江安天安

金融数据密码机

应用开发手册

北京江南天安科技有限公司

2017 年 1 月

声　明

《江安天安金融数据密码机应用开发手册》V1.48。

本手册由北京江南天安科技有限公司编写，仅赠送给用户和合作伙伴参阅。天安科技TASS保留对本手册的所有权和解释权，任何公司和个人未经允许，不得擅自使用、复制、修改、传播本手册的内容。

天安科技保留有对本手册进行重新修订的权利,随时可能对本手册中出现的错误、与最新资料不符之处、命令的更新等做必要的修改，这些不再另行通知，但全部编入新版手册内。

本书适用于北京江南天安 SJJ1310、SJJ1321-A、SJJ1511 金融数据密码机。

北京江南天安科技有限公司

二〇一七年一月

版本历史

手册版本	时间	适应HSM主机服务版本	文档更新说明
V1.48	2017-01-12	H1.24.55	增加 QC 指令，产生 IBM PIN Offset 并校验弱口令 增加 QD 指令，将 PIN 由 ZPK1 加密转换为 ZPK2 加密并校验 增加 GP 指令，计算一个字符 PIN 的 MD5 值 修订文档部分错误，RY/EC/N6
V1.47	2016-9-08	H1.24.22	增加 SW 指令，多个数据加解密 扩展 KJ 指令，增加密钥分散模式 6 每 8 字节进行分散 扩展 CB 指令，增加 05,06,07 私有算法 增加 CP 指令，校验弱口令及附加弱口令 增加 SP 指令，设置弱口令集 增加 BB 指令，ZPK 加密数字 PIN 增加 3D 指令，计算/校验 MAC 增加 S8 指令，数据转加密-非对称转对称 增加 50 指令，EDK 加/解密数据-ECB 模式 增加 52 指令，EDK 加/解密数据-CBC 模式 增加 CJ 指令，数字 PINBLOCK 私有算法转加密 增加 SF 指令，查询/增加屏蔽指令
V1.46	2016-6-24	H1.24.13	增加 PINBLOCK（字符）格式 3 补充错误码 扩展 N6 指令 EDK 的 PIN BLOCK 格式 11 扩展 N8 指令 EDK 类型的支持 扩展 D7 指令 EDK 的 PIN BLOCK 格式 21
V1.45	2016-2-18	H1.23.21	增加 GN 指令，对一个 PIN 的数据块进行哈希运算 增加 F6 指令，产生新种子并生成 OTP 动态口令
V1.44	2016-1-22	H1.23.20	增加 F7 指令，生成 OTP 增加 F8 指令，验证 OTP 扩展 CB 指令，增加私有算法选项 04
V1.43	2015-12-07	H1.23.19	修改 BA 指令，支持填充多个 F
V1.42	2015-9-16	H1.23.09	扩展 TR 指令,增加扩展标识 2,输出私钥密文(明文 DER 编码形式存在) 增加 RY 指令，生成或者校验美国运通的 CSC 增加 EC 指令，PVV 校验 ZPK 加密的 PINBLOCK 修改 KD,增加支持 TMK/EDK 类型 修改 DO,增加支持 EDK 类型
V1.41	2015-7-30	H1.23.00	原有 KD 指令,当源密钥是 DES 时,不论子密钥是不是 DES 密钥,都会对子密钥强制做奇校验; 增加 KJ 指令，当源密钥是 DES，子密钥是非 DES 密钥时，不会对子密钥做强制奇校验;
V1.40	2015-7-21	H1.22.12	扩展 KD 指令，新增子密钥分散模式 5; 增加 P6 指令，增加 ZPK 加密明文字符 PIN;
V1.39	2015-4-15	H1.21.21	扩展 N7 指令，增加公钥加密 PINBLOCK 格式;
V1.38	2015-3-19	H1.21.13	扩展 EJ 指令,支持导入外部送入的 PFX 格式被口令保护的证书; 扩展 KD 指令，新增子密钥分散模式 4
V1.37	2015-2-13	H1.21.06	增加 N5 指令，将字符 PIN 由 TPK 加密转换为公钥加密; 增加 N7 指令，将数字 PIN 由 TPK 加密转换为公钥加密; 修订 P7 指令，去除对字符 PINBLOCK 模式 01 的支持;
V1.36	2014-12-31	H1.20.09	增加 KE 指令，分散密钥输出子密钥的多个成份密文; 增加 NF 指令，根据成份密文打印密钥成份;

V1.35	2014-12-5	H1.20.07	增加 P0 指令，产生随机的字符 PIN 并由 ZPK 加密输出； 增加 P7 指令，字符 PIN 密文转加密； 增加 KA 指令，导入存储一条对称密钥； 修订 N6 指令，增加字符 PIN 格式 02 的支持； 增加 3.3.7 PIN 安全管理，和 6 PINBLOCK（字符）格式；
V1.34	2014-11-28	H1.20.02	增加 NP 指令，获取密码机运行状态；
V1.33	2014-10-31	H1.19.06	修正 A3 指令的指令协议说明，无打印后应答报文； PINBLOCK 格式 01，为符合银联规范的 PIN 块； 增加 GD 指令，TK 加密的 PIN 密文转为 KMC(Sdek)下加密； 增加 S7 指令，PIN 密文转换（通用指令）； 增加 BU 指令，RACAL 兼容的产生密钥校验值；
V1.32	2014-10-17	H1.19.03	增加 A3 指令，密钥成份打印功能； 修订 CC 指令，源 PIN 块增加 20 私有格式的支持；
V1.31	2014-9-24	H1.19.01	增加 KX 指令，PBOC 规范脱机 PIN 修改/加密功能；
V1.30	2014-9-5	H1.18.09	增加 RACAL 兼容指令：OA,RC,GI,GK,GM,MI； 修订 CB 指令，增加私有 PIN 加密算法模式 3； 修订 KD 指令，增加分散算法模式 3 的支持；
V1.29	2014-7-2	H1.17.03	增加 AES256 算法，密钥标识 N； 增加 AES192 算法，密钥标识 M； 修订 KD 指令，增加分散算法模式 2 的支持； 修订 KR/S3/S4/S5 指令，增加 AES256 的支持； 增加 D7 指令，PIN 密文转换，支持 ZPK 密钥分散运算；
V1.28	2014-5-29	H1.16.03	增加 LR 指令，HMAC 的计算； 增加 KF 指令，删除内部指定索引密钥； 修订 EW/EY/3A/3B 指令，增加 OAEP 填充方式的支持； 修订 S0 指令，输出域增加 MAC 值的密文； 修订 SI 指令，导入密钥类型不受限； 修订 CB 指令，增加私有算法标识 2 的支持； 修订 E3/E4 指令，增加大包数据的加解密支持； 修订 KI/SI 指令，密钥头输入全 0 时不进行正确性验证；
V1.27	2014-4-8	H1.15.01	增加 EE/PG 两条 RACAL 兼容指令； 增加 CB 指令，将 PIN 由 ZPK 下加密转换到私有算法下加密；
V1.26	2014-2-26	H1.14.00	增加 KY/KW 指令，支持 EMV 规范的交易认证功能； 扩展 SH/SI/TR 指令，报文增加扩展域（填充模式、公钥输出格式），向下兼容； PINBLOCK 格式增加 41、42 两种 PIN 修改格式的说明；
V1.25	2014-2-18	H1.13.01	A0/A6 指令，扩展支持内部索引模式的形式存储；
V1.24	2014-1-22	H1.13.00	增加 OTP 动态口令功能指令，F3/F4/F5；
V1.23	2013-10-29	H1.12.00	增加 EH/E8 指令，支持产生明文非对称密钥对； 增加 H1/H2/H3 指令，支持大数据包的摘要运算； 增加 CFB/OFB 两种对称运算模式； 增加 10、11 两种数据填充模式；
V1.22	2013-9-10	H1.11.12	增加 ED/EF 指令，支持对数据的摘要结果做 SM2 签名验证运算；
V1.21	2013-9-4	H1.11.11	N6 指令，增加 MAC 域的输出；

V1.20	2013-8-6	V1.11.10	修改部分文字描述；
V1.19	2013-7-26	V1.11.10	PINBLOCK 格式扩充 11 模式的 128 位分组算法；
V1.18	2013-7-18	V1.11.09	增加 N6/N8 指令； 按新版规范，SM2 密文串变更为 C1 || C3 || C2 序列； PINBLOCK 格式支持 128 位分组算法；
V1.17	2013-7-15	V1.11.08	第一个正式版本；

目 录

表 目 录

1. 编程指南

1.1. 简要介绍

江南天安金融数据密码机是以现代密码技术为核心的主机安全模块（HSM），是一个具有物理安全保护措施的硬件设备，具有自主密钥管理机制，将密码运算过程封装在其内部完成，为业务系统提供安全的应用层密码服务，包括密钥管理、消息验证、数据加密、签名的产生和验证等，保证业务数据产生、传输、接收到处理整个过程的安全性、有效性、完整性、不可抵赖性。

江南天安金融数据密码机作为主机的外围设备，为主机在一个物理上安全的环境中实现加/解密运算功能。它通过 TCP/IP 连接方式接收主机传送过来的命令（Command），完成相应的加解密运算，再将运算的结果生成响应消息（Response）返回主机。

一般地，HSM 主要在实时、联机的环境中，完成系统需要的密钥管理、pin 和 MAC 相关运算功能。

应用程序发送命令给 HSM，然后从 HSM 中接收响应信息。每一条命令和响应消息都包含可变数量的域。

为了使数据可以通过串行数据形式的连接被发送，数据需要编码成 ASCII 码或 EBCDIC 码。

1.2. 报文协议

密码机的主机服务支持 TCP/IP 通讯模式。应用系统向密码机请求密码服务时，需按指令格式组合成正确的命令报文，发送给与密码机建立的 socket 上，并等待接收密码机的应答报文。

与密码机通讯的每个报文的长度不能超过 65520 字节。

1.2.1. TCP 命令报文格式

报文长度	消息头	命令代码	数据元素

- 报文长度

2 个字节，取值在 X’0002 to X’FFEE 之间的 16 进制数，用于标识后续报文（包括’消息头|命令代码|数据元素’ 域）的长度，字节数。

例如，对于命令报文’NC’，该域取值为 0x00, 0x02。

- 消息头

  n 个 ASCII 字符，应用系统标识数据。不参与运算，应答时原样返回。

  长度必须与密码机的配置一致。

- 命令代码

  2 个 ASCII 字符，命令报文的指令代码，标识运算类型。

- 数据元素

  变长数据，对应命令代码的相关命令数据内容，需参考各个命令说明。

1.2.2. 应答报文格式

报文长度	消息头	响应代码	返回码	数据元素

- 报文长度

  2 个字节，取值在 X’0002 to X’FFEE 之间的 16 进制数，用于标识 [消息头+响应代码+状态代码+数据元素] 的长度，字节数。

- 消息头

  n 个 ASCII 字符，应用系统标识数据。原样返回命令报文中的消息头内容。

- 响应代码

  2 个 ASCII 字符，对应命令报文的响应代码，命令代码+1。

- 返回码

  2 个 ASCII 字符，标识本次操作的错误码。“00”标识运算正常。

- 数据元素

  变长数据，对应命令代码的相关应答数据内容，需参考各个命令说明。

1.2.3. 指令报文缩写约定

表 1-1 报文缩写表

m	报文头长度
n	可变长度域
A	字母数字字符，包括任何ASCII字符
H	十六进制字符，’0’ – ‘9’和’A’ – ‘F’
N	十进制数字字符，’0’ – ‘9’
B	二进制字符（字节）， X’00 to X’FF
K	密钥索引标识。该域存在，后续则为4N的数字字符，标识密钥在密码机中的存储位置。如：K0003；0003是密钥在密码机中的存储位置

1.3. 数据表示

密码机支持通讯报文采用 ASCII 和 EBCDIC 编码方式，应用系统采用的编码方式必须与密码机的配置一致。

1.3.1. EBCDIC 字符编码

下表列出 EBCDIC 字符编码及其相关的十六进制值

表 1-2 EBCDIC 字符编码表

EBCDIC	HEX	EBCDIC	HEX	EBCDIC	HEX	EBCDIC	HEX
NUL	00	SP	40		80		C0
SOH	01		41	a	81	A	C1
STX	02		42	b	82	B	C2
ETX	03		43	c	83	C	C3
	04		44	d	84	D	C4
HT	05		45	e	85	E	C5
	06		46	f	86	F	C6
DEL	07		47	g	87	G	C7
	08		48	h	88	H	C8
	09		49	i	89	I	C9
	0A		4A		8A		CA
VT	0B	.	4B	{	8B		CB
FF	0C	<	4C		8C		CC
CR	0D	(	4D		8D		CD
SO	0E	+	4E		8E		CE
SI	0F	|	4F		8F		CF
DLE	10	&	50		90		D0
DC1	11		51	j	91	J	D1
DC2	12		52	k	92	K	D2
DC3	13		53	l	93	L	D3

	14		54	m	94	M	D4
	15		55	n	95	N	D5
BS	16		56	o	96	O	D6
	17		57	p	97	P	D7
CAN	18		58	q	98	Q	D8
EM	19		59	r	99	R	D9
	1A	!	5A		9A		DA
	1B	$	5B	}	9B		DB
	1C	*	5C		9C		DC
	1D	)	5D		9D		DD
	1E	;	5E		9E		DE
	1F		5F		9F		DF
	20	-(minus)	60		A0	\	E0
	21	/	61	~	A1		E1
FS	22		62	s	A2	S	E2
	23		63	t	A3	T	E3
	24		64	u	A4	U	E4
LF	25		65	v	A5	V	E5
ETB	26		66	w	A6	W	E6
ESC	27		67	x	A7	X	E7
	28		68	y	A8	Y	E8
	29		69	z	A9	Z	E9
	2A		6A		AA		EA
	2B	,(comma)	6B		AB		EB
	2C	%	6C		AC		EC
ENQ	2D	_	6D	[	AD		ED
ACK	2E	>	6E		AE		EE
BEL	2F	?	6F		AF		EF
	30		70		B0	0	F0
	31		71		B1	1	F1
SYN	32		72		B2	2	F2
	33		73		B3	3	F3
	34		74		B4	4	F4
	35		75		B5	5	F5
	36		76		B6	6	F6
EOT	37		77		B7	7	F7
	38		78		B8	8	F8
	39	`(grave)	79		B9	9	F9
	3A	:	7A		BA		FA
	3B	#	7B		BB		FB
DC4	3C	@	7C		BC		FC
NAK	3D	‘	7D	]	BD		FD
	3E	=	7E		BE		FE
SUB	3F	“	7F		BF		FF

1.3.2. EBCDIC 编码至 ASCII 编码转换表

表 1-3 EBCDIC/ASCII 编码转换表

EBCDIC HEX	Char	ASCII HEX	EBCDIC HEX	Char	ASCII HEX	EBCDIC HEX	Char	ASCII HEX	EBCDIC HEX	Char	ASCII HEX
00	NUL	00	40	SP	20	80			C0		

01	SOH	01	41			81	a	61	C1	A	41
02	STX	02	42			82	b	62	C2	B	42
03	ETX	03	43			83	c	63	C3	C	43
04			44			84	d	64	C4	D	44
05	HT	09	45			85	e	65	C5	E	45
06			46			86	f	66	C6	F	46
07	DEL	7F	47			87	g	67	C7	G	47
08			48			88	h	68	C8	H	48
09			49			89	i	69	C9	I	49
0A			4A			8A			CA		
0B	VT	0B	4B	.	2E	8B	{	7B	CB		
0C	FF	0C	4C	<	3C	8C			CC		
0D	CR	0D	4D	(	28	8D			CD		
0E	SO	0E	4E	+	2B	8E			CE		
0F	SI	0F	4F	|	7C	8F			CF		
10	DLE	10	50	&	26	90			D0		
11	DC1	11	51			91	j	6A	D1	J	4A
12	DC2	12	52			92	k	6B	D2	K	4B
13	DC3	13	53			93	l	6C	D3	L	4C
14			54			94	m	6D	D4	M	4D
15			55			95	n	6E	D5	N	4E
16	BS	08	56			96	o	6F	D6	O	4F
17			57			97	p	70	D7	P	50
18	CAN	18	58			98	q	71	D8	Q	51
19	EM	19	59			99	r	72	D9	R	52
1A			5A	!	21	9A			DA		
1B			5B	$	24	9B	}	7D	DB		
1C			5C	*	2A	9C			DC		
1D		1D	5D	)	29	9D			DD		
1E		1E	5E	;	3B	9E			DE		
1F		1F	5F		5F	9F			DF		
20			60	-	2D	A0			E0	\	5C
21			61	/	2F	A1	~	7E	E1		
22	FS	1C	62			A2	s	73	E2	S	53
23			63			A3	t	74	E3	T	54
24			64			A4	u	75	E4	U	55
25	LF	0A	65			A5	v	76	E5	V	56
26	ETB	17	66			A6	w	77	E6	W	57
27	ESC	1B	67			A7	x	78	E7	X	58
28			68			A8	y	79	E8	Y	59
29			69			A9	z	7A	E9	Z	5A
2A			6A			AA			EA		
2B			6B	,	2C	AB			EB		
2C			6C	%	25	AC			EC		
2D	ENQ	05	6D	_	5F	AD	[	5B	ED		
2E	ACK	06	6E	>	3E	AE			EE		
2F	BEL	07	6F	?	3F	AF			EF		
30			70			B0			F0	0	30
31			71			B1			F1	1	31
32	SYN	16	72			B2			F2	2	32
33			73			B3			F3	3	33
34			74			B4			F4	4	34
35			75			B5			F5	5	35
36			76			B6			F6	6	36

37	EOT	04	77			B7			F7	7	37
38			78			B8			F8	8	38
39			79	`	60	B9			F9	9	39
3A			7A	:	3A	BA			FA		
3B			7B	#	23	BB			FB		
3C	DC4	14	7C	@	40	BC			FC		
3D	NAK	15	7D	‘	27	BD	]	5D	FD		
3E			7E	=	3D	BE			FE		
3F	SUB	1A	7F	“	22	BF			FF		

1.4. 本地主密钥

HSM 本地主密钥（LMKS）从 key00 计数到 key49，共 50 组，每组 192 比特，由设备主密钥 DMK 派生产生。各组都有自己的功能，用于加密不同类型的密钥或机密数据。

1.4.1. LMK 密钥组功能

表 1-4 LMK 密钥组功能表

LMK 组	代码	功能
00-02		包含两个需要用来将 HSM 设置为授权状态的智能卡“密钥”（如果 HSM 设置为密码模式则为密码）。
03-05		加密保存在主机存储域内的 PIN。
06-08	00	加密区域主密钥（ZMK）和密钥加密密钥（KEK）。
09-11	01	为互换交易而加密区域 PIN 密钥（ZPK）。
12-14		用于生成随机数。
15-17		用于加密存储在 HSM 缓冲器中的密钥。
18-20		用户创建秘密值的初始设置；用于生成所有的其它主密钥对。
21-23	02	加密终端主密钥（TMK），终端 PIN 密钥（TPK）和 PIN 校验密钥（PVK）。加密变量下的卡确认密钥（CVK）。
24-26	03	加密终端认证密钥（TAK）。
27-29	04	加密请求信封的参考数。
30-32	05	加密‘不用的’变量下的 PIN 校验密钥（PVK）和卡确认密钥（CVK）。
33-35	06	加密口令密钥。
36-38	07	加密区域传送密钥（ZTK）。
39-41	08	加密区域认证密钥（ZAK）。
42-44	09	加密 BDK，数据主密钥（MDK），MK-AC/MK-SMI/MK-SMC/MK-DAK/

		MK-DN。
45-47	0A	加密区域加密密钥（ZEK）和数据加密密钥（DEK）。
48-50	0B	加密终端加密密钥（TEK）。
51-53	0C	加密 RSA 密钥、HMAC 密钥。
54-56	0D	
57-59	0E	
60-62	0F	
63-65	10	加密 SM2 私钥。
66-68	11	加密卡片主控密钥 KMC。
69-149		为将来保留。
	为了匹配特殊的要求，有一些密钥存在变种	

1.4.2. LMK 测试密钥集

江南天安金融数据密码机在出厂时，内部装载有测试主密钥，其 LMK 密钥集的明文采用下表中内容。

表 1-5 LMK 测试密钥集

LMK 组	代码	标准的测试用 LMK 集		
00-02		0101010101010101	7902CD1FD36EF8BA	0101010101010101
03-05		2020202020202020	3131313131313131	2020202020202020
06-08	00	4040404040404040	5151515151515151	4040404040404040
09-11	01	6161616161616161	7070707070707070	6161616161616161
12-14		8080808080808080	9191919191919191	8080808080808080
15-17		A1A1A1A1A1A1A1A1	B0B0B0B0B0B0B0B0	A1A1A1A1A1A1A1A1
18-20		C1C1010101010101	D0D0010101010101	C1C1010101010101
21-23	02	E0E0010101010101	F1F1010101010101	E0E0010101010101
24-26	03	1C587F1C13924FEF	0101010101010101	1C587F1C13924FEF
27-29	04	0101010101010101	0101010101010101	0101010101010101
30-32	05	0202020202020202	0404040404040404	0202020202020202
33-35	06	0707070707070707	1010101010101010	0707070707070707
36-38	07	1313131313131313	1515151515151515	1313131313131313
39-41	08	1616161616161616	1919191919191919	1616161616161616
42-44	09	1A1A1A1A1A1A1A1A	1C1C1C1C1C1C1C1C	1A1A1A1A1A1A1A1A
45-47	0A	2323232323232323	2525252525252525	2323232323232323
48-50	0B	2626262626262626	2929292929292929	2626262626262626

51-53	0C	2A2A2A2A2A2A2A2A	2C2C2C2C2C2C2C2C	2A2A2A2A2A2A2A2A
54-56	0D	2F2F2F2F2F2F2F2F	3131313131313131	2F2F2F2F2F2F2F2F
57-59	0E	0101010101010101	0101010101010101	0101010101010101
60-62	0F	2020202020202020	3131313131313131	2020202020202020
63-65	10	4040404040404040	5151515151515151	4040404040404040
66-68	11	6161616161616161	7070707070707070	6161616161616161
69-71	12	8080808080808080	9191919191919191	8080808080808080
72-149	…	…		

1.4.3. LMK 变种说明

HSM 中的本地主密钥（LMK）变种是用来加密已定义的密钥或密钥成份。根据密钥类型（见表 2-1 密钥类型表），采用相应的 LMK 变种对密钥或数据进行加密。

这些变种是按照以下步骤进行运算的，以 MDK（密钥类型：109）为例：

1) 根据密钥类型选择合适的 LMK 组：

1A1A1A1A1A1A1A1A 1C1C1C1C1C1C1C1C 1A1A1A1A1A1A1A1A

2) 确定所需要的 LMK 变种，选择合适的偏移值：

变种 1：A6

3) 用所选择的偏移值对 LMK 组第一个密钥的第一个字节和第三个密钥的第一个字节（在上例中为 01）进行异或运算。

4) 用第 3 步所得的结果替换 LMK 组第一个密钥的第一个字节和第三个密钥的第一个字节，将所产生的密钥作为指定的密钥变种：

BC1A1A1A1A1A1A1A1A 1C1C1C1C1C1C1C1C **BC**1A1A1A1A1A1A1A1A

使用该变种后的密钥对 MDK 密钥明文加密保护；

密码机支持的变种如下：

变种 1：A6

变种 2：5A

变种 3：6A

变种 4：DE

变种 5：2B

变种 6：50

变种 7：74

变种 8：9C

1.4.4. LMK 加密对称密钥的方案

1.4.4.1. ANSI X9.17 方式

在 ANSI X9.17 方式中，使用 LMK 密钥直接 ECB 模式加密各应用密钥，并以 1A 形式标明密钥的算法类型：

- Z – 8 字节 DES 密钥
- X – 16 字节的 3DES 密钥
- Y – 24 字节的 3DES 密钥
- P – 16 字节 SM1 密钥
- R – 16 字节 SM4 密钥
- L – 16 字节 AES 密钥
- M – 24 字节 AES 密钥
- N – 32 字节 AES 密钥

1.4.4.2. TDEA 变量方式

为兼容使用 RACAL 体系的应用系统，密码机保留对 3DES 密钥的变量加密方式，以 1A 形式标明密钥的算法类型：

- U－双倍长度的 3DES 密钥，变种方式加密
- T－三倍长度的 3DES 密钥，变种方式加密

1) 双倍长的 3DES 应用密钥

包含第一个 8 字节密钥和第二个 8 字节密钥。LMK 分组在加密这两个密钥前，

先将 LMK 自身第二个密钥 K_2 的第一个字节与下述变量异或后再加密：

- 第一个密钥：A6
- 第二个密钥：5A

过程：

a) 将 LMK 分组 K_2 的第一个字节与 A6 异或，加密应用密钥的第一个 8 字节密钥，得到 8 字节密文 C1；

b) 将 LMK 分组 K_2 的第一个字节与 5A 异或，加密应用密钥的第二个 8 字节密钥，得到 8 字节密文 C2；

c) 组合 C1 || C2，得到该应用密钥的 U 模式密文；

2) 三倍长的 3DES 应用密钥

包含第一个 8 字节密钥、第二个 8 字节密钥和第三个 8 字节密钥。LMK 分组在加密这三个密钥前，先将 LMK 自身第二个密钥 K_2 的第一个字节与下述变量异或后再加密：

- 第一个密钥：6A
- 第二个密钥：DE
- 第二个密钥：2B

过程：

a) 将 LMK 分组 K_2 的第一个字节与 6A 异或，加密应用密钥的第一个 8 字节密钥，得到 8 字节密文 C1；

b) 将 LMK 分组 K_2 的第一个字节与 DE 异或，加密应用密钥的第二个 8 字节密钥，得到 8 字节密文 C2；

c) 将 LMK 分组 K_2 的第一个字节与 2B 异或，加密应用密钥的第三个 8 字节密钥，得到 8 字节密文 C3；

d) 组合 C1 || C2 || C3，得到该应用密钥的 T 模式密文；

2. 密钥管理体系

2.1. 密码机密钥简介

2.1.1. 设备主密钥 DMK

密码机自身有一条设备主密钥 DMK，128 比特 SM1 密钥，由多个成份卡合成。一个分量形式存储于加密卡内，一个分量存储于开机卡中。开机时需插入正确的开机卡以恢复 DMK 密钥。

DMK 仅用于分散产生 LMKs，不能参与任何业务数据的运算。

DMK 可在管理终端上通过原始初始化或恢复初始化完成重置 DMK 的操作。

2.1.2. 本地主密钥 LMKs

LMKs，由 DMK 派生产生，共 50 组，每组 192 比特，用于加密保护不同类型的应用密钥或机密数据。

各组 LMK 的用途参见 1.4.1 章节内容。

设备出厂时内装测试 DMK，对应一系列测试 LMK，其密钥明文值参见 1.4.2 章节内容。

2.1.3. 应用密钥

应用系统中使用的各类应用密钥，包括上表提到的 ZMK/ZAK/ZPK/KEK/DEK/MDK/RSA/SM2 等等，支持内部存储和外部存储模式。使用时在命令报文中提供索引号或密钥密文。

内部存储，密码机内支持存储 2048 条对称密钥、64 对 RSA 密钥及 64 对 SM2 密钥，索引号从 1 起始。

外部存储，对称密钥及非对称的私钥部分由相应 LMK 分组加密保护，保证密钥外部存储的安全性。

2.2. 应用密钥详述

应用密钥不论是内部存储还是外部存储，均有密钥角色的概念，可称为密钥类型。不同的密钥角色可完成的工作是不同的，例如，ZPK 可以进行 PIN 加密转换不可以解密 PIN；密钥加密密钥可以加密其他密钥不可以进行解密操作；等等。

2.2.1. 密钥类型表

密钥类型在命令报文中以 3H 形式标识：第一个字符标识 LMK 变种号，取值 0-9；后两个字符标识 LMK 代码，表明在哪组 LMK 下加密保护。

表 2-1 密钥类型表

变 种 →		0	1	2	3	4	5	6	7	8	9	对应的 LMK 对
LMK 组	代码											
06-08	00	ZMK KEK										04-05
09-11	01	ZPK										06-07
21-23	02	PVK TPK TMK				CVK						14-15
24-26	03	TAK										16-17
27-29	04											18-19
30-32	05											20-21
33-35	06											22-23
36-38	07	EDK										24-25
39-41	08	ZAK										26-27
42-44	09		MK-AC MDK	MK-SMI	MK-SMC	MK-DAK	MK-DN					28-29
45-47	0A	ZEK DEK										30-31
48-50	0B	TEK										32-33
51-53	0C	RSA-SK										34-35
54-56	0D											36-37
57-59	0E											38-39
60-62	0F											40-41
63-65	10	SM2										42-43
66-68	11	KMC										44-45

依上表，密钥类型标识的示例：

ZMK/KEK – 000

ZPK – 001

MDK – 109

表 2-2 密钥类型说明表

	简写	代码	全称	名称	用途说明
1.	ZMK	000	Zone Master Key	区域主密钥	用于加密保护 ZAK、ZPK 等数据密钥的安全传输； 通常应用于分行与总行之间的区域安全网络中；
2.	ZPK	001	Zone Pin Key	区域 PIN 加密密钥	用于加密保护用户 PIN 的安全传输； 通常应用于分行与总行之间的区域安全网络中；
3.	ZAK	008	Zone Authentication Key	区域认证密钥	用于计算用户数据的 MAC，保证数据的完整性； 通常应用于分行与总行之间的区域安全网络中；
4.	ZEK	00A	Zone Encryption Key	区域加密密钥	用于加解密保护用户数据，保证数据的机密性； 通常应用于分行与总行之间的区域安全网络中；
5.	TMK	002	Terminal Master Key	终端主密钥	用于加密保护 TAK、TPK 等数据密钥的安全传输； 通常应用于终端与前置之间的终端安全网络；
6.	TPK	002	Terminal Pin Key	终端 PIN 加密密钥	用于加密保护用户 PIN 的安全传输； 通常应用于终端与前置之间的终端安全网络中；
7.	TAK	003	Terminal Authentication Key	终端认证密钥	用于计算用户数据的 MAC，保证数据的完整性； 通常应用于终端与前置之间的终端安全网络中；
8.	TEK	00B	Terminal Encryption Key	终端加密密钥	用于加解密保护用户数据，保证数据的机密性； 通常应用于终端与前置之间的终端安全网络中；
9.	PVK	002	Pin Verfication Key	PIN 验证密钥	用于计算用户 PIN 的 PVV 或 PINOFFSET，保证 PIN 的安全存储； 通常应用于帐务主机系统中；
10.	CVK	402	Card Verfication Key	卡验证密钥	用于计算用户卡的 CVV 或 CVV2，验证卡片的有效性；通常应用于帐务主机系统中；
11.	MK-AC	109	Master Key for Authentication Cryptograms	用于计算认证密文的主密钥	
12.	MK-SMI	209	Master Key for Secure Messaging Integrity	用于安全报文完整性的主密钥	
13.	MK-SMC	309	Master Key for Secure Messaging Confidentiality	用于安全报文机密性的主密钥	

14.	MK-DAK	409	Master Key for Data Authentication Codes	用于计算数据认证码的主密钥	
15.	MK-DN	509	Master Key for Dynamic Numbers	用于产生动态数字的主密钥	
16.	MDK	109	Master DEA Key	主密钥	各类应用主密钥，可/必须分散后产生会话密钥，对数据进行加密、MAC 产生/校验；
17.	KEK	000	Key Encryption Key	密钥加密密钥	在密钥管理中，用于保护其他应用主密钥以安全报文的形式导入导出密码机；在个人化过程中，用于对机密数据进行保护，提供加密、转密功能，不提供解密功能；
18.	KMC	011		IC 卡片的主控密钥	
19.	DEK	00A	Data Encryption Key	数据加密密钥	用于 DP 与发卡系统间加密解密制卡文件的保护密钥

2.2.2. 密钥的使用

2.2.2.1. 对称密钥的使用

1. 产生或导入密钥

对称密钥在产生或导入时，若要存储到密码机内某索引中，则指令中的“密钥存储标识”域必须存在一个标识'K'，紧跟的密钥索引域是 4N 形式[0001-2048]，密钥标签长度域必须存在 2N 模式[00-16]，指示后面密钥标签域的长度（字符数）；

若不存储到密码机内，则指令中的“密钥存储标识”域为空不填，后续紧跟的 3 个域（密钥索引、密钥标签长度、密钥标签）也均不存在；

2. 使用对称密钥

密钥在运算的指令报文中使用时，首先需指定密钥类型标识（参见 2.2.1 章节内容），然后输入密钥内容，形式支持：'K' + 4N / 16 H / 1A + 32H / 1A + 48H / 1A + 64H。

- 'K' + 4N ，指明使用内部存储的密钥，4N 标识密钥索引号，范围：0001-2048。
- 16H，指明使用外部送入的密钥密文，单长度的 DES 密钥，8 字节；
- 1A+32H，指明使用外部送入的密钥密文，1A 标识密钥的算法，双长度的

3DES 密钥或 SM1、SM4、AES-128 算法密钥；

- 1A+48H，指明使用外部送入的密钥密文，三长度的 3DES 密钥或 AES-192 算法密钥；
- 1A+64H，指明使用外部送入的密钥密文，AES-256 算法密钥；

2.2.2.2. 非对称密钥的使用

1. 产生非对称密钥（RSA/SM2）

非对称密钥在产生时，若要存储到密码机内某索引中，则指令中的“密钥存储标识”域必须存在一个标识’K’，紧跟的密钥索引域是 4N 形式[0001-0064]，密钥标签长度域必须存在 2N 模式[00-16]，指示后面密钥标签域的长度（字符数）；

若不存储到密码机内，则指令中的“密钥存储标识”域为空不填，后续紧跟的 3 个域（密钥索引、密钥标签长度、密钥标签）也均不存在；

2. 装载导入非对称密钥（RSA/SM2）

非对称密钥的导入，支持 LMK 加密的密钥密文形式导入到某索引中；

在对应的指令 EJ（装载 RSA 密钥对）、E1（装载 SM2 密钥对）中，必须指明要导入的目标索引值：4N 形式[0001-0064]，密钥标签长度域必须存在 2N 模式[00-16]，指示后面密钥标签域的长度（字符数）；

另外请注意，本服务仍支持兼容的 RACAL 命令 EK（装载 RSA 密钥对），其报文中的 RSA 密钥为 2N 模式。

3. 获取公钥

密码机支持获取内部某索引 RSA 或 SM2 密钥的公钥的功能，在对应的指令 ER 和 E2 中，需指定要获取公钥的密钥索引，请采用密钥索引标识’K’+密钥索引 4N 的形式。

另外，ER 指令为兼容 RSA 的旧版指令应用模式，当不存在密钥索引标识’K’时，后面的密钥索引为 2N 形式。

4. 使用非对称密钥

密钥在运算的指令报文中使用时，包括加密解密签名验签等功能，需在报文中指定要使用的非对称密钥，请采用密钥索引标识’K’+密钥索引 4N 的形式。

另外，为兼容 RSA 的旧版指令应用模式，RSA 运算的相关指令报文中，若不存在密钥索引标识'K'，则后面的密钥索引域为 2N 形式。

- 若使用外部存储的公钥或密文私钥，则密钥索引需标记为'9999'（4N 模式）或'99'（2N 模式），后面按报文要求填入公钥或/和密文私钥。

2.2.3. 对称密钥算法标识

密码机支持多种对称密码算法，使用时根据其算法标识使用相应的密码算法。

密钥标识	注释
Z	单倍长的 DES 算法密钥；
U	双倍长的 3DES 算法密钥，LMK 加密输出时使用变量方式；
T	三倍长的 3DES 算法密钥，LMK 加密输出时使用变量方式；
X	双倍长的 3DES 算法密钥；
Y	三倍长的 3DES 算法密钥；
P	SM1 算法密钥；
R	SM4 算法密钥；
L	AES-128 算法密钥；
M	AES-192 算法密钥；
N	AES-256 算法密钥；

3. 主机命令

3.1. 主机命令列表(按字母排序)

表 3-1 主机命令表（字母排序）

序号	代码	功能简述	章节	备注
1	3A	RSA 公钥加密运算	3.5.1.6	扩展
2	3B	RSA 私钥解密运算	3.5.1.7	扩展
3	3C	计算数据摘要	3.3.6.1	扩展
4	3D	计算/校验 MAC	3.5.3.1	扩展
5	50	EDK 加密/解密数据－ECB 模式	3.3.4.7	RACAL 兼容
6	52	EDK 加密/解密数据－CBC 模式	3.3.4.8	RACAL 兼容
7	A0	产生工作密钥	3.4.1.1	RACAL 兼容
8	A2	生产并打印一个成份	3.4.8.4	RACAL 兼容
9	A3	生成并打印一个密钥成份及其校验值	3.4.8.5	扩展
10	A4	由密文成份合成一个密钥	3.4.1.2	RACAL 兼容
11	A6	导入密钥	3.4.1.3	RACAL 兼容
12	A8	导出密钥	3.4.1.4	RACAL 兼容
13	BA	LMK 加密一个明文 PIN	3.4.3.2	RACAL 兼容
14	BB	ZPK 加密数字 PIN	3.3.7.13	金融 IC 卡扩展
15	BU	生成密钥校验值	3.4.1.14	RACAL 兼容
16	CA	将 PIN 由 TPK 加密转换为 ZPK 加密	3.4.4.4	RACAL 兼容
17	CB	将 PIN 由 ZPK 下加密转换到私有算法加密	3.3.7.10	扩展
18	CC	将 PIN 由 ZPK1 加密转换为 ZPK2 加密	3.4.4.5	RACAL 兼容
19	CJ	数字 PINBLOCK 私有算法转加密	3.3.7.14	金融 IC 卡扩展
20	CP	弱口令校验	3.3.7.11	金融 IC 卡扩展
21	CR	产生随机数	3.3.8.1	扩展
22	CW	产生 VISA CVV	3.4.6.1	RACAL 兼容
23	CY	校验 VISA CVV	3.4.6.2	RACAL 兼容
24	D0	计算数据 MAC/TAC	3.3.5.1	金融 IC 卡扩展
25	D1	验证数据 MAC/TAC	3.3.5.2	金融 IC 卡扩展
26	D3	数据加密	3.3.4.1	金融 IC 卡扩展

27	D4	数据解密	3.3.4.2	金融 IC 卡扩展
28	D7	PIN 密文转换	3.3.7.4	金融 IC 卡扩展
29	DA	校验一个用 IBM 方式的终端 PIN	3.4.5.4	RACAL 兼容
30	DE	产生 IBM PIN Offset	3.4.5.1	RACAL 兼容
31	DG	产生 VISA PVV	3.4.5.6	RACAL 兼容
32	E0	数据加解密	3.4.7.1	旧版本兼容
33	E1	装载 SM2 密钥对	3.5.2.3	扩展
34	E2	获取 SM2 公钥	3.5.2.4	扩展
35	E3	SM2 公钥加密运算	3.5.2.5	扩展
36	E4	SM2 私钥解密运算	3.5.2.6	扩展
37	E5	SM2 私钥签名运算	3.5.2.7	扩展
38	E6	SM2 公钥验签运算	3.5.2.8	扩展
39	E7	产生 SM2 密钥对	3.5.2.1	扩展
40	E8	产生明文 SM2 密钥对	3.5.2.2	扩展
41	EA	校验一个用 IBM 方式的交换 PIN	3.4.5.5	RACAL 兼容
42	EC	PVV 校验 ZPK 加密的 PINBLOCK	3.4.5.7	RACAL 兼容
43	ED	SM2 私钥签名（对数据的摘要值）运算	3.5.2.9	扩展
44	EE	使用 IBM 方式得到一个 PIN	3.4.5.2	RACAL 兼容
45	EF	SM2 公钥验证（对数据的摘要值）运算	3.5.2.10	扩展
46	EH	产生明文 RSA 密钥对	3.5.1.2	扩展
47	EI	产生 RSA 密钥对	3.5.1.1	RACAL 兼容
48	EJ	装载 RSA 密钥对 – 扩展	3.5.1.4	扩展
49	EK	装载 RSA 密钥对 – 兼容旧版本保留	3.5.1.3	旧版本兼容
50	EO	为 RSA 公钥产生一个 MAC	3.5.1.16	RACAL 兼容
51	ER	获取 RSA 公钥	3.5.1.5	旧版本兼容
52	EW	RSA 私钥签名运算	3.5.1.8	RACAL 兼容
53	EY	RSA 公钥验签运算	3.5.1.9	RACAL 兼容
54	F3	产生令牌种子	3.6.1	扩展
55	F4	解密种子密文	3.6.2	扩展
56	F5	生成 OTP 动态口令	3.6.3	扩展
57	F6	产生新种子并生成 OTP 动态口令	3.6.4	
58	F7	生成 OTP	3.6.4	
59	F8	验证 OTP	3.6.6	
60	FA	ZPK 从 ZMK 加密转换为 LMK 加密	3.4.1.6	RACAL 兼容

61	FK	ZEK/ZAK 从 ZMK 加密转换为 LMK 加密	3.4.1.9	RACAL 兼容
62	FI	产生一个 ZEK/ZAK	3.4.1.8	RACAL 兼容
63	FM	ZEK/ZAK 从 LMK 加密转换为 ZMK 加密	3.4.1.10	RACAL 兼容
64	G0	KMC(Kdek)保护导出一对 SM2 密钥	3.3.2.10	金融 IC 卡扩展
65	G1	厂商 KMC 加密导出发行商 KMC 三条卡片密钥	3.3.2.1	金融 IC 卡扩展
66	G2	KMC(Kdek)加密导出多条应用密钥	3.3.2.2	金融 IC 卡扩展
67	G3	KMC(Kdek)加密敏感数据	3.3.2.3	金融 IC 卡扩展
68	G4	KMC(Kenc)加密数据	3.3.2.4	金融 IC 卡扩展
69	G5	KMC(Kmac)计算数据 C-MAC	3.3.2.5	金融 IC 卡扩展
70	G6	KMC(Kmac)验证数据 R-MAC	3.3.2.6	金融 IC 卡扩展
71	G7	外部认证	3.3.2.7	金融 IC 卡扩展
72	G8	保护密钥加密导出 KMC 三条会话密钥	3.3.2.8	金融 IC 卡扩展
73	GC	ZPK 从 LMK 加密转换为 ZMK 加密	3.4.1.7	RACAL 兼容
74	GD	TK 加密的 PIN 密文转为 KMC(Sdek)下加密	3.3.2.11	金融 IC 卡扩展
75	GF	KMC(Kdek)保护导出一对 RSA 密钥	3.3.2.9	金融 IC 卡扩展
76	GI	RSA 公钥加密导出一条 DES 密钥，RACAL 兼容	3.5.1.14	RACAL 兼容
77	GK	RSA 公钥加密导入一条 DES 密钥，RACAL 兼容	3.5.1.15	RACAL 兼容
78	GM	对一个数据块进行哈希运算	3.4.9.2	RACAL 兼容
79	GN	对一个 PIN 的数据块进行哈希运算	3.4.9.3	
80	GP	计算一个字符 PIN 的 MD5 值	3.4.9.4	
81	H1	大包数据摘要的初始化	3.3.6.2	金融 IC 卡扩展
82	H2	大包数据摘要的过程运算	3.3.6.3	金融 IC 卡扩展
83	H3	大包数据摘要的结束，输出摘要结果	3.3.6.4	金融 IC 卡扩展
84	HA	产生一个 TAK	3.4.1.12	RACAL 兼容
85	HC	产生一个 TMK/TPK/PVK	3.4.1.11	RACAL 兼容
86	IA	产生一个 ZPK	3.4.1.5	RACAL 兼容
87	JA	产生一个随机 PIN 码	3.4.3.1	RACAL 兼容
88	JC	将 PIN 由 TPK 加密转换为 LMK 加密	3.4.4.1	RACAL 兼容
89	JE	将 PIN 由 ZPK 加密转换为 LMK 加密	3.4.4.2	RACAL 兼容
90	JG	将 PIN 由 LMK 加密转换为 ZPK 加密	3.4.4.3	RACAL 兼容
91	K2	PBOC 脚本加密	3.3.3.2	旧版本兼容
92	K4	PBOC 脚本 MAC	3.3.3.3	旧版本兼容
93	K6	PBOC 验证 ARQC，可选的产生 ARPC	3.3.3.1	旧版本兼容
94	KA	导入存储一条对称密钥	3.3.1.10	金融 IC 卡扩展

95	KD	分散产生新密钥，可选的存储到密码机内	3.3.1.2	金融 IC 卡扩展
96	KE	分散密钥输出子密钥的多个成份密文	3.3.1.11	金融 IC 卡扩展
97	KF	删除内部指定索引的密钥	3.3.1.9	金融 IC 卡扩展
98	KG	获取对称密钥状态信息	3.3.1.8	金融 IC 卡扩展
99	KH	传输密钥保护导出一条对称密钥（密文+MAC）	3.3.1.4	金融 IC 卡扩展
100	KI	传输密钥保护导入一条对称密钥（密文+MAC）	3.3.1.5	金融 IC 卡扩展
101	KJ	分散产生新密钥，可选的存储到密码机内	3.3.1.3	金融 IC 卡扩展
102	KR	产生一条随机密钥，可选的存储到密码机内	3.3.1.1	金融 IC 卡扩展
103	KW	EMV4.X 验证 ARQC，可选的产生 ARPC	3.3.3.4	RACAL 兼容
104	KX	PBOC 脱机 PIN 修改/加密	3.3.3.6	金融 IC 卡扩展
105	KY	EMV4.X 脚本安全报文/PIN 修改	3.3.3.5	RACAL 兼容
106	LR	计算数据 HMAC – 明文密钥	3.3.5.4	金融 IC 卡扩展
107	MA	TAK 计算数据 MAC	3.4.2.1	RACAL 兼容
108	MC	TAK 验证数据 MAC	3.4.2.2	RACAL 兼容
109	MI	将 TAK 从 ZMK 下加密转为 LMK 下加密	3.4.1.13	RACAL 兼容
110	MQ	ZAK 计算数据 MAC/TAC	3.4.2.3	旧版本兼容
111	MS	ZAK/TAK 产生 X9.9/X9.19 的报文 MAC	3.4.2.6	RACAL 兼容
112	MU	ZAK/TAK 产生银联标准报文 MAC	3.4.2.5	旧版本兼容
113	N5	将字符 PIN 由 TPK 加密转为公钥加密	3.3.7.5	扩展
114	N6	公钥加密的字符 PIN 密文转为 ZPK 加密	3.3.7.6	扩展
115	N7	将数字 PIN 由 TPK 加密转为公钥加密	3.3.7.7	扩展
116	N8	公钥加密的数字 PIN 密文转为 ZPK 加密	3.3.7.8	扩展
117	NC	获取密码机版本信息	3.4.9.1	RACAL 兼容
118	NE	生产密钥并以分开的成份形式打印	3.4.8.3	RACAL 兼容
119	NF	根据成份密文打印成份信函	3.4.8.9	扩展
120	NG	LMK 解密 PIN	3.4.3.3	RACAL 兼容
121	NP	获取密码机运行状态	3.3.8.2	扩展
122	OA	打印一个 PIN 请求信函	3.4.8.7	RACAL 兼容
123	P0	产生指定长度的随机字符 PIN	3.3.7.1	金融 IC 卡扩展
124	P6	ZPK 加密明文字符 PIN	3.3.7.2	金融 IC 卡扩展
125	P7	字符 PINBLOCK 转加密	3.3.7.3	金融 IC 卡扩展
126	PA	装载打印格式数据	3.4.8.1	RACAL 兼容
127	PE	打印 PIN/PIN 请求数据	3.4.8.2	RACAL 兼容

128	PG	验证 PIN/PIN 和请求信封密码	3.4.8.6	RACAL 兼容
129	QC	产生 IBM PIN Offset 并校验弱口令	3.4.5.2	
130	QD	将 PIN 由 ZPK1 加密转 ZPK2 加密并校验	3.4.4.6	
131	RC	验证请求信封密码	3.4.8.8	RACAL 兼容
132	RY	生成或者校验美国运通的 CSC	3.4.5.8	RACAL 兼容
133	S0	计算数据 MAC/TAC – 通用	3.3.5.3	金融 IC 卡扩展
134	S3	数据加密 – 通用	3.3.4.3	金融 IC 卡扩展
135	S4	数据解密 – 通用	3.3.4.4	金融 IC 卡扩展
136	S5	数据转加密 – 通用	3.3.4.5	金融 IC 卡扩展
137	S7	PIN 密文转换 – 通用	3.3.7.5	金融 IC 卡扩展
138	S8	数据转加密－非对称转对称	3.5.3.2	扩展
139	SF	查询/增加屏蔽指令	3.3.8.3	扩展
140	SH	保护密钥加密导出一条对称密钥 – 通用	3.3.1.6	金融 IC 卡扩展
141	SI	保护密钥加密导入一条对称密钥 – 通用	3.3.1.7	金融 IC 卡扩展
142	SP	设置弱口令集	3.3.7.12	金融 IC 卡扩展
143	SW	多个数据加解密	3.3.4.6	金融 IC 卡扩展
144	TI	将 PIN 由 TPK1/ZPK1 加密转换为 TPK2/ZPK2 加密	3.4.4.6	扩展
145	TQ	为 SM2 公钥产生一个 MAC	3.5.2.15	扩展
146	TR	保护密钥（对称）加密导出一条 RSA 密钥	3.5.1.10	扩展
147	TS	保护密钥（对称）加密导入一对 RSA 密钥	3.5.1.11	扩展
148	TT	保护密钥（对称）加密导出一对 SM2 密钥	3.5.2.11	扩展
149	TU	保护密钥（对称）加密导入一对 SM2 密钥	3.5.2.12	扩展
150	TV	RSA 公钥加密导出一条对称密钥	3.5.1.12	扩展
151	TW	RSA 公钥加密导入一条对称密钥	3.5.1.13	扩展
152	TX	SM2 公钥加密导出一条对称密钥	3.5.2.13	扩展
153	TY	SM2 公钥加密导入一条对称密钥	3.5.2.14	扩展
154	UQ	ZPK 计算数据 MAC	3.4.2.4	旧版本兼容
说明				

