基于 CIU98_B V2 的 T-BOX SE[V3160-1.1] 用户使用手册

V1.0

北京中电华大电子设计有限责任公司
CEC Huada Electronic Design Co.,Ltd

2021 年 10 月

声　明

变更记录

版本	修改描述	日期
V1.0	初稿	2021-10-29

目 录

1. 产品简介

基于华大高安全芯片 CIU98_B V2 开发的 SE 产品，针对物联网领域的信息安全诉求，作为信任根集成到终端设备内，提供各类密码服务功能，支持设备端的唯一标识、通讯加密、安全存储、安全启动、安全升级等各类安全应用。

芯片安全特性：

- 采用 32 位 ARM SC000 安全处理器内核，CPU 频率 72MHz
- 硬件 PKE 协处理器、硬件 CRC、定时/计数器、WDT
- 真随机数发生器
- 支持存储器数据加密、存储器地址加扰
- 支持存储器访问权限保护机制
- 电压检测/温度检测/外部频率检测等安全传感器
- 有源屏蔽层

产品特性：

- 支持 SPI/I2C 接口
- 支持使用 7816_RST 管脚进行 SE 复位
- 支持设备权限、管理员权限、用户权限三种安全权限，设备权限通过 EXTERNAL AUTHENTICATION 命令获取，管理员权限、用户权限通过 VERIFY PIN 命令获取
- 支持明文/密文两种安全报文格式
- 支持 1-251 字节的 SE ID
- 支持存储证书和用户关键数据
- 支持 ECC/RSA/3DES/AES/SHA/SM2/SM3/SM4 算法
  - ECC：支持 NIST P-256 曲线，支持 ECDSA、ECIES、ECDH/ECDHE，符合 SEC/NIST 规范及 SSL/TLS 协议要求
  - RSA：支持 1024-2048 位长的密钥（32 位步长），支持 CRT 模式和 ND 模式，支持

NOPADDING 及 PKCS#1 填充

- 3DES：支持 128 位/192 位长的密钥，支持 ECB、CBC 加解密及 MAC 计算
- AES：支持 128 位/192 位/256 位长的密钥，支持 ECB、CBC 加解密及 MAC 计算
- SHA：支持 SHA1、SHA224、SHA256、SHA384、SHA512
- SM 系列：符合国家商用密码管理局 GM-T 0002、0003、0004 等规范

- 支持安全的文件系统，具备权限管理和访问控制机制
- 支持 SE 固件的离线升级或 OTA 升级
- 用户空间 256K 字节
- 支持文件 50 万次擦写
- 工作环境温度：-40℃ ~ 125℃
- 工作电压（VCC）：1.62V ~ 5.5V
- 支持 Standby 省电模式

SE 出厂状态：

- I2C 接口从设备地址为 7 位的 0x2A
- 设备主控密钥为 SM4 算法，最大认证次数为 128 次
- 对称算法 MAC 计算方式符合 ISO9797-1 的计算模式 3
- PIN 验证算法采用 SM3 算法，最大验证次数为 128 次
- SE 默认自动进入 Standby 模式

2. 通讯接口

本产品支持 SPI 和 I2C 接口通讯, 接口都工作在从模式。

2.1. APDU 格式定义

SPI 和 I2C 通讯接口的通讯协议支持短 APDU 和扩展 APDU 两种格式，SE 根据下发的命令数据格式进行 APDU 格式的适配及处理。

主机设备 HD 与 SE 之间传输的 APDU 格式定义如下：

- APDU 命令/响应对结构

命令头	命令体
CLA INS P1 P2	[Lc][Data][Le]

响应体	响应尾
[Data]	SW1 SW2

- APDU 命令串定义

{C(1)=CLA} {C(2)=INS} {C(3)=P1} {C(4)=P2} {C(5)…… C(n)}

- APDU 命令编码格式

类型	C(5)	C(6)C(7)	命令长度（字节）
CASE1	不存在	不存在	4
CASE2S	存在，任意值	不存在	5
CASE3S	存在，≠'00'	C(6)存在，C(7)可能存在	5+ (C(5))
CASE4S	存在，≠'00'	存在，任意值	6+ (C(5))
CASE2E	存在，='00'	存在，任意值	7
CASE3E	存在，='00'	存在，≠'0000'	7+ (C(6)C(7))
CASE4E	存在，='00'	存在，≠'0000'	9+ (C(6)C(7))

2.2. I2C 通讯

SE 的 I2C 接口为从接口，通信协议符合《HED_I2C 通讯协议规范 V2.0》。

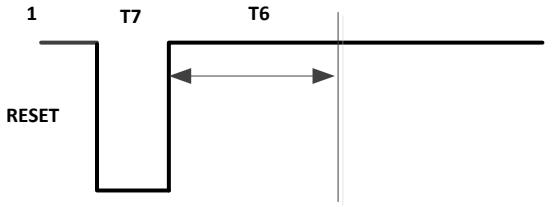
2.2.1. 接口特性

- 通讯速率：支持 100kbps/400kbps/1Mbps
- 最大数据长度：4224 字节（不包括帧结构）
- 单次通讯最大长度：1032 字节（帧头+数据+CRC）
- 从机地址：默认 7 位的 2AH，可配置，7 位时：配置范围 00H~7FH，10 位时：配置范围 000H~3FFH
- 接收轮询时间：1ms
- 数据帧超时等待时间：700ms
- 从 Standby 唤醒等待时间：至少 200us

- 协议帧间隔时间：至少 200us

2.2.2. 时序图

2.2.2.1 复位时序图：



2.2.3. 时间间隔要求

2.2.3.1. SE 复位时序时间间隔要求

名称	T7(ms)	T6(ms)
最小值	1	10

注：T7 为拉低 RESET 信号时间，T6 为释放 RESET 信号后等待 SE 完成复位的时间。T7、T6 均是最小时间间隔，假如 MCU 端定时不准，可适当放大这些时间间隔。

2.2.4.复位信息

TS	T0	TA	Historical bytes
3B	17	11	81 00 31 60 00 xx xx

2.3. SPI 通讯

SE 的 SPI 接口为从接口，为标准 4 线模式。通信协议符合《HED_SPI 通讯协议规范 V2.0》。

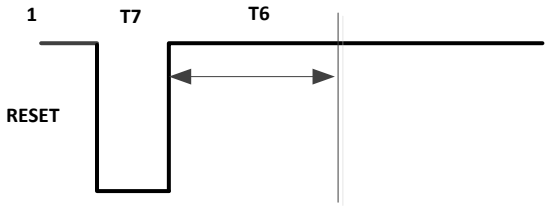
2.3.1. 接口特性

- 通讯速率：最高支持 15Mbps
- 传输方式：采用 MSB 传输，采用 Standard 模式，采用 Mode0 模式
- 最大数据长度：4224 字节（不包括帧结构）
- 单次通讯最大长度：1032 字节（帧头+数据+CRC）
- 数据帧超时等待时间：700ms
- 从 Standby 唤醒等待时间：至少 200us

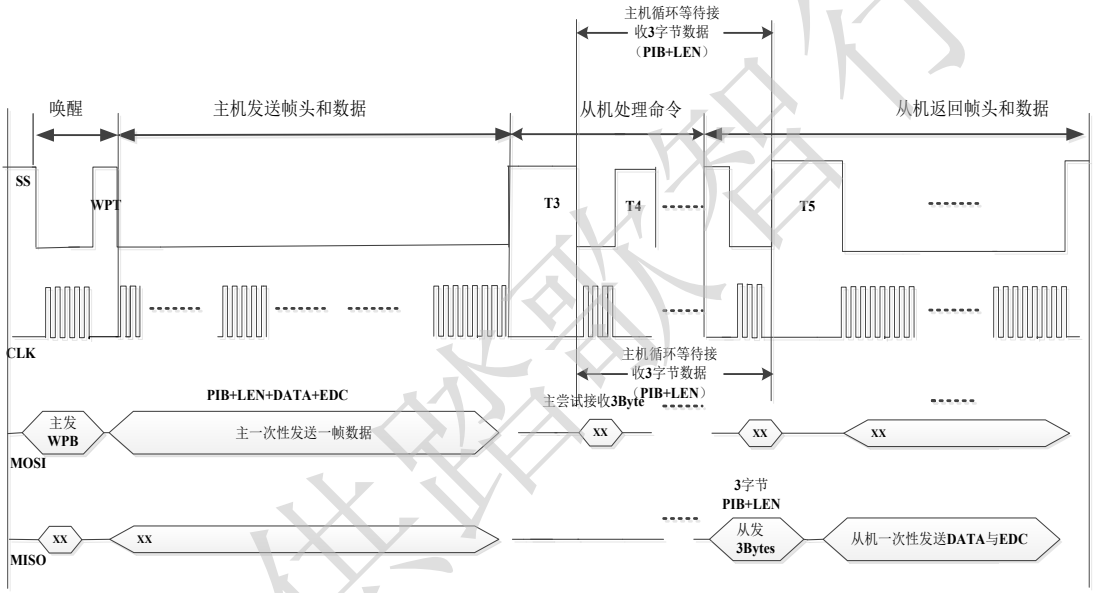
- 协议帧间隔时间：至少 200us

2.3.2. 时序图

2.3.2.1. 复位时序图：



2.3.2.2. 通信时序图：



2.3.3. 时间间隔要求

2.3.3.1. SE 复位时序时间间隔要求

名称	T7(ms)	T6(ms)
最小值	1	10

注：T7 为拉低 RESET 信号时间，T6 为释放 RESET 信号后等待 SE 完成复位的时间。T7、T6 均是最小时间间隔，假如 MCU 端定时不准，可适当放大这些时间间隔。

2.3.3.2. SPI 通信过程 SPI 时序时间间隔要求

名称	WPT(us)	T3(us)	T4(us)	T5(us)
最小值	210	200	20	30

注：上表时间间隔均是最小要求，假如 MCU 端定时不准，可适当放大这些时间间隔。

2.3.4. 超时睡眠时间

SE 唤醒后 1 分钟内 SPI 总线上无数据通信，则 SE 可自动进入 Standby 状态。

是否自动进入 Standby 状态以及超时时间均可配置。

2.3.5. 复位信息

TS	T0	TA	Historical bytes
3B	17	00	81 00 31 60 00 xx xx

3. 数据管理

3.1. 数据存储

本产品采用文件方式进行数据存储管理，支持数据、密钥安全存储功能。

二进制文件用于存储用户数据，通过文件 FID 和偏移地址的方式，对敏感信息、配置信息以及证书等数据进行写入与读取。文件支持创建、删除、选择、读、写、更新等操作，可以创建多个二进制文件用于存储不同类型的数据。

二进制文件可以设置访问权限，满足访问权限后才可以进行读、写、更新等操作。

3.1.1. 数据安全保护

本产品支持存储数据安全保护，支持包括数据的断电保护机制、防数据误写保护机制、敏感数据校验保护等。

3.2. 数据交换模式

主端与 SE 之间的数据交换有两种模式：数据可以是明文、密文。当 APDU 命令 CLA 字节的后半字节等于十六进制‘4’时，表明命令数据采用密文传输；当 CLA 字节的后半字节等于十六进制‘0’时，表明命令数据采用明文传送。。

针对密文的数据传输模式，数据必须由 8/16 个字节组成一个数据块，使用指定的对称密钥对数据加密。

3.2.1. 明文模式

如果对数据传输的安全性没有要求，可以采用明文模式。数据交换中的明文模式就是命令报文的数据域中和响应报文的数据域中的数据不经过任何形式的变换处理直接传送。

3.2.2. 加密模式

如果侧重于数据在传输中的安全性，可以采用加密模式。数据交换中的加密模式就是命令报文的数据域中和响应报文的数据域中的数据先经过加密变换，然后再放在相应的数据域中传送。

