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--SAM卡部分

SAM Card Specification Supporting

E-card Pass Service

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

7. APDU 命令

命令APDU及响应APDU的格式符合ISO/IEC 7816-4。

7.1 选择文件（SELECT）

7.1.1 定义和范围

SELECT命令通过文件名或AID来选择SAM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SAM卡的响应报文应由回送的FCI组成。

7.1.2 命令报文

SELECT命令报文见表7-1：

表7-1 SELECT命令报文

代码	值
CLA	00h
INS	A4h
P1	引用控制参数（见表7-2）
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7-2 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			通过文件名选择
						0	0	

7.1.3 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。

7.1.4 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7-3定义了成功选择PSE后回送的FCI：

表7-3 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7-4）	M

表7-4定义了SELECT PSE的响应报文中的发卡方自定义数据的FCI内容（MF下的SFI为21、22的文件内容）：

表7-4 SELECT PSE的响应报文中的发卡方自定义数据的FCI

字节	数据元	长度
1-10	SAM序列号	10
11	SAM版本号	1
12	密钥卡类型	1
13	指令集版本（参见附录B）	1
14	发卡方自定义FCI数据	1
15-20	终端机编号	6

表7-5定义了成功选择DDF后回送的FCI：

表7-5 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7-6定义了成功选择ADF后回送的FCI：

表7-6 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7-7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7-7 SELECT ADF的响应报文中的发卡方自定义数据的FCI

字节	数据元	长度
1	交易密钥索引号	1
2-9	全国应用发行者标识	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

7.1.5 状态码

执行成功返回9000h。表7-8为错误状态码：

表7-8 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

7.2 读记录文件（READ RECORD）

7.2.1 定义和范围

READ RECORD命令用于读取记录文件中的内容。
SAM卡的响应由回送的记录数据组成。

7.2.2 命令报文

READ RECORD命令报文见表7-9：

表7-9 READ RECORD命令报文

代码	值
CLA	00h
INS	B2h
P1	记录的序号
P2	引用控制参数（见表7-10）
L_c	不存在；
Data	不存在；
L_e	00h

表7-10 READ RECORD命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	含义
X	X	X	X	X				SFI

					1	0	0	P1为记录的序号

7.2.3 命令报文数据域

命令报文数据域不存在。

7.2.4 响应报文数据域

所有执行成功的READ RECORD命令响应报文数据域由读取的记录组成。

7.2.5 状态码

执行成功返回9000h。表7-11为错误状态码：

表7-11 READ RECORD命令状态码

SW1	SW2	含义
62	81	回送的数据可能有错
67	00	长度错误
68	82	不支持安全报文
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，应用暂时锁定
6A	82	该文件未找到
6A	83	记录未找到
6A	86	P1或P2不正确
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
61	Xx	需发出GET RESPONSE命令

7.3 写记录文件（UPDATE RECORD）

7.3.1 定义和范围

UPDATE RECORD命令用命令APDU中给定的数据更改指定的记录。在使用当前记录地址时，该命令将在修改记录成功后重新设定记录指针。在使用安全报文更新记录时，若安全报文连续三次出错，则永久锁定SAM卡上当前应用。

7.3.2 命令报文

UPDATE RECORD命令报文见表7-12：

表7-12 UPDATE RECORD命令报文

代码	值
CLA	00h或04h
INS	DCh
P1	P1=00h：表示当前记录 P1≠00h：指定的记录号
P2	见表7-13
L_c	后续数据域长度
Data	输入数据
L_e	不存在

表7-13 UPDATE RECORD命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	含义
X	X	X	X	X				SFI
					0	0	0	第一个记录
					0	0	1	最后一个记录
					0	1	0	下一个记录
					0	1	1	上一个记录
					1	0	0	记录号在P1中给出
其余值								RFU

7.3.3 命令报文数据域

命令报文数据域由更新原有记录的新记录组成。使用安全报文时，命令报文的数据域中应包括MAC。MAC是由SAM卡维护密钥或应用维护密钥对更新原有记录的新记录计算而得到的。

