中 国 移 动 通 信 企 业 标 准

QB-XX-XXX-XXXX

中国移动一卡通业务安全技术规范-密钥母卡设备要求

Security Specification of Key Management Card for China Mobile 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

1 密钥母卡接口要求

1.1 基本接口

密钥母卡接口符合 ISO7816 规范，采用标准的 APDU 协议。

命令 APDU 格式：

命令 APDU 由 4 字节长的必备头后跟一个可变长的条件体组成，见下图：

CLA	INS	P1	P2	Lc	Data	Le
← 必备头 →				← 条件体 →		

命令 APDU 中发送的数据字节数用 Lc(命令数据域的长度)表示。

响应 APDU 中期望返回的数据字节数用 Le(期望数据长度)表示。在无法确定数据的长度的时候，可以将 Le 设为 00，代表将可能的数据全部返回。在 T=0 的协议中，可以按如下两种方式处理均可：

- 方式 1：如果后续数据有效，卡片返回 6CXX，然后需要以 XX 作为 Le 重新发送此命令；如果后续数据无效，则卡片应返回‘6F00’。
- 方式 2：卡片返回 61XX，然后执行 GetResponse 取后续数据

命令 APDU 报文的内容见下表：

命令 APDU 的内容

代码	描　　述	长度（字节数）
CLA	命令类别	1
INS	指令代码	1
P1	指令参数 1	1
P2	指令参数 2	1
Lc	命令数据域中存在的字节数	0 或 1
Data	命令发送的数据(长度=Lc)	可变
Le	响应数据域中期望的最大数据字节数	0 或 1

响应 APDU 格式

响应APDU格式由一个变长的条件体和后随两字节长的必备尾组成，见下图：

Data	SW1	SW2
← 条件体 →	← 必备尾 →	

响应 APDU 的内容

代码	描　　述	长度（字节数）
Data	响应中接收的数据位串(长度=Le)	变长

SW1	命令处理状态	1
SW2	命令处理限定	1

所有指令的响应状态字 SW1 SW2 = ‘90 00’ 或 ‘61 XX’均表示命令的成功执行。但由于可读性的需要，在整篇文章中这两种应答码只用了’90 00’作为参考。当响应状态字为‘61 XX’时，响应 APDU 的条件体为空，指令执行成功后的响应数据（长度为 XX）暂存在卡片内存当中，可以使用获取响应数据（Get Response）指令来取出响应数据。

1.1.1 校验密码（Verify PIN）

在执行大部分指令前均需要校验 PIN（在指令说明中提出了要求）。目前 PIN 的尝试次数是三次，连续输错三次 PIN 则 PIN 锁定，需要调用 PIN 重置的指令（见“充值密码”部分的说明），对 PIN 进行恢复。PIN 更改指令见“更改密码”部分的说明。

1) 命令报文

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

Verify PIN 命令报文见下表。

表 8-1-1 Verify PIN 命令报文

代码	值
CLA	F0h
INS	20h
P1	00h
P2	见 P2 说明
Lc	08h
Data	见命令报文数据域的说明
Le	不存在

2) P2 说明

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

P2 = 01 ， 主目录 PIN。

P2 = 02 ， 应用目录 PIN。

P2 = 03 ， 密钥导出 PIN（密钥导出至企业平台）。

3) 命令报文数据域

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

表 8-1-2 Verify PIN 命令报文数据域

字段	长度（字节）	说明
持卡人密码（PIN）	8	

4) 响应报文数据域

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

无。

5) 状态码

带格式的: 1 级, 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

执行成功返回 9000h。下表为错误状态码：

表 8-1-3 Verify PIN 命令报文数据域

SW1	SW2	含义
63	CX	PIN验证失败，还有X次机会重试
64	75	记录未找到
64	80	文件未找到
69	85	PIN文件锁定
6A	86	P1P2不正确

1.1.2　更改密码（Change PIN）

通过该指令可以更改密钥母卡的 PIN。

1) 命令报文

带格式的：编号 + 级别：1 + 编号样式：1，2，3，… + 起始编号：1 + 对齐方式：左侧 + 对齐位置： 0 厘米 + 制表符后于： 0 厘米 + 缩进位置： 0.74 厘米

Change PIN 命令报文见下表。

表 8-1-4　Change PIN 命令报文

代码	值
CLA	F0h
INS	24h
P1	00h
P2	见 P2 说明
Lc	10h
Data	见命令报文数据域的说明
Le	不存在

2) P2 说明

带格式的：编号 + 级别：1 + 编号样式：1，2，3，… + 起始编号：1 + 对齐方式：左侧 + 对齐位置： 0 厘米 + 制表符后于： 0 厘米 + 缩进位置： 0.74 厘米

P2 = 01 ， 主目录 PIN。
P2 = 02 ， 应用目录 PIN。
P2 = 03 ， 密钥导出 PIN（密钥导出至企业平台）。

3) 命令报文数据域

带格式的：编号 + 级别：1 + 编号样式：1，2，3，… + 起始编号：1 + 对齐方式：左侧 + 对齐位置： 0 厘米 + 制表符后于： 0 厘米 + 缩进位置： 0.74 厘米

表 8-1-5 Change PIN 命令报文数据域

字段	长度（字节）	说明
原持卡人密码（PIN）	8	目前卡内密码
欲更新的密码（PIN）	8	更改成功后，将以此作为密码进行校验

4) 响应报文数据域

带格式的：编号 + 级别：1 + 编号样式：1，2，3，… + 起始编号：1 + 对齐方式：左侧 + 对齐位置： 0 厘米 + 制表符后于： 0 厘米 + 缩进位置： 0.74 厘米

无。

5) 状态码

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

执行成功返回 9000h。下表为错误状态码：

表 8-1-6 Change PIN 指令状态码

SW1	SW2	含义
63	CX	原PIN验证失败，还有X次机会重试
64	75	记录未找到
64	80	文件未找到
69	85	PIN文件锁定
6A	86	P1P2不正确

1.1.3 重置密码（Reload PIN）

在 PIN 锁定后可以重新设置 PIN，这个需要对密钥母卡（母卡认证卡、工作母卡相同）进行最高级别主控密钥的外部认证。密钥母卡的 PIN 重置需要在发卡端完成，企业端仅凭母卡认证卡不能对密钥母卡进行 PIN 重置。

密钥母卡在执行重置密码操作时，必须首先对密钥母卡进行外部认证操作后才能获得此功能权限。外部认证需要采用密钥母卡或工作母卡的移动主控密钥，因此第二主控密钥的外部认证不能获得此权限。

1) 命令报文

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

Reload PIN 命令报文见下表。

表 8-1-7 Reload PIN 命令报文

代码	值
CLA	F0h
INS	26h
P1	00h
P2	见 P2 说明
Lc	08h
Data	见命令报文数据域的说明
Le	不存在

2) P2 说明

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

P2 = 01 ， 主目录 PIN。

P2 = 02 ， 应用目录 PIN。

P2 = 03 ， 密钥导出 PIN（密钥导出至企业平台）。

3) 命令报文数据域

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

表 8-1-8 Reload PIN 命令报文数据域

字段	长度（字节）	说明
新的持卡人密码（PIN）	8	重置成功后，使用此密码进行校验

4) 响应报文数据域

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

无。

5) 状态码

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

执行成功返回 9000h。下表为错误状态码：

表 8-1-9 Reload PIN 指令状态码

SW1	SW2	含义
64	75	记录未找到
64	80	文件未找到
6A	86	P1P2不正确
69	82	安全状态不满足

1.1.4 取随机数（Get Challenge）

1) 命令报文

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

Get Challenge 命令报文见下表。

表 8-1-10 Get Challenge 命令报文

代码	值
CLA	F0h
INS	84h
P1	00h
P2	00h
Lc	不存在
Data	不存在
Le	N

2) 命令报文数据域

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

无。

3) 响应报文数据域

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

表 8-1-11 Get Challenge 命令报文数据域

字段	长度（字节）	说明
随机数	4	密钥母卡产生的随机数

1.1.5 外部认证（External Authentication）

外部认证指令是向卡片中传递一个经过卡片中特定密钥（比如移动母卡主控密钥）加密的随机数（之前通过 GetChallenge 指令获取），卡片采用同样的密钥加密该随机数后与密文数据比对，实现对外部实体的验证。执行该指令前需要执行 GetChallenge 指令，中间不能间隔其它指令。

需要说明的是，外部认证数据为 8 字节，即采用指定密钥（比如移动母卡主控密钥）对 8 字节明文数据（4 字节随机数+4 字节填充位）加密得到的密文数据，加密过程无须在明文前增加长度字节。

1) 命令报文

External Authentication 命令报文见下表。

表 8-1-12 External Authentication 命令报文

代码	值
CLA	F0h
INS	82h
P1	00h
P2	见 P2 的说明
Lc	08h
Data	见命令报文数据域的说明
Le	不存在

2) P2 说明

- P2 = 00 ，对于母卡认证卡，采用母卡认证卡主控密钥进行外部认证
- P2 = 01 ，对于密钥母卡，采用移动母卡主控密钥进行外部认证（通过加密机）
- P2 = 02 ：
  - 对于密钥母卡，采用母卡主控密钥进行外部认证（通过母卡认证卡）
  - 对于工作母卡，采用工作母卡主控密钥进行外部认证（通过加密机）