3.2. 主机命令列表(按功能排序)

表 3-2 主机命令表（功能排序）

序号	代码	功能简述	章节	备注
金融 IC 卡 – 密钥管理功能				
1	KR	产生一条随机密钥，可选的存储到密码机内	3.3.1.1	金融 IC 卡扩展
2	KD	分散产生新密钥，可选的存储到密码机内	3.3.1.2	金融 IC 卡扩展
3	KJ	分散产生新密钥，可选的存储到密码机内	3.3.1.3	金融 IC 卡扩展
4	KH	传输密钥保护导出一条对称密钥（密文+MAC）	3.3.1.4	金融 IC 卡扩展
5	KI	传输密钥保护导入一条对称密钥（密文+MAC）	3.3.1.5	金融 IC 卡扩展
6	SH	保护密钥加密导出一条对称密钥 – 通用	3.3.1.6	金融 IC 卡扩展
7	SI	保护密钥加密导入一条对称密钥 – 通用	3.3.1.7	金融 IC 卡扩展
8	KG	获取对称密钥状态信息	3.3.1.8	金融 IC 卡扩展
9	KF	删除内部指定索引的密钥	3.3.1.9	金融 IC 卡扩展
10	KA	导入存储一条对称密钥	3.3.1.10	金融 IC 卡扩展
11	KE	分散密钥输出子密钥的多个成份密文	3.3.1.11	金融 IC 卡扩展
金融 IC 卡 – GP SCP02 发卡功能				
12	G1	厂商 KMC 加密导出发行商 KMC 三条卡片密钥	3.3.2.1	金融 IC 卡扩展
13	G2	KMC(Kdek)加密导出多条应用密钥	3.3.2.2	金融 IC 卡扩展
14	G3	KMC(Kdek)加密敏感数据	3.3.2.3	金融 IC 卡扩展
15	G4	KMC(Kenc)加密数据	3.3.2.4	金融 IC 卡扩展
16	G5	KMC(Kmac)计算数据 C-MAC	3.3.2.5	金融 IC 卡扩展
17	G6	KMC(Kmac)验证数据 R-MAC	3.3.2.6	金融 IC 卡扩展
18	G7	外部认证	3.3.2.7	金融 IC 卡扩展
19	G8	保护密钥加密导出 KMC 三条会话密钥	3.3.2.8	金融 IC 卡扩展
20	GF	KMC(Kdek)保护导出一对 RSA 密钥	3.3.2.9	金融 IC 卡扩展
21	G0	KMC(Kdek)保护导出一对 SM2 密钥	3.3.2.10	金融 IC 卡扩展
22	GD	TK 加密的 PIN 密文转为 KMC(Sdek)下加密	3.3.2.11	金融 IC 卡扩展
金融 IC 卡 – PBOC/EMV 规范交易功能				
23	K6	PBOC 验证 ARQC，可选的产生 ARPC	3.3.3.1	旧版本兼容
24	K2	PBOC 脚本加密	3.3.3.2	旧版本兼容
25	K4	PBOC 脚本 MAC	3.3.3.3	旧版本兼容
26	KW	EMV4.X 验证 ARQC，可选的产生 ARPC	3.3.3.4	RACAL 兼容
27	KY	EMV4.X 脚本安全报文/PIN 修改	3.3.3.5	RACAL 兼容

28	KX	PBOC 脱机 PIN 修改/加密	3.3.3.6	金融 IC 卡扩展
金融 IC 卡 – 数据加解密运算功能				
29	D3	数据加密	3.3.4.1	金融 IC 卡扩展
30	D4	数据解密	3.3.4.2	金融 IC 卡扩展
31	S3	数据加密 – 通用	3.3.4.3	金融 IC 卡扩展
32	S4	数据解密 – 通用	3.3.4.4	金融 IC 卡扩展
33	S5	数据转加密 – 通用	3.3.4.5	金融 IC 卡扩展
34	SW	多个数据加解密	3.3.4.6	金融 IC 卡扩展
35	50	EDK 加密/解密数据－ECB 模式	3.3.4.7	
36	52	EDK 加密/解密数据－CBC 模式	3.3.4.8	
金融 IC 卡 – 数据 MAC 运算功能				
37	D0	计算数据 MAC/TAC	3.3.5.1	金融 IC 卡扩展
38	D1	验证数据 MAC/TAC	3.3.5.2	金融 IC 卡扩展
39	S0	计算数据 MAC/TAC – 通用	3.3.5.3	金融 IC 卡扩展
40	LR	计算数据 HMAC – 明文密钥	3.3.5.4	金融 IC 卡扩展
金融 IC 卡 – PIN 安全管理功能				
41	P0	产生指定长度的随机字符 PIN	3.3.7.1	金融 IC 卡扩展
42	P6	ZPK 加密明文字符 PIN	3.3.7.2	金融 IC 卡扩展
43	P7	字符 PINBLOCK 转加密	3.3.7.3	金融 IC 卡扩展
44	D7	PIN 密文转换	3.3.7.4	金融 IC 卡扩展
45	S7	PIN 密文转换 – 通用	3.3.7.5	金融 IC 卡扩展
46	N5	将字符 PIN 由 TPK 加密转为公钥加密	3.3.7.6	扩展
47	N6	公钥加密的字符 PIN 密文转为 ZPK 加密	3.3.7.7	扩展
48	N7	将数字 PIN 由 TPK 加密转为公钥加密	3.3.7.8	扩展
49	N8	公钥加密的数字 PIN 密文转为 ZPK 加密	3.3.7.9	扩展
50	CB	将 PIN 由 ZPK 下加密转换到私有算法加密	3.3.7.10	扩展
51	CP	弱口令校验	3.3.7.11	金融 IC 卡扩展
52	SP	设置弱口令集	3.3.7.12	金融 IC 卡扩展
53	BB	ZPK 加密数字 PIN	3.3.7.13	金融 IC 卡扩展
54	CJ	数字 PINBLOCK 私有算法转加密	3.3.7.14	金融 IC 卡扩展
RACAL 兼容应用 – 密钥管理				
55	A0	产生工作密钥	3.4.1.1	RACAL 兼容

56	A4	由密文成份合成一个密钥	3.4.1.2	RACAL 兼容
57	A6	导入密钥	3.4.1.3	RACAL 兼容
58	A8	导出密钥	3.4.1.4	RACAL 兼容
59	IA	产生一个 ZPK	3.4.1.5	RACAL 兼容
60	FA	ZPK 从 ZMK 加密转换为 LMK 加密	3.4.1.6	RACAL 兼容
61	GC	ZPK 从 LMK 加密转换为 ZMK 加密	3.4.1.7	RACAL 兼容
62	FI	产生一个 ZEK/ZAK	3.4.1.8	RACAL 兼容
63	FK	ZEK/ZAK 从 ZMK 加密转换为 LMK 加密	3.4.1.9	RACAL 兼容
64	FM	ZEK/ZAK 从 LMK 加密转换为 ZMK 加密	3.4.1.10	RACAL 兼容
65	HC	产生一个 TMK/TPK/PVK	3.4.1.11	RACAL 兼容
66	HA	产生一个 TAK	3.4.1.12	RACAL 兼容
67	MI	将 TAK 从 ZMK 下加密转为 LMK 下加密	3.4.1.13	RACAL 兼容
68	BU	生成密钥校验值	3.4.1.14	RACAL 兼容
RACAL 兼容应用 – PIN 运算相关功能				
69	JA	产生一个随机 PIN 码	3.4.3.1	RACAL 兼容
70	BA	LMK 加密一个明文 PIN	3.4.3.2	RACAL 兼容
71	NG	LMK 解密 PIN	3.4.3.3	RACAL 兼容
72	JC	将 PIN 由 TPK 加密转换为 LMK 加密	3.4.4.1	RACAL 兼容
73	JE	将 PIN 由 ZPK 加密转换为 LMK 加密	3.4.4.2	RACAL 兼容
74	JG	将 PIN 由 LMK 加密转换为 ZPK 加密	3.4.4.3	RACAL 兼容
75	CA	将 PIN 由 TPK 加密转换为 ZPK 加密	3.4.4.4	RACAL 兼容
76	CC	将 PIN 由 ZPK1 加密转换为 ZPK2 加密	3.4.4.5	RACAL 兼容
77	QD	将 PIN 由 ZPK1 加密转 ZPK2 加密并校验	3.4.4.6	
78	TI	将 PIN 由 TPK1/ZPK1 加密转换为 TPK2/ZPK2 加密	3.4.4.6	扩展
79	DE	产生 IBM PIN Offset	3.4.5.1	RACAL 兼容
80	QC	产生 IBM PIN Offset 并校验弱口令	3.4.5.2	
81	EE	使用 IBM 方式得到一个 PIN	3.4.5.2	RACAL 兼容
82	DA	校验一个用 IBM 方式的终端 PIN	3.4.5.4	RACAL 兼容
83	EA	校验一个用 IBM 方式的交换 PIN	3.4.5.5	RACAL 兼容
84	DG	产生 VISA PVV	3.4.5.6	RACAL 兼容
85	EC	PVV 校验 ZPK 加密的 PINBLOCK	0	RACAL 兼容
86	RY	生成或者校验美国运通的 CSC	3.4.5.8	RACAL 兼容
RACAL 兼容应用 – CVV 计算				

87	CW	产生 VISA CVV	3.4.6.1	RACAL 兼容
88	CY	校验 VISA CVV	3.4.6.2	RACAL 兼容
RACAL 兼容应用 – 数据运算				
89	MA	TAK 计算数据 MAC	3.4.2.1	RACAL 兼容
90	MC	TAK 验证数据 MAC	3.4.2.2	RACAL 兼容
91	MQ	ZAK 计算数据 MAC/TAC	3.4.2.3	旧版本兼容
92	UQ	ZPK 计算数据 MAC	3.4.2.4	旧版本兼容
93	MU	ZAK/TAK 产生银联标准报文 MAC	3.4.2.5	旧版本兼容
94	MS	ZAK/TAK 产生 X9.9/X9.19 的报文 MAC	3.4.2.6	RACAL 兼容
95	E0	数据加解密	3.4.7.1	旧版本兼容
96	GM	对一个数据块进行哈希运算	3.4.9.2	RACAL 兼容
97	GN	对一个 PIN 的数据块进行哈希运算	3.4.9.3	
98	GP	计算一个字符 PIN 的 MD5 值	3.4.9.4	
RACAL 兼容应用 – 信函打印				
99	PA	装载打印格式数据	3.4.8.1	RACAL 兼容
100	PE	打印 PIN/PIN 请求数据	3.4.8.2	RACAL 兼容
101	NE	生产密钥并以分开的成份形式打印	3.4.8.3	RACAL 兼容
102	A2	生产并打印一个成份	3.4.8.4	RACAL 兼容
103	A3	生成并打印一个密钥成份及其校验值	3.4.8.5	扩展
104	PG	验证 PIN/PIN 和请求信封密码	3.4.8.6	RACAL 兼容
105	OA	打印一个 PIN 请求信函	3.4.8.7	RACAL 兼容
106	RC	验证请求信封密码	3.4.8.8	RACAL 兼容
107	NF	根据成份密文打印成份信函	3.4.8.9	扩展
非对称（RSA）应用				
108	EI	产生 RSA 密钥对	3.5.1.1	RACAL 兼容
109	EH	产生明文 RSA 密钥对	3.5.1.2	扩展
110	EK	装载 RSA 密钥对 – 兼容旧版本保留	3.5.1.3	旧版本兼容
111	EJ	装载 RSA 密钥对 – 扩展	3.5.1.4	扩展
112	ER	获取 RSA 公钥	3.5.1.5	旧版本兼容
113	3A	RSA 公钥加密运算	3.5.1.6	扩展
114	3B	RSA 私钥解密运算	3.5.1.7	扩展
115	EW	RSA 私钥签名运算	3.5.1.8	RACAL 兼容
116	EY	RSA 公钥验签运算	3.5.1.9	RACAL 兼容

117	TR	保护密钥（对称）加密导出一对 RSA 密钥	3.5.1.10	扩展
118	TS	保护密钥（对称）加密导入一对 RSA 密钥	3.5.1.11	扩展
119	TV	RSA 公钥加密导出一条对称密钥	3.5.1.12	扩展
120	TW	RSA 公钥加密导入一条对称密钥	3.5.1.13	扩展
121	GI	RSA 公钥加密导出一条 DES 密钥，RACAL 兼容	3.5.1.14	RACAL 兼容
122	GK	RSA 公钥加密导入一条 DES 密钥，RACAL 兼容	3.5.1.15	RACAL 兼容
123	EO	为 RSA 公钥产生一个 MAC	3.5.1.16	RACAL 兼容
非对称（SM2）应用				
124	E7	产生 SM2 密钥对	3.5.2.1	扩展
125	E8	产生明文 SM2 密钥对	3.5.2.2	扩展
126	E1	装载 SM2 密钥对	3.5.2.3	扩展
127	E2	获取 SM2 公钥	3.5.2.4	扩展
128	E3	SM2 公钥加密运算	3.5.2.5	扩展
129	E4	SM2 私钥解密运算	3.5.2.6	扩展
130	E5	SM2 私钥签名运算	3.5.2.7	扩展
131	E6	SM2 公钥验签运算	3.5.2.8	扩展
132	ED	SM2 私钥签名（对数据的摘要值）运算	3.5.2.9	扩展
133	EF	SM2 公钥验证（对数据的摘要值）运算	3.5.2.10	扩展
134	TT	保护密钥（对称）加密导出一对 SM2 密钥	3.5.2.11	扩展
135	TU	保护密钥（对称）加密导入一对 SM2 密钥	3.5.2.12	扩展
136	TX	SM2 公钥加密导出一条对称密钥	3.5.2.13	扩展
137	TY	SM2 公钥加密导入一条对称密钥	3.5.2.14	扩展
138	TQ	为 SM2 公钥产生一个 MAC	3.5.2.15	扩展
OTP 动态口令应用				
139	F3	产生令牌种子	3.6.1	扩展
140	F4	解密种子密文	3.6.2	扩展
141	F5	生成 OTP 动态口令	3.6.3	扩展
142	F6	产生新种子并生成 OTP 动态口令	3.6.4	
143	F7	生成 OTP	3.6.4	
144	F8	验证 OTP	3.6.6	
数据摘要运算				
145	3C	计算单包数据摘要	3.3.6.1	扩展
146	H1	大包数据摘要初始化	3.3.6.2	扩展

147	H2	大包数据摘要更新	3.3.6.3	扩展
148	H3	大包数据摘要结束，输出摘要结果	3.3.6.4	扩展
其他功能				
149	NC	获取密码机版本信息	3.4.9.1	RACAL 兼容
150	NP	获取密码机运行状态	3.3.8.2	扩展
151	CR	产生随机数	3.3.8.1	扩展
152	SF	查询/增加屏蔽指令	3.3.8.3	扩展
153	3D	计算/校验 MAC	3.5.3.1	扩展
154	S8	数据转加密－非对称转对称	3.5.3.2	扩展

3.3. 金融 IC 卡应用主机命令

3.3.1. 密钥管理功能

3.3.1.1. 产生一条随机密钥，可选的存储到密码机内（KR）

如果存储到密码机内，需满足主机服务的密钥管理权限。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	KR
密钥类型	3 H	支持全类型 000 - ZMK/KEK; 001 - ZPK; 002 - PVK/TPK/TMK; 402 - CVK; 003 - TAK; 008 - ZAK; 009 - BDK; 109 - MK-AC/MDK; 209 - MK-SMI; 309 - MK-SMC; 409 - MK-DAK; 509 - MK-DN; 00A - ZEK/DEK; 00B - TEK; 10C - HMAC; 011 - KMC;
密钥标识(LMK)	1 A	Z - 8 字节 DES 密钥 X/U - 16 字节 3DES 密钥 Y/T - 24 字节 3DES 密钥 P - 16 字节 SM1 密钥 R - 16 字节 SM4 密钥 L - 16 字节 AES 密钥 M - 24 字节 AES 密钥 N - 32 字节 AES 密钥
密钥存储标识	1 A	可选域。 （1）取值’K’，表明密钥产生后存储在加密机中，当选择此值，后续域“密钥索引”、“密钥标签长度“、“密钥标签”必须存在。 （2）此项为空（没有任何数据），表明密钥不保存加密机中，而是由 LMK 加密后输出密文。
密钥索引	4 N	可选域。仅当密钥存储标识域存在时存在该域 存储到密码机内的密钥索引号，0001 - 2048
密钥标签长度	2 N	可选域，仅当密钥存储标识域存在时存在该域 取值：00-16
密钥标签	0-16 A	可选域。仅当密钥存储标识域存在时存在该域 用于在密钥内部存储时标记密钥的标签说明，0-16 个 ASCII 字符
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	KS
错误码	2 A	00：成功 04：非法的密钥类型 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 26：非法的密钥标识

		41：无主密钥或加密卡运算单元错误 96：密钥标签长度错误
密钥密文	16 H / 1 A + 32 H / 1 A + 48 H / 1 A + 64 H	LMK 加密的密钥密文
校验值	16 H	密钥校验值

示例 1. 产生 SM4 算法的随机 ZMK，不存储

```
[
KR 000 R
|
KS 00 RFD1186F466B2E883EED441894F8E1076 14A47A611D68AB5B
]
```

示例 2. 产生 SM1 算法的随机 MDK，存储到索引 10

```
[
KR 109 P K0010 10 TESTSM1KEY
|
KS 00 PF3354ADA039C991BA1A272F424EE6499 000BE2E970513B9E
]
```

3.3.1.2. 分散产生新密钥，可选的存储到密码机内（KD）

当源密钥是 DES 时，不论子密钥是不是 DES 密钥，都会对子密钥强制做奇校验。如果存储到密码机内，需满足主机服务的密钥管理权限。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**KD**
源密钥类型	3 H	用于分散产生子密钥的源密钥类型 000 - ZMK/KEK; 109 - MK-AC/MDK; 002 - PVK/TPK/TMK; 007 - EDK; 209 - MK-SMI; 309 - MK-SMC; 409 - MK-DAK; 509 - MK-DN; 00A - ZEK/DEK; 011 - KMC; 008 - ZAK;
源密钥	K + 4N / 16H / 1A+16H / 1A + 32H / 1A + 48H / 1A + 64H	用于分散产生新密钥的源密钥索引或密文
子密钥类型	3 H	000 - ZMK/KEK; 109 - MK-AC/MDK; 209 - MK-SMI; 309 - MK-SMC; 409 - MK-DAK; 509 - MK-DN; 00A - ZEK/DEK; 011 - KMC; 008 - ZAK;
子密钥标识(LMK)	1 A	X/U - 16 字节 3DES 密钥 P - 16 字节 SM1 密钥 R - 16 字节 SM4 密钥 L - 16 字节 AES 密钥 N - 32 字节 AES 密钥

分散算法模式	1 H	0 - PBOC 子密钥分散算法 用于分散产生应用子密钥。 8 字节分散因子 D，使用源密钥对 16 字节[D|D 的非]采用源密钥的算法标识进行 ECB 模式加密 1 - ECB 模式加密 16 字节分散因子 2 - ECB 模式加密 16 字节分散因子，并复制扩展为 32 字节长度密钥（仅限子密钥标识为 N） 3 - CBC 模式加密 16 字节分散因子 4 - ECB 模式加密分散因子，分散因子必须为 8 字节的倍数，且至少 16 字节。截取加密结果的前后各 8 字节作为子密钥（仅限子密钥标示为 X/U） 5 - CBC 模式加密分散因子，分散因子必须为 16 字节的倍数。截取加密结果的最后 16 字节作为子密钥（仅限源密钥和子密钥标识为 L）
IV	32 H	可选域，仅当分散算法模式为 5 时存在。
分散级数	2 H	取值 01-08。该域取值决定后面几个分散因子域的长度 当分散算法模式为 4 时，此值至少为 02
分散因子	n*16 H/ n*32 H	n 级分散因子串联 当分散算法模式为 0 时，每级分散因子为 8 字节（16H）； 当分散算法模式为 1 或 2 或 3 时，每级分散因子为 16 字节（32H）； 当分散算法模式为 4 时，分散因子为 n*16H，并且只当做一级分散
密钥存储标识	1 A	可选域。 （1）取值’K’，表明密钥产生后存储在加密机中，当选择此值，后续域“密钥索引”、“密钥标签长度“、“密钥标签”必须存在。 （2）此项为空（没有任何数据），表明密钥不保存加密机中，而是由 LMK 加密后输出密文。
密钥索引	4 N	可选域。仅当密钥存储标识域存在时存在该域 存储到密码机内的密钥索引号，0001 - 2048
密钥标签长度	2 N	可选域，仅当密钥存储标识域存在时存在该域 取值：00-16
密钥标签	0-16 A	可选域。仅当密钥存储标识域存在时存在该域 用于在密钥内部存储时标记密钥的标签说明，0-16 个 ASCII 字符
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	KE
错误码	2 A	00：成功 03：非法的分散算法模式 04：非法的密钥类型 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 26：非法的密钥标识 36：非法的分散级数 41：无主密钥或加密卡运算单元错误 45：密钥不存在 96：密钥标签长度错误
密钥密文	1 A + 32 H / 1 A + 64 H	LMK 加密的密钥密文 当分散算法模式域取值为 2 时，返回 1A+64H 的密钥密文

校验值	16 H	密钥校验值

示例 1. 由 MDK 密钥分散产生一个新的 KEK，不存储

```
[
KD 109 R088F8927B0DCC6DD34B6AD1577A4864E 000 R 1 01
11223344556677881122334455667788
|
KE 00 R32CE58735D8F7C04298B80592D50C2B4 BA3431E9A33E38B7
]
```

3.3.1.3. 分散产生新密钥，可选的存储到密码机内（KJ）

当源密钥是 DES，子密钥是非 DES 密钥时，不会对子密钥做强制奇校验。如果存储到密码机内，需满足主机服务的密钥管理权限。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	KJ
源密钥类型	3 H	用于分散产生子密钥的源密钥类型 000 - ZMK/KEK; 109 - MK-AC/MDK; 209 - MK-SMI; 309 - MK-SMC; 409 - MK-DAK; 509 - MK-DN; 00A - ZEK/DEK; 011 - KMC; 008 - ZAK;
源密钥	K + 4N / 16H / 1A+16H / 1A + 32H / 1A + 48H / 1A + 64H	用于分散产生新密钥的源密钥索引或密文
子密钥类型	3 H	000 - ZMK/KEK; 109 - MK-AC/MDK; 209 - MK-SMI; 309 - MK-SMC; 409 - MK-DAK; 509 - MK-DN; 00A - ZEK/DEK; 011 - KMC; 008 - ZAK;
子密钥标识(LMK)	1 A	X/U - 16 字节 3DES 密钥 P - 16 字节 SM1 密钥 R - 16 字节 SM4 密钥 L - 16 字节 AES 密钥 N - 32 字节 AES 密钥 Z - 8 字节 DES 密钥
分散算法模式	1 H	0 - PBOC 子密钥分散算法 用于分散产生应用子密钥。 8 字节分散因子 D，使用源密钥对 16 字节[D|D 的非]采用源密钥的算法标识进行 ECB 模式加密 1 - ECB 模式加密 16 字节分散因子 2 - ECB 模式加密 16 字节分散因子，并复制扩展为 32 字节长度密钥（仅限子密钥标识为 N） 3 - CBC 模式加密 16 字节分散因子 4 - ECB 模式加密分散因子，分散因子必须为 8 字节的倍数，且至少 16 字节。截取加密结果的前后各 8 字节

		作为子密钥（仅限子密钥标示为 X/U） 5 - CBC 模式加密分散因子，分散因子必须为 16 字节的倍数。截取加密结果的最后 16 字节作为子密钥（仅限源密钥和子密钥标识为 L） 6 - ECB 模式加密分散因子，分散因子为 8 字节的倍数。得到 8 字节的子密钥（仅限源密钥为 DES 和子密钥标识为 Z）
IV	32 H	可选域，仅当分散算法模式为 5 时存在。
分散级数	2 H	取值 01-08。该域取值决定后面几个分散因子域的长度 当分散算法模式为 4 时，此值至少为 02
分散因子	n*16 H/ n*32 H	n 级分散因子串联 当分散算法模式为 0 时，每级分散因子为 8 字节（16H）; 当分散算法模式为 1 或 2 或 3 或 5 时，每级分散因子为 16 字节（32H）; 当分散算法模式为 4 时，分散因子为 n*16H，并且只当做一级分散; 当分散算法模式为 6 时，分散因子为 n*16H
密钥存储标识	1 A	可选域。 （1）取值’K’，表明密钥产生后存储在加密机中，当选择此值，后续域“密钥索引”、“密钥标签长度“、“密钥标签”必须存在。 （2）此项为空（没有任何数据），表明密钥不保存加密机中，而是由 LMK 加密后输出密文。
密钥索引	4 N	可选域。仅当密钥存储标识域存在时存在该域 存储到密码机内的密钥索引号，0001 - 2048
密钥标签长度	2 N	可选域，仅当密钥存储标识域存在时存在该域 取值：00-16
密钥标签	0-16 A	可选域。仅当密钥存储标识域存在时存在该域 用于在密钥内部存储时标记密钥的标签说明，0-16 个 ASCII 字符
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	KK
错误码	2 A	00：成功 03：非法的分散算法模式 04：非法的密钥类型 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 26：非法的密钥标识 36：非法的分散级数 41：无主密钥或加密卡运算单元错误 45：密钥不存在 96：密钥标签长度错误
密钥密文	16 H / 1 A + 32 H / 1 A + 64 H	LMK 加密的密钥密文 当分散算法模式域取值为 2 时，返回 1A+64H 的密钥密文 当分散算法模式域取值为 6 时，返回 16H 的密钥密文
校验值	16 H	密钥校验值

3.3.1.4. 传输密钥保护导出一条密钥（KH）

- 适用于密钥管理系统

  适用于从上级 HSM 导出应用主密钥发给下级 HSM；

  或者从密管 HSM 中导出密钥送给 DP/发卡/交易 HSM；

- 适用于发卡系统

  作为主控密钥的 MDK 起传输密钥作用，保护其他应用密钥 MDK 的卡片子密钥 UDK 导出，灌装给 IC 卡；

【指令功能】使用传输密钥加密被导出密钥输出密文，及密文的 MAC。

使用保护密钥或分散后的子密钥按指定算法模式加密密钥数据块（密钥头||被导出的明文密钥值||80000000…，采用填充模式 0 进行填充），其中密钥值为被导出密钥或分散后的子密钥。

密文 MAC 的计算：

M=命令头||密钥密文||800000000…，采用填充模式 1 进行填充；

R=IC 卡生成的 4 字节随机数；

M’ =M[0]^R[0]||M[1]^R[1]||M[2]^R[2]||M[3]^R[3] ||M[4]||M[5]||…

mac = mac(MAC 密钥或分散后的子密钥, M’)，mac 算法由“MAC 算法模式”域指定。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**KH**
加密算法模式	2 H	00 - ECB 01 - CBC
MAC 算法模式	2 H	01 - ISO9797-1 MAC 算法模式 1 使用 MAC 密钥 CBC 模式加密数据，取最后一段密文； 03 - ISO9797-1 MAC 算法模式 3，限密钥标识为 X/U 等同于 ANSI X9.19，MAC 密钥 16 字节，KL 对数据 DES CBC 加密运算，最后一段结果 KR DES 解密，再 KL DES 加密，得 8 字节 MAC 结果；
MAC 取值方式	2 H	按前个域模式产生的密文值输出下述结果作为 MAC： 01-08 输出 MAC 值的左 n 字节（n 取值为第 2 个数字） 11-18 输出 MAC 值的右 n 字节 21-28 左右异或后取左 n 字节输出 31-38 左右异或后取右 n 字节输出 44 - 四字节异或，最后输出 4 字节 10 - 密钥标识为 P/L/R 时输出完整的 16 字节 MAC 值
保护密钥类型	3 H	用于加密保护被导出密钥的源密钥类型 000 - KEK; 109 - MDK;
保护密钥	K + 4 N / 16 H / 1 A + 16 H / 1 A + 32 H /	用于加密保护被导出密钥的密钥索引或密文

	1 A + 48 H	
保护密钥分散级数	2 H	分散级数。取值 00 - 08
保护密钥分散因子	n*16 H	n 个分散因子的串联。每个分散因子必须为 8 个字节。 用于产生卡片传输密钥或卡片的应用主控密钥；
导出密钥类型	3 H	被导出密钥的类型 000 - KEK; 109 - MK-AC/MDK; 209 - MK-SMI; 309 - MK-SMC; 409 - MK-DAK; 509 - MK-DN; 011 - KMC; 00A - DEK;
导出密钥	K + 4 N / 16 H / 1 A + 16 H / 1 A + 32 H / 1 A + 48 H	被导出密钥的密钥索引或密文
导出密钥分散级数	2 H	分散级数。取值 00 - 08
导出密钥分散因子	n*16 H	n 个分散因子的串联。每个分散因子必须为 8 个字节
MAC 密钥类型	3 H	999 - 与保护密钥同，则下面 3 个域不存在； 000 - KEK; 109 - MDK;
MAC 密钥	K + 4 N / 16 H / 1 A + 16 H / 1 A + 32 H / 1 A + 48 H	可选域，仅当 MAC 密钥类型不为 999 时存在 用于计算密文 MAC 的密钥索引或密文
MAC 密钥分散级数	2 H	分散级数。取值 00 - 08
MAC 密钥分散因子	n*16 H	n 个分散因子的串联。每个分散因子必须为 8 个字节
密钥头长度	2 H	下个域的长度，取值 00-20（即 0-32 字节）
密钥头	n*2 H	IC 卡内存储此密钥的密钥头，用于计算密钥密文 通常为密钥属性
命令头长度	2 H	下个域的长度，取值 00-20（即 0-32 字节）
命令头	n*2 H	IC 卡密钥导入命令的命令头，用于计算密文 MAC 通常 5 字节，最大不超过 32 字节
随机数长度	2 H	下个域的长度，取值 00-20（即 0-32 字节）
随机数	n*2 H	IC 卡生成的随机数，用于计算密文 MAC 通常为 4 字节，最大不超过 32 字节
IV	16 H / 32 H	用于计算密文 MAC 的初始向量 128 位分组（密钥标识 P/L/R）时，该域 16 字节（32H）； 否则该域为 8 字节（16H）；
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**KI**
错误码	2 A	00：成功 03：非法的加密算法模式 04：非法的密钥类型 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 26：非法的密钥标识（可能与 MAC 算法模式不符） 32：非法的密钥头/命令头/随机数长度 34：非法的 MAC 算法模式 35：非法的 MAC 取值方式 36：非法的分散级数 41：无主密钥或加密卡运算单元错误 45：密钥不存在

密文长度	4 H	密钥密文长度
密钥数据块密文	n*2 H	密钥数据块密文
密文 MAC	n*2 H	密文 MAC 结果，长度由 MAC 输出方式域指定
校验值	16 H	密钥校验值

示例 1. 由 SM4 算法的 MDK 密钥不分散，保护导出一个 SM1 算法的 MDK 密钥

```
[
KH
00
01
10
109
R088F8927B0DCC6DD34B6AD1577A4864E
00
109
P507FA708D347757C74C7E9440577655F
00
999
00
00
00
0000000000000000 0000000000000000
|
KI
00
0010
0A454BD287D5A655 E34E175433A258DF
A290BE806507BBDF 87DC3BABED64F0EB
65521449AD048A0E
]
```

3.3.1.5. 传输密钥保护导入一条密钥（KI）

密钥管理指令，适用于将上级 HSM（或发卡母卡）导出的应用主密钥导入到下级 HSM，或者是将密管 HSM 导出的密钥导入到 DP/发卡/交易 HSM 中。

向密码机内导入一条密钥。

先验证密文 MAC，通过后解密出密钥明文存储到指定索引或输出 LMK 加密的密文；

密文及 MAC 算法同导出指令。

如果存储到密码机内，需满足主机服务的密钥管理权限。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**KI**
输入类型	1 H	0 - 仅密文 1 - 密文 + MAC
加密算法模式	2 H	00 - ECB 01 - CBC

MAC 算法模式	2 H	仅当输入类型为 1 时存在 01 – ISO9797-1 MAC 算法模式 1 使用 MAC 密钥 CBC 模式加密数据，取最后一段密文； 03 – ISO9797-1 MAC 算法模式 3，限密钥标识为 X/U 等同于 ANSI X9.19，MAC 密钥 16 字节，KL 对数据 DES CBC 加密运算，最后一段结果 KR DES 解密，再 KL DES 加密，得 8 字节 MAC 结果；
MAC 取值方式	2 H	仅当输入类型为 1 时存在 按前个域模式产生的 MAC 值取下述结果进行 MAC 验证： 01-08 取 MAC 值的左 n 字节（n 取值为第 2 个数字） 11-18 取 MAC 值的右 n 字节 21-28 左右异或后取左 n 字节输出 31-38 左右异或后取右 n 字节输出 44 – 四字节异或，最后输出 4 字节 10 – 密钥标识为 P/L/R 时完整的 16 字节 MAC 值
保护密钥类型	3 H	用于加密保护被导入密钥的源密钥类型 000 – KEK; 109 – MDK;
保护密钥	K + 4 N / 16 H / 1 A + 16 H / 1 A + 32 H / 1 A + 48 H	用于加密保护被导入密钥的密钥索引或密钥密文
保护密钥分散级数	2 H	分散级数。取值 00 – 08
保护密钥分散因子	n*16 H	n 个分散因子的串联。每个分散因子必须为 8 个字节
导入密钥类型	3 H	被导入密钥的类型 011 – KMC; 109 – MDK; 00A – DEK;
导入密钥标识(LMK)	1 A	Z – 8 字节 DES 密钥 X/U – 16 字节 3DES 密钥 Y/T – 24 字节 3DES 密钥 P – 16 字节 SM1 密钥 R – 16 字节 SM4 密钥 L – 16 字节 AES 密钥 M – 24 字节 AES 密钥 N – 32 字节 AES 密钥
导入密钥存储标识	1 A	可选域。取值‘K’； 如存在该标识，则表明存储到 HSM 中某索引，必须存在后续 3 个域。 否则：输出 LMK 下加密的密钥
导入密钥索引	4 N	可选域： 仅当导入密钥存储标识域存在时存在该域 存储到密码机内的密钥索引号，0001 – 2048
导入密钥标签长度	2 N	可选域： 仅当导入密钥存储标识域存在时存在该域 取值：00-16
导入密钥标签	0-16 A	用于标记被导入密钥的标签说明，0-16 个 ASCII 字符
MAC 密钥类型	3 H	可选项： 仅当输入类型为 1 时存在该域 999 – 与保护密钥同，下面 3 个域不存在 000 – KEK; 109 – MDK;

MAC 密钥	K + 4 N / 16 H / 1 A + 16 H / 1 A + 32 H / 1 A + 48 H	可选域，输入类型为 1，MAC 密钥类型不为 999 时存在 用于计算密文 MAC 的密钥索引或密文
MAC 密钥分散级数	2 H	可选域，输入类型为 1，MAC 密钥类型不为 999 时存在 分散级数。取值 00 – 08。
MAC 密钥分散因子	n*16 H	可选域，输入类型为 1，MAC 密钥类型不为 999 时存在 n 个分散因子的串联。每个分散因子必须为 8 个字节。
密钥头长度	2 H	下个域的长度，取值 00-20（即 0-32 字节）
密钥头	n*2 H	IC 卡内存储此密钥的密钥头，用于计算密钥密文 通常为密钥属性 若该域输入全 00，则密码机不验证密钥头的有效性；
命令头长度	2 H	可选域，输入类型为 1 时存在 下个域的长度，取值 00-20（即 0-32 字节）
命令头	n*2 H	可选域，输入类型为 1 时存在 IC 卡密钥导入命令的命令头，用于验证密文 MAC 通常 5 字节，最大不超过 32 字节
随机数长度	2 H	可选域，输入类型为 1 时存在 下个域的长度，取值 00-20（即 0-32 字节）
随机数	n*2 H	可选域，输入类型为 1 时存在 IC 卡生成的随机数，用于验证密文 MAC 通常为 4 字节，最大不超过 32 字节
IV	16 H / 32 H	可选项,仅当输入类型为 1 时存在该域 用于计算密文 MAC 的初始向量。 128 位分组（密钥标识 P/L/R）时，该域 16 字节（32H）； 否则该域为 8 字节（16H）；
密文长度	4 H	被导入的密钥数据密文长度
密钥数据块密文	n*2 H	保护密钥加密下的被导入的密钥数据块密文
密文 MAC	16 H	可选项，仅当安全报文类型为 1 时存在。 如果 MAC 不满 16H，则左对齐后右补字符‘0’；MAC 校验时忽略右边为 0 的位。 例如： MAC 为 8H(12345678)，则该项为 1234567800000000
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**KJ**
错误码	2 A	00：成功 01：MAC 验证失败 03：非法的加密算法模式 04：非法的密钥类型 08：非法的输入类型 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 26：非法的密钥标识（可能与 MAC 算法模式不符） 34：非法的 MAC 算法模式 35：非法的 MAC 取值方式 36：非法的分散级数 41：无主密钥或加密卡运算单元错误 45：密钥不存在 70：无效的密文数据，密钥解密去 padding 失败
新密钥密文(LMK)	16 H /	LMK 加密的被导入密钥密文

	1 A + 32 H / 1 A + 48 H	
密钥校验值	16 H	被导入密钥的校验值

示例 1. 由 SM4 算法的 MDK 密钥不分散，保护导出一个 SM1 算法的 MDK 密钥

```
[
KI
1
00
01
10
109
R088F8927B0DCC6DD34B6AD1577A4864E
00
109
P
999
00
00
00
0000000000000000 0000000000000000
0010
0A454BD287D5A655 E34E175433A258DF
A290BE806507BBDF
|
KJ
00
P507FA708D347757C74C7E9440577655F
65521449AD048A0E
]
```

3.3.1.6. 保护密钥加密导出一条密钥 – 通用（SH）

通用的指令，分散因子为 16 字节的外部组合的数据，使用源密钥直接 ECB 模式加密该分散因子数据块得到目标子密钥；

保护密钥可使用源密钥或源分散后的子密钥或产生的会话密钥，按指定算法模式加密密钥数据块（密钥头||被密钥值||80000000…，采用填充模式 0 进行填充），其中密钥值为被导出密钥或分散后的子密钥，输出密文。

保护密钥加密被导出密钥时采用的算法，由保护密钥的密钥方案（密钥标识 1A）指定，算法的模式由“加密算法模式”域指定。

本指令仅输出密文，若要密文的 MAC 请另行使用 MAC 产生指令。

报文后部的扩展域，仅限主机服务 H1.14.00 版本以上支持。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机

命令代码	2 A	SH
加密算法模式	2 H	标识保护密钥加密被导出密钥时的算法模式 00 - ECB 01 - CBC
保护密钥类型	3 H	用于加密保护被导出密钥的源密钥类型 000 - ZMK/KEK; 109 - MDK; 011 - KMC;
保护密钥	K + 4 N / 16 H / 1 A + 16 H / 1 A + 32 H / 1 A + 48 H	用于加密保护被导出密钥的密钥索引或密文
保护密钥分散级数	2 H	分散级数。取值 00 - 03。
保护密钥分散因子	n*32 H	n 个分散因子的串联。每个分散因子必须为 16 个字节
会话密钥模式	2 H	会话密钥的产生模式： 00 - 不产生会话密钥； 01 - ECB 模式加密 8 字节会话密钥因子，得 8 字节会话密钥； 02 - ECB 模式加密 16 字节会话密钥因子，得 16 字节会话密钥； 03 - 密钥的左右 8 字节异或，得 8 字节会话密钥； 04 - 取密钥的左 8 字节做为会话密钥； 05 - CBC 模式加密 16 字节会话密钥因子，得 16 字节会话密钥；
会话密钥因子	16 H / 32 H	仅当会话密钥模式取值为 01/02/05 时存在 • 会话密钥模式为 01 时，该域为 8 字节（16H），适用于产生 PBOC 规范的单长度会话密钥，取值：6 字节 0x00||2 字节 ATC； • 会话密钥模式为 02 时，该域为 16 字节（32H），适用于产生 PBOC 规范的双长度会话密钥，取值：6 字节 0x00||2 字节 ATC||6 字节 0x00||2 字节 ATC 的非； • 会话密钥模式为 05 时，该域为 16 字节（32H），适用于产生 GP 规范 SCP02 的卡片会话密钥，取值：2 字节密钥类型||2 字节卡计数器||12 字节 0x00；
导出密钥类型	3 H	被导出密钥的类型 000 - KEK; 109 - MK-AC/MDK; 209 - MK-SMI; 309 - MK-SMC; 409 - MK-DAK; 509 - MK-DN; 011 - KMC; 00A - DEK;
导出密钥	K + 4 N / 16 H / 1 A + 16 H / 1 A + 32 H / 1 A + 48 H	被导出密钥的密钥索引或密文
导出密钥分散级数	2 H	分散级数。取值 00 - 03
导出密钥分散因子	n*32 H	n 个分散因子的串联。每个分散因子必须为 16 个字节
密钥头长度	2 H	下个域的长度，取值 00-20（即 0-32 字节）
密钥头	n*2 H	IC 卡内存储此密钥的密钥头（通常为密钥属性） 用于计算密钥密文。
扩展标识	1 A	可选域，若该域存在，说明下面的扩展域存在； 若该域不存在，后面的扩展域均不存在，HSM 默认采用填充模式 00 和一个分组全 00 的 IV（CBC 加密模式）；

		取值’P’
PAD 标识	2 H	可选域，当且仅当“扩展标识”域取值 P 时存在 标识加密被导出密钥块前的填充规则 取值范围：00 – 05 或 10 – 11，详细规则参见 4.1
IV	16 H / 32 H	可选域，仅当“扩展标识”域取值 P 且加密算法模式为 01 时存在 若密钥算法为 128 分组，该域为 16 字节（32H）； 若密钥算法为 64 分组，该域为 8 字节（16H）；
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	SI
错误码	2 A	00：成功 03：非法的加密算法模式 04：非法的密钥类型 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 32：非法的密钥头长度 36：非法的分散级数 39：非法的数据填充方式 41：无主密钥或加密卡运算单元错误 45：密钥不存在
密文长度	4 H	密钥密文长度
密钥数据块密文	n*2 H	密钥数据块密文
校验值	16 H	被导出密钥或子密钥的校验值

示例 1. 由 SM1 算法的 MDK 密钥不分散，保护导出一个 3DES 算法 KMC 分散后的子密钥

```
[
SH
00
109
P76298B89E695BC15036ADC0897419C5F
00
00
011
XFB1EBAD4D27986591CDD805C09C6E5AC
01
00112233445566778899AABBCCDDEEFF
05
0102030405
|
SI
00
0020
009094562CCF5A68ABBFDC78D93F806D
14149D14AD29997761D9E415C68D0EAA
A1F3C0E167D545C6
]
```

3.3.1.7. 保护密钥加密导入一条密钥 – 通用（SI）

通用的指令，分散因子为 16 字节的外部组合的数据，使用源密钥直接 ECB 模式加密该数据得

到目标子密钥；

保护密钥解密被导入密钥密文时采用的算法，由保护密钥的密钥方案（密钥标识 1A）指定，算法的模式由“加密算法模式”域指定。

本指令仅解密密文，存储到指定位置，若要验证密文的 MAC 请另行使用 MAC 验证指令。

如果存储到密码机内，需满足主机服务的密钥管理权限。

报文后部的扩展域，仅限主机服务 H1.14.00 版本以上支持。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	SI
加密算法模式	2 H	标识保护密钥加密被导入密钥时的算法模式 00 - ECB 01 - CBC
保护密钥类型	3 H	用于加密保护被导出密钥的源密钥类型 000 - KEK; 109 - MDK; 011 - KMC;
保护密钥	K + 4 N / 16 H / 1 A + 16 H / 1 A + 32 H / 1 A + 48 H	用于加密保护被导出密钥的密钥索引或密文
保护密钥分散级数	2 H	分散级数。取值 00 - 03
保护密钥分散因子	n*32 H	n 个分散因子的串联。每个分散因子必须为 16 个字节
会话密钥模式	2 H	会话密钥的产生模式： 00 - 不产生会话密钥； 01 - ECB 模式加密 8 字节会话密钥因子，得 8 字节会话密钥； 02 - ECB 模式加密 16 字节会话密钥因子，得 16 字节会话密钥； 03 - 密钥的左右 8 字节异或，得 8 字节会话密钥； 04 - 取密钥的左 8 字节做为会话密钥； 05 - CBC 模式加密 16 字节会话密钥因子，得 16 字节会话密钥；
会话密钥因子	16 H / 32 H	仅当会话密钥模式取值为 01/02/05 时存在 • 会话密钥模式为 01 时，该域为 8 字节（16H），适用于产生 PBOC 规范的单长度会话密钥，取值：6 字节 0x00||2 字节 ATC； • 会话密钥模式为 02 时，该域为 16 字节（32H），适用于产生 PBOC 规范的双长度会话密钥，取值：6 字节 0x00||2 字节 ATC||6 字节 0x00||2 字节 ATC 的非； • 会话密钥模式为 05 时，该域为 16 字节（32H），适用于产生 GP 规范 SCP02 的卡片会话密钥，取值：2 字节密钥类型||2 字节卡计数器||12 字节 0x00；
导入密钥类型	3 H	被导入密钥的类型 000 - ZMK/KEK; 001 - ZPK; 002 - PVK/TPK/TMK; 402 - CVK;

		003 - TAK; 008 - ZAK; 009 - BDK; 109 - MK-AC/MDK; 209 - MK-SMI; 309 - MK-SMC; 409 - MK-DAK; 509 - MK-DN; 00A - ZEK/DEK; 00B - TEK; 011 - KMC;
导入密钥标识(LMK)	1 A	Z - 8 字节 DES 密钥 X/U - 16 字节 3DES 密钥 Y/T - 24 字节 3DES 密钥 P - 16 字节 SM1 密钥 R - 16 字节 SM4 密钥 L - 16 字节 AES 密钥
导入密钥密文长度	4 H	被导入的密钥的密文长度
导入密钥密文	n*2H	被导入的密钥密文
导入密钥存储标识	1 A	可选域。取值‘K’； 如存在该标识，则表明存储到 HSM 中某索引，必须存在后续域。
导入密钥索引	4 N	可选域。仅当导入密钥存储标识域存在时存在该域 存储到密码机内的密钥索引号，0001 - 2048
导入密钥标签长度	2 N	可选域，仅当导入密钥存储标识域存在时存在该域 取值：00-16
导入密钥标签	0-16 A	用于标记被导入密钥的标签说明，0-16 个 ASCII 字符
密钥头长度	2 H	下个域的长度，取值 00-20（即 0-32 字节）
密钥头	n*2 H	IC 卡内存储此密钥的密钥头（通常为密钥属性） 若该域输入全 00，则密码机不验证密钥头的有效性；
扩展标识	1 A	可选域，若该域存在，说明下面的扩展域存在； 若该域不存在，后面的扩展域均不存在，HSM 默认采用填充模式 00 去除填充，一个分组全 00 的 IV（CBC 加密模式），不校验 KEYCV； 取值’P’
PAD 标识	2 H	可选域，当且仅当“扩展标识”域取值 P 时存在 标识加密被导出密钥块前的填充规则 取值范围：00－05 或 10 - 11，详细规则参见 4.1
IV	16 H / 32 H	可选域，仅当“扩展标识”域取值 P 且加密算法模式为 01 时存在 若密钥算法为 128 分组，该域为 16 字节（32H）； 若密钥算法为 64 分组，该域为 8 字节（16H）；
被导入密钥的校验值 KEYCV	16 H	可选域，当且仅当“扩展标识”域存在时存在 用于校验被导入密钥的合法性 如果校验值不满 16H，则左对齐后右补字符‘0’；校验时忽略右边为 0 的位。若输入全 0 则不进行验证。
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	SJ
错误码	2 A	00：成功 03：非法的加密算法模式 04：非法的密钥类型 07：密钥校验值无效或验证失败 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 26：非法的密钥标识 32：非法的密钥头长度

		36：非法的分散级数 39：非法的数据填充方式 41：无主密钥或加密卡运算单元错误 45：密钥不存在 70：无效的密文数据，密钥解密去 padding 失败 97：会话密钥模式与源密钥类型冲突
新密钥密文(LMK)	16H / 1A + 32H / 1A + 48H	LMK 加密的被导入密钥密文
校验值	16 H	被导入密钥的校验值

示例 1. 由 SM1 算法的 MDK 密钥，保护导入一个 3DES 算法的 DEK 密钥，存储到 1 号索引

```
[
SI
00
109
P76298B89E695BC15036ADC0897419C5F
00
00
00A
X
0020
009094562CCF5A68ABBFDC78D93F806D
14149D14AD29997761D9E415C68D0EAA
K0001
08
IMP-TEST
05
0102030405
|
SJ
00
X7EFF855D83B8A908A307606791100888
A1F3C0E167D545C6
]
```

3.3.1.8. 获取对称密钥状态信息（KG）

获取密码机内某索引对称密钥的状态信息，包括密钥类型、算法标识等；若不存在则报告错误。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**KG**
密钥索引号	4 N	密钥索引号（1-2048） 获取状态信息密钥的指定索引
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**KH**
错误码	2 A	00：成功 21：非法的密钥索引 41：无主密钥或加密卡运算单元错误