7.3.4 响应报文数据域

响应报文数据域不存在。

7.3.5 状态码

执行成功返回9000h。表7-14为错误状态码：

表7-14 UPDATE RECORD 命令状态码

SW1	SW2	含义
64	00	标志状态位没变
65	81	内存失败
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
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

7.4 读二进制文件（READ BINARY）

7.4.1 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）。

7.4.2 命令报文

READ BINARY命令报文见表7-15：

表7-15 READ BINARY命令报文

代码	值
CLA	00h
INS	B0h
P1	见表7-16
P2	从文件中读取的第一个字节的偏移地址
L_c	不存在
Data	不存在
L_e	00

表7-16 READ BINARY命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	含义
X								读取模式： －1：用SFI方式，b5~b1标明SFI； －0：对选定的EF进行操作，需要先选定某个EF
	0	0						RFU（如果b8＝1）
			X	X	X	X	X	SFI（取值范围21－30）

7.4.3 命令报文数据域

命令报文数据域不存在。

7.4.4 响应报文数据域

当L_e的值为0时，只要文件的最大长度在255（短长度）或65535（扩展长度）之内，则其全部字节将被读出。

7.4.5 状态码

执行成功返回9000h。表7-17为错误状态码：

表7-17 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

7.5 写二进制文件（UPDATE BINARY）

7.5.1 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。

7.5.2 命令报文

UPDATE BINARY命令报文见表7-18：

表7-18 UPDATE BINARY命令报文

代码	值
CLA	00h或04h
INS	D6h
P1	见表7-19
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

表7-19 UPDATE BINARY命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	含义
X								读取模式： －1：用SFI方式，b5~b1标明SFI； －0：对选定的EF进行操作，需要先选定某个EF
	0	0						RFU（如果b8＝1）
			X	X	X	X	X	SFI（取值范围21－30）

7.5.3 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SAM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。

7.5.4 响应报文数据域

响应报文数据域不存在。

7.5.5 状态码

执行成功返回9000h。表7-20为错误状态码：

表7-20 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

7.6 外部认证（EXTERNAL AUTHENTICATION）

7.6.1 定义和范围

EXTERNAL AUTHENTICATION命令用于实现SAM卡外部安全认证。计算的方法是利用SAM卡中的SAM卡主控密钥或应用主控密钥，对SAM卡产生的随机数（使用GET CHALLENGE命令）和接口设备传输进来的认证数据进行验证。在使用外部认证命令时，若连续三次出错，则无法使用同该密钥相关的命令。

7.6.2 命令报文

EXTERNAL AUTHENTICATION命令报文见表7-21：

表7-21 EXTERNAL AUTHENTICATION命令报文

代码	值
CLA	00h
INS	82h
P1	00h
P2	00h
L_c	08h
Data	发卡方认证数据
L_e	不存在

7.6.3 命令报文数据域

命令报文数据域中包含8字节的加密数据，该数据是用主控密钥对此命令前一条命令“GET CHALLENGE”命令获得的随机数后缀“00 00 00 00”之后做3DES加密运算产生的。

7.6.4 响应报文数据域

响应报文数据域不存在。

7.6.5 状态码

执行成功返回9000h。表7-22为错误状态码：

表7-22 EXTERNAL AUTHENTICATION命令状态码

SW1	SW2	含义
63	00	外部认证失败
64	00	标志状态位没变
67	00	长度错误（L_c为空）
69	83	认证方法锁定
69	84	随机数无效
69	85	使用条件不满足（应用被锁定）
6A	81	不支持此功能
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

