的专用数据	RFID-SIM卡或普通IC卡	b	3	取值全0 所有其他值保留为将来使用
应用锁定标识	应用是否锁定标识	RFID-SIM卡或普通IC卡	b	1	值： 0x00：未锁定； 0x01：锁定
应用激活标识	应用是否激活标识	RFID-SIM卡或普通IC卡	b	1	值： 0x00：未激活； 0x01：激活
应用管理密钥	参见《中国移动一卡通业务安全技术规范-密钥与算法要求》	RFID-SIM卡或普通IC卡终端	b	16	
空中传输密钥	同上	RFID-SIM卡或普通IC卡终端	b	16	
空中报文MAC密钥	同上	RFID-SIM卡或普通IC卡终端	b	16	
企业名称	员工所属企业的名称	RFID-SIM卡或普通IC卡		16	Length(1字节) + DCS（1字节）+ 企业名称 企业中文名称采用UCS2编码

钱包（脱机或联机）名称		RFID-SIM卡或普通IC卡		16	Length(1字节) + DCS（1字节）+ 钱包名称 钱包中文名称采用UCS2编码
钱包是否脱机标识	标识钱包是脱机类型还是联机类型	RFID-SIM卡或普通IC卡	b	1	值： 0x00：联机； 0x01：脱机
脱机电子钱包脱机交易序号	卡中的一个计数器，每当脱机电子钱包脱机消费交易发生就增加1	RFID-SIM卡或普通IC卡	B	2	初始值0x0000，每次成功交易加1，达到0xFFFF后，再加1返回0x0000.
脱机电子钱包联机交易序号	卡中的一个计数器，每当脱机电子钱包圈存交易发生就增加1，该计时器和主机同步，且可以在过程密钥的产生中使用。	RFID-SIM卡或普通IC卡主机	b	2	初始值0x0000，每次成功交易加1，达到0xFFFF后，再加1返回0x0000.
钱包类型	有限次（或余额）或不限次（余额）	RFID-SIM卡或普通IC卡	b	1	值： 0x01：有限余额； 0x02：不限余额 0x11：有限次； 0x12：不限次
钱包余额（或剩余使用次数）	脱机电子钱包的余额（或剩余使用次数）	RFID-SIM卡或普通IC卡	b	4	钱包余额（或剩余使用次数）为真实余额（或剩余使用次数）同透支限额之和，暂时不支持透支限额功能，因此钱包余额（或剩余使用次数）等于真实余额

					（或剩余使用次数）。
钱包余额有效期启用标识	标识是否启用钱包余额有效期字段	RFID-SIM卡或普通IC卡	b	1	值： 0x00：不启用钱包余额有效期； 0x01：启用钱包余额有效期
钱包余额（或剩余使用次数）有效期	该日期后余额无效	RFID-SIM卡或普通IC卡	cn	4	格式：YYYYMMDD（4位年、2位月、2位日）
钱包余额（或剩余使用次数）类型	脱机电子钱包的余额（或剩余使用次数）类型	RFID-SIM卡或普通IC卡	b	1	值： 0x00：钱包余额（或剩余使用次数）为补贴方式； 0x01：钱包余额（或剩余使用次数）为个人充值方式； 所有其他值保留为将来使用
透支限额	发卡方给持卡人指定的最大透支额度（金额或次数）	RFID-SIM卡或普通IC卡	b	3	值： 暂不使用，取值全0.
钱包累计消费金额（或消费次数）	不限次脱机电子钱包的累计消费金额（或累计消费次数）	RFID-SIM卡或普通IC卡	b	4	值： 初始值：0 每次消费该值增加消费金额（或次数）
交易金额	消费或圈存等当前交易中涉及的金额	终端	b	4	
交易类型标识	用于标识持卡人选择的交易类型（例如：圈存、消费等等）而分配的一个值。	RFID-SIM卡或普通IC卡 终端	cn	1	值： 02：圈存 06：脱机消费 21：联机消费 22：脱机撤销 23：联机撤销 24：退费 所有其他值

					保留为将来使用
终端机编号	用来唯一标识商户终端的一个数字	终端	cn	6	保存在SAM卡中
交易日期（终端）	交易发生日期	终端	cn	4	格式：YYYYMMDD（4位年、2位月、2位日）
交易时间（终端）	交易发生时间	终端	cn	3	格式：HHMMSS（2位时、2位分、2位秒）
联机交易鉴权密钥（联机消费密钥）	参见《中国移动一卡通业务安全技术规范-密钥与算法要求》	RFID-SIM卡或普通IC卡主机	b	16	
联机交易TAC密钥（联机消费密钥）	同上	RFID-SIM卡或普通IC卡主机	b	16	
消费密钥（脱机消费密钥）	同上	RFID-SIM卡或普通IC卡终端	b	16	
充值密钥（脱机消费密钥）	同上	RFID-SIM卡或普通IC卡主机	b	16	
脱机交易TAC密钥（脱机消费密钥）	同上	RFID-SIM卡或普通IC卡主机	b	16	
企业ID	唯一标识某一企业的数字	RFID-SIM卡或普通IC卡	cn	6	6字节长的BCD编码，共14位数字；编码规则：2位省代码＋12位序号，详细编码规则参见《中国移动一卡通业务总体技术要求》
员工ID	唯一标识企业内某一员工的数字	RFID-SIM卡或普通IC卡	an	20	具体取值由各企业自行定义
员工企业流水号	唯一标识企业内某一员工的数字	RFID-SIM卡或普通IC卡	cn	4	具体取值由各企业自行定义，可考虑采用顺序流