		45：密钥不存在
密钥类型	3 H	000/001/008 …
密钥算法标识	1 A	Z/X/Y/U/T/L/P/R/M/N
KeyCV	16 H	密钥校验值
密钥标签长度	2 N	取值：00-16
密钥标签	n A	用于在密钥内部存储时标记密钥的标签说明，0-16 个 ASCII 字符
时间长度	2 N	密钥最后更新时间长度
时间	n A	密钥最后更新时间

示例 1. 获取 1 号索引的密钥信息

```
[
KG
0001
|
KH
00
00A
X
A1F3C0E167D545C6
0019
2013-06-20 17:45:47
]
```

3.3.1.9. 删除内部指定索引的密钥（KF）

需满足主机服务的密钥管理权限，删除内部指定索引的对称密钥或非对称密钥。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**KF**
密钥类型	2 N	指定待删除密钥的类型 00 - 对称密钥 01 - RSA 密钥对 02 - SM2 密钥对
密钥索引号	K + 4 N / G + 6 N	密钥索引号（1-2048） 待删除的密钥的索引号
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**KG**
错误码	2 A	00：成功 21：非法的密钥索引 41：无主密钥或加密卡运算单元错误 45：密钥不存在

3.3.1.10. 导入存储一条对称密钥（KA）

将 LMK 加密的密钥密文，导入到密码机内，内部验证校验值通过后存储到指定索引中。

需满足主机服务的密钥管理权限。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**KA**
密钥类型	3 H	支持全类型 000 - ZMK/KEK; 001 - ZPK; 002 - PVK/TPK/TMK; 402 - CVK; 003 - TAK; 008 - ZAK; 009 - BDK; 109 - MK-AC/MDK; 209 - MK-SMI; 309 - MK-SMC; 409 - MK-DAK; 509 - MK-DN; 00A - ZEK/DEK; 00B - TEK; 10C - HMAC; 011 - KMC;
密钥密文	16 H / 1 A + 32 H / 1 A + 48 H / 1 A + 64 H	LMK 加密的密钥密文
校验值	16 H	密钥校验值，校验通过后内部存储 输入全 0 则不验证，直接存储覆盖
密钥索引	K + 4 N	存储到密码机内的密钥索引号，0001 - 2048
密钥标签长度	2 N	取值：00-16
密钥标签	0-16 A	用于在密钥内部存储时标记密钥的标签说明，0-16 个 ASCII 字符
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**KB**
错误码	2 A	00：成功 04：非法的密钥类型代码（或索引内密钥类型不合法） 05：非法的密钥长度（或索引内密钥长度不符） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 41：无主密钥或加密卡运算单元错误 45：密钥不存在
校验值	16 H	密钥校验值

3.3.1.11. 分散密钥输出子密钥的多个成分密文（KE）

分散产生新密钥，并输出子密钥的密文和多个成分密文，成分密文采用子密钥的类型所对应的 LMK 加密。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**KE**
源密钥类型	3 H	用于分散产生子密钥的源密钥类型 000 - ZMK/KEK; 109 - MK-AC/MDK; 209 - MK-SMI; 309 - MK-SMC; 409 - MK-DAK; 509 - MK-DN;

		00A - ZEK/DEK; 011 - KMC; 008 - ZAK;
源密钥	K+4N / 16H / 1A + 32H / 1A + 48H / 1A + 64H	用于分散产生新密钥的源密钥索引或密文
子密钥类型	3 H	000 - ZMK/KEK; 109 - MK-AC/MDK; 209 - MK-SMI; 309 - MK-SMC; 409 - MK-DAK; 509 - MK-DN; 00A - ZEK/DEK; 011 - KMC; 008 - ZAK;
子密钥标识(LMK)	1 A	X/U - 16 字节 3DES 密钥 P - 16 字节 SM1 密钥 R - 16 字节 SM4 密钥 L - 16 字节 AES 密钥 N - 32 字节 AES 密钥
分散算法模式	1 H	0 - PBOC 子密钥分散算法 用于分散产生应用子密钥。 8 字节分散因子 D，使用源密钥对 16 字节[D|D 的非]采用源密钥的算法标识进行 ECB 模式加密 1 - ECB 模式加密 16 字节分散因子 2 - ECB 模式加密 16 字节分散因子，并复制扩展为 32 字节长度密钥（仅限子密钥标识为 N） 3 - CBC 模式加密 16 字节分散因子
分散级数	2 H	取值 01-08。该域取值决定后面几个分散因子域的长度
分散因子	n*16 H / n*32 H	n 级分散因子串联 当分散算法模式为 0 时，每级分散因子为 8 字节（16H）; 当分散算法模式为 1 或 2 或 3 时，每级分散因子为 16 字节（32H）;
密钥成分个数	1 N	成分个数（2-8）
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**KF**
错误码	2 A	00：成功 04：非法的密钥类型代码（或索引内密钥类型不合法） 05：非法的密钥长度（或索引内密钥长度不符） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 41：无主密钥或加密卡运算单元错误 45：密钥不存在
子密钥校验值	16 H	分散后的子密钥的校验值
密钥成份 1 密文	1 A + 32 H / 1 A + 64 H	加密的子密钥成份 1
密钥成份 1 校验值	8 H	
密钥成份 2 密文	1 A + 32 H / 1 A + 64 H	加密的子密钥成份 2
密钥成份 2 校验值	8 H	
…		…
…		…
密钥成份 n 密文	1 A + 32 H / 1 A + 64 H	加密的子密钥成份 n
密钥成份 2 校验值	8 H	

3.3.2. GP 规范发卡专用功能

本部分为发卡系统的密码安全应用专用功能指令，适用于符合 GP 规范 V2.1.1 SCP02 协议的卡片应用。

【注意】本节功能指令仅支持双倍长 3DES 密钥的密钥（X / U）。

3.3.2.1. 厂商 KMC 加密保护导出发行商 KMC 三条卡片密钥（G1）

发卡洗卡命令。厂商 KMC 与发行商 KMC 通过密码机管理终端导入到 HSM 中，每张 IC 卡出厂时存有厂商的卡片主密钥（3 条 Kenc/Kmac/Kdek）；在发卡洗卡时需要首先替换成发行商的卡片主密钥（3 条 Kenc/Kmac/Kdek）。

该命令使用厂商 KMC（Sdek）加密保护导出发行商 KMC 密钥（Kenc/Kmac/Kdek），其密文用于替换 IC 卡中的 3 条主密钥。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	G1
加密算法模式	2 H	用于指定厂商 Sdek 加密被导出的发行商密钥时采用的算法模式 00 - ECB 01 - CBC
保护密钥(厂商KMC)	K + 4N / 16 H / 1A + 32H / 1A + 48H	用于加密保护被导出密钥的源密钥(厂商 KMC)索引或密文
导出密钥(发行商KMC)	K + 4N / 16 H / 1A + 32H / 1A + 48H	被导出密钥(发行商 KMC)的密钥索引或密文
卡片个人化密钥数据 keydata	6*2 H	由 6 字节 KMCID 和 4 字节芯片序号（CSN）组成，该域取 6 个最低有效字节 用于分散产生 Kenc / Kmac / Kdek
卡片计数器	4 H	用于计算厂商 Sdek 会话密钥的计数器，2 字节
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	G2
错误码	2 A	00：成功 03：非法的加密算法模式 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 21：非法的密钥索引 26：非法的密钥标识(或不支持的算法) 36：非法的分散级数 41：无主密钥或加密卡运算单元错误 45：密钥不存在
Issue Kenc 密文	32 H	卡片厂商 Sdek 会话密钥加密的发行商 Kenc 密文。

Issue Kenc 校验值	16 H	卡片发行商 Kenc 密钥校验值
Issue Kmac 密文	32 H	卡片厂商 Sdek 会话密钥加密的发行商 Kmac 密文。
Issue Kmac 校验值	16 H	卡片发行商 Kmac 密钥校验值
Issue Kdek 密文	32 H	卡片厂商 Sdek 会话密钥加密的发行商 Kdek 密文。
Issue Kdek 校验值	16 H	卡片发行商 Kdek 密钥校验值

示例 1. 厂商 KMC 保护导出发行商 KMC 的三条卡片主密钥

```
[
G1
00
XFB1EBAD4D27986591CDD805C09C6E5AC
XFB1EBAD4D27986591CDD805C09C6E5AC
010203040506
0001
|
G2
00
E5B52F3ED098EE1FDE658331005C3AA0
6A9D8C46EDBAAA6B
CDFA079975DB41C58D928763FBE626F9
C894E3437BF82F72
2888B72909BFE51B0E4E3EA3206BB877
257015EE57055C0A
]
```

3.3.2.2. KMC(Kdek)加密导出多条应用密钥（G2）

发行商 KMC（使用 Sdek 会话密钥）加密一系列 MDK 分散后的卡片密钥，输出密钥密文，用于向 IC 卡发行灌装。如需形成安全报文模式另行使用 KMC 加密数据指令和 KMC 计算 MAC 指令。

1. 使用发行商 KMC，根据 IC 卡的密钥数据（keydata，由 KMCID 和芯片序号（CSN）组成，共 10 字节的最右 6 字节）分散产生卡片发行商 Kdek，再根据会话密钥因子['0181'||2 字节计数器||12 个'00']生成厂商 Sdek 会话密钥。
2. 密码机内组合密钥数据块：

   [密钥头 1 || UDK1 || 密钥头 2 || UDK2 || …密钥头 n || UDKn || 800000]

   其中 UDKn 是 MDKn 根据卡账号分散产生，采用填充模式 0 对密钥块进行填充；
3. 使用 Sdek 会话密钥按指定算法模式加密该数据块，输出密文；

域	长度&类型	描述
	命令报文	
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	G2
加密算法模式	2 H	用于指定 Sdek 加密被导出密钥时采用的算法模式 00 - ECB 01 - CBC
保护密钥（发行商 KMC）	K + 4N / 16 H /	用于加密保护被导出密钥的源密钥(发行商 KMC)索引或密文

	1A + 32H / 1A + 48H	
密钥派生数据	12 H	由 6 字节 KMCID 和 4 字节芯片序号（CSN）组成，该域取 6 个最低有效字节 用于分散产生卡片 Kdek
卡序列计数器（SCP02）	4 H	用于由 Kdek 产生 Sdek 会话密钥： Kdek 3DES-CBC 加密[‘0181’+2 字节计数器+12 个’00’]；
每个密钥头长度	2 H	被导出密钥的单个密钥头的长度，取值 00-20（即 0-32 字节）
被导出密钥的分散级数	2 H	分散级数。取值 01 – 08 因为是发卡指令，所以该密钥必须被分散成卡片密钥再加密导出
被导出密钥分散因子	32*n H	用于将被导出密钥分散产生卡片的密钥 UDK。每个分散因子 16 字节（32H） 通常为 8 字节 PAN 或 PAN 序列||8 字节前段数据的非
要导出密钥个数 NUM	2 H	要导出密钥的个数，取值 01-08
被导出密钥 1 类型	3 H	被导出密钥的类型 109 – MDK/MK-AC; 209 – MK-SMI; 309 – MK-SMC; 409 – MK-DAK; 509 – MK-DN;
被导出密钥 1	K + 4N / 16 H / 1A + 32H / 1A + 48H	被加密导出的密钥 1 索引或 LMK 加密的密钥密文
密钥头 1	n*2 H	被导出密钥 1 的密钥头数据。长度必须与“每个密钥头长度”域一致
被导出密钥 2 类型	3 H	被导出密钥的类型 109 – MDK/MK-AC; 209 – MK-SMI; 309 – MK-SMC; 409 – MK-DAK; 509 – MK-DN;
。。。		
被导出密钥 n 类型	3 H	被导出密钥的类型 109 – MDK/MK-AC; 209 – MK-SMI; 309 – MK-SMC; 409 – MK-DAK; 509 – MK-DN;
被导出密钥 n	K + 4N / 1A + 16 H / 1A + 32H / 1A + 48H	被加密导出的密钥 n 索引或 LMK 加密的密钥密文
密钥头 n	n*2 H	被导出密钥 n 的密钥头数据。长度必须与“每个密钥头长度”域一致
分隔符	1 A	‘;’ 标识所有密钥结束；
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	G3
错误码	2 A	00：成功 03：非法的加密算法模式或密钥算法标识 04：非法的密钥类型（或索引内密钥类型不合法） 09：非法的密钥导出个数 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误）

		21：非法的密钥索引 26：非法的密钥标识(或不支持的算法) 32：非法的密钥头长度 36：非法的分散级数 41：无主密钥或加密卡运算单元错误 45：密钥不存在
密文长度	4 H	密钥块密文的长度，字节数
密钥块密文	n*2 H	密钥块的密文
子密钥 1 校验值	16 H	被导出的子密钥 1 的校验值
…		
子密钥 n 校验值	16 H	被导出的子密钥 n 的校验值

示例 1. 发行商 KMC 保护导出 2 条应用 UDK

```
[
G2
00
XFB1EBAD4D27986591CDD805C09C6E5AC
010203040506
0001
02
01
1234567890123456EDCBA9876FEDCBA9
02
109
X84BE3F9DF32844D77B60C89583EBC6B2
0001
109
R8DBD3678578715FF669C473B64EDDA3E
0002
;
|
G3
00
0028
E991942161B3EAE15A9D99085C95228F
CA7A499D825A37A4D52E61C37097018D
E182098AED4ECC56
E3B0E34559D8EC15
C38E5ED8EB7C962B
]
```

3.3.2.3. KMC(Sdek)加密敏感数据（G3）

发行商 KMC（使用 Sdek 会话密钥）加密卡片敏感数据，如脱机 PIN 等，输出数据密文，用于向 IC 卡发行灌装。如需形成安全报文模式另行使用 KMC 加密数据指令和 KMC 计算 MAC 指令。

1. 使用发行商 KMC，根据 IC 卡的密钥数据（keydata，由 KMCID 和芯片序号（CSN）组成，共 10 字节的最右 6 字节）分散产生卡片发行商 Kdek，再根据会话密钥因子['0181'||2 字节计数器||12 个'00']生成厂商 Sdek 会话密钥。
2. 使用 Sdek 会话密钥按指定算法模式加密填充后的数据块，输出密文；

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	G3
加密算法模式	2 H	用于指定 Sdek 加密机密数据时采用的算法模式 00 - ECB 01 - CBC
KMC 源密钥	K + 4N / 16 H / 1A + 32H / 1A + 48H	用于加密机密数据的源密钥(发行商 KMC)索引或密文
密钥派生数据	12 H	由 6 字节 KMCID 和 4 字节芯片序号（CSN）组成，该域取 6 个最低有效字节 用于分散产生卡片 Kdek。
卡序列计数器（SCP02）	4 H	用于由 Kdek 产生 Sdek 会话密钥：Kdek 3DES-CBC 加密[‘0181’+2 字节 Counter+12 个’00’]
机密数据长度	4 H	要被加密的机密数据的长度 取值 0000-03D8（即 0-984 字节）
机密数据	n*2 H	要被加密的机密数据
PAD 标识	2 H	标识加密前数据的填充规则 取值范围：00 - 05，详细规则参见 4.1
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	G4
错误码	2 A	00：成功 03：非法的加密算法模式 04：非法的密钥类型 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 26：非法的密钥标识(或不支持的算法) 36：非法的分散级数 39：非法的数据填充方式 41：无主密钥或加密卡运算单元错误 45：密钥不存在 80：非法的数据长度
密文长度	4 H	数据密文的长度，字节数
数据密文	n*2 H	数据的密文

示例 1. 发行商 KMC 加密用户卡片的脱机 PIN（123456）

```
[
G3
00
XFB1EBAD4D27986591CDD805C09C6E5AC
010203040506
0001
0006
313233343536
01
|
G4
00
```

0008
55A28985ED43F759
]

3.3.2.4. KMC(Senc)加密数据（G4）

发行商 KMC（使用 Senc 会话密钥）加密输入数据，通常用于加密 APDU 命令报文保证其安全性；如安全报文有报文完整性的需求，请另行使用 KMC 计算 MAC 指令。

1. 使用发行商 KMC，根据 IC 卡的密钥数据（keydata，由 KMCID 和芯片序号（CSN）组成，共 10 字节的最右 6 字节）分散产生卡片发行商 Kenc，再根据会话密钥因子['0182'||2 字节计数器||12 个'00']生成厂商 Senc 会话密钥。
2. 使用 Senc 会话密钥按指定算法模式加密填充后的数据块，输出密文；

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	G4
加密算法模式	2 H	用于指定 Senc 加密数据时采用的算法模式 00 - ECB 01 - CBC
KMC 源密钥	K + 4N / 16 H / 1A + 32H / 1A + 48H	用于加密数据的源密钥(发行商 KMC)索引或密文
密钥派生数据	12 H	由 6 字节 KMCID 和 4 字节芯片序号（CSN）组成，该域取 6 个最低有效字节 用于分散产生卡片 Kenc。
卡序列计数器（SCP02）	4 H	用于由 Kenc 产生 Senc 会话密钥：Kenc 3DES-CBC 加密['0182' +2 字节 Counter+12 个' 00']；
输入数据长度	4 H	要被加密的数据的长度 取值 0000-03D8（即 0-984 字节）
输入数据	n*2 H	要被加密的数据
PAD 标识	2 H	标识加密前数据的填充规则 取值范围：00 - 05，详细规则参见 4.1
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	G5
错误码	2 A	00：成功 03：非法的加密算法模式 04：非法的密钥类型 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 26：非法的密钥标识(或不支持的算法) 36：非法的分散级数 39：非法的数据填充方式 41：无主密钥或加密卡运算单元错误 45：密钥不存在 80：非法的数据长度

密文长度	4 H	数据密文的长度，字节数。
数据密文	n*2 H	数据的密文

示例 1. 发行商 KMC 加密一段数据

```
[
G4
00
XFB1EBAD4D27986591CDD805C09C6E5AC
010203040506
0001
0006
313233343536
01
|
G5
00
0008
73BD82A066034416
]
```

3.3.2.5. KMC(Scmac)计算数据 C-MAC（G5）

发行商 KMC（使用 Sc-mac 会话密钥）计算数据的 MAC。通常用于在需要完整性安全报文的 APDU 命令中对 [命令头 CLA+INS+P1+P2+Lc||数据域] 计算 C-MAC。如安全报文模式需要保密性，则请另行使用 KMC 加密数据指令。

1. 使用发行商 KMC，根据 IC 卡的密钥数据（keydata，由 KMCID 和芯片序号（CSN）组成，共 10 字节的最右 6 字节）分散产生卡片发行商 Kmac，再根据会话密钥因子['0101'||2 字节计数器||12 个'00']生成厂商 Sc-mac 会话密钥。
2. 使用 Sc-mac 会话密钥按指定模式计算数据块的 MAC，输出；

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	G5
MAC 算法模式	2 H	用于指定 Sc-mac 产生报文 C-MAC 时采用的算法模式 01 - ISO9797-1 模式 1，即 Full Triple DES MAC 03 - ISO9797-1 模式 3，即 Single Des Final Triple Des MAC
KMC 源密钥	K + 4N / 16 H / 1A + 32H / 1A + 48H	用于计算报文 C-MAC 的源密钥(发行商 KMC)索引或密文
密钥派生数据	12 H	由 6 字节 KMCID 和 4 字节芯片序号（CSN）组成，该域取 6 个最低有效字节 用于分散产生卡片 Kmac
卡序列计数器（SCP02）	4 H	用于产生 Sc-mac 会话密钥：Kmac 3DES-CBC 加密[‘0101’+2 字节 Counter+12 个’00’]
输入数据长度	4 H	要计算 C-MAC 的报文数据的长度 取值 0000-03D8（即 0-984 字节）

输入数据	n*2 H	用于产生 C-MAC 的 APDU 命令报文，包含命令头（CLA+INS+P1+P2+Lc）和命令的数据域。
PAD 标识	2 H	标识运算前数据的填充规则 取值范围：00－05，详细规则参见 4.1
ICV 使用模式	1 H	0 － 直接使用 ICV 域参与 MAC 运算 1 － 使用 Sc-mac 左 8 字节加密 ICV 域后参与 MAC 运算
ICV	16 H	8 字节初始化向量。
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	G6
错误码	2 A	00：成功 04：非法的密钥类型 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 26：非法的密钥标识(或不支持的算法) 32：非法的 ICV 使用模式 34：非法的 MAC 算法模式 36：非法的分散级数 39：非法的数据填充方式 41：无主密钥或加密卡运算单元错误 45：密钥不存在 80：非法的数据长度
MAC 值	16 H	输出的 MAC 值

示例 1. 发行商 KMC 计算一段数据的 MAC

```
[
G5
01
X5A03495FDD7B5BCA565ABAD9403B8B4E
1122334455660102
001A
000102030405060708090A0B0C0D0E0F10111213141516171819
01
0
0102030405060708
|
G6
00
C8942F0B18BEADCC
]
```

3.3.2.6. KMC(Srmac)验证数据 R-MAC（G6）

发行商 KMC（使用 Sr-mac 会话密钥）验证数据的 MAC。通常用于在需要完整性安全报文的 APDU 命令中对应答数据验证 R-MAC。

1. 使用发行商 KMC，根据 IC 卡的密钥数据（keydata，由 KMCID 和芯片序号（CSN）组成，共 10 字节的最右 6 字节）分散产生卡片发行商 Kmac，再根据会话密钥因子['0102'||2 字节计数器||12 个'00']生成厂商 Sr-mac 会话密钥。

2. 使用 Sr-mac 会话密钥按指定模式计算填充后的数据块的 MAC，与输入的 MAC 值比对，输出验证结果；

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	G6
MAC 算法模式	2 H	用于指定 Sr-mac 产生报文 R-MAC 时采用的算法模式 01 – ISO9797-1 模式 1，即 Full Triple DES MAC 03 – ISO9797-1 模式 3，即 Single Des Final Triple Des MAC
KMC 源密钥	K + 4N / 16 H / 1A + 32H / 1A + 48H	用于计算报文 R-MAC 的源密钥(发行商 KMC)索引或密文
密钥派生数据	12 H	由 6 字节 KMCID 和 4 字节芯片序号（CSN）组成，该域取 6 个最低有效字节 用于分散产生卡片 Kmac
卡序列计数器（SCP02）	4 H	用于由 Kmac 产生 Sr-mac 会话密钥：Kmac 3DES-CBC 加密[‘0102’+2 字节 Counter+12 个’00’]
输入数据长度	4 H	要验证 R-MAC 的报文数据的长度 取值 0000-03D8（即 0-984 字节）
输入数据	n*2 H	用于验证 R-MAC 的 APDU 应答报文
PAD 标识	2 H	标识运算前数据的填充规则 取值范围：00－05，详细规则参见 4.1
ICV 使用模式	1 H	0 – 直接使用 ICV 域参与 MAC 运算 1 – 使用 Smac 左 8 字节加密 ICV 域后参与 MAC 运算
ICV	16 H	8 字节初始化向量
待验证的 MAC	16 H	待验证的应答报文 R-MAC，验证时忽略大小写
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	G7
错误码	2 A	00：成功 01：MAC 验证失败 04：非法的密钥类型 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 26：非法的密钥标识(或不支持的算法) 32：非法的 ICV 使用模式 34：非法的 MAC 算法模式 36：非法的分散级数 39：非法的数据填充方式 41：无主密钥或加密卡运算单元错误 45：密钥不存在 80：非法的数据长度
R-MAC 值	16 H	可选域；仅当错误码为 01（验证失败）时存在 HSM 重新计算出的 R-MAC 值

3.3.2.7. 外部认证（G7）

适用于卡片与外部实体初始化安全通道时的双向认证，外部实体通过调用 HSM 来完成对卡片的认证工作。

双向认证过程：

1. 终端向卡发起 INITIALIZE UPDATE 命令，并送入一个 8 字节终端随机数，SCP02 卡片返回 [10 字节密钥派生数据+2 字节密钥信息+2 字节计数器+6 字节卡随机数+8 字节卡片认证密文] ；
2. 终端调用 HSM 完成认证密文的计算：
   1) 使用发行商 KMC，根据 IC 卡的密钥数据（keydata，由 KMCID 和芯片序号（CSN）组成，共 10 字节的最右 6 字节）分散产生卡片发行商 Kenc，再根据会话密钥因子['0182'||2 字节计数器||12 个'00']生成厂商 Senc 会话密钥。
   2) 组数据包 [8 字节终端随机数 || 2 字节计数器 || 6 字节卡随机数 || 8000000000000000]，使用 Senc 会话密钥对数据包做全 CBC MAC，得 8 字节密文，与 IC 卡返回的 8 字节卡片认证密文比对，一致则通过对卡的认证；
   3) 另组数据包 [2 字节计数器 || 6 字节卡随机数 || 8 字节终端随机数 || 8000000000000000]，使用 Senc 会话密钥对数据包做全 CBC MAC，得 8 字节密文作为终端认证密文输出；
3. 终端将 HSM 返回的认证密文通过 EXTERNAL AUTHENTICATE 命令送给卡片，进行卡对终端的认证。完成卡与终端的双向认证。

其中的步骤 2 的过程，为本指令提供的密码运算功能。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	G7
KMC 源密钥	K + 4N / 16 H / 1A + 32H / 1A + 48H	用于进行外部认证的源密钥(发行商 KMC)索引或密文
密钥派生数据	12 H	由 6 字节 KMCID 和 4 字节芯片序号（CSN）组成，该域取 6 个最低有效字节 用于分散产生卡片 Kenc
Host Challenge	16 H	8 字节终端随机数
Card Challenge	16 H	对 SCP02，该域为 2 字节计数器+6 字节卡片随机数
卡片认证密文	16 H	8 字节卡片认证密文，用于主机对卡片的认证
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	G8
错误码	2 A	00：成功 01：卡片认证失败 04：非法的密钥类型 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 26：非法的密钥标识(或不支持的算法)

		36：非法的分散级数 41：无主密钥或加密卡运算单元错误 45：密钥不存在
主机认证密文	16 H	主机认证密文 用于在 EXTERNAL AUTHENTICATE 命令中传送给卡片，以验证 Host 身份

示例 1.

```
[
G7
XFB1EBAD4D27986591CDD805C09C6E5AC
010203040506
0102030405060708
00010A0B0C0D0E0F
58031BFBC8D51290
|
G8
00
F1D7E2C5A67B41F2
]
```

3.3.2.8. 保护密钥加密导出 KMC 三条会话密钥（G8）

适用于远程发卡系统，该系统向 IC 卡加载新的应用。

KMC 存储于总行或总中心的密码机内，发卡系统部署于分行或分支机构，分行要对卡片增加一项业务应用时，发卡系统先对卡片进行外部认证，通过后再将应用 applet 加密并计算 MAC，然后灌装给卡片，加密和计算 MAC 的密钥为卡片 KMC 的会话密钥（Senc/Smac/Sdek）。

本指令用于从总行导出 KMC 的三条会话密钥，由传输密钥加密保护，该传输密钥是分行与总行共享的一条密钥加密密钥。在进行加密或 MAC 运算前需使用 SI 指令导入成本地应用密钥的形式方可使用。

说明，本指令输出的 S_{MAC} 为计算 C-MAC 的会话密钥。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	G8
加密算法模式	2 H	标识保护密钥加密三条会话密钥时的算法模式 00 - ECB 01 - CBC
保护密钥类型	3 H	用于加密保护三条会话密钥的源密钥类型 000 - KEK; 109 - MDK;
保护密钥	K + 4N / 1A + 16 H / 1A + 32H / 1A + 48H	用于加密保护三条会话密钥的密钥索引或密文
保护密钥分散级数	2 H	分散级数。取值 00 - 03
保护密钥分散因子	n*32 H	n 个分散因子的串联。每个分散因子必须为 16 个字节
保护密钥的会话密	2 H	保护密钥的会话密钥的产生模式：

钥产生模式		00 - 不产生会话密钥; 01 - ECB 模式加密 8 字节会话密钥因子，得 8 字节会话密钥; 02 - ECB 模式加密 16 字节会话密钥因子，得 16 字节会话密钥; 03 - 密钥的左右 8 字节异或，得 8 字节会话密钥; 04 - 取密钥的左 8 字节做为会话密钥; 05 - CBC 模式加密 16 字节会话密钥因子，得 16 字节会话密钥;
保护密钥的会话密钥因子	16 H / 32 H	仅当保护密钥的会话密钥模式取值为 01/02/05 时存在 会话密钥模式为 01 时，该域为 8 字节（16H），适用于产生 PBOC 规范的单长度会话密钥，取值：6 字节 0x00||2 字节 ATC; 会话密钥模式为 02 时，该域为 16 字节（32H），适用于产生 PBOC 规范的双长度会话密钥，取值：6 字节 0x00||2 字节 ATC||6 字节 0x00||2 字节 ATC 的非; 会话密钥模式为 05 时，该域为 16 字节（32H），适用于产生 GP 规范 SCP02 的卡片会话密钥，取值：2 字节密钥类型||2 字节卡计数器||12 字节 0x00;
导出密钥(KMC)	K + 4N / 16 H / 1A + 32H / 1A + 48H	被导出 KMC 的密钥索引或密文
卡片个人化密钥数据 keydata	6*2 H	由 6 字节 KMCID 和 4 字节芯片序号（CSN）组成，该域取 6 个最低有效字节 用于分散产生 Kenc/Kmac/Kdek
卡片计数器	4 H	用于计算卡片三条会话密钥的计数器，2 字节
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	G9
错误码	2 A	00：成功 03：非法的加密算法模式 04：非法的密钥类型(或与索引中密钥类型不一致) 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 26：非法的密钥标识(或不支持的算法) 36：非法的分散级数 37：非法的会话密钥产生模式 41：无主密钥或加密卡运算单元错误 45：密钥不存在
Senc 密文	32 H	保护密钥加密的 Senc 密文
Senc 校验值	16 H	Senc 密钥校验值
Scmac 密文	32 H	保护密钥加密的 Scmac 密文
Scmac 校验值	16 H	Smac 密钥校验值
Sdek 密文	32 H	保护密钥加密的 Sdek 密文
Sdek 校验值	16 H	Sdek 密钥校验值

示例 1.

[
G8
00
109

```
X84BE3F9DF32844D77B60C89583EBC6B2
01
1122334455667788EEDDCCBBAA998877
00
XFB1EBAD4D27986591CDD805C09C6E5AC
010203040506
0001
|
G9
00
07C7E7147DF762BFB0D1B6E3DBD801F5
0538C166860F5816
81E2131A3EB344D643049708BBD2A4B7
8AA732A023548296
F5A75BFBF6A96F3375243F7FA50BB63A
9AEA571D43E52A0B
]
```

3.3.2.9. KMC(Sdek)保护导出一对 RSA 密钥（GF）

发行商 KMC（使用 Sdek 会话密钥）加密导出一对 RSA 密钥，输出公钥明文和 Sdek 加密的各私钥分量密文，用于向 IC 卡发行灌装。如需形成安全报文模式另行使用 KMC 加密数据指令和 KMC 计算 MAC 指令。

Sdek 加密 RSA 密钥的各私钥分量时，先采用填充模式 1 填充后再加密。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	GF
加密算法模式	2 H	00 - ECB 01 - CBC
保护密钥（KMC）	K + 4N / 16 H / 1A + 32H / 1A + 48H	用于加密保护 RSA 密钥的 KMC 密钥索引或密文
密钥派生数据	12 H	由 6 字节 KMCID 和 4 字节芯片序号（CSN）组成，该域取 6 个最低有效字节 用于分散产生卡片 Kdek
卡序列计数器	4 H	用于由Kdek产生Sdek会话密钥：Kdek 3DES-CBC加密[‘0181’+2字节Counter+12个’00’]
RSA 密钥索引标识	1 A	可选域： • 取值’K’，表明下个域为 4N 模式 • 此项为空（没有任何数据），下个域为 2N 模式
RSA 密钥索引号	2 N / 4 N	RSA 公钥在密码机内存储的索引号。取值：1 - 64；99（2N 模式）或 9999（4N 模式）标识私钥使用下面域的值。
私钥长度	4 N	可选域，仅当密钥索引为‘99’or ‘9999’时存在 私钥数据的长度，字节数
私钥数据	n B	可选域，仅当密钥索引为‘99’ or ‘9999’时存在 LMK 加密的私钥（包括 m, e, d 和 5 个 CRT 成份）

响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	GG
错误码	2 A	00：成功 03：非法的加密算法模式 04：非法的密钥类型(或与索引中密钥类型不一致) 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的 KMC 密钥索引 26：非法的密钥标识(或不支持的算法) 36：非法的分散级数 41：无主密钥或加密卡运算单元错误 45：密钥不存在 55：非法的 RSA 密钥索引 57：非法的 RSA 密钥对
公钥	n B	公钥， ASN.1 格式 DER 编码（模，指数序列）
私钥指数 d 长度	4 N	私钥指数 d 密文长度，字节数
私钥指数 d	n B	私钥指数 d 密文
私钥分量 P 长度	4 N	私钥分量 p 密文长度，字节数
私钥分量 P	n B	私钥分量 p 密文
私钥分量 Q 长度	4 N	私钥分量 q 密文长度，字节数
私钥分量 Q	n B	私钥分量 q 密文
私钥分量 dP 长度	4 N	私钥分量 dP 密文长度，字节数
私钥分量 dP	n B	私钥分量 dP 密文
私钥分量 dQ 长度	4 N	私钥分量 dQ 密文长度，字节数
私钥分量 dQ	n B	私钥分量 dQ 密文
私钥分量 qInv 长度	4 N	私钥分量 qInv 密文长度，字节数
私钥分量 qInv	n B	私钥分量 qInv 密文

3.3.2.10. KMC(Sdek)保护导出一对 SM2 密钥（G0）

发行商 KMC（生成 Sdek 会话密钥）加密导出一对 SM2 密钥，输出公钥明文和 Sdek 加密的私钥分量 d 密文，用于向 IC 卡发行灌装。如需形成安全报文模式另行使用 KMC 加密数据指令和 KMC 计算 MAC 指令。

Sdek 加密 SM2 私钥 d 分量时，先采用填充模式 1 填充后再加密。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	G0
加密算法模式	2 H	00 - ECB 01 - CBC
保护密钥（KMC）	K + 4N / 16 H / 1A + 32H / 1A + 48H	用于加密保护 SM2 密钥对的 KMC 密钥索引或密文
密钥派生数据	12 H	由 6 字节 KMCID 和 4 字节芯片序号（CSN）组成，该域取 6 个最低有效字节 用于分散产生卡片 Kdek

卡序列计数器	4 H	用于由 Kdek 产生 Sdek 会话密钥：Kdek 3DES-CBC 加密[‘0181’+2 字节 Counter+12 个’00’]
曲线标识	2 N	07 - 国密-256 新曲线，SM2
SM2 密钥索引号	4 N	SM2 密钥索引号 0001 - 0064，标识密码机内的密钥索引位置； 9999 标识密钥使用下面域的值。
SM2 公钥	n B	可选域，仅当密钥索引为‘9999’时存在该域 公钥， ASN.1 格式 DER 编码（公钥 x、y 序列）
SM2 私钥密文长度	4 N	可选域，仅当密钥索引为‘9999’时存在该域 私钥数据的长度，字节数
SM2 私钥密文	n B	可选域，仅当密钥索引为‘9999’时存在该域 LMK 加密的私钥密文
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	G1
错误码	2 A	00：成功 03：非法的加密算法模式 04：非法的密钥类型(或与索引中密钥类型不一致) 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的 KMC 密钥索引 26：非法的密钥标识(或不支持的算法) 36：非法的分散级数 41：无主密钥或加密卡运算单元错误 45：密钥不存在 55：非法的 SM2 密钥索引 57：非法的 SM2 密钥对 58：非法的曲线标识
公钥	n B	公钥， ASN.1 格式 DER 编码（公钥 x、y 序列）
私钥 d 密文长度	4 N	Sdek 加密的私钥分量 d 密文长度，字节数
私钥 d 密文	n B	Sdek 加密的私钥分量 d 密文

3.3.2.11. TK 加密的 PIN 密文转为 KMC(Sdek)下加密（GD）

发卡系统接收到 DP 发来的 TK 加密的 PIN 密文，转换到发行商 KMC（使用 Sdek 会话密钥）下加密，输出数据密文，用于向 IC 卡发行灌装。

该指令支持 PINBLOCK 格式的转换。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	GD
源密钥类型	3 H	用于加密 PINBLOCK 的源密钥类型 000 - KEK; 00A - ZEK/DEK; 00B - TEK;
源密钥	K + 4 N / 16 H / 1 A + 32 H /	用于加密 PINBLOCK 的源密钥索引或密文

	1 A + 48 H / 1 A + 64 H	
目的 KMC 密钥	K + 4 N / 16 H / 1 A + 32 H / 1 A + 48 H	用于加密 PINBLOCK 的目的主密钥（IMK）索引或密文
密钥派生数据	12 H	由 6 字节 KMCID 和 4 字节芯片序号（CSN）组成，该域取 6 个最低有效字节 用于分散产生卡片 Kdek。
卡序列计数器（SCP02）	4 H	用于由 Kdek 产生 Sdek 会话密钥：Kdek 3DES-CBC 加密［‘0181’ +2 字节 Counter+12 个’ 00’ ］
源 PINBLOCK 密文	16 H / 32 H	在源密钥下加密的 PINBLOCK 密文 源密钥方案为 R/P/L/M/N 时该域为 32H，否则 16H
源 PINBLOCK 格式	2 N	源密钥下加密 PIN 数据块的格式代码，参见 5 PINBLOCK(数字)格式
源账号	12 N / 18 N	用户主账号 当源 PIN 数据块格式为 04 时，该域为 18N，去除校验位的 18 位主账号，不足 18 位则右对齐左填 F； 当源 PIN 数据块格式为其他值时，该域为 12N，去除校验位的最右 12 位主账号；
目标 PINBLOCK 格式	2 N	目标密钥下加密 PIN 数据块的格式代码，参见 5 PINBLOCK(数字)格式
目标账号	12 N / 18 N	用户主账号 当目标 PIN 数据块格式为 04 时，该域为 18N，去除校验位的 18 位主账号，不足 18 位则右对齐左填 F； 当 PIN 数据块格式为其他值时，该域为 12N，去除校验位的最右 12 位主账号；
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	GE
错误码	2 A	00：成功 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 20：PIN 数据块没有包含有效的值 21：非法的密钥索引 22：无效的账号 23：非法的 PIN BLOCK 格式 24：非法的 PIN 长度 41：无主密钥或加密卡运算单元错误 45：密钥不存在
目标 PINBLOCK 密文	16 H	在目标密钥下加密的 PINBLOCK 密文

3.3.3. PBOC/EMV 规范交易功能

3.3.3.1. PBOC 验证 ARQC/TC/AAC，可选的产生 ARPC（K6）

验证一个 ARQC(or TC/ACC),并且可选的产生一个 ARPC。该指令也可以用做单独产生 ARPC。

若验证 ARQC，则填充交易数据（填充模式采用 4.1.2 模式 1）后，使用会话密钥 SDK 计算其 ARQC 值，与输入的 ARQC 对比，若失败则输出诊断数据；

当 MDK 源密钥为 DES/3DES 算法时，依 PBOC2.0 规范，ARQC 为交易数据的 8 字节 MAC 值；

当 MDK 源密钥为 AES/SM1 算法时，依 PBOC2.0 规范，ARQC 为交易数据的 16 字节 MAC 值左右异或后的 8 字节结果数据；

当 MDK 源密钥为 SM4 算法时，依 PBOC3.0 规范，ARQC 为交易数据的 16 字节 MAC 值的左 8 字节数据。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**K6**
模式标志	1 H	0 - ARQC 验证 1 - ARQC 验证和 ARPC 产生 2 - 产生 ARPC
MDK 源密钥	K + 4 N / 16 H / 1 A + 16 H / 1 A + 32 H / 1 A + 48 H	用于运算的 MK-AC/MDK 源密钥索引或 LMK 下加密的密文
PAN 或 PAN 序列号	16 H	用于分散 MDK 产生卡片 UDK 的分散因子 账号+账号应用序列号取最右 16 个数字，若小于 16 个则后对齐左补’0’
ATC	4 H	ATC，2 字节。应用交易计数器 用于计算交易会话密钥
交易数据长度	2 H	仅当模式标志为 0 和 1 时存在
交易数据	2*n H	仅当模式标志为 0 和 1 时存在 用于验证 ARQC
分隔符	1 A	仅当模式标志为 0 和 1 时存在，值为’;’ 用于标识交易数据的结束
ARQC/TC/AAC	16 H	待验证的 ARQC/TC/AAC，或用于产生 ARPC
ARC	4 H	仅当模式标志为 1 和 2 时存在，用于产生 ARPC
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**K7**
错误码	2 A	00：成功 01：ARQC 验证失败 03：非法的模式标志 04：非法的密钥类型(或与索引中密钥类型不一致) 10：密钥不符合奇校验

		15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 41：无主密钥或加密卡运算单元错误 45：密钥不存在
ARPC	16 H / 32 H	产生的 ARPC 仅当模式标志为 1 和 2 时，且错误码为 00 时存在。 如密钥采用 64 分组算法，返回 8 字节 ARPC(16H)； 如密钥采用 128 分组算法，则返回 16 字节 ARPC(32H)；
ARQC 诊断数据	16 H	当模式标志为 0 或 1 时，且错误码为 01（ARQC 验证失败）时存在 输出密码机运算的 ARQC

示例 1. 3DES 算法的 MDK 密钥验证 ARQC

```
[
K6
0
X84BE3F9DF32844D77B60C89583EBC6B2
1234567890123456
0102
12
000102030405060708090a0b0c0d0e0f1011
;
EA15874CD3904B01
|
K7
00
]
```

示例 2. SM4 算法的 MDK 密钥验证 ARQC 并产生 ARPC

```
[
K6
1
R8DBD3678578715FF669C473B64EDDA3E
1234567890123456
0102
12
000102030405060708090a0b0c0d0e0f1011
;
41BFEEE7B6E7F5EB
1122
|
K7
00
661C7A1D472BCDD2A32EC0C96052B43E
]
```

3.3.3.2. PBOC 脚本加密（K2）

分散 MDK 源密钥产生卡片主密钥 UDK，根据 ATC 值计算交易会话密钥 SDK；

对输入数据进行填充（填充模式采用 4.1.1 模式 0），使用 SDK 进行加密运算，输出密文数据；

域	长度&类型	描述

命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	K2
MDK 源密钥	K + 4 N / 16 H / 1 A + 16 H / 1 A + 32 H / 1 A + 48 H	用于运算的 MK-AC/MDK 源密钥索引或 LMK 下加密的密文
PAN 或 PAN 序列号	16 H	用于分散 MDK 产生卡片 UDK 的分散因子 账号+账号应用序列号取最右 16 个数字，若小于 16 个则后对齐左补’0’
ATC	4 H	ATC，2 字节。应用交易计数器 用于计算交易会话密钥 SDK
数据长度	3 H	输入数据的长度 取值 000-3D8（即 0-984 字节）
数据	2*n H	输入的数据
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	K3
错误码	2 A	00：成功 04：非法的密钥类型(或与索引中密钥类型不一致) 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 41：无主密钥或加密卡运算单元错误 45：密钥不存在 80：非法的数据长度
加密后的数据	2*n H	加密后的数据密文

示例 1. SM4 算法的 MDK 密钥加密脚本数据

```
[
K2
R8DBD3678578715FF669C473B64EDDA3E
1234567890123456
0102
012
000102030405060708090a0b0c0d0e0f1011
|
K3
00
4BCB3AB8E66A837C78F7868353F88043224BA9C12939F8DFD4F44004D45FE576
]
```

3.3.3.3. PBOC 脚本 MAC（K4）

分散 MDK 源密钥产生卡片主密钥 UDK，根据 ATC 值计算交易会话密钥 SDK；

对输入数据进行填充（填充模式采用 4.1.2 模式 1），使用 SDK 进行 MAC 运算，输出；

当 MDK 源密钥为双长度 3DES 密钥时，采用 ISO9797-1 的 MAC 算法 3，输出 8 字节 MAC 结果；

当 MDK 源密钥为 SM1/SM4/AES 密钥时，采用 ISO9797-1 的 MAC 算法 1，输出 16 字节 MAC 结果；

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**K4**
MDK 源密钥	K + 4 N / 16 H / 1 A + 16 H / 1 A + 32 H / 1 A + 48 H	用于运算的 MK-AC/MDK 源密钥索引或 LMK 下加密的密文
PAN 或 PAN 序列号	16 H	用于分散 MDK 产生卡片 UDK 的分散因子 账号+账号应用序列号取最右 16 个数字，若小于 16 个则后对齐左补’0’
ATC	4 H	ATC，2 字节。应用交易计数器 用于计算交易会话密钥
数据长度	3 H	输入数据的长度 取值 000-3D8（即 0-984 字节）
数据	2*n H	输入的数据
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**K5**
错误码	2 A	00：成功 04：非法的密钥类型(或与索引中密钥类型不一致) 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 41：无主密钥或加密卡运算单元错误 45：密钥不存在 80：非法的数据长度
MAC	16 H / 32 H	MAC 结果数据 如密钥采用 64 分组算法，返回 8 字节 MAC 结果(16H)； 如密钥采用 128 分组算法，返回 16 字节 MAC 结果(32H)；

示例 1. SM4 算法的 MDK 密钥计算脚本 MAC

```
[
K4
R8DBD3678578715FF669C473B64EDDA3E
1234567890123456
0102
012
000102030405060708090a0b0c0d0e0f1011
|
K5
00
41BFEEE7B6E7F5EB56B854690EC83B3F
]
```

3.3.3.4. EMV4.X 验证 ARQC/TC/AAC，可选的产生 ARPC（KW）

支持 EMV2000 规范和 PBOC2.0 规范。

该指令目前版本仅支持 DES/3DES 算法。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**KW**
模式标志	1 H	操作模式： 0 = 仅执行 ARQC 验证 1 = 执行 ARQC 验证，和 EMV 4.1 方法一 ARPC 产生 2 = 仅执行 EMV 4.1 方法一 ARPC 产生 3 = 执行 ARQC 验证，和 EMV 4.1 方法二 ARPC 产生 4 = 仅执行 EMV 4.1 方法二 ARPC 产生
方案 ID	1 N	指定密钥离散方案 0 = VIS1.4.0 或 M/Chip4 使用 EMV4.1 卡密钥离散方法 A 及 EMV2000 会话密钥离散方式 1 = VIS1.4.0 或 M/Chip4 使用 EMV4.1 卡密钥离散方法 B 及 EMV2000 会话密钥离散方式 2 = VIS1.4.0 或 M/Chip4 使用 EMV4.1 卡密钥离散方法 A 及 EMV 通用会话密钥离散方式 3 = VIS1.4.0 或 M/Chip4 使用 EMV4.1 卡密钥离散方法 B 及 EMV 通用会话密钥离散方式 9 = PBOC2.0
*MK-AC	K + 4 N / 1 A + 32 H	发行商的应用主密钥索引或密文
IV-AC	16 B	仅当 “方案 ID”为 0 或 1 时存在 用于离散产生卡片会话密钥的初始向量（EMV2000 过程密钥离散方式使用）
PAN/PAN 序列号长度	2 N	仅当 “方案 ID”为 1 或 3 时存在 范围值为 08-99
PAN/PAN 序列号	8 B / n B	离散卡片密钥使用的帐号或者帐号序列号，该数据的填充由应用完成。 当“方案 ID”为 1 或 37 时，为“PAN/PAN 序列号长度”标识的长度。
分隔符	1 A	仅当“方案 ID”为 1 或 3 时存在 值为 ‘;’
B/H 参数	1 N	仅当“方案 ID”为 0 或 1 时存在 分支因子和数高参数，用于产生会话密钥（EMV2000 过程密钥离散方式使用） 0 = B 为 2，H 为 16 1 = B 为 4，H 为 8
ATC	2 B	用于产生会话密钥
交易数据长度	2 H	仅当“模式标志”为 0、1 或 3 时存在 用于计算 ARQC 的明文数据长度(1-255)
交易数据	n B	仅当“模式标志”为 0、1 或 3 时存在 用于计算 ARQC 的明文数据
分隔符	1 A	值为“;”
ARQC/TC/AAC	8 B	待验证的应用密文 ARQC/TC/AAC，以及用于 ARPC 的计算
ARC	2 B	仅当“模式标志”为 1 或 2 时存在 认证应答码，用于计算 ARQC

CSU	4 B	仅当“模式标志”为 3 或 4 时存在 卡状态更新值，用于计算 ARPC
认证数据长度	1 N	仅当“模式标志”为 3 或 4 时存在 值为 0-8
认证数据	n B	仅当“模式标志”为 3 或 4 时存在 专有的认证数据，用于计算 ARPC
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	KX
错误码	2 A	00：无错误 01：ARQC/TC/AAC 校验失败 04：模式标志错或密钥类型非法 05：未定义的方案 ID 10：MK-AC 奇偶校验错 12：用户存储区没有装载密钥 13：LMK 错误 15：输入数据错。 52：非法的 B/H 选择 80：数据长度错 81：PAN 长度错。
ARPC	8 B	仅当“模式标志”为 1、2、3 或 4，且错误码为 00 时存在 产生的 ARPC
重新加密的密文数据	8 B	仅当“模式标志”为 0 和 1，且错误代码为“01”时存在 加密机计算的 ARQC/TC/ACC 值，供诊断调试使用

示例 1.

