Simlinker PKI SAM 嵌入式安全模块技术参考手册

北京芯凌科技有限公司

BeijingSimlinkerTech Co.,Ltd

目录

1 关于本手册

1.1 内容概述

本手册介绍了 SIMLINKER ESAM 嵌入式安全模块的体系结构、安全报文的传输方式以及指令的详细使用方式，使您对 SIMLINKER ESAM 嵌入式安全模块有一个初步的了解。

1.2 支持的算法

- 支持的对称算法
  - DES/3DES
  - AES128
  - SM1(国密)
  - SM4(国密)
- 支持的非对称算法
  - SM2(国密)
  - RSA（1024/2048）
- 支持的数据摘要算法
  - SHA1、SH224、SHA256
  - SM3(国密)

2 SIMLINKER ESAM 嵌入式安全模块系统简介

2.1 主要特征

- 支持一卡多应用，各应用之间相互独立（多应用，防火墙功能）。
- 卡片内部用户可用空间为 64KB。
- 支持多种文件类型，包括二进制文件，定长记录文件，变长记录文件，循环文件。
- 支持多种安全访问方式和权限（认证功能、口令保护以及安全报文传输）。
- 支持多种对称算法、非对称算法以及摘要算法。
- 支持接触面 T=0 通讯协议。

2.2 SIMLINKER ESAM 嵌入式安全模块系统模块划分

SIMLINKER ESAM 嵌入式安全模块系统由传输管理、文件管理、安全体系、命令解析四个功能模块组成。

3 SIMLINKER ESAM 嵌入式安全模块指令集

3.1 Create File（建立文件）

3.1.1 定义和范围

Create File 命令用于建立文件系统。

3.1.2 命令报文

代码	长度(byte)	值(Hex)	描述
CLA	1	80	-
INS	1	E0	-
P1P2	2	XXXX	文件标识（FileID）
Lc	1	XX	-
DATA	XX	XX…XX	文件控制信息（和DF名称）

注：
MF的文件标识符必须是“3F00”；
KEY文件的文件标识符必须是“0000”。

3.1.3 命令报文数据域

主文件（MF）

数据域	文件类型	文件空间	建立权限	擦除权限	8字节传输代码
长度（byte）	1	2	1	1	8
值（HEX）	38	FFFF	XX	XX	FFFFFFFFFFFFFFFF

专用文件（DF）

数据域	文件类型	文件空间	建立权限	擦除权限	保留字	DF名称(可选)
长度(byte)	1	2	1	1	3	5-16
值（HEX）	38	XXXX	XX	XX	FFFFFF	DF 名称

基本文件（EF）

数据域 / 文件类型	B1	B2	B3	B4	B5	B6	B7

二进制文件	28	文件空间		读权限	写权限	【说明1】	【说明2】
定长记录文件	2A	2≤记录数≤254	记录长度≤178	读权限	写权限	【说明1】	【说明2】
循环文件	2E	2≤记录数≤254	记录长度≤178	读权限	写权限	【说明1】	【说明2】
变长记录文件	2C	文件空间=所有记录长度和 每条记录=记录长度+1字节校验码（由COS计算）		读权限	写权限	【说明1】	【说明2】
密钥文件	3F	文件空间		‘FF’	增加权限	【说明1】	‘FF’

非对称密钥文件

公钥文件	3C	文件空间	读权限	写权限	【说明1】	【说明2】
私钥文件	3D	文件空间	0F【说明3】	写权限	【说明1】	【说明2】

【说明 1】

安全报文传输控制（写）

BIT1	BIT0	安全报文传输控制
0	0	明文写入
1	0	明文+MAC 写入
1	1	密文+MAC 写入

安全报文传输控制（读）

BIT3	BIT2	安全报文传输控制
0	0	明文读取
1	0	明文+MAC 读取
1	1	密文+MAC 读取

注：

文件在初始化阶段，可以忽略安全报文传输控制，即可以明文初始化文件，在卡片复位或者更换操作目录后安全报文传输控制生效。

【说明 2】

在文件创建过程中，如果定义了安全状态（见说明 1），本子节指定所使用的维护密钥（36 密钥）ID。

【说明 3】

私钥文件在使用过程中，一般严禁做导出操作，所以读权限一般设置成‘0F’，禁止导出。

3.1.4 响应报文数据域

无

3.1.5 响应报文状态码

状态字（HEX）	描述
9000	正确执行
6700	长度错误/传输代码错误
6581	FLASH 操作失败
6982	权限不足
6983	应用临时锁定
6985	卡片锁定/应用永久锁定
6986	文件 ID 或者文件名重复
6A80	数据域参数不正确
6A84	空间不足
6A86	P1P2 错误（P1P2 指定文件已创建）

3.2 Write Key（增加或修改密钥）

3.2.1 定义与范围

Write Key命令向卡中装载密钥或更新卡中已存在的密钥。

3.2.2 注意事项

在满足当前DF下KEY文件的增加权限时时,可用Write Key命令向KEY文件中写入密钥。
当满足密钥的修改权限时，可以对密钥值进行修改。
密钥文件的写权限以及更新权限、安全报文传输方式在初始化完成之后生效。

3.2.3 命令报文

代码	长度(byte)	值(Hex)	描述
CLA	1	80/84	-
INS	1	D4	-
P1	1	01	用于密钥装载
		XX	密钥类型，用于密钥更新
P2	1	XX	密钥标识，KEYID
Lc	1	XX	数据长度
DATA	XX	XX…XX	数据

3.2.4 命令报文数据域

数据域 / 密钥类型	Byte1	Byte2	Byte3	Byte4【说明 1】		Byte5【说明 2】		密钥长度（Byte）
				BIT7-4	BIT3-0	BIT7-4	BIT3-0	
外部认证	39	使用权限	更改权限	密钥版本号	后续状态	算法标识	错误计数器	16/8
内部认证	30	使用权限	更改权限	密钥版本号	‘F’	算法标识	‘F’	16/8
维护密钥	36	使用权限	更改权限	密钥版本号	‘F’	算法标识	错误计数器	16/8
PIN	3A	使用权限	更改权限	密钥版本号	后续状态	算法标识	错误计数器	2~8
解锁/重装 PIN 密钥	37	使用权限	更改权限	密钥版本号	‘F’	算法标识	错误计数器	16/8
加密密钥	10	使用权限	更改权限	密钥版本号	‘F’	算法标识	‘F’	16/8

解密密钥	11	使用权限	更改权限	密钥版本号	‘F’	算法标识	‘F’	16/8
MAC 计算密钥	09	使用权限	更改权限	密钥版本号	‘F’	算法标识	‘F’	16/8

【说明 1】

BYTE4：该传输控制字分为高半字节和低半字节。

高半字节：密钥的版本号

低半字节：密钥的后续状态

【说明 2】

BYTE5：该传输控制字分为高半字节和低半字节。

高半字节：密钥的算法标识，卡片系统在使用密钥时，根据算法标识的不同，采用不同的算法。

算法标识	HEX 值
3DES	0x00
DES	0x01
AES(128)	0x02
SM1	0x03
SM4	0x04

低半字节：密钥的错误计数器。

3.2.5 响应报文数据域

无

3.2.6 响应报文状态码

状态字(HEX)	描述
9000	正确执行
6E00	CLA 不支持
6700	Lc 长度错误
6581	FLASH 操作失败
6982	权限不足
6983	密钥已锁定
6984	未取随机数
6986	文件 ID 或者文件名重复
6988	Mac 错
6A80	密钥长度不一致
6A82	文件不存在
6A84	文件空间不足
6A86	P1P2 错误
9403	密钥未找到