3) 命令报文数据域

表 8-1-13 External Authentication 命令报文数据域

字段	长度（字节）	说明
认证数据	8	P2=00：由母卡认证卡主控密钥加密的认证数据 P2=01：由移动母卡主控密钥加密的认证数据 P2=02：由母卡主控密钥或工作母卡主控密钥加密的认证数据

4) 响应报文数据域

带格式的：编号 + 级别：1 + 编号样式：1, 2, 3, … + 起始编号：1 + 对齐方式：左侧 + 对齐位置：0 厘米 + 制表符后于：0 厘米 + 缩进位置：0.74 厘米

无。

5) 状态码

执行成功返回9000h。下表为错误状态码：

表8-1-14 External Authentication命令状态码

SW1	SW2	含义
63	00	外部认证失败，不能再重试
63	0x	认证失败，还有X次机会重试
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（未取随机数）
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

1.1.6 SELECT 命令

1.1.6.1 定义和范围

SELECT命令通过文件名或AID来选择密钥母卡中的DDF或ADF，命令执行成功后，DDF或ADF的路径被设定。

应用到AEF的后续命令将采用SFI方式联系到所选定的DDF或ADF。

来自密钥母卡的响应报文应由回送FCI组成。

说明，密钥母卡内采用单一目录结构，并且已经设置上电后默认选择该目录，因此在执行其它指令前无需发送此命令。但是为了辨别卡片的种类（终端密钥导入），需要执行这个命令，以便于根据选择后返回的FCI来分辨。

1.1.6.2 命令报文

SELECT命令报文编码见下表：

表8-1-15 SELECT命令报文

代码	值
CLA	‘F0’
INS	‘A4’
P1	引用控制参数（见后续表格）
P2	‘00’第一个或仅有一个 ‘02’下一个

Lc	‘05’-’10’
Data	文件名
Le	‘00’

命令报文中的引用控制参数参见下表：

表8-1-16 SELECT命令引用控制参数

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	

1.1.6.3　命令报文数据域

命令报文数据域应包括所选择的PSE名、DF名或AID。

1.1.6.4　响应报文数据域

响应报文中的数据域应该包括所选择的DDF或ADF的FCI。本标准不规定FCI中回送的附加标识。

下表定义了成功选择DDF后回送的FCI：

表8-1-17 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

下表定义了成功选择ADF后回送的FCI：

表8-1-18 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

下表定义了ADF回送的‘A5’中包含的数据，其中必须包含标签为’9F08’的应用版本号，其数值由中国移动负责定义和维护。

表8-1-19 SELECT ADF的应答报文中的FCI数据专用模板

‘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

下表定义了ADF 回送的‘9F0C’中包含的数据，成功地选择了一卡通应用后，密钥母卡回送应用必备的发卡方专用数据。

表8-1-20 发卡方自定义数据的FCI

9F0C	发卡方自定数据的FCI		
	预留 （为与用户卡指令兼容，将密钥母卡中不使用的字段改为预留）	25字节	M
	发卡方自定义FCI数据 （取值 0x000001：(U)SIM卡或普通IC卡； 0x000002：工作母卡 0x000003：母卡认证卡 0x000004：密钥母卡 其他值保留）	3字节	M

1.1.6.5 响应报文状态码

此命令执行成功的状态码是'9000'。

密钥母卡可能回送的警告状态码如下表所示：

表8-1-21 SELECT警告状态

SW1	SW2	含　义
'62'	'83'	选择的文件无效
'62'	'84'	FCI格式与P2指定的不符

密钥母卡可能回送的错误状态码如下表所示：

表8-1-22 SELECT错误状态

SW1	SW2	含　义
'64'	'00'	标识状态位没变
'67'	'00'	P1 P2与Lc不一致
'6A'	'81'	不支持此功能
'6A'	'82'	未找到文件
'6A'	'86'	参数P1 P2不正确
'6D'	'00'	INS不支持或错误
'6E'	'00'	CLA不支持或错误
'93'	'03'	应用永久锁定

注：SW1 SW2='6A82'用于表示当密钥母卡支持部分文件名选择时，没有与此部分文件名相匹配的文件。

1.1.7 获取响应数据（Get Response）

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

1) 命令报文

Get Response 命令报文见下表。

表 8-1-23 Get Response 命令报文

代码	值

CLA	00h
INS	C0h
P1	00h
P2	00h
Lc	不存在
Data	不存在
Le	根据要获取的数据长度

2) 响应报文数据域

响应报文数据域的长度由 L_e 的值决定。

指令成功执行后，响应数据如下：

表 8-1-24 Get Response 命令报文数据域

字段	长度（字节）	说明
上一条指令的响应数据	Le	可以将卡片内暂存的响应数据全部取出，也可以取出一部分靠前面的数据，其余的数据仍然暂存于卡片之中

3) 状态码

执行分为两种情况，响应数据全部取出后，执行成功返回9000h。响应数据取出一部分之后，执行成功返回‘61 xx’，‘xx’为取出一部分数据后，剩余还可以获取的数据长度。错误状态码如下表所示：

表8-1-25 Get Response命令状态码

SW1	SW2	含义
‘67’	‘00’	长度错误
‘6A’	‘86’	参数P1和P2不正确
‘6C’	‘XX’	长度错误，Le 不正确，超过了卡内实际数据长度，’ XX’表示可获取的最大实际长度
‘6D’	‘00’	INS不支持或错误
‘6E’	‘00’	CLA不支持或错误
‘6F’	‘00’	数据无效

1.2 密钥及信息管理接口

1.2.1 读取密钥属性

1.2.1.1 定义和范围

密钥母卡中密钥的属性包括：

- 密钥类型；
- 密钥版本；
- 密钥索引；
- 密钥算法标识：标识该密钥所采用的算法
- 密钥导入导出属性：密钥在导入/导出过程中需要采用的保护密钥信息等
- 密钥分散属性：标识密钥分散级数等属性
- 密钥状态：密钥是否可用的标志
- 密钥使用状态计数器：可以用于密钥使用的计数

该指令无需外部认证。

1.2.1.2 读取密钥属性（Read KeyInfo）

1) 命令报文

带格式的：编号 + 级别：1 + 编号样式：1，2，3，… + 起始编号：1 + 对齐方式：左侧 + 对齐位置：0 厘米 + 制表符后于：0 厘米 + 缩进位置：0.74 厘米

Read KeyInfo 命令报文见下表。

表 8-2-1 Read KeyInfo 命令报文

代码	值
CLA	00h
INS	B4h
P1	见 P1 说明
P2	00h
Lc	不存在
Data	不存在
Le	0Bh

2) P1 说明

带格式的：编号 + 级别：1 + 编号样式：1，2，3，… + 起始编号：1 + 对齐方式：左侧 + 对齐位置：0 厘米 + 制表符后于：0 厘米 + 缩进位置：0.74 厘米

P1 用于指示密钥的记录号，起始值为 01h，最大为 FFh。

3) 命令报文数据域

带格式的：编号 + 级别：1 + 编号样式：1，2，3，… + 起始编号：1 + 对齐方式：左侧 + 对齐位置：0 厘米 + 制表符后于：0 厘米 + 缩进位置：0.74 厘米

无。

4) 响应报文数据域

带格式的：编号 + 级别：1 + 编号样式：1，2，3，… + 起始编号：1 + 对齐方式：左侧 + 对齐位置：0 厘米 + 制表符后于：0 厘米 + 缩进位置：0.74 厘米

表 8-2-2 Read KeyInfo 响应报文数据域

字段	长度（字节）	说明
密钥类型	1	标识密钥的种类
密钥版本	1	密钥的版本号
密钥索引	1	密钥的索引号
密钥算法标识	1	密钥的算法标识（00 代表 3DES，其他保留）
密钥导入导出属性	1	前半字节为导入密钥索引号，后半字节为导出密钥索引号
密钥分散属性	1	前半字节为分散级数，后半字节为使用属性
密钥状态	1	表明密钥的使用状态（AA 代表可用）
密钥使用状态计数	4	第一位（BIT）为启用标志（1 表示启用），其他位为计数器值

1.2.1.3 状态码

如果状态码为 6B00，则表明已达到密钥文件最大的密钥记录数。

1.2.2 密钥生成

1.2.2.1 定义和范围

密钥生成命令用于由 IC 卡产生密钥。密钥母卡采用密钥产生初始化命令中指定的种子码单和密钥数量，通过算法产生所有的密钥值。根据命令中的密钥属性设定形成完整的密钥记录并存储在密钥母卡中。

密钥母卡在执行密钥生成操作时，必须首先需要对密钥母卡进行外部认证和校验密码操作后才能获得此功能权限。

密钥生成接口包括两条指令：

- INIT_FOR_GENERATE：用于发送密钥生成请求，包括密钥的数量和种子值，对于密钥生成操作（1 个或多个密钥），该指令只需要执行一次
- GENERATE KEY：该指令用于传递密钥属性信息，根据密钥数量，该指令需要执行多次，每次生成 1 个密钥

带格式的: 项目符号 + 级别: 2 + 对齐位置: 0.74 厘米 + 制表符后于: 0 厘米 + 缩进位置: 1.48 厘米

说明：

- 同样的码单，同样的密钥属性生成的密钥值相同
- 同样的密钥属性，在卡片中只有一个存储空间，如果生成新的密钥，则旧的密钥值将被覆盖。在判定密钥属性时，仅根据密钥类型、密钥索引、密钥版本、密钥算法标识，以上属性四个字节相同的密钥，即认为是同一条密钥