使用 EMV4.1 卡密钥离散方法 A 及 EMV 通用会话密钥离散方式，验证 ARQC 并产生 ARPC（方法一）

```
[
KW
1
2
X1FE96E4D04066C3A842D970B0F7BAB4A
&1234567890123456!
&0102!
10
&00112233445566778899AABBCCDDEEFF!
;
& CA52FF1DCAE99C81 !
& 1122 !
|
KX
00
& D8FE8F511C05B681 !
]
```

3.3.3.5. EMV4.X 脚本安全报文 / PIN 修改（KY）

为发卡行到卡片产生一个包含 MAC 的安全信息，并且可选地包含加密数据以及用在 PIN CHANGE 功能中的 PIN 密文。安全报文中的密文信息的输入形式也是被其他密钥加密的，本命令将完成密钥的转换工作，另外对于 PIN 还包括 PINBLOCK 格式的转换。

万事达规范 PINBLOCK 填充密钥使用应用认证密钥（MK-AC）的子密钥，但是 PBOC 标准定义的可能使用的是离散 PIN 加密的子密钥，本指令现在均使用 VISA 标准计算。

该指令目前版本仅支持 DES/3DES 算法。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**KY**
模式标志	1 H	操作模式： 0 = 仅计算 MAC（使用 EMV4.1 卡密钥离散方法 A 及 EMV2000 会话密钥离散方式） 2 = MAC 计算和数据加密 4 = MAC 计算和 PIN CHANGE 5 = 仅计算 MAC（使用方案 ID 指定算法）
方案 ID	1 N	仅当“模式标志”为 2、4 或 5 时存在 指定密钥离散及加密方案 0 = VIS1.4.0 使用 EMV4.1 卡密钥离散方法 A 及 EMV2000 会话密钥离散方式（与模式标志 0 相同） 1 = M/Chip 4 使用 EMV4.1 卡密钥离散方法 A 及 EMV2000 会话密钥离散方式 4 = CCD 使用 EMV4.1 卡密钥离散方法 B 及 EMV2000 会话密钥离散方式 5 = VIS1.4.0 使用 EMV4.1 卡密钥离散方法 A 及 EMV 通用会话密钥离散方式 6 = M/Chip 4 使用 EMV4.1 卡密钥离散方法 A 及 EMV 通用会话密钥离散方式 7 = CCD 使用 EMV4.1 卡密钥离散方法 B 及 EMV 通用会话密钥离散方式 9 = PBOC2.0
*MK-SMI	K + 4 N / 1 A + 32 H	用于计算 MAC 的主密钥索引或密文
IV-SMI	16 B	仅当“模式标志”为 0，或“方案 ID”为 0、1 或 4 时存在 用于离散产生 MAC 计算的卡片会话密钥的初始向量（EMV2000 过程密钥离散方式使用）
PAN/PAN 序列号长度	2 N	仅当 “方案 ID”为 4 或 7 时存在 范围值为 08-99
PAN/PAN 序列号	8 B / n B	离散卡片密钥使用的帐号或者帐号序列号，该数据的填充由应用完成。 当“方案 ID”为 4 或 7 时，为“PAN/PAN 序列号长度”标识的长度。
分隔符	1 A	仅当“方案 ID”为 4 或 7 时存在 值为 ‘;’
B/H 参数	1 N	仅当“模式标志”为 0 或 “方案 ID”为 0、1、或 4 时存在 分支因子和数高参数，用于产生会话密钥 0 = B 为 2，H 为 16 1 = B 为 4，H 为 8
ATC	2 B	仅当“模式标志”为 0 或 “方案 ID”为 0、1、4 或 9 时存在 应用交易序号 用于按 EMV2000 和 PBOC 会话密钥离散方式产生会话密钥
AC	8 B	仅当“方案 ID”为 5、6 或 7 时存在 应用密文 用于按 EMV 通用会话密钥离散方式产生会话密钥

明文数据长度	4 H	用于参与 MAC 计算的明文数据长度 取值 0000-03D8（即 0-984 字节）
明文数据	n B	用于参与 MAC 计算的明文数据
分隔符	1 A	值为“;”
*MK-SMC	K + 4 N / 1 A + 32 H	仅当“模式标志”为 2 或 4 时存在 用于加密计算的主密钥索引或密文
IV-SMC	16 B	仅当“模式标志”为 2 或 4，且“方案 ID”为 0、1 和 4 时存在 用于离散产生加密计算的卡片会话密钥的初始数据（EMV2000 会话密钥离散方式使用）
TK（ZEK/DEK）	K + 4 N / 1 A + 32 H	仅当“模式标志”为 2 时存在 输入的密文数据的源加密密钥的索引或密文
偏移量	4 H	仅当“模式标志”为 2 或 4 时存在 在计算 MAC 时，将 MK-SMC 卡片会话密钥加密的密文数据插入到参与 MAC 计算的明文数据的位置
密文数据长度	4 H	仅当“模式标志”为 2 或 4 时存在 TK 加密的密文数据或 ZPK/TPK 加密的 PINBLOCK 密文的长度
密文数据	n B	仅当“模式标志”为 2 或 4 时存在 TK 加密的密文数据或 ZPK/TPK 加密的 PINBLOCK 密文 TK 加密的数据将不做任何改变的转换到 MK-SMC 卡片过程密钥下加密 目的 PINBLOCK 格式为 42 时，该域由当前 PIN 密文右边连接新 PIN 密文组成
分隔符	1 A	仅当“模式标志”为 2 或 4 时存在 值为“;”
源 PIN 加密密钥类型	1 N	仅当“模式标志”为 4 时存在 0=ZPK；1=TPK
源 PIN 加密密钥	K + 4 N / 1 A + 32 H	仅当“模式标志”为 4 时存在 源 PIN 加密密钥的索引或密文
源PINBLOCK格式	2 N	仅当“模式标志”为 4 时存在，格式参见 5 PINBLOCK(数字)格式
目的 PINBLOCK 格式	2 N	仅当“模式标志”为 4 时存在 指定 MK-SMC 会话密钥加密 PIN 块时的格式 34 = 标准 EMV 格式 35 = Mastercard 格式 41 = VISA/PBOC 不使用当前 PIN 42 = VISA/PBOC 使用当前 PIN
帐号	12 N / 18 H	仅当“模式标志”为 4 时存在 PIN 转换中使用的帐号（不包含校验位） 当源 PINBLOCK=4 时为 18H，不足 18 位左补 F
*MK-AC	K + 4 N / 1 A + 32 H	仅当“模式标志”为 4，且目的 PINBLOCK 格式为 41 或 42 时存在 用来产生 PINBLOCK 的填充（UDK-A） 发卡行应用主密钥的索引或密文
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	KZ
错误码	2 A	00：无错误 04：模式标志错或密钥类型非法 05：未定义的方案 ID 06：非法的偏移量 07：明文数据长度错

		08：明文数据错 09：TK/ZPK/TPK 奇校验错 10：MK-SMI 奇偶校验错 11：MK-SMC 奇偶校验错 12：用户存储区没有装载密钥 13：LMK 错误 15：输入数据错。 21：存储索引错 23：PINBLOCK 格式代码错 50：源 PIN 加密密钥类型错 51：MK-AC 奇偶校验错 52：非法的 B/H 选择 80：输入密文数据长度错 81：输入密文数据长度不是 8 的倍数。
MAC	8 B	MAC 计算结果
重新加密的密文数据长度	4 H	仅当“模式标志”为 2 和 4 时存在 MK-SMC 卡片会话密钥加密的密文长度
重新加密的密文数据	n B	仅当“模式标志”为 2 和 4 时有本域； MK-SMC 卡片会话密钥加密的密文

示例 1.VIS1.4.0，使用 EMV4.1 卡密钥离散方法 A 及 EMV 通用会话密钥离散方式，计算安全报文

```
[
KY
2
5
X72DDDBE3F5B41E1361A3E01C37C30EEC
&1234567890123456!
&08D7B4FB629D0885!
0008
&0102030405060708!
;
X8A55D00FB556C20CDD9386CF4D4CC311
X8DED96D653E378689CA486167074F689
0002
0010
&D117BD6373549FAA2CA972DFFA10114D!
;
|
KZ
00
& BEA666E2AB3B6E06 !
0010
& 42AB1DB61409843F9080474393142360 !
]
```

3.3.3.6. PBOC 脱机 PIN 修改/加密（KX）

密钥分散并计算会话密钥后，按 PINBLOCK 格式加密 PIN，用于卡片重置脱机 PIN。

当前版本支持 PBOC3.0 规范的密钥分散和会话密钥离散方式，支持 DES/3DES、AES 及

SM1/SM4 算法应用。支持输入明文 PIN 模式和密文 PIN 模式。

卡片会话密钥加密前的 PIN 块为 8 字节，采用 10 模式填充后再加密。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机。
命令代码	2 A	KX
方案 ID	1 N	指定密钥分散算法和会话密钥离散算法及填充模式的规范标识 9 - PBOC3.0
应用主密钥类型	3 H	109 - MDK/MK-AC;
应用主密钥	K + 4 N / 16 H / 1 A + 16 H / 1 A + 32 H / 1 A + 48 H / 1 A + 64 H	用于加密 PIN 块的卡应用主密钥索引或密文 该密钥按指定规范定义的算法进行分散和产生会话密钥后再加密 PIN 块
PAN 或 PAN 序列号	16 H	用于分散 MDK 产生卡片 UDK 的分散因子 账号+账号应用序列号取最右 16 个数字，若小于 16 个则后对齐左补’0’
ATC	4 H	ATC，2 字节。应用交易计数器 用于计算交易会话密钥
PINBLOCK 格式 1	2 N	指定卡片会话密钥下加密 PIN 数据块的格式代码： 34 = 标准 EMV 格式 35 = Mastercard 格式 41 = VISA/PBOC 不使用当前 PIN 42 = VISA/PBOC 使用当前 PIN
PIN 输入模式	1 N	1 - 明文 PIN 2 - ZPK 加密的密文 PIN 3 - TPK 加密的密文 PIN
明文 PIN（新）	4-12 N	可选域，仅当“PIN 输入模式”为 1 时存在
分隔符 1	1 A	可选域，仅当“PIN 输入模式”为 1 时存在 标识明文 PIN（新）域的结束，取值：;
明文 PIN（旧）	4-12 N	可选域，仅当“PIN 输入模式”为 1 且“PINBLOCK 格式 1”为 42 时存在
分隔符 2	1 A	可选域，仅当“PIN 输入模式”为 1 且“PINBLOCK 格式 1”为 42 时存在 标识明文 PIN（旧）域的结束，取值：;
源 PIN 加密密钥密钥	K + 4 N / 16 H / 1 A + 16 H / 1 A + 32 H / 1 A + 48 H / 1 A + 64 H	可选域，仅当“PIN 输入模式”不为 1 时存在 用于加密 PIN 的源 ZPK/TPK 密钥索引或密文
PINBLOCK 格式 2	2 N	可选域，仅当“PIN 输入模式”不为 1 时存在 ZPK/TPK 下加密 PIN 数据块的格式代码，参见 5 PINBLOCK(数字)格式
PIN 密文（新）	16 H / 32 H	可选域，仅当“PIN 输入模式”不为 1 时存在 在 TPK/ZPK 下加密的新 PINBLOCK 密文 密钥方案为 R/P/L/M/N 时该域为 32H，否则 16H
PIN 密文（旧）	16 H / 32 H	可选域，仅当“PIN 输入模式”不为 1 且“PINBLOCK 格式 1”为 42 时存在

		在 TPK/ZPK 下加密的旧 PINBLOCK 密文 密钥方案为 R/P/L/M/N 时该域为 32H，否则 16H
帐号	12 N / 18 H	用于参与 PINBLOCK 加密运算的帐号（不包含校验位） 当“PINBLOCK 格式 2”=4 时为 18H，不足 18 位左补 F 注意：当采用明文 PIN 输入模式且“PINBLOCK 格式 1”域取值不为 35 时，该域无效但必须存在，可输入 12 个‘0’
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**KY**
错误码	2 A	00：成功 04：非法的密钥类型或内部密钥类型不符预期 05：未定义的方案 ID 08：无效的 PIN 输入模式 15：无效的输入数据（无效的格式/字符或长度错误） 21：无效的密钥索引 23：非法的 PIN BLOCK 格式 24：非法的 PIN 长度，或 PIN 包含非法字符 45：指定索引密钥不存在 其他：参见**错误码说明**
PIN 密文长度	4 H	卡片会话密钥加密的 PIN 密文长度
PIN 密文数据	n*2 H	卡片会话密钥加密的 PIN 密文

示例 1.将 ZPK 加密的 PIN 密文（格式 01）转为卡片会话密钥下加密（格式 41）

```
[
KX
9
109
X60CE7A28F50AF3BC60CE7A28F50AF3BC
0601100000053001
0090
41
2
XC7017E70ACC013FFC7017E70ACC013FF
01
2ED2 ABDE E40B 4453
123456789012
|
KY
00
0010
04B1 5504 3D09 E9CE 38EB D1D9 14A9 82D7
]
```

3.3.4. 数据加解密运算

3.3.4.1. 数据加密（D3）

数据运算功能，可用于交易系统和发卡过程。

1. DP 系统，向发卡系统制卡数据时，使用 DEK 加密制卡文件数据；
2. DP 系统，使用与发卡系统共享的 KEK 加密二磁道信息及其他机密数据；
3. 交易系统，行业卡的外部认证，使用认证 MDK 加密随机数；
4. 交易系统，使用 MDK_enc 完成脚本加密功能；

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	D3
加密算法模式	2 H	00 - ECB 01 - CBC 02 - CFB 03 - OFB
源密钥类型	3 H	用于加密数据的源密钥类型 000 - KEK; 109 - MDK; 309 - MK-SMC; 00A - ZEK/DEK; 00B - TEK; 007 - EDK;
源密钥	K + 4 N / 16 H / 1 A + 16 H / 1 A + 32 H / 1 A + 48 H / 1 A + 64 H	用于加密数据的源密钥索引或密文
分散级数	2 H	00-08
分散因子	n*16 H	n 级分散因子串联。每级分散因子为 8 字节（16H）；
会话密钥产生模式	2 H	会话密钥的产生模式： 00 - 不产生会话密钥； 01 - ECB 模式加密 8 字节会话密钥因子[6 字节‘00’||2 字节 ATC]，得 8 字节会话密钥； 02 - ECB 模式加密 16 字节会话密钥因子[6 字节‘00’||2 字节 ATC||6 字节‘00’||2 字节 ATC 的非]，得 16 字节会话密钥； 03 - 密钥的左右 8 字节异或，得 8 字节会话密钥； 04 - 取密钥的左 8 字节做为会话密钥；
会话密钥因子	4 H	可选域，仅当会话密钥产生模式为 1 或 2 时存在 该域通常为 2 字节 ATC
PAD 标识	2 H	标识加密前数据的填充规则 取值范围：00 - 05 或 10 - 11，详细规则参见 4.1
要加密的数据长度	4 H	要加密的数据长度，字节数 取值 0000-03D8（即 0-984 字节）
要加密的数据	n*2 H	要加密的数据
IV	16 H / 32 H	可选域，仅当加密算法模式为 01/02/03 时存在 CBC 模式加密时的初始向量
响应报文		

报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	D4
错误码	2 A	00：成功 03：非法的加密算法模式 04：非法的密钥类型 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 36：非法的分散级数 37：非法的会话密钥产生方式 39：非法的数据填充方式 41：无主密钥或加密卡运算单元错误 45：密钥不存在 80：非法的数据长度
密文长度	4 H	加密后的密文长度，字节数
数据密文	n*2 H	加密后的密文

示例 1. 3DES 算法的 MDK 密钥一级分散后使用会话密钥加密 18 字节的输入数据

```
[
D3
00
109
X84BE3F9DF32844D77B60C89583EBC6B2
01
1234567890123456
02
0001
01
0012
000102030405060708090A0B0C0D0E0F 1011
|
D4
00
0018
A9CC70DBAF499B9238038E8EDA22433334D3F5A2A242D62B
]
```

3.3.4.2. 数据解密（D4）

数据运算功能，用于发卡过程。

1. 发卡系统，从 DP 接收密文的制卡文件，使用 DEK 解密；

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	D4
加密算法模式	2 H	00 - ECB 01 - CBC 02 - CFB 03 - OFB
源密钥类型	3 H	用于解密数据的源密钥类型

		00A - ZEK/DEK; 00B - TEK; 309 - MK-SMC; 007 - EDK;
源密钥	K + 4 N / 16 H / 1 A + 16 H / 1 A + 32 H / 1 A + 48 H / 1 A + 64 H	用于加密数据的源密钥索引或密文
分散级数	2 H	00-08
分散因子	n*16 H	n 级分散因子串联，每级分散因子为 8 字节（16H）；
会话密钥产生模式	2 H	会话密钥的产生模式： 00 - 不产生会话密钥； 01 - ECB 模式加密 8 字节会话密钥因子[6 字节‘00’||2 字节 ATC]，得 8 字节会话密钥； 02 - ECB 模式加密 16 字节会话密钥因子[6 字节‘00’||2 字节 ATC||6 字节‘00’||2 字节 ATC 的非]，得 16 字节会话密钥； 03 - 密钥的左右 8 字节异或，得 8 字节会话密钥； 04 - 取密钥的左 8 字节做为会话密钥；
会话密钥因子	4 H	可选域，仅当会话密钥产生模式为 1 或 2 时存在 该域通常为 2 字节 ATC
PAD 标识	2 H	标识加密前数据的填充规则 取值范围：00 - 05 或 10 - 11，详细规则参见 4.1
要解密的密文长度	4 H	要解密的密文长度，字节数 取值 0000-03E0（即 0 - 992 字节）
要解密的密文	n*2 H	要解密的密文
IV	16 H / 32 H	可选域，仅当加密算法模式为 01/02/03 时存在 CBC 模式解密时的初始向量
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	D5
错误码	2 A	00：成功 03：非法的加密算法模式 04：非法的密钥类型 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 36：非法的分散级数 37：非法的会话密钥产生方式 39：非法的数据填充方式 41：无主密钥或加密卡运算单元错误 45：密钥不存在 70：无效的密文数据，数据解密去 padding 失败 80：非法的数据长度
数据长度	4 H	解密后的数据长度，字节数
数据明文	n*2 H	解密后的数据。去掉加密时的填充字符

示例 1. 3DES 算法的 DEK 密钥一级分散后 CBC 模式解密 24 字节的输入数据

```
[
D4
01
00A
XA682B4986BB94B1B7BF87080159B12C3
```

```
01
1234567890123456
00
01
0018
C0420BF76626894D6AC2E3F046960ABF2A6F9C4942A26872
0000000000000000
|
D5
00
0012
000102030405060708090A0B0C0D0E0F1011
]
```

3.3.4.3. 数据加密 – 通用（S3）

通用的数据加密指令，分散因子为 16 字节的外部组合的数据，使用源密钥直接 ECB 模式加密该数据得到目标子密钥；会话密钥增加支持 CBC 加密会话密钥因子的模式。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	S3
加密算法模式	2 H	标识密钥加密数据时的算法模式 00 – ECB 01 – CBC 02 – CFB 03 – OFB
密钥类型	3 H	用于加密数据的源密钥类型 000 – KEK; 109 – MDK; 309 – MK-SMC; 00A – ZEK/DEK; 00B – TEK; 011 – KMC;
密钥	K + 4 N / 16 H / 1 A + 16 H / 1 A + 32 H / 1 A + 48 H / 1 A + 64 H	用于加密数据的密钥索引或密文
密钥分散级数	2 H	分散级数。取值 00 – 08
密钥分散因子	n*32 H	n 个分散因子的串联。每个分散因子必须为 16 个字节
会话密钥模式	2 H	会话密钥的产生模式： 00 – 不产生会话密钥； 01 – ECB 模式加密 8 字节会话密钥因子，得 8 字节会话密钥； 02 – ECB 模式加密 16 字节会话密钥因子，得 16 字节会话密钥； 03 – 密钥的左右 8 字节异或，得 8 字节会话密钥； 04 – 取密钥的左 8 字节做为会话密钥； 05 – CBC 模式加密 16 字节会话密钥因子，得 16 字节会话密钥；
会话密钥因子	16 H / 32 H	仅当会话密钥模式取值为 01/02/05 时存在

		• 会话密钥模式为 01 时，该域为 8 字节（16H），适用于产生 PBOC 规范的单长度会话密钥，仅限 3DES 算法的密钥。取值：6 字节 0x00||2 字节 ATC； • 会话密钥模式为 02 时，该域为 16 字节（32H），适用于产生 PBOC 规范的双长度会话密钥，取值：6 字节 0x00||2 字节 ATC||6 字节 0x00||2 字节 ATC 的非； • 会话密钥模式为 05 时，该域为 16 字节（32H），适用于产生 GP 规范 SCP02 的卡片会话密钥，取值：2 字节密钥类型||2 字节卡计数器||12 字节 0x00；
PAD 标识	2 H	标识加密前数据的填充规则 取值范围：00 - 05 或 10 - 11，详细规则参见 4.1
输入数据长度	4 H	下个域的长度，字节数 取值 0000-07B0（即 0-1968 字节）
输入数据	n B	待加密的数据
IV	16 H / 32 H	仅当加密算法模式为 01/02/03 时存在。 若密钥算法为 128 分组，该域为 16 字节（32H）； 若密钥算法为 64 分组，该域为 8 字节（16H）；
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	S4
错误码	2 A	00：成功 03：非法的加密算法模式 04：非法的密钥类型 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 36：非法的分散级数 37：非法的会话密钥产生方式 39：非法的数据填充方式 41：无主密钥或加密卡运算单元错误 45：密钥不存在 80：非法的数据长度
密文长度	4 H	数据密文长度
密文	n B	数据块密文

示例 1. SM4 算法的 MDK 密钥 CBC 模式直接加密 26 字节的输入数据

```
[
S3
01
109
R8DBD3678578715FF669C473B64EDDA3E
00
00
01
001a
abcdefghijklmnopqrstuvwxyz
00000000000000000000000000000000
|
S4
00
0020
```

& 44B9F99E1C81FCCD910DFD8EADF1BF2538D1262236418D463919AB603B54D80A !
]
‘&’与‘!’之间的字符为扩展 16 进制字符数据；

3.3.4.4. 数据解密 – 通用（S4）

通用的数据解密指令，分散因子为 16 字节的外部组合的数据，使用源密钥直接 ECB 模式加密该数据得到目标子密钥；会话密钥增加支持 CBC 加密的模式。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	S4
解密算法模式	2 H	标识密钥解密数据时的算法模式 00 – ECB 01 – CBC 02 – CFB 03 – OFB
密钥类型	3 H	用于解密数据的源密钥类型 309 – MK-SMC; 00A – ZEK/DEK; 00B – TEK;
密钥	K + 4 N / 16 H / 1 A + 16 H / 1 A + 32 H / 1 A + 48 H / 1 A + 64 H	用于解密数据的密钥索引或密文
密钥分散级数	2 H	分散级数。取值 00 – 08。
密钥分散因子	n*32 H	n 个分散因子的串联。每个分散因子必须为 16 个字节。
会话密钥模式	2 H	会话密钥的产生模式： 00 – 不产生会话密钥； 01 – ECB 模式加密 8 字节会话密钥因子，得 8 字节会话密钥； 02 – ECB 模式加密 16 字节会话密钥因子，得 16 字节会话密钥； 03 – 密钥的左右 8 字节异或，得 8 字节会话密钥； 04 – 取密钥的左 8 字节做为会话密钥； 05 – CBC 模式加密 16 字节会话密钥因子，得 16 字节会话密钥；
会话密钥因子	16 H / 32 H	仅当会话密钥模式取值为 01/02/05 时存在 • 会话密钥模式为 01 时，该域为 8 字节（16H），适用于产生 PBOC 规范的单长度会话密钥，取值：6 字节 0x00||2 字节 ATC； • 会话密钥模式为 02 时，该域为 16 字节（32H），适用于产生 PBOC 规范的双长度会话密钥，取值：6 字节 0x00||2 字节 ATC||6 字节 0x00||2 字节 ATC 的非； • 会话密钥模式为 05 时，该域为 16 字节（32H），适用于产生 GP 规范 SCP02 的卡片会话密钥，取值：2 字节密钥类型||2 字节卡计数器||12 字节 0x00；
PAD 标识	2 H	标识加密前数据的填充规则 取值范围：00 – 05 或 10 – 11，详细规则参见 4.1

输入数据长度	4 H	下个域的长度，字节数 取值 0000-07C0（即 0 - 1984 字节）
输入数据	n B	待解密的数据
IV	16 H / 32 H	仅当加密算法模式为 01/02/03 时存在。 若密钥算法为 128 分组，该域为 16 字节（32H）； 若密钥算法为 64 分组，该域为 8 字节（16H）；
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	S5
错误码	2 A	00：成功 03：非法的加密算法模式 04：非法的密钥类型 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 36：非法的分散级数 37：非法的会话密钥产生方式 39：非法的数据填充方式 41：无主密钥或加密卡运算单元错误 45：密钥不存在 70：无效的密文数据，数据解密去 padding 失败 80：非法的数据长度
输出数据长度	4 H	解密后的数据长度
输出数据	n B	解密后的数据明文，去除 PADDING 的结果

示例 1. SM4 算法的 ZEK 密钥 CBC 模式直接解密 32 字节的输入数据

```
[
S4
01
00A
RFA7BFEA8C36D1286879DE89861BFB86B
00
00
01
0020
& 9C23BFE8BBCDA49B5E1E0EE987719DFBBEB931DA01B061F8102EBB8E1C7A7C27 !
00000000000000000000000000000000
|
S5
00
001a
abcdefghijklmnopqrstuvwxyz
]
```

‘&’与‘!’之间的字符为扩展 16 进制字符数据，发送密码机时需转换为 BCD 码数据串，2 个字符转换成一个字节，如“9C”转换为 0x9C；

3.3.4.5. 数据转加密 – 通用（S5）

通用的转加密指令，分散因子为 16 字节的外部组合的数据，使用源密钥直接 ECB 模式加密该数据得到目标子密钥；会话密钥增加支持 CBC 加密的模式。

将源密钥 A 加密的数据密文转换到目标密钥 B 下加密，输出。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	S5
源密钥加密算法模式	2 H	标识源密钥加密数据时的算法模式 00 - ECB 01 - CBC 02 - CFB 03 - OFB
源密钥类型	3 H	用于加密数据的源密钥类型 000 - KEK; 109 - MDK; 309 - MK-SMC; 00A - ZEK/DEK; 00B - TEK; 011 - KMC;
源密钥	K + 4 N / 16 H / 1 A + 16 H / 1 A + 32 H / 1 A + 48 H / 1 A + 64 H	用于加密数据的源密钥索引或密文
源密钥分散级数	2 H	分散级数。取值 00 - 08。
源密钥分散因子	n*32 H	n 个分散因子的串联。每个分散因子必须为 16 个字节。
源密钥会话密钥模式	2 H	会话密钥的产生模式： 00 - 不产生会话密钥； 01 - ECB 模式加密 8 字节会话密钥因子，得 8 字节会话密钥； 02 - ECB 模式加密 16 字节会话密钥因子，得 16 字节会话密钥； 03 - 密钥的左右 8 字节异或，得 8 字节会话密钥； 04 - 取密钥的左 8 字节做为会话密钥； 05 - CBC 模式加密 16 字节会话密钥因子，得 16 字节会话密钥；
源密钥会话密钥因子	16 H / 32 H	仅当源密钥会话密钥模式取值为 01/02/05 时存在 • 会话密钥模式为 01 时，该域为 8 字节（16H），适用于产生 PBOC 规范的单长度会话密钥，取值：6 字节 0x00||2 字节 ATC； • 会话密钥模式为 02 时，该域为 16 字节（32H），适用于产生 PBOC 规范的双长度会话密钥，取值：6 字节 0x00||2 字节 ATC||6 字节 0x00||2 字节 ATC 的非； • 会话密钥模式为 05 时，该域为 16 字节（32H），适用于产生 GP 规范 SCP02 的卡片会话密钥，取值：2 字节密钥类型||2 字节卡计数器||12 字节 0x00；
源密钥加密时的数据 PAD 标识	2 H	标识源密钥加密前数据的填充规则 取值范围：00 - 05 或 10 - 11，详细规则参见 4.1
源密钥加密时的 IV	16 H / 32 H	可选域，仅当源密钥加密算法模式为 01/02/03 时存在。做为 CBC 加密时的初始向量。
目标密钥加密算法模式	2 H	标识目标密钥加密数据时的算法模式 00 - ECB 01 - CBC 02 - CFB 03 - OFB
目标密钥类型	3 H	用于加密数据的目标密钥类型

		000 - KEK; 109 - MDK; 309 - MK-SMC; 00A - ZEK/DEK; 00B - TEK; 011 - KMC;
目标密钥	K + 4 N / 16 H / 1 A + 16 H / 1 A + 32 H / 1 A + 48 H / 1 A + 64 H	用于加密数据的目标密钥索引或密文
目标密钥分散级数	2 H	分散级数。取值 00 - 08。
目标密钥分散因子	n*32 H	n 个分散因子的串联。每个分散因子必须为 16 个字节。
目标密钥会话密钥模式	2 H	会话密钥的产生模式： 00 - 不产生会话密钥； 01 - ECB 模式加密 8 字节会话密钥因子，得 8 字节会话密钥； 02 - ECB 模式加密 16 字节会话密钥因子，得 16 字节会话密钥； 03 - 密钥的左右 8 字节异或，得 8 字节会话密钥； 04 - 取密钥的左 8 字节做为会话密钥； 05 - CBC 模式加密 16 字节会话密钥因子，得 16 字节会话密钥；
目标密钥会话密钥因子	16 H / 32 H	仅当目标会话密钥模式取值为 01/02/05 时存在 • 会话密钥模式为 01 时，该域为 8 字节（16H），适用于产生 PBOC 规范的单长度会话密钥，取值：6 字节 0x00||2 字节 ATC； • 会话密钥模式为 02 时，该域为 16 字节（32H），适用于产生 PBOC 规范的双长度会话密钥，取值：6 字节 0x00||2 字节 ATC||6 字节 0x00||2 字节 ATC 的非； • 会话密钥模式为 05 时，该域为 16 字节（32H），适用于产生 GP 规范 SCP02 的卡片会话密钥，取值：2 字节密钥类型||2 字节卡计数器||12 字节 0x00；
目标密钥加密时的数据 PAD 标识	2 H	标识目标密钥加密前数据的填充规则 取值范围：00 - 05 或 10 - 11，详细规则参见 4.1
目标密钥加密时的 IV	16 H / 32 H	可选域，仅当目标密钥加密算法模式为 01/02/03 时存在。做为 CBC 加密时的初始向量。
密文长度	4 H	下个域的长度，字节数 取值 0000-07C0（即 0 - 1984 字节）
源密钥加密的数据密文	n B	源密钥加密的数据密文
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	S6
错误码	2 A	00：成功 03：非法的加密算法模式 04：非法的密钥类型 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 36：非法的分散级数 37：非法的会话密钥产生方式 39：非法的数据填充方式

		41：无主密钥或加密卡运算单元错误 45：密钥不存在 70：无效的密文数据，数据解密去 padding 失败 80：非法的数据长度
密文长度	4 H	数据密文长度
目标密钥加密的数据密文	n B	目标密钥加密的数据密文

示例 1. SM4 算法 MDK 密钥 CBC 模式加密的数据密文转换为 SM4 算法 DEK 密钥下 ECB 模式加密

[
S5
01
109
R8DBD3678578715FF669C473B64EDDA3E
00
00
01
00000000000000000000000000000000
00
00A
RFA7BFEA8C36D1286879DE89861BFB86B
00
00
01
0020
& 44B9F99E1C81FCCD910DFD8EADF1BF2538D1262236418D463919AB603B54D80A !
|
S6
00
0020
& 9C23BFE8BBCDA49B5E1E0EE987719DFB017C13C6DA501B25E94B8D1ED20E5847 !
]

‘&’与‘!’之间的字符为扩展 16 进制字符数据，发送密码机时需转换为 BCD 码数据串，2 个字符转换成一个字节，如“9C”转换为 0x9C；

3.3.4.6. 多个数据加解密（SW）

通用的数据加密指令，分散因子为 16 字节的外部组合的数据，使用源密钥直接 ECB 模式加密该数据得到目标子密钥；会话密钥增加支持 CBC 加密会话密钥因子的模式。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	SW
运算标识	1N	0 - 加密 1 - 解密
加密算法模式	2 H	标识密钥加密数据时的算法模式 00 - ECB 01 - CBC 02 - CFB 03 - OFB
密钥类型	3 H	用于加密数据的源密钥类型 000 - KEK; 109 - MDK; 309 - MK-SMC; 00A - ZEK/DEK; 00B - TEK; 011 - KMC;
密钥	K + 4 N / 16 H / 1 A + 16 H / 1 A + 32 H / 1 A + 48 H / 1 A + 64 H	用于加密/解密数据的密钥索引或密文
密钥分散级数	2 H	分散级数。取值 00 - 08
密钥分散因子	n*32 H	n 个分散因子的串联。每个分散因子必须为 16 个字节
会话密钥模式	2 H	会话密钥的产生模式： 00 - 不产生会话密钥； 01 - ECB 模式加密 8 字节会话密钥因子，得 8 字节会话密钥； 02 - ECB 模式加密 16 字节会话密钥因子，得 16 字节会话密钥； 03 - 密钥的左右 8 字节异或，得 8 字节会话密钥； 04 - 取密钥的左 8 字节做为会话密钥； 05 - CBC 模式加密 16 字节会话密钥因子，得 16 字节会话密钥；
会话密钥因子	16 H / 32 H	仅当会话密钥模式取值为 01/02/05 时存在 • 会话密钥模式为 01 时，该域为 8 字节（16H），适用于产生 PBOC 规范的单长度会话密钥，仅限 3DES 算法的密钥。取值：6 字节 0x00||2 字节 ATC； • 会话密钥模式为 02 时，该域为 16 字节（32H），适用于产生 PBOC 规范的双长度会话密钥，取值：6 字节 0x00||2 字节 ATC||6 字节 0x00||2 字节 ATC 的非； • 会话密钥模式为 05 时，该域为 16 字节（32H），适用于产生 GP 规范 SCP02 的卡片会话密钥，取值：2 字节密钥类型||2 字节卡计数器||12 字节 0x00；
PAD 标识	2 H	标识加密前数据的填充规则 取值范围：00 - 05 或 10 - 11，详细规则参见 4.1
待加解密的数据总数	2N	该域用于确定下面的数据输入项个数 必须大于 0，最大为 99
输入数据 D1 长度	4 H	下个域的长度，字节数

		取值 0000-1000（即 0-4096 字节）
输入数据 D1	n B	待加密/解密的数据
...	...	...
输入数据 Dn 长度	4H	下个域的长度，字节数 取值 0000-1000（即 0-4096 字节）
输入数据 Dn	nB	待加密/解密的数据
IV	16 H / 32 H	仅当加密算法模式为 01/02/03 时存在。 若密钥算法为 128 分组，该域为 16 字节（32H）； 若密钥算法为 64 分组，该域为 8 字节（16H）；
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	SX
错误码	2 A	00：成功 03：非法的加密算法模式 04：非法的密钥类型 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 36：非法的分散级数 37：非法的会话密钥产生方式 39：非法的数据填充方式 41：无主密钥或加密卡运算单元错误 45：密钥不存在 80：非法的数据长度
密文/明文长度 D1	4 H	数据密文长度或解密后的明文长度
密文/明文 D1	n B	数据块密文或去掉 padding 后的明文
...	...	...
密文/明文长度 Dn	4 H	数据密文长度或解密后的明文长度
密文/明文 Dn	n B	数据块密文或去掉 padding 后的明文

3.3.4.7. EDK 加密/解密数据-ECB 模式（50）

域	长度&类型	描述
命令报文		
报文头	m A	不做任何修改直接返回给主机
命令代码	2 A	**值为“50”。**
加解密标识	1 N	1： ECB 解密 0：ECB 加密
EDK 密钥	1 A + 48 H	LMK 对（24-25）下加密的 EDK
数据长度	4 N	要加密的数据长度，字节数=n/2。8 的倍数
要加/解密的数据	n H	要加/解密的数据
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**值为“51”。**
错误码	2 A	00：成功 04：非法的密钥类型 05：非法的标识 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 45：密钥不存在
加/解密后的数据	n H	密文或明文

3.3.4.8. EDK 加密/解密数据-CBC 模式（52）

域	长度&类型	描述
		命令报文
报文头	m A	不做任何修改直接返回给主机
命令代码	2 A	**值为“52”。**
加解密标识	1 N	1：CBC 解密（带 iv） 0：CBC 加密 （带 iv） IV 为全 0
EDK 密钥	1 A + 48 H	LMK 对（24-25）下加密的 EDK
数据长度	4 N	要加密的数据长度，字节数=n/2。8 的倍数
要加/解密的数据	n H	要加/解密的数据
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**值为“53”。**
错误码	2 A	00：成功 04：非法的密钥类型 05：非法的标识 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 45：密钥不存在
加/解密后的数据	n H	密文或明文

3.3.5. 数据 MAC 运算

3.3.5.1. 计算数据 MAC/TAC（D0）

数据运算功能，可用于交易系统和发卡过程。

1. 发卡过程中，DP->发卡，发送制卡文件时，需计算密文 MAC 以保证数据传输的完整性，使用 KEK 计算；
2. 交易系统，脚本 MAC，使用 MDK 计算；
3. 交易系统，交易数据的 MAC/TAC 的计算；

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**D0**
MAC 算法模式	2 H	01 – ISO9797-1 MAC 算法模式 1 使用 MAC 密钥 CBC 模式加密数据，取最后一段密文； 03 – ISO9797-1 MAC 算法模式 3，限密钥标识为 X/U 等同于 ANSI X9.19，MAC 密钥 16 字节，KL 对数据 DES CBC 加密运算，最后一段结果 KR DES 解密，再 KL DES 加密，得 8 字节 MAC 结果；
MAC 取值方式	2 H	按前个域模式产生的密文值输出下述结果作为 MAC：

		01-08　输出密文值的左 n 字节 10　　输出 16 字节 MAC（限密钥标识为 P/L/R） 11-18　输出密文值的右 n 字节 21-28　左右异或后取左 n 字节输出 31-38　左右异或后取右 n 字节输出 44　　四字节异或，最后输出 4 字节
源密钥类型	3 H	用于计算 MAC 的源密钥类型 109 - MDK;　209 - MK-SMI; 000 - KEK;　011 - KMC; 008 - ZAK;　003 - TAK; 007 - EDK;
源密钥	K + 4 N / 16 H / 1 A + 16 H / 1 A + 32 H / 1 A + 48 H / 1 A + 64 H	用于计算 MAC 的源密钥索引或密文
分散级数	2 H	取值 00-08。该域取值决定后面存在几个分散因子域。
分散因子	n*16 H	n 级分散因子串联，每级分散因子为 8 字节（16H）；
会话密钥产生模式	2 H	会话密钥的产生模式： 00 - 不产生会话密钥； 01 - ECB 模式加密 8 字节会话密钥因子[6 字节‘00’||2 字节 ATC]，得 8 字节会话密钥； 02 - ECB 模式加密 16 字节会话密钥因子[6 字节‘00’||2 字节 ATC||6 字节‘00’||2 字节 ATC 的非]，得 16 字节会话密钥； 03 - 密钥的左右 8 字节异或，得 8 字节会话密钥； 04 - 取密钥的左 8 字节做为会话密钥；
会话密钥因子	4 H	可选域，仅当会话密钥产生模式为 1 或 2 时存在 该域通常为 2 字节 ATC
PAD 标识	2 H	标识加密前数据的填充规则 取值范围：00 - 05 或 10 - 11，详细规则参见 4.1
数据长度	4 H	要计算 MAC 的数据长度，字节数 取值 0000-03D8（即 0 - 984 字节）
数据	n*2 H	要计算 MAC 的数据
IV	16 H / 32 H	用于计算 MAC 的初始向量 128 位分组（密钥标识 P/L/R）时，该域 16 字节（32H）； 否则该域为 8 字节（16H）；
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	D1
错误码	2 A	00：成功 04：非法的密钥类型 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 34：非法的 MAC 算法模式（或与密钥的算法标识不符） 35：非法的 MAC 取值方式 36：非法的分散级数 37：非法的会话密钥产生方式 39：非法的数据填充方式 41：无主密钥或加密卡运算单元错误 45：密钥不存在

		80：非法的数据长度
数据 MAC	n*2 H	数据 MAC 值，长度由取值标识域指定

示例 1. 3DES 算法的 KEK 密钥计算 18 字节输入数据的 MAC 值，采用 ISO9797-1 模式 3 算法

```
[
D0
03
08
000
X801617441513A2F135AB14EAAD1069DF
00
00
01
0012
000102030405060708090A0B0C0D0E0F 1011
0000000000000000
|
D1
00
70F3C90691D6F170
]
```

示例 2. SM4 算法的 ZAK 密钥分散一级的子密钥计算 18 字节输入数据的 MAC 值

```
[
D0
11
10
008
RD1F902CE578A176D848CFCD78D495E7F
01
1234567890123456
00
01
0012
000102030405060708090A0B0C0D0E0F 1011
00000000000000000000000000000000
|
D1
00
1FEAFE33C9DBE8C2E96F15702888E854
]
```

3.3.5.2. 验证数据 MAC/TAC（D1）

数据运算功能，可用于交易系统和发卡过程。

1. 发卡过程中，发卡系统收到 DP 传来的制卡文件时，需验证密文 MAC 以保证数据传输的完整性。
2. MDK 计算的 MAC 验证

域	长度&类型	描述
命令报文		

报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	D1
MAC 算法模式	2 H	01 – ISO9797-1 MAC 算法模式 1 使用 MAC 密钥 CBC 模式加密数据，取最后一段密文； 03 – ISO9797-1 MAC 算法模式 3，限密钥标识为 X/U 等同于 ANSI X9.19，MAC 密钥 16 字节，KL 对数据 DES CBC 加密运算，最后一段结果 KR DES 解密，再 KL DES 加密，得 8 字节 MAC 结果；
MAC 取值方式	2 H	按前个域模式产生的密文值按下述结果作为 MAC： 01-08 密文值的左 n 字节 10 全 16 字节 MAC（限密钥标识为 P/L/R） 11-18 密文值的右 n 字节 21-28 左右异或后取左 n 字节输出 31-38 左右异或后取右 n 字节输出 44 四字节异或，最后输出 4 字节
源密钥类型	3 H	用于计算 MAC 的源密钥类型 109 – MDK; 209 – MK-SMI; 000 – KEK; 011 – KMC; 008 – ZAK; 003 – TAK;
源密钥	K + 4 N / 16 H / 1 A + 16 H / 1 A + 32 H / 1 A + 48 H / 1 A + 64 H	用于计算 MAC 的源密钥索引或密文
分散级数	2 H	取值 00-08。该域取值决定后面存在几个分散因子域。
分散因子	n*16 H	n 级分散因子串联，每级分散因子为 8 字节（16H）；
会话密钥产生模式	2 H	会话密钥的产生模式： 00 – 不产生会话密钥； 01 – ECB 模式加密 8 字节会话密钥因子[6 字节‘00’||2 字节 ATC]，得 8 字节会话密钥； 02 – ECB 模式加密 16 字节会话密钥因子[6 字节‘00’||2 字节 ATC||6 字节‘00’||2 字节 ATC 的非]，得 16 字节会话密钥； 03 – 密钥的左右 8 字节异或，得 8 字节会话密钥； 04 – 取密钥的左 8 字节做为会话密钥；
会话密钥因子	4 H	可选域，仅当会话密钥产生模式为 1 或 2 时存在 该域通常为 2 字节 ATC
PAD 标识	2 H	标识加密前数据的填充规则 取值范围：00 – 05 或 10 – 11，详细规则参见 4.1
数据长度	4 H	要计算 MAC 的数据长度，字节数 取值 0000-03D8（即 0 – 984 字节）
数据	n*2 H	要计算 MAC 的数据
IV	16 H / 32 H	用于计算 MAC 的初始向量 128 位分组（密钥标识 P/L/R）时，该域 16 字节（32H）； 否则该域为 8 字节（16H）；
待验证的 MAC/TAC	n*2 H	数据 MAC 值，长度由取值标识域指定
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	D2

错误码	2 A	00：成功 01：MAC 验证失败 04：非法的密钥类型 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 34：非法的 MAC 算法模式（或与密钥的算法标识不符） 35：非法的 MAC 取值方式 36：非法的分散级数 37：非法的会话密钥产生方式 39：非法的数据填充方式 41：无主密钥或加密卡运算单元错误 45：密钥不存在 80：非法的数据长度
MAC 诊断数据	2*n H	仅当错误码为 01 时存在，输出 HSM 计算的 MAC 值

3.3.5.3. 计算数据 MAC/TAC – 通用（S0）

数据运算功能，可用于交易系统和发卡过程。

本指令为通用指令，可自定义 MAC 算法模式、取值模式，支持多种密钥类型，自定义数据 PADDING 规则、计算 MAC 的 IV 数据等。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	S0
MAC 算法模式	2 H	01 – ISO9797-1 MAC 算法模式 1 使用 MAC 密钥 CBC 模式加密数据，取最后一段密文； 03 – ISO9797-1 MAC 算法模式 3，限密钥标识为 X/U 等同于 ANSI X9.19，MAC 密钥 16 字节，KL 对数据 DES CBC 加密运算，最后一段结果 KR DES 解密，再 KL DES 加密，得 8 字节 MAC 结果；
MAC 取值方式	2 H	按前个域模式产生的密文值按下述结果作为 MAC： 01-08 密文值的左 n 字节 10 全 16 字节 MAC（限密钥标识为 P/L/R） 11-18 密文值的右 n 字节 21-28 左右异或后取左 n 字节输出 31-38 左右异或后取右 n 字节输出 44 四字节异或，最后输出 4 字节
源密钥类型	3 H	用于计算 MAC 的源密钥类型 109 – MDK; 209 – MK-SMI; 000 – KEK; 011 – KMC; 008 – ZAK; 003 – TAK;
源密钥	K + 4 N / 16 H / 1 A + 16 H / 1 A + 32 H / 1 A + 48 H / 1 A + 64 H	用于计算 MAC 的源密钥索引或密文

分散级数	2 H	取值 00-03。该域取值决定后面存在几个分散因子域。
分散因子	n*32 H	n 级分散因子串联，每级分散因子为 16 字节（32H）；
会话密钥产生模式	2 H	会话密钥的产生模式： 00 - 不产生会话密钥； 01 - ECB 模式加密 8 字节会话密钥因子，得 8 字节会话密钥； 02 - ECB 模式加密 16 字节会话密钥因子，得 16 字节会话密钥； 03 - 密钥的左右 8 字节异或，得 8 字节会话密钥； 04 - 取密钥的左 8 字节做为会话密钥； 05 - CBC 模式加密 16 字节会话密钥因子，得 16 字节会话密钥；
会话密钥因子	16 H / 32 H	仅当会话密钥模式取值为 01/02/05 时存在 • 会话密钥模式为 01 时，该域为 8 字节（16H），适用于产生 PBOC 规范的单长度会话密钥，取值：6 字节 0x00||2 字节 ATC； • 会话密钥模式为 02 时，该域为 16 字节（32H），适用于产生 PBOC 规范的双长度会话密钥，取值：6 字节 0x00||2 字节 ATC||6 字节 0x00||2 字节 ATC 的非； • 会话密钥模式为 05 时，该域为 16 字节（32H），适用于产生 GP 规范 SCP02 的卡片会话密钥，取值：2 字节密钥类型||2 字节卡计数器||12 字节 0x00；
PAD 标识	2 H	标识加密前数据的填充规则 取值范围：00 - 05 或 10 - 11，详细规则参见 4.1
数据长度	4 H	要计算 MAC 的数据长度，字节数 取值 0000-07B0（即 0 - 1968 字节）
数据	n B	要计算 MAC 的数据
IV	16 H / 32 H	用于计算 MAC 的初始向量 128 位分组（密钥标识 P/L/R）时，该域 16 字节（32H）； 否则该域为 8 字节（16H）；
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	S1
错误码	2 A	00：成功 04：非法的密钥类型 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 34：非法的 MAC 算法模式（或与密钥的算法标识不符） 35：非法的 MAC 取值方式 36：非法的分散级数 37：非法的会话密钥产生方式 39：非法的数据填充方式 41：无主密钥或加密卡运算单元错误 45：密钥不存在 80：非法的数据长度
数据 MAC	n*2 H	数据 MAC 值，长度由取值标识域指定
MAC 密文	16 H	仅当源密钥为 X/U 类型时存在 MAC 值的密文，使用会话密钥的左 8 字节对 MAC 全值的左 8 字节加密；通常用于做下次交易 MAC 计算的 IV。

示例 1. 3DES 算法的 KEK 密钥计算 18 字节输入数据的 MAC 值

```
[
S0
03
08
000
X801617441513A2F135AB14EAAD1069DF
00
00
01
0012
& 000102030405060708090A0B0C0D0E0F 1011 !
0000000000000000
|
S1
00
70F3C90691D6F170
]
```

‘&’与‘!’之间的字符为扩展 16 进制字符数据，发送密码机时需转换为 BCD 码数据串，2 个字符转换成一个字节，如“70”转换为 0x70；

3.3.5.4. 计算数据 HMAC – 明文密钥（LR）

采用明文密钥对输入数据计算 HMAC 值。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	LR
HASH 算法标识	2 N	01 ： SHA-1 02 ： MD5
密钥长度	4 N	用于计算 HMAC 的明文密钥的长度，字节数 取值范围：1 – 256
密钥明文	n B	用于计算 HMAC 的明文密钥
分隔符	1 A	取值’;’，标识密钥明文输入结束
数据长度	4 N	用于计算 HMAC 的输入数据的长度，字节数 取值范围：1 – 1984
输入数据	n B	用于计算 HMAC 的输入数据
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	LS
错误码	2 A	00：成功 否则，失败
HMAC 长度	4 N	输出的 HMAC 的长度，字节数
HMAC 值	n B	输出的 HMAC 结果