3.3 Select File（选择文件）

3.3.1 定义与范围

Select File 命令通过文件名、文件标识符来选择卡片中 MF、DDF 或 ADF 以及 EF。

3.3.2 注意事项

正确选择 MF 后，MF 安全寄存器将被复位为 0。
正确选择 MF 下各个 DF 后，DF 安全寄存器将被复位为 0，MF 安全寄存器的值不变。

3.3.3 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	00	-
INS	1	A4	-
P1	1	00/04	【说明 1】
P2	1	00	-
Lc	1	XX	-
DATA	XX	XX…XX	文件标识符或 DF AID

【说明 1】

P1=00，标识按文件标识符选择（P2 必须等于 0），可选择当前目录（DF）下基本文件或子目录文件。

P1=04，标识用 DF 名称选择，用此方法可以选择 DF。

在任何情况下均可通过标识符‘3F00’选择 MF。

3.3.4 命令报文数据域

文件标识符或 DF AID。

3.3.5 响应报文状态码

状态字(HEX)	描述
9000	正确执行
6E00	CLA 不支持
6700	Lc 错误
6A82	文件不存在
6A86	P1 或者 P2 错误

3.4 Update Binary（写二进制文件）

3.4.1 定义与范围

Update Binary 命令用于写二进制文件。

3.4.2 注意事项

Update Binary 命令只适用于二进制文件。

访问二进制文件的命令：

建立文件（Create File）

选择文件（Select File）

读二进制文件（Read Binary）/写二进制文件（Update Binary）

只有满足二进制文件写权限时才能执行此命令。

3.4.3 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	00/04	-
INS	1	D6	-
P1	1	XX	【说明 1】
P2	1	XX	【说明 1】
Lc	1	XX	【说明 2】
DATA	XX	XX…XX	写入文件的数据

【说明 1】

若 P1 的高三位为 100，则低 5 位为短文件标识符，P2 为文件的偏移量。

P1								P2
b7	b6	b5	b4	b3	b2	b1	b0	
1	0	0	短文件标识符					文件的偏移量

若 P1 的最高位不为 1，则 P1P2 为文件的偏移量，所写文件为当前文件。

P1								P2
b7	b6	b5	b4	b3	b2	b1	b0	
0	文件偏移量							

【说明 2】

Lc 标识数据域字节数

若为明文方式更新，Lc 为要写入数据的长度。

若为线路保护方式更新，Lc 为要写入数据的长度加 4 字节 MAC。

若为加密线路保护方式更新，Lc 为加密后数据的长度加 4 字节 MAC。

3.4.4 命令报文数据域

命令报文数据域包括要写入的新数据。
若为明文方式更新，则为要写入的数据。
若为线路保护方式更新，则为要写入的数据和 4 字节 MAC 码。
若为加密线路保护方式更新，则为加密后的数据和 4 字节 MAC 码。
用维护密钥加密数据和计算 MAC。

3.4.5 响应报文数据域

无

3.4.6 响应报文状态码

状态字(HEX)	描述
9000	正确执行
6E00	CLA 不支持
6700	长度错误
6581	Flash 操作失败
6981	文件类型不匹配
6982	权限不足
6983	密钥锁定
6984	未取随机数
6988	Mac 错误
6A82	文件不存在
6A84	文件偏移量超出
9403	密钥不存在

3.5 Read Binary（读二进制文件）

3.5.1 定义与范围

Read Binary 命令用于读取二进制文件内容（或部分内容）。

3.5.2 注意事项

Read Binary 命令只适用于二进制文件。
访问二进制文件的命令如下：
建立文件（Create File）
选择文件（Select File）
读二进制文件（Read Binary）/写二进制文件（Update Binary）
只有满足二进制文件读权限时才能执行此命令。

3.5.3 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	00/04	-
INS	1	B0	-
P1	1	XX	【说明 1】
P2	1	XX	【说明 1】
Lc	1	-	不存在（CLA=04 时除外）
DATA	XX	-	不存在（CLA=04 时，应包括 MAC）
Le	1	XX	要读取的数据长度

【说明 1:】
若 P1 的高三位为 100，则低 5 位为短文件标识符，P2 为偏移量。

P1								P2
b7	b6	b5	b4	b3	b2	b1	b0	
1	0	0	短文件标识符					文件偏移量

若 P1 的最高位不为 1，则 P1P2 为文件偏移量，所读的文件为当前文件。

P1								P2
b7	b6	b5	b4	b3	b2	b1	b0	
0	文件的偏移量							

3.5.4 命令报文数据域

一般情况下，命令报文数据域不存在。
当使用安全报文时，命令报文数据域中应包含 4 字节 MAC。
使用维护密钥加密数据和计算 MAC。

3.5.5 响应报文数据域

响应报文数据域由读取的数据组成。
若为明文方式读，则为读取的数据。
若为线路保护方式读，则为读取的数据和 4 字节 MAC。
若为加密线路保护方式读，则为加密后的数据和 4 字节 MAC 码。

3.5.6响应报文状态码

状态字(HEX)	描述
9000	正确执行
6E00	CLA 不支持
6700	长度错误
61XX	正确执行 XX 标识响应数据长度。 可用 Get Response 命令取回响应数据（仅用于 T=0）
6581	Flash 操作失败
6981	文件类型不匹配
6982	权限不足
6983	密钥锁定
6984	未取随机数
6988	Mac 错误
6A81	不支持此功能
6A82	文件不存在
6A84	文件偏移量超出
9403	密钥不存在

3.6 Read Record（读记录文件）

3.6.1 定义与范围

Read Record 命令用于读取记录文件的内容。

3.6.2 注意事项

Read Record 命令只适用于定长记录文件、循环记录文件、变长记录文件。
访问记录文件的命令如下：

建立文件（Create File）
选择文件（Select File）
读记录（Read Record
写记录（Update Binary）
增加记录（Append Record）

只有满足记录文件读权限时才能执行此命令。

3.6.3 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	00/04	-
INS	1	B2	-
P1	1	XX	记录个数/标识
P2	1	XX	引用控制参数【说明 1】
Lc	1	-	
DATA	XX	-	
Le	1	XX	‘00’

【说明 1】

命令报文中的引用控制参数

b7	b6	b5	b4	b3	b2	b1	b0	含义
X	X	X	X	X				SFI
					1	0	0	P1 为记录的个数

3.6.4 命令报文数据域

当无报文认证码(MAC)时，命令报文数据域不存在。
当有报文认证码(MAC)时，命令报文数据域包含 MAC。

3.6.5 响应报文数据域

响应报文数据域由读取的数据组成。

3.6.6 响应报文状态码

状态字(HEX)	描述
9000	指令执行成功
6E00	CLA 不支持
6700	长度错误
6581	Flash 操作失败
6981	文件类型不匹配
6982	权限不足
6983	密钥锁定
6988	Mac 错误
6A82	文件不存在
6A83	记录未找到
6A84	文件偏移量超出
6A86	P1P2 错误
6CXX	Le 长度错误
9403	密钥不存在