4. 安全计算

4.1. 支持的算法

本产品支持的算法如下表所示：

类别	算法	长度（字节）	说明
对称算法	3DES-128	16	分组长度 64 位
	3DES-192	24	分组长度 64 位
	AES-128	16	分组长度 128 位
	AES-192	24	分组长度 128 位
	AES-256	32	分组长度 128 位
	SM4	16	国密 SM4，分组长度 128 位
非对称算法	RSA_Standard	128~256	RSA 标准密钥类型，1024~2048 位（32 位递进）
	RSA_CRT	128~256	RSA 中国余数定理类型，1024~2048 位（32 位递进）
	ECC	32	曲线参数 NIST P256，公钥长度 64 字节，私钥长度 32 字节
	SM2	32	国密 SM2，公钥长度 64 字节，私钥长度 32 字节。
哈希算法	SHA-1	—	输出长度 20 字节
	SHA-224	—	输出长度 28 字节
	SHA-256	—	输出长度 32 字节
	SHA-384	—	输出长度 48 字节
	SHA-512	—	输出长度 64 字节
	SM3	—	国密 SM3，输出长度 32 字节

4.2. 密钥类型

本产品支持的密钥类型如下表所示：

类型	名称	是否可读	KID	算法	管理命令	用途
主控密钥	MK	×	--	3DES-128 、3DES-192 、AES128 、AES192 、AES256 、SM4	WRITE KEY	获得设备权限
传输密钥	TK	×	02-FF	3DES-128 、3DES-192 、AES128 、AES192 、AES256 、SM4	WRITE KEY	文件读写过程中的数据加密。
管理员 PIN/用户 PIN	PIN	×	00/01	--	WRITE KEY、CHANGE/RELOAD PIN、VERIFY PIN	文件操作权限和密钥使用权限
固定对称密钥	--	×	00-EF	3DES-128 、3DES-192 、AES128 、AES192 、AES256 、SM4	GENERATE KEY、IMPORT KEY	加密、解密、计算 MAC、验证 MAC
固定非对称密钥	Public Key	√		RSA、ECC、SM2	GENERATE KEY、IMPORT KEY、EXPORT KEY	验签、加密
	Private Key	×				签名、解密
临时对称密钥	Session Key	√	F0~FF	3DES-128 、3DES-192 、AES128 、AES192 、AES256 、SM4	GENERATE KEY、IMPORT KEY、EXPORT KEY	加密、解密、计算 MAC、验证 MAC
临时非对称	Public Key	√	F0-FF（最	RSA、ECC、	GENERATE KEY、	验签、加密

类型	名称	是否可读	KID	算法	管理命令	用途
密钥			多占用两个 KID）	SM2	IMPORT KEY、EXPORT KEY	
	Private Key	√	F0-FF（最多占用两个 KID）			签名、解密
协商密钥	Shared Key	√	F0-FF	3DES-128 、3DES-192 、AES128 、AES192 、AES256 、SM4	GENERATE SHARED KEY	密钥衍生、加密、解密、计算 MAC、验证 MAC

4.3. MAC 计算

按照如下步骤使用相应算法的加密方式产生 MAC：

第一步：	取相应算法分组数据长度的初始值，不同应用中初始值取值不同，详见下节具体 MAC 计算；
第二步：	将待计算 MAC 的数据组成数据块 D。
第三步：	将该数据块分成相应算法分组数据长度为单位的数据块，表示为 BLOCK1、BLOCK2、BLOCK3、BLOCK4 等。最后的数据块有可能是 1~‘相应算法分组数据长度’个字节。
第四步：	如果最后的数据块的长度是相应算法分组数据长度，则在该数据块之后再加一个完整的相应算法分组数据长度的数据块 ’80 00 00 ……’， 转到第五步。 如果最后的数据块的长度不足相应算法分组数据长度，则在其后加入 16 进制数‘80’，如果达到相应算法分组数据长度，则转到第五步；否则继续在其后加入 16 进制数‘00’直到长度达到相应算法分组数据长度。
第五步：	按照图 4-1 或图 4-2、4-3 所述的方法对这些数据块使用指定密钥进行加密，得到与分组数据长度等长字节的计算结果。
第六步：	取计算结果的前 4/8 字节作为 MAC 计算结果。

- 对于 SM4、AES 算法：

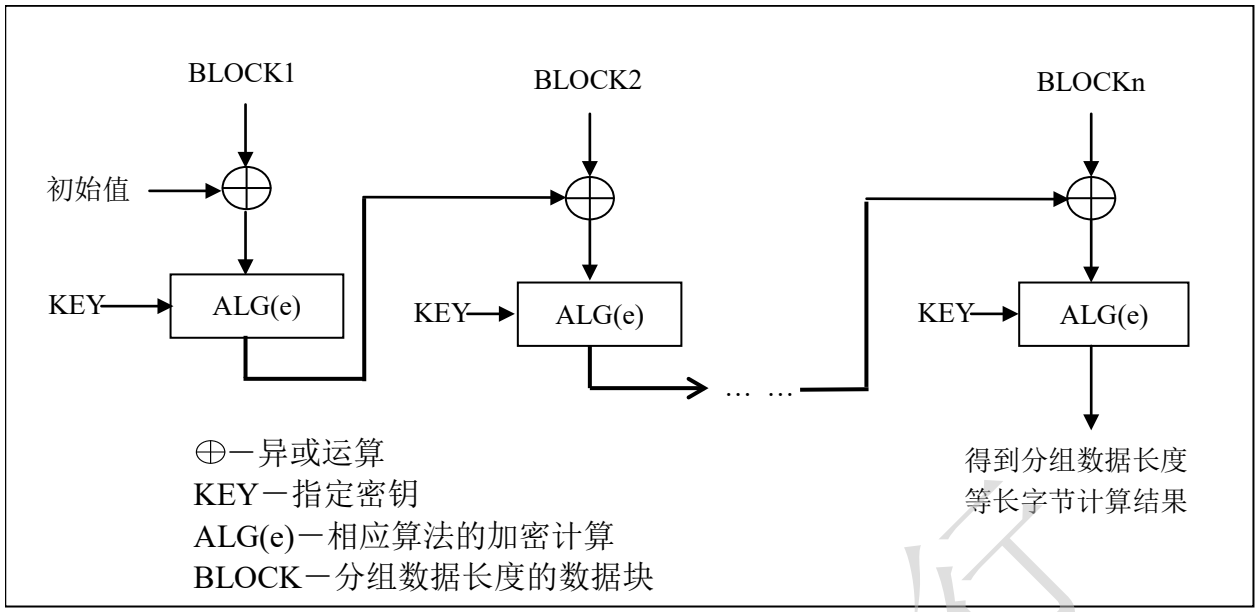


图 4–1 用 SM4、AES 密钥产生 MAC 的算法

- 对于 3DES 算法，符合 ISO9797-1 规范，分为如下两种模式。出厂默认为计算模式 3，可使用 CONFIG APP INFO 命令进行配置。

  1） ISO9797-1 的计算模式 3：

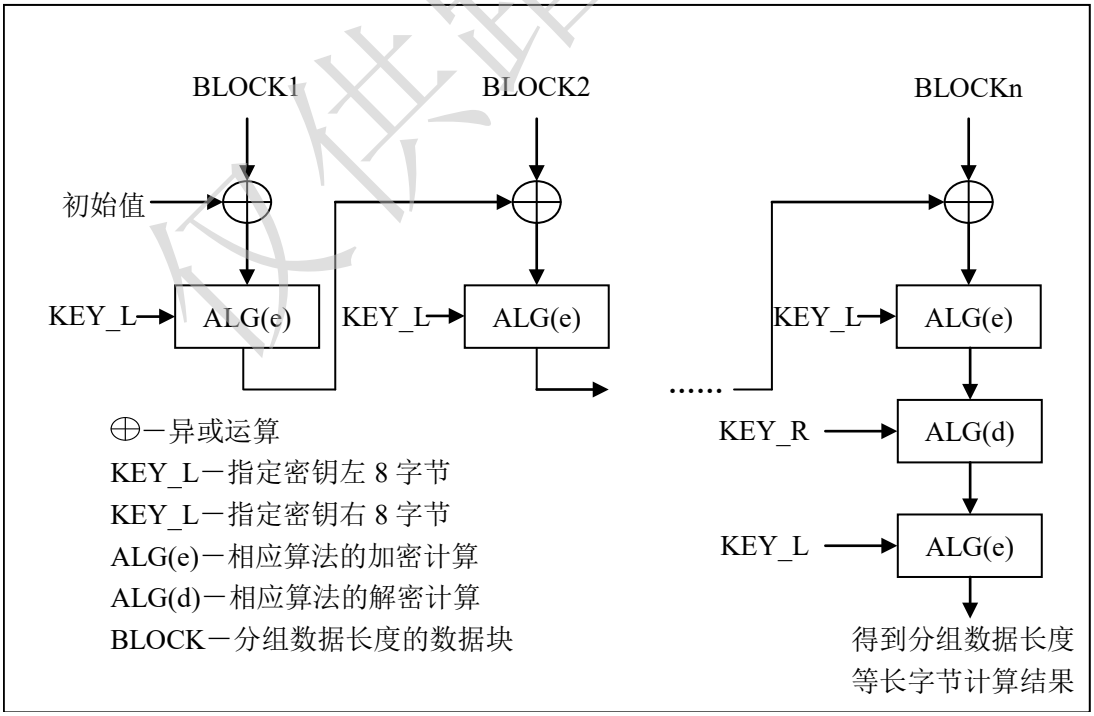


图 4–2 用 3DES 密钥产生 MAC 的算法（ISO9797-1 的计算模式 3）

2） ISO9797-1 的计算模式 1：

计算步骤与图 4-2 描述的过程一致，只是每块运算需要同时使用左 key 和右 key，见下图：

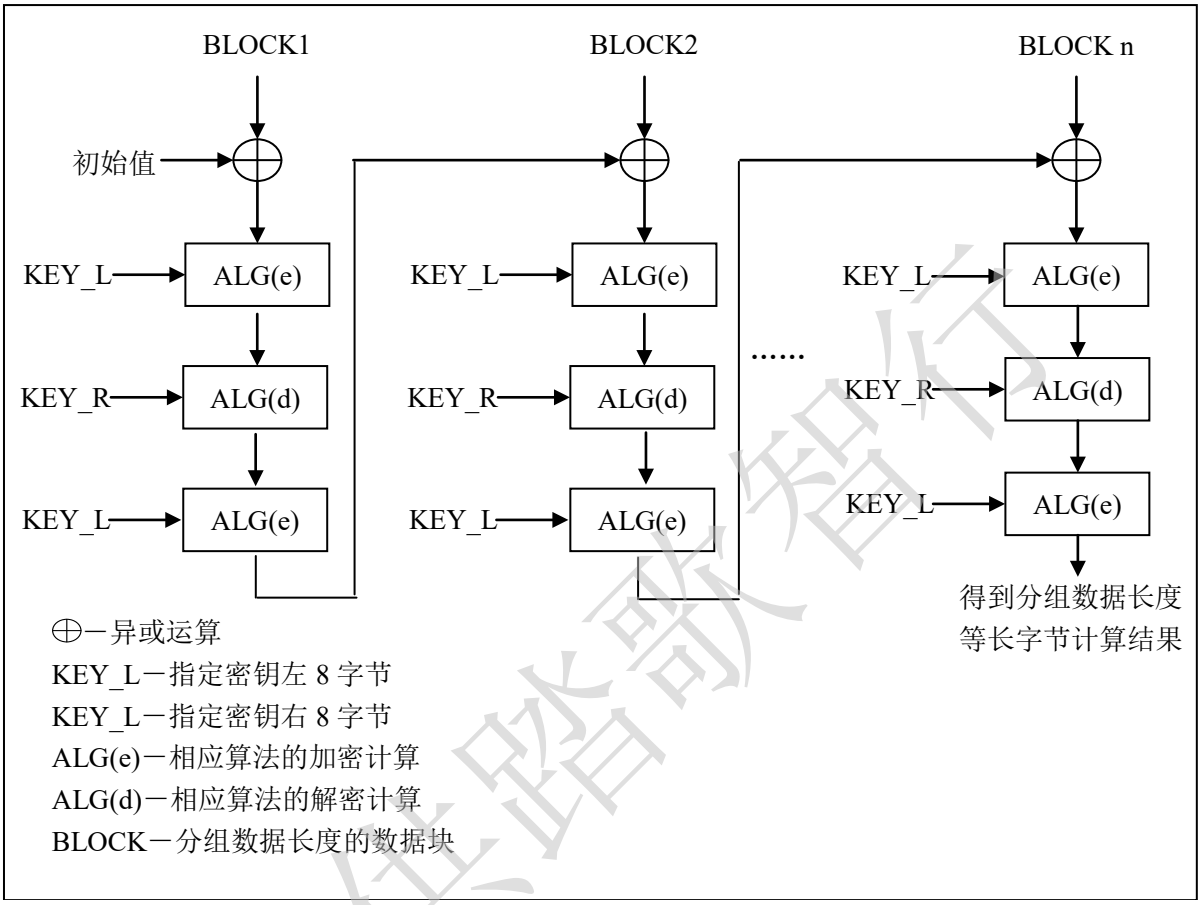


图 4-3 用 3DES 密钥产生 MAC 的算法（ISO9797-1 的计算模式 1）

4.4. 数据加解密

按照如下步骤使用相应算法对数据进行加密：

第一步：	用 LD（2 字节）表示明文数据的长度，在明文数据前加上 LD 产生新的数据块，LD 的值不小于 1。
第二步：	将该数据块分成相应算法分组数据长度为单位的数据块，表示为 BLOCK1、BLOCK2 … … BLOCKn 等。最后的数据块有可能是 1~‘相应算法分组数据长度’个字节。
第三步：	如果最后的数据块的长度是相应算法分组数据长度，转到第四步； 如果不足相应算法分组数据长度，则在其后加入 16 进制数‘80’，如果达到相应算