					水号的方式。
子应用索引号	唯一标识企业内某一子应用的数字	RFID-SIM 卡或普通IC卡	b	1	主控子应用的索引号为0x00； 非主控子应用的索引号取非0x00值，但要求企业内的非主控子应用索引号不重复。
子应用有效期	该日期后子应用终止	RFID-SIM 卡或普通IC卡	cn	4	格式：YYYYMMDD（4位年、2位月、2位日）
子应用类型	子应用的具体类型	RFID-SIM 卡或普通IC卡	b	1	值： 0x00：主控子应用； 0x01：门禁； 0x02：考勤； 0x03：脱机消费； 0x04：联机消费； 0x10~0x1F：企业自定义应用； 所有其他值保留为将来使用
子应用锁定标识	子应用是否锁定标识	RFID-SIM 卡或普通IC卡	b	1	值： 0x00：未锁定； 0x01：锁定
企业主控密钥	参见《中国移动一卡通业务安全技术规范-密钥与算法要求》	RFID-SIM 卡或普通IC卡	b	16	
企业空中传输密钥	同上	RFID-SIM 卡或普通IC卡	b	16	
企业空中报文MAC密钥	同上	RFID-SIM 卡或普通IC卡	b	16	
门禁名称		RFID-SIM 卡或普通IC卡		16	Length(1 字节) + DCS（1字节）+ 门禁

					名称 门禁中文名称采用UCS2编码
门禁密钥	用于门禁的身份识别应用密钥，参见《中国移动一卡通业务安全技术规范-密钥与算法要求》	RFID-SIM卡或普通IC卡终端	b	16	
考勤名称		RFID-SIM卡或普通IC卡		16	Length(1字节) + DCS（1字节）+ 考勤名称 考勤中文名称采用UCS2编码
考勤密钥	用于考勤的身份识别应用密钥，参见《中国移动一卡通业务安全技术规范-密钥与算法要求》	RFID-SIM卡或普通IC卡终端	b	16	
密钥标识	由密钥分散级数、密钥标识组成，参见《中国移动一卡通业务安全技术规范-密钥与算法要求》	RFID-SIM卡或普通IC卡终端/主机	b	1	
密钥版本	密钥的版本，参见《中国移动一卡通业务安全技术规范-密钥与算法要求》	RFID-SIM卡或普通IC卡终端/主机	b	1	
密钥索引号	密钥的索引号，参见《中国移动一卡通业务安全技术规范-密钥与算法要求》	RFID-SIM卡或普通IC卡终端/主机	b	1	
算法标识	密钥所支持的加密算法，参见《中国移动一卡通业务安全技术规范-密钥与算法要求》	RFID-SIM卡或普通IC卡终端	b	1	

附录D. 一卡通应用AID

AID= D156000101800000000000100000000

附录 E. APDU 指令

附录 E.1 Write Key

附录 E.1.1 定义和范围

WRITE KEY命令可向RFID-SIM卡中装载（第一次写入）密钥或更新卡中已存在的密钥。本命令可支持8字节或16字节的密钥，密钥写入必须采用加密的方式，在应用管理密钥的控制下进行。

在密钥装载前必须用GET CHANLLEGE命令从RFID-SIM卡取一个4字节的随机数。

注：

本指令适用的密钥仅包括：1）应用管理密钥；2）空中传输密钥；3）空中报文MAC密钥。

附录 E.1.2 命令报文

WRITE KEY命令报文见表E-1：

表E-1 WRITE KEY命令报文

代码	值
CLA	84h
INS	D4h
P1	00h
P2	00h
L_c	14h或1Ch
Data	密钥密文信息||MAC
L_e	不存在

附录 E.1.3 命令报文数据域

命令报文数据域包括要装载的密钥密文信息和MAC。

密钥密文信息是用应用管理密钥对以下数据加密（按所列顺序）产生的：

——密钥用途（参见《中国移动一卡通业务安全技术规范-密钥与算法要求》）

——密钥版本

——密钥算法标识（参见《中国移动一卡通业务安全技术规范-密钥与算法要求》）

——密钥值

MAC是用应用管理密钥对下述数据进行MAC计算（按所列顺序）产生的：

——CLA

——INS

——P1

——P2

——Lc

——密钥密文信息

加密和MAC计算的方法参见《中国移动一卡通业务安全技术规范-密钥与算法要求》。

装载8字节的单长度密钥时，数据长度为14h；装载16字节的双长度密钥时，数据长度为1Ch。

附录 E.1.4 响应报文数据域

响应报文数据域不存在。

附录 E.1.5 状态码

执行成功返回9000h。表E-2为错误状态码：

表E-2 WRITE KEY 命令状态码

SW1	SW2	含义
65	81	内存失败
67	00	长度错误
69	81	命令与文件结构不相容，当前文件非所需文件
69	82	操作条件不满足
69	84	随机数无效
69	85	使用条件不满足（应用被锁定）
69	86	不满足命令执行条件，当前文件不是EF
69	87	MAC丢失
69	88	MAC不正确
6A	81	应用锁定
6A	84	文件空间不够
6A	86	P1或P2不正确
6D	00	INS不正确
6E	00	CLA不正确
93	03	应用被永久锁定
94	03	未找到相应的密钥