3.7 Update Record（写记录文件）

3.7.1 定义与范围

Update Record 命令用于添加记录或更改指定的记录。

对当前记录进行操作时，该命令执行成功后将重新设定记录指针。

3.7.2 注意事项

Update Record 命令适用于定长记录文件、变长记录文件和循环记录文件。

访问记录文件的命令如下：

建立文件（Create File）

选择文件（Select File）

读记录（Read Record）

写记录（Update Record）

增加记录（Append Record）

只有满足记录文件写权限时才能执行该命令。

对于变长记录文件，更新记录时，新记录长度必须与卡中原有记录长度相同，否则本次更新无效。

3.7.3 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	00/04	-
INS	1	DC	-
P1	1	XX	记录号或记录标识符（00 表示当前记录）
P2	1	XX	【说明 1】
Lc	1	XX	数据长度
DATA	XX	XXXX	添加的或更新原有记录的新纪录

【说明 1】

b7	b6	b5	b4	b3	b2	b1	b0	含义
X	X	X	X	X				SFI
					1	0	0	记录号在 P1 中给出
其余值								RFU

3.7.4命令报文数据域

命令报文数据域由新记录和报文认证码(MAC，4 字节）组成。

3.7.5 响应报文数据域

无

3.7.6 响应报文状态码

状态字(HEX)	描述
9000	指令执行成功
6E00	CLA 不支持
6700	长度错误
6581	Flash 操作失败
6981	文件类型不匹配
6982	权限不足
6983	密钥锁定
6984	未取随机数
6988	Mac 错误
6A82	文件不存在
6A83	记录未找到
6A84	文件偏移量超出
6A86	P1P2 错误
6A87	TLV Tag 已存在
6CXX	Le 长度错误
9403	密钥不存在

3.8 Append Record（增加记录）

3.8.1 定义与范围

Append Record 命令用于对变长记录文件、循环记录文件追加记录。

3.8.2 意事项

Append Record 命令适用于变长记录文件和循环记录文件。
访问记录文件的命令如下：
建立文件（Create File）
选择文件（Select File）
读记录（Read Record）
写记录（Update Record）
增加记录（Apend Record）
只有满足记录文件写权限时才能执行此命令。
若循环记录文件记录已满则覆盖最早写入的记录，且新增加记录的记录号总为 1。

3.8.3 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	00/04	-
INS	1	E2	-
P1	1	00	-
P2	1	XX	【说明 1】
Lc	1	XX	-
DATA	XX	XX…XX	写入的数据

【说明 1】
参数 P2 的含义

b7	b6	b5	b4	b3	b2	b1	b0	含义
X	X	X	X	X	0	0	0	B3-b7为短文件标识符
0	0	0	0	0	0	0	0	当前文件

3.8.4命令报文数据域

命令报文数据域由要追加的记录组成。
若为线路保护则由要追加的记录附上 4 字节 MAC 码组成。
若为线路加密保护则由被加密过的要追加的记录附上 4 字节 MAC 码组成。
用维护密钥加密数据和计算 MAC。

3.8.5 响应报文数据域

无

3.8.6 响应报文状态码

状态字(HEX)	描述
9000	指令执行成功
6E00	CLA 不支持
6700	长度错误
6581	Flash 操作失败
6981	文件类型不匹配
6982	权限不足
6983	密钥锁定
6984	未取随机数
6988	Mac 错误
6A82	文件不存在
6A83	记录未找到
6A84	文件偏移量超出
6A86	P1P2 错误
6A87	TLV Tag 已存在
6CXX	Le 长度错误
9403	密钥不存在

3.9 Verify PIN（验证口令）

3.9.1 定义与范围

Verify PIN 命令用于校验命令数据域的口令密钥正确性。

3.9.2 注意事项

在满足该口令密钥的使用权限时才可执行该命令。

3.9.3 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	00/04	-
INS	1	20	-
P1	1	00	-
P2	1	XX	口令密钥标识
Lc	1	02-08	-
DATA	XX	XX….XX	外部输入的口令密钥

【说明】

若口令验证成功，则安全状态寄存器的值被置成该密钥的后续状态，同时口令错误计数器被置成初始值。

若口令验证失败，则口令可试次数减 1，若口令已被锁死，则不能再执行该命令。

当口令已被锁死时，可用 UnblockPIN 命令对其进行解锁重装，修改原口令，同时口令错误计数器被恢复成初始值。

3.9.4 命令报文数据域

命令报文数据域由持卡者口令组成。

若为线路保护则由口令密钥附上 4 字节 MAC 码组成。

若为线路加密保护则由被加密的口令密钥附上 4 字节 MAC 码组成。

使用 ID = 01 的维护密钥加密口令和计算 MAC。

3.9.5 响应报文数据域

无

3.9.6 响应报文状态码

状态字(HEX)	意义
9000	正确执行
6E00	CLA 不支持
6700	长度错误
6283	口令密钥校验错误
63CX	还剩 X 此可试机会
6581	Flash 操作失败
6901	非应用目录
6981	不是口令密钥
6982	权限不足
6983	密钥锁定
6984	未取随机数
6988	Mac 错误
6A82	文件不存在
6A86	P1P2 错误
9302	密钥线路保护错误
9403	密钥未找到

3.10 Unblock/Change PIN（解锁\修改口令）

3.10.1 定义与范围

Unblock PIN 命令用于对锁死的 PIN 进行解锁操作。

3.10.2 注意事项

在满足口令解锁密钥的使用权限时才可执行该命令。
使用 ID = 01 的口令解锁密钥执行解锁操作。
若密钥解锁/重装成功，错误计时器回复初始值。
若口令解锁密钥可试次数为 0，则口令解锁密钥被锁死，不能再执行该命令。

3.10.3 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	84	-
INS	1	24	-
P1	1	00	-
P2	1	XX	要解锁的口令密钥标识
Lc	1	XX	-
DATA	XX	XX….XX	

3.10.4 命令报文数据域

由加密后的新密钥和 4 字节 MAC 码组成。

3.10.5 响应报文数据域

无

3.10.6 响应报文状态码

状态字(HEX)	描述
9000	指令执行成功
6E00	CLA 不支持
6700	长度错误
63CX	还剩 X 此可试机会
6581	Flash 操作失败

6901	非应用目录
6982	权限不足
6983	密钥锁定
6984	未取随机数
6988	Mac 错误
6A80	密钥过长
6A82	文件不存在
6A86	P1P2 错误
9302	密钥线路保护错误
9403	密钥不存在

3.11 External Authentication（外部认证）

3.11.1 定义与范围

外部认证命令使用指定的外部认证密钥实现。
执行前必须先取 8/16 字节随机数。

3.11.2 注意事项

在满足该外部认证密钥的使用权限且该密钥未被锁死时才可执行该命令。
根据指定外部认证密钥的算法标识采用不同的加密算法。

3.11.3 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	00	-
INS	1	82	-
P1	1	00	-
P2	1	XX	外部认证密钥标识
Lc	1	8/16	-
DATA	8/16	XX…XX	