带格式的: 项目符号 + 级别: 1 + 对齐位置: 0.74 厘米 + 制表符后于: 0 厘米 + 缩进位置: 1.48 厘米

1.2.2.2　密钥产生初始化命令（INIT_FOR_GENERATE）

1)　命令报文

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

INIT_FOR_ GENERATE 命令报文见下表。

表 8-2-3　INIT_FOR_ GENERATE 命令报文

代码	值
CLA	80h
INS	E1h
P1	00h
P2	00h
Lc	11h
Data	见命令报文数据域的说明
Le	不存在

2)　命令报文数据域

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

表 8-2-4 INIT_FOR_ GENERATE 命令报文数据域

字段	长度（字节）	说明
密钥数量	1	需要产生的密钥总数量。
种子值	16	

3)　响应报文数据域

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

无。

4)　状态码

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

表 8-2-5 INIT_FOR_ GENERATE 指令状态码

错误码(SW)	含义
6700	数据长度不正确
6982	安全状态不满足
6A80	输入数据错误
6A86	P1、P2 不正确
6D00	指令的 INS 错误
6E00	指令的类型不支持
6F00	未知错误
9303	此应用已被锁定

1.2.2.3　密钥生成命令（Generate Key）

1)　命令报文

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

Generate Key 命令报文见下表。

表 8-2-6 Generate Key 命令报文

代码	值
CLA	80h
INS	E2h
P1	00h
P2	00h
Lc	0Bh
Data	见命令报文数据域的说明
Le	不存在

2) 命令报文数据域

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

表 8-2-7 Generate Key 命令报文数据域

字段	长度（字节）	说明
密钥类型	1	标识密钥的种类
密钥版本	1	密钥的版本号
密钥索引	1	密钥的索引号
密钥算法标识	1	密钥的算法标识（00 代表 3DES，其他保留）
密钥导入导出属性	1	前半字节为导入密钥索引号，后半字节为导出密钥索引号
密钥分散属性	1	前半字节为分散级数，后半字节为使用属性
密钥状态	1	表明密钥的使用状态（AA 代表可用）
密钥使用状态计数	4	第一位（BIT）为启用标志（1 表示启用），其他位为计数器值

表 8-2-8 密钥的使用属性说明

使用属性	意义
0	导出前不能分散，密钥可以进行计算
1	导出前必须分散，密钥可以进行计算
2	导出前可以分散，也可以不分散，可以计算
3	导出前不能分散，密钥不能进行计算
4	导出前必须分散，密钥不能进行计算
5	导出前可以分散，也可以不分散，不能计算

3) 响应报文数据域

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

无。

1.2.2.4 状态码

表 8-2-9 状态码

错误码(SW)	含义
6476	密钥类型错误
6484	密钥使用状态不满足
6700	数据长度不正确
6982	安全状态不满足
6985	指令使用状态不满足 （包括未调用 INIT_FOR_GENERATE 指令、INIT_FOR_GENERATE 指令中指定的密钥数量用完、生成密钥过程中途调用了其他指令等）
6A80	输入数据错误
6A84	文件空间不足
6A86	P1、P2 不正确
6D00	指令的 INS 错误
6E00	指令的类型不支持
6F00	未知错误
9303	此应用已被锁定

1.2.3 密钥-数据导出

1.2.3.1 定义和范围

密钥-数据导出命令可以按照要求将密钥母卡中的密钥以及输入的数据加密导出。该指令可以用于如下操作前的指令数据生成：

- 用户卡发卡：
  - 创建子应用：CREATE SUB_APPLICATION
  - 更新应用数据：UPDATE SUB_APPLICATION DATA
  - 更新应用密钥：UPDATE SUB_APPLICATION KEYS

  说明：由于密钥-数据导出指令只支持密文+MAC 输出，如果要求明文、密文混合输出，则需要采用密钥-数据导出指令和指令 MAC 计算指令相结合来满足要求。
- SAM 卡发卡：
  - SAM 卡更新密钥

带格式的：项目符号 + 级别：1 + 对齐位置： 0.74 厘米 + 制表符后于： 0 厘米 + 缩进位置： 1.48 厘米

带格式的：项目符号 + 级别：2 + 对齐位置： 1.48 厘米 + 制表符后于： 0 厘米 + 缩进位置： 2.22 厘米

带格式的：项目符号 + 级别：1 + 对齐位置： 0.74 厘米 + 制表符后于： 0 厘米 + 缩进位置： 1.48 厘米

带格式的：项目符号 + 级别：2 + 对齐位置： 1.48 厘米 + 制表符后于： 0 厘米 + 缩进位置： 2.22 厘米

密钥母卡在执行密钥-数据导出操作时，必须首先对密钥母卡进行外部认证和校验密码操作后才能获得此功能权限。权限范围如下：

外部认证密钥	导出密钥	被导出密钥
母卡主控密钥	不能为终端初始密钥	企业管理密钥和企业应用密钥

1.2.3.2 密钥-数据导出命令（Export Keys&Data）

1) 命令报文

Export Key 命令报文见下表。

表 8-2-10 Export Keys&Data 命令报文

代码	值
CLA	80h
INS	C2h
P1	见 P1 说明
P2	00h
Lc	根据命令报文数据域各字段长度计算得出
Data	见命令报文数据域说明
Le	不存在

2) P1 说明

P1 参数长度为 1 个字节，采用 P1 的 8 个 bit 分别定义如下属性：

- 导出密钥的分散因子长度
- 被导出密钥的分散因子长度
- 导出密钥的分散方式
- 被导出密钥的分散方式
- 导出密钥是否采用会话密钥
- MAC 算法

详细定义如下表所示：

b8	b7	b6	b5	b4	b3	b2	b1	含　义
x	x	x	x	x	x	x	0	导出密钥采用8字节分散因子
x	x	x	x	x	x	x	1	导出密钥采用16字节分散因子
x	x	x	x	x	x	0	x	密钥采用8字节分散因子
x	x	x	x	x	x	1	x	密钥采用16字节分散因子
x	x	x	x	0	0	x	x	导出密钥采用标准3DES方式分散
x	x	x	x	0	1	x	x	预留
x	x	0	0	x	x	x	x	密钥采用标准3DES方式分散
x	x	0	1	x	x	x	x	预留
x	0	x	x	x	x	x	x	导出密钥采用会话密钥
x	1	x	x	x	x	x	x	导出密钥不采用会话密钥
0	x	x	x	x	x	x	x	MAC采用9.19算法
1	x	x	x	x	x	x	x	MAC采用9.9算法

P1 参数的使用举例如下：

例如，为用户卡导出密钥，密钥和导出密钥都采用 8 字节分散因子，都采用标准 3DES 分散，使用会话密钥，9.19 算法计算 MAC，此时 P1=00h。

如果为 SAM 卡导出密钥，密钥采用 8 字节分散因子，采用标准 3DES 分散，导出密钥采用 16 字节分散因子，标准 3DES 分散，不采用会话密钥，9.19 算法计算 MAC，此时 P1=41h。

3) 命令报文数据域

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

表 8-2-11 Export Keys&Data 命令报文数据域

字段	长度（字节）	说明
用户卡密钥装载指令头（CIPP）	4	l 密钥导出后，在进行用户卡密钥装载时使用的 APDU 指令。 l 数据格式： 1. CLA ：1 字节 2. INS：1 字节 3. P1：1 字节 4. P2：1 字节
用户卡随机数	4	用于生成加密和 MAC 会话密钥
导出密钥的分散级数	1	导出密钥的分散级数
导出密钥的分散因子	分散级数×8（或分散级数*16）	导出密钥的分散因子数据，数据长度必须为 8 的倍数或 16 的倍数（只用于 SAM 卡的主控和维护密钥） *说明：* *1、多级分散因子的排列顺序按低字节向高字节依次排列（一级分散因子在最后，以下同）* *2、如果导出密钥的分散级数为 0， 则本字段不存在*
导出密钥的属性（版本/索引/类型）	3	l 导出密钥的属性。 l 数据格式： 1. 版本：1 字节 2. 索引：1 字节 3. 类型：1 字节
需要导出密钥个数	1	*本指令需要导出的密钥个数，如果需要导出多个密钥，则为每个密钥均需要提供下面的 5 个字段，如果该个数为 0，则不需要导出密钥，也不需要提供如下五个字段*
密钥分散级数	1	密钥分散级数
密钥分散因子（可选域）	分散级数×8	被导出密钥的分散因子数据，数据长度必须为 8 的倍数。 *如果被导出密钥的分散级数为 0， 则本字段不存在*
密钥属性（版本/索引/类型）	3	l 需要被导出的密钥属性。 l 数据格式： 1. 版本：1 字节 2. 索引：1 字节 3. 类型：1 字节
目标卡内密钥属性长度	1	密钥属性长度

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0.74 厘米 + 制表符后于: 0 厘米 + 缩进位置: 1.48 厘米

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0.74 厘米 + 制表符后于: 0 厘米 + 缩进位置: 1.48 厘米

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0.74 厘米 + 制表符后于: 0 厘米 + 缩进位置: 1.48 厘米