7.7 取响应数据（GET RESPONSE）

7.7.1 定义和范围

当APDU不能用现有协议传输时，GET RESPONSE命令提供了一种从SAM卡向接口设备传送APDU（或APDU的一部分）的传输方法。

7.7.2 命令报文

GET RESPONSE命令报文见表7-23：

表7-23 GET RESPONSE命令报文

代码	值
CLA	00h
INS	C0h
P1	00h
P2	00h
L_c	不存在
Data	不存在
L_e	期望数据的最大长度

7.7.3 命令报文数据域

命令报文数据域不存在。

7.7.4 响应报文数据域

响应报文数据域的长度由L_e的值决定。如果L_e的值为0，在后续数据有效时，SAM卡必须回送状态码‘6Cxx’，否则‘6F00’。

7.7.5 状态码

执行成功返回9000h。表7-24为错误状态码：

表7-24 GET RESPONSE 命令状态码

SW1	SW2	含义
62	81	回送的数据可能有错
67	00	长度错误（L_e为空）
6A	81	不支持此功能，应用被锁定
6A	86	P1或P2不正确
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
6F	00	数据无效

7.8 取随机数（GET CHALLENGE）

7.8.1 定义和范围

GET CHALLENGE命令用于从SAM卡中获得一个长度为4字节的随机数。该随机数服务于安全过程（安全报文、外部认证），下一个命令必须使用该随机数，否则该随机数失效。

7.8.2 命令报文

GET CHALLENGE命令报文见表7-25：

表7-25 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

7.8.3 命令报文数据域

命令报文数据域不存在。

7.8.4 响应报文数据域

SAM卡产生的随机数，长度为4字节。

7.8.5 状态码

执行成功返回9000h。表7-26为错误状态码：

表7-26 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

7.9 写入密钥（WRITE KEY）

7.9.1 定义和范围

WRITE KEY命令可向卡中装载（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，在主控密钥（SAM卡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SAM卡取一个4字节的随机数。

7.9.2 命令报文

WRITE KEY命令报文见表7-27：

表7-27 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

7.9.3 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是用主控密钥对下数据进行MAC计算（按所列顺序）产生的：

——CLA

——INS

——P1

——P2

——L_c

——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。

7.9.4 响应报文数据域

响应报文数据域不存在。

7.9.5 状态码

执行成功返回9000h。表7-28为错误状态码：

表7-28 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

7.10 通用 DES 计算初始化（INIT_FOR_DES_CRYPT）

7.10.1 定义和范围

INIT_FOR_DES_CRYPT命令用来初始化通用密钥计算过程。SAM卡将利用卡中指定的密钥进行运算，产生一个临时密钥。运算方式由指定的密钥类型、密钥分散级数和密钥算法标识确定。

不支持计算临时密钥的密钥类型有：

——主控密钥

——SAM卡维护密钥

双长度密钥产生双长度临时密钥的密钥类型有：

——应用维护密钥

指定密钥经过几级处理由密钥分散级数和Lc确定，若二者不一致，则返回错误信息。

临时密钥在SAM卡下电后自动消失，任何时候都不允许读。

临时密钥产生后，与原密钥的属性一致。

7.10.2 命令报文

INIT_FOR_DES_CRYPT命令报文见表7-29：

表7-29 INIT_FOR_DES_CRYPT命令报文

代码	值
CLA	80h
INS	1Ah
P1	密钥用途
P2	密钥版本
L_c	待处理数据的长度
Data	待处理的数据
L_e	无

7.10.3 命令报文数据域

命令报文数据域包括待处理的输入数据。数据长度为8的整数倍，长度也可以为0。密钥类型取密钥用途的低5位，密钥分散级数取密钥用途的高3位。（参见《中国移动一卡通业务安全技术规范-密钥与算法要求》）

如待处理的输入数据包括多级的分散因子，按最后一次分散因子在前、最先一次分散因子在后的顺序输入。

7.10.4 响应报文数据域

响应报文数据域不存在。

7.10.5 状态码

执行成功返回9000h。表7-30为错误状态码：

表7-30 INITIALIZE_FOR_DES_CRYPT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
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	80	数据参数不正确（如：密钥分散级数与分散数不符）
6A	81	应用锁定
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

