Simlinker 密钥 KEY
用户手册

北京芯凌科技有限公司

北京芯凌科技有限公司

Beijing Simlinker Tech Co., LTD

目录

北京华大信安科技有限公司

北京卓微科技有限公司

北京兆芯科技有限公司

北京芯凌科技有限公司

1. 关于本手册

1.1 内容概述

本手册各部分内容概述如下：

♦ Simlinker 密钥KEY 简介

本章介绍了Simlinker 密钥KEY 的特点及体系结构，使您对Simlinker 密钥KEY 有一个初步的了解。

♦ Simlinker 密钥KEY 文件管理

本章从文件组织结构、文件格式、文件访问方式及各种类型文件的特点来详细描述了Simlinker 密钥KEY 的文件管理系统。

♦ Simlinker 密钥KEY 的安全体系

安全体系是Simlinker 的核心部分，它涉及到卡的鉴别与核实，对文件访问时的权限控制机制。本章从安全状态、安全属性、安全机制和密码算法四个方面详细描述了Simlinker 密钥KEY 的安全体系。

♦ 命令与应答

本章描述了命令与应答结构及命令返回状态码SW1SW2 的意义。

♦ Simlinker 密钥KEY 命令

命令包括SIMLINKER基本命令，SIMLINKER专有命令，密钥KEY专用命令。

♦ 附录一 Simlinker 密钥KEY 的复位应答

1.2 参考文献

[1] ISO/IEC 7816 PART 3：识别卡，带触点的集成电路卡：电气特性和传输协议。
[2] ISO/IEC 7816 PART 4：识别卡，带触点的集成电路卡：行业间交换用命令。
[3] 交通运输部《收费公路联网收费多义性路径识别技术要求》。

北京芯凌科技有限公司

1.3 定义

♦ 命令Command

外部终端向SAM发出的一条信息，该信息启动一个操作或请求一个应答。

♦ 响应Response

SAM处理完成收到的命令报文后，返回给终端的报文。

♦ 功能Function

由一个或多个命令实现的处理过程，其操作结果用于完成全部或部分交易。

♦ 报文Message

由终端向SAM或SAM向终端发出的，不含传输控制字符的字节串。

♦ 报文鉴别代码Message Authentication Code

对交易数据及其相关参数进行运算后产生的代码。主要用于验证报文的完整性。

♦ 明文Plaintext

没有加密的信息。

♦ 密文Ciphertext

通过密码系统产生的不可理解的文字或信号。

♦ 密钥Key

控制加密转换操作的符号序列。

♦ 加密算法Cryptographic Algorithm

为了隐藏或揭露信息内容而变换数据的算法。

♦ 对称加密技术Symmetric Cryptographic Technique

发送方和接收方使用相同保密密钥进行数据变换的加密技术。在不掌握保密密钥的情况下，不可能推导出发送方或接收方的数据变换。

♦ 数据完整性Data Integrity

数据不受未经许可的方法变更或破坏的属性。

♦ T=0

面向字符的异步半双工传输协议。

北京芯凌科技有限公司

1.4 缩略语和符号表示

以下缩略语和符号表示适用于本手册：

AID ： 应用标识符（Application Identifier）
APDU ： 应用协议数据单元（Application Protocol Data Unit）
ATR ： 复位应答（Answer to Reset）
b ： 二进制（Binary）
BER ： 基本编码规则（Basic Encoding Rules）
BWI ： 块等待时间整数（Block Waiting Time Integer）
CLA ： 命令报文的类别字节（Class Byte of the Command Message）
CWI ： 字符等待时间整数（Character Waiting Time Integer）
DEA ： 数据加密算法（Data Encryption Algorithm）
DES ： 数据加密标准（Data Encryption Satandard）
DF ： 专用文件（Dedicated File）
DIR ： 目录（Directory）
ED ： 电子存折（Electronic Deposit）
EDC ： 错误检测代码（Error Detection Code）
EF ： 基本文件（Elementary File）
EMV ： Europay、Mastercard、VISA
EP ： 电子钱包（Electronic Purse）
ETC: 电子不停车收费（Electronic Toll Collection）
Etu ： 基本时间单元（Elementary Time Unit）
FCI ： 文件控制信息（File Control Information）
FID ： 文件标识（File Identifier）
GND ： 地（Ground）
Hex. ： 十六进制数（Hexadecimal）
IC ： 集成电路（Integrated Circuit）
ICC ： 集成电路卡（Integrated Circuit Card）
IEC ： 国际电工委员会（International Electrotechnical Commission）
INS ： 命令的指令字节（Instruction Byte of Command Message）
ISO ： 国际标准化组织（International Standardization Organization）
Lc ： 终端发出的命令数据域的实际长度
Le ： 响应数据的最大期望长度
LEN ： 长度（Length）
MAC ： 报文鉴别代码（Message Authentication Code）
MF ： 主控文件（Master File）
OBE: 车载设备(On Board Equipment)
P1 ： 参数1（Parameter 1）
P2 ： 参数2（Parameter 2）
PBOC ： 中国人民银行
PIN ： 个人密码（Personal Identification Number）
PIX ： 专用应用标识符扩展码（Proprietary Application Identifier Extension）
PSA ： 支付系统应用（Payment System Application）

北京华大信安科技有限公司

PSE ： 支付系统环境（Payment System Environment）
RFU ： 保留为将来使用（Reserved for Future Use）
RID ： 已注册的应用提供者标识（Registered Application Provider Identify）
RST ： 复位（Reset）
SAM ： 安全存取模块（Secure Access Module）
SFI ： 短文件标识符（Short File Identifier）
SW1 ： 状态码1（Status Word One）
SW2 ： 状态码2（Status Word Two）
TAC ： 交易认证码（Transaction Authorization Crypogram）
TCK ： 校验字符（Check Character）
TLV ： 标签、长度、值（Tag Length Value）
VCC ： 电源电压（Supply Voltage）
VPP ： 编程电压（Programming Voltage）
‘0’～‘9’和‘A’ ～‘F’ ： 十六进制数
0x00～0x0F ： 十六进制数
XX ： 1 个字节16 进制数
XXXX ： 2 个字节16 进制数
XX…XX ： 未知个字节16 进制数

北京芯凌科技有限公司

2. Simlinker 密钥 Key 简介

2.1 关于 Simlinker 密钥 Key

Simlinker 密钥KEY是由北京芯凌科技有限公司开发的智能卡操作系统，完全符合《收费公路联网收费多义性路径识别技术要求》标准要求。

Simlinker 密钥KEY具有以下主要特征：

- 具有COS的接触式CPU卡；
- 支持一卡多应用，各应用之间相互独立；
- 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；
- 在通讯过程中支持多种安全保护机制（信息的机密性和完整性保护）；
- 支持多种安全访问方式和权限（认证功能和口令保护）；
- 支持SM4算法；
- 支持多级密钥分散机制，用分散后的密钥作为临时密钥对数据进行加密、解密、MAC等运算，以完成终端与卡片之间的合法性认证等功能。

2.2 Simlinker 体系结构

2.2.1 内部逻辑结构

Simlinker 密钥KEY内部包括四部分模块

♦ CPU及加密逻辑

保证EEPROM 中数据安全，使外界不能用任何非法手段获取EEPROM 中的数据。

♦ RAM

Simlinker工作时存放命令参数、返回结果、安全状态及临时工作密钥的区域。

♦ CODE区

存放Simlinker 程序的区域。

♦ EEPROM

存放用户应用数据区域，Simlinker 将用户数据以文件形式保存在EEPROM 中，在满足用户规定的安全条件时，可进行读或写。

北京芯凌科技有限公司

2.2.2 功能模块划分

Simlinker 由传输管理、文件管理、安全体系、命令解释四个功能模块组成:

♦ 传输管理

按ISO7816-3 标准与终端之间的通信，保证数据正确地传输，防止与终端之间通讯的数据被非法窃取和篡改。

♦ 文件管理

将用户数据以文件形式存储在EEPROM 中，保证访问文件时快速性和数据安全性。

♦ 安全体系

安全体系是Simlinker 的核心部分，它涉及到鉴别与核实，对文件访问时的权限控制机制。

♦ 命令解释

根据接收到的命令检查各项参数是否正确，执行相应的操作。

北京芯凌科技有限公司

2.2.3 Simlinker 密钥 KEY 命令集

表2.1 Simlinker 密钥KEY 命令集

编号	命令	CLA	INS	功能描述	兼容性
1	External Authentication	00	82	外部认证	ISO&PBOC
2	Internal Authentication	00	88	内部认证	ISO&PBOC
3	Get Challenge	00	84	取随机数	ISO&PBOC
4	Select File	00	A4	选择文件	ISO&PBOC
5	Read Binary	00/04	B0	读二进制文件	ISO&PBOC
6	Read Record	00/04	B2	读记录文件	ISO&PBOC
7	Get Response	00	C0	取响应数据	ISO&PBOC
8	Update Binary	00/04	D6	写二进制文件	ISO&PBOC
9	Update Record	00/04	DC	写记录文件	ISO&PBOC
10	Application UnBlock	84	18	应用解锁	ISO&PBOC
11	Delivery Key	80	1A	分散密钥	密钥 KEY
12	Cipher Data	80	FA	安全计算	密钥 KEY
13	Set Algorithm	80	FE	设置密钥算法	密钥 KEY
14	Write Key	80/84	D4	增加/更新密钥	专有
15	Create File	80	E0	建立文件	专有
16	Read Product Number	80	CB	读取产品号	专有