目标卡内密钥属性	N	密钥导入目标卡时，密钥组中每条密钥都有各自的属性，可能包括密钥标识、密钥版本、密钥索引、密钥算法标识等等，可在这个字段内指定。密钥母卡在进行密钥导出时，将这个密钥属性放在密钥值前面，形成密钥组进行加密
密钥前缀/后缀标志	1	是否存在前缀或后缀的标志： 0x00：不存在前缀和后缀 0x01：存在前缀 0x02：存在后缀 0x03：前缀后缀均存在
密钥组前缀长度	1	密钥组前缀长度 ***本字段当密钥前缀/后缀标志为 0x01 或 0x03 时存在。***
密钥组前缀数据	N	需要附加在被导出密钥组明文前的数据 ***本字段当密钥前缀/后缀标志为 0x01 或 0x03 时存在。***
密钥组后缀长度	1	密钥组后缀长度 ***本字段当密钥前缀/后缀标志为 0x02 或 0x03 时存在。***
密钥组后缀数据	N	需要附加在被导出密钥组明文后的数据 ***本字段当密钥前缀/后缀标志为 0x02 或 0x03 时存在。***

带格式的: 项目符号 + 级别: 1 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

4) 响应报文数据域

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

表 8-2-12 Export Keys&Data 响应报文数据域

字段	长度（字节）	说明
密文长度	1	
密钥密文	N	被导出密钥的密文数据，采用导出密钥对如下数据加密： 前缀 密钥组 后缀
MAC 码	4	MAC 码，对以下数据计算得出： ——CLA ——INS ——P1 ——P2 ——Lc ——密钥密文信息

带格式的: 项目符号 + 级别: 1 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

1.2.3.3 状态码

表 8-2-13 Export Keys&Data 状态码

错误代码	说明
6473	密钥的分散级数错误
6474	导出密钥不存在
6479	需要导出的密钥不存在
6476	密钥未找到
6484	密钥使用状态不满足
6700	数据长度不正确
6982	安全状态不满足
6A80	输入数据错误
6A86	P1、P2 不正确
9408	文件类型不匹配

1.2.4 密钥复制导出

1.2.4.1 定义和范围

密钥复制导出命令用于将密钥母卡中的密钥复制到其它设备中（如工作母卡等），导出密钥只能采用母卡主控密钥或工作母卡主控密钥，而不能采用移动母卡主控密钥。

该指令将指定的密钥（包括所有的属性信息）复制导出，因此，目标设备的密钥属性必须与密钥母卡中的被导出密钥一致。

密钥母卡在执行密钥复制导出操作时，必须首先的需要对密钥母卡进行外部认证（采用母卡主控密钥）和校验密码操作后才能获得此功能权限。

1.2.4.2 密钥复制导出命令（CopyExport Key）

带格式的：编号 + 级别：1 + 编号样式：1, 2, 3, … + 起始编号：1 + 对齐方式：左侧 + 对齐位置：0 厘米 + 制表符后于：0 厘米 + 缩进位置：0.74 厘米

1) 命令报文

CopyExport Key 命令报文见下表。

表 8-2-14 CopyExport Key 命令报文

代码	值
CLA	80h
INS	C4h
P1	00h
P2	见 P2 说明
Lc	根据命令报文数据域各字段长度计算得出
Data	见命令报文数据域说明
Le	不存在

2) P2的说明

P2 = 00 ，导出至工作母卡

P2 = 01，导出至企业前置平台用于交易验证（密文导出），报文数据域中CIPP、导出密钥属性及导入设备随机数三个字段均无效（需要留出位置）

3) 命令报文数据域

表8-2-15 CopyExport Key命令报文数据域

字段	长度（字节）	说明
母卡密钥导入的指令头（CIPP）	4	l 密钥导出后，在进行母卡密钥装载时使用的APDU指令。 l 数据格式： 1. CLA ：1字节 2. INS：1字节 3. P1：1字节 4. P2：1字节
导出密钥的属性(版本/索引/类型)	3	l 导出密钥的属性。 l 数据格式： 1. 版本：1字节 2. 索引：1字节 3. 类型：1字节
密钥属性（版本/索引/类型）	3	l 需要被导出的密钥属性。 l 数据格式： 1. 版本：1字节 2. 索引：1字节 3. 类型：1字节
导入设备随机数	4	l 导入设备生成随机数

4) 响应报文数据域

表8-2-16 CopyExport Key响应报文数据域

字段	长度（字节）	说明
密钥记录密文	20h	l 由导出密钥（母卡主控密钥/工作母卡主控密钥）加密的密钥记录。 l 密钥记录明文格式为： 1. 记录长度：1字节，固定为1Bh 2. 密钥属性：11字节 3. 密钥值：16字节
MAC码	4	l 由导出密钥（母卡主控密钥/工作母卡主控密钥）计算的MAC码。 l MAC计算数据格式： 1. CIPP 2. Lc

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0.74 厘米 + 制表符后于: 0 厘米 + 缩进位置: 1.48 厘米

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0.74 厘米 + 制表符后于: 0 厘米 + 缩进位置: 1.48 厘米

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0.74 厘米 + 制表符后于: 0 厘米 + 缩进位置: 1.48 厘米

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

带格式的: 项目符号 + 级别: 1 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0.74 厘米 + 制表符后于: 0 厘米 + 缩进位置: 1.48 厘米

带格式的: 项目符号 + 级别: 1 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0.74 厘米 + 制表符后于: 0 厘米 + 缩进位置: 1.48 厘米

		3. 密钥记录密文：32 字节

1.2.4.3 状态码

表 8-2-17 CopyExport Key 状态码

错误代码	说明
6473	密钥的分散级数错误
6476	密钥未找到
6484	密钥使用状态不满足
6700	数据长度不正确
6982	安全状态不满足
6A80	输入数据错误
6A86	P1、P2 不正确
9408	文件类型不匹配

1.2.5 密钥导入

1.2.5.1 定义和范围

密钥导入命令用于将外部的密钥注入到密钥母卡中。导入密文数据由加密机或母卡认证卡生成，具体参见母卡认证卡接口。

密钥母卡在执行密钥生成操作时，必须首先的需要密钥母卡进行外部认证和校验密码操作后才能获得此功能权限。各类密钥的写入权限，参考 7.2.1 部分的说明。

在装载密钥的时候，根据 APDU 中的 P2 参数来确定导入密钥的级别，一级密钥只能用移动母卡主控密钥来解密和验证，二级密钥只能用母卡主控密钥来解密和验证。解密以后，还要验证明文密钥信息中的 TVIA 来判断 P2 中所指定的密钥级别是否正确，如果不正确，不能导入。

外部发送此命令之前，需要先从密钥母卡中获取 4 字节随机数，用于此命令数据域中的 MAC 计算时使用。

1.2.5.2 密钥导入命令（Import Key）

带格式的：编号 + 级别：1 + 编号样式：1, 2, 3, … + 起始编号：1 + 对齐方式：左侧 + 对齐位置：0 厘米 + 制表符后于：0 厘米 + 缩进位置：0.74 厘米

1) 命令报文

Import Key 命令报文见下表。

表 8-2-18 Import Key 命令报文

代码	值
CLA	80h
INS	D8h

P1	00h
P2	见 P2 说明
Lc	24h
Data	见命令报文数据域说明
Le	不存在

2) P2 说明

表 8-2-19 Import Key 指令 P2 参数说明

P2 值		密钥母卡	工作母卡	母卡认证卡
00h	功能	更新密钥母卡/工作母卡/母卡认证卡信息（见“Update Info”指令）		
	需要状态	PIN 校验+使用各自解密密钥进行外部认证		
	解密密钥	移动母卡主控密钥	移动工作母卡主控密钥	母卡认证卡主控密钥
01h	功能	装载除终端初始密钥外的其他母卡密钥	装载移动工作母卡主控、工作母卡主控密钥	装载所有母卡认证卡密钥
	需要状态	PIN 校验+使用各自解密密钥进行外部认证		
	解密密钥	同 P2 = 00h		
02h	功能	装载终端初始密钥		无
	需要状态	PIN 校验+使用母卡主控密钥进行外部认证	PIN 校验	
	解密密钥	母卡主控密钥	工作母卡主控密钥	
03h	功能	无	装载工作母卡中唯一的应用密钥	无
	需要状态		PIN 校验	
	解密密钥		工作母卡主控密钥	

3) 命令报文数据域

表 8-2-20 Import Key 命令报文数据域

字段	长度（字节）	说明
密钥记录密文	20h	▌密钥记录密文（由移动母卡主控密钥/母卡主控密钥加密）。 ▌密钥记录明文格式为： 1. 记录长度：1 字节，固定为 1Bh 2. 密钥属性：11 字节 3. 密钥值：16 字节 说明：该指令通过密钥属性信息指定要导入密钥的类型、版本和索引等信息
MAC 码	4	▌MAC 码（由移动母卡主控密钥/母卡主控密钥计算） ▌MAC 计算数据格式： 1. CIPP 2. Lc 3. 密钥记录密文：32 字节

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

带格式的: 项目符号 + 级别: 1 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0.74 厘米 + 制表符后于: 0 厘米 + 缩进位置: 1.48 厘米

带格式的: 项目符号 + 级别: 1 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0.74 厘米 + 制表符后于: 0 厘米 + 缩进位置: 1.48 厘米

4) 响应报文数据域

无。

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

1.2.5.3 状态码

表 8-2-21 Import Key 状态码

错误代码	说明
6475	记录未找到
6478	加密密钥未找到
6480	文件未找到
6700	数据长度不正确
6982	安全状态不满足（包括导入权限不正确）
6983	文件被锁定
6985	使用状态不满足（未取随机数）
6988	MAC 不正确
6CXX	记录长度不正确，应为 XX
9408	文件类型不匹配