7.11 通用 DES 计算（DES_CRYPT）

7.11.1 定义和范围

DES_CRYPT命令利用指定的密钥来进行运算。若一条命令无法传输所有的待处理数据，可分几条命令输入。

加密计算采用ECB模式，数据的填充在SAM卡外进行，SAM卡只支持长度为8的整数倍数据的加密。

MAC计算方法参见《中国移动一卡通业务安全技术规范-密钥与算法要求》，数据的填充在SAM卡外面进行，SAM卡只支持长度为8的整数倍数据的MAC计算。

DES_CRYPT命令必须在INIT_FOR_DES_CRYPT命令成功执行后才能进行。SAM卡状态在执行无后续块计算后，复原为通用DES计算初始化执行前的状态。

7.11.2 命令报文

DES_CRYPT命令报文见表7-31：

表7-31 DES_CRYPT命令报文

代码	值
CLA	80h
INS	FAh

P1	见表7-32
P2	00h
L_c	要加密的数据长度
Data	要加密的数据
L_e	不存在

表7-32 DES_CRYPT命令引用控制参数

b8	b7	b6	b5	b4	b3	b2	b1	含义
							X	计算模式 ——0，加密 ——1，MAC计算
						X		后续块 ——0，无后续块 ——1，有后续块
					X			初始值（仅对MAC计算有效） ——0，无初始值 ——1，有初始值

P1值计算模式如下：

——0，无后续块加密

——1，最后一块MAC计算

——2，有后续块加密

——3，下一块MAC计算

——5，唯一一块MAC计算

——7，第一块MAC计算

——其他，保留

7.11.3 命令报文数据域

命令报文数据域包括要加密的数据。加密数据的长度为8的整数倍。在P1的b3位为1时，待处理数据的前8个字节作为MAC计算的初始值。

7.11.4 响应报文数据域

在P1的b1位为0时，响应报文数据域包括加密结果，数据长度是8的整数倍。

在P1的b1位为1时，且P1的b2位为0时，响应报文数据域包括4字节的MAC。

7.11.5 状态码

执行成功返回9000h。表7-33为错误状态码：

表7-33 DES_CRYPT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
69	01	命令不接受（无效状态）
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	应用锁定
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

7.12 应用解锁（APPLICATION UNBLOCK）

7.12.1 定义和范围

APPLICATION UNBLOCK命令用于恢复当前应用。当命令成功完成后，对应用访问的限制将被取消，利用XX密钥校验MAC2的错误计数器将被重置。如果应用解锁连续失败三次，将永久锁定SAM卡上的该应用。

在APPLICATION UNBLOCK命令执行前必须执行GET CHANLLENGE命令取得4字节的随机数。

7.12.2 命令报文

APPLICATION UNBLOCK命令报文见表7-34：

表7-34 APPLICATION UNBLOCK命令报文

代码	值
CLA	84h
INS	18h
P1	00
P2	00
Lc	数据字节数
Data	报文鉴别代码数据元
Le	不存在

7.12.3 命令报文数据域

命令报文数据域包括报文鉴别代码，由应用维护密钥对以下数据（按所列顺序）进行MAC计算而得到的：

—CLA

—INS

—P1

—P2

—L_c

MAC计算的方式参见《中国移动一卡通业务安全技术规范-密钥与算法要求》。

7.12.4 响应报文数据域

响应报文数据域不存在。

7.12.5 状态码

执行成功返回9000h。表7-35为错误状态码：

表7-35 APPLICATION UNBLOCK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
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	87	MAC丢失
69	88	MAC不正确
6A	81	应用锁定
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

7.13 消费交易 MAC1 计算（INIT_SAM_FOR_PURCHASE）

7.13.1 定义和范围

INIT_SAM_FOR_PURCHASE命令利用过程密钥对交易信息进行加密计算得到MAC1，过程密钥的生成过程参见《中国移动一卡通业务安全技术规范-密钥与算法要求》。