3.3.6. 数据摘要运算

3.3.6.1. 计算单包数据摘要（3C）

该指令支持小报文（0-1984 字节）的数据摘要运算。

支持通用的摘要算法及 SM3 国密算法。其中 SM3 算法支持带 ID 和不带 ID 的模式：

- 带 ID 的 SM3 算法，需输入正确的 SM2 公钥数据及用户 ID；若用户 ID 若不存在，则 HSM 内采用国密局发布的默认 ID：”1234567812345678”；
- 不带 ID 的 SM3 算法，“用户 ID 长度”与“公钥长度”域全部填入 0000；

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	3C
HASH 算法标识	2 N	01 ： SHA-1 02 ： MD5 03 ： ISO 10118-2 05 ： SHA-224 06 ： SHA-256 07 ： SHA-384 08 ： SHA-512 20 ： SM3-256
数据块长度	4 N	待运算的数据长度，字节数 取值 0000-4096
数据块	n B	输入数据
分隔符	1 A	‘;’ 标识数据块域的结束
用户 ID 长度	4 N	仅当 HASH 算法标识为 20 时存在 取值 0000-0032
用户 ID	n B	仅当 HASH 算法标识为 20 时存在 用户 ID
公钥长度	4 N	仅当 HASH 算法标识为 20 时存在 DER 编码的公钥长度，字节数
SM2 算法公钥	n B	仅当 HASH 算法标识为 20 时存在 公钥，ASN.1 格式 DER 编码（x，y）
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	3D
错误码	2 A	00：成功 15：无效的输入数据（无效的格式/字符或长度错误） 32：非法的用户 ID 长度 79：非法的 HASH 算法标识 80：非法的数据长度
HASH 结果长度	2 N	摘要值的长度
HASH	n B	计算后的摘要值

3.3.6.2. 大包数据摘要的初始化（H1）

摘要 Init 功能，该指令与 H2/H3 指令配合，可支持大报文的数据摘要运算。

支持通用的摘要算法及 SM3 国密算法。其中 SM3 算法支持带 ID 和不带 ID 的模式：

- 带 ID 的 SM3 算法，需输入正确的 SM2 公钥数据及用户 ID；若用户 ID 若不存在，则 HSM 内采用国密局发布的默认 ID：”1234567812345678”；
- 不带 ID 的 SM3 算法，“用户 ID 长度”与“公钥长度”域全部填入 0000；

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	H1
HASH 算法标识	2 N	01 ： SHA-1 02 ： MD5 03 ： ISO 10118-2 05 ： SHA-224 06 ： SHA-256 07 ： SHA-384 08 ： SHA-512 20 ： SM3-256
用户 ID 长度	4 N	仅当 HASH 算法标识为 20 时存在 取值 0000-0032
用户 ID	n B	仅当 HASH 算法标识为 20 时存在 用户 ID
公钥长度	4 N	仅当 HASH 算法标识为 20 时存在 DER 编码的公钥长度，字节数
SM2 算法公钥	n B	仅当 HASH 算法标识为 20 时存在 公钥，ASN.1 格式 DER 编码（x，y）
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	H2
错误码	2 A	00：成功 15：无效的输入数据（无效的格式/字符或长度错误） 32：非法的用户 ID 长度 79：非法的 HASH 算法标识
HASH CONTEXT 长度	4 N	初始化后的摘要上下文内容长度
HASH CONTEXT	n B	摘要上下文内容

3.3.6.3. 大包数据摘要的过程运算（H2）

摘要 Update 功能，该指令与 H1/H3 指令配合，可支持大报文的数据摘要运算。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	H2
HASH CONTEXT 长度	4 N	摘要上下文内容长度
HASH CONTEXT	n B	摘要上下文内容，摘要初始化后的结果或前一块数据运

		算的结果
数据块长度	4 N	待运算的数据长度，字节数 取值 0000-4096
数据块	n B	输入数据
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	H3
错误码	2 A	00：成功 15：无效的输入数据（无效的格式/字符或长度错误） 80：非法的数据长度
HASH CONTEXT 长度	4 N	本包运算后的摘要上下文内容长度
HASH CONTEXT	n B	摘要的上下文内容，用于下个包的运算或获取摘要结果

3.3.6.4. 大包数据摘要的结束，输出摘要结果（H3）

摘要 Final 功能，该指令与 H1/H2 指令配合，可支持大报文的数据摘要运算。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	H3
HASH CONTEXT 长度	4 N	摘要上下文内容长度
HASH CONTEXT	n B	摘要上下文内容，最后一块数据运算的结果
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	H4
错误码	2 A	00：成功 15：无效的输入数据（无效的格式/字符或长度错误） 80：非法的数据长度
HASH 长度	2 N	摘要结果的长度，字节数
HASH 结果	n B	摘要的结果

3.3.7. PIN 安全管理

本部分指令包含对数字 PIN 和字符 PIN 的密文转换、产生等功能。字符 PIN 通常用于网银或网上支付系统的安全登录，字符 PIN 包含字母和数字的组合：’0’-‘9, ‘A’-‘Z’, ‘a’-‘z’。。

3.3.7.1. 产生指定长度的随机字符 PIN（P0）

随机产生指定长度的字符 PIN，并由 ZPK 加密输出。

字符 PINBLOCK 格式参见 6 PINBLOCK(字符)格式。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机。
命令代码	2 A	P0

PIN 长度	2 N	待产生的随机 PIN 的长度，取值范围：04 – 16
ZPK 密钥	K + 4 N / 16 H / 1 A + 32 H / 1 A + 48 H / 1 A + 64 H	用于加密 PIN 的 ZPK 的密钥索引或密文
字符 PINBLOCK 格式	2 N	标识使用 ZPK 加密 PIN 时的 PIN 数据块组成格式，详细参见 **6 PINBLOCK(字符)格式**。 00 – PIN 与账号分别左对齐，以填充 0x00 方式扩展为 48H（采用 64 位分组算法）或 64H（采用 128 位分组算法），再异或后得到 PIN 数据块； 01 – ASCII 码序列[账号|PIN|填充字符]得到 PIN 数据块。填充规则：根据密钥算法的分组长度，按需要填充的字节数填入相应字符，例如缺少 6 个字节，则填入 6 个字符'6'；若满足分组长度的倍数则不填充； 02 – PIN 与账号分别左对齐，以填充 0x00 方式扩展为 32H，再异或后得到 PIN 数据块；
账号长度	2 N	标识账号长度，账号位数，01-24
账号 PAN	n N	用户有效主帐号或客户号 当“字符 PINBLOCK 格式”取值为 02 时，该域不能超过 16 个数字
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	P1
错误码	2 A	00：成功 15：无效的输入数据（无效的格式/字符或长度错误） 41：无主密钥或加密卡运算单元错误 80：非法的数据长度
PIN 密文长度	2 N	ZPK 下加密的随机字符 PIN 的密文长度
PIN 密文	n*2 H	ZPK 下加密的随机字符 PIN 的密文

3.3.7.2. ZPK 加密字符 PIN（P6）

明文字符 PIN 由 ZPK 直接加密输出。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机。
命令代码	2 A	P6
ZPK 密钥	K + 4 N / 16 H / 1 A + 32 H / 1 A + 48 H / 1 A + 64 H	用于加密 PIN 的 ZPK 的密钥索引或密文
字符 PIN 明文长度	2 N	字符 PIN 的明文长度
字符 PIN 明文	N A	字符 PIN 明文
字符 PINBLOCK 格式	2 N	标识使用 ZPK 加密 PIN 时的 PIN 数据块组成格式，详细参见 6 PINBLOCK(字符)格式。 00 – PIN 与账号分别左对齐，以填充 0x00 方式扩展为 48H（采用 64 位分组算法）或 64H（采用 128 位分

		组算法），再异或后得到 PIN 数据块； 02 – PIN 与账号分别左对齐，以填充 0x00 方式扩展为 32H，再异或后得到 PIN 数据块； 03 – 柜员登录密码的加密规范，限定 PIN 的最大长度为 8。柜员号前补 0 至 16 或 32 位作为二进制串，PIN 密码 BCD 扩展后补 0 至 16 或 32 位，然后异或用密钥加密。
账号长度	2 N	标识账号长度，账号位数，01-24
账号 PAN	n N	用户有效主帐号或客户号 当“源字符 PINBLOCK 格式”取值为 02/03 时，该域不能超过 16 个数字
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	P7
错误码	2 A	00：成功 15：无效的输入数据（无效的格式/字符或长度错误） 41：无主密钥或加密卡运算单元错误 80：非法的数据长度
PIN 密文长度	2 N	ZPK 密钥下加密的字符 PIN 的密文长度
PIN 密文	n*2 H	ZPK 密钥下加密的字符 PIN 的密文

3.3.7.3. 字符 PINBLOCK 转加密（P7）

ZPK 下加密的字符 PIN 密文，转换到其他密钥下加密，该指令不支持密钥分散。

字符 PIN 包含字母和数字的组合：’0’-‘9, ‘A’-‘Z’, ‘a’-‘z’。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机。
命令代码	2 A	P7
源 ZPK 密钥	K + 4 N / 16 H / 1 A + 32 H / 1 A + 48 H / 1 A + 64 H	用于加密 PIN 的源 ZPK 的密钥索引或密文
目的密钥类型	3 H	用于加密 PIN 的目的密钥的类型 001 – ZPK; 002 – TPK/PVK;
目的密钥	K + 4 N / 16 H / 1 A + 32 H / 1 A + 48 H / 1 A + 64 H	用于加密 PIN 的目的密钥索引或密文
源 PINBLOCK 密文长度	2 N	源 ZPK 下加密的字符 PIN 块的密文长度
源 PINBLOCK 密文	n*2 H	在源密钥下加密的 PINBLOCK 密文
源字符 PINBLOCK 格式	2 N	标识使用源 ZPK 加密 PIN 时的 PIN 数据块组成格式，详细参见 6 PINBLOCK(字符)格式。 00 – PIN 与账号分别左对齐，以填充 0x00 方式扩展为 48H（采用 64 位分组算法）或 64H（采用 128 位分组算法），再异或后得到 PIN 数据块； 02 – PIN 与账号分别左对齐，以填充 0x00 方式扩展为 32H，再异或后得到 PIN 数据块；

		03 – 柜员登录密码的加密规范，限定 PIN 的最大长度为 8。柜员号前补 0 至 16 或 32 位作为二进制串，PIN 密码 BCD 扩展后补 0 至 16 或 32 位，然后异或用密钥加密。
源账号长度	2 N	标识账号长度，账号位数，01-24
源账号 PAN	n N	用户有效主帐号或客户号 当“源字符 PINBLOCK 格式”取值为 02/03 时，该域不能超过 16 个数字
目的字符 PINBLOCK 格式	2 N	标识使用目标密钥加密 PIN 时的 PIN 数据块组成格式，详细参见 **6 PINBLOCK(字符)格式**。 00 – PIN 与账号分别左对齐，以填充 0x00 方式扩展为 48H（采用 64 位分组算法）或 64H（采用 128 位分组算法），再异或后得到 PIN 数据块； 02 – PIN 与账号分别左对齐，以填充 0x00 方式扩展为 32H，再异或后得到 PIN 数据块； 03 – 柜员登录密码的加密规范，限定 PIN 的最大长度为 8。柜员号前补 0 至 16 或 32 位作为二进制串，PIN 密码 BCD 扩展后补 0 至 16 或 32 位，然后异或用密钥加密。
目的账号长度	2 N	标识账号长度，账号位数，01-24
目的账号 PAN	n N	用户有效主帐号或客户号 当“目的字符 PINBLOCK 格式”取值为 02/03 时，该域不能超过 16 个数字
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	P8
错误码	2 A	00：成功 15：无效的输入数据（无效的格式/字符或长度错误） 41：无主密钥或加密卡运算单元错误 80：非法的数据长度
PIN 明文长度	2 N	PIN 明文的长度，字节数
PIN 密文长度	2 N	目的密钥下加密的随机字符 PIN 的密文长度
PIN 密文	n*2 H	目的密钥下加密的随机字符 PIN 的密文

3.3.7.4. 数字 PINBLOCK 转加密（D7）

该指令支持 ZPK 密钥的分散。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	D7
源密钥扩展标识	1A	‘P’,可选域
密钥扩展类型	1N	当密钥扩展标识存在时存在，0-ZPK，1-EDK
源 ZPK 密钥	K + 4N / 1A + 16 H / 1A + 32H / 1A + 48H	用于加密 PIN 的源 ZPK 密钥索引或密文
源密钥分散级数	2 H	分散级数。取值 00 – 08。
源密钥分散因子	n*16 H	n 级分散因子串联，每级分散因子为 8 字节（16H）；
源密钥会话密钥模式	2 H	会话密钥的产生模式： 00 – 不产生会话密钥；

		01 - ECB 模式加密 8 字节会话密钥因子[6 字节‘00’||2 字节 ATC]，得 8 字节会话密钥； 02 - ECB 模式加密 16 字节会话密钥因子[6 字节‘00’||2 字节 ATC||6 字节‘00’||2 字节 ATC 的非]，得 16 字节会话密钥； 03 - 密钥的左右 8 字节异或，得 8 字节会话密钥； 04 - 取密钥的左 8 字节做为会话密钥；
源密钥会话密钥因子	4 H	可选域，仅当会话密钥产生模式为 1 或 2 时存在 该域通常为 2 字节 ATC
密钥扩展标识	1A	‘P’,可选域
密钥扩展类型	1N	当密钥扩展标识存在时存在，0-ZPK，1-EDK
目标 ZPK 密钥	K + 4N / 1A + 16 H / 1A + 32H / 1A + 48H	用于加密 PIN 的目标 ZPK 密钥索引或密文
目标密钥分散级数	2 H	分散级数。取值 00 - 08。
目标密钥分散因子	n*16 H	n 级分散因子串联，每级分散因子为 8 字节（16H）；
目标密钥会话密钥模式	2 H	会话密钥的产生模式： 00 - 不产生会话密钥； 01 - ECB 模式加密 8 字节会话密钥因子[6 字节‘00’||2 字节 ATC]，得 8 字节会话密钥； 02 - ECB 模式加密 16 字节会话密钥因子[6 字节‘00’||2 字节 ATC||6 字节‘00’||2 字节 ATC 的非]，得 16 字节会话密钥； 03 - 密钥的左右 8 字节异或，得 8 字节会话密钥； 04 - 取密钥的左 8 字节做为会话密钥；
目标密钥会话密钥因子	4 H	可选域，仅当会话密钥产生模式为 1 或 2 时存在 该域通常为 2 字节 ATC
最大 PIN 长度	2 N	取值 12
源 PINBLOCK 密文	16 H / 32 H	在源 TPK/ZPK 下加密的 PINBLOCK 密文 源密钥方案为 R/P/L 时该域为 32H，否则 16H
源 PINBLOCK 格式	2 N	源密钥下加密 PIN 数据块的格式代码，参见 **5 PINBLOCK(数字)格式** 源密钥扩展类型标识为 1 时,该域必须为 21.
源账号	12 N / 18 N	用户主账号 当源 PIN 数据块格式为 04 时，该域为 18N，去除校验位的 18 位主账号，不足 18 位则右对齐左填 F； 当源 PIN 数据块格式为其他值时，该域为 12N，去除校验位的最右 12 位主账号；
目标 PINBLOCK 格式	2 N	目标密钥下加密 PIN 数据块的格式代码，参见 **5 PINBLOCK(数字)格式** 目的密钥扩展类型标识为 1 时,该域必须为 21.
目标账号	12 N / 18 N	用户主账号 当目标 PIN 数据块格式为 04 时，该域为 18N，去除校验位的 18 位主账号，不足 18 位则右对齐左填 F； 当 PIN 数据块格式为其他值时，该域为 12N，去除校验位的最右 12 位主账号；
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	D8
错误码	2 A	00：成功 03：非法的加密算法模式

		04：非法的密钥类型 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 36：非法的分散级数 37：非法的会话密钥产生方式 39：非法的数据填充方式 41：无主密钥或加密卡运算单元错误 45：密钥不存在 70：无效的密文数据，数据解密去 padding 失败 80：非法的数据长度
目标 PINBLOCK 密文	16 H / 32 H	在目标密钥下加密的 PINBLOCK 密文 目标密钥方案为 R/P/L 时该域为 32H，否则 16H

3.3.7.5. 数字 PINBLOCK 转加密 – 通用（S7）

该指令支持源密钥、目的密钥的分散和会话密钥的产生，支持 PINBLOCK 格式和账号的变换。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	S7
源密钥类型	3 H	用于加密 PINBLOCK 的源密钥类型 000 - KEK; 109 - MDK; 309 - MK-SMC; 00A - ZEK/DEK; 00B - TEK; 011 - KMC; 001 - ZPK; 002 - TPK;
源密钥	K + 4N / 16H / 1A+16H / 1A + 32H / 1A + 48H / 1A + 64H	用于加密 PIN 的源密钥索引或密文
源密钥分散级数	2 H	分散级数。取值 00 - 08。
源密钥分散因子	n*32 H	n 个分散因子的串联。每个分散因子必须为 16 个字节。
源密钥会话密钥模式	2 H	会话密钥的产生模式： 00 - 不产生会话密钥； 01 - ECB 模式加密 8 字节会话密钥因子，得 8 字节会话密钥； 02 - ECB 模式加密 16 字节会话密钥因子，得 16 字节会话密钥； 03 - 密钥的左右 8 字节异或，得 8 字节会话密钥； 04 - 取密钥的左 8 字节做为会话密钥； 05 - CBC 模式加密 16 字节会话密钥因子，得 16 字节会话密钥；
源密钥会话密钥因子	16 H / 32 H	仅当源密钥会话密钥模式取值为 01/02/05 时存在 • 会话密钥模式为 01 时，该域为 8 字节（16H），适用于产生 PBOC 规范的单长度会话密钥，取值：6 字节 0x00||2 字节 ATC； • 会话密钥模式为 02 时，该域为 16 字节（32H），适用于产生 PBOC 规范的双长度会话密钥，取值：6 字节 0x00||2 字节 ATC||6 字节 0x00||2 字节 ATC 的非； • 会话密钥模式为 05 时，该域为 16 字节（32H），

		适用于产生 GP 规范 SCP02 的卡片会话密钥,取值: 2 字节密钥类型||2 字节卡计数器||12 字节 0x00;
目的密钥类型	3 H	用于加密 PINBLOCK 的目的密钥类型 000 - KEK; 109 - MDK; 309 - MK-SMC; 00A - ZEK/DEK; 00B - TEK; 011 - KMC; 001 - ZPK; 002 - TPK;
目的密钥	K + 4N / 16H / 1A+16H / 1A + 32H / 1A + 48H / 1A + 64H	用于加密 PIN 的目的密钥索引或密文
目的密钥分散级数	2 H	分散级数。取值 00 - 08。
目的密钥分散因子	n*32 H	n 个分散因子的串联。每个分散因子必须为 16 个字节。
目的密钥会话密钥模式	2 H	会话密钥的产生模式: 00 - 不产生会话密钥; 01 - ECB 模式加密 8 字节会话密钥因子,得 8 字节会话密钥; 02 - ECB 模式加密 16 字节会话密钥因子,得 16 字节会话密钥; 03 - 密钥的左右 8 字节异或,得 8 字节会话密钥; 04 - 取密钥的左 8 字节做为会话密钥; 05 - CBC 模式加密 16 字节会话密钥因子,得 16 字节会话密钥;
目的密钥会话密钥因子	16 H / 32 H	仅当目的密钥会话密钥模式取值为 01/02/05 时存在 • 会话密钥模式为 01 时,该域为 8 字节(16H),适用于产生 PBOC 规范的单长度会话密钥,取值:6 字节 0x00||2 字节 ATC; • 会话密钥模式为 02 时,该域为 16 字节(32H),适用于产生 PBOC 规范的双长度会话密钥,取值:6 字节 0x00||2 字节 ATC||6 字节 0x00||2 字节 ATC 的非; • 会话密钥模式为 05 时,该域为 16 字节(32H),适用于产生 GP 规范 SCP02 的卡片会话密钥,取值:2 字节密钥类型||2 字节卡计数器||12 字节 0x00;
最大 PIN 长度	2 N	取值 12
源 PINBLOCK 密文	16 H / 32 H	在源密钥下加密的 PINBLOCK 密文 源密钥方案为 R/P/L/M/N 时该域为 32H,否则 16H
源 PINBLOCK 格式	2 N	源密钥下加密 PIN 数据块的格式代码,参见 **5 PINBLOCK(数字)格式**
源账号	12 N / 18 N	用户主账号 当源 PIN 数据块格式为 04 时,该域为 18N,去除校验位的 18 位主账号,不足 18 位则右对齐左填 F; 当源 PIN 数据块格式为其他值时,该域为 12N,去除校验位的最右 12 位主账号;
目标 PINBLOCK 格式	2 N	目标密钥下加密 PIN 数据块的格式代码,参见 **5 PINBLOCK(数字)格式**
目标账号	12 N / 18 N	用户主账号 当目标 PIN 数据块格式为 04 时,该域为 18N,去除校验位的 18 位主账号,不足 18 位则右对齐左填 F; 当 PIN 数据块格式为其他值时,该域为 12N,去除校验位的最右 12 位主账号;
响应报文		

报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	S8
错误码	2 A	00：成功 03：非法的加密算法模式 04：非法的密钥类型 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 36：非法的分散级数 37：非法的会话密钥产生方式 39：非法的数据填充方式 41：无主密钥或加密卡运算单元错误 45：密钥不存在 70：无效的密文数据，数据解密去 padding 失败 80：非法的数据长度
目标 PINBLOCK 密文	16 H / 32 H	在目标密钥下加密的 PINBLOCK 密文 目标密钥方案为 R/P/L/M/N 时该域为 32H，否则 16H

3.3.7.6. 将字符 PIN 由 TPK 加密转为公钥加密（N5）

该指令支持字符类型的 PIN 密文转换。通常用于网银系统中用户 PIN 的密文转换。

TPK 加密 PIN 数据块时采用 ECB 模式。

域	长度&类型	描述
	命令报文	
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	N5
TPK 密钥	K + 4 N / 16 H / 1 A + 32 H / 1 A + 48 H	用于加密 PIN 的 TPK 密钥索引或密文
TPK 加密的 PIN 密文长度	2 N	TPK 下加密的字符 PIN 块的密文长度
TPK 加密的 PIN 密文	n*2 H	在 TPK 密钥下加密的 PINBLOCK 密文，Expanded Hex 格式
字符 PINBLOCK 格式	2 N	标识使用 TPK 加密 PIN 时的 PIN 数据块组成格式，详细参见 6 PINBLOCK(字符)格式。 00 - PIN 与账号分别左对齐，以填充 0x00 方式扩展为 48H（采用 64 位分组算法）或 64H（采用 128 位分组算法），再异或后得到 PIN 数据块； 02 - PIN 与账号分别左对齐，以填充 0x00 方式扩展为 32H，再异或后得到 PIN 数据块；
账号长度	2 N	标识账号长度，账号位数，01-24
账号 PAN	n N	用户有效主帐号或客户号 当“字符 PINBLOCK 格式”取值为 02 时，该域不能超过 16 个数字
公钥算法标识	2 N	标识公钥加密字符 PIN 时采用的非对称算法 01 - RSA 07 - SM2
公钥索引号	4 N	9999 标识公钥使用下面域的值。
公钥	n B	公钥， ASN.1 格式 DER 编码

认证数据	n B	用于计算公钥 MAC 的额外的数据，不能包含’;’字符。
认证数据分隔符	1 A	‘;’,用于标识认证数据域的结束。
公钥 MAC	4 B	公钥 MAC 值，用于验证公钥的合法可信；
公钥加密 PIN 组成格式	2 N	标识公钥加密 PIN 时的 PIN 块字符串组成格式 00 - ID 长度(2N)+ID 码+PIN 长度(2N)+PIN 明文 01 - PIN 明文块 02 - PIN 长度(2N)+PIN 明文+ID 长度(2N)+ID 码
ID 码长度	2 N	仅当公钥加密 PIN 组成格式为 0 或 2 时存在 01-20
ID 码	n*2 H	仅当公钥加密 PIN 组成格式为 0 或 2 时存在 ID 码明文，Expanded Hex 格式
公钥加密的填充模式	2 N	标识公钥加密 PIN 数据块时采用的填充模式，仅当公钥算法标识为 01 时存在； 01 - PKCS#1 v1.5 填充方式 07 - 在 PIN 数据块前面补 0x00，以使数据长度等于 RSA 密钥模长
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	N6
错误码	2 A	00：成功 01：公钥 MAC 验证失败 03：无效的公钥算法标识 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 23：非法的 PIN 组成格式 24：非法的 PIN 长度 34：非法的 MAC 算法模式（或与密钥的算法标识不符） 39：非法的填充模式 41：无主密钥或加密卡运算单元错误 45：密钥不存在
公钥加密的 PIN 密文长度	4 N	标识公钥加密的 PIN 数据块密文的长度，字节数
公钥加密的 PIN 密文	n B	公钥加密的 PIN 数据块密文

3.3.7.7. 公钥加密的字符 PIN 密文转为 ZPK 加密（N6）

该指令支持字符类型的 PIN 密文转换。通常用于网银系统中用户 PIN 的密文转换。

命令域中的 PIN 明文指 ASCII 码形式的 PIN 字符串。

ZPK 加密 PIN 数据块时采用 ECB 模式。可选的，输出 ZPK 对私钥解密后的 PIN 数据块计算的 MAC 值。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	N6
公钥算法标识	2 N	标识公钥加密字符 PIN 时采用的非对称算法 01 - RSA 07 - SM2

私钥索引	4 N	用于解密（公钥加密的）PIN 密文的私钥索引号，0001-0064 9999 标识使用私钥使用下面两个域的值。
私钥长度	4 N	下个域的长度，仅当私钥索引号为 9999 时存在；
私钥	n B	LMK 加密的私钥密文，仅当私钥索引号为 9999 时存在；
公钥加密 PIN 组成格式	2 N	标识公钥加密 PIN 时的 PIN 块字符串组成格式 00 - ID 长度(2N)+ID 码+PIN 长度(2N)+PIN 明文 01 - PIN 明文块 02 - PIN 长度(2N)+PIN 明文+ID 长度(2N)+ID 码
公钥加密的填充模式	2 N	标识公钥加密 PIN 数据块时采用的填充模式，仅当公钥算法标识为 01 时存在； 01 - PKCS#1 v1.5 填充方式 07 - 在 PIN 数据块前面补 0x00，以使数据长度等于 RSA 密钥模长
密钥扩展标识	1A	‘P’,可选域
密钥扩展类型	1N	当密钥扩展标识存在时存在，0-ZPK，1-EDK
ZPK 密钥	K + 4N / 16 H / 1 A + 32 H / 1 A + 48 H	用于加密 PIN 的 ZPK 密钥索引或密文
ZPK 加密 PIN 组成格式	2 N	标识使用 ZPK 加密 PIN 时的 PIN 数据块组成格式，详细参见 **6 PINBLOCK(字符)格式**。 00 - PIN 与账号分别左对齐，以填充 0x00 方式扩展为 48H（采用 64 位分组算法）或 64H（采用 128 位分组算法），再异或后得到 PIN 数据块； 01 - ASCII 码序列[账号|PIN|填充字符]得到 PIN 数据块。填充规则：根据密钥算法的分组长度，按需要填充的字节数填入相应字符，例如缺少 6 个字节，则填入 6 个字符’6’；若满足分组长度的倍数则不填充； 02 - PIN 与账号分别左对齐，以填充 0x00 方式扩展为 32H，再异或后得到 PIN 数据块； 11-当密钥扩展类型标识为 1 时,该域必须为 11.
账号存在标识	1A	可选域，仅当密要类型为 EDK，PIN 组成格式为 11 时存在 0- 不存在账号 1- 存在账号
账号长度	2 N	标识账号长度，账号位数，01-24
账号 PAN	n N	用户有效主帐号或客户号
公钥加密的 PIN 密文长度	4 N	标识公钥加密的 PIN 数据块密文的长度，字节数
公钥加密的 PIN 密文	n B	公钥加密的 PIN 数据块密文
扩展输出标识	1 A	可选域 1) 取值为’T’，则扩展输出数据块 MAC 值（使用 ZPK 对私钥解密后的 PIN 数据块计算 MAC）；必须包含后续两个域内容； 2) 此域为空，则输出域中不包含数据块 MAC，后续两个域也不存在；
MAC 算法模式	2 H	仅当“扩展输出标识”为 T 时存在 01 - ISO9797-1 MAC 算法模式 1 使用 MAC 密钥全 CBC 模式加密数据，取最后一段

		密文； 03 – ISO9797-1 MAC 算法模式 3，限 ZPK 标识为 X/U 等同于 ANSI X9.19，MAC 密钥 16 字节，KL 对数据 DES CBC 加密运算，最后一段结果 KR DES 解密，再 KL DES 加密，得 8 字节 MAC 结果；
计算 MAC 的数据块 PAD 标识	2 H	仅当“扩展输出标识”为 T 时存在，标识计算 MAC 前数据的填充规则 取值范围：00 – 05 或 10 – 11，详细规则参见 4.1
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	N7
错误码	2 A	00：成功 03：无效的公钥算法标识 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 23：非法的 PIN 组成格式 24：非法的 PIN 长度 34：非法的 MAC 算法模式（或与密钥的算法标识不符） 39：非法的填充模式 41：无主密钥或加密卡运算单元错误 45：密钥不存在
明文 PIN 长度	2 N	PIN 明文的长度，04-20
ZPK 加密的 PIN 密文长度	2 N	标识 ZPK 加密的 PIN 数据块密文的长度，字节数
ZPK 加密的 PIN 密文	n*2 H	ZPK 加密的 PIN 数据块密文，Expanded Hex 格式
ID 码长度	2 N	仅当公钥加密 PIN 组成格式为 0 或 2 时存在 01-20
ID 码	n*2 H	仅当公钥加密 PIN 组成格式为 0 或 2 时存在 ID 码明文，Expanded Hex 格式
数据块 MAC 值	16 H / 32 H	仅当扩展输出标识为 T 时存在 使用 ZPK 对私钥解密后的 PIN 数据块按指定算法计算出来的 MAC 值 当 ZPK 密钥标识为 Z/X/U 时，该域为 16H 当 ZPK 密钥标识为 R/P/L 时，该域为 32H

3.3.7.8. 将数字 PIN 由 TPK 加密转为公钥加密（N7）

该指令支持数字类型的 PIN 密文转换。通常用于网银系统中用户 PIN 的密文转换。

TPK 加密 PIN 数据块时采用 ECB 模式。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	N7
TPK 密钥	K + 4N / 16 H / 1 A + 32 H / 1 A + 48 H	用于加密 PIN 的 TPK 密钥索引或密文
TPK 加密的 PIN 密文长度	2 N	标识 TPK 加密的 PIN 数据块密文的长度，字节数
TPK 加密的 PIN 密文	n*2 H	TPK 加密的 PIN 数据块密文，Expanded Hex 格式

		TPK 为 64 位分组算法密钥时，PIN 密文结果为 16H； TPK 为 128 位分组算法密钥时，PIN 密文结果为 32H；
PINBLOCK 格式	2 N	TPK 加密 PINBLOCK 的格式代码，参见 **5 PINBLOCK(数字)格式**
账号 PAN	12/18 N	用户主账号 当 PIN 数据块格式为 04 时，该域为 18N，去除校验位的 18 位主账号，不足 18 位则右对齐左填 F； 当 PIN 数据块格式为其他值时，该域为 12N；
公钥算法标识	2 N	标识公钥加密字符 PIN 时采用的非对称算法 01 - RSA 07 - SM2
公钥索引号	4 N	9999 标识公钥使用下面域的值。
公钥	n B	公钥， ASN.1 格式 DER 编码
认证数据	n B	用于计算公钥 MAC 的额外的数据，不能包含’;’字符。
认证数据分隔符	1 A	‘;’,用于标识认证数据域的结束。
公钥 MAC	4 B	公钥 MAC 值，用于验证公钥的合法可信；
公钥加密 PIN 组成格式	2 N	标识公钥加密 PIN 时的 PIN 数据块组成格式 00 - ID 长度(2N)+ID 码+PIN 长度(2N)+PIN 明文 01 - PIN 明文块 10 - PINBLOCK 块
ID 码长度	2 N	仅当公钥加密 PIN 组成格式为 0 时存在 01-20
ID 码	n*2 H	仅当公钥加密 PIN 组成格式为 0 时存在 ID 码明文，Expanded Hex 格式
PINBLOCK 格式	2 N	仅当公钥加密 PIN 格式组成格式为 10 时存在 公钥加密 PINBLOCK 的格式代码，参见 **5 PINBLOCK(数字)格式**
公钥加密的填充模式	2 N	标识公钥加密 PIN 数据块时采用的填充模式，仅当公钥算法标识为 01 时存在； 01 - PKCS#1 v1.5 填充方式 07 - 在 PIN 数据块前面补 0x00，以使数据长度等于 RSA 密钥模长
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	N8
错误码	2 A	00：成功 01：公钥 MAC 验证失败 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 23：非法的 PIN 组成格式 24：非法的 PIN 长度 39：非法的填充模式 41：无主密钥或加密卡运算单元错误 45：密钥不存在
公钥加密的 PIN 密文长度	4 N	标识公钥加密的 PIN 数据块密文的长度，字节数
公钥加密的 PIN 密文	n B	公钥加密的 PIN 数据块密文

3.3.7.9. 公钥加密的数字 PIN 密文转为 ZPK 加密（N8）

该指令支持数字类型的 PIN 密文转换。通常用于网银系统中用户 PIN 的密文转换。

ZPK 加密 PIN 数据块时采用 ECB 模式。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	N8
公钥算法标识	2 N	标识公钥加密字符 PIN 时采用的非对称算法 01 - RSA 07 - SM2
私钥索引	4 N	用于解密（公钥加密的）PIN 密文的私钥索引号，0001-0064 9999 标识使用私钥使用下面两个域的值。
私钥长度	4 N	下个域的长度，仅当私钥索引号为 9999 时存在；
私钥	n B	LMK 加密的私钥密文，仅当私钥索引号为 9999 时存在；
公钥加密PIN组成格式	2 N	标识公钥加密 PIN 时的 PIN 数据块组成格式 00 - ID 长度(2N)+ID 码+PIN 长度(2N)+PIN 明文 01 - PIN 明文块
公钥加密的填充模式	2 N	标识公钥加密 PIN 数据块时采用的填充模式，仅当公钥算法标识为 01 时存在； 01 - PKCS#1 v1.5 填充方式 07 - 在 PIN 数据块前面补 0x00，以使数据长度等于 RSA 密钥模长
密钥扩展标识	1A	‘P’,可选域
密钥扩展类型	1N	当密钥扩展标识存在时存在，0-ZPK，1-EDK
ZPK 密钥	K + 4N / 16 H / 1 A + 32 H / 1 A + 48 H	用于加密 PIN 的 ZPK 密钥索引或密文
PINBLOCK 格式	2 N	ZPK 加密 PINBLOCK 的格式代码，参见 **5 PINBLOCK(数字)格式**
账号 PAN	12/18 N	用户主账号 当 PIN 数据块格式为 04 时，该域为 18N，去除校验位的 18 位主账号，不足 18 位则右对齐左填 F； 当 PIN 数据块格式为其他值时，该域为 12N；
公钥加密的PIN密文长度	4 N	标识公钥加密的 PIN 数据块密文的长度，字节数
公钥加密的 PIN 密文	n B	公钥加密的 PIN 数据块密文
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	N9
错误码	2 A	00：成功 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 23：非法的 PIN 组成格式 24：非法的 PIN 长度 39：非法的填充模式 41：无主密钥或加密卡运算单元错误 45：密钥不存在

明文 PIN 长度	2 N	PIN 明文的长度，04-20
ZPK 加密的 PIN 密文长度	2 N	标识 ZPK 加密的 PIN 数据块密文的长度，字节数
ZPK 加密的 PIN 密文	n*2 H	ZPK 加密的 PIN 数据块密文，Expanded Hex 格式 ZPK 为 64 位分组算法密钥时，PIN 密文结果为 16H； ZPK 为 128 位分组算法密钥时，PIN 密文结果为 32H；
ID 码长度	2 N	仅当公钥加密 PIN 组成格式为 0 时存在 01-20
ID 码	n*2 H	仅当公钥加密 PIN 组成格式为 0 时存在 ID 码明文，Expanded Hex 格式

3.3.7.10. 将数字 PIN 从 ZPK 下加密转换到私有算法加密（CB）

当用户系统中的 PIN 采用私有算法加密存储时，密码机可使用该指令将前端送来的 ZPK 加密的 PINBLOCK 密文转换为客户私有算法加密的密文用以做 PIN 验证。

域	长度&类型	描述
	命令报文	
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	CB
源 ZPK 密钥	K + 4 N / 16 H / 1A + 32 H / 1A + 48 H	用于加密 PIN 的源 ZPK 密钥索引或密文
目标PIN加密密钥类型	3 H	采用私有算法加密 PIN 的目标密钥类型 001 - ZPK; 002 - PVK; 05,06 算法密钥类型为 PVK
目标 PIN 加密密钥	K + 4N / 16 H / 1A + 32 H / 1A + 48 H	用于加密 PIN 的目标密钥索引或密文
最大 PIN 长度	2 N	取值 12
源 PINBLOCK 密文	16 H / 32 H	在源 ZPK 下加密的 PINBLOCK 密文 源 ZPK 密钥方案为 R/P/L：32H，其它 16H
源 PINBLOCK 格式	2 N	源 ZPK 下加密 PIN 数据块的格式代码，参见 5PINBLOCK(数字)格式
源 PINBLOCK 所用账号	12 N / 18 N	源 ZPK 下加密 PIN 块时使用的用户主账号 当 PIN 数据块格式为 04 时，该域为 18N，去除校验位的 18 位主账号，不足 18 位则右对齐左填 F； 当 PIN 数据块格式为其他值时，该域为 12N，去除校验位的最右 12 位主账号；
私有PIN加密算法标识	2 N	标识采用私有算法加密 PIN 的算法： 01 - 乌海银行特殊 DES 算法； 02 - 浙商银行电话项目私有算法； 03 - 山西农信 PINBLOCK 加密算法； 04 - 张家港农商行 PINBLOK 转私有算法 pin 密文 05 - 苏州银行新核心算法 PIN 06 - 苏州银行无账号新核心算法 PIN 07 - BCD 拓展 pin 且按 PKCS#5 标准填充至分组长度 08~99，预留（当前版本不支持）。
日期	8 N	可选域，仅当“私有 PIN 加密算法标识”取值为 01 时存在 日期格式为 yyyymmdd

附加弱口令验证标识	1 A	取值 Y 或 N ● 不存在或为 N 时，不附加弱口令验证。 ● 取值为 Y 时，需验证附加弱口令 当“私有 PIN 加密算法标识” 为 “06 - 苏州银行新核心算法 PIN”时存在。
弱口令个数	2 H	需比对的弱口令个数（1-10） 当“附加弱口令验证标识”为 Y 时存在
弱口令长度	2 N	每个弱口令的长度，4-12，长度相同 当“附加弱口令验证标识”为 Y 时存在
弱口令集	N A	弱口令串，根据以上两个域确定 当“附加弱口令验证标识”为 Y 时存在
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	CC
错误码	2 A	00：成功 01：弱口令长度与解密出来的 PIN 明文长度不等 03：不支持的加密算法标识 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 23：非法的 PIN BLOCK 格式 24：非法的 PIN 长度 41：无主密钥或加密卡运算单元错误 45：密钥不存在 99：弱口令
PIN 长度	2 N	返回的 PIN 长度
目标 PINBLOCK 密文	n B/12N	在目标密钥下加密的 PIN 密文 当私有 PIN 加密算法标识为 05/06 时为 12N,其余为 n B

3.3.7.11. 弱口令校验（CP）

该指令支持数字格式的 PIN 明文校验

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	CP
密钥类型	3 H	解密 PIN 的密钥类型 001 - ZPK; 002 - TPK;
ZPK/TPK 密钥	K + 4N / 16 H / 1A + 32 H / 1A + 48 H	用于解密 PIN 的 ZPK/TPK 密钥索引或密文
通用 PIN 格式或私有 PIN 格式标识	1 N	0:通用 PINBLOCK 格式 1:私有 PINBLOCK 格式
PINBLOCK 格式	2 N	源 ZPK 下加密 PIN 数据块的格式代码 (当格式标识为 0 存在) 通用 PINBLOCK 格式: PINBLOCK(数字)格式 (当格式标识为 1 存在)

		私有算法加密 PIN 的算法： 03 – 山西农信　PINBLOCK　加密算法； 其他，预留（当前版本不支持）
PIN 密文长度	2N	可选域； 当 PIN 格式标识为 1,且 PINBLOCK 格式为 03 时存在。
PINBLOCK 密文	16 H / 32 H nB	在源 ZPK 下加密的 PINBLOCK 密文 通用格式下：源 ZPK 密钥方案为 R/P/L：32H，其它 16H 私有格式 03 为 nB
源 PINBLOCK 所用账号	12 N / 18 N	可选域； 当通用 PINBLOCK 格式时存在 用户主账号 当 PIN 数据块格式为 04 时，该域为 18N，去除校验位的 18 位主账号，不足 18 位则右对齐左填 F； 当 PIN 数据块格式为其他值时，该域为 12N，去除校验位的最右 12 位主账号；
附加弱口令验证标识	1 A	取值 Y 或 N ● 不存在或为 N 时，不附加弱口令验证。 ● 取值为 Y 时，需验证附加弱口令
弱口令个数	2 H	需比对的弱口令个数（1-10） 当“附加弱口令验证标识”为 Y 时存在
弱口令长度	2 N	每个弱口令的长度，4-12，长度相同 当“附加弱口令验证标识”为 Y 时存在
弱口令集	N A	弱口令串，根据以上两个域确定 当“附加弱口令验证标识”为 Y 时存在
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	CQ
错误码	2 A	**00：成功（非弱口令）** **99：错误（弱口令）** 01：弱口令长度与解密出来的 PIN 明文长度不等 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 12：数据库获取弱口令出错 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 23：非法的 PIN BLOCK 格式 24：非法的 PIN 长度 41：无主密钥或加密卡运算单元错误 45：密钥不存在

假设数据库为空，则先调用指令 SP 设置弱口令集

SP
02
08
0000000011111111

示例 1. 不带附加弱口令验证，解密后 PIN 明文为 01234567，若 PIN 该值不在弱口令列表中，则返回 CQ00：

[
CP
001
Z8B4ECCAE01B4B17A
1

```
    03
    08
    &FECE28F58618B10A!
    |
    CQ
    00
]
```

示例 2. 带附加弱口令验证，解密后 PIN 明文为 01234567，若 PIN 该值不在弱口令列表中，也不在附加弱口令集中，则返回 CQ00，若该 PIN 值存在于其中一个弱口令列表中，则返回 CQ99：

```
    [
    CP
    001
    Z8B4ECCAE01B4B17A
    1
    03
    08
    &FECE28F58618B10A!
    y
    02
    08
    0123456722222222
    |
    CQ
    99
]
```

3.3.7.12. 设置弱口令集（SP）

设置弱口令集，每次设置覆盖更新之前的弱口令，该指令需主机 PIN 解密类授权

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	SP
弱口令个数	2 H	设置的弱口令个数
弱口令长度	2 N	每个弱口令的长度，4-12，长度相同
弱口令集	N A	弱口令串，根据以上两个域确定
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	SQ
错误码	2 A	00：成功（非弱口令） 15：失败 24：PIN 长度不在 4-12 内

3.3.7.13. ZPK 加密数字 PIN（BB）

明文数字 PIN 由 ZPK 直接加密输出

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	BB
ZPK 密钥	K + 4N / 16 H / 1 A + 32 H/ 1 A + 48 H/ 1A + 64 H	用于加密 PIN 的 ZPK 的密钥索引或密文
PIN 格式	2N	PIN 格式代码
PIN 明文	LN	数字 PIN 明文
账号	12 N	用户主账号有效位的最右 12 个数字
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	BC
错误码	2 A	00：成功 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 22：非法的 PIN 明文数字或账号数字 23：非法的 PIN 数据块格式代码
PIN 密文	16H/32H	在 ZPK 密钥下加密的 PINBLOCK 密文 ZPK 密钥方案为 R/P/L 时该域为 32H，否则 16H

3.3.7.14. 数字 PINBLOCK 私有算法转加密（CJ）

私有算法加密下的 PIN 密文转为 ZPK 加密的 PIN 密文

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	CJ
源 PIN 加密密钥类型	3 H	采用私有算法加密 PIN 的密钥类型 001 - ZPK; 002 - PVK;
源 PIN 加密密钥	K + 4N / 16 H / 1A + 32 H / 1A + 48 H	用于加密 PIN 的密钥索引或密文
源 PIN 加密算法标识	2 N	标识采用私有算法加密 PIN 的算法： 03 - 山西农信 PINBLOCK 加密算法； 01，02，04~99，预留（当前版本不支持）。
源 PIN 密文长度	2 N	私有算法加密 PIN 的密文长度
源 PIN 密文	n B	长度由源 PIN 密文长度确定
目标 ZPK 密钥	K + 4 N / 16 H / 1A + 32 H / 1A + 48 H	用于加密 PIN 的 ZPK 密钥索引或密文
最大 PIN 长度	2 N	取值 12
目标 PINBLOCK 格式	2 N	ZPK 下加密 PIN 数据块的格式代码，参见 5PINBLOCK(数

		字)格式
目标 PINBLOCK 所用账号	12 N / 18 N	目标 ZPK 下加密 PIN 块时使用的用户主账号 当 PIN 数据块格式为 04 时，该域为 18N，去除校验位的 18 位主账号，不足 18 位则右对齐左填 F； 当 PIN 数据块格式为其他值时，该域为 12N，去除校验位的最右 12 位主账号；
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	CK
错误码	2 A	00：成功 03：不支持的加密算法标识 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 23：非法的 PIN BLOCK 格式 24：非法的 PIN 长度 41：无主密钥或加密卡运算单元错误 45：密钥不存在
目标 PINBLOCK 密文	16 H/ 32H	目标 ZPK 密钥方案为 R/P/L:32H，其它 16H

3.3.8. 其他功能报文

3.3.8.1. 产生随机数（CR）

产生指定长度的随机数。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机。
命令代码	2 A	CR
随机数长度	4 N	随机数的长度，取值 0001-2048
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	CS
错误码	2 A	00：成功 15：无效的输入数据（无效的格式/字符或长度错误） 41：无主密钥或加密卡运算单元错误 80：非法的数据长度
随机数	n B	n 为随机数长度

3.3.8.2. 获取密码机运行状态（NP）

获取密码机的运行状态，用于设备诊断、审计等。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机。

命令代码	2 A	NP
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	NQ
错误码	2 A	00：成功 41：无主密钥或加密卡运算单元错误
设备自检状态	8 H	每位代表下面每项自检结果：1-正常，0-自检失败 0 - 设备主密钥是否 OK； 1 - 设备服务状态是否 OK； 2-7，预留
当前支持的最大连接数	4 H	
当前已被占用的连接数	4 H	
CPU 利用率	6 A	示例“00.10%”
内存使用率	6 A	示例“16.07%”
开机后总业务数	16 H	

3.3.8.3. 查询/增加屏蔽指令（SF）

可以用于禁用含解密功能指令

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	SF
功能选项	1N	0 - 查询已被屏蔽指令 1 - 增加需要屏蔽的指令
待屏蔽指令	2A	仅当功能选项为 1 时存在
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	SG
错误码	2 A	00：成功 66：功能选项错误 15：无效的输入数据（无效的格式/字符或长度错误） 46：指令已屏蔽，无需重复设置 21：设置屏蔽的指令超过最大个数(100 个) 45：配置文件不存在(未设置过该指令,第一次查询时可能出现该错)
已被屏蔽的指令个数	3N	仅当功能选项为 0 时存在(最大 100)
已被屏蔽的指令	n*3A	被屏蔽的指令，以|分割 仅当功能选项为 0 时存在

3.4. 雷卡（RACAL）兼容主机命令

3.4.1. 工作密钥管理

【说明】

该版本密码机对 RACAL 工作密钥增加了 SM4 算法的支持，但工作密钥在 LMK 下加密的标识和在 ZMK 下加密的标识必须符合如下的特定规则。

密钥算法标识见“2.2.3 对称密钥算法标识”章节，名词约定如下：

- keyscheme_lmk，工作密钥在 LMK 下加密的标识；
- keyscheme_zmk，工作密钥在 ZMK 下加密的标识；
- zmkscheme_lmk，ZMK 在 LMK 下加密的标识；

在产生密钥和密钥导入导出时，上述 3 个标识是相互约束的，规则如下：

1) keyscheme_lmk 为 Z，即工作密钥为单长度 DES 密钥类型，仅允许被 DES/3DES 的 ZMK 保护导入导出，且其在 ZMK 下加密的标识必须为 Z。
   a) 若 zmkscheme_lmk 为 R、P、L，则返回 26 错（密钥标识错）；
   b) 否则，keyscheme_zmk 必须为 Z。此时与 RACAL 标准处理一致；
2) keyscheme_lmk 为 X 或 U，即双长度 3DES 密钥类型，允许被任意算法类型的 ZMK 保护导入导出。但当 ZMK 为 128 分组算法时，使用对应的该算法直接加密工作密钥，且工作密钥在 ZMK 下加密的标识必须为 X。
   a) 若 zmkscheme_lmk 为 R、P、L，则 keyscheme_zmk 必须为 X。此时 ZMK 直接使用对应的算法加密密钥明文输出；
   b) 否则，keyscheme_zmk 必须为 X 或 U。此时与 RACAL 标准处理一致；
3) keyscheme_lmk 为 Y 或 T，即三长度 3DES 密钥类型，仅允许被 DES/3DES 的 ZMK 保护导入导出，且其在 ZMK 下加密的标识必须为 Y 或 T。
   a) 若 zmkscheme_lmk 为 R、P、L，则返回 26 错（密钥标识错）；
   b) 否则，keyscheme_zmk 必须为 Y 或 T。此时与 RACAL 标准处理一致；
4) keyscheme_lmk 为 R、P、L，即 128 位分组算法密钥类型，允许被任意算法类型的 ZMK 保护导入导出，但 keyscheme_zmk 必须与 keyscheme_lmk 一致。
   a) keyscheme_zmk 必须与 keyscheme_lmk 一致。此时不限 zmkscheme_lmk 标识，直接使用 ZMK 密钥采用其标识对应的算法加密密钥明文；
   b) 否则，返回 26 错（密钥标识错）；