北京芯凌科技有限公司

3. Simlinker 密钥 Key 文件管理

本章介绍Simlinker 密钥KEY 的文件系统，包括文件组织结构、文件格式、文件的访问方式及文件空间计算。其中文件结构与文件的访问方式是以文件类型为索引来叙述的。

3.1 文件结构

Simlinker 密钥KEY 的文件系统是由专用文件DF（Dedicated File）和基本文件EF（Elementary File）组成的。

卡内数据的逻辑组织结构由专用文件（DF）的结构化分级组成。

♦ 在根处的DF 称作主文件（MF）。该MF 是必备的。

♦ 其他DF 是任选的。

MF（第1 级）为根DF，是必须有的，所有其他的文件都是她的分支。在MF 的下一级可以由DF 和EF 组成。我们将不包含子DF 的DF 称为ADF，包含子DF 的DF 称为DDF。

3.2 文件格式

3.2.1 概述

♦ Simlinker 密钥KEY 中的所有文件都是由文件头和文件体组成（如图3-1 所示）。文件头：Simlinker 密钥KEY 用这些信息来管理文件。

文件头 （文件类型，文件标识符，文件主体空间大小，权限，校验等）
文件主体

图3-1 文件在EEPROM 中存放的格式

♦ 文件头用于存储文件类型、文件标识、文件大小和访问权限等内容（见表3.1）。文件体是存放数据的区域。

北京芯凌科技有限公司

3.2.2 文件类型

♦ Simlinker 密钥KEY 支持下列两种文件：

——专用文件(DF)。

——基本文件(EF)。

♦ 在根处的DF 称作主文件(MF)。该MF 是必备的。

♦ Simlinker 密钥KEY定义了以下两种基本文件（EF）：

1、工作基本文件

用于存储不由卡所解释的数据(即用户数据)，包括二进制文件、定长记录文件、循环文件和变长记录文件。

2、内部基本文件

用于存储由卡所解释的数据，指为了管理和控制目的由卡分析和使用的数据，包括密钥文件。

♦ EF 支持的文件类型及相应的文件结构如表3.2 所示。

表3.2 文件类型字节的定义

类型字节（HEX）	文件描述	文件结构
18	MF 或DF	
08	二进制文件	透明文件
0A	定长记录文件	定长线性文件
0E	循环文件	循环文件
0F	钱包文件	循环文件
0C	变长记录文件	变长线性文件
1F	密钥文件（存放密钥和PIN，不允许外部访问）	变长线性文件

3.2.3 文件标识和文件名称

Simlinker 密钥KEY 是通过逻辑寻址而非物理寻址方式来管理文件的,支持通过文件名称和文件标识两种方式来访问文件。

3.2.3.1 文件标识（FID）

文件标识符（File Indentifier）是文件的标识代码，用2个字节来表示，在选择文件时只要指出文件标识符，Simlinker 密钥KEY就可以找到相应文件（KEY文件除外），同一目录下的文件标识符必须是唯一的。

□ 注意： MF 的文件标识均为’3F00’，‘FFFF’保留将来使用。同一目录下的文件标识

符必须是唯一的。

3.2.3.2 短文件标识符SFI

短文件标识符由5 个二进制位组成，可选择的最大文件标识符为31。若文件需要用短文件标识符进行选择，则建立文件时就需将文件标识符取在1-31（00001-11111）之间。

3.2.3.3 文件名称

文件名称是指DF 名称，用于标识DF，卡中任何ADF 或DDF 可通过其DF 名称进行选择。ADF 的DF 名称对应其应用标识（AID），应用标识的格式可参考ISO/IEC 7816-5 的有关规定。应用标识的长度为5～16 字节，分为2 部分（见图3-4）：第一部分内容叫注册ID（Registered ID），长度为5 字节，由注册机构分配，包含国家代码、应用类别和应用提供商的标识号；第二部分（PIX）是可选的，由应用提供商定义，长度为0～11 字节。

AID	
RID	PIX
5 Byte	0...11 Byte

图3-2 应用标识编码

3.3 文件访问方式

- ♦ 通过文件标识符（FID ）进行访问
  在选择文件（Select File）时只要指出文件标识符，Simlinker 密钥KEY 就可以找到相应文件。（KEY文件不能通过文件标识进行选择）
- ♦ 通过短文件标识符（SFI）进行访问

短文件标识符选择可以通过Read Binary、Update Binary命令的参数P1来实现文件的选择：

P	B7	B6	B5	B4	B3	B2	B1	B0
1	1	0	0	短文件标识符				

若参数P1的高三位为100，则低5位为短的文件标识符。

短文件标识符选择还可以通过Read Record、Update Record命令的参数P2来实现文件的选择：

P	B7	B6	B5	B4	B3	B2	B1	B0
2	短文件标识符					1	0	0

若P2的高五位不全为0，低三位为100，则高五位为短的文件标识符。

♦ 通过DF 文件名称进行访问

在选择文件（Select File）时只要指出该DF 的文件名称，Simlinker 密钥KEY 就可以找到相应的DF。

3.4 专用文件（DF）

3.4.1 主文件（MF）

3.4.1.1 定义

在Simlinker 密钥KEY 中，在根处的DF 称作主文件(MF)。该MF 是必备的。它相当于DOS 的根目录。

♦ 复位后，卡片自动选择MF 为当前文件。

♦ 在金融应用中，MF 与MF 下的目录文件（DIR 文件，一个记录型文件）一起构成支付系统环境（PSE），MF 的文件名称是1PAY.SYS.DDF01.

3.4.1.2 文件操作命令

♦ 建立文件命令(Create File)

在无MF 时，必须首先建立MF 才能对SAM进行其它操作。

♦ 选择文件命令（Select MF）

可以用Select File 命令通过文件标识符‘3F00’或文件名称1PAY.SYS.DDF01 来选择文件。

♦ 擦除DF 命令（Erase DF）

在满足当前MF 的擦除权限时，可以用此命令擦除MF 下的所有文件(包括DF 或EF)，但MF 当前的访问权限、空间等信息并没有改变（即不能擦除MF 的文件头信息）。

3.4.2 专用文件（DF）

3.4.2.1 定义

在Simlinker 密钥KEY 中，专用文件DF 相当于DOS 的目录。每一个DF 下可以存放多个EF 和多个下级DF。

北京飞天诚信科技有限公司

- SAM可支持2 级目录（MF-DF）。我们称包含下级目录的专用文件（DF）为DDF，不包含下级目录的专用文件为ADF.
- 任何一个DF 在物理上和逻辑上都保持独立，都有自己的安全机制和应用数据。
- DF 的个数仅受EEPROM 空间的限制。

3.4.2.2 **文件名称**

见“3.2.3.3 文件名称”。

3.4.2.3 **文件操作命令**

- 建立文件命令(Create File)
  当满足卡片当前DF 的建立权限时，可以用Create File 命令创建文件。
- 选择文件命令（Select MF）
  可以用Select File 命令通过文件标识符或DF 名称来选择文件。

3.5 工作基本文件

工作基本文件用于存储不由SAM所解释的数据（即用户数据），包括二进制文件、定长记录文件、循环文件、钱包文件和变长记录文件。

3.5.1 二进制文件

3.5.1.1 **定义**

二进制文件为一个数据单元序列，数据以二进制为单位进行读写。

3.5.1.2 **文件体结构▌透明文件**

透明文件通常又叫二进制文件或流文件，即透明文件不处理任何内部结构。存储在文件中的数据通过使用地址偏移量访问（文件逻辑地址从0 开始）。

透明文件的结构如下图所示：

长度（单位Byte）

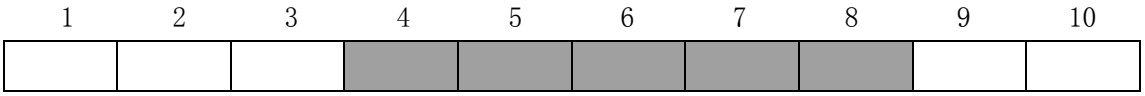
1　　2　　3……m

北京芯凌科技有限公司

图3-3 透明结构

[例] 从一个10 字节的文件中读取偏移量为3 的5 个字节：

长度(单位Byte)



3.5.1.3 **文件操作命令**

- 建立文件命令（Create File ）
  当满足卡片当前DF 的建立权限时，可以用Create File 命令创建文件。
- 选择文件命令（Select File）
  可以用Select File 命令通过文件标识符来选择文件。
- 读二进制文件（Read Binary）
  当满足文件的读权限时，可以用Read Binary 命令读取文件信息。
- 写二进制文件（Update Binary）
  当满足文件的写权限时，可以用Update Binary 命令写入文件信息。