	法分组数据长度，则转到第四步；否则继续在其后加入 16 进制数‘00’直到长度达到相应算法分组数据长度。
第四步：	按照图 4-4 所述的方法使用指定密钥对每一个数据块进行加密。
第五步：	计算结束后，所有加密后的数据块依照原顺序连接在一起。

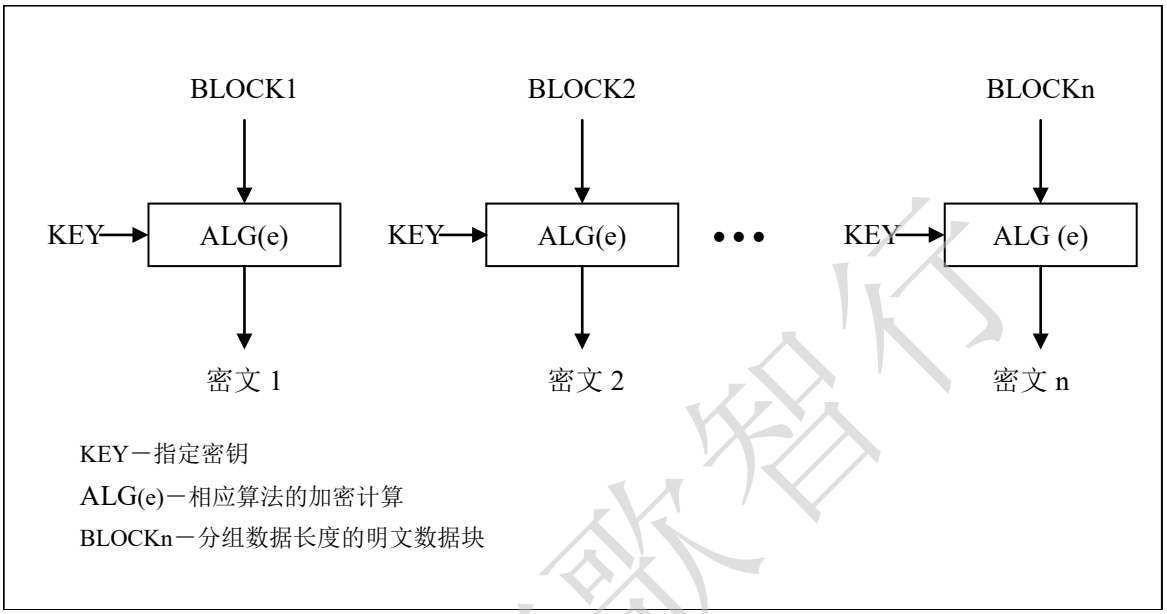


图 4–4 对数据加密的过程

数据解密则采用与加密相反的过程，见图 4-5。

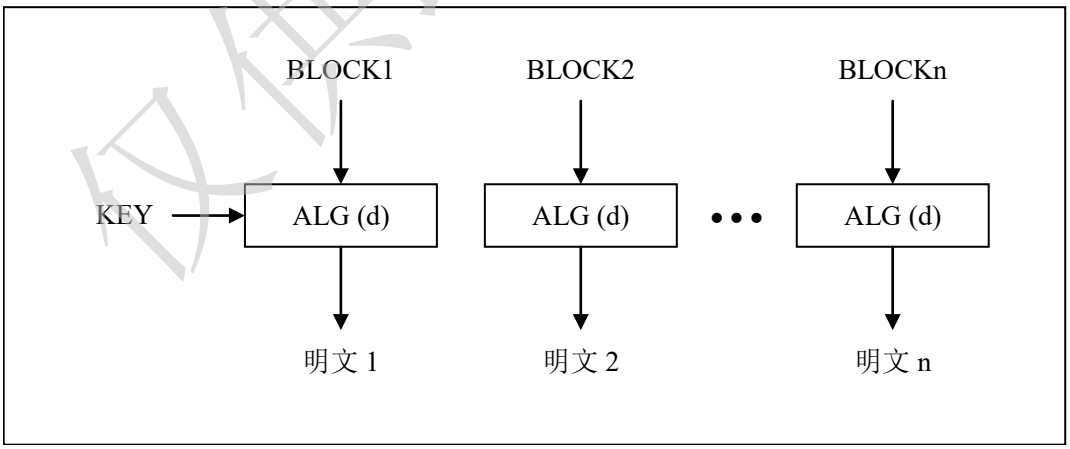


图 4–5 对数据解密的过程

5. 命令接口描述

5.1. 命令接口描述

SE 与主端之间使用命令与应答的通信机制，即主端发送命令，SE 接收并处理后发送响应数据给主端。这种机制包括两种数据单元——命令应用数据单元与响应应用数据单元。

SPI 和 I2C 通讯接口的通讯协议支持短 APDU 和扩展 APDU 两种格式，SE 根据下发的命令数据格式进行 APDU 格式的适配及处理。

命令应用数据单元包含两部分：固定的四个字节命令头和长度可变的命令体（可以不存在），其内容参见下表。

- APDU 命令/响应对结构

命令头				**命令体**		
CLA	INS	P1	P2	(Lc field)	数据域	(Le field)

响应应用数据单元也包括两部分：可能存在的响应数据体（应答体）和两个状态字节（应答尾部），如下表所示：

应答体	**应答尾部**
响应数据体	SW1 SW2

- APDU 命令串定义

{C(1)=CLA} {C(2)=INS} {C(3)=P1} {C(4)=P2} {C(5)…… C(n)}

- APDU 命令编码格式

类型	C(5)	C(6)C(7)	命令长度（字节）
CASE1	不存在	不存在	4
CASE2S	存在，任意值	不存在	5
CASE3S	存在，≠'00'	C(6)存在，C(7)可能存在	5+ (C(5))
CASE4S	存在，≠'00'	存在，任意值	6+ (C(5))
CASE2E	存在，='00'	存在，任意值	7
CASE3E	存在，='00'	存在，≠'0000'	7+ (C(6)C(7))
CASE4E	存在，='00'	存在，≠'0000'	9+ (C(6)C(7))

INS 字节为命令编码。

P1、P2 为命令参数。

Lc 表示数据域的长度。

Le 表示期望 SE 返回的数据长度。

5.2. 设备认证命令

5.2.1. EXTERNAL AUTHENTICATE 命令

5.2.1.1. 命令描述

EXTERNAL AUTHENTICATE 命令用于设备认证，所使用的密钥为设备主控密钥。

验证失败，密钥剩余次数减一，并清除设备权限。密钥剩余次数递减为 0 时，设备主控密钥将被锁定。

5.2.1.2. 使用条件和安全

上一条命令必须是 GET CHALLENGE 命令。

5.2.1.3. 命令格式

代码	数值（Hex）
CLA	‘00’
INS	‘82’
P1	‘00’
P2	‘00’
Lc	密钥分组长度
DATA	认证数据
Le	不存在

5.2.1.4. 响应信息

响应信息中可能的状态码为：

SW1	SW2	说明
90	00	命令执行成功
63	Cx	认证失败，还可认证 x 次（当剩余认证次数大于 15 时，x 为 ‘F’；否则，x 为剩余认证次数）
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	83	认证密钥锁定

69	84	引用数据无效（未申请随机数）
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错

5.3. PIN 操作指令

5.3.1. VERIFY PIN 命令

5.3.1.1. 命令描述

VERIFY PIN 命令要求 SE 对外部提供的 PIN 与 SE 中存放的参考 PIN 做比较验证。

验证失败，PIN 剩余次数减 1，并清除 PIN 对应的安全状态。剩余次数递减为 0 时，PIN 将被锁定。

5.3.1.2. 使用条件和安全

- 不能在 MF 下执行；
- 上一条命令必须是 GET CHALLENGE 命令。

5.3.1.3. 命令格式

代码	**数值（Hex）**								
CLA	‘00’								
INS	‘20’								
P1	‘00’								
P2	b8	b7	b6	b5	b4	b3	b2	b1	说　明
	0	0	0	0	0	0	0	0	管理员 PIN
	0	0	0	0	0	0	0	1	用户 PIN
Lc	‘10’								
DATA	验证数据								
Le	不存在								

将随机数和 PIN 明文顺序拼接后做摘要计算，取摘要计算结果的前 16 字节作为验证数据。

随机数按 16 字节使用，不足 16 字节的，先后补‘00’至 16 字节后，再使用。摘要计算时，PIN 明文仅考虑 PIN 的有效长度。摘要算法根据命令 CONFIG APP INFO 中“验证 PIN 算法”的配置值确定。

5.3.1.4. 响应信息

响应信息中可能的状态码为：

SW1	SW2	说明
90	00	命令执行成功
63	Cx	验证失败，‘x’表示剩余次数（当剩余认证次数大于 15 时，x 为‘F’；否则，x 为剩余认证次数）
65	81	写 FLASH 失败
67	00	Lc 长度错误
69	83	认证 PIN 锁定
6A	86	P1、P2 参数错
6A	88	未找到 PIN 数据
6D	00	命令不存在
6E	00	CLA 错

5.3.2. CHANGE/RELOAD PIN 命令

5.3.2.1. 命令描述

CHANGE PIN/ RELOAD PIN 命令允许修改管理员 PIN 和用户 PIN，或者使用管理员 PIN 重置用户 PIN。修改、重置后 PIN 的剩余次数恢复到建立时的初值。

如果新 PIN 密文解密失败，算作验证 PIN 失败一次，将清除 PIN 对应的安全状态，减少并返回 PIN 的剩余次数；当剩余次数为 0 时，表示 PIN 已经被锁死。相反，新 PIN 密文解密成功将获得相应的安全状态。

5.3.2.2. 使用条件和安全

- 不能在 MF 下执行；
- 上一条命令必须是 GET CHALLENGE 命令。

5.3.2.3. 命令格式

代码	数值（Hex）
CLA	‘80’
INS	‘5E’
P1	‘01’：修改 PIN ‘02’：重置用户 PIN 其他：RFU
P2	修改 PIN 时：

	‘00’：修改管理员 PIN ‘01’：修改用户 PIN 其他：RFU 重置用户 PIN 时：0
Lc	‘10’/‘20’
Data	新 PIN 密文
Le	不存在

将随机数和旧 PIN 明文（修改 PIN）/管理员 PIN 明文（重置用户 PIN）顺序拼接后做摘要计算，取摘要计算结果的前 16 字节作为子密钥，利用子密钥对新 PIN 进行异或加密。

随机数按 16 字节使用，不足 16 字节的，先后补‘00’至 16 字节后，再使用。摘要计算时，PIN 明文仅考虑 PIN 的有效长度。摘要算法根据命令 CONFIG APP INFO 中“验证 PIN 算法”的配置值确定。

