新莞人识别卡片技术规范

1 数据元

持卡人 ID 认证应用 AID: 5041592E535A66

公共应用基本数据文件

文件标识(SFI)		0x15
文件类型		二进制文件(TEF)
文件大小		30
文件存取控制	读=自由	改写=需要安全信息
字段	数据元	长度
1	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
文件标识(SFI)		‘24’ (十进制)
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

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 APDU 命令

2.1 支持的命令

(U)SIM卡支持命令如下：

- Select（应用选择）
- Read Binary（读取文件）
- Update Binary（更新文件）
- Get Challenge (获取随机数)
- Write Key（写密钥）

2.1 选择文件（SELECT）

2.1.1 定义和范围

SELECT命令通过文件名或AID来选择IC卡中的PSE、DDF或ADF。命令执行成功后，PSE、DDF或ADF的路径被设定。后续的APDU命令将采用SFI方式联系到所选定的PSE、DDF或ADF。

来自IC卡的响应报文应由回送的FCI组成。

2.1.2 命令报文

SELECT命令报文见表2-1：

表2-1 SELECT命令报文

代码	值
CLA	00h
INS	A4h
P1	引用控制参数（见表2-2）
P2	00h：第一个或仅有一个 02h：下一个（注：必须先使用00h，才能使用02h）
L_c	05h～10h
Data	文件名
L_e	00h

表2-2 SELECT命令引用控制参数P1

b8	b7	b6	b5	b4	b3	b2	b1	含义
0	0	0	0	0				
					1 0			通过AID选择 通过FID选择EF
						0	0	

2.1.3 命令报文数据域

命令报文数据域应包括所选择的PSE、DDF或ADF的名称或AID。

2.1.4 响应报文数据域

响应报文数据域应包括所选择PSE、DDF或ADF的FCI

表2-3定义了成功选择PSE后回送的FCI：

表2-3 SELECT PSE的响应报文（FCI）

标志	值	存在方式
'6F'	FCI模板	M
'84'	DF名	M
'A5'	FCI专用数据	M
'88'	目录基本文件的SFI	M
'9F0C'	发卡方自定义数据的FCI（见表6-4）	M

表2-5定义了成功选择DDF后回送的FCI：

表2-5 SELECT DDF的响应报文（FCI）

标志	值	存在方式
'6F'	FCI模板	M
'84'	DF名	M
'A5'	FCI专用数据	M
'88'	目录基本文件的SFI	M

表2-6定义了成功选择ADF后回送的FCI：

表2-6 SELECT ADF的响应报文（FCI）

标志	值	存在方式
'6F'	FCI模板	M
'84'	DF名	M
'A5'	FCI专用数据	M
'9F0C'	发卡方自定义数据的FCI	O

表2-7定义了SELECT ADF的响应报文中的发卡方自定义数据的FCI内容（ADF下的SFI为23的文件内容）：

表2-7 SELECT ADF的应答报文中的FCI数据专用模版

'A5'	FCI数据专用模板		M
	‘50’	应用标签	O
	‘87’	应用优先指示符	O
	‘9F08’	应用版本号	M
	‘9F12’	应用优先名称	O

2.1.5 状态码

执行成功返回9000h。表6-8为错误状态码：

表6-8 SELECT命令状态码

SW1	SW2	含义
‘62’	‘83’	选中的文件无效
‘62’	‘84’	FCI格式与P2指定不符
‘64’	‘00’	标志状态位没变
‘67’	‘00’	长度错误
‘6A’	‘81’	应用锁定
‘6A’	‘82’	该文件未找到
‘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
‘61’	‘xx’	需发出GET RESPONSE命令

2.2 取随机数（GET CHALLENGE）

2.2.1 定义和范围

GET CHALLENGE命令用于从IC卡中获得一个长度为4字节的随机数。该随机数用于后续指令，该随机数有效期一直到IC卡接收到另外一条GET CHALLENGE命令。

2.2.2 命令报文

GET CHALLENGE命令报文见表6-25：

表6-25 GET CHALLENGE命令报文

代码	值
CLA	00h
INS	84h
P1	00h
P2	00h
L_c	不存在
Data	不存在
L_e	04h

2.2.3 命令报文数据域

命令报文数据域不存在。

2.2.4 响应报文数据域

IC卡产生的随机数，长度为4字节。

2.2.5 状态码

执行成功返回9000h。表6-26为错误状态码：

表6-26 GET CHALLENGE 命令状态码

SW1	SW2	含义
67	00	长度错误（L_c为空）
6A	81	不支持此功能，应用被锁定
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

2.4 读二进制文件（READ BINARY）

2.4.1 定义和范围

READ BINARY命令用于读取二进制文件的内容（或部分内容）。

2.4.2 命令报文

READ BINARY命令报文见表6-15：

表2-15 READ BINARY命令报文

代码	值
CLA	00h或04h
INS	B0h
P1	见说明
P2	从文件中读取的第一个字节的偏移地址
L_c	不存在: (CLA=’04’时除外)
Data	不存在: (CLA=’04’时，应包括MAC)
L_e	期望返回数据的长度