1.2.6 指令 MAC 计算

1.2.6.1 定义和范围

该指令用于在发卡过程中，为各种指令生成 MAC（不包括加密功能）。密钥母卡在执行该操作时，必须首先对密钥母卡进行外部认证和校验密码操作后才能获得此功能权限。

1.2.6.2 指令 MAC 计算（INST_MAC GENERATE）

1) 命令报文

Inst_MAC Generate 命令报文见下表。

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

表 8-2-22 Inst_MAC Generate 命令报文

代码	值
CLA	80h
INS	32h
P1	见 P1 说明
P2	00h
Lc	根据命令报文数据域各字段长度计算得出
Data	见命令报文数据域说明
Le	不存在

2) P1 说明

P1 参数长度为 1 个字节，采用 P1 的 8 个 bit 分别定义如下属性：

- MAC 密钥的分散因子长度
- MAC 密钥的分散方式
- MAC 密钥是否采用会话密钥
- MAC 算法

详细定义如下表所示：

b8	b7	b6	b5	b4	b3	b2	b1	含　义
x	x	x	x	x	x	x	0	MAC密钥采用8字节分散因子
x	x	x	x	x	x	x	1	MAC密钥采用16字节分散因子
x	x	x	x	0	0	x	x	MAC密钥采用标准3DES方式分散
x	0	x	x	x	x	x	x	MAC密钥采用会话密钥
x	1	x	x	x	x	x	x	MAC密钥不采用会话密钥
0	x	x	x	x	x	x	x	MAC采用9.19算法
1	x	x	x	x	x	x	x	MAC采用9.9算法

对 P1 参数的使用举例如下：

例如：如果为用户卡计算 MAC，采用 8 字节分散因子，标准 3DES 分散，采用会话密钥，9.19 算法计算 MAC，则 P1=00h。

如果为 SAM 卡计算 MAC，采用 16 字节分散因子，标准 3DES 分散，不采用会话密钥，9.19 算法计算 MAC，则 P1=41h。

3) 命令报文数据域

表 8-2-23 Inst_MAC Generate 命令报文数据域

字段	长度（字节）	说明
用户卡密钥装载指令头（CIPP）	4	▪ 密钥导出后，在进行用户卡密钥装载时使用的 APDU 指令。 ▪ 数据格式： 1. CLA ：1 字节 2. INS：1 字节 3. P1：1 字节 4. P2：1 字节
用户卡随机数	4	用户卡生成随机数
MAC 密钥分散级数	1	MAC 密钥的分散级数。 ***MAC 计算的指令需要对 MAC 密钥分散后再计算，以和目标卡片的验证密钥一致***
MAC 密钥分散因子	MAC 密钥分散级数*8（或密钥分散级数*16）	MAC 密钥的分散因子数据，数据长度必须为 8 的倍数（或 16 的倍数），如果分散级数为 0，那么本字段不存在。

MAC 密钥属性（版本/索引/类型）	3	▪ MAC 密钥的属性。 ▪ 数据格式： 1. 版本：1 字节 2. 索引：1 字节 3. 类型：1 字节
数据长度	1	数据的长度
数据明文	N	需要做 MAC 计算的明文数据

带格式的：编号 + 级别：1 + 编号样式：1, 2, 3, … + 起始编号：1 + 对齐方式：左侧 + 对齐位置：0.74 厘米 + 制表符后于：0 厘米 + 缩进位置：1.48 厘米

4) 响应报文数据域

带格式的：编号 + 级别：1 + 编号样式：1, 2, 3, … + 起始编号：1 + 对齐方式：左侧 + 对齐位置：0 厘米 + 制表符后于：0 厘米 + 缩进位置：0.74 厘米

表 8-2-24 Inst_MAC Generate 响应报文数据域

字段	长度（字节）	说明
MAC 码	4	MAC 码，对以下数据计算得出： ——CLA ——INS ——P1 ——P2 ——Lc ——需要做 MAC 计算的明文信息

1.2.6.3 状态码

表 8-2-25 Inst_MAC Generate 状态码

错误代码	说明
6982	安全状态不满足
6476	密钥未找到
6485	使用条件不满足
6484	密钥使用状态不满足
6700	数据长度不正确
6A86	P1、P2 不正确

1.2.7 更新密钥母卡信息

1.2.7.1 定义和范围

更新密钥母卡信息指令用于向密钥母卡中写入，或更新密钥母卡内的企业 ID 以及其它信息。

密钥母卡在执行该操作时，必须首先的需要对密钥母卡进行外部认证和校验密码操作后才能获得此功能权限。其中，工作母卡和母卡认证卡需要使用其各自主控密钥进行外部认证；密钥母卡需要根据导入信息的不同，来使用主控密钥或第二主控密钥的外部认证获得此权限。

外部发送此命令之前，需要先从密钥母卡中获取 4 字节随机数，用于此命令数据域中的 MAC 计算时使用。

1.2.7.2 更新密钥母卡信息命令（Update Info）

1) 命令报文

Update Info 命令报文见下表。

表 8-2-26 Update Info 命令报文

代码	值
CLA	80h
INS	D8h
P1	00h
P2	00h
Lc	根据命令报文数据域各字段长度计算得出
Data	见命令报文数据域说明
Le	不存在

2) 命令报文数据域

表 8-2-27 Update Info 命令报文数据域

字段	长度（字节）	说明
数据	N	数据密文： 1、数据类型（1 字节）： 0x01：企业 ID 其它：保留 2、数据长度（1 字节） 3、数据（M 字节） ***说明：*** *1、密钥母卡：企业 ID 只能由移动母卡主控密钥加密，其它企业自有信息可以由母卡主控密钥加密* *2、母卡认证卡：企业 ID 只能由母卡认证卡主控密钥加密* *3、工作母卡:企业 ID 只能由移动工作母卡主控密钥加密，其它企业自有信息可以由工作母卡主控密钥加密*
MAC 码	4	MAC 码（采用与加密密钥同样的密钥计算 MAC） MAC 计算数据格式： 1. CIPP 2. Lc 3. 数据密文：N 字节

3) 响应报文数据域

无。

1.2.7.3 状态码

表 8-2-28 Update Info 状态码

错误代码	说明
6475	记录未找到
6478	加密密钥未找到
6480	文件未找到
6700	数据长度不正确
6982	安全状态不满足
6983	文件被锁定
6985	使用状态不满足（未取随机数）
6988	MAC 不正确
6A80	输入数据错误
6CXX	记录长度不正确，应为 XX
9408	文件类型不匹配

2 母卡认证卡接口要求

2.1 基本接口

2.1.1 校验密码（Verify PIN）

同密钥母卡接口中的“校验密码”接口，见 7.1.1 节。

2.1.2 更改密码（Change PIN）

同密钥母卡接口中的“更改密码”接口，见 7.1.2 节。

2.1.3 重置密码（Reload PIN）

同密钥母卡接口中的“重置密码”接口，见 7.1.3 节。

2.1.4 取随机数（Get Challenge）

同密钥母卡接口中的“取随机数”接口，见 7.1.4 节。

2.1.5 外部认证（External Authentication）

同密钥母卡接口中的“外部认证”接口，见 7.1.5 节。

2.1.6 获取响应数据（Get Response）

同密钥母卡接口中的“获取响应数据”接口，见 7.1.7 节。

2.2 密钥及密码服务接口

2.2.1 读取密钥属性（Read KeyInfo）

同密钥母卡接口中的“读取密钥属性”接口，见 7.2.1 节。

2.2.2 数据加密

2.2.2.1 定义和范围

数据加密用于使用母卡认证卡中的母卡主控密钥进行数据加密运算。该接口用于向密钥母卡提供外部认证数据。

密钥母卡在执行密钥生成操作时，必须首先的需要对母卡认证卡进行校验密码操作后才能获得此功能权限。

2.2.2.2 加密数据命令（Encrypt Data）

1) 命令报文

Encrypt Data 命令报文见下表。

表 9-2-1 Encrypt Data 命令报文

代码	值
CLA	80h
INS	30h
P1	00h
P2	00h
Lc	N
Data	见命令报文数据域说明
Le	不存在

2) 命令报文数据域

带格式的：编号 + 级别：1 + 编号样式：1，2，3，… + 起始编号：1 + 对齐方式：左侧 + 对齐位置：0 厘米 + 制表符后于：0 厘米 + 缩进位置：0.74 厘米

带格式的：编号 + 级别：1 + 编号样式：1，2，3，… + 起始编号：1 + 对齐方式：左侧 + 对齐位置：0 厘米 + 制表符后于：0 厘米 + 缩进位置：0.74 厘米

表 9-2-2 Encrypt Data 命令报文数据域

字段	长度（字节）	说明
密钥母卡随机数	4	密钥母卡生成的随机数，用于会话密钥生成
数据长度	1	后续数据明文的长度，如果该字段为 0，则卡片将直接使用密钥对随机数进行加密，返回加密结果
数据明文	N	对于向密钥母卡中写入初始密钥的指令，则需要首先向母卡认证卡发送该指令请求，母卡认证卡返回密钥密文，请求格式参见密钥母卡的“密钥导入”指令中定义的导入格式

3) 响应报文数据域

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

表 9-2-3 Encrypt Data 响应报文数据域

字段	长度（字节）	说明
数据密文长度	1	
数据密文	N	由母卡主控密钥加密的数据密文，长度为 8 的倍数。

2.2.2.3 状态码

表 9-2-4 Encrypt Data 状态码

错误代码	说明
6479	密钥未找到
6485	使用条件不满足
6484	密钥使用状态不满足
6700	数据长度不正确
6A80	指令数据域中数据有错误，含有不合法数据
6A86	P1、P2 不正确