5.3.2.4. 响应信息

响应信息中可能返回的状态码为：

SW1	SW2	含义
90	00	命令执行成功
63	Cx	验证失败，’x’ 表示剩余次数（当剩余认证次数大于 15 时，x 为‘F’；否则，x 为剩余认证次数）
65	81	FLASH 损坏，导致 SE 锁定
67	00	Lc 长度错
69	83	验证 PIN 锁定
6A	80	数据域参数不正确
6A	86	P1，P2 参数不正确
6A	88	未找到 PIN 数据
6D	00	命令不存在
6E	00	命令类型错

5.4. 密钥管理命令

5.4.1. WRITE KEY 命令

5.4.1.1. 命令描述

WRITE KEY 命令用于写入管理密钥（PIN/传输密钥），及更新设备主控密钥/传输密钥，

不支持更新 PIN。管理密钥将写入安全文件。

更新传输密钥时要求密钥用途、密钥标识符、密钥算法必须一致。

当 CLA 字节的后半字节等于十六进制‘4’时，表明命令数据采用密文方式传送。更新设备主控密钥时，使用设备主控密钥进行安全计算；写入/更新其他密钥时，使用安全文件中指定的传输密钥进行安全计算。当 CLA 字节的后半字节等于十六进制‘0’时，表明命令数据采用明文传送。

5.4.1.2. 使用条件和安全

- 修改设备主控密钥，需要获得设备权限；
- 写入管理密钥，更新传输密钥，需要获得安全文件的写权限。

5.4.1.3. 命令格式

代码	数值（Hex）
CLA	‘80’/‘84’
INS	‘D4’
P1	bit8~bit2：RFU bit1：操作类型 ‘0’：写入新密钥 ‘1’：更新已有密钥
P2	写入新密钥：无意义 更新已有密钥： ‘00’：更新设备主控密钥 其他：更新其他密钥
Lc	数据长度
Data	密钥信息明文/密文
Le	不存在

- 更新设备主控密钥时：

  密钥信息为设备主控密钥值。

- 更新其他密钥时：

  密钥信息为密钥用途+密钥标识符+密钥算法+密钥值；更新 PIN 时，密钥算法无意义，不检查。

- 写入管理密钥时：

密钥信息是密钥属性+密钥值，密钥属性定义如下：

PIN 属性：

用途	标识符	RFU	长度
1 字节	1 字节	4 字节	2 字节

传输密钥属性：

用途	标识符	算法	RFU	长度
1 字节	1 字节	1 字节	3 字节	2 字节

参数说明：

用途：密钥的用途

PIN：‘00’

传输密钥：‘01’

标识符：密钥的索引

管理员 PIN：‘00’，固定值

用户 PIN：‘01’，固定值

传输密钥：‘02’～‘FF’（当前 DF 下，仅首先写入的传输密钥有效，其他传输密钥不可用）

算法：高半字节为算法类型标识，低半字节为算法类型子标识（传输密钥仅支持 SM4 算法）

算法	值
3DES-128	‘00’
3DES-192	‘01’
SM4	‘40’
AES-128	‘60’
AES-192	‘61’
AES-256	‘62’

长度：

密钥类型	具体密钥分类	长度（字节）	说明
PIN		6~16	
DES	3DES_128	16	

	3DES_192	24	
AES	AES_128	16	
	AES_192	24	
	AES_256	32	
SM4		16	

5.4.1.4. 响应信息

响应信息中可能的状态码：

SW1	SW2	说 明
90	00	命令执行成功
65	81	写 FLASH 失败
67	00	长度错误
69	82	不满足权限
6A	80	数据域参数错误
6A	86	P1P2 错误
6D	00	命令不存在
6E	00	CLA 错误

5.4.2. GENERATE KEY 命令

5.4.2.1. 命令描述

GENERATE KEY 命令用于生成一个对称应用密钥，或完整的非对称应用密钥对，根据 KID 不同分为固定密钥和临时密钥。产生的非对称密钥对的公钥值，在响应报文中返回。

产生密钥时，无论是否已经存在密钥，无论算法类型和位长是否相同，SE 都会生成新的密钥。

5.4.2.2. 使用条件和安全

生成固定密钥需要获得安全文件的写权限。

5.4.2.3. 命令格式

代码	数值（Hex）
CLA	‘80’
INS	‘46’
P1	‘00’

P2	‘00’
Lc	‘08’ /‘10’
Data	命令数据
Le	不存在

如果生成对称应用密钥，数据域为：对称密钥的密钥属性，其中的“长度”数据项无意义。

如果使用一个密钥标识符 KID 管理生成的非对称密钥对，数据域为：密钥对的密钥属性，其中的“长度”数据项无意义。

如果使用不同密钥标识符 KID 管理生成的非对称密钥对，数据域为：公钥的密钥属性 + 私钥的密钥属性，其中的“长度”数据项无意义。

5.4.2.4. 响应信息

响应信息中的数据不存在，或为产生的密钥对的公钥，RSA 算法返回 E 和 N。

响应信息中可能的状态码为：

SW1	SW2	说 明
90	00	命令执行成功
67	00	Lc 长度错误
69	82	安全条件不满足
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错

5.4.3. GENERATE SHARED KEY 命令

5.4.3.1. 命令描述

GENERATE SHARED KEY 命令，生成用于对称运算的临时密钥。本命令支持以下三种生成方式：

- 基于 ECC256 的 NIST 曲线的 ECDH 密钥协商
- 基于 SM2 曲线的 ECDH 密钥协商
- 符合 SM2 国密规范的 SM2 密钥交换协议

5.4.3.2. 使用条件和安全

无使用条件限制。

5.4.3.3. 命令格式

代码	数值（Hex）
CLA	‘80’
INS	‘44’
P1	bit8~bit7：RFU bit6：SM2 密钥交换是否输出 64 字节校验值 S 0：不输出 1：输出 bit5：是否输出临时密钥 0：不输出 1：输出 bit4~bit1：密钥协商算法 0000：ECDH（ECC256） 0001：ECDH（SM2 曲线） 0010：SM2 密钥交换 其他：RFU
P2	ECDH：SE 内私钥标识符 KID SM2 密钥交换：无意义
Lc	命令数据长度
DATA	ECDH： 临时密钥的密钥标识符（1 字节） 临时密钥的算法类型（1 字节） 对方公钥（64 字节） SM2 密钥交换： 协商过程中 SE 的角色（1 字节），00：SE 为响应方，01：SE 为发起方 临时密钥的密钥标识符（1 字节） 临时密钥的算法类型（1 字节） SE 临时公钥 KID（1 字节） SE 临时私钥 KID（1 字节） SE 固有公钥 KID（1 字节） SE 固有私钥 KID（1 字节） 对方临时公钥（64 字节） 对方固有公钥（64 字节） SE 的 id 长度（1~32 字节） SE 的 id

	对方 id 长度（1~32 字节） 对方 id
Le	不存在

5.4.3.4. 响应信息

响应信息中的数据能为空，或期望长度的临时密钥，或期望长度的临时密钥+64 字节校验值 S。

响应信息中可能的状态码为：

SW1	SW2	说　明
90	00	命令执行成功
67	00	Lc 长度错误
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错

5.4.4. IMPORT KEY 命令

5.4.4.1. 命令描述

IMPORT KEY 命令可使用明文或密文方式导入应用密钥。固定应用密钥保存在安全文件中，密钥标识符 KID 为 00~EF。临时应用密钥保存在 SE 的 RAM 中，最多存储 16 条对称临时应用密钥，最多存储 2 条非对称临时应用密钥，密钥标识符 KID 为 F0~FF，密钥在 SE 掉电/选择 DDF 后自动失效。密文方式导入时，支持对称/非对称加密导入对称应用密钥，及对称加密导入非对称密钥。导入密钥时，无论指定应用密钥是否存在，及密钥属性是否一致，导入操作都会正常执行。

5.4.4.2. 使用条件和安全

- 导入固定应用密钥时，要需要获得安全文件的写权限；
- 非对称加密导入对称应用密钥时，需要获得指定私钥使用权限。

5.4.4.3. 命令格式

代码	数值（Hex）
CLA	‘80’
INS	‘3C’

P1	bit8：标识是否存在级联数据 ‘0’：不存在 ‘1’：存在 bit7：RFU bit6：加密密钥类型，密文导入时有效 ‘0’：应用密钥 ‘1’：传输密钥 bit5：密钥导入方式 ‘0’：明文导入 ‘1’：密文导入 bit4~bit1：加密算法，密文导入时有效 ‘0000’：DES ‘0100’：SM4 ‘0110’：AES ‘1000’：RSA ‘1001’：SM2 ‘1010’：ECC 其他：RFU
P2	明文导入密钥：无意义 密文导入密钥：解密用密钥的 KID，00~FF
Lc	数据域长度
Data	密钥信息
Le	不存在

导入应用密钥的数据格式为：

- 密钥属性+密钥值明文/密文

RSA 算法加密的密文数据在 SE 内处理流程如下：

- 使用 SE 内私钥解密数据；
- 根据 PKCS#1 规范，去除填充值，获得明文密钥值。

SM2/ECC 算法加密的密文数据，在 SE 内使用私钥解密数据获得明文密钥值。

对称密钥加密的密文数据，按 ISO9797_M2 方式解密，获得明文密钥值。

密钥属性定义如下：

- 对称应用密钥属性：

用途	标识符	算法	RFU	长度
1 字节	1 字节	1 字节	3 字节	2 字节

- 非对称应用密钥属性：

用途	标识符	算法	模长	使用权限	RFU	长度
1 字节	1 字节	1 字节	1 字节	1 字节	1 字节	2 字节

参数说明：

用途：密钥的用途

应用密钥：‘02’

标识符：密钥的索引

应用密钥：‘00’～ ‘FF’，其中，‘00’～ ‘EF’为保存在安全文件中的固定密钥，‘F0’～ ‘FF’为保存在临时密钥缓冲区中的临时密钥，最多支持 16 条临时对称密钥、2 条非对称临时密钥

算法：高半字节为算法类型标识，低半字节为算法类型子标识

算法	值
3DES-128	‘00’
3DES-192	‘01’
SM4	‘40’
AES-128	‘60’
AES-192	‘61’
AES-256	‘62’
RSA 公钥	‘80’
RSA_ND 私钥	‘81’
RSA_CRT 私钥	‘82’
RSA_ND 密钥对	‘83’
RSA_CRT 密钥对	‘84’
SM2 公钥	‘90’
SM2 私钥	‘91’
SM2 密钥对	‘92’
ECC 公钥	‘A0’

ECC 私钥	‘A1’
ECC 密钥对	‘A2’

使用权限：仅规定单私钥或公私钥对中私钥的使用权限

Bit8： APIN：1 使用密钥时，需要获得管理员权限

0 使用密钥时，不需获得管理员权限

Bit7： UPIN：1 使用密钥时，需要获得用户权限

0 使用密钥时，不需获得用户权限

模长：

算法	模长（字节）
RSA	32~64，模长/32 的值
SM2	32
ECC	32（仅支持 ECC256）

长度：

密钥类型	具体密钥分类	长度（字节）	说明
DES	3DES_128	16	
	3DES_192	24	
AES	AES_128	16	
	AES_192	24	
	AES_256	32	
SM4		16	
RSA	公钥	N+4	N 为模长，存储顺序 RSA-E、RSA-N
	ND 私钥	2N	N 为模长，存储顺序 RSA-N、RSA-D
	ND 密钥对	2N+4	N 为模长，存储顺序为 RSA-E、RSA-N、RSA-D
	CRT 私钥	5*（N/2）+4	N 为模长，存储顺序为 RSA-E、RSA-CRT-P、RSA-CRT-Q、RSA-CRT-DP、RSA-CRT-DQ、RSA-CRT-INVQ
	CRT 密钥对	7*（N/2）+4	N 为模长，存储顺序为 RSA-E、RSA-N、RSA-CRT-P、RSA-CRT-Q、