3.5.2 定长记录文件

3.5.2.1 **定义**

定长记录文件为具有固定长度记录的文件。

3.5.2.2 **文件体结构▌定长线性文件**

定长线性文件又叫定长记录文件，它的结构是相同长度的记录。不同的记录通过顺序号来区分访问。记录只能整条访问，不允许访问记录的部分数据。

3.5.2.3 **文件头定义**

表3.6 文件操作命令

北京芯凌科技有限公司

- 建立文件命令（Create File ）
  当满足卡片当前DF 的建立权限时，可以用Create File 命令创建文件。

- 选择文件命令（Select File）
  可以用Select File 命令通过文件标识符来选择文件。

- 读记录文件（Read Record）
  当满足文件的读权限时，可以用Read Record 命令读取一条记录。

- 写记录文件（Update Record）
  当满足文件的写权限时，可以用Update Record 命令写（或更新）一条记录。

3.5.3 循环文件

3.5.3.1 定义

循环文件为具有固定长度记录的环行文件。

3.5.3.2 文件体结构▌循环文件

循环文件又叫循环记录文件。循环文件的每条记录都只有一个数据域，数据以记录为单位进行存储。不同的记录通过顺序号或记录指针来区分访问，应用时只能顺序增加记录。当写记录时，当前写入的为第一条记录，则上一次写入的记录为第二条，依此类推，滚动写入。记录只能在文件头中所规定的范围内滚动写入，当写完最后一条记录时将覆盖最先写入的记录。

3.5.3.3 文件操作命令

- 建立文件命令（Create File ）
  当满足卡片当前DF 的建立权限时，可以用Create File 命令创建文件。

- 选择文件命令（Select File）
  可以用Select File 命令通过文件标识符来选择文件。

- 读记录文件（Read Record）
  当满足文件的读权限时，可以用Read Record 命令读取一条记录。

北京总线科技有限公司

♦ 写记录文件（Update Record）

当满足文件的添加权限时，可以用Update Record 命令增加一条新记录。

3.5.4 变长记录文件

3.5.4.1 定义

变长记录文件为具有可变长度记录的文件。

3.5.4.2 文件体结构——变长线性文件

变长线性文件又叫变长记录文件。变长记录文件的数据以记录为单位进行存储，通过记录号或记录标识来选择每条记录。更新记录时，新的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。

一个文件中的记录数为2～254，不同的操作系统所支持的记录长度最大值不一样，Simlinker 密钥KEY支持的记录长度最大值为178 字节。

通常，变长记录以TLV（Tag-Length-Value）格式存在。在Simlinker 密钥KEY 中，变长记录文件和密钥文件都采用变长记录格式。

说明：

♦ 文件主体空间=所有记录长度和；

每条记录长度=1 字节记录标识符(T)+1 字节记录长度（L）+L 字节数据+1 字节校验码（由COS 计算）每条记录长度的最大为178 个字节。

3.5.4.3 文件操作命令

♦ 建立文件命令（Create File ）

当满足卡片当前DF 的建立权限时，可以用Create File 命令创建文件。

♦ 选择文件命令（Select File）

可以用Select File 命令通过文件标识符来选择文件。

♦ 读记录文件（Read Record）

当满足文件的读权限时，可以用Read Record 命令读文件中的记录。

♦ 写记录文件（Update Record）

当满足文件的写权限时，可以用Update Record 命令写（或更新）一条记录。

北京芯安科技有限公司

3.6 内部基本文件

用于存储由卡所解释的数据，指为了管理和控制目的由SAM分析和使用的数据，包括密钥文件。

3.6.1 密钥文件（KEY 文件）

3.6.1.1 定义

存放密钥的文件，不可由外界读出。当满足文件的增加密钥权限时可以向文件中写入一条密钥；当满足密钥的使用权限时可在卡内进行相应的密码运算；当满足某条密钥的更改权限时可以修改此密钥。

注：

♦ **每个*DF* 下只能有一个*KEY* 文件，且必须最先被建立。在任何情况下密钥数据均无法读出。**

3.6.1.2 文件体结构——变长记录格式

一个KEY 文件中可以包含多种密钥，每种密钥可以有多个。在Simlinker 密钥KEY 中，密钥文件采用变长记录格式，数据项定义如下表所示，记录中的T、L 字节由COS 维护。

表3.12 KEY 文件记录格式

数据元		长度
T（由COS 维护）		1
L（由COS 维护）		1
Value	密钥头	5
	密钥值	不同的密钥类型长度不同

说明：

♦ 每条记录长度=1 字节TAG+1 字节的长度+5 字节的密钥头+1字节的密钥值长度属性+密钥值长度。

北京总线科技有限公司

♦ 密钥头和密钥值的设置见“7.3 Write Key 命令”。

注： 在 DF 下的 KEY 文件中增加一条链接 MF 下密钥的 KEY 记录，则记录长度=1 字节 TAG+1 字节的长度+1 字节密钥类型。

见

3.6.1.3 **文件操作命令**

♦ 建立文件命令（Create File ）

当满足卡片当前DF 的建立权限时，可以用Create File 命令创建文件。

♦ 增加或修改密钥命令（Write Key）

在满足密钥文件的增加密钥的权限时，可以用Write Key 命令向密钥文件中写入一条密钥（设置密钥头和密钥值）；在满足密钥的更改权限时可以用Write Key 命令更改密钥数据（即不能更改密钥头数据）。

3.7 文件空间计算

如前所述，每个文件在EEPROM 中存放的格式如下：

文件头 （文件类型，文件标识符，文件主题空大小，权限，校验等）
文件主体

♦ 每个基本文件所占的EEPROM 空间=文件头+文件主体空间

♦ 定长、钱包和循环文件的主体空间=记录个数*（记录长度+1）

♦ 每个DF 所占的EEPROM 空间=DF 头+DF 下所有文件的空间和+DF 名称长度

♦ MF 的空间=MF 头16 字节+MF 下所有文件空间之和

3.8 安全报文传送

3.8.1 安全报文传送概念

安全报文传送的目的是保证数据的机密性、完整性和对发送方的认证。数据的机密性通过对数据域的加密得到保证。数据完整性和对发送方的认证通过使用报文鉴别代码MAC来实

北京芯安科技有限公司

现。

1. 完整性保护（线路保护）

对传输的数据附加4字节MAC码，接收方收到后首先进行校验，只有校验正确的数据才予以接受，这样就防止了对传输数据的篡改。

数据完整性和对发送方的认证通过使用MAC来实现。

2. 机密性保护（加密保护）

对传输的数据进行加密，这样传输的就是密文，攻击者即使获得数据也没有意义，分析后只能得到错误的结果。

数据的机密性通过对数据域的加密来得到保证。

3. 机密性和完整性保护（线路加密保护）

此种方式最安全。对传输的数据进行加密，后对传输的数据附加4字节MAC码，接收方收到后首先进行校验，只有校验正确的数据才予以接受。

至于采取哪种方法进行安全报文传送由用户根据实际情况来决定。应该指出，高安全性是以降低速度，增加实现难度来换取的，所以并不是安全性越高越好，而一定要根据具体的要求来确定。

3.8.2 如何实现安全报文传送

3.8.2.1 文件

二进制文件、定长记录文件、变长记录文件、循环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，只需要建立文件时改变文件类型字节高两位即可。文件类型定义如下：

b7	b6	b5	b4	b3	b2	b1	b0	线路保护方式
0	0	文件类型						无
1	0	文件类型						MAC
1	1	文件类型						密文&MAC

表3.18 文件类型设置

【例】建立文件时若需要进行线路保护则将文件类型最高位置1，如二进制类型由08变为88.

卡片可以在建立文件时分别设置读/写文件所使用的维护密钥标识（详见Create File）

3.8.2.2 密钥

对于密钥也可以采用安全报文传送。

如对密钥进行安全报文传送（使用Write Key、Verify PIN），只需在安装密钥时改变密钥类型字节高两位即可。

北京芯卡科技有限公司

密钥类型字节定义如下：

b7	b6	b5	b4	b3	b2	b1	b0	线路保护方式
0	0	密钥类型						无
0	1	密钥类型						密文
1	1	密钥类型						密文&MAC

表 3.19 密钥类型设置

【例】对密钥若需要进行线路加密保护（密文&MAC）则将密钥类型最高位及次高位均置1。

3.8.2.3 MAC计算

MAC总是命令或命令响应数据域中最后一个数据元素。在Simlinker中规定MAC的长度皆为4个字节。

按照如下方式使用DEA加密方式产生MAC:

第一步：终端向SAM发出一个Get Challenge命令，从SAM取回4字节随机数。
然后在该随机数后补12字节0x00，所得到的结果作为初始值。

第二步：按照顺序将以下数据连接在一起形成数据块；
——命令报文：CLA,INS,P1,P2,Lc+4,DATA.
必须置CLA的后半字节为十六进制‘4’
在命令报文数据域中（如果存在）包含明文或加密的数据。（例;如果要进行线路加密保护，加密后的数据块放在命令数据域中传输）
——命令响应报文：DATA（包含明文或密文）
——Simlinker命令中定义的数据