3.11.4 命令报文数据域

指定外部认证密钥加密后的 8/16 字节随机数密文。

3.11.5 响应报文数据域

无

3.11.6 响应报文状态码

状态字(HEX)	描述
9000	指令正确执行
6700	长度错误
63CX	还剩 X 此可试机会
6581	Flash 操作失败
6982	权限不足
6983	密钥锁定

6984	未取随机数或随机数长度不符
6985	卡片锁定
6A82	未找到 key 文件
6A86	P1 P2 错
9403	密钥不存在

3.12 Internal Authentication（内部认证）

3.12.1 定义与范围

内部认证指令根据内部认证密钥的算法标识，采取不同的加密算法对输入的 8/16 字节数据进行加密。

3.12.2 注意事项

必须满足内部认证密钥的使用权限。

3.12.3 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	00	-
INS	1	88	-
P1	1	00	-
P2	1	XX	内部认证密钥标识
Lc	1	8/16	-
DATA	8/16	XX…XX	

3.12.4 命令报文数据域

8/16 字节待加密数据，数据长度必须等于待使用密钥对应算法的分组长度。

3.12.5 响应报文数据域

无

3.12.6 响应报文状态码

状态字(HEX)	描述
9000	指令正确执行
6E00	CLA 错误
6700	长度错误
61XX	指令正确执行，需要通过 GetResponse 指令读取 XX 个字节的数据。
6982	权限不足

6983	密钥锁定
6A82	未找到 key 文件
6A86	P1P2 错
9403	密钥不存在

3.13 Get Response（取响应数据）

3.13.1 定义与范围

当 APDU 不能用现有协议传输时，Get Response 命令提供了一种从模块向接口设备传送 APDU（或 APDU 的一部分）的传输方法。

3.13.2 注意事项

此命令只用于 T=0 通讯协议。

3.13.3 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	00	-
INS	1	C0	-
P1	1	00	-
P2	1	00	-
Le	1	XX	期望响应数据的长度

3.13.4 命令报文数据域

无

3.13.5 响应报文数据域

响应报文数据域的长度由 Le 的值决定。

3.13.6 响应报文状态码

状态字(HEX)	描述
9000	正确执行
6E00	CLA 不支持
6700	长度错误（Le 大于卡中响应数据长度）
61xx	正确执行，XX 标识剩余数据长度。 （仅用于 T=0）
6A86	P1P2 错误
6CXX	Le 长度错误
6F00	卡中无数据可返回

3.14 Get Randnum（取随机数）

3.14.1 定义与范围

Get Randnum 命令用于请求一个用于安全相关过程（如安全报文）的随机数。

3.14.2 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	00	-
INS	1	84	-
P1	1	00	-
P2	1	00	-
Le	1	04/08/10	要求模块返回的随机数长度

3.14.3 命令报文数据域

无

3.14.4 响应报文数据域

响应报文数据域包括请求的随机数，长度为 Le 个字节。

3.14.5 响应报文状态码

状态字(HEX)	描述
9000	正确执行
6E00	CLA 不支持
6A86	P1P2 错误

3.15 Application Block（应用锁定）

3.15.1 定义与范围

Application Block命令使当前选择的应用失效。

使用ID = 00的维护密钥计算MAC。

3.15.2 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	84	-
INS	1	1E	-
P1	1	00	-
P2	1	00/01	【说明 1】
Lc	1	04	MAC
DATA	04	XX…XX	4 字节 MAC 值

【说明 1】

参数 P2 说明

00	临时锁定，应用锁定后可由 Application unblock 指令解锁
01	应用永久锁定，应用锁定后不可由 Application unblock 指令解锁

3.15.3 命令报文数据域

命令报文数据域包括报文鉴别码（MAC）数据元。

3.15.4 响应报文数据域

无

3.15.5 响应报文状态码

状态字(HEX)	描述
9000	正确执行
6E00	CLA 错误
6700	长度错误
6982	权限不足
6983	密钥锁定
6984	未取随机数

6988	Mac 错误
6A81	不支持此功能
6A82	文件不存在
6A86	P1P2 错误
9403	密钥不存在

3.16 Application Unblock（应用解锁）

3.16.1 定义与范围

Application UnBlock命令用于恢复被临时锁定的应用。

使用ID = 00的维护密钥计算MAC。

3.16.2 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	84	-
INS	1	18	-
P1	1	00	-
P2	1	00	-
Lc	1	04	-
DATA	04	XX…XX	4 字节 MAC 值

3.16.3 命令报文数据域

命令报文数据域包括报文鉴别码（MAC）数据元。

3.16.4 响应报文数据域

无

3.16.5 响应报文状态码

状态字(HEX)	描述
9000	正确执行
6E00	CLA 错误
6700	长度错误
6581	Flash 操作失败
6982	权限不足
6983	密钥锁定
6984	未取随机数
6985	应用永久锁定
6988	安全报文认证码(MAC)错误
6A81	不支持此功能

6A82	文件不存在
6A86	P1P2 错误
9303	应用永久锁定
9403	密钥不存在

3.17 Generate Key Pair(SM2)（生成密钥对）

3.17.1 定义与范围

Generate Key Pair(SM2)命令用于生成 SM2 密钥对。

3.17.2 注意事项

需要满足数据域中指定的公私钥文件的修改权限。

3.17.3 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	36	-
P1	1	00	-
P2	1	00	-
Lc	1	04	-
DATA	XX	XX…XX	公钥 ID+私钥 ID

3.17.4 命令报文数据域

命令报文数据域由 2 字节公钥 ID 和 2 字节私钥 ID 组成。
当公钥 ID 为 0x0000 时，公钥可以通过 Get Response 指令取回。

3.17.5 响应报文数据域

无。

3.17.6 响应报文状态码

状态字(HEX)	描述
9000	正确执行
6E00	CLA 不支持
6700	长度错误
61XX	需要通过 Get Response 指令取回的公钥数据
6581	Flash 操作失败
6981	文件类型不匹配

6982	权限不足
6A82	文件不存在
6A86	P1P2 错误

3.18 Data Encrypt(SM2)(公钥加密数据)

3.18.1 定义与范围

使用指定的卡片内公钥或者外部传入的公钥对数据进行非对称(SM2 算法)加密。
使用内部公钥时，需要满足公钥文件的使用权限。

3.18.2 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	4C	-
P1	1	XX	P1P2 大数据传输控制字，见【说明 1】
P2	1	XX	
Lc	1	XX	公钥和待加密数据长度总和
DATA	XX	XX…XX	公钥和待加密数据

【说明 1】

P1P2 传输控制字说明

B8	B7	B6	B5	B4	B3	B2	B1	B8	B7	B6	B5	B4	B3	B2	B1	含义
0	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	首块
X	x	1	1	1	1	1	1	1	1	1	1	1	1	1	1	有后续块
X	X	数据总长度（不全为 1 时，则为最后一块数据）														最后一块