			RSA-CRT-DP 、 RSA-CRT-DQ 、 RSA-CRT-INVQ
SM2	公钥	64	存储顺序为 SM2-W-X、SM2-W-Y
	私钥	32	
	密钥对	96	存储顺序为公钥 SM2-W-X、SM2-W-Y、私钥 SM2-S
ECC	公钥	64	存储顺序为 ECC -W-X、ECC -W-Y
	私钥	32	
	密钥对	96	存储顺序为公钥 ECC -W-X、ECC -W-Y、私钥 ECC -S

注：

[1]装载密钥数据为级联时，第一块数据为密钥属性数据和第一包密钥值内容，后续块仅为密钥值内容；

[2]当密钥属性数据长度+密钥数据值内容长度小于等于单包最大数据长度时，必须一次性装载完所有密钥数据；

[3]级联数据必须为同一密钥的密钥组成元素。

5.4.4.4. 响应信息

响应信息中可能的状态码为：

SW1	**SW2**	**说 明**
90	00	命令执行成功
67	00	Lc 长度错误
69	81	指定解密密钥算法不符
6A	86	P1、P2 参数错
6A	88	指定解密密钥不存在
6D	00	命令不存在
6E	00	CLA 错

5.4.5. EXPORT KEY 命令

5.4.5.1. 命令描述

EXPORT KEY 命令用于以明文或密文的形式导出对称临时应用密钥和非对称临时应用私钥，及明文导出固定/临时非对称应用公钥。密文导出对称临时应用密钥时，支持非对称加密

和对称加密导出。密文导出非对称临时应用私钥时，仅支持对称加密导出。

待导出的应用密钥不存在，或密钥算法不符时，返回特定的错误状态码。

5.4.5.2. 使用条件和安全

- 导出非对称临时应用私钥时，需要获得该私钥的使用权限。

5.4.5.3. 命令格式

代码	数值（Hex）
CLA	‘80’
INS	‘3A’
P1	bit8~ bit7：RFU bit6：加密密钥类型，密文导出时有效 ‘0’：应用密钥 ‘1’：传输密钥 bit5：密钥导出方式 ‘0’：明文导出 ‘1’：密文导出 bit4~bit1：加密算法，密文导出时有效 ‘0000’：DES ‘0100’：SM4 ‘0110’：AES ‘1000’：RSA ‘1001’：SM2 ‘1010’：ECC 其他：RFU
P2	明文导出密钥：无意义 密文导出密钥：加密用密钥的 KID，00~FF
Lc	‘02’
Data	待导出应用密钥的密钥标识符（00~FF）+密钥算法
Le	不存在

其中，密钥算法可取值包括对称密钥算法值和非对称公钥/私钥算法值，不包括 RSA /SM2/ECC 密钥对。即便指定的应用密钥是 RSA /SM2/ECC 密钥对，为标识待导出密钥是公钥/私钥，密钥算法也只能取非对称公钥/私钥算法值。

5.4.5.4. 响应信息

响应信息中的数据为导出的应用密钥的值：

- 明文导出应用密钥时，应答数据即应用密钥值。
- RSA 算法加密导出对称临时应用密钥时，应答数据为对称临时应用密钥按照 PKCS#1 规范填充后的加密数据。
- SM2/ECC 算法加密导出对称临时应用密钥时，应答数据为对称临时应用密钥的加密数据。
- 对称算法加密导出临时应用密钥时，应答数据为临时应用密钥按照按 ISO9797_M2 方式计算的加密数据。

响应信息中可能的状态码为：

SW1	SW2	说　明
90	00	命令执行成功
67	00	Lc 长度错误
69	81	指定加密密钥算法不符
6A	86	P1、P2 参数错
6A	88	指定待导出密钥/加密密钥不存在
6D	00	命令不存在
6E	00	CLA 错

5.4.6. DELETE KEY 命令

5.4.6.1. 命令描述

DELETE KEY 命令用于删除指定密钥标识符 KID 的应用密钥。若指定的应用密钥不存在，DELETE KEY 命令仍能正常执行。

5.4.6.2. 使用条件和安全

删除固定应用密钥时，要需要获得安全文件的写权限。

5.4.6.3. 命令格式

代码	数值（Hex）
CLA	‘80’
INS	‘48’
P1	‘00’
P2	待删除的应用密钥标识符 KID：‘00’~‘FF’

Lc	‘00’
DATA	不存在
Le	不存在

5.4.6.4. 响应信息

响应信息中可能的状态码为：

SW1	SW2	说 明
90	00	命令执行成功
67	00	Lc 长度错误
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错

5.4.7. V2X GENERATE KEY DERIVE SEED 命令

5.4.7.1. 命令描述

V2X GENERATE KEY DERIVE SEED 命令用于根据指定的密钥衍生模式，生成密钥衍生种子。

SE 内部生成密钥衍生种子，包括：

1）1 个 SM4 密钥 KS，即签名对称密钥；

2）1 个 SM4 密钥 KE，即加密对称密钥；

3）1 对 SM2 密钥对（a，A=a * G），即签名密钥对，签名私钥 a 和签名公钥 A；

4）1 对 SM2 密钥对（p，P=p * G），即加密密钥对，加密私钥 p 和加密公钥 P；

上述密钥衍生种子中的 KS，KE，A，P 在命令响应信息中发送；KS、KE、a 和 p 保存在 SE 内，用于后续重构私钥。

5.4.7.2. 使用条件和安全

无

5.4.7.3. 命令格式

代码	数 值
CLA	‘80’

INS	‘4C’
P1	‘00’
P2	‘00’
Lc	不存在
DATA	不存在
Le	‘A0’

5.4.7.4. 响应信息

响应信息数据域包括：

SM4 密钥 KS	16 字节
SM4 密钥 KE	16 字节
SM2 公钥 A	64 字节
SM2 公钥 P	64 字节

响应信息中可能的状态码为：

SW1	**SW2**	**说　明**
90	00	命令执行成功
65	81	写 EEPROM 失败
67	00	Lc 长度错误
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错

5.4.8. V2X RECONSITUTION KEY 命令

5.4.8.1. 命令描述

V2X RECONSITUTION KEY 命令用于密钥衍生流程中重构私钥，并保存在指定 KID 中。

5.4.8.2. 使用条件和安全

必须存在密钥衍生种子。

5.4.8.3. 命令格式

代码	**数　值**
CLA	‘80’

INS	‘50’
P1	‘00’
P2	重构私钥的 KID(取值范围 00~EF)
Lc	数据长度
DATA	i（4 字节） j（4 字节） CTij（SM2 密文，对假名证书 PC 和私钥 c 加密得到的结果）
Le	不存在

密钥衍生算法流程如下表所示，其中步骤 1/2/8/9 为 SE 需要实现的内容。步骤 9 中需要的验签功能使用 VERIFY SIGNATURE 命令实现，本命令不做验签处理。

V2X设备	PRA	PCA
1) 生成： a) 1个SM4密钥k_S，即签名对称密钥； b) 1个SM4密钥k_E，即加密对称密钥； c) 1对SM2密钥对$(a, A = a * G)$，即签名密钥对，签名私钥因子a和公钥因子A； d) 1对SM2密钥对$(p, P = p * G)$，即加密种子密钥对，加密私钥因子p和公钥因子P。 2) 将(k_S, k_E, A, P)随EeRaCertRequest发送至PRA。	3) 对于每个(i^{INT}, j^{INT})，计算： a) 签名扩展公钥$B_{i,j}$，$B_{i,j} = A + f_S(k_S, i^{INT}, j^{INT}) * G$； b) 加密扩展公钥$Q_{i,j}$，$Q_{i,j} = P + f_E(k_E, i^{INT}, j^{INT}) * G$； 4) 对于每个$(i^{INT}, j^{INT})$，将生成的$(B_{i,j}, Q_{i,j})$随RaAcaCertRequest发送至PCA。	5) 生成1对SM2密钥$(c, C=c * G)$，用于向PRA隐藏假名证书中的完整公钥，计算完整公钥$S_{i,j} = B_{i,j} + C$； 6) 使用完整公钥$S_{i,j}$构ToBeSignedCertificate，签发显式证书$PC_{i,j}$，使用$Q_{i,j}$加密$(PC_{i,j}, c)$得到密文$CT_{i,j}$，PCA对该密文再次进行签名得到$SCT_{i,j}$，并将$SCT_{i,j}$发送至PRA。
	7) 对于某个V2X设备，PRA整理并打包其在某个i阶段所有的$SCT_{i,j}$，以及每一条$SCT_{i,j}$对应的j，待该V2X设备发起假名证书下载请求后返回。	

8) 对于每个(i^{INT}, j^{INT})，计算： a) 签名扩展私钥，$b_{i,j}=(a+f_S(k_S, i^{INT}, j^{INT}))$ mod l b) 加密扩展私钥，$q_{i,j}=(p+f_E(k_E, i^{INT}, j^{INT}))$ mod l 9) 对于每个(i^{INT}, j^{INT}), 验证$SCT_{i,j}$中的PCA签名： a) 如果验签成功，使用$q_{i,j}$解密$CT_{i,j}$得到($PC_{i,j}$, c)，计算该$PC_{i,j}$中的公钥对应的完整私钥$s_{i,j}=(b_{i,j}+c)$ mod l b) 如果验证失败，退出		

5.4.8.4. 响应信息

响应信息数据域包括：假名证书 PC。

响应信息中可能的状态码为：

SW1	SW2	说 明
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	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错

5.4.9. GET KEY INFO 命令

5.4.9.1. 命令描述

GET KEY INFO 命令用于读取密钥信息。

5.4.9.2. 使用条件和安全

无使用条件限制。

5.4.9.3. 命令格式

代码	数值（Hex）
CLA	‘80’
INS	‘42’
P1	‘00’：管理密钥 ‘01’：应用密钥 其他：RFU
P2	‘00’
Lc	不存在
Data	不存在
Le	‘xx’

5.4.9.4. 响应信息

响应信息中的数据固定为 512 字节，对应 256 条管理密钥/应用密钥的信息，密钥信息以密钥标识符为序号顺序排列，不存在的密钥，以 0xFFFF 标识。

管理密钥查询响应报文数据格式如下：

算法类型	首字节	次字节
PIN	‘00’：初始 PIN 值未更新 其他：初始 PIN 值已更新	剩余验证次数
传输密钥	算法类型	--

应用密钥查询响应报文数据格式如下：

算法类型	首字节：算法标识	次字节：非对称算法模长
3DES-128	‘00’	--
3DES-192	‘01’	--
SM4	‘40’	--
AES-128	‘60’	--
AES-192	‘61’	--
AES-256	‘62’	--
RSA 公钥	‘80’	32~64，模长/32 的值

RSA_ND 私钥	‘81’	
RSA_CRT 私钥	‘82’	
RSA_ND 密钥对	‘83’	
RSA_CRT 密钥对	‘84’	
SM2 公钥	‘90’	32
SM2 私钥	‘91’	
SM2 密钥对	‘92’	
ECC 公钥	‘A0’	32（仅支持 ECC256）
ECC 私钥	‘A1’	
ECC 密钥对	‘A2’	

响应信息中可能的状态码为：

SW1	SW2	说　明
90	00	命令执行成功
67	00	Lc 长度错误
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错

5.5. 密码运算命令

5.5.1. COMPUTE SIGNATURE 命令

5.5.1.1. 命令描述

COMPUTE SIGNATURE 命令用于非对称算法的签名运算，支持 RSA、ECC、SM2 算法。

RSA 算法支持对未摘要数据先计算摘要值，再按照 PKCS#1 进行数据填充后进行签名。

RSA 算法支持对摘要值按照 PKCS#1 进行数据填充后进行签名，也支持外部填充。外部填充时，SE 不做格式检查，长度合理的情况下直接签名即可。

ECC、SM2 支持对未摘要数据/摘要值计算签名。

5.5.1.2. 使用条件和安全

需要获得指定私钥的使用权限。

5.5.1.3. 命令格式

代码	数值（Hex）
CLA	‘80’
INS	‘36’
P1	bit8：标识是否存在级联数据 ‘0’：不存在 ‘1’：存在 bit7~bit5：非对称算法 ‘000’：RSA ‘001’：SM2 ‘010’：ECC 其他：RFU bit4：输入数据类型 ‘0’：未摘要数据 ‘1’：摘要值 bit3~bit1，标识摘要算法类型（输入数据是摘要值时无意义，不检查） ‘000’：SHA-1（适用于 RSA） ‘001’：SHA-224（适用于 RSA） ‘010’：SHA-256（适用于 RSA、ECC256） ‘011’：SHA-384（适用于 RSA） ‘100’：SHA-512（适用于 RSA） ‘101’：SM3（适用于 SM2） 其他：RFU
P2	‘00’~’FF’：应用密钥标识符 KID
Lc	待处理数据长度
Data	待处理数据
Le	不存在