第三步：将该数据块分成16字节为单位的数据块，标号为D1,D2,D3等。最后的数据块有可能是1-16个字节。

第四步：如果最后的数据块长度是16字节的话，也必须在其后加上16进制数字‘80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00’，转到第五步。
如果最后的数据块长度不足16字节，则在其后加上16进制数字‘80’，如果达到16字节长度，则转到第五步；否则在其后加上16进制数字‘00’直到长度达到16字节为止。

第五步：对这些数据块使用响应密钥进行加密。
如果该密钥长度为8字节，则依照图3-19的方式来产生MAC

第六步：最终得到是从计算结果左侧取得的4字节唱的的MAC。

北京兆芯科技有限公司

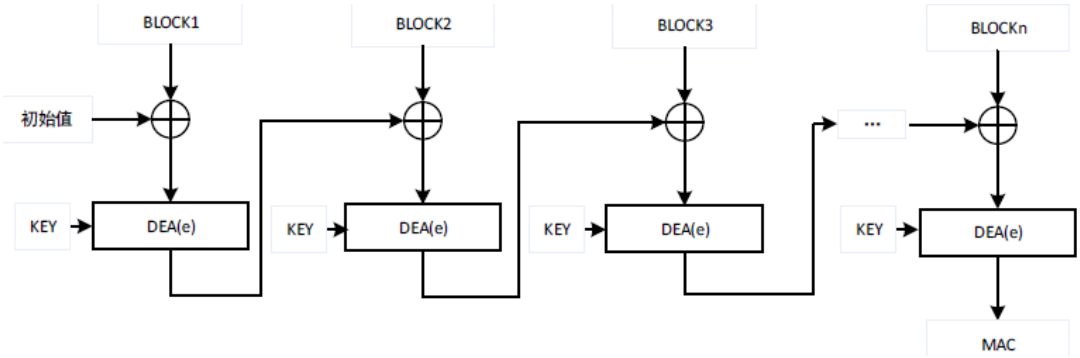


图 3.19 用SM4密钥产生MAC的算法

3.8.2.4 数据加密和解密

1. 数据加密

按照如下方式对数据进行加密：

第一步：用LD标识明文数据的长度，在明文数据前加上LD长生新的数据块。

第二步：将第一步中生成的数据块分解成16字节数据块，标号为D1,D2,D3,D4等。最后一个数据块长度有可能不是16字节。

第三步：如果最后（或唯一）的数据块长度等于8字节，转到第四步；如果不足8字节，在右边添加16进制数字‘80’。如果长度已达到16字节，转到第四步；否则，在其右边添加16进制数字‘00’直到长度到达16字节。

第四步：对每一个数据块使用相应密钥进行加密。

如果该密钥长度为16字节，则依照图3-22的方式来加密数据块。

第五步：计算结束后，所有加密后的数据块依照原数需连接在一起（加密后的D1,D2,D3等）。并将结果数据块插入到命令数据域。

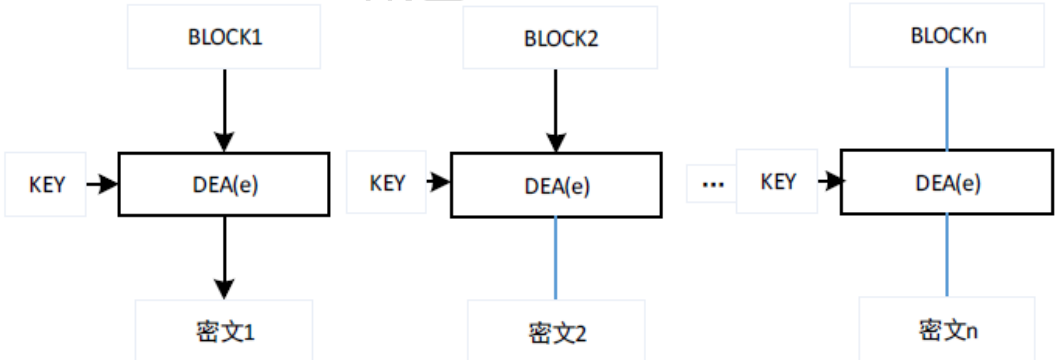


图 3.22 用SM4密钥进行数据加密的算法

2. 数据解密

按照如下方式对数据进行解密：

第一步：将命令数据域块分解成8字节长的数据块，标号为D1,D2,D3等等。

第二步：对每一个数据块使用与数据加密相同的密钥进行解密。

第三步：计算结束后，所有解密后的数据块依照顺序（解密后的D1，D2等）连接在一起。数据块由LD、明文数据、填充字符组成。

第四步：应为LD标识明文数据长度，因此，它被用来恢复明文数据。

3. 过程密钥

过程密钥是由指定密钥对可变数据加密产生的单倍长密钥。过程密钥产生后只能在某一（消费、取现等）过程中有效。

第一步：将输入数据 In 按位去翻得到（~In），即（~In）= In ⊕ (0xFF||0xFF||0xFF||0xFF||0xFF||0xFF||0xFF||0xFF)，按照 In||（~In）的顺序连接在一起，组成16字节输入数据。

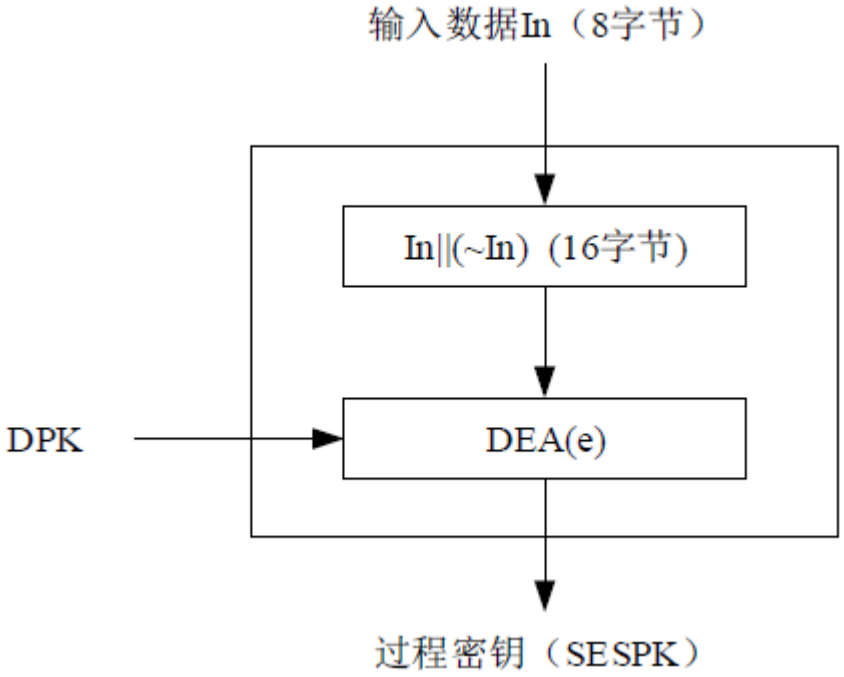


图 3.26 过程密钥的产生

第二步：将DPK作为加密密钥；

第三部：用DPK对In||(~In)进行DEA加密运算得到过程密钥。

4. Simlinker 密钥 Key 的安全体系

4.1 安全状态

安全状态是指SAM在当前所处的一种安全级别。Simlinker 密钥KEY的MF和DF分别具有16种不同的安全状态。

Simlinker 密钥KEY在内部用两个4位寄存器来标识安全状态，每个寄存器的值可以是0至F之间的某一值。两个寄存器如下：

MF安全状态寄存器 它表示整个卡所处的安全级别。

DF安全状态寄存器 它表示当前应用所处的安全级别。

4.1.1 MF 安全状态寄存器

- 在以下几种情况下，MF 安全寄存器将被复位为0：
  [1]复位后；
  [2] 当在MF 下的核对口令或外部认证命令返回的错误状态为63CX.

- 应用目录的改变不会影响该寄存器的值。

- 只有MF 下的口令核对或外部认证通过后MF 的安全状态寄存器值才发生变化。

4.1.2 DF 安全状态寄存器

- 在以下几种情况下，DF 安全寄存器将被复位为0：
  [1] 复位后。
  [2] 选择DF 后（如选择下级子目录或同级其他目录等）。
  [3] 当前DF 下的核对口令或外部认证命令返回的错误状态为63CX.