说明：

若P1的高三位为100，则低5位为短的文件标识符，P2为读的偏移量。

若P1的最高位不为1，则P1 P2为欲读文件的偏移量，所读的文件为当前文件。

2.4.3 命令报文数据域

当使用安全报文时，命令报文数据域中应包含MAC。MAC的计算方法和长度由应用决定。

2.4.4 响应报文数据域

该文件被置成线路保护时，若CLA置为00时响应报文不含MAC，CLA置为04时响应报文包含MAC。

2.4.5 状态码

执行成功返回9000h。表6-17为错误状态码：

表6-17 READ BINARY命令状态码

SW1	SW2	含义
62	81	回送的数据可能有错
62	82	文件长度小于L_e
67	00	长度错误
68	82	不支持安全报文
69	00	不能处理
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	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
6A	81	不支持此功能，应用暂时被锁定
6A	82	该文件未找到
6A	86	P1或P2不正确
6B	00	参数错误（偏移量超出EF）
6C	xx	L_e长度错误，实际长度是xx
6D	00	INS 不正确
6E	00	CLA不正确
93	03	应用被永久锁定

2.5 写二进制文件（UPDATE BINARY）

2.6.1 定义和范围

UPDATE BINARY命令用命令APDU中给定的数据修改EF文件中已有的数据。

2.6.2 命令报文

UPDATE BINARY命令报文见表6-18：

表6-18 UPDATE BINARY命令报文

代码	值
CLA	00h或04h
INS	D6h

P1	见说明
P2	要修改的第一个字节的偏移地址
L_c	后续数据域的长度
Data	修改用的数据
L_e	不存在

说明：
若P1的高三位为100，则低5位为短的二进制文件标识符，P2为欲写文件的偏移量。
若P1的最高位不为1，则P1 P2为欲写文件的偏移量，所写的文件为当前文件。
Lc 表示要写入的字节数。

2.6.3 命令报文数据域

命令报文数据域包括更新原有数据的新数据。使用安全报文时，命令报文的数据域中应包括MAC。MAC是由IC卡维护密钥或应用维护密钥对更新原有数据的新数据计算而得到的。

2.6.4 响应报文数据域

响应报文数据域不存在。

2.6.5 状态码

执行成功返回9000h。表6-20为错误状态码：

表6-20 UPDATE BINARY 命令状态码

SW1	SW2	含义
64	00	标志状态位没变
65	81	内存失败
67	00	长度错误（L_c为空）
69	00	不能处理
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	82	该文件未找到
6A	83	记录未找到
6A	86	P1或P2不正确
6B	00	参数错误（偏移量超出EF）
6D	00	INS不正确

6E	00	CLA不正确
93	03	应用被永久锁定

2.7 WRITE KEY 命令

2.7.1 定义和范围

WRITE KEY 命令可向(U)SIM 卡中装载（第一次写入）密钥或更新(U)SIM 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，在主控密钥（卡片主控密钥或应用主控密钥）的控制下进行。

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

2.7.2 命令报文

WRITE KEY 命令报文编码见表 7-64：

表 7-64 WRITE KEY 命令报文

代码	值
CLA	84h
INS	D4h
P1	00
P2	00h
Lc	1Ch
Data	密钥密文信息||MAC
Le	不存在

2.7.3 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。

密钥密文信息是用主控密钥的会话密钥对以下数据加密（按所列顺序）产生的：

——密钥标识

——密钥版本

——密钥索引号

——密钥算法标识

——密钥值

MAC 是用主控密钥的会话密钥对下数据进行 MAC 计算（按所列顺序）产生的：

——CLA

——INS

——P1

——P2

——Lc

——密钥密文信息

此命令的加密和 MAC 使用的会话密钥：
输入参数：
——应用主控密钥（Key 保护密钥）
——随机数（用 Get Challenge 获得的 4 字节随机数，后缀以 0x80 0x00 0x00 0x00）
输出数据：
——8 字节的应用主控会话密钥

对于密钥更新必须用应用主控密钥（Key 保护密钥），来计算命令的加密和 MAC。

加密和 MAC 的计算的方法参见《中国金融集成电路（IC）卡电子钱包存折规范 v2.0--卡片部分》8.3 节。

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。

写主控密钥时，用旧的主控密钥加密新主控密钥并算 MAC，其它密钥用更新后的主控密钥做加密和 MAC 运算。

密钥标识

各密钥用途长度为1字节。密钥标识约定如下表所示：

密钥标识								含义
B8	b7	b6	b5	b4	b3	b2	b1	
0	0	0	0	0	0	0	1	0x01—应用主控密钥
0	0	0	0	0	0	1	0	0x02—应用维护密钥

密钥使用详解

	会话密钥计算	MAC 初始向量	MAC 算法	加密算法
应用主控密钥	**A**	**C**	**E**	**G**
应用维护密钥	**B**	**D**	**F**	**H*(若需要)**

A：《中国金融集成电路（IC）卡电子钱包存折规范 v2.0-应用规范》附录 B3
B：不使用会话密钥
C：8 个字节长的初始值设定为 16 进制的’0x 00 00 00 00 00 00 00 00’
D：8 个字节长的初始值设定为 4 字节随机数后缀以’ 0x 00 00 00 00’
E：《中国金融集成电路（IC）卡电子钱包存折规范 v2.0-应用规范》附录 B4
F：《中国金融集成电路（IC）卡电子钱包存折规范 v2.0-卡片部分》8.3.2.4 双长度 DES Key 的 MAC 算法

G:《中国金融集成电路（IC）卡电子钱包存折规范 v2.0-卡片部分》8.3.3.3 使用单倍长 DES 密钥的数据加密

H:《中国金融集成电路（IC）卡电子钱包存折规范 v2.0-卡片部分》8.3.3.3 使用双长度 DES 密钥的数据加密