命令报文数据域为待签名的数据：

a）输入数据为未摘要数据

SM2：摘要算法必须是 SM3（SM2_SM3）

ECC：摘要算法必须是 SHA-256（ECC256_SHA256）

RSA：摘要算法必须是 SHA-1/SHA-224/ SHA-256/ SHA-384/ SHA-512，填充规则符合 RSA PKCS#1 规范：00||01||PS||00||D||摘要值。其中：

- “D”字段如下：

RSA_SHA1：3021300906052b0e03021a05000414

RSA_SHA224：302d300d06096086480165030402040500041c

RSA_SHA256：3031300d06096086480165030402010500420

RSA_SHA384：3041300d06096086480165030402020500430

RSA_SHA512：3051300d06096086480165030402030500440

- “PS”字段为全 FF。

b）当输入数据为摘要值时：

SM2：摘要值必须是 32 字节（SM2_SM3）

ECC：摘要值必须是 32 字节（ECC256_SHA256）

RSA：可以是公钥模长（已由外部完成填充），也可是 20/28/32/48/64 字节（依次对应 SHA-1/SHA-224/ SHA-256/ SHA-384/ SHA-512 的结果，则继续按照 RSA PKCS#1 规范进行填充）

5.5.1.4. 响应信息

响应信息中的数据为签名结果。

响应信息中可能的状态码为：

SW1	SW2	说　明
90	00	命令执行成功
67	00	Lc 长度错误
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错

5.5.2. VERIFY SIGNATURE 命令

5.5.2.1. 命令描述

VERIFY SIGNATURE 命令用于非对称算法的验签运算，支持 RSA、ECC、SM2 算法。

5.5.2.2. 使用条件和安全

无使用条件限制。

5.5.2.3. 命令格式

代码	数值（Hex）
CLA	‘80’
INS	‘38’
P1	bit8：标识是否存在级联数据 ‘0’：不存在 ‘1’：存在 bit7~bit5：非对称算法 ‘000’：RSA ‘001’：SM2 ‘010’：ECC 其他：RFU bit4：输入数据类型 ‘0’：未摘要数据 ‘1’：摘要值 bit3~bit1，标识摘要算法类型（输入数据是摘要值时无意义，不检查） ‘000’：SHA-1（适用于 RSA） ‘001’：SHA-224（适用于 RSA） ‘010’：SHA-256（适用于 RSA、ECC256） ‘011’：SHA-384（适用于 RSA） ‘100’：SHA-512（适用于 RSA） ‘101’：SM3（适用于 SM2） 其他：RFU
P2	‘00’~’FF’：应用密钥标识符 KID
Lc	待处理数据长度
Data	待处理数据
Le	不存在

命令报文数据域格式要求：签名数据+未摘要数据/摘要值/已填充数据。

a）输入数据为未摘要数据

SM2：摘要算法必须是 SM3（SM2_SM3）

ECC：摘要算法必须是 SHA-256（ECC256_SHA256）

RSA：摘要算法必须是 SHA-1/SHA-224/ SHA-256/ SHA-384/ SHA-512，填充规则符合 RSA PKCS#1 规范：00||01||PS||00||D||摘要值。其中：

- “D”字段如下：

RSA_SHA1：3021300906052b0e03021a05000414

RSA_SHA224：302d300d06096086480165030402040500041c

RSA_SHA256：3031300d06096086480165030402010500420

RSA_SHA384：3041300d06096086480165030402020500430

RSA_SHA512：3051300d06096086480165030402030500440

- “PS”字段为全 FF。

b）当输入数据为摘要值时：

SM2：摘要值必须是 32 字节（SM2_SM3）

ECC：摘要值必须是 32 字节（ECC256_SHA256）

RSA：可以是公钥模长（已由外部完成填充），也可是 20/28/32/48/64 字节（依次对应 SHA-1/SHA-224/ SHA-256/ SHA-384/ SHA-512 的结果，则继续按照 RSA PKCS#1 规范进行填充）

5.5.2.4. 响应信息

响应信息中可能的状态码为：

SW1	SW2	说　明
90	00	命令执行成功
67	00	Lc 长度错误
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错

5.5.3. PKI ENCIPHER 命令

5.5.3.1. 命令描述

PKI ENCIPHER 命令用于非对称算法的数据加密运算，支持 RSA、ECC、SM2 算法。

5.5.3.2. 使用条件和安全

无使用条件限制。

5.5.3.3. 命令格式

代码	数值（Hex）
CLA	‘80’
INS	‘30’
P1	bit8：标识是否存在级联数据 ‘0’：不存在 ‘1’：存在 bit7~bit5：非对称算法 ‘000’：RSA ‘001’：SM2 ‘010’：ECC 其他：RFU bit4~bit2：RFU bit1：RSA 填充模式（指定密钥为 RSA 算法时有效） ‘0’：NOPADDING ‘1’：PKCS#1
P2	‘00’~’FF’：应用密钥标识符 KID
Lc	待处理数据长度
Data	待处理数据
Le	不存在/待读取数据长度

命令报文数据域为待加密的数据。

注 1：RSA 加密计算说明：

a）采用 NOPADDING 模式时，填充过程在 SE 外部实现；

b）采用 PKCS#1 时，填充规则为 00||02||PS||00||M，其中：

- PS 字段为非零随机数，至少是 8 字节；
- M 为待加密的明文，长度不能大于（模长-11）。

注 2：SM2 、ECC 加密数据最大支持 4096 字节。

5.5.3.4. 响应信息

响应信息中的数据为加密结果。

定义	要求
RSA	RSA 模长
SM2	C1||C3||C2，其中： C1 长度为 64 字节， C3 长度为 32 字节， C2 长度最大不超过 4096 字节
ECC	加密输出数据格式符合 SEC 标准，结构为 R||EM||D，其中： R 长度为 64 字节， EM 长度最大不超过 4096 字节， D 长度为 32 字节

响应信息中可能的状态码为：

SW1	SW2	说 明
90	00	命令执行成功
61	xx	剩余 xx 字节应答数据可读取
67	00	Lc 长度错误
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错

5.5.4. PKI DECIPHER 命令

5.5.4.1. 命令描述

PKI DECIPHER 命令用于非对称算法的数据解密运算，支持 RSA、ECC、SM2 算法。

5.5.4.2. 使用条件和安全

需要获得指定私钥的使用权限。

5.5.4.3. 命令格式

代码	数值（Hex）
CLA	‘80’
INS	‘32’

P1	bit8：标识是否存在级联数据 ‘0’：不存在 ‘1’：存在 bit7~bit5：非对称算法 ‘000’：RSA ‘001’：SM2 ‘010’：ECC 其他：RFU bit4~bit2：RFU bit1：RSA 填充模式（指定密钥为 RSA 算法时有效） ‘0’：NOPADDING ‘1’：PKCS#1
P2	‘00’~’FF’：应用密钥标识符 KID
Lc	待处理数据长度
Data	待处理数据
Le	不存在/待读取数据长度

命令报文数据域为待解密的数据。

注 1：RSA 解密计算说明：

a）采用 NOPADDING 模式时，去填充过程在 SE 外部实现；

b）采用 PKCS#1 时，去填充过程在 SE 内部实现。

注 2：SM2 、ECC 解密最大支持 96+4096 字节。

5.5.4.4. 响应信息

响应信息中的数据为解密结果。

响应信息中可能的状态码为：

SW1	**SW2**	**说 明**
90	00	命令执行成功
61	xx	剩余 xx 字节应答数据可读取
67	00	Lc 长度错误
6A	86	P1、P2 参数错
6D	00	命令不存在

6E	00	CLA 错

5.5.5. CIPHER DATA 命令

5.5.5.1. 命令描述

CIPHER DATA 命令用于对称算法的加密、解密、MAC 计算、MAC 验证运算。

对称算法的 MAC 计算/验证，除了支持 NoPadding 模式，同时也支持 M1 和 M2 的 Padding 模式。其中，NoPadding 表示不进行内部补位，输入数据必须为分组长度的整数倍；M1 为强制补‘00’后，再使用‘00’填充到分组长度整数倍；M2 为强制补‘80’后，再用‘00’填充到分组长度整数倍。

5.5.5.2. 使用条件和安全

无使用条件限制。

5.5.5.3. 命令格式

代码	**数值（Hex）**
CLA	‘80’
INS	‘3E’
P1	bit8：标识是否存在级联数据 ‘0’：不存在 ‘1’：存在 bit7~bit5：对称算法 ‘000’：DES ‘100’：SM4 ‘110’：AES 其他：RFU bit4~bit3：计算类型 ‘00’：加密 ‘01’：解密 ‘10’：MAC 计算 ‘11’：MAC 验证 bit2-bit1：加解密模式，加解密计算时有效 ‘00’：ECB ‘01’：CBC

	其他：RFU bit2-bit1：MAC 填充方式，MAC 计算/验算时有效 ‘00’：NOPADDING ‘01’：ISO9797_M1 ‘10’：ISO9797_M2 其他：RFU
P2	‘00’~’FF’：应用密钥标识符 KID
Lc	待处理数据长度
Data	待处理数据
Le	不存在

命令数据域报文格式如下：

定义	算法模式	字节数	说明
IV	CBC 加密、解密 MAC 计算/ MAC 验证	8/16	初始向量
	其他	0	
数据	全部		待计算数据
MAC	MAC 验证	8/16	待验证 MAC 值
	其他	0	

5.5.5.4. 响应信息

响应信息中的数据为计算结果：

模式	字节数	说明
加密操作 解密操作	0 或 8/16 整数倍	当收到密钥算法块长度的数据后进行加解密运算并返回
计算 MAC	0 或 8/16	在收到所有数据后返回 MAC 值，MAC 值为 CBC 算法计算的最后一块。
验证 MAC	0	无返回

响应信息中可能的状态码为：

SW1	SW2	说　明
90	00	命令执行成功
61	xx	剩余 xx 字节应答数据可读取

67	00	Lc 长度错误
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错

5.5.6. HASH OPERATION 命令

5.5.6.1. 命令描述

HASH OPERATION 命令是将命令输入的数据通过指定的摘要算法计算成一个摘要值。支持 SHA-1、SHA-224、SHA-256、SHA-384、SHA-512 和 SM3 摘要算法。待计算的数据通过一条或多条 HASH OPERATION 命令发送至 SE，SE 收完所有的待计算数据块后，返回一个固定长度的摘要值。

5.5.6.2. 使用条件和安全

无使用条件限制。

5.5.6.3. 命令格式

代码	**数值（Hex）**
CLA	‘80’
INS	‘34’
P1	bit8：标识是否存在级联数据 ‘0’：不存在 ‘1’：存在 bit7：标识是否存在对称应用密钥参与摘要计算 ‘0’：不存在 ‘1’：存在 bit6：标识对称应用密钥与外部输入数据的级联关系（存在对称应用密钥参与摘要计算、且同时输入外部数据时有效） ‘0’：对称应用密钥在前、外部输入数据在后 ‘1’：外部输入数据在前、对称应用密钥在后 bit5~bit4：RFU bit3~bit1：标识摘要算法类型（仅首条命令有效，后续命令不检查） ‘000’：SHA-1（适用于 RSA） ‘001’：SHA-224（适用于 RSA） ‘010’：SHA-256（适用于 RSA、ECC256）

	‘011’：SHA-384（适用于 RSA） ‘100’：SHA-512（适用于 RSA） ‘101’：SM3（适用于 SM2） 其他：RFU
P2	‘00’~‘FF’：存在对称应用密钥参与摘要计算时有效，否则无意义
Lc	待处理数据的长度
Data	待处理数据/不存在
Le	不存在