2.2.3 MAC 计算

2.2.3.1 定义和范围

MAC 计算用于使用母卡认证卡中的母卡认证卡主控密钥进行报文 MAC 运算。

密钥母卡在执行密钥生成操作时，必须首先的需要对母卡认证卡进行校验密码操作后才能获得此功能权限。

2.2.3.2 MAC 计算命令（MAC Generate）

1) 命令报文

MAC Generate 命令报文见下表。

表 9-2-5 MAC Generate 命令报文

代码	值
CLA	80h
INS	32h
P1	00h
P2	00h
Lc	N
Data	见命令报文数据域说明
Le	不存在

2) 命令报文数据域

表 9-2-6 MAC Generate 命令报文数据域

字段	长度（字节）	说明
密钥母卡随机数	4	密钥母卡生成的随机数，用于会话密钥生成
MAC 数据长度	1	
MAC 数据	N	

3) 响应报文数据域

表 9-2-7 MAC Generate 响应报文数据域

字段	长度（字节）	说明
MAC 码	4	由母卡主控密钥计算的 MAC 码。密钥母卡首先会在 MAC 数据后强制填充 80h，如果 MAC 数据长度不是 8 的倍数，密钥母卡会自动补齐 00h 至尾。然后对整个数据块进行 MAC 运算。

2.2.3.3 状态码

表 9-2-8 MAC Generate 状态码

错误代码	说明
6479	密钥未找到
6485	使用条件不满足
6484	密钥使用状态不满足
6700	数据长度不正确
6A80	指令数据域中数据有错误，含有不合法数据
6A86	P1、P2 不正确

2.2.4 密钥导入

2.2.4.1 定义和范围

母卡认证卡密钥导入命令用于将母卡认证卡主控密钥和母卡主控密钥导入至母卡认证卡中。

母卡认证卡内的密钥均采用母卡认证卡主控密钥控制下装载。

工作母卡在执行密钥导入操作时，必须首先的需要对母卡进行校验密码操作后才能获得此功能权限。

2.2.4.2 密钥导入命令（Import Key）

导入命令要求与密钥母卡一致，参见密钥母卡的密钥导入接口，见 7.2.5 节。

密钥采用移动工作母卡主控密钥或工作母卡的主控密钥加密。

2.2.5 更新卡片信息（Update Info）

参见密钥母卡接口中的“更新密钥母卡信息”接口，见 7.2.7 节。

3 工作母卡接口要求

3.1 基本接口

3.1.1 校验密码（Verify PIN）

同密钥母卡接口中的“校验密码”接口，见 7.1.1 节。

3.1.2 更改密码（Change PIN）

同密钥母卡接口中的“更改密码”接口，见 7.1.2 节。

3.1.3 重置密码（Reload PIN）

同密钥母卡接口中的“重置密码”接口，见 7.1.3 节。

3.1.4 SELECT 命令

同密钥母卡接口中的“SELECT”接口，见7.1.6节。

3.1.5 取随机数（Get Challenge）

同密钥母卡接口中的“取随机数”接口，见 7.1.4 节。

3.1.6 外部认证（External Authentication）

同密钥母卡接口中的“外部认证”接口，见 7.1.5 节。

3.1.7 获取响应数据（Get Response）

同密钥母卡接口中的“获取响应数据”接口，见 7.1.7 节。

3.2 密钥及密码服务接口

3.2.1 读取密钥属性（Read KeyInfo）

同密钥母卡接口中的“读取密钥属性”接口，见 7.2.1 节。

3.2.2 密钥导出

3.2.2.1 定义和范围

工作母卡密钥导出命令用于将工作母卡中的终端密钥导出。需要按照终端的密钥写入接口生成指令。

说明：工作母卡内存储唯一的终端应用密钥和唯一的初始密钥，该指令可以采用卡内存储的应用密钥通过子应用索引号分散出终端的子应用密钥，并采用卡内存储的终端初始密钥加密后输出。

每个工作母卡只针对于一个应用，根据终端传递的子应用索引号，可以为多个终端实例写入密钥。

3.2.2.2 密钥导出命令（Export Key）

1) 命令报文

Export Key 命令报文见下表。

带格式的：编号 + 级别：1 + 编号样式：1，2，3，… + 起始编号：1 + 对齐方式：左侧 + 对齐位置： 0 厘米 + 制表符后于： 0 厘米 + 缩进位置： 0.74 厘米

表 10-2-1 Export Key 命令报文

代码	值
CLA	80h
INS	C0h
P1	00h
P2	00h
Lc	根据命令报文数据域各字段长度计算得出
Data	见命令报文数据域说明
Le	不存在

2) 命令报文数据域

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

表 10-2-2 Export Key 命令报文数据域

字段	长度（字节）	说明
终端随机数	4	进行加密和 MAC 计算时的随机因子
子应用索引号分散因子	8	子应用索引号分散因子，子应用索引号+密钥版本号+800000000000（需要终端传递该号码） ***说明：此处传入经过拼装的分散因子（而不是子应用索引号），以避免由于分散因子的变化导致接口的变化***
终端密钥属性长度	1	终端的密钥存储时需要的密钥头属性长度
终端密钥属性	N	终端密钥头属性
MAC	4	采用终端初始密钥对以上所有字段计算的 MAC

3) 响应报文数据域

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

表 10-2-3 Export Key 响应报文数据域

字段	长度（字节）	说明
密文长度	1	
密钥密文	N	被导出密钥的密文数据，对以下数据加密得出： ——密钥头 ——密钥值
MAC 码	4	MAC 码数据，对以下数据计算得出： 密文长度 密钥密文信息

3.2.2.3 状态码

表 10-2-4 Export Key 状态码

错误代码	说明
6473	密钥的分散级数错误
6476	密钥未找到
6484	密钥使用状态不满足
6700	数据长度不正确
6982	安全状态不满足
6A80	输入数据错误
6A86	P1、P2 不正确
9408	文件类型不匹配

3.2.3 数据导出

3.2.3.1 定义和范围

工作母卡数据导出命令用于将工作母卡中的企业 ID 信息导出后，写入终端。

3.2.3.2 数据导出命令（Export Data）

1) 命令报文

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

Export Data 命令报文见下表。

表 10-2-5 Export Data 命令报文

代码	值
CLA	80h
INS	C0h
P1	00h
P2	00h
Lc	根据命令报文数据域各字段长度计算得出
Data	见命令报文数据域说明
Le	不存在

2) 命令报文数据域

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

表 10-2-6 Export Data 命令报文数据域

字段	长度（字节）	说明
终端随机数	4	与工作母卡随机数一起作为进行加密和 MAC 计算时的随机因子
MAC	4	采用终端应用密钥对以上所有字段计算的 MAC

3) 响应报文数据域

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0 厘米 + 制表符后于: 0 厘米 + 缩进位置: 0.74 厘米

表 10-2-7 Export Data 响应报文数据域

字段	长度（字节）	说明
企业 ID	6	
MAC 码	4	MAC 码数据，对以下数据计算得出： 企业ID

3.2.3.3 状态码

表 10-2-8 Export Data 状态码

错误代码	说明
6476	密钥未找到
6484	密钥使用状态不满足
6700	数据长度不正确
6982	安全状态不满足
6A80	输入数据错误
6A86	P1、P2 不正确
9408	文件类型不匹配

3.2.4 密钥导入

3.2.4.1 定义和范围

工作母卡密钥导入命令用于将终端初始密钥和终端应用密钥导入至工作母卡中。

在装载密钥的时候，根据 APDU 中的 P2 参数来确定导入密钥的级别，一级密钥只能用移动工作母卡主控密钥来解密和验证，二级密钥只能用工作母卡主控密钥来解密和验证。解密以后，还要验证明文密钥信息中的 TVIA 来判断 P2 中所指定的密钥级别是否正确，如果不正确，不能导入。