3.4.1.1. 产生工作密钥（A0）

随机产生一个工作密钥，输出 LMK 加密的密钥密文，可选的输出 ZMK 下加密的密文。

如果存储到密码机内，需满足主机服务的密钥管理权限。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**A0**
产生模式	1 H	0 - 产生密钥 1 - 产生密钥并在 ZMK 下加密
密钥类型	3 H	工作密钥类型 000 - ZMK/KEK; 001 - ZPK; 002 - PVK/TPK/TMK; 402 - CVK; 003 - TAK; 008 - ZAK; 009 - BDK; 109 - MK-AC/MDK; 209 - MK-SMI; 309 - MK-SMC; 409 - MK-DAK; 509 - MK-DN; 00A - ZEK/DEK; 00B - TEK; 10C - HMAC; 011 - KMC;
密钥标识(LMK)	1 A	在 LMK 下加密的密钥密文标识，Z/X/Y/U/T/P/L/R
ZMK 密文	K + 4N / 16 H / 1A + 32H / 1A + 48H	ZMK 密钥索引或 $LMK_{006-008}$ 下加密的 ZMK 密文 仅当产生模式为 1 时存在
密钥标识(ZMK)	1 A	在 ZMK 下加密的密钥密文标识，Z/X/Y/P/L/R 仅当产生模式为 1 时存在
密钥存储标识	1 A	可选域。 （1）取值’K’，表明密钥产生后存储在加密机中，当选择此值，后续域“密钥索引”、“密钥标签长度“、“密钥标签”必须存在。 （2）此项为空（没有任何数据），表明密钥不保存加密机中，而是由 LMK 加密后输出密文。
密钥索引	4 N	可选域。仅当密钥存储标识域存在时存在该域 存储到密码机内的密钥索引号，0001 - 2048
密钥标签长度	2 N	可选域，仅当密钥存储标识域存在时存在该域 取值：00-16
密钥标签	0-16 A	可选域。仅当密钥存储标识域存在时存在该域 用于在密钥内部存储时标记密钥的标签说明，0-16 个 ASCII 字符
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**A1**
错误码	2 A	00：成功 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 26：非法的密钥标识 32：非法的产生模式 41：无主密钥或加密卡运算单元错误 45：密钥不存在
密钥密文(LMK)	16 H / 1A + 32 H / 1A + 48 H	LMK 对应分组下加密的密钥密文

密钥密文(ZMK)	16 H / 1A + 32 H / 1A + 48 H	ZMK 加密的密钥密文 仅当产生模式为 1 时存在
密钥校验值	16 H	新产生密钥的校验值

示例 1. 产生随机的 ZMK 密钥，SM1 算法

```
[
A0
0
000
P
|
A1
00
P3BDCBDD298AD88E07BF7B01F89A6536A
7DA5F38574A1A2D2
]
```

示例 2. 产生随机的 ZPK 密钥并在 ZMK 下加密，3DES 算法

```
[
A0
1
001
U
X801617441513A2F135AB14EAAD1069DF
X
|
A1
00
UA8B358A59A737872D348E74B369BAAE4
XF663276551E51A36E1FDBB326AC44783
7660692C7B85AFF7
]
```

3.4.1.2. 由密文成份合成一个密钥（A4）

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**A4**
密钥成分	1 N	成分个数（2-8）
密钥类型	3 H	密钥类型 000 - ZMK　　001 - ZPK 002 - PVK/TPK/TMK　　003 - TAK 008 - ZAK　　00A - ZEK 109 - MDK　　402 - CVK
密钥标识(LMK)	1 A	在 LMK 下加密的密钥密文标识，Z/X/Y/U/T/
密钥成份 1	16 H / 1A + 32 H / 1A + 48 H	加密的密钥成份 1
密钥成份 2	16 H / 1A + 32 H / 1A + 48 H	加密的密钥成份 2

密钥成份 n	16 H / 1A + 32 H / 1A + 48 H	加密的密钥成份 n
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	A5
错误码	2 A	00：成功 04：非法的密钥类型 05：密钥长度与密钥成份长度不一致 其他：参见**错误码说明**
密钥密文(LMK)	16 H / 1A + 32 H / 1A + 48 H	LMK 对应分组下加密的密钥密文
密钥校验值	8 H	密钥校验值

3.4.1.3. 导入密钥（A6）

导入 ZMK 加密的密钥，即 ZMK 加密的密钥转换为 LMK 下加密。

如果存储到密码机内，需满足主机服务的密钥管理权限。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	A6
密钥类型	3 H	被导入的密钥类型 000 - ZMK/KEK; 001 - ZPK; 002 - PVK/TPK/TMK; 402 - CVK; 003 - TAK; 008 - ZAK; 009 - BDK; 109 - MK-AC/MDK; 209 - MK-SMI; 309 - MK-SMC; 409 - MK-DAK; 509 - MK-DN; 00A - ZEK/DEK; 00B - TEK; 10C - HMAC; 011 - KMC;
ZMK 密文	K + 4N / 16 H / 1 A + 32 H / 1 A + 48 H	ZMK 密钥索引或 $LMK_{006-008}$ 下加密的 ZMK 密文
ZMK 下加密的密钥	16 H / 1 A + 32 H / 1 A + 48 H	ZMK 下加密的密钥密文
密钥标识(LMK)	1 A	在 LMK 下加密的密钥密文标识，Z/X/Y/U/T/P/L/R
密钥存储标识	1 A	可选域。 （1）取值’K’，表明密钥产生后存储在加密机中，当选择此值，后续域“密钥索引”、“密钥标签长度“、“密钥标签”必须存在。 （2）此项为空（没有任何数据），表明密钥不保存加密机中，而是由 LMK 加密后输出密文。
密钥索引	4 N	可选域。仅当密钥存储标识域存在时存在该域

		存储到密码机内的密钥索引号，0001 - 2048
密钥标签长度	2 N	可选域，仅当密钥存储标识域存在时存在该域 取值：00-16
密钥标签	0-16 A	可选域。仅当密钥存储标识域存在时存在该域 用于在密钥内部存储时标记密钥的标签说明，0-16 个 ASCII 字符
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	A7
错误码	2 A	00：成功 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 26：非法的密钥标识 41：无主密钥或加密卡运算单元错误 45：密钥不存在
密钥密文(LMK)	16 H / 1 A + 32 H / 1 A + 48 H	LMK 下加密的密钥密文
密钥校验值	16 H	密钥校验值

3.4.1.4. 导出密钥（A8）

LMK 加密的密钥转换成 ZMK 下加密导出。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	A8
密钥类型	3 H	密钥类型 000 - ZMK/KEK; 001 - ZPK; 002 - PVK/TPK/TMK; 402 - CVK; 003 - TAK; 008 - ZAK; 009 - BDK; 109 - MK-AC/MDK; 209 - MK-SMI; 309 - MK-SMC; 409 - MK-DAK; 509 - MK-DN; 00A - ZEK/DEK; 00B - TEK; 10C - HMAC; 011 - KMC;
ZMK 密文	K + 4N / 16 H / 1A + 32 H / 1A + 48 H	ZMK 密钥索引或 $LMK_{006-008}$ 下加密的 ZMK 密文
LMK 下加密的密钥	K + 4N / 16 H / 1A + 32 H / 1A + 48 H	密钥索引或 LMK 下加密的密钥密文
密钥标识(ZMK)	1 A	在 ZMK 下加密的密钥标识，Z/X/Y/P/L/R
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	A9

错误码	2 A	00：成功 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 26：非法的密钥标识 41：无主密钥或加密卡运算单元错误 45：密钥不存在
密钥密文(ZMK)	16 H / 1A + 32 H / 1A + 48 H	ZMK 下加密的密钥密文
密钥校验值	16 H	密钥校验值

3.4.1.5. 产生一个 ZPK（IA）

产生随机的 ZPK，在 ZMK 和 LMK 下加密输出。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	IA
ZMK 密文	K + 4N / 16 H / 1 A + 32 H / 1 A + 48 H	ZMK 密钥索引或 $LMK_{006-008}$ 下加密的 ZMK 密文
分隔符	1 A	可选项，如果存在，下面的三个域必须存在。值为“;”。如果其中的一个选项不需要，则用一个有效值或 0 填充
密钥标识(ZMK)	1 A	可选项。ZMK 下加密的密钥标识
密钥标识(LMK)	1 A	可选项。LMK 下加密的密钥标识
密钥校验值类型(KCV)	1 A	可选项。密钥校验的生成方式 0 - KCV 16H 1 - KCV 6H
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	IB
错误码	2 A	00：成功 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 26：非法的密钥标识 32：非法的密钥校验值类型 41：无主密钥或加密卡运算单元错误 45：密钥不存在
ZPK 密文(ZMK)	16 H / 1 A + 32 H / 1 A + 48 H	ZMK 加密的 ZPK 密钥密文
ZPK 密文(LMK)	16 H / 1 A + 32 H / 1 A + 48 H	LMK_{09-11} 加密的 ZPK 密钥密文

密钥校验值	16 H / 6 H	用 ZPK 加密一个分组全 0 的结果，加密的算法取决于密钥在 LMK 下加密的密钥标识； 16H 还是 6H 取决于 KCV 的类型选项

3.4.1.6. ZPK 从 ZMK 加密转换为 LMK 加密（FA）

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机。
命令代码	2 A	FA
ZMK 密文（LMK）	K + 4N / 16 H / 1 A + 32 H / 1 A + 48 H	ZMK 密钥索引或 $LMK_{006-008}$ 下加密的 ZMK 密文
ZPK 密文（ZMK）	16 H / 1 A + 32 H / 1 A + 48 H	ZMK 下加密的 ZPK 密文
分隔符	1 A	可选项，如果存在，下面的三个域必须存在。值为“;”。 如果其中的一个选项不需要，则用一个有效值或 0 填充。
密钥标识(ZMK)	1 A	可选项. ZMK 下加密的 ZPK 的密钥标识
密钥标识(LMK)	1 A	可选项. LMK 下加密的 ZPK 的密钥标识
密钥校验值(KCV)	1 A	可选项.密钥校验值计算方法 0 - KCV 16H 1 - KCV 6H
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	FB
错误码	2 A	00：成功 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 26：非法的密钥标识 32：非法的密钥校验值类型 41：无主密钥或加密卡运算单元错误 45：密钥不存在
ZPK 密文（LMK）	16 H / 1 A + 32 H / 1 A + 48 H	LMK_{09-11} 加密的 ZPK 密钥密文
密钥校验值	16 H / 6 H	用 ZPK 加密一个分组全 0 的结果，加密的算法取决于密钥在 LMK 下加密的密钥标识； 16H 还是 6H 取决于 KCV 的类型选项

3.4.1.7. ZPK 从 LMK 加密转换为 ZMK 加密（GC）

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机。
命令代码	2 A	GC
ZMK 密文（LMK）	K + 4N /	ZMK 密钥索引或 $LMK_{006-008}$ 下加密的 ZMK 密文

	16 H / 1 A + 32 H / 1 A + 48 H	
ZPK 密文（LMK）	K + 4N / 16 H / 1 A + 32 H / 1 A + 48 H	ZPK 密钥索引或 $LMK_{009-011}$ 加密的 ZPK 密钥密文
分隔符	1 A	可选项，如果存在，下面的三个域必须存在。值为“;”。如果其中的一个选项不需要，则用一个有效值或 0 填充。
密钥标识(ZMK)	1 A	可选项. ZMK 下加密的 ZPK 的密钥标识
密钥标识(LMK)	1 A	可选项. LMK 下加密的 ZPK 的密钥标识
密钥校验值(KCV)	1 A	可选项.密钥校验值计算方法 0 - KCV 16H 1 - KCV 6H
响应报文		
报文头	n A	不做任何修改直接返回给主机。
响应代码	2 A	GD
错误码	2 A	00：成功 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 26：非法的密钥标识 32：非法的密钥校验值类型 41：无主密钥或加密卡运算单元错误 45：密钥不存在
ZPK 密文（ZMK）	16 H / 1 A + 32 H / 1 A + 48 H	ZMK 下加密的 ZPK 密文
密钥校验值	16 H / 6 H	用 ZPK 加密一个分组全 0 的结果，加密的算法取决于密钥在 LMK 下加密的密钥标识； 16H 还是 6H 取决于 KCV 的类型选项

3.4.1.8. 产生一个 ZEK/ZAK（FI）

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机。
命令代码	2 A	FI
密钥类型标志	1 N	0 - ZEK 1 - ZAK
ZMK 密文	K + 4N / 16 H / 1 A + 32 H / 1 A + 48 H	ZMK 密钥索引或 $LMK_{006-008}$ 下加密的 ZMK 密文
分隔符	1 A	可选项，如果存在，下面的三个域必须存在。值为“;”。如果其中的一个选项不需要，则用一个有效值或 0 填充。
密钥标识(ZMK)	1 A	可选项. ZMK 下加密的 ZEK/ZAK 的密钥标识
密钥标识(LMK)	1 A	可选项. LMK 下加密的 ZEK/ZAK 的密钥标识
密钥校验值类型	1 A	可选项.密钥校验值计算方法 0 - KCV 16H

		1 - KCV 6H
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	FJ
错误码	2 A	00：成功 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 26：非法的密钥标识 32：非法的密钥校验值类型 41：无主密钥或加密卡运算单元错误 45：密钥不存在
密钥密文（ZMK）	16 H / 1 A + 32 H / 1 A + 48 H	ZMK 加密的 ZEK/ZAK 密钥密文
密钥密文（LMK）	16 H / 1 A + 32 H / 1 A + 48 H	LMK 加密的 ZEK/ZAK 密钥密文
密钥校验值	16 H / 6 H	用 ZEK/ZAK 加密一个分组长度 0 的结果 16H 还是 6H 取决于 KCV 的类型选项

3.4.1.9. ZEK/ZAK 从 ZMK 加密转换为 LMK 加密（FK）

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机。
命令代码	2 A	FK
密钥类型标志	1 N	0 - ZEK 1 - ZAK
ZMK 密文	K + 4N / 16 H / 1 A + 32 H / 1 A + 48 H	ZMK 密钥索引或 $LMK_{006-008}$ 下加密的 ZMK 密文
ZEK/ZAK 密文（ZMK）	16 H / 1 A + 32 H/ 1 A + 48 H	ZMK 下加密的 ZAK 或 ZEK
分隔符	1 A	可选项，如果存在，下面的三个域必须存在。值为“;”。 如果其中的一个选项不需要，则用一个有效值或 0 填充。
密钥标识(ZMK)	1 A	可选项. ZMK 下加密的 ZEK/ZAK 的密钥标识
密钥标识(LMK)	1 A	可选项. LMK 下加密的 ZEK/ZAK 的密钥标识
密钥校验值(KCV)	1 A	可选项. 密钥校验值计算方法 0 - KCV 16H 1 - KCV 6H
响应报文		
报文头	n A	不做任何修改直接返回给主机。
响应代码	2 A	FL
错误码	2 A	00：成功 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误）

		21：非法的密钥索引 26：非法的密钥标识 32：非法的密钥校验值类型 41：无主密钥或加密卡运算单元错误 45：密钥不存在
ZEK/ZAK 密文（LMK）	16 H / 1 A + 32 H / 1 A + 48 H	LMK 下加密的 ZEK/ZAK
密钥校验值	16 H / 6 H	用 ZEK/ZAK 加密一个分组长度 0 的结果 16H 还是 6H 取决于 KCV 的类型选项

3.4.1.10. ZEK/ZAK 从 LMK 加密转换为 ZMK 加密（FM）

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机。
命令代码	2 A	**FM**
密钥类型标志	1 N	0 - ZEK 1 - ZAK
ZMK 密文	K + 4N / 16 H / 1 A + 32 H / 1 A + 48 H	ZMK 密钥索引或 $LMK_{006-008}$ 下加密的 ZMK 密文
ZEK 密文（LMK）	K + 4N / 16 H / 1 A + 32 H / 1 A + 48 H	ZEK 密钥索引或 $LMK_{045-047}$ 下加密的 ZEK 密文 仅当标志为 0 时存在
ZAK 密文（LMK）	K + 4N / 16 H / 1 A + 32 H / 1 A + 48 H	ZAK 密钥索引或 $LMK_{039-041}$ 下加密的 ZAK 密文 当标志位 1 时存在
分隔符	1 A	可选项，如果存在，下面的三个域必须存在。值为“;”。 如果其中的一个选项不需要，则用一个有效值或 0 填充。
密钥标识 ZMK	1 A	可选项，ZMK 下加密的密钥标识
密钥标识 LMK	1 A	可选项，LMK 下加密的密钥标识
密钥校验值(KCV)	1 A	可选项.密钥校验值计算方法 0 - KCV 16H 1 - KCV 6H
响应报文		
报文头	n A	不做任何修改直接返回给主机。
响应代码	2 A	**FN**
错误码	2 A	00：成功 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 26：非法的密钥标识 32：非法的密钥校验值类型 41：无主密钥或加密卡运算单元错误 45：密钥不存在
ZEK/ZAK 密文（ZMK）	16 H /	ZMK 下加密的 ZEK/ZAK

	1 A + 32 H / 1 A + 48 H	
密钥校验值	16 H / 6 H	用 ZEK/ZAK 加密一个分组长度 0 的结果 16H 还是 6H 取决于 KCV 的类型选项

3.4.1.11. 产生一个 TMK, TPK, PVK（HC）

产生一个随机 TMK/TPK/PVK 密钥，在 TMK 和 LMK 下加密输出。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	HC
TMK 密文	K + 4N / 16 H / 1A + 32 H / 1A + 48 H	TMK 密钥索引或 $LMK_{021-023}$ 下加密的 TMK 密文
分隔符	1 A	可选项，如果存在，下面的三个域必须存在。值为“;”。 如果其中的一个选项不需要，则用一个有效值或 0 填充。
新密钥标识(TMK)	1 A	可选项。TMK 下加密的新密钥标识
新密钥标识(LMK)	1 A	可选项。LMK 下加密的新密钥标识
密钥校验值类型	1 A	可选项。密钥校验值计算方法 0 - KCV 16H 1 - KCV 6H
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	HD
错误码	2 A	00：成功 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 26：非法的密钥标识 32：非法的密钥校验值类型 41：无主密钥或加密卡运算单元错误 45：密钥不存在
密钥密文(TMK)	16 H / 1A + 32 H / 1A + 48 H	TMK 下加密的新 TMK/TPK/PVK 密钥密文
密钥密文(LMK)	16 H / 1A + 32 H / 1A + 48 H	LMK_{21-23} 下加密的新 TMK/TPK/PVK 密文
密钥校验值	16H / 6H	用新产生的密钥加密一个分组长度 0 的结果 16H 还是 6H 取决于 KCV 的类型选项

3.4.1.12. 产生一个 TAK（HA）

产生一个随机的 TAK，使用 TMK/TPK/PVK 加密。

域	长度&类型	描述

命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**HA**
TMK 密文	K + 4N / 16 H / 1A + 32 H / 1A + 48 H	TMK 密钥索引或 $LMK_{021-023}$ 下加密的 TMK 密文
分隔符	1 A	可选项，如果存在，下面的三个域必须存在。值为“;”。如果其中的一个选项不需要，则用一个有效值或 0 填充。
密钥标识(TMK)	1 A	可选项。TMK 下加密的新密钥标识
密钥标识(LMK)	1 A	可选项。LMK 下加密的新密钥标识
密钥校验值(KCV)	1 A	可选项。密钥校验值计算方法 0 - KCV 16H 1 - KCV 6H
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**HB**
错误码	2 A	00：成功 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 26：非法的密钥标识 32：非法的密钥校验值类型 41：无主密钥或加密卡运算单元错误 45：密钥不存在
密钥密文(TMK)	16 H / 1A + 32 H / 1A + 48 H	TMK 加密的密钥密文
密钥密文(LMK)	16 H / 1A + 32 H / 1A + 48 H	LMK 加密的密钥密文
密钥校验值	16H / 6H	用 TAK 加密一个分组长度 0 的结果 16H 还是 6H 取决于 KCV 的类型选项

3.4.1.13. 将 TAK 从 ZMK 下加密转为 LMK 下加密（MI）

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**MI**
ZMK 密文（LMK）	K + 4N / 16 H / 1 A + 32 H / 1 A + 48 H	ZMK 密钥索引或 LMK006-008 下加密的 ZMK 密文
TAK 密文（ZMK）	16 H / 1 A + 32 H / 1 A + 48 H	ZMK 下加密的 TAK 密文
分隔符	1 A	可选项，如果存在，下面的三个域必须存在。值为“;”。如果其中的一个选项不需要，则用一个有效值或 0 填充。

密钥标识(ZMK)	1 A	可选项. ZMK 下加密的 ZPK 的密钥标识
密钥标识(LMK)	1 A	可选项. LMK 下加密的 ZPK 的密钥标识
密钥校验值(KCV)	1 A	可选项.密钥校验值计算方法 0 - KCV 16H 1 - KCV 6H
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	MJ
错误码	2 A	00：成功 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 26：非法的密钥标识 32：非法的密钥校验值类型 41：无主密钥或加密卡运算单元错误 45：密钥不存在
TAK 密文（LMK）	16 H / 1 A + 32 H / 1 A + 48 H	LMK 加密的 TAK 密钥密文
密钥校验值	16 H / 6 H	用 TAK 加密一个分组全 0 的结果，加密的算法取决于密钥在 LMK 下加密的密钥标识； 16H 还是 6H 取决于 KCV 的类型选项

3.4.1.14. 生成密钥校验值（BU）

为 LMK 加密的密钥生成密钥校验值。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	BU
密钥类型代码	2 H	标识加密密钥的 LMK 组: 00 - LMK 对 04-05 01 - LMK 对 06-07 02 - LMK 对 14-15 03 - LMK 对 16-17 07 - LMK 对 24-25 08 - LMK 对 26-27 09 - LMK 对 28-29 0A - LMK 对 30-31 0B - LMK 对 32-33 42 - LMK 对 14-15 的变种 4 FF - 使用位于分隔符之后的特定密钥类型
密钥长度标识	1 N	0 - 单倍长密钥，8 字节 DES 1 - 双倍长密钥，16 字节 3DES/SM1/SM4/AES 2 - 三倍长密钥，24 字节 3DES/AES 3 - 32 字节 AES
密钥密文	K + 4 N / 16 H / 1 A + 32 H / 1 A + 48 H /	指定的 LMK 对下加密的密钥密文

	1 A + 64 H	
分隔符	1 A	可选项，仅当密钥类型代码取值‘FF’时存在 取值：‘;’
密钥类型	3 H	仅当密钥类型代码取值‘FF’时，该域存在 查看密钥类型表
分隔符	1 A	可选项，仅当下述三个域存在时存在 取值：‘;’ 如果命令不需要一个可选域，则用一个有效值或 0 填充
密钥标识(ZMK)	1 A	可选项，在 ZMK 下加密的密钥密文标识
密钥标识(LMK)	1 A	可选项，在 LMK 下加密的密钥密文标识
密钥校验值类型	1 A	可选项，标识密钥校验值计算方式： 0 - 16H KCV，向后兼容 1 - 6H KCV
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**BV**
错误码	2 A	00：成功 04：非法的密钥类型代码（或索引内密钥类型不合法） 05：非法的密钥长度（或索引内密钥长度不符） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 41：无主密钥或加密卡运算单元错误 45：密钥不存在
密钥校验值	16 H / 6 H	对给定密钥生成的校验值

3.4.2. 消息认证（MAC 运算）

3.4.2.1. TAK 计算数据 MAC（MA）

使用 TAK 密钥对数据进行 MAC 计算。

采用模式 2 的填充规则（参见 4.1.3），MAC 算法根据密钥算法和长度选择：

- TAK 密钥为单长度 DES/SM1/AES/SM4，采用 ISO9797-1 MAC 算法 1（全密钥 CBC-MAC）；
- TAK 密钥为双长度 3DES，采用 ISO9797-1 MAC 算法 3；

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**MA**
TAK	K + 4N / 16 H / 1 A + 32 H	TAK 密钥索引或 $LMK_{024-026}$ 下加密的 TAK 密文
数据	0-n B	要产生 MAC 所用的数据，最大 4096 字节
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**MB**
错误码	2 A	00：成功

		04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 26：非法的密钥标识 41：无主密钥或加密卡运算单元错误 45：密钥不存在 80：非法的数据长度
MAC	16 H / 32 H	数据的 MAC 值 当 TAK 密钥标识为 Z/X/U 时，该域为 16H 当 TAK 密钥标识为 R/P/L 时，该域为 32H

3.4.2.2. TAK 验证数据 MAC（MC）

使用 LMK 加密的 TAK 对数据进行 MAC 校验。

采用模式 2 的填充规则（参见 4.1.3），MAC 算法根据密钥算法和长度选择：

- TAK 密钥为单长度 DES/SM1/AES/SM4，采用 ISO9797-1 MAC 算法 1（全密钥 CBC-MAC）；
- TAK 密钥为双长度 3DES，采用 ISO9797-1 MAC 算法 3；

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**MC**
TAK	K + 4N / 16 H / 1 A + 32 H	TAK 密钥索引或 $LMK_{024-026}$ 下加密的 TAK 密文
MAC	8 H	待验证的 MAC 数据
数据	0-n B	用于计算 MAC 的数据，最大 4096 字节
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**MD**
错误码	2 A	00：成功 01：MAC 验证失败 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 26：非法的密钥标识 41：无主密钥或加密卡运算单元错误 45：密钥不存在 80：非法的数据长度

3.4.2.3. ZAK 计算数据 MAC（MQ）

使用 LMK 加密的 ZAK 对数据进行 MAC 计算。

采用模式 2 的填充规则（参见 4.1.3），MAC 算法根据密钥算法和长度选择：

- ZAK 密钥为单长度 DES/SM1/AES/SM4，采用 ISO9797-1 MAC 算法 1（全密钥 CBC-MAC）；
- ZAK 密钥为双长度 3DES，采用 ISO9797-1 MAC 算法 3；

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**MQ**
报文块标识	1 N	0 - 唯一块 1 - 第一块 2 - 中间块 3 - 最后一块
ZAK 密钥密文	K + 4N / 16 H / 1 A + 32 H	ZAK 密钥索引或 $LMK_{039-041}$ 下加密的 ZAK 密文
IV	16 H / 32 H	用于计算 MAC/TAC 的初始向量 仅当报文块标识为 2/3 时有此域 当 ZAK 密钥标识为 Z/X/U 时，该域为 16H 当 ZAK 密钥标识为 R/P/L 时，该域为 32H
报文长度	3 H	报文的长度，字节数 取值 000-FFF（即 0-4095 字节）
报文	n B	报文数据
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**MR**
错误码	2 A	00：成功 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 26：非法的密钥标识 32：无效的报文块标识 41：无主密钥或加密卡运算单元错误 45：密钥不存在 80：非法的数据长度
MAC	16 H / 32 H	当报文块标识为 1 或 2 时，此域为下一个数据块的 IV 当报文块标识为 0 或 3 时，此域为数据的 MAC。 当 ZAK 密钥标识为 Z/X/U 时，该域为 16H 当 ZAK 密钥标识为 R/P/L 时，该域为 32H

3.4.2.4. ZPK 计算数据的 CBC-MAC（UQ）

用于银联应用系统中，在线分发 ZPK 时验证密钥的有效性。

采用模式 2 的填充规则（参见 4.1.3），MAC 算法采用 ISO9797-1 规范的 MAC 算法 1，即使用全密钥对 PADDING 后的数据进行 CBC 加密取最后一段密文作为 MAC 值。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机

命令代码	2 A	UQ
报文块标识	1 N	0 - 唯一块 1 - 第一块 2 - 中间块 3 - 最后一块
ZPK 密钥密文	K + 4N / 16 H / 1 A + 32 H	ZPK 密钥索引或 $LMK_{009-011}$ 下加密的 ZPK 密文
IV	16 H / 32 H	用于计算 MAC/TAC 的初始向量。 仅当报文块标识为 2/3 时有此域。 当密钥标识为 Z/X/U 时，该域为 16H 当密钥标识为 R/P/L 时，该域为 32H
报文长度	3 H	报文的长度，字节数 取值 000-FFF（即 0-4095 字节）
报文	n B	报文数据。
输出 MAC 长度	2 H	输出 MAC/TAC 值长度的字节数。0x01-0x10
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	UR
错误码	2 A	00：成功 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 32：无效的报文块标识 35：无效的输出 MAC 长度 41：无主密钥或加密卡运算单元错误 45：密钥不存在 80：非法的数据长度
MAC	n*2 H	当报文块标识为 1 或 2 时，此域为下一个数据块的 IV。 当报文块标识为 0 或 3 时，此域为数据的 MAC。

3.4.2.5. ZAK/TAK 计算数据的 CBC-MAC（MU）

用于银联应用系统中，在线分发 ZAK/TAK 时验证密钥的有效性。

采用模式 2 的填充规则（参见 4.1.3），MAC 算法采用 ISO9797-1 规范的 MAC 算法 1，即使用全密钥对 PADDING 后的数据进行 CBC 加密取最后一段密文作为 MAC 值。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机。
命令代码	2 A	MU
报文块标识	1 N	0 - 唯一块 1 - 第一块 2 - 中间块 3 - 最后一块
密钥类型	1 N	0 - TAK 1 - ZAK
密钥长度	1 N	0 - 8 字节，单长度 DES 密钥 1 - 16 字节，双长度 DES、SM1、SM4、AES 密钥

数据类型	1 N	0 - 二进制 1 - 扩展十六进制
TAK/ZAK	K + 4N / 16 H / 1 A + 32 H	TAK/ZAK 密钥索引或 LMK 下加密的 TAK/ZAK 密文
IV	16 H/32H	用于计算 MAC/TAC 的初始向量。 仅当报文块标识为 2/3 时有此域。 当 TAK/ZAK 密钥标识为 Z/X/U 时，该域为 16H 当 TAK/ZAK 密钥标识为 R/P/L 时，该域为 32H
报文长度	4 H	要计算 MAC 的数据长度，字节数 取值 0000-1000（即 0-4096 字节）
报文	n B	报文数据
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**MV**
错误码	2 A	00：成功 04：非法的密钥类型（或索引内密钥类型不合法） 05：非法的密钥长度 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 26：非法的密钥标识 32：无效的报文块标识或数据类型 35：无效的输出 MAC 长度 41：无主密钥或加密卡运算单元错误 45：密钥不存在 80：非法的数据长度
MAC	16 H / 32 H	当报文块标识为 1 或 2 时，此域为下一个数据块的 IV。 当报文块标识为 0 或 3 时，此域为数据的 MAC。 当密钥标识为 Z/X/U 时，该域为 16H 当密钥标识为 R/P/L 时，该域为 32H

3.4.2.6. ZAK/TAK 产生 X9.9 和 X9.19 的报文 MAC（MS）

采用模式 2 的填充规则（参见 4.1.3），MAC 算法根据密钥算法和长度选择：

- ZAK 密钥为单长度 DES/SM1/AES/SM4，采用 ISO9797-1 MAC 算法 1（全密钥 CBC-MAC）；
- ZAK 密钥为双长度 3DES，采用 ISO9797-1 MAC 算法 3；

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机。
命令代码	2 A	**MS**
报文块标识	1 N	0 - 唯一块 1 - 第一块 2 - 中间块 3 - 最后一块
密钥类型	1 N	0 - TAK 1 - ZAK
密钥长度	1 N	0 - 8 字节，单长度 DES 密钥

		1 - 16 字节，双长度 DES、SM1、SM4、AES 密钥
数据类型	1 N	0 - 二进制 1 - 扩展十六进制
TAK/ZAK	K + 4N / 16 H / 1 A + 32 H	TAK/ZAK 密钥索引或 LMK 下加密的 TAK/ZAK 密文
IV	16 H/32H	用于计算 MAC/TAC 的初始向量。 仅当报文块标识为 2/3 时有此域。 当密钥标识为 Z/X/U 时，该域为 16H 当密钥标识为 R/P/L 时，该域为 32H
报文长度	4 H	要计算 MAC 的数据长度，字节数 取值 0000-1000（即 0-4096 字节）
报文	n B	报文数据
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**MT**
错误码	2 A	00：成功 04：非法的密钥类型（或索引内密钥类型不合法） 05：非法的密钥长度 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 26：非法的密钥标识 32：无效的报文块标识或数据类型 35：无效的输出 MAC 长度 41：无主密钥或加密卡运算单元错误 45：密钥不存在 80：非法的数据长度
MAC	16 H / 32 H	当报文块标识为 1 或 2 时，此域为下一个数据块的 IV。 当报文块标识为 0 或 3 时，此域为数据的 MAC。 当密钥标识为 Z/X/U 时，该域为 16H 当密钥标识为 R/P/L 时，该域为 32H

3.4.3. PIN 产生与加密

3.4.3.1. 产生一个随机 PIN 码（JA）

产生一个长度为 4-12 的随机数字 PIN 码，输出 LMK_{03-05} 加密的 PIN 密文。

如果 PIN 的长度没有定义，产生一个长度为 4 的随机 PIN。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**JA**
账号	12 N	用户主账号有效位的最右 12 个数字
PIN 长度	2 N	可选项。范围(04-12)。如果该项不存在，默认长度为 4
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**JB**

错误码	2 A	00：成功 15：无效的输入数据（无效的格式/字符或长度错误） 24：非法的 PIN 长度 41：无主密钥或加密卡运算单元错误
PIN	L H	LMK 加密的 PIN 密文，L 为明文 PIN 长度+1

3.4.3.2. LMK 加密一个明文 PIN 码（BA）

需满足主机服务的 PIN 加解密权限。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	BA
PIN 明文	L H	PIN 明文左对齐，右边填充多个字符’F’
账号	12 N	用户主账号有效位的最右 12 个数字
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	BB
错误码	2 A	00：成功 15：无效的输入数据（无效的格式/字符或长度错误） 20：PIN 块没有包含有效的值 24：非法的 PIN 长度 41：无主密钥或加密卡运算单元错误
PIN 密文	L N	LMK 加密的 PIN 密文，L 为明文 PIN 长度+1

3.4.3.3. LMK 解密 PIN 码（NG）

需满足主机服务的 PIN 加解密权限。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	NG
账号	12 N	用户主账号，有效位的最右 12 个数字
PIN 密文	L N	LMK 加密的 PIN 密文数据
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	NH
错误码	2 A	00：成功 15：无效的输入数据（无效的格式/字符或长度错误） 20：PIN 块没有包含有效的值 24：非法的 PIN 长度 41：无主密钥或加密卡运算单元错误
PIN 明文	L H	PIN 明文

3.4.4. PIN 密文转换

3.4.4.1. 将 PIN 由 TPK 加密转换为 LMK 加密（JC）

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	JC
源 TPK 密钥	K + 4N / 16 H / 1 A + 32 H / 1 A + 48 H	用于加密 PIN 的 TPK 密钥索引或密文
源 PINBLOCK 密文	16 H / 32 H	在源 TPK 下加密的 PINBLOCK 密文 源 TPK 密钥方案为 R/P/L 时该域为 32H,否则该域为 16H
PINBLOCK 格式	2 N	PIN 数据块的格式代码，参见 5 PINBLOCK(数字)格式
账号	12 N / 18 N	用户主账号。 当 PIN 数据块格式为 04 时，该域为 18N，去除校验位的 18 位主账号，不足 18 位则右对齐左填 F; 当 PIN 数据块格式为其他值时，该域为 12N，去除校验位的最右 12 位主账号;
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	JD
错误码	2 A	00：成功 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 23：非法的 PIN BLOCK 格式 24：非法的 PIN 长度 41：无主密钥或加密卡运算单元错误 45：密钥不存在
PIN 密文	L H	LMK 下加密的 PIN 密文

3.4.4.2. 将 PIN 由 ZPK 加密转换为 LMK 加密（JE）

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	JE
源 ZPK 密钥	K + 4N / 16 H / 1 A + 32 H / 1 A + 48 H	用于加密 PIN 的 ZPK 密钥索引或密文
源 PINBLOCK 密文	16 H / 32 H	在源 ZPK 下加密的 PINBLOCK 密文 源 ZPK 密钥方案为 R/P/L 时该域为 32H,否则该域为 16H
PINBLOCK 格式	2 N	PIN 数据块的格式代码，参见 5 PINBLOCK(数字)格式
账号	12 N / 18 N	用户主账号。 当 PIN 数据块格式为 04 时，该域为 18N，去除校验位的 18 位主账号，不足 18 位则右对齐左填 F;

		当 PIN 数据块格式为其他值时，该域为 12N，去除校验位的最右 12 位主账号；
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	JF
错误码	2 A	00：成功 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 22：无效的账号 23：非法的 PIN BLOCK 格式 24：非法的 PIN 长度 41：无主密钥或加密卡运算单元错误 45：密钥不存在
PIN 密文	LH	LMK 下加密的 PIN 密文

3.4.4.3. 将 PIN 由 LMK 加密转换为 ZPK 加密（JG）

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	JG
目标 ZPK 密钥	K + 4N / 16 H / 1 A + 32 H / 1 A + 48 H	用于加密 PIN 的 ZPK 密钥索引或密文
PINBLOCK 格式	2 N	PIN 数据块的格式代码，参见 5 PINBLOCK(数字)格式
账号	12 N / 18 N	用户主账号。 当 PIN 数据块格式为 04 时，该域为 18N，去除校验位的 18 位主账号，不足 18 位则右对齐左填 F； 当 PIN 数据块格式为其他值时，该域为 12N，去除校验位的最右 12 位主账号；
PIN 密文	L N	LMK 下加密的 PIN 密文
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	JH
错误码	2 A	00：成功 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 23：非法的 PIN BLOCK 格式 24：非法的 PIN 长度 41：无主密钥或加密卡运算单元错误 45：密钥不存在
目标 PINBLOCK 密文	16 H / 32 H	在目标 ZPK 下加密的 PINBLOCK 密文 ZPK 密钥方案为 R/P/L 时该域为 32H，否则该域为 16H

3.4.4.4. 将 PIN 由 TPK 加密转换为 ZPK 加密（CA）

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	CA
源 TPK 密钥	K + 4N / 16 H / 1 A + 32 H / 1 A + 48 H	用于加密 PIN 的源 TPK 密钥索引或密文
目标 ZPK 密钥	K + 4N / 16 H / 1 A + 32 H / 1 A + 48 H	用于加密 PIN 的目标 ZPK 密钥索引或密文
最大 PIN 长度	2 N	取值 12
源 PINBLOCK 密文	16 H / 32 H	在源 TPK 下加密的 PINBLOCK 密文 源 TPK 密钥方案为 R/P/L 时该域为 32H，否则该域为 16H
源 PINBLOCK 格式	2 N	源 TPK 下加密 PIN 数据块的格式代码，参见 5 PINBLOCK(数字)格式
目标 PINBLOCK 格式	2 N	目标 ZPK 下加密 PIN 数据块的格式代码，参见 5 PINBLOCK(数字)格式
账号	12 N / 18 N	用户主账号 当 PIN 数据块格式为 04 时，该域为 18N，去除校验位的 18 位主账号，不足 18 位则右对齐左填 F； 当 PIN 数据块格式为其他值时，该域为 12N，去除校验位的最右 12 位主账号；
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	CB
错误码	2 A	00：成功 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 23：非法的 PIN BLOCK 格式 24：非法的 PIN 长度 41：无主密钥或加密卡运算单元错误 45：密钥不存在
PIN 长度	2 N	返回的 PIN 长度
目标 PINBLOCK 密文	16 H / 32 H	在目标 ZPK 下加密的 PINBLOCK 密文 ZPK 密钥方案为 R/P/L 时该域为 32H，否则该域为 16H
目标 PINBLOCK 格式	2 N	目标 PINBLOCK 的格式代码，同命令报文中内容

3.4.4.5. 将 PIN 由 ZPK1 加密转换为 ZPK2 加密（CC）

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	CC
源 ZPK 密钥	K + 4N / 16 H /	用于加密 PIN 的源 ZPK 密钥索引或密文

	1 A + 32 H / 1 A + 48 H	
目标 ZPK 密钥	K + 4N / 16 H / 1 A + 32 H / 1 A + 48 H	用于加密 PIN 的目标 ZPK 密钥索引或密文
最大 PIN 长度	2 N	取值 12
源 PINBLOCK 密文	16 H / 32 H	在源 ZPK 下加密的 PINBLOCK 密文 源 ZPK 密钥方案为 R/P/L：32H，其它 16H
源 PINBLOCK 格式	2 N	源 ZPK 下加密 PIN 数据块的格式代码，参见 5 PINBLOCK(数字)格式
目标 PINBLOCK 格式	2 N	目标 ZPK 下加密 PIN 数据块的格式代码，参见 5 PINBLOCK(数字)格式 额外的 PIN 格式 20，支持 4-6 个数字的 PIN，组成 8 字节数据块形式："04nnnn00" – "06nnnnnn"
账号	12 N / 18 N	用户主账号 当 PIN 数据块格式为 04 时，该域为 18N，去除校验位的 18 位主账号，不足 18 位则右对齐左填 F； 当 PIN 数据块格式为其他值时，该域为 12N，去除校验位的最右 12 位主账号；
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	CD
错误码	2 A	00：成功 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 23：非法的 PIN BLOCK 格式 24：非法的 PIN 长度 41：无主密钥或加密卡运算单元错误 45：密钥不存在
PIN 长度	2 N	返回的 PIN 长度
目标 PINBLOCK 密文	16 H / 32 H	在目标 ZPK 下加密的 PINBLOCK 密文 ZPK 密钥方案为 R/P/L 时该域为 32H，否则该域为 16H
目标 PINBLOCK 格式	2 N	目标 PINBLOCK 的格式代码，同命令报文中内容

3.4.4.6. 将 PIN 由 ZPK1 加密转换为 ZPK2 加密并校验（QD）

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	QD
源 ZPK 密钥	K + 4N / 16 H / 1 A + 32 H / 1 A + 48 H	用于加密 PIN 的源 ZPK 密钥索引或密文
目标 ZPK 密钥	K + 4N / 16 H / 1 A + 32 H /	用于加密 PIN 的目标 ZPK 密钥索引或密文

	1 A + 48 H	
最大 PIN 长度	2 N	取值 12
源 PINBLOCK 密文	16 H / 32 H	在源 ZPK 下加密的 PINBLOCK 密文 源 ZPK 密钥方案为 R/P/L：32H，其它 16H
源 PINBLOCK 格式	2 N	源 ZPK 下加密 PIN 数据块的格式代码，参见 5 PINBLOCK(数字)格式
目标 PINBLOCK 格式	2 N	目标 ZPK 下加密 PIN 数据块的格式代码，参见 5 PINBLOCK(数字)格式 额外的 PIN 格式 20，支持 4-6 个数字的 PIN，组成 8 字节数据块形式：″04nnnn00″ - ″06nnnnnn″
账号	12 N / 18 N	用户主账号 当 PIN 数据块格式为 04 时，该域为 18N，去除校验位的 18 位主账号，不足 18 位则右对齐左填 F； 当 PIN 数据块格式为其他值时，该域为 12N，去除校验位的最右 12 位主账号；
规则 1 启用标识	1 A	取值 Y/y 或 N/n，当为 Y/y 时校验该规则 弱密码判定规则 1：密码由 6 位相同数字组成，如 111111、222222 等（取决于 pin 长度）
规则 2 启用标识	1A	取值 Y/y 或 N/n，当为 Y/y 时校验该规则 弱密码判定规则 2：密码由 6 位相连数字组成，如 123456、654321 等（取决于 pin 长度）
规则 3 启用标识	1A	取值 Y/y 或 N/n，当为 Y/y 时校验该规则 弱密码判定规则 3：密码与输入校验数据（如客户联系电话、客户生日日期、客户证件号码等）的连续 6 位数字相同（取决于 pin 长度） 当为 Y/y 时存在以下域
规则 3 下校验数据长度	4H	用于弱密码验证规则 3 的校验数据长度 可选域，当规则 3 启用标识为 Y/y 时存在
规则 3 下校验数据	nA	以逗号分隔的用于比对弱密码的校验数据组合 如输入 13813572468, 20010101, 440881198510143176, 当密码为 138135/135724，或 200101/010101，或 143176/440881 均为弱密码 当某个校验数据的长度小于待校验 PIN 的长度时认为该数据不进行校验 可选域，当规则 3 启用标识为 Y/y 时存在
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**QE**
错误码	2 A	00：成功 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 23：非法的 PIN BLOCK 格式 24：非法的 PIN 长度 41：无主密钥或加密卡运算单元错误 45：密钥不存在
PIN 长度	2 N	返回的 PIN 长度
目标 PINBLOCK 密文	16 H / 32 H	在目标 ZPK 下加密的 PINBLOCK 密文 ZPK 密钥方案为 R/P/L 时该域为 32H，否则该域为 16H
目标 PINBLOCK 格式	2 N	目标 PINBLOCK 的格式代码，同命令报文中内容

3.4.4.7. 将 PIN 由 TPK1/ZPK1 加密转换为 TPK2/ZPK2 加密（TI）

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	TI
源密钥类型	1 N	源密钥类型。取值 1 或 2 1：TPK 2：ZPK
源 TPK/ZPK 密钥	K + 4N / 16 H / 1 A + 32 H / 1 A + 48 H	用于加密 PIN 的源 TPK/ZPK 密钥索引或密文
目标密钥类型	1 N	目标密钥类型。取值 1 或 2 1：TPK/PVK 2：ZPK
目的 TPK/ZPK 密钥	K + 4N / 16 H / 1 A + 32 H / 1 A + 48 H	用于加密 PIN 的目标 TPK/ZPK 密钥索引或密文
最大 PIN 长度	2 N	取值 12
源 PINBLOCK 密文	16 H / 32 H	在源 TPK/ZPK 下加密的 PINBLOCK 密文 源密钥方案为 R/P/L 时该域为 32H，否则 16H
源 PINBLOCK 格式	2 N	源密钥下加密 PIN 数据块的格式代码，参见 5 PINBLOCK(数字)格式
源账号	12 N / 18 N	用户主账号 当源 PIN 数据块格式为 04 时，该域为 18N，去除校验位的 18 位主账号，不足 18 位则右对齐左填 F； 当源 PIN 数据块格式为其他值时，该域为 12N，去除校验位的最右 12 位主账号；
目标 PINBLOCK 格式	2 N	目标密钥下加密 PIN 数据块的格式代码，参见 5 PINBLOCK(数字)格式
目标账号	12 N / 18 N	用户主账号 当目标 PIN 数据块格式为 04 时，该域为 18N，去除校验位的 18 位主账号，不足 18 位则右对齐左填 F； 当 PIN 数据块格式为其他值时，该域为 12N，去除校验位的最右 12 位主账号；
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	TJ
错误码	2 A	00：成功 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 20：PIN 数据块没有包含有效的值 21：非法的密钥索引 22：无效的账号 23：非法的 PIN BLOCK 格式 24：非法的 PIN 长度 41：无主密钥或加密卡运算单元错误 45：密钥不存在
目标 PINBLOCK 密文	16 H / 32 H	在目标密钥下加密的 PINBLOCK 密文

		目标密钥方案为 R/P/L 时该域为 32H，否则 16H

3.4.5. PIN 验证

密码机支持两种模式的 PIN 校验方式：IBM 3624 的 PINOFFSET 和 VISA 的 PVV 方式。

密码机当前版本支持 “十进制转换表”明文形式的使用模式；16 位的十进制表必须包含 8 位不同的数字，而且每个数字的使用不能超过 4 次。如果这个条件没有满足，则返回错误代码 25。

目前不支持 128 位分组算法的 PIN OFFSET 的运算，当 PVK 标识为 P/L/R 时，返回 26 错。

3.4.5.1. 产生 IBM PIN Offset（DE）

使用 IBM 3624 方法产生一个 PIN 偏移量。源 PIN 支持 LMK 加密的 PIN 密文形式。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**DE**
PVK 密文	K + 4N / 16 H/ 1A + 32 H/ 1A + 48 H	PVK 密钥索引或 LMK 下加密的 PVK 密文 用于产生 OFFSET
PIN 密文	L H	LMK 下加密的 PIN 密文
PIN 校验长度	2 N	最小的 PIN 校验长度
账号	12 N	用户主账号有效位的最右 12 个数字
十进制转换表	16 N	转换 16 进制到 10 进制数的表
PIN 校验数据	12 A	用户定义的数据，包含 11 个 16 进制字符和 1 个字符 N(向密码机指出在哪里插入帐号的最后 5 位)
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**DF**
错误码	2 A	00：成功 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 20：PIN 数据块没有包含有效的值 21：非法的密钥索引 22：无效的账号 24：非法的 PIN 长度 25：无效的十进制转换表或 PIN 校验数据 26：密钥算法标识不支持 41：无主密钥或加密卡运算单元错误