7.13.2 命令报文

INIT_SAM_FOR_PURCHASE命令报文见表7-36：

表7-36 INIT_SAM_FOR_PURCHASE命令报文

代码	值
CLA	80h
INS	70h
P1	00h

P2	00h
Lc	14h＋8×N（N＝1，2，3）（N：分散次数，此处表明送入分散因子）
Data	要处理的数据
Le	08

7.13.3 命令报文数据域

命令报文数据域包括的数据以下列顺序排列：

- RFID-SIM卡随机数，4字节
- RFID-SIM卡交易序号，2字节
- 交易金额，4字节
- 交易类型标识，1字节
- 交易日期（终端），4字节
- 交易时间（终端），3字节
- 消费密钥版本号，1字节
- 消费密钥算法标识，1字节
- 分散因子，8或16字节

7.13.4 响应报文数据域

响应报文数据域包括以下数据（按顺序返回）：

—4字节的终端脱机交易序号

—4字节的MAC1

7.13.5 状态码

执行成功返回9000h。表7-37为错误状态码：

表7-37 INIT_SAM_FOR_PURCHASE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
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	88	MAC不正确
6A	80	数据参数不正确
6A	86	P1或P2不正确
6A	88	引用数据未找到
6D	00	INS不正确
6E	00	CLA不正确
93	03	应用被永久锁定
94	03	密钥版本不支持

61	Xx	需发出GET RESPONSE命令

7.14 消费交易校验 MAC2（CREDIT_SAM_FOR_PURCHASE）

7.14.1 定义和范围

CREDIT_SAM_FOR_PURCHASE命令利用INIT_SAM_FOR_PURCHASE命令产生的过程密钥SESPKP校验MAC2，过程如下所示：

- 检查MAC2尝试计数器，如MAC2未被锁定，SAM在其内部用SESPK对交易金额加密得到MAC2，与命令报文中的数据进行比较；
- 若命令执行成功，SAM卡将应用中的终端脱机交易序号加1；
- 如命令执行不成功，SAM卡将MAC2尝试计数器减1，并回送状态码'63Cx'，这里'x'是MAC2尝试计数器的新值；
- 如果'x'为零，SAM卡将锁定密钥所在的ADF。

在此过程中，所有的中间结果只保留在SAM卡内部，外界无法得到。

CREDIT_SAM_FOR_PURCHASE命令必须在INIT_SAM_FOR_PURCHASE命令成功执行后才能进行。

若MAC2尝试计数器为0的话，密钥所在的应用将被锁定，只能在应用维护密钥的控制下应用解锁后使用。

应用下的MAC2错误计数器在应用下所有密钥MAC2校验错误的情况下都要被减1。

SAM卡的状态在命令执行后将复原为MAC1校验前的状态。

7.14.2 命令报文

CREDIT_SAM_FOR_PURCHASE命令报文见表7-38：

表7-38 CREDIT_SAM_FOR_PURCHASE命令报文

代码	值
CLA	80h
INS	72h
P1	00h
P2	00h
Lc	04h
Data	MAC2
Le	不存在

7.14.3 命令报文数据域

命令报文数据域包括4字节的MAC2。

7.14.4 响应报文数据域

响应报文数据域不存在。

7.14.5 状态码

执行成功返回9000h。表7-39为错误状态码：

表7-39 CREDIT_SAM_FOR_PURCHAS命令状态码

SW1	SW2	含义
63	Cx	命令执行失败，x表示MAC2尝试计数器的新值
64	00	标志状态位没变
65	81	内存失败
67	00	长度错误
69	01	命令不接受（无效状态）
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
69	87	MAC2丢失
69	88	MAC2不正确
6A	80	数据参数不正确
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

7.15 身份校验类交易 MAC1 计算（INIT_SAM_FOR_IDENTIFY）

7.15.1 定义和范围

INIT_SAM_FOR_IDENTIFY命令利用过程密钥对交易信息进行加密计算得到MAC1，过程密钥的生成过程参见《中国移动一卡通业务安全技术规范-密钥与算法要求》。

7.15.2 命令报文

INIT_SAM_FOR_IDENTIFY命令报文见表7-40：

表7-40 INIT_SAM_FOR_IDENTIFY命令报文

代码	值
CLA	80h
INS	74h
P1	00h
P2	00h
Lc	10h＋8×N（N＝0，1，2，3）（N：分散次数，此处表明送入分散因子）
Data	待处理的数据
Le	08