3.18.3 命令报文数据域

报文数据域由公钥文件 ID（2 字节）+(公钥)+待加密数据组成。

- 当公钥文件 ID = 0x0000 时
  数据域 =公钥文件 ID（2 字节）+公钥(64 字节) +待加密数据
- 当公钥文件 ID != 0x0000 时
  数据域 = 公钥文件 ID（2 字节）+待加密数据

注：待加密数据长度要小于等于 128 字节。

3.18.4 响应报文数据域

响应报文为公钥加密(SM2)后的密文，密文格式为：C1（X，Y）+C3（Hash）+ C2。
响应报文通过 Get Response 命令取回。

3.18.5 响应报文状态码

状态字(HEX)	描述
9000	正确执行
6E00	CLA 不支持
6700	长度错误
61XX	需要通过 Get Response 指令取回的密文
6981	文件类型不匹配
6982	权限不足
6A82	文件不存在
6A84	数据接收缓冲区超限
6A86	P1P2 错误

3.19 Data Decrypt(SM2)(数据解密 SM2)

3.19.1 定义和范围

Data Decrypt 命令用于非对称国密算法(SM2)的私钥解密。
使用内部私钥时，需满足私钥文件的使用权限。

3.19.2 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	4E	-
P1	1	XX	P1P2 大数据传输控制字，见【说明 1】
P2	1	XX	
Lc	1	XX	私钥和待解密数据长度总和
DATA	XX	XX…XX	私钥和待解密数据

【说明 1】

P1P2 传输控制字说明

B8	B7	B6	B5	B4	B3	B2	B1	B8	B7	B6	B5	B4	B3	B2	B1	含义
0	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	首块
X	x	1	1	1	1	1	1	1	1	1	1	1	1	1	1	有后续块
X	X	数据总长度（不全为 1 时，则为最后一块数据）														最后一块

3.19.3 命令报文数据域

报文数据域由私钥文件 ID（2 字节）+(私钥)+待解密数据组成。
当私钥文件 ID = 0x0000 时（外部传入私钥解密）
数据域 =私钥文件 ID（2 字节）+ 私钥(32 字节) + 待解密数据
当私钥文件 ID != 0x0000 时
数据域 =私钥文件 ID（2 字节）+ 待解密数据

注：待解密数据格式为
C1（X，Y）+ C3（Hash）+ C2。

3.19.4 响应报文数据域

非对称密钥（SM2）解密后的明文。
响应报文通过 Get Response 命令取回。

3.19.5 响应报文状态码

状态字(HEX)	描述
9000	数据正确接受
6E00	CLA 不支持
6700	长度错误
61XX	需要通过 Get Response 指令取回解密后的明文
6981	文件类型不匹配
6982	权限不足
6A80	输入数据格式错误
6A82	文件不存在
6A84	数据接收缓冲区超限
6A86	P1P2 错误

3.20 Data Verify(SM2)（公钥验签）

3.20.1 定义与范围

使用指定的卡片内公钥或者外部传入的公钥对数据进行（SM2 算法）签名验签。
使用内部公钥时，需要满足公钥文件的使用权限。

3.20.2 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	48	-
P1	1	00	
P2	1	00	
Lc	1	62/A2	
DATA	XX	XX…XX	公钥 ID(2Byte)+(公钥)+签名后的数据+原始数据

3.20.3 命令报文数据域

报文数据域由公钥文件 ID（2 字节）+公钥(64 字节)+签名后的值（64 字节）+原始数据。

当公钥文件 ID = 0x0000 时，数据域 = 公钥文件 ID（2 字节）+ 公钥(64 字节) + 签名后的值（64 字节）+ 签名前数据(32 字节)组成

当公钥文件 ID != 0x0000 时，数据域 = 公钥文件 ID（2 字节）+ 签名后的值(64 字节) + 签名前数据(32 字节)组成

3.20.4 响应报文数据域

无

3.20.5 响应报文状态码

状态字(HEX)	描述
9000	正确执行
6E00	CLA 不支持
6700	长度错误
6881	验签失败
6981	文件类型不匹配
6982	权限不足

6A82	文件不存在
6A84	数据接收缓冲区超限
6A86	P1P2 错误

3.21 Data Sign(SM2)（私钥签名）

3.21.1 定义与范围

使用指令的卡片内私钥或者外部传入的私钥对数据进行（SM2 算法）签名。
使用内部私钥时，需要满足私钥文件的使用权限。

3.21.2 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	4A	-
P1	1	00	
P2	1	00	
Lc	1	22	
DATA	XX	XX…XX	私钥文件 ID(2Byte)待签名数据

3.21.3 命令报文数据域

数据域 = 私钥文件 ID（2 字节）+ 待签名数据（32 字节）

3.21.4 响应报文数据域

签名值。响应报文通过 Get Response 命令取回。

3.21.5 响应报文状态码

状态字(HEX)	描述
9000	正确执行
6E00	CLA 不支持
6700	长度错误
61xx	正确执行 XX 标识剩余数据长度（仅用于 T=0）
6981	文件类型不匹配
6982	权限不足
6A82	文件不存在
6A84	数据接收缓冲区超限
6A86	P1P2 错误

3.22 Import (SM2) Key（导入 SM2 非对称密钥）

3.22.1 定义与范围

本指令可以将 SM2/RSA 公私钥导入到指定的密钥文件中。

3.22.2 注意事项

需要满足密钥文件写权限时才能执行此命令。
本指令支持：非对称公钥（类型：0x3D）,非对称私钥（类型：0x3C）

3.22.3 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	80/84	-
INS	1	38	-
P1	1	XX	【说明 1】
P2	1	XX	【说明 1】
Lc	1	XX	【说明 2】
DATA	XX	XX…XX	导入密钥数据

【说明 1】

若 P1 的高三位为 100，则低 5 位为短文件标识符，P2 为文件偏移量。

P1								P2
b7	b6	b5	b4	b3	b2	b1	b0	
1	0	0	短文件标识符					文件偏移量

若 P1 的最高位不为 1，则 P1P2 为文件偏移量，导入文件为当前文件。

P1								P2
b7	b6	b5	b4	b3	b2	b1	b0	
0	文件偏移量							

【说明 2】

Lc 标识命令报文数据域字节数。

若为明文导入方式，Lc 为导入密钥数据的字节数。

若为线路保护导入方式，Lc 为导入密钥数据长度+4 字节 MAC。

若为加密线路保护导入方式，Lc 为加密后导入密钥数据的长度+4 字节 MAC。

3.22.4 命令报文数据域

命令报文数据域包括导入密钥数据。

若为明文导入方式，则为导入密钥数据。
若为线路保护导入方式，则为导入密钥数据和 4 字节 MAC 码。
若为加密线路保护导入方式，则为加密的导入密钥数据和 4 字节 MAC 码。
用维护密钥加密数据和计算 MAC。

3.22.5 响应报文数据域

无

3.22.6 响应报文状态码

状态字(HEX)	描述
9000	正确执行
6E00	CLA 不支持
6700	长度错误
6581	Flash 操作失败
6981	文件类型不匹配
6982	权限不足
6983	密钥锁定
6984	未取随机数
6A82	文件不存在
6A84	文件偏移量超出
6A86	P1P2 错误