- 只有当前目录下的口令核对或外部认证通过后DF 的安全状态寄存器值才发生变化。
  若当前目录为MF，则当前目录的DF安全状态寄存器的值等于MF的安全状态寄存器值。

4.2 安全属性

安全属性是指对某个文件/密钥进行某种操作时所必须满足的条件，也就是在进行某种操作时要求安全状态寄存器的值是什么。

北京芯凌科技有限公司

安全属性又称访问权限，如下表所示：

表4.1 访问权限

文件类型	访问权限
MF/DF	建立/擦除
KEY 文件	增加
KEY 文件中的密钥	使用/更改
二进制文件	读/写
定长记录文件	读/写
循环文件	读/写
电子存折/电子钱包文件	使用
变长记录文件	读/写

每种文件访问权限在建立该文件（Create File）时用一个字节指定；每种密钥访问权限在增加密钥(Write Key)时用一个字节指定。

Simlinker的访问权限有别于其它任何操作系统的访问权限，它用一个区间来严格限制其他非法访问者。

假设当前安全状态寄存器的值用V来表示。

- 访问权限为‘0Y’时表示要求MF的安全状态寄存器的值大于等于Y。

  即：访问权限=‘0Y’ V>=Y

  [例] 如某文件读的权限为‘05’表示在对该文件进行读之前必须使MF的安全状态寄存器的值大于等于5. 即：文件的读权限=‘05’ V>=5

- 访问权限为‘XY’时（X不为0）表示要求当前目录的安全状态寄存器的值大于等于Y且小于等于X.

  [1] 当X>Y时

  即访问权限=‘XY’，且X>Y， 如此 Y≤V≤X

  [2] 当X=Y时,当前安全状态寄存器必须等于X.

  即访问权限=‘XY’，且X=Y， 如此 V=X=Y

  [3] 当X<Y时，表示禁止相应的操作。

  [例1] 如某文件写的权限为53表示对该文件进行写之前必须使当前目录的安全状态寄存器的值为3、4或5.

  [例2] 某文件读的权限为F0，写的权限为F1，代表可任意读取，写时必须满足当前目录的安全状态寄存器的值大于等于1.

北京北洋科技有限公司

4.3 安全机制

安全机制是指某种安全状态转移为另一种安全状态所采用的方法和手段。

为改变安全状态寄存器的值，必须通过某个密钥的口令或外部认证认证来实现；在密钥装载时，它的后续状态字（8bit）已经规定好了相应的安全状态，认证通过后，密钥的后续状态字节低4位将被置入安全状态寄存器。

- 在MF下认证通过后，将同时改变MF和当前目录的安全状态寄存器的值；
  在非MF下认证通过后，将只改变当前目录的安全状态寄存器值。
  为更好的理解Simlinker 的安全机制，下面举一例说明：
  设卡中某目录下有一个二进制文件，参数定义如下：
  读权限=‘F1’；
  写权限=‘F2’；
  该目录下有一个口令密钥，口令核对通过之后的后续状态为1；
  该目录下有一外部认证密钥，使用权限为11，外部认证通过之后后续状态为2。
  请看下面的操作及当前目录的状态寄存器的变化情况：

卡终端操作	方向	当前目录安全状态寄存器的值
选择 DF	→	0
	←	送返回信息
读二进制文件	→	0
	←	读的权限不满足，不允许读
验证口令	→	1
	←	口令核对正确
读二进制文件	→	1
	←	送出读出的数据
写二进制文件	→	1
	←	写的权限不满足，不允许写
外部认证	→	2
	←	外部认证正确
写二进制文件	→	2
	←	写成功
读二进制文件	→	2
	←	送出读出的数据

图4.2 访问权限控制

北京兴波科技有限公司

5. 命令与应答

5.1 命令与响应格式

从终端发出的命令和SAM响应的信息必须遵从以下4 种格式。

情形*1:*

命令 :

CLA	INS	P1	P2	00

响应 :

SW1	SW2

情形*2*:

命令:

CLA	INS	P1	P2	Le

响应:

Le字节的DATA	SW1	SW2

情形*3*:

命令:

CLA	INS	P1	P2	DATA

响应 :

SW1	SW2

情形*4*:

命令:

CLA	INS	P1	P2	Lc	DATA	Le

响应:

北京芯凌科技有限公司

Le字节的DATA	SW1	SW2

5.2 命令格式

Simlinker 命令由4 字节的命令头和命令体组成，见图8-1。

命令头				命令体		
CLA	INS	P1	P2	Lc	DATA	Le

图5-1 命令格式

5.2.1 命令头域

命令头定义报文的内容如下表所示：

表5.1 命令头域

代码	长度(byte)	值(Hex)	描述
CLA	1	X0	不带安全报文的命令
		X4	带安全报文的命令
INS	1	XX	指令代码
P1	1	XX	参数1
P2	1	XX	参数2

5.2.2 命令体

命令体中各项是可选的。

Lc 命令数据域中DATA 的长度。

Data 命令和响应中的数据域。

Le 响应数据域中期望数据的长度。

Le=00，表示需要最大字节数。

XX → 1个字节**16** 进制数

XXXX → 2个字节**16** 进制数

XX...XX → 未知个字节**16** 进制数

北京芯凌科技有限公司

5.3 响应数据格式

Simlinker 命令的应答由数据和状态字组成，见图6-2。

数据	状态字	
响应中接收的数据位串	SW1	SW2

图5-2 响应数据格式

5.4 状态字 SW1SW2 意义

状态字说明了命令处理的情况，即命令是否被正确执行,状态字由2部分组成：

SW1（status word1）：表示命令处理状态；

SW2（status word1）：表示命令处理限定。

表5.2 状态字SW1SW2

SW1	SW1	意义
90	00	正确执行
61	XX	正确执行 XX 表示响应数据长度。可用Get Response 命令取回响应数据。
63	CX	X 表示还可再试次数
65	8X	写EEPROM 不成功
67	00	错误的长度
69	00	CLA 与线路保护要求不匹配
69	01	无效的状态
69	81	命令与文件结构不相容
69	82	不满足安全状态
69	83	密钥被锁死
69	85	使用条件不满足
69	88	安全报文数据项不正确
6A	80	数据域参数错误
6A	81	功能不支持或SAM无MF 或卡片已锁定
6A	82	文件未找到
6A	83	记录未找到
6A	84	文件无足够空间

北京握奇科技有限公司

6A	86	参数P1 P2 错误
6B	00	在达到Le/Lc 字节之前文件结束，偏移量错误
6C	XX	Le 错误
6E	00	无效的CLA
6F	00	数据无效
93	02	MAC 错误
93	03	应用已被锁定
94	01	金额不足
94	03	密钥未找到

北京芯凌科技有限公司

6. Simlinker 密钥 Key 基本命令

6.1 Update Record（写记录文件）

6.1.1 定义与范围

Update Record 命令用于添加记录或更改指定的记录。
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。

6.1.2 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）
读记录文件（Read Record）
写记录文件（Update Record）
♦ 只有满足记录文件写权限时才能执行此命令。
♦ 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。

6.1.3 命令报文

表 6.1 Update Record 命令报文编码

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
P2	1	XX	见说明
Lc	1	XX	-数据长度
DATA	XX	XXXX	添加的或更新原有记录的新纪录
Le	-	-	不存在

说明：

北京世凌科技有限公司

参数 P2 的含义

b7	b6	b5	b4	b3	b2	b1	b0	含　义
X	X	X	X	X				SFI
					0	0	0	添加一条新记录
					0	0	1	
					0	1	0	
					0	1	1	
					1	0	0	记录号在 P1 中给出，当 P1 为 0 时，表示添加新记录
其余值								RFU

注：XXXXX 代表短文件标识符（SFI）；----- 代表全 0 或短文件标识符
对循环文件添加记录，P1=00

6.1.4 命令报文数据域

命令报文数据域由添加的或更新原有记录的新记录组成。

6.1.5 响应报文数据域

响应报文数据域不存在。

6.1.6 响应报文状态码

SAM 可能回送的状态码如下所示：
表 6.2 Update Record 命令响应状态码

SW1	SW1	意义
90	00	正确执行
67	00	长度错误（Lc 域为空）
69	81	当前文件不是定长或变长记录文件
69	82	写的条件不满足
6A	81	不支持此功能
6A	82	未找到文件
6A	83	未找到记录
6A	84	文件无足够空间

北京先锋发科技有限公司

6.2 External Authentication（外部认证）

6.2.1 定义与范围

External Authentication 命令利用 SAM 内部的计算结果，有条件的修改安全状态。

6.2.2 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。

6.2.3 命令报文

表 6.3 External Authentication 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	00	-
INS	1	82	-
P1	1	00	-
P2	1	00	--
Lc	1	8	-
DATA	8	XX…XX	8 字节加密后的随机数
Le	-	--	-

说明：

命令报文数据域中包含 8 字节的加密数据，该数据是用 P2 制定的密钥对此命令的前一条命令“GET CHALLENGE”命令获得的随机数(16 字节)做加密运算产生的。对于 SM4 算法，认证数据为 16 字节密文前后 8 字节进行异或的结果。

将命令中的数据用指定外部认证密钥解密，然后与先前产生的随机数进行比较，

若一致则表示认证通过，置安全状态寄存器为该密钥规定的后续状态，错误计数器恢复成初始值；

若不一致则认证失败，可再试错误数减一，且不改变安全状态寄存器的值。

6.2.4 命令报文数据域

命令报文数据域包括 8 字节加密后的随机数。

6.2.5 响应报文数据域

响应报文数据不存在

北京北洋科技有限公司

6.2.6 响应报文状态码

SAM 可能回送的状态码如下所示：

表 6.4External Authentication 命令响应状态码

SW1	SW1	意义
90	00	正确执行
63	CX	还剩 X 次可试机会
67	00	长度错误
69	82	密钥使用条件不满足
69	83	外部认证密钥锁死
6A	82	未找到 key 文件
94	03	密钥未找到