		45：密钥不存在
PIN OFFSET	12 H	偏移量，左对齐，右边填充 F

3.4.5.2. 产生 IBM PIN Offset 并校验弱口令（QC）

QC，在 DE 指令的基础上添加校验规则

使用 IBM 3624 方法产生一个 PIN 偏移量。源 PIN 支持 LMK 加密的 PIN 密文形式。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	QC
PVK 密文	K + 4N / 16 H/ 1A + 32 H/ 1A + 48 H	PVK 密钥索引或 LMK 下加密的 PVK 密文 用于产生 OFFSET
PIN 密文	L H	LMK 下加密的 PIN 密文
PIN 校验长度	2 N	最小的 PIN 校验长度
账号	12 N	用户主账号有效位的最右 12 个数字
十进制转换表	16 N	转换 16 进制到 10 进制数的表
PIN 校验数据	12 A	用户定义的数据，包含 11 个 16 进制字符和 1 个字符 N(向密码机指出在哪里插入帐号的最后 5 位)
分隔符	1A	分隔符，取值“;” 标识以下域的开始
规则 1 启用标识	1 A	取值 Y/y 或 N/n，当为 Y/y 时校验该规则 弱密码判定规则 1:密码由 6 位相同数字组成,如 111111、222222 等（取决于 pin 长度）
规则 2 启用标识	1A	取值 Y/y 或 N/n，当为 Y/y 时校验该规则 弱密码判定规则 2:密码由 6 位相连数字组成,如 123456、654321 等（取决于 pin 长度）
规则 3 启用标识	1A	取值 Y/y 或 N/n，当为 Y/y 时校验该规则 弱密码判定规则 3：密码与输入校验数据（如客户联系电话、客户生日日期、客户证件号码等）的连续 6 位数字相同（取决于 pin 长度） 当为 Y/y 时存在以下域
规则 3 下校验数据长度	4H	用于弱密码验证规则 3 的校验数据长度 可选域，当规则 3 启用标识为 Y/y 时存在
规则 3 下校验数据	nA	以逗号分隔的用于比对弱密码的校验数据组合 如输入 13813572468，20010101，440881198510143176，当密码为 138135/135724，或 200101/010101，或 143176/440881 均为弱密码 当某个校验数据的长度小于待校验 PIN 的长度时认为该数据不进行校验 可选域，当规则 3 启用标识为 Y/y 时存在
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	QD
错误码	2 A	00：成功 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 20：PIN 数据块没有包含有效的值

		21：非法的密钥索引 22：无效的账号 24：非法的 PIN 长度 25：无效的十进制转换表或 PIN 校验数据 26：密钥算法标识不支持 41：无主密钥或加密卡运算单元错误 45：密钥不存在
PIN OFFSET	12 H	偏移量，左对齐，右边填充 F

3.4.5.3. 使用 IBM 方式得到一个 PIN（EE）

使用 IBM 方式产生一个 4 到 12 位的 PIN。

注意： 如果包含了 offset，则 PIN 由 offset 外加其它数据得到。

如果不包含 offset，则如生成 IBM PIN offset 中所描述的方式生成 PIN。

十进制表可以按与存储密钥相同的方式存储在用户存储区。

16 位的十进制表必须包含 8 位不同的位，而且不存在出现超过 4 次的位。如果这个条件没有满足，则返回错误代码 25。

如果显示的是双倍或三倍长度的 PVK，则返回警告“02”，但将用 TDES 代替 DES 来继续生成 PIN。

域	长度&类型	描述
命令报文		
报文头	m A	不做任何修改直接返回给主机
命令代码	2 A	EE
PVK	K + 4 N / 16 H / 1 A + 32 H/ 1 A + 48 H	PVK 索引或密文
Offset	12 H	值为“000000FFFFFF” 该域包含 offset(如果有 offset 的话),左对齐、右填充’F’
检查长度	2 N	最小的 PIN 长度
账号	12 N	账号中去除校验位的最右 12 位
十进制转换表	16 N	将十六进制转换为十进制的转换表
PIN 校验数据	12 A	用户定义的、包含十六进制字符和字符“N”的数据，用来指示 HSM 插入账号最后 5 位的位置
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	EF
错误码	2 N	00：成功 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 20：PIN 数据块没有包含有效的值 21：非法的密钥索引 22：无效的账号

		24：非法的 PIN 长度 25：无效的十进制转换表或 PIN 校验数据 26：密钥算法标识不支持 41：无主密钥或加密卡运算单元错误 45：密钥不存在
PIN	LN 或 LH	LMK 对（02-03）下加密的 PIN 密文

3.4.5.4. 校验一个用 IBM 方式的终端 PIN（DA）

使用 IBM3624 方式校验一个 TPK 加密的 PIN BLOCK。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	DA
TPK	K + 4N / 16 H/ 1A + 32 H/ 1A + 48 H	TPK 密钥索引或 LMK 下加密的 TPK 密文
PVK 密文	K + 4N / 16 H/ 1A + 32 H/ 1A + 48 H	PVK 密钥索引或 LMK 下加密的 PVK 密文，用于校验 PIN OFFSET
PIN 最大长度	2 N	强制 取值 12
PIN 密文	16 H / 32 H	TPK 加密的 PINBLOCK 密文 TPK 的密钥标识为 R/P/L 时该域为 32H，否则 16H
PINBLOCK 格式代码	2 N	PIN 数据块的格式代码，参见 5 PINBLOCK(数字)格式
检查长度	2 N	最小的 PIN 校验长度
账号	12 N / 18 N	用户主账号 当目标 PIN 数据块格式为 04 时，该域为 18N，去除校验位的 18 位主账号，不足 18 位则右对齐左填 F； 当 PIN 数据块格式为其他值时，该域为 12N，去除校验位的最右 12 位主账号；
十进制转换表	16 N	转换 16 进制到 10 进制数的表
PIN 校验数据	12 A	用户定义的数据，包含 11 个 16 进制字符和 1 个字符 N(向密码机指出在哪里插入帐号的最后 5 位)
PIN OFFSET	12 H	待校验的 PIN OFFSET
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	DB
错误码	2 A	00：成功 01：校验失败或 PIN 校验数据非法 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 20：PIN 数据块没有包含有效的值 21：非法的密钥索引 22：无效的账号 24：非法的 PIN 长度 25：无效的十进制转换表或 PIN 校验数据

		41：无主密钥或加密卡运算单元错误 45：密钥不存在

3.4.5.5. 校验一个用 IBM 方式的交换 PIN（EA）

使用 IBM3624 方式校验一个 ZPK 加密的 PIN BLOCK。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**EA**
ZPK	K + 4N / 16 H/ 1A + 32 H/ 1A + 48 H	ZPK 密钥索引或 LMK 下加密的 ZPK 密文
PVK 密文	K + 4N / 16 H/ 1A + 32 H/ 1A + 48 H	PVK 密钥索引或 LMK 下加密的 PVK 密文，用于校验 PIN OFFSET
PIN 最大长度	2 N	强制 取值 12
PIN 密文	16 H / 32 H	ZPK 加密的 PINBLOCK 密文 ZPK 的密钥标识为 R/P/L 时该域为 32H，否则 16H
PIN 格式代码	2 N	PIN 数据块的格式代码，参见 5 PINBLOCK(数字)格式
检查长度	2 N	最小的 PIN 校验长度
账号	12 N / 18 N	用户主账号 当目标 PIN 数据块格式为 04 时，该域为 18N，去除校验位的 18 位主账号，不足 18 位则右对齐左填 F； 当 PIN 数据块格式为其他值时，该域为 12N，去除校验位的最右 12 位主账号；
十进制转换表	16 N	转换 16 进制到 10 进制数的表。
PIN 校验数据	12 A	用户定义的数据，包含 11 个 16 进制字符和 1 个字符 N(向密码机指出在哪里插入帐号的最后 5 位)
PIN OFFSET	12 H	待校验的 PIN OFFSET
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**EB**
错误码	2 A	00：成功 01：校验失败或 PIN 校验数据非法 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 20：PIN 数据块没有包含有效的值 21：非法的密钥索引 22：无效的账号 24：非法的 PIN 长度 25：无效的十进制转换表或 PIN 校验数据 41：无主密钥或加密卡运算单元错误 45：密钥不存在

3.4.5.6. 产生 VISA PVV（DG）

计算一个 4 位数字的 VISA PVV。源 PIN 支持 LMK 加密的 PIN 密文形式。

域	长度&类型	描述
	命令报文	
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**DG**
PVK 密文	K + 4N / 1A + 32 H	PVK 密钥索引或 LMK 下加密的 PVK 密文，用于产生 PVV
PIN 密文	L H	LMK 下加密的 PIN 密文
账号	12 N	用户主账号有效位的最右 12 个数字
PVKI	1 H	PVK 标识，取值 0-F
	响应报文	
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**DH**
错误码	2 A	00：成功 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 26：非法的密钥标识（或不支持的密钥算法） 41：无主密钥或加密卡运算单元错误 45：密钥不存在
PVV	4 N	VISA PVV

3.4.5.7. PVV 校验 ZPK 加密的 PINBLOCK（EC）

域	长度&类型	描述
	命令报文	
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**EC**
ZPK 密文	K + 4N/ 16 H / 1A + 32H/ 1A+48H	ZPK 密钥索引或 LMK 下加密的 ZPK 密文，用于产生 PINBLOCK 密文
PVK 密文	K + 4N / 1A + 32 H	PVK 密钥索引或 LMK 下加密的 PVK 密文，用于产生 PVV
PINBLOCK 密文	16 H/ 32H	ZPK 下加密的 PINBLOCK 密文 ZPK 密钥方案为 R/P/L 时该域为 32H，否则该域为 16H
PINBLOCK 格式	2 N	PIN 数据块的格式代码，参见 5 PINBLOCK（数字）格式
账号	12 N	用户主账号有效位的最右 12 个数字
PVKI	1 H	PVK 标识，取值 0-F
PVV	4 N	VISA PVV
	响应报文	
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**ED**

错误码	2 A	00： 成功 01： 校验失败 04： 非法的密钥类型（或索引内密钥类型不合法） 10： 密钥不符合奇校验 15： 无效的输入数据（无效的格式/字符或长度错误） 21： 非法的密钥索引 26： 非法的密钥标识（或不支持的密钥算法） 41： 无主密钥或加密卡运算单元错误 45： 密钥不存在

3.4.5.8. 生成或者校验美国运通的 CSC （RY）

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**RY**
模式	1N	3:产生 CSC 4:校验 CSC
标识	1N	标识特殊处理模式 当前为固定值 0
CVK 密文	K + 4N / 1A + 32 H	PVK 密钥索引或 LMK 下加密的 PVK 密文，用于产生 PVV
账号	19 N	帐号的全部数字；如果不足 19 位则左对齐补 0 至 19 位。
过期时间	4 N	卡的过期时间（9301 代表 93 年 1 月）
5 位的“CSC”	5 N	可选域:当且仅当模式为 4 时存在 5 位的“CSC”值。如果不存在则输入值“FFFFF”。
4 位的“CSC”	4 N	可选域:当且仅当模式为 4 时存在 4 位的“CSC”值。如果不存在则输入值“FFFF”。
3 位的“CSC”	3 N	可选域:当且仅当模式为 4 时存在 3 位的“CSC”值。如果不存在则输入值“FFF”。
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**RZ**
错误码	2 A	00： 成功 01： 校验失败 04： 非法的密钥类型（或索引内密钥类型不合法） 10： 密钥不符合奇校验 15： 无效的输入数据（无效的格式/字符或长度错误） 21： 非法的密钥索引 26： 非法的密钥标识（或不支持的密钥算法） 41： 无主密钥或加密卡运算单元错误 45： 密钥不存在
模式	1 N	和输入值相同
5 位的“CSC”	5 N	可选域:当且仅当模式为 3 时存在
4 位的“CSC”	4 N	可选域:当且仅当模式为 3 时存在
3 位的“CSC”	3 N	可选域:当且仅当模式为 3 时存在
5 位“CSC”的校验结果	1 N	可选域:当且仅当模式为 4 时存在 0：通过 1：输入不存在 2：校验失败

4 位“CSC”的校验结果	1 N	可选域:当且仅当模式为 4 时存在 0：通过 1：输入不存在 2：校验失败
3 位“CSC”的校验结果	1 N	可选域:当且仅当模式为 4 时存在 0：通过 1：输入不存在 2：校验失败

3.4.6. CVV 计算

卡校验值的计算，VISA CVV 的产生和验证。

3.4.6.1. 产生 VISA CVV（CW）

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**CW**
CVK A/B	K + 4N / 1A + 32 H	CVK 密钥索引或 LMK 下加密的 VISA CVK A / B
主账号	n N	卡的主账号
分隔符	1 A	值 ；
过期时间	4 N	卡的过期时间 (9301 代表 93 年一月)
服务码	3 N	卡的服务码
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**CX**
错误码	2 A	00：成功 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 22：账号域长度非法 26：非法的密钥标识（或不支持的密钥算法） 41：无主密钥或加密卡运算单元错误 45：密钥不存在
CVV	3 N	产生的 CVV

3.4.6.2. 校验 VISA CVV（CY）

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机。
命令代码	2 A	**CY**
CVK A/B	K + 4N / 1A + 32 H	CVK 密钥索引或 LMK 下加密的 VISA CVK A / B
CVV	3 N	待校验的 CVV
主账号	n N	卡的主账号

分隔符	1 A	值 ；
有效期	4 N	卡的过期时间 (9301 代表 93 年一月)
服务码	3 N	卡的服务码
响应报文		
报文头	n A	不做任何修改直接返回给主机。
响应代码	2 A	CZ
错误码	2 A	00：成功 01：校验失败 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 22：账号域长度非法 26：非法的密钥标识（或不支持的密钥算法） 41：无主密钥或加密卡运算单元错误 45：密钥不存在

3.4.7. 数据加解密运算

3.4.7.1. 数据加解密（E0）

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	E0
报文块标识	1 N	0 - 唯一块 1 - 第一块 2 - 中间块 3 - 最后一块
运算标识	1 N	0 - 加密 1 - 解密
算法模式	1 N	1 - ECB 2 - CBC 3 - CFB 4 - OFB
密钥类型	1 N	0 - ZEK
密钥密文	K + 4N / 16 H / 1A + 32 H/ 1A + 48 H	密钥索引或 LMK 下加密的密钥密文
输入数据格式	1 N	0 - Binary 模式, 1 - Expanded Hex 模式
输出数据格式	1 N	0 - Binary 模式, 1 - Expanded Hex 模式
Pad 模式	1 N	仅当报文块标识为 0 或 3 时存在。 0 - 如果数据长度为算法分组长度的整数倍，不填充；否则，填充的字符由下一个域(Pad 字符)定义，直到数据长度为算法分组长度的整数倍。 1 - 不管数据长度是否为算法分组长度的整数倍，强制填充，填充字符由下一个域(Pad 字符)定义，直到数据长度为算法分组长度的整数倍。
Pad 字符 (Pad character)	4 H	仅当报文块标识为 0 或 3 时存在。 Pad mode | Pad character | Pad count flag

		ANSI X9.19: 0 ANSI X9.23: 1 PBOC MAC: 1	0000 0000 8000	0 1 0
Pad 计数标识（Pad count flag）	1 N	仅当报文块标识为 0 或 3 时存在。 0：最后一个字节不是 padding 计数 1：最后一个字节是 padding 计数，取值范围为 0x01 – 0x10		
IV	16 H / 32 H	初始化的 IV，仅当算法标识为 2/3/4 时存在 当 ZEK 密钥标识为 Z/X/U/Y/T 时，该域为 16H 当 ZEK 密钥标识为 R/P/L 时，该域为 32H		
数据长度	3 H	实际输入数据的长度 二进制：nB 扩展十六进制：n/2 n 必须是偶数 加密时，n 最大取值 1968 字节 解密时，n 最大取值 1984 字节		
数据块	n B	待加密/解密的数据		
响应报文				
报文头	n A	不做任何修改直接返回给主机		
响应代码	2 A	E1		
错误码	2 A	00：成功 03：非法的算法模式 04：非法的密钥类型 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 32：非法的报文块标识/数据格式 38：非法的运算标识 39：非法的数据填充方式 41：无主密钥或加密卡运算单元错误 45：密钥不存在 70：无效的密文数据，数据解密去 padding 失败 80：非法的数据长度		
输出数据的格式	1 N	0 – Binary 模式，1 – Expanded Hex 模式		
输出数据长度	3 H	加密/解密的数据块长度		
输出数据	n B / 2*n H	加密/解密的数据块		
Next IV	16 H / 32 H	下一数据块的 IV，仅当模式为 CBC 且报文块标识为 1 或 2 时存在 当 ZEK 密钥方案为 Z/X/U/Y/T 时，该域为 16H 当 ZEK 密钥方案为 R/P/L 时，该域为 32H		

3.4.8. 信函打印

密码机当前版本支持用户 PIN 的信函打印，支持并口和串口通讯模式，配置见设备管理相关文档。

在向密码机发送打印指令前，需发送一个自定义的信函格式给密码机（PA 指令），发送的格式定义有效至关机或下个 PA 指令的到来。

向密码机发送打印指令（当前支持 PE 指令），密码机内验证数据报文的正确性，返回 PF 响应，

若存在错误则返回对应的错误码且终止该操作；若报文数据有效，则向打印机发送打印消息内容，完成打印后再次向主机应答一个 PZ00 响应，报告完成此次打印任务。

密码机支持连接符合 ESC/P 控制字符标准的各类打印机。

格式符号列表：

表 3-3 打印格式符号表

符号	EBCDIC 码	ASCII 码	说明
>L	6E D3	3E 4C	回车，换行。
>V	6E E5	3E 56	垂直标号。
>H	6E C8	3E 48	水平标号。
>F	6E C6	3E 46	换页。
>nnn	6E Fn Fn Fn	3E 3n 3n 3n	从左边缘跳过“nnn”列，其中“nnn”为三位的十进制数。
^M	5F D6	5E	对于密钥文档，打印第三个明文成份。
^P	5F D7	5E	对于 PIN 信封，为信封 1 打印明文 PIN。对于密钥文档，打印明文成份。
^Q	5F D8	5E	对于 PIN 信封，为信封 2 打印明文 PIN。对于密钥文档，打印明文成份或加密的 TMK（仅当“one-up”打印允许密钥文档）。
^R	5F D9	5E	为 PIN 信封 1 打印参考数。
^S	5F E2	5E	为 PIN 信封 2 打印参考数。
^T	5F E3	5E	在 PIN 信封 1 中打印帐号的最后六位。
^U	5F E4	5E	在 PIN 信封 2 中打印帐号的最后六位。
|<L><hh hh hh ..>	6A <L><hh hh hh hh ..>	7C <L><hh hh hh ..>	发送二进制数据（如打印机控制字符串）至打印机。 |字节形式的字符串长度之后的字符<L>0-F 接着为附加的十六进制的字符串<hh hh hh ..>。
^0	5F F0	5E 30	插入打印域 0。
^1	5F F1	5E 31	插入打印域 1。
^2	5F F2	5E 32	插入打印域 2。
.	.	.	.
.	.	.	.
.	.	.	.
^F	5F C6	5E 46	插入打印域 15。

格式定义举例：

.+….1….+….2….+….3….+….4….+….5….+….6

```
1       THOMAS M SMITH
2       APT 4B                          1782
3       39 ELM DR
4       MEDIA PA 19063
5
6       YOUR FULL SERVICE BANK
```

“PA”命令中的格式符号为：

>L>013^0>L>013^1>051^P>L>013^2>L>013^3>L>L>013 YOUR FULL SERVICE BANK>F>

第一行： >L>013^0

第二行： >L>013^1>051^P

第三行： >L>013^2

第四行： >L>013^3

第五行： >L

第六行： >L>013 YOUR FULL SERVICE BANK

格式输入：>F

3.4.8.1. 装载格式数据（PA）

将自定义的打印格式数据装载到 HSM 中。

需满足主机服务的信函打印权限。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**PA**
格式数据	n A	打印格式符号表中定义的符号和常量
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**PB**
错误码	2 A	00：成功 其他：参见**错误码说明**

3.4.8.2. 打印 PIN/PIN 请求数据（PE）

HSM 收到正确的信函打印指令后均向主机返回两次响应报文。

需满足主机服务的信函打印权限。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**PE**
文档类型	1 A	A：“two-up”格式中的第一个信封 B：“two-up”格式中的第二个信封 C：1 步格式
账号	12 N	账号中去除校验位的最右 12 位

PIN	LN/LH	$LMK_{003-005}$下加密的 PIN 密文
打印域 0	nA	在打印格式定义中作为“Print Field 0”定义的打印域（一定不能包含“;”字符）
分隔符	1A	值为“;”
打印域 1	nA	在打印格式定义中作为“Print Field 1”定义的打印域（一定不能包含“;”字符）
分隔符	1A	值为“;”
.	.	.
.	.	.
最后打印域	nA	在打印格式定义中定义的最后打印域一定不能包含“;”字符
响应报文（打印前）		
报文头	nA	不做任何修改直接返回给主机
响应代码	2A	PF
错误码	2A	00：成功 其他：参见**错误码说明**
PIN&参考数检查值	L+12H	对 PIN 和请求参考数的密码检查。
响应报文（打印后）		
报文头	nA	不做任何修改直接返回给主机
响应代码	2A	PZ
错误码	2A	00：成功 其他：参见**错误码说明**

3.4.8.3. 生成密钥并以分开的成份形式打印（NE）

生成一个随机密钥，在 LMK 下加密，并按要求打印成份信函。

需满足主机服务的信函打印权限。

注意事项：

打印机必须连接到 HSM 打印端口。

HSM 必须有一个已定义的打印格式。

对于一个单倍长度的密钥，密钥被分割成 2 个 8 字符长度的值。打印格式中的^P 和^Q 分别标识左半和右半部分。

对于一个双倍长度的密钥，打印格式中的^P 和^Q 分别标识第一和第二个密钥。

对于一个三倍长度的密钥，打印格式中的^P、^Q 和^R 分别标识第一、第二和第三个密钥。

打印格式中的^T 标识密钥的校验值。

域	长度&类型	描述
命令报文		
报文头	nA	不做任何修改直接返回给主机
命令代码	2A	NE
密钥类型	3H	密钥类型 000 - ZMK 001 - ZPK

		002 - PVK/TPK/TMK 003 - TAK 008 - ZAK 00A - ZEK 109 - MDK 402 - CVK
密钥标识(LMK)	1 A	在 LMK 下加密的密钥密文标识，Z/X/Y/U/T/
打印域 0	n A	在打印格式定义中作为“Print Field 0”定义的打印域（一定不能包含“;”字符）
分隔符	1 A	值为“;”
打印域 1	n A	在打印格式定义中作为“Print Field 1”定义的打印域（一定不能包含“;”字符）
分隔符	1 A	值为“;”
.	.	.
.	.	.
最后打印域	n A	在打印格式定义中定义的最后打印域一定不能包含“;”字符
响应报文（打印前）		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	NF
错误码	2 A	00：成功 04：非法的密钥类型 其他：参见**错误码说明**
密钥密文(LMK)	16 H / 1A + 32 H / 1A + 48 H	LMK 对应分组下加密的密钥密文
密钥校验值	8 H	密钥校验值
响应报文（打印后）		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	NZ
错误码	2 A	00：成功 其他：参见**错误码说明**

3.4.8.4. 生成并打印一个密钥成份（A2）

随机产生一个密钥成份，通过连接于密码机的打印机打印出明文，并返回成份的密文。

需满足主机服务的信函打印权限。

注意：

打印机必须连接在密码机的打印端口。

密码机内必须有一个已经定义好的打印格式。

密钥类型代码可在密钥类型表中查找。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	A2
密钥类型	3 H	密钥类型 000 - ZMK 001 - ZPK 002 - PVK/TPK/TMK 003 - TAK

		008 - ZAK 00A - ZEK 109 - MDK 402 - CVK
密钥标识(LMK)	1 A	在 LMK 下加密的密钥密文标识，Z/X/Y/U/T/
打印域 0	n A	在打印格式定义中作为“Print Field 0”定义的打印域（一定不能包含“;”字符）
分隔符	1 A	值为“;”
打印域 1	n A	在打印格式定义中作为“Print Field 1”定义的打印域（一定不能包含“;”字符）
分隔符	1 A	值为“;”
…	.	…
…	.	…
最后打印域	n A	在打印格式定义中定义的最后打印域一定不能包含“;”字符
响应报文（打印前）		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	A3
错误码	2 A	00：成功 其他：参见**错误码说明**
密钥密文(LMK)	16 H / 1A + 32 H / 1A + 48 H	LMK 对应分组下加密的密钥成分
密钥校验值	8H	密钥校验值
响应报文（打印后）		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	AZ
错误码	2 A	00：成功 其他：参见**错误码说明**

3.4.8.5. 生成并打印一个密钥成份及其校验值（A3）

功能：产生指定长度随机数据和随机数据的校验值，按照 PA 设置的打印格式进行打印

用途：随机产生指定长度的密钥分量和分量的校验数据

校验值在 PA 内使用^T 标识，沿用已有的规则

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	A3
生成模式	1A	0，表示存在【密钥类型】和【密钥标识(LMK)】字段 1，表示存在【密钥分量长度】字段
密钥类型	3H	可选项，当且仅当生成模式为 0 时存在 指定要产生的密钥类型 000 - ZMK 001 - ZPK 002 - PVK/TPK/TMK 003 - TAK 008 - ZAK 00A - ZEK 109 - MDK 402 - CVK
密钥标识(LMK)	1 A	可选项，当且仅当生成模式为 0 时存在 在 LMK 下加密的密钥密文标识，Z/X/Y/U/T/

密钥分量长度	2 H	可选项，当且仅当生成模式为 1 时存在 标识生成随机数密钥分量的长度（00H-20H，不超过 32 字节。）
校验值算法标识	2 N	00 ： 无格式，不打印校验值 01 ： SHA-1 02 ： MD5 03 ： ISO 10118-2 05 ： SHA-224 06 ： SHA-256 07 ： SHA-384 08 ： SHA-512 20 ： SM3-256 30： 加密一组全 0 数据得到校验值，当且仅当生成模式为 0 时，有效
校验值取值方式	2 H	可选项，当且仅当校验值算法标识不为 0 时存在 01-08　校验值的左 n 字节，比如 08 就是左 8 字节 10　全部校验值的结果 11-18　校验值的右 n 字节 20 校验值左右异或
打印域 0	n A	在打印格式定义中作为“Print Field 0”定义的打印域（一定不能包含“;”字符）
分隔符	1 A	值为“;”
打印域 1	n A	在打印格式定义中作为“Print Field 1”定义的打印域（一定不能包含“;”字符）
分隔符	1 A	值为“;”
…	.	…
…	.	…
最后打印域	n A	在打印格式定义中定义的最后打印域一定不能包含“;”字符
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	A4
错误码	2 A	00：成功 其他：参见错误码说明
密钥分量密文(LMK)	16 H / 1A + 32 H / 1A + 48 H	可选项，当且仅当生成模式为 0 时存在 LMK 对应分组下加密的密钥分量密文
密钥分量	n*2 H	可选项，当且仅当生成模式为 1 时存在 生成的随机数据，十六进制字符串表示
校验值	n*2 H	可选项，当且仅当校验值算法标识不为 0 时存在 校验值，长度由校验值取值方式指定，十六进制字符串表示 其他：参见错误码说明

3.4.8.6. 验证 PIN/PIN 和请求信封密码（PG）

验证 HSM 完成的“PE”命令处理过程。

注意：建议通过“PG”命令来验证一台 HSM 完成的“PE”命令时，使用另一台不同的 HSM。

域	长度&类型	描述
	命令报文	
报文头	m A	不做任何修改直接返回给主机
命令代码	2 A	PG
账号	12 N	账号中去除校验位的最右 12 位
PIN	L N 或 L H	LMK 下加密的 PIN
PIN&参考数检查值	L + 12 H	对 PIN 和请求参考数的密码检查
	响应报文	
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	PH
错误码	2 N	00：成功 01：验证失败 14：来自主机的 PIN 错误 15：输入数据错 41：无主密钥或加密卡运算单元错误

3.4.8.7. 打印一个 PIN 请求信函（OA）

域	长度&类型	描述
	命令报文	
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	OA
文档类型	1 A	A：“two-up”格式中的第一个信封 B：“two-up”格式中的第二个信封 C：1 步格式
账号	12 N	账号中去除校验位的最右 12 位
打印域 0	n A	在打印格式定义中作为“Print Field 0”定义的打印域（一定不能包含“;”字符）
分隔符	1 A	值为“;”
打印域 1	n A	在打印格式定义中作为“Print Field 1”定义的打印域（一定不能包含“;”字符）
分隔符	1 A	值为“;”
.	.	.
.	.	.
最后打印域	n A	在打印格式定义中定义的最后打印域一定不能包含“;”字符
	响应报文（打印前）	
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	OB
错误码	2 A	00：成功 其他：参见**错误码说明**
参考数检查值	12 H	对请求参考数的密码检查。
	响应报文（打印后）	
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	OZ
错误码	2 A	00：成功 其他：参见**错误码说明**

3.4.8.8. 验证请求信封密码（RC）

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	RC
账号	12 N	账号中去除校验位的最右 12 位
参考数检查值	12 H	对请求参考数的密码检查。
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	RD
错误码	2 A	00：成功 41：无主密钥或加密卡运算单元错误

3.4.8.9. 根据密钥成份密文打印密钥成份（NF）

根据输入的密钥成份密文，打印出密钥成份。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	NF
密钥类型	3 H	密钥成份所属的密钥类型 000 - ZMK/KEK; 109 - MK-AC/MDK; 209 - MK-SMI; 309 - MK-SMC; 409 - MK-DAK; 509 - MK-DN; 00A - ZEK/DEK; 011 - KMC; 008 - ZAK;
密钥成份密文	16H / 1A+16H / 1A + 32H / 1A + 48H / 1A + 64H	用于打印的密钥成份的密文
打印域 0	n A	在打印格式定义中作为“Print Field 0”定义的打印域 （一定不能包含“;”字符）
分隔符	1 A	值为“;”
打印域 1	n A	在打印格式定义中作为“Print Field 1”定义的打印域 （一定不能包含“;”字符）
分隔符	1 A	值为“;”
.	.	.
.	.	.
最后打印域	n A	在打印格式定义中定义的最后打印域一定不能包含“;”字符
		响应报文（打印前）
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	NG
错误码	2 A	00：成功 04：非法的密钥类型代码（或索引内密钥类型不合法） 05：非法的密钥长度（或索引内密钥长度不符）

		10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 41：无主密钥或加密卡运算单元错误 45：密钥不存在
密钥成份校验值	8 H	密钥成份的校验值
响应报文（打印后）		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	NZ
错误码	2 A	00：成功 其他：参见**错误码说明**

3.4.9. 其他功能报文

3.4.9.1. 获取密码机信息（NC）

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	NC
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	ND
错误码	2 A	00：成功 41：无主密钥或加密卡运算单元错误
密钥校验值(KCV)	16 H	DMK 的校验值
主机服务版本信息	8 A	主机密码服务版本号
管理服务版本信息	8 A	设备管理服务版本号
密码模块版本信息	8 A	应用密码层版本号
设备序列号	12 A	设备唯一序列号

3.4.9.2. 对一个数据块进行哈希运算（GM）

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	GM
哈希标识	2 N	用于计算数据摘要的算法标识： 01 ： SHA-1 02 ： MD5 03 ： ISO 10118-2 05 ： SHA-224 06 ： SHA-256 07 ： SHA-384 08 ： SHA-512 20 ： SM3-256
数据块长度	5 N	待运算的数据长度，字节数 取值范围：00000 - 04096

数据块	n B	输入数据
用户 ID 长度	4 N	可选域，仅当哈希标识取值为 20 时存在 取值范围：0000 - 0032
用户 ID	n B	可选域，仅当哈希标识取值为 20 时存在
公钥长度	4 N	仅当 HASH 算法标识为 20 时存在 SM2 公钥长度，字节数，必须为 64
SM2 算法公钥	64 B	仅当 HASH 算法标识为 20 时存在 公钥，（x，y）序列
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	GN
错误码	2 A	00：成功 05：非法的哈希算法标识 15：无效的输入数据（无效的格式/字符或长度错误） 32：非法的用户 ID 长度 76：非法的公钥长度 80：非法的数据长度
哈希值	n B	计算后的摘要值，长度由哈希标识的算法决定

3.4.9.3. 对一个 PIN 的数据块进行哈希运算（GN）

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	GN
源 ZPK 密钥	K + 4N / 16 H / 1 A + 32 H / 1 A + 48 H	用于加密 PIN 的源 ZPK 密钥索引或密文
最大 PIN 长度	2 N	取值 12
源 PINBLOCK 密文	16 H / 32 H	在源 ZPK 下加密的 PINBLOCK 密文 源 ZPK 密钥方案为 R/P/L：32H，其它 16H
源 PINBLOCK 格式	2 N	源 ZPK 下加密 PIN 数据块的格式代码，参见 5 PINBLOCK(数字)格式
账号	12 N / 18 N	用户主账号 当 PIN 数据块格式为 04 时，该域为 18N，去除校验位的 18 位主账号，不足 18 位则右对齐左填 F； 当 PIN 数据块格式为其他值时，该域为 12N，去除校验位的最右 12 位主账号；
PIN 块前缀长度	4N	PIN 块前缀长度，最大为 1024 字节
PIN 块前缀	nB	PIN 块前缀
PIN 块后缀长度	4N	PIN 块后缀长度，最大为 1024 字节
PIN 块后缀	nB	PIN 块后缀
PIN 块处理方式	2N	01 ： SHA-1 02 ： MD5 03 ： ISO 10118-2 05 ： SHA-224 06 ： SHA-256 07 ： SHA-384 08 ： SHA-512 20 ： SM3-256
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	GO
错误码	2 A	00：成功 03：非法的加密算法模式 04：非法的密钥类型 05：非法的哈希算法标识 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 36：非法的分散级数 37：非法的会话密钥产生方式 39：非法的数据填充方式 41：无主密钥或加密卡运算单元错误 45：密钥不存在 70：无效的密文数据，数据解密去 padding 失败 80：非法的数据长度
哈希值	n B	计算后的摘要值，长度由哈希标识的算法决定

3.4.9.4. 计算一个字符 PIN 的 MD5 值（GP）

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	GP
源 ZPK 密钥	K + 4N / 16 H / 1 A + 32 H / 1 A + 48 H	用于加密 PIN 的源 ZPK 密钥索引或密文
源 PINBLOCK 密文长度	2 N	源ZPK下加密的字符PIN块的密文长度
源 PINBLOCK 密文	n*2 H	在源密钥下加密的PINBLOCK密文
源字符 PINBLOCK 格式	2 N	标识使用 ZPK 加密 PIN 时的 PIN 数据块组成格式，详细参见 6 PINBLOCK(字符)格式。 00 - PIN 与账号分别左对齐，以填充 0x00 方式扩展为 48H（采用 64 位分组算法）或 64H（采用 128 位分组算法），再异或后得到 PIN 数据块； 01 - ASCII 码序列[账号|PIN|填充字符]得到 PIN 数据块。填充规则：根据密钥算法的分组长度，按需要填充的字节数填入相应字符，例如缺少 6 个字节，则填入 6 个字符'6'；若满足分组长度的倍数则不填充； 02 - PIN 与账号分别左对齐，以填充 0x00 方式扩展为 32H，再异或后得到 PIN 数据块；
源账号长度	2 N	标识账号长度，账号位数，01-24
源账号 PAN	n N	用户有效主帐号或客户号 当“源字符 PINBLOCK 格式”取值为 02 时，该域不能超过 16 个数字
操作员标识符长度	2 N	操作员标识符长度
操作员标识符	n B	操作员标识符
PIN 块前缀长度	4N	PIN 块前缀长度，最大为 1024 字节
PIN 块前缀	n B	PIN 块前缀
PIN 块后缀长度	4N	PIN 块后缀长度，最大为 1024 字节
PIN 块后缀	n B	PIN 块后缀
PIN 块处理方式	2N	01 ： SHA-1 02 ： MD5 03 ： ISO 10118-2 05 ： SHA-224 06 ： SHA-256 07 ： SHA-384 08 ： SHA-512 20 ： SM3-256
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	GQ
错误码	2 A	00：成功 03：非法的加密算法模式 04：非法的密钥类型 05：非法的哈希算法标识 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 36：非法的分散级数

		37：非法的会话密钥产生方式 39:非法的数据填充方式 41：无主密钥或加密卡运算单元错误 45：密钥不存在 70：无效的密文数据，数据解密去 padding 失败 80：非法的数据长度
哈希值	n B	计算后的摘要值，长度由哈希标识的算法决定

3.5. 非对称应用主机命令

【注意】，在对称密钥保护非对称密钥导入导出时，被加密的非对称密钥分量采用模式 1（详见 4.1.2）的填充模式。相关指令包括：

- GF，KMC 保护导出一对 RSA 密钥
- G0，KMC 保护导出一对 SM2 密钥
- TR，G0/TS/TT/TU。

3.5.1. RSA 算法应用

3.5.1.1. 产生 RSA 密钥对（EI）

随机产生一对指定模长和指数的 RSA 密钥对，输出公钥和 LMK 加密的私钥密文。

该指令兼容 RACAL 的同功能指令，扩展支持内部存储模式。

如果存储到密码机内，需满足主机服务的密钥管理权限。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	EI
密钥用途	1 N	该域仅为兼容指令保留，无意义 0 - 签名密钥 1 - 密钥管理密钥 2 - 不限，建议使用此项
密钥模长	4 N	取值：1024 - 2048，且必须为 8 的倍数
公钥编码类型	2 N	公钥编码规则： 01 - ASN.1 格式 DER 编码的公钥。整数使用 2 的补码表示法
公钥指数长度	4 N	可选项。如果命令中提供了公钥指数，则此域必须存在。指公钥指数的长度（字节数）
公钥指数	n B	可选项。 必须为奇数，若此两域不存在，则默认为 65537。
密钥存储标识	1 A	可选域。

		取值’K’，表明密钥产生后存储在加密机中，后续 3 个域必须存在 此项为空（没有任何数据），以下三个域不存在
密钥索引	4 N	可选域。仅当密钥存储标识域存在时存在该域。 存储到密码机内的密钥索引号，1 - 64。
密钥标签长度	2 N	可选域，仅当密钥存储标识域存在时存在该域。 取值：00-16
密钥标签	0-16 A	用于标记密钥的标签说明，0-16 个 ASCII 字符。
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	EJ
错误码	2 A	00：成功 15：无效的输入数据（无效的格式/字符或长度错误） 41：无主密钥或加密卡运算单元错误 52：非法的密钥用途 53：非法的密钥模长 54：非法的公钥编码类型 55：非法的 RSA 密钥索引 96：非法的密钥标签长度
公钥	n B	公钥， ASN.1 格式 DER 编码（模，指数序列）
私钥长度	4 N	私钥数据的长度，字节数。
私钥数据	n B	LMK 加密的私钥（包括 m,e,d 和 5 个 CRT 成份）

示例 1. 产生一个指数为 3 的 RSA 密钥对

```
[
EI
2
1024
01
0001
& 03 !
|
EJ
00
…
]
```

示例 2. 产生一个指数为 65537 的 RSA 密钥对，模长 2048 位，存储到索引 1 中

```
[
EI
2
2048
01
0003
& 01 00 01 !
K0001
03
RSA
|
EJ
00
…
```

]

‘&’与‘!’之间的字符为扩展 16 进制字符数据，发送密码机时需转换为 BCD 码数据串，2 个字符转换成一个字节，如“03”转换为 0x03；

3.5.1.2. 产生明文 RSA 密钥对（EH）

随机产生一对指定模长和指数的 RSA 密钥对，输出公钥和私钥各分量的明文。

该指令产生出来明文的 RSA 密钥对，不支持内部存储，仅可用于测试环境中的算法测试。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**EH**
密钥模长	4 N	mbits，取值：1024 – 2048，且必须为 8 的倍数
公钥指数长度	4 N	指公钥指数的长度（字节数）
公钥指数	n B	必须为奇数
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**EI**
错误码	2 A	00：成功 15：无效的输入数据（无效的格式/字符或长度错误） 41：无主密钥或加密卡运算单元错误 53：非法的密钥模长 54：非法的公钥编码类型
公钥 n	n B	公钥模，n = mbits / 8
公钥幂指数 e	4 B	e 值，3 或 65537
私钥 d	n B	私钥 d，n = mbits / 8
私钥 p	m B	私钥 p，m = (mbits/8 + 1)/2
私钥 q	m B	私钥 q，m = (mbits/8 + 1)/2
私钥 dp	m B	私钥 dp，m = (mbits/8 + 1)/2
私钥 dq	m B	私钥 dq，m = (mbits/8 + 1)/2
私钥 qinv	m B	私钥 qinv，m = (mbits/8 + 1)/2

3.5.1.3. 装载 RSA 密钥对 - 兼容旧版本保留（EK）

为兼容旧版本服务保留的功能指令，建议使用 EJ 指令。

需满足主机服务的密钥管理权限。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**EK**
密钥索引	2 N	01-64，要存储到密码机内的索引号
私钥长度	4 N	私钥数据的长度，字节数
私钥数据	n B	LMK 加密的私钥（包括 m,e,d 和 5 个 CRT 成份）
		响应报文
报文头	n A	不做任何修改直接返回给主机

响应代码	2 A	EL
错误码	2 A	00：成功 15：无效的输入数据（无效的格式/字符或长度错误） 41：无主密钥或加密卡运算单元错误 55：非法的 RSA 密钥索引 57：非法的私钥密文数据

3.5.1.4. 装载 RSA 密钥对（EJ）

LMK 加密的密文 RSA，导入到密码机内某索引中存储。

需满足主机服务的密钥管理权限。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	EJ
私钥长度	4 N	私钥数据的长度，字节数
扩展标识	1 A	可选域，若该域存在，说明下面的扩展域存在； 若该域不存在，后面的扩展域均不存在 取值’P’
私钥格式	2 H	可选域，当且仅当“扩展标识”域取值 P 时存在 标识私钥编码格式，若“扩展标识”域和此域都不存在则默认为 00 00 - LMK 加密的私钥（包括 m,e,d 和 5 个 CRT 成份） 01 -带口令保护 PFX 文件
私钥口令长度	2 N	可选域，当且仅当“私钥格式”域取值为 01 时存在 标识 PFX 文件私钥保护口令长度 限制为 1-32
私钥口令	n A	可选域，当且仅当“私钥格式”域取值为 01 时存在 标识 PFX 文件私钥保护口令
私钥数据	n B	1-4096
密钥索引	4 N	存储到密码机内的密钥索引号，0001 - 0064
密钥标签长度	2 N	取值：00-16
密钥标签	0-16 A	用于标记密钥的标签说明，0-16 个 ASCII 字符
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	EK
错误码	2 A	00：成功 01：口令验证失败 15：无效的输入数据（无效的格式/字符或长度错误） 41：无主密钥或加密卡运算单元错误 55：非法的 RSA 密钥索引 57：非法的私钥密文数据 96：非法的密钥标签长度

示例 1. 装载一对 RSA 密钥对到 20 号索引中

[

EJ

```
0628
&
00020270184CA0FE7AF650BF92CD0566 96BBB83D584079987FB5F75917AF5DBB
6C5D278317AF5DBB6C5D2783E2EB1ED4 D9DECED2239B703155B2207CCB626CEA
66FD59D4D05B9042F50345F44FFFBA94 A1B7BC496B5ED43F8F437FC6AFBE5810
A045F97AF67929768BAC0C3EA50C93A6 11E20D50693354A052C8EE7BE7F05269
ED5303DDA9C91D1ED335809CF9A181EA 99D9F2C287960EB9556046239B9277F2
44CDC974F03D06A2A9E9BEAAF354D4A8 85CB5726A4B8C3D3262F0AFC2190498D
D767F9E410CA09860B9E40DCC91A8D89 FD8CF76B1C93769AB2B2B53335262812
5F671C43913787B957E28AE3D881252D 5E6C55C536BA00F3BBEC41D66B1D7D2A
C2877453D73978182FF93628E8AE5980 A38888328F812065538D596486413D92
265762DF4CA6FD5BB6B8161125A1C6FC E5668F27854BB77FB930A62C93813FDD
E42177E3FE63FA473A832CB0F0EBF0C5 EA07BFDB983662A35E0BED87EFD44D81
479CF16C38CCB5B4F866CA398F69A2C1 F71AE98F5D797F57CB7D035E45269074
8C317BCD3661FEA942BF99F6E3263D30 9B53EA4A9564208A4782497138FDADF8
FCB45B4CABE92BCD4364D016C8D5E9B6 72EB5E83D9BFAA8E9E8BBA0DA5279A58
30B99E19943B8A9EB15A8C8C1267094C 4395532542BC667B761AA687EA670444
6B65CFBF0871633B74EACC9F406B182D 2719B76B6E9E3D7215D55BE738DCA475
11BE168D851FD959A118F55A346B0C74 292A722F92D63AE8F6A60CDA3D0443E1
B5C345AE2CD017BA2B12277720D0E8D2 0DE0F7C82A3F2E91A950A89E69DE8EA6
5CE7010707E2C5E233E90F92CE39D406 27F0B48C719C567DD71EB2C477728C53
BA0922A0EE21044F3D2F22AF04970519 AFE2F960
!
0020
08
TEST-RSA
|
EK
00
]
```

‘&’与‘!’之间的字符为扩展 16 进制字符数据，发送密码机时需转换为 BCD 码数据串，2 个字符转换成一个字节，如“AFE2F960”转换为 0xAF 0xE2 0xF9 0x60；

3.5.1.5. 获取 RSA 公钥（ER）

获取密码机指定索引的 RSA 公钥。

RSA 密钥索引号支持 2N 模式，以兼容旧版应用模式。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	ER
密钥索引标识	1 A	可选域： • 取值’K’，表明下个域为 4N 模式; • 此项为空（没有任何数据），下个域为 2N 模式
密钥索引号	2 N / 4 N	取值范围：1 - 64 要导出公钥的 RSA 密钥对存储在密码机中的索引位置
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	ES

错误码	2 A	00：成功 15：无效的输入数据（无效的格式/字符或长度错误） 41：无主密钥或加密卡运算单元错误 45：密钥不存在 55：非法的 RSA 密钥索引
公钥	n B	公钥， ASN.1 格式 DER 编码（模，指数序列）

示例 1. 获取 20 号索引中的公钥数据

```
[
ER
20
|
ES
00
&
30818702818100DEAA74D26F6EF74344 B301B784262BE8FAFFF9D74570EFFB92
2291F465ADA490CB47710BF745201EB9 A0E55354ECCA3E34C28982CA4D0CBEFD
17DAAF89D2DB590258A83DD8B76E6693 B0422BBDF4CAA8F6929D2B5F5F7759C0
07DD33FA59BF733F9AC2726E5B7664F2 007C8334D85268A7410795ED530A8203
49DC3211DD4271020103
!
]
```

‘&’与‘!’之间的字符为扩展 16 进制标识的字符数据。

3.5.1.6. RSA 公钥加密运算（3A）

使用 RSA 公钥加密数据，支持 PKCS#1 v1.5 版本的数据填充方式。

RSA 密钥索引号支持 2N 模式，以兼容旧版应用模式。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	3A
算法标识	2 N	01 - RSA
填充模式	2 N	00 - 不填充（数据块长度必须和模长等长） 01 - PKCS#1 V1.5 方法（EME-PKCS1-v1_5） 02 - OAEP（EME-OAEP-ENCODE）
MGF	2 N	可选域，仅当“填充模式”域取值为 02（OAEP）时存在 标识掩码产生函数： 01 - MGF1（PKCS#1 V2.0 中定义）
MGF 杂凑算法	2 N	可选域，仅当“填充模式”域取值为 02（OAEP）时存在 定义在 MGF 中使用的杂凑算法： 01 - SHA1 02 - MD5 05 - SHA224 06 - SHA256 07 - SHA384 08 - SHA512
OAEP 编码参数长度	2 N	可选域，仅当“填充模式”域取值为 02（OAEP）时存在 取值范围：00 - 99
OAEP 编码参数	n B	可选域，仅当“填充模式”域取值为 02（OAEP）时存在

		如果存在，则应参照 PKCS#1 v2.0 第 11.2.1 节进行编码。 HSM 不解释和验证该域的内容。 如果使用 OAEP 填充模式而不提供编码参数，则 OAEP 编码参数长度为 00，并且该域为空
OAEP 编码参数分隔符	1 A	可选域，仅当“填充模式”域取值为 02（OAEP）时存在 值：“;”
数据块长度	4 N	待加密的数据长度，字节数 取值 0000-0256
数据块	n B	输入数据
分隔符	1 A	‘;’ 标识数据块域的结束
密钥索引标识	1 A	可选域： • 取值’K’，表明下个域为 4N 模式; • 此项为空（没有任何数据），下个域为 2N 模式
RSA 密钥索引号	2 N / 4 N	RSA 公钥在密码机内存储的索引号。取值：1 - 64； 99（2N 模式）或 9999（4N 模式）标识公钥使用下面域的值。
公钥	n B	可选项，仅当密钥索引号为 99 或 9999 时存在。 公钥， ASN.1 格式 DER 编码（模，指数序列）
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	3B
错误码	2 A	00：成功 03：非法的算法标识 15：无效的输入数据（无效的格式/字符或长度错误） 39：无效的填充模式 41：无主密钥或加密卡运算单元错误 45：密钥不存在 55：非法的 RSA 密钥索引 80：非法的数据长度
密文长度	4 N	密文的长度，字节数
数据密文	n B	加密后的数据密文

示例 1. 使用外部公钥加密一段输入数据

```
[
3A
01
01
0026
ABCDEFGHIJKLMNOPQRSTUVWXYZ
;
99
&
30818702818100DEAA74D26F6EF74344 B301B784262BE8FAFFF9D74570EFFB92
2291F465ADA490CB47710BF745201EB9 A0E55354ECCA3E34C28982CA4D0CBEFD
17DAAF89D2DB590258A83DD8B76E6693 B0422BBDF4CAA8F6929D2B5F5F7759C0
07DD33FA59BF733F9AC2726E5B7664F2 007C8334D85268A7410795ED530A8203
49DC3211DD4271020103
!
|
3B
00
```

0128
…
]

‘&’与‘!’之间的字符为扩展 16 进制字符数据，发送密码机时需转换为 BCD 码数据串，2 个字符转换成一个字节，如“AFE2F960”转换为 0xAF 0xE2 0xF9 0x60；