3.23 Export（SM2）Key（导出 SM2 非对称密钥）

3.23.1 定义与范围

本指令可以将 SM2/RSA 的公私钥以明文方式或者线路保护方式导出卡片。
线路保护方式由密钥文件的线路保护属性决定。

3.23.2 注意事项

需要满足密钥文件的读取权限。

3.23.3 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	80/84	-
INS	1	3A	-
P1	1	XX	【说明 1】
P2	1	XX	【说明 1】
Lc	1	-	不存在（CLA=04 时除外）
DATA	XX	-	不存在（CLA=04 时，应包括 MAC）
Le	1	XX	要读取的密钥长度

【说明 1】

若 P1 的高三位为 100，则低 5 位为短文件标识符，P2 为偏移量

P1								P2
b7	b6	b5	b4	b3	b2	b1	b0	
1	0	0	短文件标识符					文件偏移量

若 P1 的最高位不为 1，则 P1P2 为文件偏移量，要导出的文件为当前文件。

P1								P2
b7	b6	b5	b4	b3	b2	b1	b0	
0	文件偏移量							

3.23.4 命令报文数据域

一般情况下，命令报文数据域不存在。
当使用安全报文时，命令报文数据域应包含 MAC。
用维护密钥加密数据和计算 MAC。

3.23.5 响应报文数据域

响应报文数据域由导出密钥数据组成。
若为明文导出方式，则为导出密钥数据。
若为线路保护导出方式，则为导出密钥数据和 4 字节 MAC。
若为加密线路保护导出方式，则为被加密导出密钥数据和 4 字节 MAC。

3.23.6 响应报文状态码

状态字(HEX)	描述
9000	正确执行
6E00	CLA 不支持
6700	长度错误
61xx	正确执行 XX 标识响应数据长度。 可用 Get Response 命令取回响应数据（仅用于 T=0）
6581	Flash 操作失败
6981	文件类型不匹配
6982	权限不足
6983	密钥锁定
6984	未取随机数
6988	Mac 错误
6A81	不支持此功能
6A82	文件不存在
6A84	文件偏移量超出
6CXX	Le 长度错误
9403	密钥不存在

3.24 Generate Key Pair(RSA)（生成密钥对）

3.24.1 定义与范围

生成 RSA 密钥对。

3.24.2 注意事项

需要满足报文数据域中指定的公私钥文件的写权限。

3.24.3 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	B6	-
P1	1	00	
P2	1	00	00：RSA-2048 80：RSA-1024（可选）
Lc	1	04	-
DATA	XX	XX…XX	公钥 ID+私钥 ID

3.24.4 命令报文数据域

命令报文数据域由 2 字节公钥 ID 和 2 字节私钥 ID 组成。

当公钥 ID 为 0x0000 时，公钥不写入公钥文件，而是直接返回，可通过 Get Response 指令取回。

3.24.5 响应报文数据域

当公钥 ID 为 0x0000 时，为公钥数据，可通过 Get Response 指令取回。

当公钥 ID 不为 0x0000 时，无响应数据。

3.24.6 响应报文状态码

状态字(HEX)	描述
9000	正确执行
6E00	CLA 不支持
6700	长度错误
61XX	需要通过 Get Response 指令取回的公

	钥数据
6981	文件类型不匹配
6982	权限不足
6581	Flash 操作失败
6A82	文件不存在
6A84	密钥文件空间不足
6A86	P1P2 错误

3.25 Data Encrypt(RSA)（RSA 公钥加密数据）

3.25.1 定义与范围

使用指定的卡片内公钥或者外部传入的公钥对数据进行非对称(RSA1024/2048 算法)加密或验签。支持对 1K 数据做运算。

使用内部公钥时，需要满足公钥文件的使用权限。

3.25.2 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	CC	-
P1	1	XX	P1P2 大数据传输控制字，见【说明 1】
P2	1	XX	
Lc	1	XX	公钥和待加密数据长度总和
DATA	XX	XX…XX	公钥和待加密数据

【说明 1】

P1P2 传输控制字说明

B7	B6	B5	B4	B3	B2	B1	B0	B7	B6	B5	B4	B3	B2	B1	B0	含义
0		1	1	1	1	1	1	1	1	1	1	1	1	1	1	首块数据
X		1	1	1	1	1	1	1	1	1	1	1	1	1	1	中间块数据
X		数据总长度（不全为 1 时，则为最后一块数据）														最后一块数据

3.25.3 命令报文数据域

报文数据域由公钥文件 ID（2 字节）+【公钥长度（2 字节）+公钥模数 N】+待加密数据组成。

当公钥文件 ID = 0x0000 时

数据域 =公钥文件 ID（2 字节）+公钥长度（2 字节）+公钥模数 N + 待加密数据

当公钥文件 ID != 0x0000 时

数据域 =公钥文件 ID（2 字节）+ 待加密数据

在加密时，将被加密数据按照长度 n-11 字节分包（n 为公钥模畅），最后一包长度应小于或等于 n-11，然后每包数据按照 PKCS#1 规范方式填充后使用公钥加密。

3.25.4 响应报文数据域

当为公钥加密时，响应报文为公钥加密(RSA)后的密文。

当为签名验签时，响应报文为验签结果，即签名的原始数据。
响应数据可通过 Get Response 指令取回。

3.25.5 响应报文状态码

状态字(HEX)	描述
9000	正确执行
6E00	CLA 不支持
6700	长度错误
61XX	需要通过 Get Response 指令取回的密文
6300	编解码失败
6981	文件类型不匹配
6982	权限不足
6A80	数据长度不匹配
6A84	数据接收缓冲区超限
6A86	P1P2 错误

3.26 Data Decrypt(RSA)(RSA 数据解密)

3.26.1 定义和范围

Data Decrypt 命令用于使用指定的卡片内私钥进行非对称算法(RSA1024)解密签名。需满足内部私钥文件的使用权限。

3.26.2 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	CE	-
P1	1	00	P1P2 大数据传输控制字
P2	1	00	
Lc	1	XX	私钥和待解密数据长度总和
DATA	XX	XX…XX	私钥和待解密数据

3.26.3 命令报文数据域

当为私钥解密操作时，命令报文数据域由私钥文件 ID（2 字节）和待解密数据组成。私钥文件 ID 不为 0。

3.26.4 响应报文数据域

当为私钥解密操作时，响应报文数据域为解密后的值。

3.26.5 响应报文状态码

状态字(HEX)	描述
9000	数据正确接受
6E00	CLA 不支持
6700	长度错误
61XX	需要通过 Get Response 指令取回解密后的明文
6300	编解码失败
6981	文件类型不匹配
6982	权限不足
6A80	输入数据格式错误
6A82	文件不存在
6A84	数据接收缓冲区超限
6A86	P1P2 错误
6A88	解密签名失败

3.27 Import Session key(公钥 SM2 导入对称密钥)

3.27.1 定义与范围

Import Session key 使用非对称算法的公钥对对称密钥加密后导入卡片内部，成功导入后可以通过（Session Oper）指令，根据不同的算法标识调用不同的对称算法对输入的数据进行加密/解密以及计算 MAC。

3.27.2 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	3C	-
P1	1	XX	P1P2，私钥 ID
P2	1	XX	
Lc	1	XX	数据域字节数
DATA	XX	XX…XX	