工作母卡在执行密钥导入操作时，必须首先的需要对工作母卡进行校验密码操作后才能获得此功能权限。

3.2.4.2 密钥导入命令（Import Key）

导入命令要求与密钥母卡一致。

密钥采用移动工作母卡主控密钥或工作母卡的主控密钥加密。

3.2.5 更新卡片信息（Update Info）

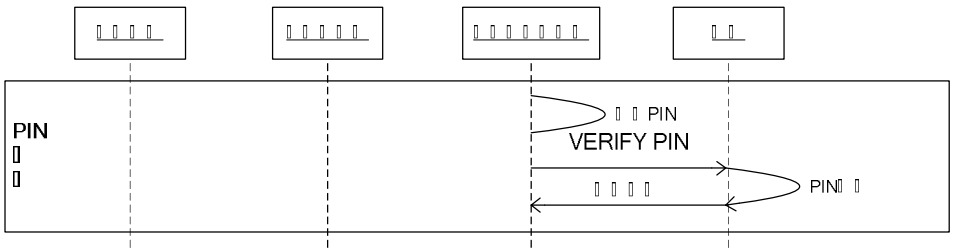
同密钥母卡接口中的“更新密钥母卡信息”接口，见 7.2.7 节。

4 母卡操作流程

4.1 企业端管理系统相关流程

4.1.1 母卡 PIN 校验流程

在使用母卡（包括密钥母卡、母卡认证卡、工作母卡）做其它操作之前需要完成母卡 PIN 校验流程，如下图所示：



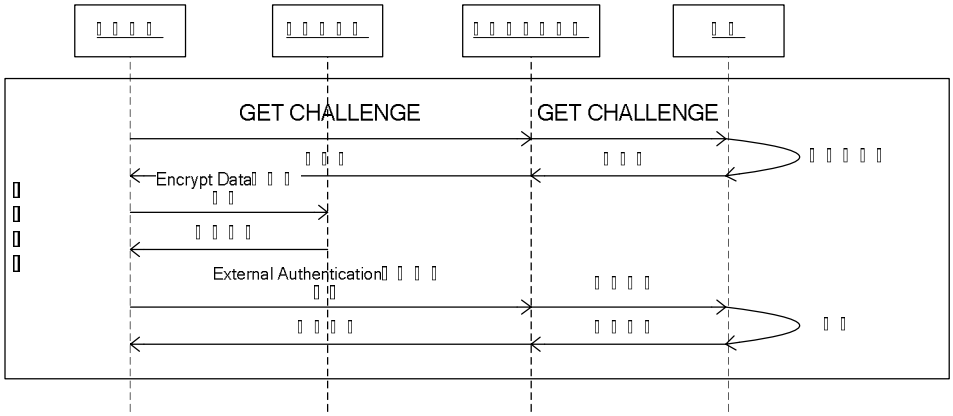
流程说明：

1、 通过企业端管理系统管理终端输入 PIN
2、 企业端管理系统向母卡发送 Verify PIN 指令
3、 母卡做 PIN 校验
4、 母卡返回校验结果

带格式的：编号 + 级别：1 + 编号样式：1，2，3，… + 起始编号：1 + 对齐方式：左侧 + 对齐位置： 0.74 厘米 + 制表符后于： 0 厘米 + 缩进位置： 1.38 厘米

4.1.2 外部认证流程

外部认证流程是母卡对外部实体（如母卡认证卡）进行认证的流程，如下图所示：



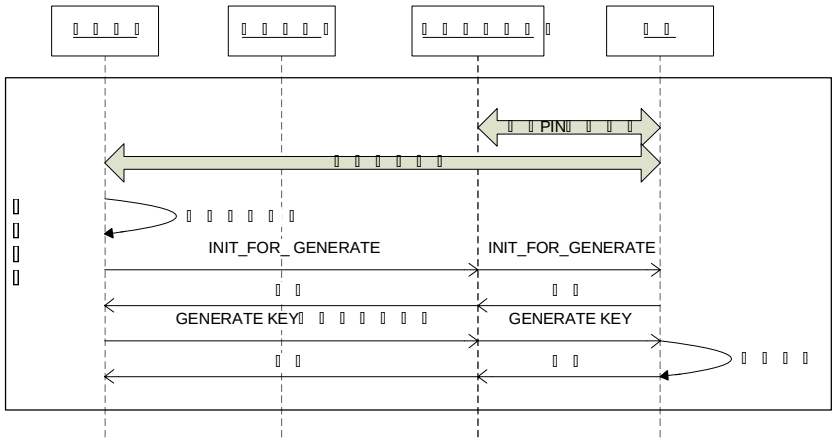
流程说明：

1、发卡终端向企业端管理系统发送 GET CHALLEGE 指令
2、企业端管理系统向母卡转发 GET CHALLEGE 指令
3、母卡生成随机数
4、母卡通过企业端管理系统向发卡终端返回随机数
5、发卡终端向母卡认证卡发送 Encrypt Data 指令（携带母卡随机数）
6、母卡认证卡返回认证数据
7、发卡终端通过企业端管理系统向母卡发送 External Authentication 指令（携带认证数据）
8、母卡对认证数据进行验证
9、母卡返回验证结果

带格式的：编号 + 级别：1 + 编号样式：1，2，3，… + 起始编号：1 + 对齐方式：左侧 + 对齐位置：0.74 厘米 + 制表符后于：0 厘米 + 缩进位置：1.38 厘米

4.1.3 密钥生成

密钥母卡通过密钥生成流程生成新密钥，如下图所示：



流程说明：

1、企业端管理系统首先需要通过密钥母卡 PIN 校验流程（插卡后只需要验证一次）

2、发卡终端采用母卡认证卡与密钥母卡完成外部认证流程

3、用户通过发卡终端输入密钥码单

4、发卡终端向密钥母卡发送 INIT_FOR_GENERATE 指令

5、发卡终端向密钥母卡发送 GENERATE KEY 指令，根据生成密钥的多少，该指令可以发送多次

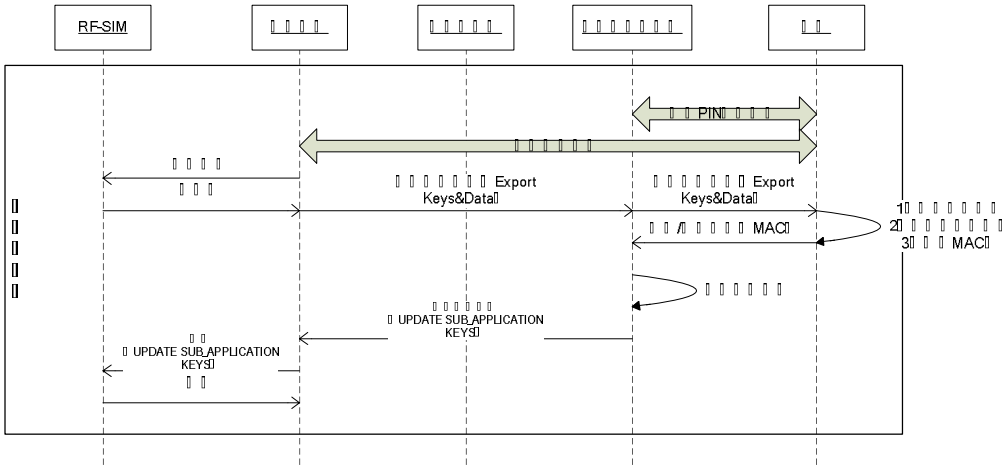
6、密钥母卡生成密钥

7、密钥母卡返回结果

带格式的：编号 + 级别：1 + 编号样式：1，2，3，… + 起始编号：1 + 对齐方式：左侧 + 对齐位置：0.74 厘米 + 制表符后于：0 厘米 + 缩进位置：1.38 厘米

4.1.4 用户卡密钥更新

密钥母卡对外提供的 Export Keys&Data 功能主要用于用户卡密钥及相关数据的更新，如下图所示：



流程说明：

1、企业端管理系统首先需要通过密钥母卡 PIN 校验流程（插卡后只需要验证一次）

2、发卡终端采用母卡认证卡与密钥母卡完成外部认证流程

3、用户通过发卡终端向企业端管理系统发起密钥导出（Export Keys&Data）请求

4、企业端管理系统把请求发送至密钥母卡

5、密钥母卡计算导出密钥、加密密钥及数据、计算 MAC 码

6、密钥母卡将密钥及数据密文、MAC 码返回企业端管理系统

7、企业端管理系统生成写卡指令

8、企业端管理系统将写卡指令返回发卡终端

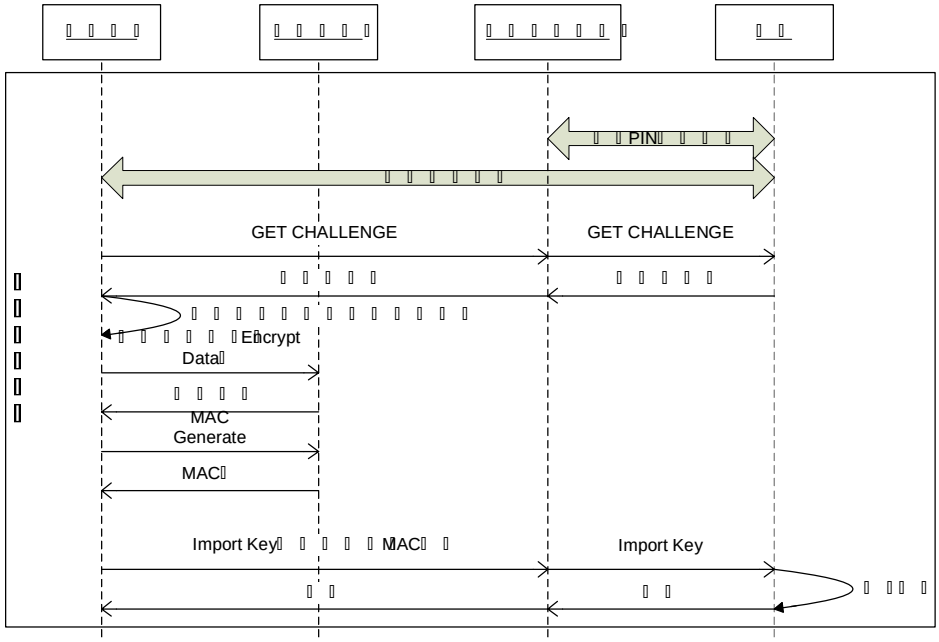
9、发卡终端执行写卡指令，将密钥和数据写入 RF-SIM 卡

10、RF-SIM 卡返回响应

带格式的：编号 + 级别：1 + 编号样式：1，2，3，… + 起始编号：1 + 对齐方式：左侧 + 对齐位置：0.74 厘米 + 制表符后于：0 厘米 + 缩进位置：1.38 厘米