7.15.3 命令报文数据域

命令报文数据域包括的数据以下述顺序排列：

- GET SUB_APPLICATION DATA命令CLA字段，1字节，84h；
- GET SUB_APPLICATION DATA命令INS字段，1字节，57h；
- GET SUB_APPLICATION DATA命令P1字段，1字节，00h；
- GET SUB_APPLICATION DATA命令P2字段，1字节，00h；
- GET SUB_APPLICATION DATA命令Lc字段，1字节，0Ah；
- 企业ID，6字节；
- 子应用索引号，1字节
- 随机数（RFID-SIM卡）RAND1，4字节
- 分散因子，（长度参见Lc的取值）

7.15.4 响应报文数据域

响应报文数据域包括以下数据（按顺序返回）：

—4字节的SAM卡随机数RAND2

—4字节的MAC1（注：MAC1的计算：1）子密钥根据SAM卡存储的根密钥对传入的分散因子计算得到；2）会话密钥根据子密钥对RAND1‖RAND2计算得到；3）利用会话密钥对命令报文数据域中“GET SUB_APPLICATION DATA命令CLA字段”到“子应用索引号”计算得到MAC1）。

7.15.5 状态码

执行成功返回9000h。表7-41为错误状态码：

表7-41 INIT_SAM_FOR_IDENTIFY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
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	88	MAC不正确
6A	80	数据参数不正确
6A	86	P1或P2不正确
6A	88	引用数据未找到
6D	00	INS不正确
6E	00	CLA不正确
93	03	应用被永久锁定
94	03	密钥版本不支持
61	Xx	需发出GET RESPONSE命令

7.16 身份校验类交易校验 MAC2（CREDIT_SAM_FOR_IDENTIFY）

7.16.1 定义和范围

CREDIT_SAM_FOR_IDENTIFY命令利用INIT_SAM_FOR_IDENTIFY命令产生的过程密钥SESPKP校验MAC2，过程如下所示：

- 检查MAC2尝试计数器，如MAC2未被锁定，SAM在其内部用SESPK对命令报文数据域中MAC2之前的数据（企业ID、员工ID、员工企业流水号、子应用索引号、子应用有效期、子应用类型、子应用锁定标识）及RAND2计算得到，与命令报文中的数据进行比较；
- 若命令执行成功，SAM卡返回9000；
- 如命令执行不成功，SAM卡将MAC2尝试计数器减1，并回送状态码’63Cx’，这里’x’是MAC2尝试计数器的新值；
- 如果’x’为零，SAM卡将锁定密钥所在的ADF。

在此过程中，所有的中间结果只保留在SAM卡内部，外界无法得到。

CREDIT_SAM_FOR_IDENTIFY命令必须在INIT_SAM_FOR_IDENTIFY命令成功执行后才能进行。

若MAC2尝试计数器为0的话，密钥所在的应用将被锁定，只能在应用维护密钥的控制下应用解锁后使用。

应用下的MAC2错误计数器在应用下所有密钥MAC2校验错误的情况下都要被减1。

SAM卡的状态在命令执行后将复原为MAC1校验前的状态。

7.16.2 命令报文

CREDIT_SAM_FOR_IDENTIFY命令报文见表7-42：

表7-42 CREDIT_SAM_FOR_IDENTIFY命令报文

代码	值
CLA	80h
INS	76h
P1	00h
P2	00h
Lc	29h
Data	MAC2
Le	不存在

7.16.3 命令报文数据域

命令报文数据域包括的数据以下述顺序排列：

- 企业ID，6字节
- 员工ID，20字节
- 员工企业流水号，4字节
- 子应用索引号，1字节

- 子应用有效期，4字节
- 子应用类型，1字节
- 子应用锁定标识，1字节
- MAC2，4字节

7.16.4 响应报文数据域

响应报文数据域不存在。

7.16.5 状态码

执行成功返回9000h。表7-43为错误状态码：

表7-43 CREDIT_SAM_FOR_IDENTIFY命令状态码

SW1	SW2	含义
63	Cx	命令执行失败，x表示MAC2尝试计数器的新值
64	00	标志状态位没变
65	81	内存失败
67	00	长度错误
69	01	命令不接受（无效状态）
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
69	87	MAC2丢失
69	88	MAC2不正确
6A	80	数据参数不正确
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