3.27.3 命令报文数据域

P1P2! = 0x0000

对称算法标识+密钥类型+公钥加密后的对称密钥密文（SM2 加密固有 96 字节密文+对称密钥密文）+密钥校验值

对称算法标识如下：

对称算法标识	HEX 值
3DES	0x00
SM4	0x04

密钥类型如下：

密钥类型	HEX 值
工作密钥	0x00
Mac 密钥	0x01

密钥校验值为密钥明文用对称算法标识指定的对称算法对一个全零数据块加密所得结果的前 8 字节数据。

3.27.4 响应报文数据域

无

3.27.5 响应报文状态码

状态字(HEX)	描述
9000	正确执行
6E00	CLA 不支持
6981	文件类型不匹配
6982	私钥使用权限不足
6A80	密钥长度错误
6A81	密钥校验失败
6A82	文件不存在
6A83	密钥类型错误

3.28 Export Session key(公钥 SM2 导出对称密钥)

3.28.1 定义与范围

Export Session key 根据外部传入的对称算法标识，生成对称密钥并通过外部传入公钥或者卡片内部公钥加密并导出。成功导出后可以通过（3.31 Session Oper）指令对输入的数据进行加密/解密以及计算 MAC。

3.28.2 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	3E	-
P1	1	XX	P1P2，公钥 ID，为 0x0000 时，采用外部传入公钥。
P2	1	XX	
Lc	1	XX	DATA 长度
DATA	XX	XX…XX	算法标识+密钥类型+（公钥）

3.28.3 命令报文数据域

P1P2 = 0x0000

算法标识 + 密钥类型 + 公钥

P1P2 != 0x0000：

算法标识 + 密钥类型

对称算法标识如下：

对称算法标识	HEX 值
3DES	0x00
SM4	0x04

密钥类型如下：

密钥类型	HEX 值
工作密钥	0x00
Mac 密钥	0x01

3.28.4 响应报文数据域

无

3.28.5 响应报文状态码

状态字(HEX)	描述
9000	指令执行成功
6E00	CLA 不支持
6700	长度错误
61XX	通过 Get Response 指令回去对称密钥密文
6981	文件类型不匹配
6982	权限不足
6A80	数据内容错误
6A82	文件不存在

3.29 Import Session key(公钥 RSA 导入对称密钥)

3.29.1 定义与范围

Import Session key 使用非对称算法的公钥对对称密钥加密后导入卡片内部，成功导入后可以通过（3.33 Session Oper）指令，根据不同的算法标识调用不同的对称算法对输入的数据进行加密/解密以及计算 MAC。

3.29.2 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	BC	-
P1	1	XX	Bit8 bit7: 00 唯一一包 01 第一包 10 中间包 11 最后一包
P2	1	XX	私钥文件短文件标识符
Lc	1	XX	数据域字节数
DATA	XX	XX…XX	

3.29.3 命令报文数据域

P1P2 = 0x0000

对称算法标识+密钥类型+私钥+公钥加密后的对称密钥密文+密钥校验值

P1P2! = 0x0000

对称算法标识+密钥类型+公钥加密后的对称密钥密文+密钥校验值

对称算法标识如下：

对称算法标识	HEX 值
3DES	0x00
SM4	0x04

密钥类型如下：

密钥类型	HEX 值
工作密钥	0x00
Mac 密钥	0x01

密钥校验值为密钥明文用对称算法标识指定的对称算法对一个全零数据块加密所得结果的前 8 字节数据。

3.29.4 响应报文数据域

无

3.29.5 响应报文状态码

状态字(HEX)	描述

9000	正确执行
6E00	CLA 不支持
6981	文件类型不匹配
6982	私钥使用权限不足
6A80	密钥长度错误
6A81	密钥校验失败
6A82	文件不存在
6A83	密钥类型错误

3.30 Export Session key(公钥 RSA 导出对称密钥)

3.30.1 定义与范围

Export Session key 根据外部传入的对称算法标识，生成对称密钥并通过外部传入公钥或者卡片内部公钥加密并导出。成功导出后可以通过（3.33 Session Oper）指令对输入的数据进行加密/解密以及计算 MAC。

3.30.2 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	BE	-
P1	1	XX	Bit8 bit7: 00 唯一一包 01 第一包 10 中间包 11 最后一包
P2	1	XX	非 00：公钥文件的短文件标识符 00：公钥由命令报文传入
Lc	1	XX	DATA 长度
DATA	XX	XX…XX	

3.30.3 命令报文数据域

P1P2 = 0x0000

算法标识 + 密钥类型 + 公钥

P1P2 != 0x0000：

算法标识 + 密钥类型

对称算法标识如下：

对称算法标识	HEX 值
3DES	0x00
SM4	0x04

密钥类型如下：

密钥类型	HEX 值
工作密钥	0x00

Mac 密钥	0x01

3.30.4 响应报文数据域

无

3.30.5 响应报文状态码

状态字(HEX)	描述
9000	指令执行成功
6E00	CLA 不支持
6700	长度错误
61XX	通过 Get Response 指令回去对称密钥密文
6981	文件类型不匹配
6982	权限不足
6A80	数据内容错误
6A82	文件不存在

3.31 Session Oper(对称密钥加密、解密、MAC 计算)

3.31.1 定义与范围

Session Oper 使用 Import Session Key 或者 Export Session key 指令导入或者生成的会话密钥，来对数据进行加密、解密、计算 MAC。

3.31.2 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	EA	-
P1	1	XX	算法控制字,见【说明 1】
P2	1	00	
Lc	1	XX	-
DATA	XX	XX…XX	数据

【说明 1】

P1 应用控制参数说明

BIT7	BIT6	BIT5	BIT4	BIT3	BIT2	BIT1	BIT0	含义
				0	0	0	0	加密，唯一块
				0	0	1	0	解密，唯一块
				0	0	0	1	计算 MAC，唯一块
				0	1	0	1	计算 MAC，最后一块
				1	0	0	1	计算 MAC，首块，有后续块
				1	1	0	1	计算 MAC，中间块，有后续块

3.31.3 命令报文数据域

1、 加解密数据必须是算法分组长度的整数倍
2、 加解密数据由应用自行分包和填充
3、 计算 MAC 时，数据域由初始向量（16 字节）+实际数据组成
4、 计算 MAC 时，由芯片自动填充，填充方法与安全报文的 MAC 填充规则一致，数据尾强制填充 0x80 00^00 直至算法分组唱的的整数倍
5、 计算 MAC 分包时，非最后一块的数据必须是算法分组长度的整数倍

3.31.4 响应报文数据域

加密解密：加解密结果。
MAC 计算：MAC。

3.31.5 响应报文状态码

状态字(HEX)	描述
9000	指令执行成功
6E00	CLA 不支持
6700	长度错误
61XX	通过 Get Response 获取相应数据
6901	会话密钥类型错误
6986	P1P2 错误
6A86	P1P2 错误