本命令数据域是外部输入的待计算数据，可能不存在。

5.5.6.4. 响应信息

响应信息中的数据为摘要计算值，若当前命令不是最后一条 HASH OPERATION 命令，则响应数据不存在。

响应信息中可能的状态码为：

SW1	SW2	说 明
90	00	命令执行成功
67	00	Lc 长度错误
6A	86	P1、P2 参数错
6A	88	指定应用密钥不存在
6D	00	命令不存在
6E	00	CLA 错

5.5.7. SM2 GET ZA 命令

5.5.7.1. 命令描述

SM2 GET ZA 命令辅助 SM2 签名运算，用于获得 32 字节 Za 数据。

5.5.7.2. 使用条件和安全

无使用条件限制。

5.5.7.3. 命令格式

代码	数值（Hex）
CLA	‘80’
INS	‘4E’

P1	‘00’
P2	‘00’
Lc	’42’~‘61’
DATA	用户 ID 长度（1 字节）+用户 ID（1~32 字节）+用户公钥（64 字节）
Le	不存在

5.5.7.4. 响应信息

响应信息中的数据为 32 字节 Za 计算结果。

响应信息中可能的状态码为：

SW1	SW2	说 明
90	00	命令执行成功
67	00	Lc 长度错误
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错

5.6. 随机数命令

5.6.1. GET CHALLENGE 命令

5.6.1.1. 命令描述

GET CHALLENGE 命令用于向 SE 请求一个用于安全过程的随机数。

该随机数只能用于紧随其后的下一条命令，无论下一条命令是否使用了该随机数，该随机数都将立即失效。

5.6.1.2. 使用条件和安全

无使用条件限制。

5.6.1.3. 命令格式

代码	数值（Hex）
CLA	‘00’
INS	‘84’
P1	‘00’
P2	‘00’

Lc	不存在
DATA	不存在
Le	‘04’/‘08’/‘10’

5.6.1.4. 响应信息

响应信息中的数据为随机数。

响应信息中可能的状态码参为：

SW1	SW2	说 明
90	00	命令执行成功
67	00	Lc 长度错误
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错

5.7. 文件管理命令

5.7.1. CREATE FILE 命令

5.7.1.1. 命令描述

CREATE FILE 命令用于在 SE 内建立 DF 和二进制文件。创建 DF 文件同时在 DF 下自动创建安全文件。

5.7.1.2. 使用条件和安全

- 创建 MF 下的 DDF 需要获得设备权限；
- 创建 DDF/ADF 下的文件，需要获得该 DF 下文件的创建权限。

5.7.1.3. 命令格式

代码	数值（Hex）
CLA	‘80’
INS	‘E0’
P1	‘00’
P2	‘01’：DDF 文件 ‘02’：ADF 文件 ‘03’：二进制文件 其它：RFU

Lc	命令数据长度
DATA	文件信息数据
Le	无

数据域定义如下：

DDF/ADF	
6~70 字节	文件标识符(FID)——2 字节 文件创建权限(Create-Right)——1 字节 bit8——APIN，创建/删除文件时，是否需要获得管理员权限，‘1’需要 bit7——UPIN，创建/删除文件时，是否需要获得用户权限，‘1’需要 bit6~bit2：RFU bit1——FLAG，创建的 DDF 是否是默选 DDF，‘1’是（创建 DDF 时有效，整个文件系统只允许创建 1 个默选 DDF） 安全文件写属性(Acw)——1 字节 bit8——APIN，写入密钥时，是否需要获得管理员权限，‘1’需要 bit7——UPIN，写入密钥时，是否需要获得用户权限，‘1’需要 bit6~bit1：RFU 安全文件传输密钥标识符(WT-KID)——1 字节 文件名长度——1 字节 文件名——0 到 64 字节
二进制文件	
9~41 字节	文件标识符(FID)——2 字节 文件大小(LNG)——2 字节 文件读属性(Acr)——1 字节 bit8——APIN，读操作时，是否需要获得管理员权限，‘1’需要 bit7——UPIN，读操作时，是否需要获得用户权限，‘1’需要 bit6~bit1：RFU 文件写属性(Acw)——1 字节 bit8——APIN，写操作时，是否需要获得管理员权限，‘1’需要 bit7——UPIN，写操作时，是否需要获得用户权限，‘1’需要 bit6~bit4：RFU bit3——DISU，‘1’不能进行修改操作

	bit2~bit1：RFU 文件读传输密钥标识符(RT-KID)——1 字节 文件写传输密钥标识符(WT-KID)——1 字节 文件名长度——1 字节 文件名——0 到 32 字节

5.7.1.4. 响应信息

响应信息中可能的状态码：

SW1	SW2	说 明
90	00	命令执行成功
65	81	写 FLASH 失败
67	00	长度错误
69	82	不满足权限
69	85	使用条件不满足
6A	80	数据域参数错误
6A	86	P1P2 错误
6D	00	命令不存在
6E	00	CLA 错误

5.7.2. DELETE FILE 命令

5.7.2.1. 命令描述

DELETE FILE 命令用于删除指定的 DDF/ADF/EF 文件。删除 DDF/ADF 时，其下的所有文件同时删除。删除 EF 后，若该 EF 为当前 EF，则当前 EF 变为空。

5.7.2.2. 使用条件和安全

- 删除 MF 下的 DDF，需要获得设备权限；
- 删除其他文件，需要获得当前 DF 的创建权限。

5.7.2.3. 命令格式

代码	数值（Hex）
CLA	‘80’
INS	‘E4’
P1	‘00’：删除指定的 DDF/ADF

	‘01’：删除指定的 EF ‘02’：删除指定的文件
P2	‘00’
Lc	P1=‘00’：‘01’~‘40’ P1=‘01’：‘01’~‘20’ P1=’02’：’02’
DATA	P1=‘00’：DF 文件名 P1=‘01’：EF 文件名 P1=’02’：文件的 FID
Le	**不存在**

5.7.2.4. 响应信息

响应信息中可能的状态码为：

SW1	**SW2**	**说 明**
90	00	命令执行成功
65	81	写 FLASH 失败
67	00	Lc 长度错误
69	82	安全条件不满足
6A	82	未找到文件
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错
69	85	使用条件不满足

5.7.3. CLEAR MF 命令

5.7.3.1. 命令描述

CLEAR MF 命令可以删除 MF 文件体的内容，保留当前 MF 文件头，同时将设备主控密钥恢复为初始值。

5.7.3.2. 使用条件和安全

需要获得设备权限。

5.7.3.3. 命令格式

代码	数值（Hex）
CLA	‘80’
INS	‘CE’
P1	‘00’
P2	‘00’
Lc	‘00’
DATA	不存在
Le	不存在

5.7.3.4. 响应信息

响应信息中可能的状态码：

SW1	SW2	说 明
90	00	命令执行成功
65	81	写 FLASH 失败
67	00	长度错误
69	82	不满足权限
6A	86	P1P2 错误
6D	00	命令不存在
6E	00	CLA 错误

5.7.4. SELECT FILE 命令

5.7.4.1. 命令描述

SELECT FILE 命令通过文件标识符或文件名来选择 COS 中的 MF、DDF、ADF 或 EF 文件。

如果成功选择 MF，则设备主控权限清零；如果成功选择了 DDF，则 DDF 的安全状态字清零。

5.7.4.2. 使用条件和安全

无使用条件限制。

5.7.4.3. 命令格式

代码	数值（Hex）
CLA	‘00’
INS	‘A4’
P1	‘00’：通过 FID 选择 MF、DF、EF（Lc=‘00’时，选择 MF） ‘04’：通过文件名选择 DF、EF 其他：RFU
P2	‘00’
Lc	若 P1=‘00’, ‘00’/‘02’ 若 P1=‘04’, ‘01’~‘40’ （DF：1~64，EF：1~32）
DATA	若 P1=‘00’，不存在或 FID 若 P1=‘04’，文件名
Le	不存在

5.7.4.4. 响应信息

响应信息中可能的状态码为：

SW1	SW2	说 明
90	00	命令执行成功
67	00	Lc 长度错误
6A	82	未找到文件
6A	86	P1、P2 参数错
6D	00	命令不存在，未初始化状态
6E	00	CLA 错

5.7.5. READ BINARY 命令

5.7.5.1. 命令描述

READ BINARY 命令用于读出二进制文件的内容。

读取的数据是否加密返回，通过 CLA 进行判断：CLA 为‘00’则明文返回，CLA 为‘04’则为密文返回。

5.7.5.2. 使用条件和安全

需要获得文件的读权限。

5.7.5.3. 命令格式

代码	数值（Hex）								
CLA	‘00’/‘04’								
INS	‘B0’								
P1	b8	b7	b6	b5	b4	b3	b2	b1	说 明
	0	x	x	x	x	x	x	x	当前 EF 文件偏移地址高字节
	1	0	0	x	x	x	x	x	通过 SFI 方式访问
P2	若 P1 的 b8=0，偏移地址低字节 若 P1 的 b8=1，偏移地址								
Lc	不存在								
DATA	不存在								
Le	期望返回的数据								

5.7.5.4. 响应信息

响应信息中的数据为二进制文件明文或密文数据。

响应信息中可能的状态码为。

SW1	SW2	说 明
90	00	命令执行成功
67	00	Lc 长度错误
6A	86	P1、P2 参数错
6C	xx	Le 错误，正确值为 xx
6D	00	命令不存在
6E	00	CLA 错

5.7.6. UPDATE BINARY 命令

5.7.6.1. 命令描述

UPDATE BINARY 命令用命令中给定的数据代替二进制文件中已有的数据。

更新数据是否采用加密模式，通过 CLA 进行判断：CLA 为‘00’则明文写，CLA 为‘04’则为密文写。

5.7.6.2. 使用条件和安全

需要获得文件的写权限。

5.7.6.3. 命令格式

代码	数值（Hex）								
CLA	‘00’/‘04’								
INS	‘D6’								
P1	b8	b7	b6	b5	b4	b3	b2	b1	说 明
	0	x	x	x	x	x	x	x	当前 EF 文件偏移地址高字节
	1	0	0	x	x	x	x	x	通过 SFI 方式访问
P2	若 P1 的 b8=0，偏移地址低字节 若 P1 的 b8=1，偏移地址								
Lc	数据长度								
DATA	明文/密文数据								
Le	不存在								

5.7.6.4. 响应信息

响应信息中可能的状态码为：

SW1	SW2	说 明
90	00	命令执行成功
67	00	Lc 长度错误
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错

5.7.7. GET FILE INFO 命令

5.7.7.1. 命令描述

GET FILE INFO 命令用于读取当前目录下的 DF 和 EF 的文件信息。DF 返回文件名、文件创建权限、DF 类型、安全文件写密钥标识符信息；EF 返回文件名、文件大小、读权限、写权限、读密钥标识符、写密钥标识符信息。

5.7.7.2. 使用条件和安全

无使用条件限制。

5.7.7.3. 命令格式

代码	数值（Hex）
CLA	‘80’
INS	‘4A’
P1	‘00’：DF 信息 ‘01’：EF 信息 其他：RFU
P2	‘00’
Lc	不存在
Data	不存在
Le	‘xx’

5.7.7.4. 响应信息

响应信息中的数据为当前目录下所有 DF 或 EF 的文件信息：

单个 DF 信息：FID 长度 + FID + 文件名长度 + 文件名 + 文件创建权限长度 + 文件创建权限 + DF 类型长度 + DF 类型 + 安全文件写权限长度 + 安全文件写权限 + 安全文件写密钥标识符长度 + 安全文件写密钥标识符。

单个 EF 信息：FID 长度 + FID +文件名长度 + 文件名 + 文件大小长度 + 文件大小 + 读权限长度 + 读权限 + 写权限长度 + 写权限 + 读密钥标识符长度 + 读密钥标识 + 写密钥标识符长度 + 写密钥标识符。

响应信息中可能的状态码为：

SW1	SW2	说 明
90	00	命令执行成功（包括无 DF 或 EF 文件）
61	xx	剩余 xx 字节应答数据可读取
6A	86	P1、P2 参数错
6D	00	命令不存在（未初始化状态）
6E	00	CLA 错