7.17 脱机消费撤销交易（OFFLINE_CANCEL）

7.17.1 定义和范围

OFFLINE_CANCEL命令利用过程密钥校验MAC1、生成MAC2，过程密钥的生成过程参见《中国移动一卡通业务接口规范--RFID-SIM卡与消费终端接口分册》、《中国移动一卡通业务安全技术规范-密钥与算法要求》。

7.17.2 命令报文

OFFLINE_CANCEL命令报文见表7-44：

表7-44 OFFLINE_CANCEL命令报文

代码	值
CLA	84h
INS	78h
P1	00h
P2	00h
Lc	1Bh＋8×N（N＝0，1，2，3）（N：分散次数，此处表明送入分散因子）
Data	待处理的数据
Le	08

7.17.3 命令报文数据域

命令报文数据域包括的数据以下述顺序排列：

- 钱包余额（或剩余使用次数），4字节
- 交易金额，4字节
- 钱包脱机交易序号，2字节
- 交易日期（终端），4字节
- 交易时间（终端），3字节
- 密钥版本号，1字节
- 算法标识，1字节
- 伪随机数（RFID-SIM卡），4字节
- MAC1，4字节（用于产生计算MAC1所需会话密钥的输入数据如下：伪随机数（RFID-SIM卡）||电子钱包脱机交易序号||'8000'；计算MAC1的数据如下：电子钱包余额、交易金额、交易类型标识（取值0x22）、终端机编号）
- 分散因子，长度参见Lc的取值

7.17.4 响应报文数据域

响应报文数据域包括以下数据（按顺序返回）：

—4字节的终端脱机交易序号

—4字节的MAC2（用于产生计算MAC2所需会话密钥同7.17.3节；计算MAC2的数据如下：交易金额、交易类型标识、终端机编号、交易日期 (终端)、交易时间 (终端)）。

7.17.5 状态码

执行成功返回9000h。表7-45为错误状态码：

表7-45 OFFLINE_CANCEL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
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	88	MAC不正确
6A	80	数据参数不正确
6A	86	P1或P2不正确
6A	88	引用数据未找到
6D	00	INS不正确
6E	00	CLA不正确
93	03	应用被永久锁定
94	03	密钥版本不支持
61	Xx	需发出GET RESPONSE命令

附录 A SAM 卡中的基本数据文件

附录 A.1 MF 下的 SAM 卡公共信息文件

表A-1 MF下的SAM卡公共信息文件

文件标识（SFI）		21（十进制）
文件类型		透明
文件大小		14字节
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	SAM序列号	10
11	SAM版本号	1
12	密钥卡类型	1
13	指令集版本（参见表9-4）	1
14	发卡方自定义FCI数据	1

附录 A.2 MF 下的终端信息文件

表A-2 MF下的终端信息文件

文件标识（SFI）		22（十进制）
文件类型		透明
文件大小		6字节
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

附录 A.3 应用的应用公共信息文件

表A-3 应用的应用公共信息文件

文件标识（SFI）		23（十进制）
文件类型		透明
文件大小		25字节
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	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

附录 B 指令集版本

为了在测试和以后对新增的整套交易的指令集实现继承和兼容，进行交易的终端需要从SAM卡上获得当前SAM卡上对这套指令集的版本的描述。

在现有的一卡通应用的FCI固定位置加入一个字节来描述新增的整套交易的指令集的版本。

表B-1 指令集版本字节的编码

b8	b7	b6	b5	b4	b3	b2	b1	含　　义
X	X	X	X					主版本号 （取值范围1~9,其它RFU）
				X	X	X	X	次版本号 1~9 - 测试版 F - 正式版 其它RFU

附录 C 一卡通应用 AID

一卡通应用的AID为D156000101800000000000100000000。