北京芯凌科技有限公司

6.3 Internal Authentication（内部认证）

6.3.1 定义与范围

Internal Authentication 命令提供了利用接口设备发来的随机数和自身存储的相关密钥进行数据认证的功能。

6.3.2 注意事项

无

6.3.3 命令报文

表 External Authentication 命令报文编码

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	Xx	认证数据长度
DATA	8	XX…XX	认证数据
Le	-	--	-

6.3.4 命令报文数据域

命令报文数据域包括用用专用的认证数据。

6.3.5 响应报文数据域

响应报文数据域的内容是相关认证数据。

6.3.6 响应报文状态码

CPC 卡可能回送的状态码如下所示：

表 Internal Authentication 命令响应状态码

SW1	SW1	意义
90	00	正确执行

北京芯凌科技有限公司

63	CX	还剩 X 次可试机会
67	00	长度错误
69	82	密钥使用条件不满足
69	83	外部认证密钥锁死
6A	82	未找到 key 文件
94	03	密钥未找到

北京芯凌科技有限公司

6.4 Get Response（取响应数据）

6.4.1 定义与范围

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

6.4.2 注意事项

此命令只用于 T=0 通讯协议。

6.4.3 命令报文

表 6.5Get Response 命令报文编码

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

6.4.4 命令报文数据域

命令报文数据域不存在。

6.4.5 响应报文数据域

响应报文数据域的长度由 Le 的值决定。

6.4.6 响应报文状态码

表 6.6 Get Response 命令响应状态码

SW1	SW1	意义
90	00	正确执行
67	00	长度错误（Le 大于卡中响应数据长度）
6F	00	卡中无数据可返回

北京芯凌科技有限公司

6.5 Get Challenge（取随机数）

6.5.1 定义与范围

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

6.5.2 命令报文

表 6.17 Get Challenge 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	00	-
INS	1	84	-
P1	1	00	-
P2	1	00	-
Lc	-	-	不存在
DATA	-	-	不存在
Le	1	04/08	要求卡片返回的随机数长度

6.5.3 命令报文数据域

命令报文数据不存在。

6.5.4 响应报文数据域

响应报文数据包括随机数，长度为 Le 个字节。

6.5.5 响应报文状态码

SAM 可能回送的状态码如下所示：

表 6.8 Get Challenge 命令响应状态码

SW1	SW1	意义
90	00	正确执行
67	00	长度错误
6A	81	不支持此功能（无 MF 或卡片已锁定）

北京志凌科技有限公司

6.6 Read Binary（读二进制文件）

6.6.1 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）。

6.6.2 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。

6.6.3 命令报文

表 6.11 Read Binary 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	00/04	-
INS	1	B0	-
P1	1	XX	见说明
P2	1	XX	见说明
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

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。

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 P1 P2 为欲读文件的偏移量，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							

北京北洋科技有限公司

6.6.4 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 MAC。
用维护密钥加密数据和计算 MAC，方法见“安全报文传送”。

6.6.5 响应报文数据域

响应报文数据域由读取的数据组成。

6.6.6 响应报文状态码

SAM 可能回送的状态码如下所示：
表 6.12 Read Binary 命令响应状态码

SW1	SW1	意义
90	00	正确执行
61	XX	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）
67	00	长度错误
69	81	不是二进制文件
69	82	读的条件不满足
69	88	MAC 不正确
6A	81	不支持此功能
6A	82	文件未找到
6B	00	参数错误（偏移地址超出了 EF）
6C	XX	Le 错误
93	03	应用永久锁定

北京卓越科技有限公司

6.7 Read Record（读记录文件）

6.7.1 定义与范围

Read Record 命令用于读取记录文件的内容。

6.7.2 注意事项

- ♦ Read Record 命令只适用于定长记录文件、循环文件、钱包文件和变长记录文件。
- ♦ 访问二进制文件的命令如下：
  建立文件（Create File）
  选择文件（Select File）
  读记录文件（Read Record）/写记录文件（Update Binary）/增加记录（Append Record）
- ♦ 只有满足二进制文件读权限时才能执行此命令。

6.7.3 命令报文

表 6.13 Read Record 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	00/04	-
INS	1	B2	-
P1	1	XX	记录号
P2	1	XX	引用控制参数，见说明
Lc	1	-	不存在（CLA=04 时，Lc = 4）
DATA	XX	-	不存在（CLA=04 时，为 MAC 数据）
Le	1	XX	‘00’

说明
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 为记录号，P1 = 0 时表示当前记录

6.7.4 命令报文数据域

当无安全报文使用时，命令报文数据域不存在。使用安全报文时，命令报文的数据

域中应包含 MAC。MAC 的计算方法和长度由应用决定。

6.7.5 响应报文数据域

响应报文数据域由读取的数据组成。

6.7.6 响应报文状态码

SAM 可能回送的状态码如下所示：

表 6.14 Read Record 命令响应状态码

SW1	SW1	意义
90	00	正确执行
61	XX	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）
67	00	长度错误
69	81	命令与文件结构不相符
69	82	读的条件不满足
6A	81	不支持此功能
6A	82	文件未找到
6A	83	未找到记录
6C	XX	Le 错误

说明：

若 CLA=04，Lc = 4，数据域为 4 字节 MAC。

若 CLA=00，当 Le 不等于该记录的实际长度时，则送回警告状态 6Cxx 请求将 Le 置为 xx 并重发该命令。

北京芯港科技有限公司

6.8 Select File（选择文件）

6.8.1 定义与范围

Select File 命令通过文件名、文件标识符或选择下一个应用来选择 SAM 中 MF、DDF 或 ADF。SAM 的响应报文应由回送文件控制信息 FCI 组成。

6.8.2 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。

6.8.3 命令报文

表 6.15 Select File 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	00	-
INS	1	A4	-
P1	1	00/04	见说明
P2	1	00/02	见说明
Lc	1	XX	-
DATA	XX	XX…XX	分拣标识符或 DF 名称
Le	1	00	对于 DF 而言为卡片自动返回的 FCI 的最大长度

说明：

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。

——同级目录文件（DF）。

P1=04，标识用 DF 名称选择，分如下两种情况：

——P2=00，标识第一个或仅有一个：

——P2=02，表示下一个。

用此方法可以选择 DF。

在任何情况下均可通过标识符‘3F00’或目录名称 1PAY.SYS.DDF01 选择 MF。

6.8.4 命令报文数据域

命令报文数据域可为空或包含文件表示符或 DF 名称。表 6.21 成功。

北京芯凌科技有限公司

6.8.5 响应报文数据域

响应报文数据域应包括所选择的 DDF 或 ADF 的文件控制信息（FCI），如表 6.21 和 6.22 所示。

表 6.16 成功选择 DDF 后回送的文件控制信息 FCI

标志	值	存在方式
6F	文件控制信息模板	必备
84	DF 名称	必备
A5	文件控制信息专用数据	可选
88	目录基本文件的短文件标识符	可选

表 6.22 成功选择 ADF 后回送的文件控制信息 FCI

标志	值	存在方式
6F	文件控制信息模板	必备
84	DF 名称	必备
A5	文件控制信息专用数据	可选
9F0C	发卡方自定义数据文件控制信息	可选

6.8.6 响应报文状态码

SAM 可能回送的状态码如下所示：

表 6.17 Select File 命令响应状态码

SW1	SW1	意义
90	00	正确执行
61	XX	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）
67	00	长度错误
6A	81	不支持此功能
6A	82	未找到文件
6A	86	参数 P1 P2 不正确

北京立科技有限公司

6.9 Update Binary（写二进制文件）

6.9.1 定义与范围

Update Binary 命令用于写二进制文件。

6.9.2 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。

6.9.3 命令报文

表 6.20 Update Binary 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	00/04	-
INS	1	D6	-
P1	1	XX	见说明
P2	1	XX	见说明
Lc	1	10	-
DATA	XX	XX…XX	写入文件的数据
Le	-	-	不存在

说明：
若 P1 的高三位为 100，则低 5 位为短的文件标识符，P2 为写文件的偏移量。

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 P1 P2 为写文件的偏移量，所写的文件为当前文件。

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

Lc 标识要写入的字节数。
——若为线路保护，Lc 为写入数据的长度+4 字节 MAC。

北京北洋科技有限公司

——若为加密线路保护，Lc 为加密后数据的长度+4 字节 MAC。

6.9.4 命令报文数据域

报文数据包括要写入的新数据。
若为线路保护文件数据域应包含 4 字节 MAC 码。
若为线路加密保护文件数据域应包含加密后的数据及 4 字节 MAC 码。
用维护密钥加密数据和计算 MAC，方法见“安全报文传送”。