5.8. 信息管理命令

5.8.1. WRITE SEID 命令

5.8.1.1. 命令描述

写入 SEID 时，COS 将命令数据域中的 SEID 值将保持到芯片内。

5.8.1.2. 使用条件和安全

需要获得设备权限。

5.8.1.3. 命令格式

代码	数值（Hex）
CLA	‘80’
INS	‘D2’
P1	‘00’
P2	‘00’
Lc	‘01’~‘FF’
DATA	SEID
Le	不存在

5.8.1.4. 响应信息

响应信息中可能的状态码为：

SW1	SW2	说 明
90	00	命令执行成功
67	00	Lc 长度错误
69	82	安全条件不满足
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错

5.8.2. GET SEID 命令

5.8.2.1. 命令描述

GET SEID 命令用于从 SE 读取 SEID 值。

5.8.2.2. 使用条件和安全

无使用条件限制。

5.8.2.3. 命令格式

代码	数值（Hex）
CLA	‘80’
INS	‘40’

P1	‘00’
P2	‘00’
Lc	不存在
DATA	不存在
Le	‘xx’

5.8.2.4. 响应信息

响应信息中的数据为 SEID 的值。

响应信息中可能的状态码为：

SW1	SW2	说 明
90	00	命令执行成功
6A	86	P1、P2 参数错
6A	88	SEID 未配置
6C	xx	Le 错误，正确值为 xx
6D	00	命令不存在
6E	00	CLA 错

5.8.3. QUERY 命令

5.8.3.1. 命令描述

QUERY 命令用于读取芯片唯一序列号、产品信息。

5.8.3.2. 使用条件和安全

无使用条件限制。

5.8.3.3. 命令格式

代码	数值（Hex）
CLA	‘80’
INS	‘C8’
P1	‘00’：读取芯片 8 字节唯一序列号 ‘01’：读取产品信息 其他：RFU
P2	‘00’
Lc	不存在
DATA	不存在

Le	P1 = ‘00’ 时：‘08’ P1 = ‘01’ 时：‘01’ ~ ‘08’

5.8.3.4. 响应信息

响应信息中的数据：

- 产品信息

说明	长度	值	备注
软件信息	3	‘316000’	
软件扩展信息	3	‘xxxxxx’	以配置值为准
RFU	2	‘0000’	保留 2 字节

响应信息中可能的状态码为：

SW1	SW2	说 明
90	00	命令执行成功
6A	86	P1、P2 参数错
6C	xx	Le 错误，正确值为 xx
6D	00	命令不存在
6C	xx	Le 错误，正确值为 xx
6E	00	CLA 错
67	00	Lc 长度错误

5.9. 其他命令

5.9.1. GET RESPONSE 命令

5.9.1.1. 命令描述

GET RESPONSE 命令用来从 SE 向主端传送 APDU 应答数据。

5.9.1.2. 使用条件和安全

无使用条件限制。

5.9.1.3. 命令格式

代码	数值（Hex）
CLA	‘00’
INS	‘C0’
P1	‘00’

P2	‘00’
Lc	不存在
DATA	不存在
Le	‘xx’

5.9.1.4. 响应信息

响应信息中的数据为应答数据。

响应信息中可能的状态码为：

SW1	SW2	说 明
90	00	命令执行成功
67	00	Lc 长度错误
6A	86	P1、P2 参数错
6C	xx	Le 错误，正确值为 xx
6D	00	命令不存在
6E	00	CLA 错
6F	00	无待读取的应答数据

5.9.2. CONFIG APP INFO 命令

5.9.2.1. 命令描述

修改 SE 应用参数配置。

5.9.2.2. 使用条件和安全

无使用条件限制。

5.9.2.3. 命令格式命令格式

代码	数值（Hex）
CLA	‘80’
INS	‘F7’
P1	‘06’：MAC 计算方式 ‘0C’：低功耗模式 ‘0E’：误唤醒后重进低功耗状态时间间隔 其他值：预留
P2	见下表

Lc	见下表
DATA	见下表
Le	不存在

配置说明如下：

P1	P2	LC	DATA
06	00	01	MAC 计算方式（默认 0x00） 00：ISO9797-1 计算模式 3 01：ISO9797-1 计算模式 1 其他：保留
0C	00	01	‘00’：空闲时 SE 保持工作状态（默认值） ‘01’/‘02’：空闲时 SE 自动进入 standby 状态 其他值：RFU
0E	00	04	误唤醒后重进低功耗状态时间间隔，SE 配置为自动进入 standby 状态时有效，单位为毫秒，取值范围 0.1 秒~12 小时（0x064~0x36EE80）。 （默认 60 秒，0x0000EA60）

5.9.2.4. 响应信息

响应信息中可能的状态码参考附录。

5.9.3. ENTER LOWPOWER 命令

5.9.3.1. 命令描述

ENTER LOWPOWER 命令用于 SE 进入低功耗模式，等待唤醒。

5.9.3.2. 使用条件和安全

无使用条件限制。

5.9.3.3. 命令格式

代码	数值（Hex）
CLA	‘80’
INS	‘E2’
P1	‘00’
P2	‘00’
Lc	‘00’

DATA	不存在
Le	不存在

5.9.3.4. 响应信息

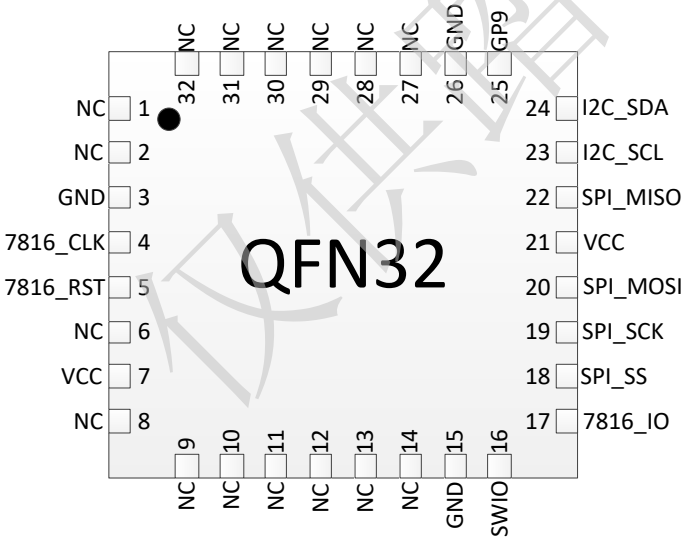
响应信息中可能的状态码：

SW1	SW2	说 明
90	00	命令执行成功
67	00	长度错误
6A	86	P1P2 错误
6D	00	命令不存在
6E	00	CLA 错误

6. 封装定义

SE 产品采用 QFN32 封装。

6.1. 封装示意图

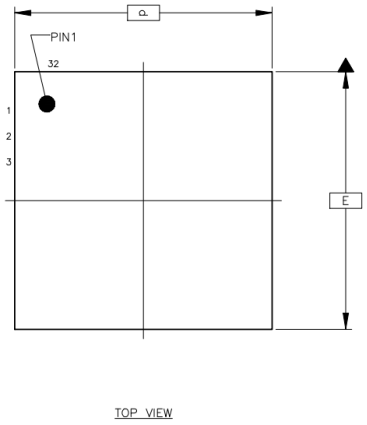


6.2. 管脚定义

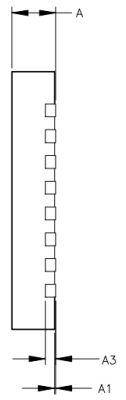
管脚编号	管脚名	管脚特性	描述
1	NC	-	-
2	NC	-	-

3	GND	电源地	-
4	7816_CLK	IO	未使用
5	7816_RST	IO	SE 复位信号，低有效
6	NC	-	-
7	VCC	电源	电源输入，1.62V～5.5V，为芯片提供电源（芯片内部与 21 脚连通）
8	NC	-	-
9	NC	-	-
10	NC	-	-
11	NC	-	-
12	NC	-	-
13	NC	-	-
14	NC	-	-
15	GND	电源地	-
16	SWIO	IO	未使用
17	7816_IO	IO	未使用
18	SPI_SS	IO	SPI_SS，内部上拉
19	SPI_SCK	IO	SPI_SCK，内部下拉
20	SPI_MOSI	IO	SPI_MOSI，内部上拉
21	VCC	电源	电源输入，1.62V~5.5V，为芯片提供电源（芯片内部与 7 脚连通）
22	SPI_MISO	IO	SPI_MISO，内部上拉
23	I2C_SCL	IO	I2C_SCL，内部上拉
24	I2C_SDA	IO	I2C_SDA，内部上拉
25	GP9	IO	未使用
26	GND	电源地	-
27	NC	-	-
28	NC	-	-
29	NC	-	-
30	NC	-	-
31	NC	-	-
32	NC	-	-

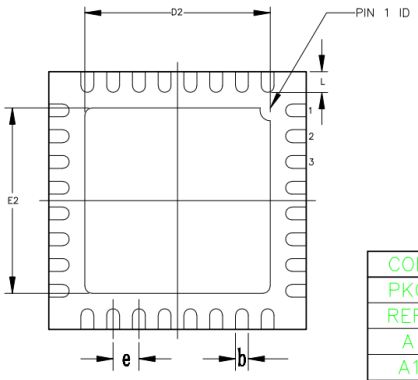
6.3. 封装尺寸



TOP VIEW



SIDE VIEW



BOTTOM VIEW

COMMON DIMENISIONS(MM)			
PKG	QFN32(5X5)		
REF.	MIN.	NOM.	MAX.
A	0.70	0.75	0.80
A1	0.00	–	0.05
A3	0.2 REF.		
D	4.90	5.00	5.10
E	4.90	5.00	5.10
b	0.18	0.25	0.30
L	0.30	0.40	0.50
D2	3.45	3.60	3.70
E2	3.45	3.60	3.70
e	0.5 BSC		

7. 附录 A：INS 支持表

CLA	INS	描述
00	20	验证 PIN 码
80	30	非对称加密计算
80	32	非对称解密计算
80	34	摘要计算
80	36	非对称签名计算
80	38	非对称验签计算
80	3A	导出对称临时应用密钥和非对称临时应用私钥 导出固定/临时非对称应用公钥
80	3C	导入应用密钥
80	3E	对称加解密计算
80	40	读取 SEID 值
80	42	读取密钥信息
80	44	密钥协商
80	46	生成对称应用密钥或者非对称应用密钥对
80	48	删除指定的应用密钥
80	4A	读取当前目录下 DF 和 EF 的文件信息
80	4C	生成密钥衍生种子
80	4E	计算 SM2 算法的 Za
80	50	密钥衍生算法重构私钥
80	5E	修改管理员 PIN 和用户 PIN，或者使用管理 PIN 重置用户 PIN
00	82	设备认证
00	84	取随机数
00	A4	选择文件
00/04	B0	读二进制文件
00	C0	Case4 情况获取响应数据
80	C8	获取 SE 信息
80	CE	删除 MF 文件体，生命周期回到已初始化状态
80	D2	写 SEID 值

80/84	D4	写入/更新管理密钥
00/04	D6	更新二进制文件
80	E0	创建文件
80	E2	进入低功耗模式
80	E4	删除指定的 DDF/ADF/EF 文件
80	F5	系统参数配置
80	F7	应用参数配置

8. 附录 B：响应状态码

SW1	SW2	描述
90	00	正确执行
61	xx	尚有数据未返回
63	Cx	x 表示剩余认证次数（当剩余认证次数大于 15 时，x 为‘F’；否则，x 为剩余认证次数）
65	81	写 FLASH 不成功
67	00	错误的长度
69	81	命令与文件结构不相容
69	82	安全条件不满足
69	83	密钥被锁死
69	84	没有取随机数
69	85	使用条件不满足
69	86	没有选择当前可操作的文件
69	88	安全报文数据项不正确
6A	80	数据结构不正确/验签失败
6A	82	文件未找到
6A	84	空间不足
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/实际返回数据是 xx
6D	00	不支持的指令代码
6E	00	无效的 CLA
6F	00	数据无效

94	06	所需的 MAC 不可用