3.32 Hash Asymc（摘要&签名/验签）

3.32.1 定义与范围

对输入数据做摘要操作和签名验签操作。

3.32.2 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	EC	-
P1	1	XX	00：计算 Hash，返回 Hash 结果 01：计算 Hash&签名，返回 Hash&签名结果 02：计算 Hash&验签，返回 Hash&验签结果 其他：保留
P2	1	XX	Bit1 bit0： 00 SHA1+RSA（可选） 01 SHA224+RSA（可选） 10 SHA256+RSA 11 SM3+SM2 Bit7 bit6: 00 唯一一包 01 第一包 10 中间包 11 最后一包
Lc	1	XX	-
DATA	XX	XX….XX	要处理的数据
Le	1	00	-

3.32.3 命令报文数据域

1、 P1 为 0 时，数据域为待 HASH 数据，有 P2 指定 HASH 算法
2、 P1 为 1 而 P2 选择非 SM3+SM2 算法时，数据域由私钥文件 ID（2 字节）+待签名数据组成
3、 P1 为 1 而 P2 选择 SM3+SM2 算法时，数据域由私钥文件 ID（2 字节）+公钥文件 ID（2 字节）+用户身份标识长度（1 字节）+用户身份标识（n 字节）+待签名数据组成
4、 P1 为 2 而 P2 选择非 SM3+SM2 算法时，数据域由公钥文件 ID（2 字节）+待验签数据组成
5、 P2 为 2 而 P2 选择 SM3+SM2 算法时，数据域由公钥文件 ID（2 字节）+用户身份标识长度（1 字节）+用户身份标识（n 字节）+签名后的值（64 字节）+待验签数据组成

3.32.4 响应报文数据域

P1=00：计算 Hash，返回 Hash 结果；

P1=01：对输入待签名数据做哈希，再对哈希结果做签名，返回 Hash 值和签名值。

P1=02：对输入待验签数据做哈希，再对输入的签名值和计算的哈希值做验签，如果操作失败，返回状态码，成功则返回 Hash 结果。

3.32.5 响应报文状态码

状态字(HEX)	描述
9000	本次指令执行成功
6E00	CLA 不支持
6700	长度错误
61xx	正确执行 XX 标识剩余数据长度（仅用于 T=0）
6881	验签失败
6981	文件类型不匹配
6A82	文件不存在
6A84	数据接收缓冲区超限
6A86	P1P2 错误

3.33 GenP10Req（生成 PKCS#10 请求）

3.33.1 定义与范围

根据输入的 CN、C、OU、O 和公私钥文件 ID 生成 PKCS#10 请求。

3.33.2 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	EE	-
P1	1	00	-
P2	1	Xx	00：HEX 编码格式 01：BASE64 编码格式
Lc	1	XX	-
DATA	XX	XX…XX	公私钥文件 ID 和 CN、C、O、OU 信息
Le	1	00	不存在

3.33.3 命令报文数据域

公钥文件 ID(2B) + 私钥文件 ID（2B） + CN、C、O、OU 等字段。

- 字段说明

目前只支持 CN、OU、C 和 O 字段，命令中可以出现的字段不限，可以都出现，也可以都不出现。如都不出现，则数据域为：公钥文件 ID(2B)+私钥文件 ID（2B）。

3.33.4 响应报文数据域

PKCS#10 请求数据

SM2 公钥使用 SM3-With-SM2 签名

RSA1024 公钥使用 SHA-With-RSA 签名

RSA2048 公钥使用 SHA256-With-RSA 签名

3.33.5 响应报文状态码

状态字(HEX)	描述
9000	执行成功
6E00	CLA 不支持
6700	长度错误

61xx	正确执行 XX 标识剩余数据长度（仅用于 T=0）
6981	文件类型不匹配
6982	权限不满足
6A82	文件不存在
6A84	文件空间不足
6A86	P1P2 错误

3.34 GetSN（获取芯片序列号）

3.34.1 定义与范围

获取 4 字节芯片序列号。本命令在任何时候均可正确返回。

3.34.2 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	F6	-
P1	1	00	-
P2	1	03	-
Lc	1	00	不存在
DATA	XX	XX….XX	不存在
Le	1	04	

3.34.3 命令报文数据域

无。

3.34.4 响应报文数据域

4 字节芯片序列号，厂商唯一的芯片序列号。

3.34.5 响应报文状态码

状态字(HEX)	描述
9000	执行成功
6E00	CLA 不支持
6C04	长度不为 04，需重新发送指令且长度为 04
6A86	P1P2 错误

4 安全报文传输方式

4.1 安全报文传送概念

安全报文传送的目的是保证数据的完成性、机密性和对发送方的认证。数据的机密性是通过对数据域的加密来得到保证;数据的完成性和对发送方的认证是通过使用安全报文鉴别码来实现的。

4.2 如何实现安全报文传送

4.2.1 文件

二进制文件、定长记录文件、变长记录文件、循环记录文件、公钥文件、私钥文件、秘钥(对称秘钥)文件都可以采用安全报文传送。如对上述文件进行安全报文传送。在创建文件时，需要设置数据域的第 6 个字节，

创建文件 BYTE6 字节说明

BIT7	BIT6	BIT5	BIT4	BIT3	BIT2	BIT1	BIT0	描述
				读出控制		写入控制		
						0	0	文明写入
						1	0	明文+MAC 写入
						1	1	密文+MAC 写入
				0	0			明文读出
				1	0			明文+MAC 读出
				1	1			密文+MAC 读出

4.2.2 对称秘钥

秘钥在写入时，如果选择安全报文方式只能是密文+MAC 写入或者更新。

- 写入时，遵循 3.2 中的描述，不支持导出操作。
- 更新时，需要在安装密钥时改变秘钥类型字节的高两位即可。

BIT7	BIT6	BIT5	BIT4	BIT3	BIT2	BIT1	BIT0	描述
1	1	秘钥类型						密文+MAC 更新

4.3 安全报文以及鉴别码（MAC）的计算

详见：中国金融集成电路（IC）卡规范相关内容。

5 复位应答

在由终端发出复位信号以后，IC卡以一串字节作为应答（即复位应答）。
卡片通讯速率默认为9600bps。

- 这些传输到终端的字节规定了卡和终端之间即将建立的通信特性。
- SIMLINKER ESAM嵌入式安全模块的复位信息完全符合ISO7816规范。

SIMLINKER ESAM嵌入式安全模块支持T=0通讯协议，复位应答信息如下表所示。

符号	值(Hex)	说明	长度（Byte）
TS	3B	正向约定，首先传送的是字符最低有效位	1
T0	9B	TA1 和 TD1 存在，历史字符为 11 个	1
TA1	18	指定 Fi 和 Di	1
TD1	40	TC2 存在，指定首选协议 T0	1
TC2	60	指定等待时间整数 WI	1
T1-TB	XX	历史字节	11

历史字符如下表所示。

符号	值(Hex)	意义
T1	‘P’(‘50’)	COS 厂商代码（PS 代表芯凌）
T2	‘S’(‘53’)	
T3-T4	‘P’ + XX	芯片型号代码（P81 代表 HSC08K1）
T5	XX	FF
T6-T7	XXXX	COS 版本号（1B）+应用版本号（1B） “3221”代表 COS 版本号为 3.2，应用版本号为 2.1（即遵循规范版本号为 2.1）
T8-TB	6X…XX	序列号