6.9.5 响应报文数据域

响应报文数据域不存在。

6.9.6 响应报文状态码

SAM 可能回送的状态码如下所示：
表 6.21 Update Binary 命令响应状态码

SW1	SW1	意义
90	00	正确执行
67	00	长度错误（Lc 域为空）
69	81	不是二进制或 FAC 密钥文件不可写
69	82	写的条件不满足
69	87	无安全报文
69	88	MAC 不正确
6A	81	不支持此功能
6A	82	未找到文件
6B	00	参数错误（偏移地址超出了 EF）
93	03	应用永久锁定

北京[illegible]科技有限公司

6.10 Delivery Key（分散密钥）

6.10.1 定义与范围

Delivery Key 命令将指定的 KEY 分散到临时密钥寄存器中。该命令只支持分散 KEY，不产生过程 KEY。分散后的子 KEY 继承原始 KEY 的属性。

6.10.2 注意事项

Delivery Key 命令的执行应满足 KEY 的访问属性。

6.10.3 命令报文

表 6.22 Delivery Key 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	1A	-
P1	1	XX	密钥用途
P2	1	XX	密钥标识
Lc	1	XX	分散数据长度 ‘00’，分散级数为 0 时- ‘08’，分散级数为 1 时 ‘10’，分散级数为 2 时 ‘18’，分散级数为 3 时 其他值保留
DATA	XX	XX…XX	Lc = ‘00’不存在分散因子
Le	-	-	不存在

6.10.4 命令报文数据域

命令报文数据域为分散因子，当 Lc=‘00’不存在分散因子。

6.10.5 响应报文数据域

响应报文数据域不存在。

北京芯凌科技有限公司

6.10.6 响应报文状态码

PSAM 可能回送的状态码如下表所示：

表 6.23 Delivery Key 命令响应状态码

SW1	SW1	意义
90	00	命令执行成功
67	00	Lc 长度错误
69	82	不满足安全状态
69	83	认证密钥锁定
69	85	使用条件不满足
6A	81	不支持此功能
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

北京芯凌科技有限公司

6.11 Cipher Data（安全计算）

6.11.1 定义与范围

Cipher Data 命令用于对输入数据进行安全计算，支持的安全计算包括：SM4 算法加解密、SM4 算法 MAC。SM4 加解密采用 ECB 模式，MAC 采用 CBC 模式。

6.11.2 注意事项

Cipher Data 命令的指令应以 Delivery Key 命令为前提条件，即该命令的上一条命令应是 Delivery Key。该命令所使用的 KEY，固定为临时密钥寄存器中的 KEY。

本命令成功执行后，临时密钥寄存器中的 KEY 即刻失效。

6.11.3 命令报文

表 6.24 Cipher Data 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	FA	-
P1	1	00 或 05 或 80	‘00’加密计算 ‘05’唯一一块 MAC 计算 ‘80’无后续块解密
P2	1	00	-
Lc	1	XX	SM4 算法：Lc 应是 16 的倍数
DATA	XX	XX…XX	安全计算数据。 P1=‘05’，则第一个数据库为 MAC 计算初始值(16 字节)； P1=‘80’，无后续块解密，该块的前 16 字节为初始向量
Le	-	-	不存在

6.11.4 命令报文数据域

命令报文数据域为安全计算数据。

6.11.5 响应报文数据域

响应报文数据域不存在。

北京芯凌科技有限公司

6.11.6 响应报文状态码

PSAM 可能回送的状态码如下表所示：

表 6.25 Cipher Data 命令响应状态码

SW1	SW1	意义
90	00	命令执行成功
61	xx	还有 xx 字节数据需要返回
67	00	Lc 长度错误
69	01	Delivery Key 命令没有执行或无效
69	85	使用条件不满足
6A	81	不支持此功能
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

北京芯凌科技有限公司

6.12 Packet SecureAPDU（封装安全 APDU）

6.11.1 定义与范围

Packet SecureAPDU 命令用于对输入 APDU 进行安全报文计算，支持：密钥更新指令封装、其它安全 APDU 指令封装。

6.11.2 注意事项

Packet SecureAPDU 命令的指令应以 Delivery Key 命令为前提条件，即该命令的上一条命令应是 Delivery Key。该命令所使用的 KEY，固定为临时密钥寄存器中的 KEY。

本命令成功执行后，临时密钥寄存器中的 KEY 即刻失效。

6.11.3 命令报文

表 6.24 Cipher Data 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	FB	-
P1	1	XX	0Xh：安全报文密钥不做分散 8Xh：对安全报文密钥做分散 X0h:WriteKey指令封装 （WriteKey指令封装之前需要先执行801A指令 X1h:其它APDU封装
P2	1	XX	00h：输出APDU明文+MAC 注：WriteKey指令封装不支持明文导出方式 01h：输出APDU密文+MAC
Lc	1	XX	数据长度
DATA	XX	XX…XX	见下文
Le	-	-	不存在

6.11.4 命令报文数据域

随机数（8 字节） + CLA INS P1 P2 + L + V(L 字节) + 安全报文密钥用途（1 字节） + 安全报文密钥标识（1 字节） + [安全报文密钥分散因子

北京芯凌科技有限公司

(8 字节 *n)]。

6.11.5 响应报文数据域

P2=00, CLA INS P1 P2 Lc +明文 + mac
P2=01, CLA INS P1 P2 Lc + 密文 + mac

6.11.6 响应报文状态码

可能回送的状态码如下表所示：

表 6.25 Cipher Data 命令响应状态码

SW1	SW1	意义
90	00	命令执行成功
61	xx	还有 xx 字节数据需要返回
67	00	Lc 长度错误
69	01	Delivery Key 命令没有执行或无效
69	85	使用条件不满足
6A	81	不支持此功能
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

北京芯凌科技有限公司

6.12 Application UnBlock（应用解锁）

6.12.1 定义与范围

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，利用消费密钥校验 MAC2 的错误计数器将被重置。

6.12.2 注意事项

此命令只能在金融应用环境下执行。

Application UnBlock 命令执行前应执行 Get Challenge 命令取的 4 字节的随机数。

Application UnBlock 命令的执行采用校验模式。计算校验码使用的 KEY 为 ADF 文件中的 BLK-KID 密钥。执行此命令应满足 BLK-KID 密钥的访问权限。

如果应用解锁连续失败 3 次，卡将永久锁定此应用。

6.12.3 命令报文

表 6.26 Application UnBlock 命令报文编码

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	XX	XX…XX	信息认证码(MAC)
Le	-	-	不存在

6.12.4 命令报文数据域

命令报文数据域为信息认证码(MAC)。

6.12.5 响应报文数据域

响应报文数据域不存在。

6.12.6 响应报文状态码

PSAM 可能回送的状态码如下表所示：

北京北洋科技有限公司

表 6.27 Application UnBlock 命令响应状态码

SW1	SW1	意义
90	00	命令执行成功
62	81	回送数据出错
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	82	不满足安全条件
69	84	引用数据无效(未申请随机数)
69	85	使用条件不满足
69	88	安全信息(MAC)数据错误
6A	81	不支持此功能
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

北京芯凌科技有限公司

6.13 Set Algorithm（设置密钥算法）

6.13.1 定义与范围

该命令实现设置密钥算法功能。

默认的密钥算法为 00。

选择密钥算法或设定默认密钥算法后，如命令不能对使用的密钥及算法进行指定时（如写二进制文件命令、应用锁定解锁命令等）， COS 自动使用此命令设定的密钥算法或默认密钥算法。

6.13.2 注意事项

执行 Set Algorithm 命令无使用条件限制。

指令设置算法的有效作用域为当前应用，新选择应用或下电，恢复默认密钥算法。INIT SAM FOR PURCHASE、 CREDIT SAM FOR PURCHASE、 CIPHER DATA、 DELIVERY KEY、 WRITE KEY 指令不受该指定算法标识影响。

6.13.3 命令报文

表 6.28 Set Algorithm 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	FE	-
P1	1	00/01/02	‘00’读取当前密钥算法 ‘01’选择 P2 指定的密钥算法 ‘02’设置 P2 指定的密钥算法为默认算法-
P2	1	00/04	P1 =‘00’时为 0x00 密钥算法，‘04’= SM4
Lc	1	不存在	-
DATA	XX	不存在	
Le	-	-	P1=‘00’时为 0x00 或 0x01，响应报文数据域返回当前密钥算法（当未选择 当前密钥组时返回默认密钥组，否则为当前密钥组）。 其他情况下为 0x00。

北京芯凌科技有限公司

6.13.4 命令报文数据域

命令报文数据域不存在。

6.13.5 响应报文数据域

P1='00'时为 0x00 或 0x01，响应报文数据域返回当前密钥算法（当未选择当前密钥组时返回默认密钥组，否则为当前密钥组）。其他情况下响应报文数据域不存在。

6.13.6 响应报文状态码

PSAM 可能回送的状态码如下表所示：

表 6.29 Set Algorithm 命令响应状态码

SW1	SW1	意义
90	00	命令执行成功
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	85	使用条件不满足
6A	81	不支持此功能
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