4.1.5 初始密钥导入

密钥导入，主要用于终端的初始密钥导入，如下图所示：



流程说明：

1、企业端管理系统首先需要通过密钥母卡 PIN 校验流程（插卡后只需要验证一次）

2、发卡终端采用母卡认证卡与密钥母卡完成外部认证流程

3、发卡终端通过企业端管理系统向密钥母卡发送 Get Challenge 指令

4、密钥母卡返回随机数

5、发卡终端向母卡认证卡发送 Encrypt Data 指令（传递密钥明文参数）

6、母卡认证卡返回密钥密文信息

7、发卡终端向母卡认证卡发送 MAC Generate 指令（传递密钥密文信息）

8、母卡认证卡返回 MAC 码

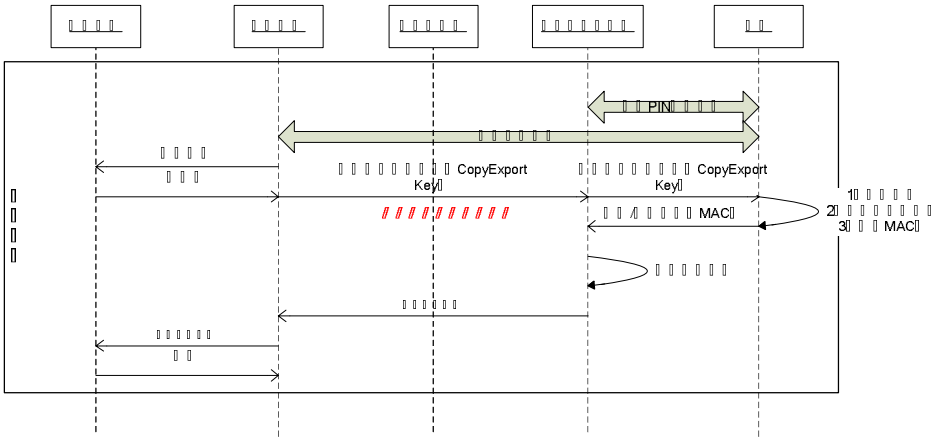
9、发卡终端向密钥母卡发送 Import Key 指令（携带密钥密文、MAC 码）

10、密钥母卡完成密钥导入

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0.74 厘米 + 制表符后于: 0 厘米 + 缩进位置: 1.38 厘米

4.1.6 工作母卡制作

工作母卡由移动统一提供给企业，并预置企业 ID。企业按照如下流程将终端密钥和应用密钥写入工作母卡，完成企业内的工作母卡制作流程。

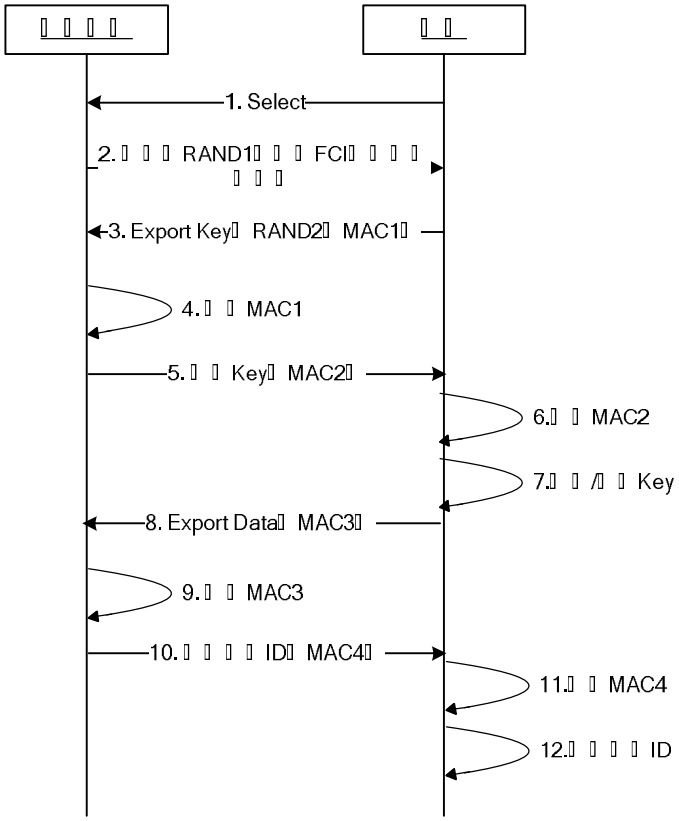


流程说明：

1、PIN 验证流程、外部认证流程
2、发卡终端向工作母卡获取随机数
3、发卡终端向通过企业端管理系统向密钥母卡发送密钥复制导出请求
4、密钥母卡导出密钥，并发送密钥密文/MAC 码
5、企业端管理系统生成写卡指令发送到发卡终端
6、发卡终端写卡

带格式的：编号 + 级别：1 + 编号样式：1，2，3，… + 起始编号：1 + 对齐方式：左侧 + 对齐位置：0.74 厘米 + 制表符后于：0 厘米 + 缩进位置：1.38 厘米

4.1.7 终端密钥写入流程



流程说明：

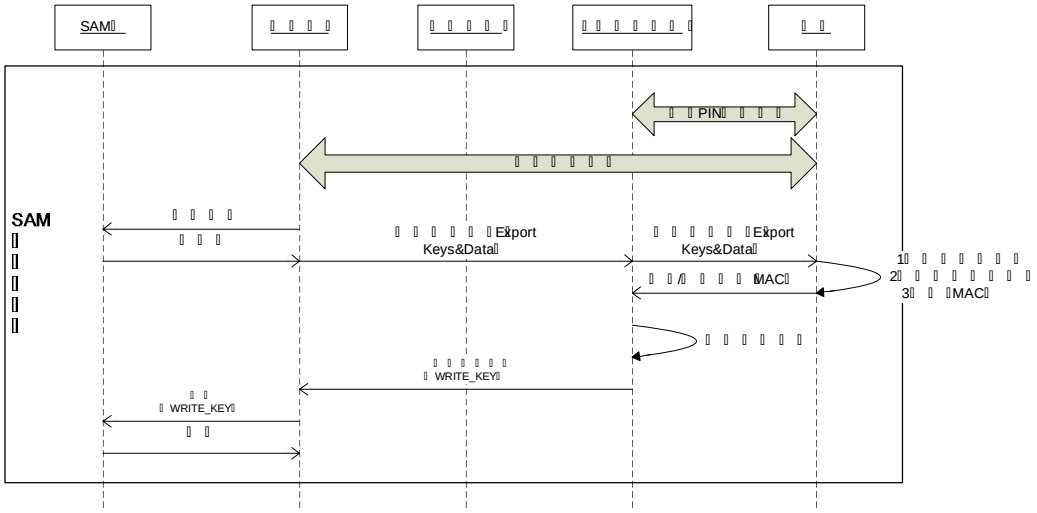
1、终端向工作密钥母卡发送 Select 指令
2、工作母卡响应随机数和 FCI 信息
3、终端发送 Export Key 指令（携带 MAC1）
4、工作母卡验证 MAC1
5、返回 Key（携带 MAC2）
6、终端验证 MAC2
7、终端写入 Key
8、终端发送 Export Data 指令（携带 MAC3）
9、工作母卡验证 MAC3
10、工作母卡返回企业 ID（携带 MAC4）
11、终端验证 MAC4
12、终端写入企业 ID

带格式的：1 级，编号 + 级别：1 + 编号样式：1，2，3，… + 起始编号：1 + 对齐方式：左侧 + 对齐位置：0.74 厘米 + 制表符后于：0 厘米 + 缩进位置：1.38 厘米

带格式的：编号 + 级别：1 + 编号样式：1，2，3，… + 起始编号：1 + 对齐方式：左侧 + 对齐位置：0.74 厘米 + 制表符后于：0 厘米 + 缩进位置：1.38 厘米

4.1.8 SAM 卡密钥更新

密钥母卡对外提供的 Export Keys&Data 功能可用于 SAM 卡密钥及相关数据的更新，如下图所示：



流程说明：

1、企业端管理系统首先需要通过密钥母卡 PIN 校验流程（插卡后只需要验证一次）

2、发卡终端采用母卡认证卡与密钥母卡完成外部认证流程

3、发卡终端通过母卡认证卡将 SAM 卡初始主控密钥导入密钥母卡

4、密钥导出/写入

对于每个密钥，均需要按以下流程从密钥母卡中导出，并按照 SAM 卡的写卡指令将密钥写入 SAM 卡：

a) 用户通过发卡终端向企业端管理系统发起密钥导出（Export Keys&Data）请求
b) 企业端管理系统把请求发送至密钥母卡
c) 密钥母卡计算导出密钥、加密密钥及数据、计算 MAC 码
d) 密钥母卡将密钥及数据密文、MAC 码返回企业端管理系统
e) 企业端管理系统生成写卡指令（WRITE_KEY）
f) 企业端管理系统将写卡指令返回发卡终端
g) 发卡终端执行写卡指令，将密钥和数据写入 SAM 卡
h) SAM 卡返回响应

带格式的: 编号 + 级别: 1 + 编号样式: 1, 2, 3, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 0.74 厘米 + 制表符后于: 0 厘米 + 缩进位置: 1.38 厘米

带格式的: 编号 + 级别: 2 + 编号样式: a, b, c, … + 起始编号: 1 + 对齐方式: 左侧 + 对齐位置: 1.48 厘米 + 制表符后于: 0 厘米 + 缩进位置: 2.22 厘米

密钥的保护关系和写入顺序参考《中国移动企业一卡通业务设备规范--SAM 卡部分》“9.1 密钥装载”部分的要求。

5 编制历史

版本号	更新时间	主要内容或重大修改
1.0.0	2009-12-14	形成评审稿