北京芯凌科技有限公司

7. Simlinker 密钥 Key 专有命令

- 此部分描述了Simlinker 密钥KEY 的初始化命令，以下各节将详细描述这些命令。
- 有关安全报文的操作见 “安全报文传送”。

表7.1 Simlinker 密钥Key 发卡命令

序号	命令	CLA	INS	功能描述	兼容性
1	**Create File**	80	E0	建立文件（DF、EF）	专有
2	**Write Key**	80/84	D4	增加或更新密钥	专有

7.1 Create File（建立文件）

7.1.1 定义与范围

Create File 命令用于建立文件系统。请参见“3.4 专用文件、3.5 工作基本文件和3.6 内部基本文件”。

7.1.2 注意事项

- 在满足当前DF 的建立权限时，可用此命令建立DF 或EF。
- 每个DF 下只能有一个KEY 文件，且必须最先被建立。
- 当前DF 被擦除后，则在该DF 下可任意建立文件和读写文件而不受文件访问权限的限制，一旦离开当前DF 再进入DF 时，将遵循文件的访问权限。
- 目录文件建立后不能自动被选择（MF 除外），需使用Select File 命令选择。

7.1.3 命令报文

表7.2 Create File 命令报文编码

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）
Le		-	不存在

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***’；

北京总线科技有限公司

7.1.4 命令报文数据域

命令数据域中的所有权限设置请参见“安全体系”。

7.1.4.1 **主文件（MF）**

♦ P1 P2 参数固定为‘3F 00’

表7.3 MF 的文件控制信息

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）	18	FFFF	XX	XX	FFFFFFFFFFFFFFFF

7.1.4.2 **专用文件（DF）**

表7.4 DF 的文件控制信息

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）	18	XXXX	XX	XX	FFFFFF	DF 名称

7.1.4.3 基本文件（**EF**）

基本文件控制信息内容如下表所示。

表7.5 EF 的文件控制信息

<table>
<tr><th>数据域
文件类型</th><th>Byte 1</th><th colspan="2">Byte 2</th><th>Byte 3</th><th>Byte 4</th><th>Byte 5</th><th>Byte 6</th><th>Byte7</th></tr>
<tr><td>二进制文件</td><td>08</td><td colspan="2">文件空间</td><td></td><td>读权限</td><td>写权限</td><td>见说明【2】</td><td>FF</td></tr>
<tr><td>定长记录文件</td><td>0A</td><td>2≤记录数≤254</td><td colspan="2">记录长度≤178</td><td>读权限</td><td>写权限</td><td>见说明【2】</td><td>FF</td></tr>
<tr><td>循环文件</td><td>0E</td><td>2≤记录数≤254</td><td colspan="2">记录长度≤178</td><td>读权限</td><td>写权限</td><td>见说明【2】</td><td>FF</td></tr>
<tr><td rowspan="2">变长记录文件</td><td rowspan="2">0C</td><td colspan="3">文件空间=所有记录长度和</td><td rowspan="2">读权限</td><td rowspan="2">写权限</td><td rowspan="2">见说明【2】</td><td rowspan="2">FF</td></tr>
<tr><td colspan="3">每条记录=记录长度+1字节校验码（由COS 计算）</td></tr>
<tr><td>密钥文件</td><td>1F</td><td colspan="3">文件空间=所有密钥记录长度之和+5 字节保留空间每条记录的计算方法见说明[2]</td><td>当前DF文件短标识符见说明[2]</td><td>增加权限</td><td>FF</td><td>FF</td></tr>
</table>

说明：

【1】二进制文件、定长记录文件、变长记录文件、循环文件、（密钥文件除外）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，只需在建立文件时改变文件类型字节高两位即可。

基本文件数据域Byte1（文件类型）定义如下：

北京北洋科技有限公司

b7	b6	b5	b4	b3	b2	b1	b0	线路保护方式
0	0	文件类型						无
1	0	文件类型						MAC
1	1	文件类型						密文&MAC

[例] 建立文件时若需进行线路保护则将文件类型最高位置1，如二进制类型由08 变为88。

【2】对文件进行线路保护时所使用的维护密钥标识设置

基本文件数据域Byte6定义如下：

b7	b6	b5	b4	b3	b2	b1	b0
是否带线路保护读	算法标识	1	1	读密钥标识符		写密钥标识符	

1）b7=1，表示该文件不支持带线路保护读，b3b2=11；
b7=0，表示该文件必须带线路保护读。

2）b6=1，表示使用3DES算法
b6=0，表示使用SM4算法

3）b5～b4位保留为1.

4）b3b2=11，表示用标识00的维护密钥；
b3b2=10，表示用标识01的维护密钥；
b3b2=01，表示用标识02的维护密钥；
b3b2=00，表示用标识03的维护密钥。

5）b1b0的设置方法与b3b2相同。

注：如果文件类型Byte1设置为不带线路保护，那么Byte7保留为‘FF’。
如果文件类型Byte1设置为带线路保护而b7设置为不带线路保护读，那么b3b2保留为1.

【3】 电子存折/电子钱包文件

1）TAC密钥标识符：Byte6为该钱包文件进行交易时用于生成交易验证码TAC的密钥标识。

2）交易明细文件短标识：Byte7的底5位为交易明细文件的短文件标识符。

注：电子存折的文件标识符必须是‘0001’；电子钱包的文件标识符必须是‘0002’；

【4】 **KEY** 文件

注：***KEY*** 文件标识符必须是‘***0000***’。

1）每条记录长度=1 字节TAG+1 字节的长度+5 字节的密钥头+密钥值的长度。
记录中的T、L 字节由COS 维护。

注：对于连接MF下密钥的KEY记录，则记录长度=1字节TAG+1字节的长度+1字节密钥类型。
记录中的T、L字节由COS维护。

2）DF文件短标识符

DF 文件短标识符如下表所示。

表7.6 DF 文件短标识符

b7	b6	b5	b4	b3	b2	b1	b0	描述
1	1	1	1	1	1	1	1	保留值

北京证凌科技有限公司

7.1.5 响应报文数据域

响应报文数据域不存在。

7.1.6 响应报文状态码

IC 卡可能回送的状态码如下所示：

表7.7 **Create File** 命令响应状态码

SW1	SW2	意义
90	00	命令成功执行
6A	81	无MF 或卡片已锁定
6A	86	文件已存在
6A	84	空间不足
69	82	创建文件权限不满足
67	00	创建文件权限不满足
6E	00	无效的CLA

北京芯凌科技有限公司

7.2 Write Key（更新密钥）

7.2.1 定义与范围

Write Key 命令可向卡中装载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。

7.2.2 注意事项

- 密钥下载支持80/84的方式，密钥的更新根据ETC标准要求，只能使用84 密文+MAC方式
- 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（口令密钥除外）。

7.2.3 命令报文

代码	长度(byte)	值(Hex)	描述
CLA	1	84	-
INS	1	D4	-
P1	1	00	-
P2	1	00	-
Lc	1	24	SM4算法
DATA	XX	XX....XX	加密后的密钥信息||MAC
Le	-	-	不存在

北京志凌科技有限公司

7.2.4 命令报文数据域

数据域数据 = 密钥属性（3 字节长） + 密钥值
密钥属性包括： 密钥用途，密钥标识，密钥算法标识
若为线路加密保护，则由加密的数据附上 4 字节 MAC 码组成。

DF01下的密钥文件结构：

密钥名称	密钥用途	密钥标识	密钥长度	算法标识	错误计数器
应用 1 主控密钥 MK_DF01	00	00	10H	-	3
应用 1 维护密钥 1 AMK1_DF01	01	01	10H	00	3
CPU 卡外部认证密钥 1 UK1_DF01	48	44	10H	04	-
CPU 卡外部认证密钥 2 UK2_DF01	48	45	10H	04	-
CPU 卡内部认证密钥 1 IK2_DF01	48	46	10H	04	-

说明：

1. 应用主控密钥在卡片主控密钥的线路保护控制下装载（密文+MAC）；
2. 应用主控密钥在自身的控制下更新（密文+MAC）；
3. 本密钥文件下其他密钥在应用主控密钥的线路保护控制下装载、更新（密文+MAC）；
4. 应用主控密钥外部认证通过后，可以在DF01目录下进行文件创建；
5. 应用维护子密钥用于DF01区域的应用数据维护。

7.2.5 响应报文数据域

响应报文数据域不存在

北京芯凌科技有限公司

7.3 Read ChipID（读取芯片序列号）

7.3.1 定义与范围

ReadChipID 命令用于读取芯片序列号。

7.3.2 命令报文

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	F6	-
P1	1	00	-
P2	1	00	-
Lc	-	-	不存在
DATA	-	-	不存在
Le	1	08	要求 SAM 返回的数据长度

7.3.3 命令报文数据域

命令报文数据不存在。

7.3.4 响应报文数据域

响应报文数据包括产品号，长度为 Le 个字节。

7.3.5 响应报文状态码

PSAM 可能回送的状态码如下所示：

SW1	SW1	意义
90	00	正确执行
67	00	长度错误
6A	86	P1，P2不正确
6E	00	CLA错

北京芯凌科技有限公司