3.5.1.7. RSA 私钥解密运算（3B）

使用 RSA 私钥解密数据，支持 PKCS#1 v1.5 版本的数据填充方式。

RSA 密钥索引号支持 2N 模式，以兼容旧版应用模式。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	3B
算法标识	2 N	01 – RSA
填充模式	2 N	00 – 不填充（数据块长度必须和模长等长） 01 – PKCS#1 V1.5 方法（EME-PKCS1-v1_5） 02 – OAEP（EME-OAEP-ENCODE）
MGF	2 N	可选域，仅当“填充模式”域取值为 02（OAEP）时存在 标识掩码产生函数： 01 – MGF1（PKCS#1 V2.0 中定义）
MGF 杂凑算法	2 N	可选域，仅当“填充模式”域取值为 02（OAEP）时存在 定义在 MGF 中使用的杂凑算法： 01 – SHA1 02 – MD5 05 – SHA224 06 – SHA256 07 – SHA384 08 – SHA512
OAEP 编码参数长度	2 N	可选域，仅当“填充模式”域取值为 02（OAEP）时存在 取值范围：00 – 99
OAEP 编码参数	n B	可选域，仅当“填充模式”域取值为 02（OAEP）时存在 如果存在，则应参照 PKCS#1 v2.0 第 11.2.1 节进行编码。HSM 不解释和验证该域的内容。 如果使用 OAEP 填充模式而不提供编码参数，则 OAEP 编码参数长度为 00，并且该域为空
OAEP 编码参数分隔符	1 A	可选域，仅当“填充模式”域取值为 02（OAEP）时存在 值：“;”
数据块密文长度	4 N	待解密的密文长度，字节数，应与密钥模长一致 取值 0128-0256
数据密文	n B	待解密的密文
分隔符	1 A	‘;’ 标识数据块域的结束
密钥索引标识	1 A	可选域： • 取值’K’，表明下个域为 4N 模式; • 此项为空（没有任何数据），下个域为 2N 模式
RSA 密钥索引号	2 N / 4 N	RSA 私钥在密码机内存储的索引号。取值：1 – 64; 99（2N 模式）或 9999（4N 模式）标识私钥使用下面两个域的值。
私钥长度	4 N	下个域的长度，仅当索引号为 99 或 9999 时存在；

私钥	n B	LMK 加密的私钥密文，仅当索引号为 99 或 9999 时存在；
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	3C
错误码	2 A	00：成功 03：非法的算法标识 15：无效的输入数据（无效的格式/字符或长度错误） 39：无效的填充模式 41：无主密钥或加密卡运算单元错误 45：密钥不存在 55：非法的 RSA 密钥索引 70：解密后去 PADDING 失败 80：非法的数据长度
数据长度	4 N	解密后的数据明文的长度，字节数
数据明文	n B	解密后的数据明文

示例 1. 使用 20 号密钥解密输入数据

```
[
3B
01
01
0128
&
B07A204291B7759F8921DDD2DC8CEEB2 D065D3D61C3436245C2F3F2141B55739
BC86A52DB2463AB6CE18A50E878FBCAC 2CB045CDA325AABE9D338DA5F9708DF8
F5701DE81115B77C7F9871022033354D 7A38E0AF564931D3E17D0CBDFE4C267D
EDFF3D9E06BD6A247544CC482A849797 3D418D5C17DECC8B9DC3E723498FE8C7
!
;
20
|
3C
00
0026
ABCDEFGHIJKLMNOPQRSTUVWXYZ
]
```

‘&’与‘!’之间的字符为扩展 16 进制字符数据，发送密码机时需转换为 BCD 码数据串，2 个字符转换成一个字节，如“AFE2F960”转换为 0xAF 0xE2 0xF9 0x60；

3.5.1.8. RSA 私钥签名运算（EW）

使用 RSA 私钥计算数据的签名值；

RSA 密钥索引号支持 2N 模式，以兼容旧版应用模式。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	EW
HASH 算法标识	2 N	’01’：SHA-1 ’02’：MD5 ’03’：ISO 10118-2

		'04' : No Hash '05' : SHA-224 '06' : SHA-256 '07' : SHA-384 '08' : SHA-512
签名算法标识	2 N	01 - RSA
填充模式	2 N	00 - 不填充（外部自行填充，配合 HASH 算法-04） 01 - PKCS#1 V1.5 方法（EMSA-PKCS1-v1_5） 02 - OAEP（EME-OAEP-ENCODE）
MGF	2 N	可选域，仅当“填充模式”域取值为 02（OAEP）时存在 标识掩码产生函数： 01 - MGF1（PKCS#1 V2.0 中定义）
MGF 杂凑算法	2 N	可选域，仅当“填充模式”域取值为 02（OAEP）时存在 定义在 MGF 中使用的杂凑算法： 01 - SHA1 02 - MD5 05 - SHA224 06 - SHA256 07 - SHA384 08 - SHA512
OAEP 编码参数长度	2 N	可选域，仅当“填充模式”域取值为 02（OAEP）时存在 取值范围：00 - 99
OAEP 编码参数	n B	可选域，仅当“填充模式”域取值为 02（OAEP）时存在 如果存在，则应参照 PKCS#1 v2.0 第 11.2.1 节进行编码。HSM 不解释和验证该域的内容。 如果使用 OAEP 填充模式而不提供编码参数，则 OAEP 编码参数长度为 00，并且该域为空
OAEP 编码参数分隔符	1 A	可选域，仅当“填充模式”域取值为 02（OAEP）时存在 值：“;”
数据块长度	4 N	待签名的数据长度，字节数(0-1984)
数据块	n B	输入数据
分隔符	1 A	‘;’ 标识数据块域的结束
密钥索引标识	1 A	可选域： • 取值’K’，表明下个域为 4N 模式; • 此项为空（没有任何数据），下个域为 2N 模式
RSA 密钥索引号	2 N / 4 N	RSA 私钥在密码机内存储的索引号。取值：1 - 64; 99（2N 模式）或 9999（4N 模式）标识私钥使用下面两个域的值。
私钥长度	4 N	下个域的长度，仅当索引号为 99 或 9999 时存在；
私钥	n B	LMK 加密的私钥密文，仅当索引号为 99 或 9999 时存在；
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**EX**
错误码	2 A	00：成功 03：非法的算法标识 15：无效的输入数据（无效的格式/字符或长度错误） 39：无效的填充模式 41：无主密钥或加密卡运算单元错误 45：密钥不存在 55：非法的 RSA 密钥索引 79：非法的 HASH 算法标识 80：非法的数据长度

签名长度	4 N	数字签名的长度，字节数
数字签名	n B	计算后的数字签名

示例 1. 使用 20 号密钥对输入数据进行签名运算

```
[
EW
01
01
01
0026
ABCDEFGHIJKLMNOPQRSTUVWXYZ
;
20
|
EX
00
0128
&
0B39FA0543D79DF443C444090BE848CB 8AEFF76EE2F070BC5C660AA3C5E72723
1D0877B24EFCC5BE1ECD94C30A3C42AE A4052E1D18A8539EFE14F38124D9FB69
66A3B1AB7E43B9863FEDD60486504808 9CAD43F3C911DF3C16E4551A2939E56D
4A0D446024F64A99D736AB517107C433 8992232653C9E91A114ACA031B70FA47
!
]
```

‘&’与‘!’之间的字符为扩展 16 进制字符数据，发送密码机时需转换为 BCD 码数据串，2 个字符转换成一个字节，如“AFE2F960”转换为 0xAF 0xE2 0xF9 0x60；

3.5.1.9. RSA 公钥验签运算（EY）

使用 RSA 公钥验证数据的签名值；

RSA 密钥索引号支持 2N 模式，以兼容旧版应用模式。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**EY**
HASH 算法标识	2 N	’01’ : SHA-1 ’02’ : MD5 ’03’ : ISO 10118-2 ’04’ : No Hash ’05’ : SHA-224 ’06’ : SHA-256 ’07’ : SHA-384 ’08’ : SHA-512
签名算法标识	2 N	01 - RSA
填充模式	2 N	00 - 不填充（外部自行填充，配合 HASH 算法-04） 01 - PKCS#1 V1.5 方法（EMSA-PKCS1-v1_5） 02 - OAEP（EME-OAEP-ENCODE）
MGF	2 N	可选域，仅当“填充模式”域取值为 02（OAEP）时存在 标识掩码产生函数： 01 - MGF1（PKCS#1 V2.0 中定义）
MGF 杂凑算法	2 N	可选域，仅当“填充模式”域取值为 02（OAEP）时存在

		定义在 MGF 中使用的杂凑算法： 01 - SHA1 02 - MD5 05 - SHA224 06 - SHA256 07 - SHA384 08 - SHA512
OAEP 编码参数长度	2 N	可选域，仅当“填充模式”域取值为 02（OAEP）时存在 取值范围：00 - 99
OAEP 编码参数	n B	可选域，仅当“填充模式”域取值为 02（OAEP）时存在 如果存在，则应参照 PKCS#1 v2.0 第 11.2.1 节进行编码。HSM 不解释和验证该域的内容。 如果使用 OAEP 填充模式而不提供编码参数，则 OAEP 编码参数长度为 00，并且该域为空
OAEP 编码参数分隔符	1 A	可选域，仅当“填充模式”域取值为 02（OAEP）时存在 值：“;”
签名长度	4 N	待验签的签名长度，字节数
待验证的签名	n B	待验签的签名
分隔符	1 A	‘;’ 标识签名域的结束
数据块长度	4 N	待验证的数据长度，字节数(0-1984)
数据块	n B	待验证的数据
分隔符	1 A	‘;’ 标识数据块域的结束
密钥索引标识	1 A	可选域： • 取值’K’，表明下个域为 4N 模式; • 此项为空（没有任何数据），下个域为 2N 模式
RSA 密钥索引号	2 N / 4 N	RSA 公钥在密码机内存储的索引号。取值：1 - 64； 99（2N 模式）或 9999（4N 模式）标识公钥使用下面域的值。
公钥	n B	可选项，仅当密钥索引号为99或9999时存在。 公钥， ASN.1 格式DER 编码（模，指数序列）
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	EZ
错误码	2 A	00：成功 01：验签失败 03：非法的算法标识 15：无效的输入数据（无效的格式/字符或长度错误） 39：无效的填充模式 41：无主密钥或加密卡运算单元错误 45：密钥不存在 55：非法的 RSA 密钥索引 79：非法的 HASH 算法标识 80：非法的数据长度

示例 1. 使用外部公钥对数据签名进行验证

[
EY
01
01
01
0128

```
&
0B39FA0543D79DF443C444090BE848CB 8AEFF76EE2F070BC5C660AA3C5E72723
1D0877B24EFCC5BE1ECD94C30A3C42AE A4052E1D18A8539EFE14F38124D9FB69
66A3B1AB7E43B9863FEDD60486504808 9CAD43F3C911DF3C16E4551A2939E56D
4A0D446024F64A99D736AB517107C433 8992232653C9E91A114ACA031B70FA47
!
;
0026
ABCDEFGHIJKLMNOPQRSTUVWXYZ
;
K9999
&
30818702818100DEAA74D26F6EF74344 B301B784262BE8FAFFF9D74570EFFB92
2291F465ADA490CB47710BF745201EB9 A0E55354ECCA3E34C28982CA4D0CBEFD
17DAAF89D2DB590258A83DD8B76E6693 B0422BBDF4CAA8F6929D2B5F5F7759C0
07DD33FA59BF733F9AC2726E5B7664F2 007C8334D85268A7410795ED530A8203
49DC3211DD4271020103
!
|
EZ
00
]
```

‘&’与‘!’之间的字符为扩展 16 进制字符数据，发送密码机时需转换为 BCD 码数据串，2 个字符转换成一个字节，如“AFE2F960”转换为 0xAF 0xE2 0xF9 0x60；

3.5.1.10. 保护密钥（对称）加密导出一对 RSA 密钥（TR）

若保护密钥需分散后再加密被导出的 RSA 密钥，则保护密钥的分散因子域为 16 字节的外部组合的数据，使用保护密钥直接 ECB 模式加密该分散因子得到其子密钥；

保护密钥加密被导出的 RSA 密钥时，采用的算法由保护密钥的密钥方案（密钥标识 1A）指定，算法模式由“加密算法模式”域指定。

加密导出 RSA 密钥时采用各分量分别加密的方式输出。

报文后部的扩展域为可选域，仅限主机服务 H1.14.00 版本以上支持。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	TR
加密算法模式	2 H	00 - ECB 01 - CBC
保护密钥类型	3 H	用于加密保护 RSA 密钥的保护密钥类型 000 - KEK; 109 - MDK;
保护密钥	K + 4N / 16 H / 1A + 32H / 1A + 48H	用于加密保护 RSA 的保护密钥索引或密文
保护密钥分散级数	2 H	分散级数。取值 00 - 08。
保护密钥分散因子	n*32 H	n 个分散因子的串联。每个分散因子必须为 16 个字节。

		用于产生卡片传输密钥或卡片的应用主控密钥；
被导出密钥索引标识	1 A	可选域： • 取值’K’，表明下个域为 4N 模式； • 此项为空（没有任何数据），下个域为 2N 模式
被导出密钥索引号	2 N / 4 N	RSA 公钥在密码机内存储的索引号。取值：1 – 64； 99（2N 模式）或 9999（4N 模式）标识私钥使用下面域的值。
被导出密钥私钥长度	4 N	可选域，仅当密钥索引为‘99’or ‘9999’时存在 私钥数据的长度，字节数
被导出密钥私钥数据	n B	可选域，仅当密钥索引为‘99’ or ‘9999’时存在 LMK 加密的私钥（包括 m,e,d 和 5 个 CRT 成份）
扩展标识	1 A	可选域，若该域存在，说明下面的三个扩展域存在； 若该域不存在，后面的扩展域均不存在，HSM 默认采用填充模式 01、明文 DER 编码格式输出公钥和一个分组全 00 的 IV（CBC 加密模式）； 取值’P’
PAD 标识	2 H	可选域，当且仅当“扩展标识”域存在时存在 标识被导出的各私钥分量的填充规则 取值范围：00－05 或 10 – 11，详细规则参见 4.1
输出格式	1 N	可选域，当且仅当“扩展标识”域存在时存在 0 – 公钥明文 DER 格式输出， ASN.1 格式 DER 编码（模，指数序列） 1 – m 及 e 采用分量密文形式输出 2 – 公钥明文 DER 编码格式输出(ASN.1 格式 DER 编码（模，指数序列）),私钥密文输出(明文 ASN.1 格式 DER 编码)
IV	16 H / 32 H	可选域，仅当“扩展标识”域存在且“加密算法模式”域为 01 时存在 若密钥算法为 128 分组，该域为 16 字节（32H）； 若密钥算法为 64 分组，该域为 8 字节（16H）；
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	TS
错误码	2 A	00：成功 03：非法的加密算法模式 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 36：非法的分散级数 39：非法的数据填充方式 41：无主密钥或加密卡运算单元错误 45：密钥不存在 55：非法的 RSA 密钥索引
公钥明文	n B	仅当“输出格式”域不存在，或取值为 0 或 2 时存在 公钥， ASN.1 格式 DER 编码（模，指数序列）
公钥模 m 密文长度	4 N	仅当“输出格式”域取值为 1 时存在 公钥模 m 密文长度，字节数
公钥模 m 密文	n B	仅当“输出格式”域取值为 1 时存在 公钥模 m 密文
公钥指数 e 密文长度	4 N	仅当“输出格式”域取值为 1 时存在 公钥指数 e 密文长度，字节数
公钥指数 e 密文	n B	仅当“输出格式”域取值为 1 时存在

		公钥指数 e 密文
私钥指数 d 密文长度	4 N	私钥指数 d 密文长度，字节数，仅当“输出格式”域不存在，或取值为 0 或 1 时存在
私钥指数 d 密文	n B	私钥指数 d 密文,仅当“输出格式”域不存在，或取值为 0 或 1 时存在
私钥分量 P 密文长度	4 N	私钥分量 p 密文长度，字节数,仅当“输出格式”域不存在，或取值为 0 或 1 时存在
私钥分量 P 密文	n B	私钥分量 p 密文,仅当“输出格式”域不存在，或取值为 0 或 1 时存在
私钥分量 Q 密文长度	4 N	私钥分量 q 密文长度，字节数,仅当“输出格式”域不存在，或取值为 0 或 1 时存在
私钥分量 Q 密文	n B	私钥分量 q 密文,仅当“输出格式”域不存在，或取值为 0 或 1 时存在
私钥分量 dP 密文长度	4 N	私钥分量 dP 密文长度，字节数,仅当“输出格式”域不存在，或取值为 0 或 1 时存在
私钥分量 dP 密文	n B	私钥分量 dP 密文,仅当“输出格式”域不存在，或取值为 0 或 1 时存在
私钥分量 dQ 密文长度	4 N	私钥分量 dQ 密文长度，字节数,仅当“输出格式”域不存在，或取值为 0 或 1 时存在
私钥分量 dQ 密文	n B	私钥分量 dQ 密文,仅当“输出格式”域不存在，或取值为 0 或 1 时存在
私钥分量 qInv 密文长度	4 N	私钥分量 qInv 密文长度，字节数,仅当“输出格式”域不存在，或取值为 0 或 1 时存在
私钥分量 qInv 密文	n B	私钥分量 qInv 密文,仅当“输出格式”域不存在，或取值为 0 或 1 时存在
私钥密文长度	4N	私钥密文长度，仅当“输出格式”域存在，且取值为 2 时存在
私钥密文	nB	私钥密文,(明文形式 DER 编码) 仅当“输出格式”域存在，且取值为 2 时存在

3.5.1.11. 保护密钥（对称）加密导入一对 RSA 密钥（TS）

将对称密钥加密的 RSA 密钥分量密文导入到密码机，可选的支持存储到密码机内某索引和外部密文存储；即，保护密钥加密的 RSA 密钥密文转换为 LMK 下加密。

TR 指令的反向功能。

如果存储到密码机内，需满足主机服务的密钥管理权限。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	TS
加密算法模式	2 H	00 - ECB 01 - CBC
保护密钥类型	3 H	用于加密保护 RSA 密钥的保护密钥类型 000 - KEK; 109 - MDK;
保护密钥	K + 4N / 16 H / 1A + 32H / 1A + 48H	用于加密保护 RSA 的保护密钥索引或密文

保护密钥分散级数	2 H	分散级数。取值 00 – 08
保护密钥分散因子	n*32 H	n 个分散因子的串联。每个分散因子必须为 16 个字节 用于产生卡片传输密钥或卡片的应用主控密钥；
被导入的 RSA 密钥索引标识	1 A	可选域： • 取值’K’，表明下个域为 4N 模式 • 此项为空（没有任何数据），下个域为 2N 模式
被导入的 RSA 密钥索引号	2 N / 4 N	RSA 密钥的索引号。取值： 1 – 64,标识存储到密码机内的目标索引号； 99（2N 模式）或 9999（4N 模式），标识不存储到密码机内,仅输出 RSA 公钥明文和 LMK 加密的 RSA 私钥密文。
RSA 密钥标签长度	2 N	可选域，仅当 RSA 密钥索引号取值 1-64 时存在 取值：00-16
RSA 密钥标签	0-16 A	可选域，仅当 RSA 密钥索引号取值 1-64 时存在 用于标记密钥的标签说明，0-16 个 ASCII 字符
公钥明文	n B	要导入的 RSA 密钥的公钥明文 公钥， ASN.1 格式 DER 编码（模，指数序列）
私钥指数 d 长度	4 N	私钥指数 d 密文长度，字节数
私钥指数 d	n B	私钥指数 d 密文
私钥分量 P 长度	4 N	私钥分量 p 密文长度，字节数
私钥分量 P	n B	私钥分量 p 密文
私钥分量 Q 长度	4 N	私钥分量 q 密文长度，字节数
私钥分量 Q	n B	私钥分量 q 密文
私钥分量 dP 长度	4 N	私钥分量 dP 密文长度，字节数
私钥分量 dP	n B	私钥分量 dP 密文
私钥分量 dQ 长度	4 N	私钥分量 dQ 密文长度，字节数
私钥分量 dQ	n B	私钥分量 dQ 密文
私钥分量 qInv 长度	4 N	私钥分量 qInv 密文长度，字节数
私钥分量 qInv	n B	私钥分量 qInv 密文
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**TT**
错误码	2 A	00：成功 03：非法的加密算法模式 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 36：非法的分散级数 41：无主密钥或加密卡运算单元错误 45：密钥不存在 55：非法的 RSA 密钥索引 57：非法的 RSA 密钥数据（公私钥不匹配） 70：解密后去 PADDING 失败 96：非法的密钥标签长度
私钥长度	4 N	私钥数据的长度，字节数
私钥数据	n B	LMK 加密的私钥（包括 m,e,d 和 5 个 CRT 成份）

3.5.1.12. RSA 公钥加密导出一条对称密钥（TV）

适用于使用非对称 RSA 算法完成密钥交换。

A 使用 B 的公钥加密本地的一条对称密钥（通常为传输密钥），导出发送给 B，B 再执行导入命令，以备双方通讯使用。使用 B 的公钥前，需要进行公钥 MAC 认证，以确保公钥所有者是 A 信任的主体；

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**TV**
填充模式	2 N	标识加密导出对称密钥时的填充模式 01 - PKCS#1 v1.5
被导出密钥类型	3 H	被保护导出的密钥的类型 000 - KEK; 00A - DEK; 109 - MDK;
被导出密钥	K + 4N / 16 H / 1A + 32H / 1A + 48H	被导出密钥的密钥索引或密文
被导出密钥分散级数	2 H	分散级数。取值 00 - 08。
被导出密钥分散因子	n*32 H	n 个分散因子的串联。每个分散因子必须为 16 个字节。 用于产生卡片传输密钥或卡片的应用主控密钥；
RSA 密钥索引标识	1 A	可选域： • 取值’K’，表明下个域为 4N 模式； • 此项为空（没有任何数据），下个域为 2N 模式
RSA 密钥索引号	2 N / 4 N	作为保护密钥的 RSA 公钥在密码机内存储的索引号。 取值：1 - 64； 99（2N 模式）或 9999（4N 模式）标识公钥使用下面域的值。
公钥	n B	可选域，仅当密钥索引为 99（2N 模式）或 9999（4N 模式）时存在； 公钥，ASN.1 格式的 DER 编码（模、指数 e 的序列）；
认证数据	n B	可选域，仅当密钥索引为 99（2N 模式）或 9999（4N 模式）时存在； 用于计算公钥 MAC 的额外的数据，不能包含’;’字符。
认证数据分隔符	1 A	可选域，仅当密钥索引为 99（2N 模式）或 9999（4N 模式）时存在； ‘;’,用于标识认证数据域的结束。
公钥 MAC	4 B	可选域，仅当密钥索引为 99（2N 模式）或 9999（4N 模式）时存在； 公钥 MAC 值，用于验证公钥的合法可信；
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**TW**
错误码	2 A	00：成功 01：公钥 MAC 验证失败 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 36：非法的分散级数 39：无效的填充模式 41：无主密钥或加密卡运算单元错误 45：密钥不存在

		55：非法的 RSA 密钥索引
密文长度	4 H	密钥密文长度
密钥数据块密文	n B	被导出的对称密钥数据块密文
校验值	16 H	被导出密钥的校验值

3.5.1.13. RSA 公钥保护导入一条对称密钥（TW）

适用于使用非对称算法完成密钥交换。

A 使用 B 的公钥加密本地的一条对称密钥（通常为传输密钥），导出发送给 B，B 执行本命令导入到本地存储，以备双方通讯使用。

TV 指令的反向功能。

如果存储到密码机内，需满足主机服务的密钥管理权限。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**TW**
填充模式	2 N	标识加密导出对称密钥时的填充模式 01 - PKCS#1 v1.5
导入密钥类型	3 H	RSA 公钥加密导入的对称密钥类型 000 - KEK; 00A - DEK; 109 - MDK;
导入密钥标识(LMK)	1 A	RSA 公钥加密导入的对称密钥算法类型标识： Z - 8 字节 DES 密钥 X/U - 16 字节 3DES 密钥 Y/T - 24 字节 3DES 密钥 P - 16 字节 SM1 密钥 R - 16 字节 SM4 密钥 L - 16 字节 AES 密钥
导入密钥存储标识	1 A	可选域。取值‘K’； 如存在该标识，则表明存储到 HSM 中某索引，必须存在后续 3 个域。
密钥索引	4 N	可选域。仅当密钥存储标识域’K’存在时存在该域。 存储到密码机内的密钥索引号，0001 - 2048。
导入密钥标签长度	2 N	可选域，仅当导入密钥存储标识域存在时存在该域。 取值：00-16
导入密钥标签	0-16 A	用于标记被导入密钥的标签说明，0-16 个 ASCII 字符。
导入密钥的校验值	16 H	全 0 则不校验，直接完成导入工作； 否则校验通过后，再继续完成导入工作； 若 128 分组算法，则截取前 8 字节进行校验；
导入密钥的密文长度	4 H	密钥密文长度
导入密钥的密文（PK 公钥）	n B	密钥密文，在 RSA 公钥下加密的密钥密文
RSA 密钥索引标识	1 A	作为保护密钥的 RSA 密钥索引标识，可选域： • 取值’K’，表明下个域为 4N 模式 • 此项为空（没有任何数据），下个域为 2N 模式
RSA 密钥索引号	2 N / 4 N	作为保护密钥的 RSA 密钥的索引号。取值： 1 - 64,标识存储到密码机内的目标索引号；

		99（2N 模式）或 9999（4N 模式），标识使用后续域的私钥数据
私钥长度	4 N	可选域，仅当密钥索引为‘99’ 或‘9999’时存在。私钥数据的长度，字节数。
私钥数据	n B	可选域，仅当密钥索引为‘99’ 或‘9999’时存在。LMK 加密的私钥（包括 e,d,m 和 5 个 CRT 成份）
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**TX**
错误码	2 A	00：成功 01：导入密钥的校验值验证失败 04：非法的密钥类型（或索引内密钥类型不合法） 07：导入密钥校验值无效或验证失败 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 36：非法的分散级数 39：无效的填充模式 41：无主密钥或加密卡运算单元错误 45：密钥不存在 55：非法的 RSA 密钥索引 70：解密后去 PADDING 失败 96：非法的密钥标签长度
被导入密钥的密文（LMK）	16 H / 1A + 32H / 1A + 48H	被导入密钥的密文，对应 LMK 分组下加密
校验值	16 H	被导入密钥的校验值

3.5.1.14. RSA 公钥保护导入一条对称密钥, RACAL 兼容（GI）

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**GI**
加密标识	2 N	用于解密对称密钥的算法标识： 01 - RSA
填充模式标识	2 N	用于加密过程中的填充模式标识： 01 - PKCS#1 V1.5 方法（EME-PKCS1-v1_5） 02 - OAEP（EME-OAEP-ENCODE）
MGF	2 N	可选域，仅当“填充模式”域取值为 02（OAEP）时存在标识掩码产生函数： 01 - MGF1（PKCS#1 V2.0 中定义）
MGF 杂凑算法	2 N	可选域，仅当“填充模式”域取值为 02（OAEP）时存在定义在 MGF 中使用的杂凑算法： 01 - SHA1 02 - MD5 05 - SHA224 06 - SHA256 07 - SHA384 08 - SHA512
OAEP 编码参数长度	2 N	可选域，仅当“填充模式”域取值为 02（OAEP）时存在

		取值范围：00 - 99
OAEP 编码参数	n B	可选域，仅当“填充模式”域取值为 02（OAEP）时存在 如果存在，则应参照 PKCS#1 v2.0 第 11.2.1 节进行编码。HSM 不解释和验证该域的内容。 如果使用 OAEP 填充模式而不提供编码参数，则 OAEP 编码参数长度为 00，并且该域为空
OAEP 编码参数分隔符	1 A	可选域，仅当“填充模式”域取值为 02（OAEP）时存在 值：“;”
对称密钥类型	4 N	指示需要的 LMK 对，包含 LMK 变种。 前 2 个数字表示用来加密密钥的 LMK 组号，后 2 个数字表示 LMK 变种，如 ZMK：0400；HMAC KEY：3401
密钥密文长度	4 N	下个域的长度，字节数
公钥下加密的密钥密文	n B	公钥下加密的对称密钥密文
分隔符	1 A	分隔符，指示密钥密文域的结束 值为“;”
RSA 密钥索引号	2 N / K + 4 N	RSA 私钥在密码机内存储的索引号。取值：1 - 64； 99（2N 模式）或 9999（4N 模式）标识私钥使用下面两个域的值。
私钥长度	4 N	下个域的长度，仅当索引号为 99 或 9999 时存在；
私钥	n B	LMK 加密的私钥密文，仅当索引号为 99 或 9999 时存在；
分隔符	1 A	分隔符，仅当下述三个域存在时存在 取值：‘;’ 如果命令不需要一个可选域，则用一个有效值或 0 填充
密钥方案（ZMK）	1 A	可选项，仅当分隔符存在时存在 ZMK 下加密密钥的方案。 预留项，忽略该值。
密钥方案（LMK）	1 A	可选项，仅当分隔符存在时存在 LMK 下加密密钥的方案。
密钥校验值类型	1 A	可选项，仅当分隔符存在时存在 密钥校验值计算方式： 0－16H 的 KCV，向后兼容 1－6H 的 KCV 6H
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	GJ
错误码	2 A	00：成功 05：无效的对称密钥类型 06：无效的加密标识 07：无效的填充模式标识 15：无效的输入数据（无效的格式/字符或长度错误） 21：无效的密钥索引号 26：不支持的密钥算法标识或与明文密钥长度不符 45：指定索引内无密钥 57：无效的校验值类型 70：密文解密后不符合填充规则 76：私钥长度域非法 77：明文数据块编码错误 78：密钥密文长度域非法 80：密文块长度非法 85：无效的 OAEP MGF 86：无效的 OAEP MGF 杂凑算法 87：无效的 OAEP 编码参数

初始化值	16 H	对 DES 密钥的初始化值。
密钥（LMK）	16 H / 1A + 32H / 1A + 48H	由指定的 LMK 对下加密的对称密钥密文
密钥校验值	16 H / 6 H	对称密钥的校验值。 16H 还是 6H 取决于 KCV 的类型选项。

3.5.1.15. RSA 公钥保护导出一条对称密钥, RACAL 兼容（GK）

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**GK**
加密标识	2 N	用于加密对称密钥的算法标识： 01 - RSA
填充模式标识	2 N	用于加密过程中的填充模式标识： 01 - PKCS#1 V1.5 方法（EME-PKCS1-v1_5） 02 - OAEP（EME-OAEP-ENCODE）
MGF	2 N	可选域，仅当“填充模式”域取值为 02（OAEP）时存在 标识掩码产生函数： 01 - MGF1（PKCS#1 V2.0 中定义）
MGF 杂凑算法	2 N	可选域，仅当“填充模式”域取值为 02（OAEP）时存在 定义在 MGF 中使用的杂凑算法： 01 - SHA1 02 - MD5 05 - SHA224 06 - SHA256 07 - SHA384 08 - SHA512
OAEP 编码参数长度	2 N	可选域，仅当“填充模式”域取值为 02（OAEP）时存在 取值范围：00 - 99
OAEP 编码参数	n B	可选域，仅当“填充模式”域取值为 02（OAEP）时存在 如果存在，则应参照 PKCS#1 v2.0 第 11.2.1 节进行编码。HSM 不解释和验证该域的内容。 如果使用 OAEP 填充模式而不提供编码参数，则 OAEP 编码参数长度为 00，并且该域为空
OAEP 编码参数分隔符	1 A	可选域，仅当“填充模式”域取值为 02（OAEP）时存在 值：“;”
对称密钥类型	4 N	指示需要的 LMK 对，包含 LMK 变种。 前 2 个数字表示用来加密密钥的 LMK 组号，后 2 个数字表示 LMK 变种，如 ZMK：0400；HMAC KEY：3401
对称密钥标记	1 N	指示对称密钥的标记： 0：单倍长度，8 字节 1：双倍长度，16 字节 2：三倍长度，24 字节
对称密钥（LMK）	16 H / 1A + 32H / 1A + 48H	由指定 LMK 对下加密的对称密钥密文
校验值	16 H	对称密钥的校验值。 如果校验值不满 16H，则左对齐后右补字符‘0’；校验时忽略右边为 0 的位。若输入全 0 则不进行验证。

MAC	4 B	对于公钥和证明数据的 MAC，用 LMK 计算
公钥	n B	公钥，用 ASN.1 格式编码的 DER（模、指数的序列）。
证明数据	n A	可选。在 MAC 计算中附加的数据（也可不包含）。
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	GL
错误码	2 A	00：成功 01：验证公钥 MAC 失败 02：对称密钥校验值验证失败 04：索引内密钥类型与输入类型不符 05：无效的对称密钥类型 06：无效的加密标识 07：无效的填充模式标识 10：对称密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：无效的对称密钥索引 26：不支持的密钥算法标识 45：指定索引内无密钥 50：公钥 DER 编码无效 56：无效的对称密钥长度标识 85：无效的 OAEP MGF 86：无效的 OAEP MGF 杂凑算法 87：无效的 OAEP 编码参数
初始化值	16 H	对对称密钥的初始化值 IV
密文密钥长度	4 N	下一个域的长度，字节数
密文密钥（PK）	n B	公钥下加密的对称密钥密文

3.5.1.16. 为 RSA 公钥产生一个 MAC(EO)

密码机需满足主机指令的公钥 MAC 授权状态。

主要用于在以非对称机制进行密钥交换时，确保用于加密密钥的公钥是本地信任许可的。该命令就是为信任的公钥和附加的认证数据计算公钥 MAC。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**EO（大写字母 O）**
公钥编码类型	2 N	公钥编码规则： 01 - ASN.1 格式 DER 编码的公钥。整数使用无符号表示法
公钥	n B	公钥，ASN.1 格式的 DER 编码(包含模、指数 e 序列)；
认证数据	n B	可选域，用于计算公钥 MAC 的额外的数据（不能包含字符’;’） 取值的长度范围：0-128 字节
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	EP
错误码	2 A	00：成功 15：无效的输入数据（无效的格式/字符或长度错误） 41：无主密钥或加密卡运算单元错误

		54：非法的公钥编码规则 80：非法的数据长度（认证数据）
MAC	4 B	使用 LMK 分组对公钥和认证数据计算的 MAC
公钥	n B	公钥， ASN.1 格式 DER 编码(包含模、指数 e 序列)

3.5.2. SM2 算法应用

3.5.2.1. 产生 SM2 密钥对（E7）

产生指定曲线的 SM2 密钥对，可选的存储到密码机内某索引中。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**E7**
曲线标识	2 N	07 - 国密-256 新曲线，SM2;
密钥存储标识	1 A	可选域。 • 取值’K’，表明密钥产生后存储在加密机中，后续 3 个域必须存在 • 此项为空（没有任何数据），以下三个域不存在
密钥索引	4 N	可选域。仅当密钥存储标识域存在时存在该域。 存储到密码机内的密钥索引号，0001 - 0064。
密钥标签长度	2 N	可选域，仅当密钥存储标识域存在时存在该域。 取值：00-16
密钥标签	0-16 A	用于标记密钥的标签说明，0-16 个 ASCII 字符。
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**E8**
错误码	2 A	00：成功 15：无效的输入数据（无效的格式/字符或长度错误） 41：无主密钥或加密卡运算单元错误 55：非法的 SM2 密钥索引 58：非法的曲线标识 96：非法的密钥标签长度
公钥	n B	公钥，ASN.1 格式 DER 编码（x，y）
私钥长度	4 N	私钥数据的长度，字节数
私钥	n B	LMK 加密的私钥

示例 1. 产生一对 SM2 密钥对

```
[
E7
07
|
E8
00
&
3059301306072A8648CE3D020106082A 811CCF5501822D0342000422FC92E664
8C45FF63D9AB23261A5B34F8A2023A0A 5E4568C70DD77BB224B9E051519160A8
38FA154B278DC1277DFED94069A9B695 0EDAD1B7C987253E385128
!
```

0040
&
F00C4BE63BD7EE7C531908E26C7FB33B DBC81797FC2719F912F527208874D9BA
33446475BCCB789F
!
]

3.5.2.2. 产生明文 SM2 密钥对（E8）

产生指定曲线的 SM2 密钥对，输出公钥和私钥各分量的明文。

该指令产生出来明文的 SM2 密钥对，不支持内部存储，仅可用于测试环境中的算法测试。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	E8
曲线标识	2 N	07 - 国密-256 新曲线，SM2;
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	E9
错误码	2 A	00：成功 15：无效的输入数据（无效的格式/字符或长度错误） 41：无主密钥或加密卡运算单元错误 58：非法的曲线标识
公钥 x	32 B	公钥 x
公钥 y	32 B	公钥 y
私钥 d	32 B	私钥 d

3.5.2.3. 装载 SM2 密钥对（E1）

将 SM2 明文公钥和 LMK 加密的密文私钥，导入到密码机内某索引中存储。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	E1
曲线标识	2 N	07 - 国密-256 新曲线，SM2;
公钥	n B	公钥， ASN.1 格式 DER 编码（x，y）
私钥长度	4 N	私钥数据的长度，字节数
私钥数据	n B	LMK 加密的私钥
密钥索引	4 N	存储到密码机内的密钥索引号，0001 - 0064
密钥标签长度	2 N	取值：00-16
密钥标签	0-16 A	用于标记密钥的标签说明，0-16 个 ASCII 字符
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	E2
错误码	2 A	00：成功 15：无效的输入数据（无效的格式/字符或长度错误） 41：无主密钥或加密卡运算单元错误

		43：无效的 DER 编码数据 55：非法的 SM2 密钥索引 57：无效的密钥数据（或公私钥不匹配） 58：非法的曲线标识 96：非法的密钥标签长度

示例 1. 装载一对 SM2 密钥对到 10 号索引中

```
[
E1
07
&
3059301306072A8648CE3D020106082A 811CCF5501822D0342000422FC92E664
8C45FF63D9AB23261A5B34F8A2023A0A 5E4568C70DD77BB224B9E051519160A8
38FA154B278DC1277DFED94069A9B695 0EDAD1B7C987253E385128
!
0040
&
F00C4BE63BD7EE7C531908E26C7FB33B DBC81797FC2719F912F527208874D9BA
33446475BCCB789F
!
0010
00
|
E2
00
]
```

3.5.2.4. 获取 SM2 公钥（E2）

获取密码机内指定索引的 SM2 公钥。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**E2**
密钥索引标识	1 A	取值’K’
密钥索引号	4 N	取值范围：0001 - 0064 要导出公钥的 RSA 密钥对存储在密码机中的索引位置
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**E3**
错误码	2 A	00：成功 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引标识 41：无主密钥或加密卡运算单元错误 45：密钥不存在 55：非法的 SM2 密钥索引
公钥	n B	公钥， ASN.1 格式 DER 编码（x，y 序列）

示例 1. 获取 10 号 SM2 的公钥

```
[
E2
K0010
```

```
|
E3
00
&
3059301306072A8648CE3D020106082A 811CCF5501822D0342000422FC92E664
8C45FF63D9AB23261A5B34F8A2023A0A 5E4568C70DD77BB224B9E051519160A8
38FA154B278DC1277DFED94069A9B695 0EDAD1B7C987253E385128
!
]
```

3.5.2.5. SM2 公钥加密运算（E3）

使用 SM2 公钥加密数据。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**E3**
曲线标识	2 N	07 - 国密-256 新曲线，SM2;
数据块长度	4 N	待加密的数据长度，字节数 取值 0001-1900
数据块	n B	输入数据
分隔符	1 A	‘;’ 标识数据块域的结束
密钥索引标识	1 A	取值’K’
SM2 密钥索引号	4 N	SM2 公钥在密码机内存储的索引号。 取值：0001 - 0064，或 9999 标识公钥使用下面域的值。
公钥	n B	可选项，仅当密钥索引号为 9999 时存在。 公钥， ASN.1 格式 DER 编码（x，y 序列）
密文编码格式	1 N	0 - 密文串（64 字节 C1||32 字节 C3||n 字节密文 C2）
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**E4**
错误码	2 A	00：成功 15：无效的输入数据（无效的格式/字符或长度错误） 41：无主密钥或加密卡运算单元错误 45：密钥不存在 54：非法的密文编码格式 55：非法的 SM2 密钥索引 58：非法的曲线标识 80：非法的数据长度
密文长度	4 N	密文的长度，字节数
数据密文	n B	加密后的数据密文，按编码格式输出

示例 1. 使用外部 SM2 公钥加密数据

```
[
E3
07
0026
ABCDEFGHIJKLMNOPQRSTUVWXYZ
;
K9999
```

```
&
3059301306072A8648CE3D020106082A 811CCF5501822D0342000422FC92E664
8C45FF63D9AB23261A5B34F8A2023A0A 5E4568C70DD77BB224B9E051519160A8
38FA154B278DC1277DFED94069A9B695 0EDAD1B7C987253E385128
!
0
|
E4
00
0122
&
042A3B6B52F62B02AEDAE2DA028BD36F 90E0DDF092A4722A0E76901372EB8D9F
93632340C706125CB27331B163F57878 3FCF6BBA8AD9D68DA90EE2D05658EF80
53D5FD6F1A23B1B1D8CFBDAEF9C5B9F9 E13B8602364194135F179D4EB6645AA7
0FFC34A3740318200CBA9CDA83C09887 9A06DFDCC1BA8962DD0D
!
]
```

3.5.2.6. SM2 私钥解密运算（E4）

使用 SM2 私钥解密数据。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**E4**
曲线标识	2 N	07 - 国密-256 新曲线，SM2;
密文编码格式	1 N	0 - 密文串（64 字节 C1||32 字节 C3||n 字节密文 C2）
数据块密文长度	4 N	待解密的密文长度，字节数（0097-1996）
数据密文	n B	待解密的密文
分隔符	1 A	‘;’ 标识数据块域的结束
密钥索引标识	1 A	取值’K’
SM2 密钥索引号	4 N	SM2 公钥在密码机内存储的索引号。取值：1 - 64； 9999 标识公钥使用下面域的值。
私钥长度	4 N	下个域的长度，仅当索引号为 9999 时存在；
私钥	n B	LMK 加密的私钥密文，仅当索引号为 9999 时存在；
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**E5**
错误码	2 A	00：成功 15：无效的输入数据（无效的格式/字符或长度错误） 41：无主密钥或加密卡运算单元错误（或解密失败） 45：密钥不存在 54：非法的密文编码格式 55：非法的 SM2 密钥索引 57：无效的密钥数据 58：非法的曲线标识 80：非法的数据长度
数据长度	4 N	解密后的数据明文的长度，字节数
数据明文	n B	解密后的数据明文

示例 1. 使用内部 10 号 SM2 私钥解密数据

```
[
E4
07
0
0122
&
042A3B6B52F62B02AEDAE2DA028BD36F 90E0DDF092A4722A0E76901372EB8D9F
93632340C706125CB27331B163F57878 3FCF6BBA8AD9D68DA90EE2D05658EF80
53D5FD6F1A23B1B1D8CFBDAEF9C5B9F9 E13B8602364194135F179D4EB6645AA7
0FFC34A3740318200CBA9CDA83C09887 9A06DFDCC1BA8962DD0D
!
;
K0010
|
E5
00
0026
ABCDEFGHIJKLMNOPQRSTUVWXYZ
]
```

3.5.2.7. SM2 私钥签名运算（E5）

使用 SM2 私钥计算数据的签名值；

用户标识若不存在，则采用国密局发布的默认 ID：”1234567812345678”。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**E5**
HASH 算法标识	2 N	20 - SM3
曲线标识	2 N	07 - 国密-256 新曲线，SM2;
用户标识长度	4 N	用户标识 userid 长度，字节数，取值 0000-0032
用户标识	n B	用户标识 userid
分隔符	1 A	‘;’ 标识用户标识域的结束
数据块长度	4 N	待签名的数据长度，字节数(0000-1984)
数据块	n B	输入数据
分隔符	1 A	‘;’ 标识数据块域的结束
密钥索引标识	1 A	取值’K’
SM2 密钥索引号	4 N	SM2 公钥在密码机内存储的索引号。 取值：0001 - 0064；9999 标识密钥使用下面 3 个域的值
SM2 公钥	n B	可选项，仅当密钥索引号为 9999 时存在 公钥， ASN.1 格式 DER 编码（x，y）
私钥长度	4 N	下个域的长度，仅当索引号为 9999 时存在；
私钥	n B	LMK 加密的私钥密文，仅当索引号为 9999 时存在；
签名编码格式	1 N	0 - 签名值数据串（r、s 序列）； 1 - DER 编码格式（r、s 序列编码），整数使用 2 的补码表示法；
		响应报文

报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	E6
错误码	2 A	00：成功 15：无效的输入数据（无效的格式/字符或长度错误） 32：非法的用户标识长度 41：无主密钥或加密卡运算单元错误 45：密钥不存在 54：非法的签名编码格式 55：非法的 SM2 密钥索引 57：无效的密钥数据 58：非法的曲线标识 79：非法的 HASH 算法标识 80：非法的数据长度
签名长度	4 N	数字签名的长度，字节数
数字签名	n B	计算后的数字签名，r、s 序列，按编码格式输出

示例 1. 使用内部 10 号 SM2 对数据进行签名

```
[
E5
20
07
0004
E11a
;
0026
ABCDEFGHIJKLMNOPQRSTUVWXYZ
;
K0010
0
|
E6
00
0064
&
6D1AE9B85BA3C8CB2FF9CCD28DEDA1AE 7AEB40F72FF83406780CAE0FB7F7E736
948D516BFDDD910446A9BAB16AA71288 34025339C6ECD61F778FC3604DBA5FCF
!
]
```

3.5.2.8. SM2 公钥验签运算（E6）

使用 SM2 公钥验证数据的签名值；用户标识若不存在，则采用国密局发布的默认 ID：”1234567812345678”。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	E6
HASH 算法标识	2 N	20 - SM3
曲线标识	2 N	07 - 国密-256 新曲线，SM2;
用户标识长度	4 N	用户标识 userid 长度，字节数(0000-0032)
用户标识	n B	用户标识 userid

分隔符	1 A	‘;’ 标识用户标识域的结束
签名编码格式	1 N	0 - 签名值数据串（r、s 序列）； 1 - DER 编码格式（r、s 序列编码），整数使用 2 的补码表示法；
签名长度	4 N	待验签的签名长度，字节数(0064-0080)
待验证的签名	n B	待验签的签名
分隔符	1 A	‘;’ 标识签名域的结束
数据块长度	4 N	待验证的数据长度，字节数(0000-1984)
数据块	n B	待验证签名的数据
分隔符	1 A	‘;’ 标识数据块域的结束
密钥索引标识	1 A	取值’K’
SM2 密钥索引号	4 N	SM2 公钥在密码机内存储的索引号。取值：0001 - 0064； 9999 标识公钥使用下面域的值。
SM2 公钥	n B	可选项，仅当密钥索引号为 9999 时存在 公钥， ASN.1 格式 DER 编码（x，y）
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**E7**
错误码	2 A	00：成功 01：验证失败 15：无效的输入数据（无效的格式/字符或长度错误） 32：非法的用户标识长度 41：无主密钥或加密卡运算单元错误 43：DER 解码失败 45：密钥不存在 54：非法的签名编码格式 55：非法的 SM2 密钥索引 58：非法的曲线标识 79：非法的 HASH 算法标识 80：非法的数据长度

示例 1. 使用外部 SM2 公钥对数据签名进行验证

```
[
E6
20
07
0004
E11a
;
0
0064
&
6D1AE9B85BA3C8CB2FF9CCD28DEDA1AE 7AEB40F72FF83406780CAE0FB7F7E736
948D516BFDDD910446A9BAB16AA71288 34025339C6ECD61F778FC3604DBA5FCF
!
;
0026
ABCDEFGHIJKLMNOPQRSTUVWXYZ
;
```

```
K9999
&
3059301306072A8648CE3D020106082A 811CCF5501822D0342000422FC92E664
8C45FF63D9AB23261A5B34F8A2023A0A 5E4568C70DD77BB224B9E051519160A8
38FA154B278DC1277DFED94069A9B695 0EDAD1B7C987253E385128
!
|
E7
00
]
```

3.5.2.9. SM2 私钥签名(对数据的摘要值)运算（ED）

使用 SM2 私钥计算数据的签名值；该指令仅对数据的摘要值（32 字节）进行 SM2 私钥签名运算，数据摘要的产生由应用系统自行负责。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**ED**
曲线标识	2 N	07 - 国密-256 新曲线，SM2;
数据块摘要值	32 B	待签名的数据的 SM3 摘要值，必须是 32 字节
密钥索引标识	1 A	取值’K’
SM2 密钥索引号	4 N	SM2 公钥在密码机内存储的索引号。 取值：0001 - 0064；9999 标识密钥使用下面 2 个域的值
私钥长度	4 N	下个域的长度，仅当索引号为 9999 时存在；
私钥	n B	LMK 加密的私钥密文，仅当索引号为 9999 时存在；
签名编码格式	1 N	0 - 签名值数据串（r、s 序列）； 1 - DER 编码格式（r、s 序列编码），整数使用 2 的补码表示法；
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**EE**
错误码	2 A	00：成功 15：无效的输入数据（无效的格式/字符或长度错误） 41：无主密钥或加密卡运算单元错误 45：密钥不存在 54：非法的签名编码格式 55：非法的 SM2 密钥索引 57：无效的密钥数据 58：非法的曲线标识 80：非法的数据长度
签名长度	4 N	数字签名的长度，字节数
数字签名	n B	计算后的数字签名，r、s 序列，按编码格式输出

3.5.2.10. SM2 公钥验签(对数据的摘要值)运算（EF）

使用 SM2 公钥验证签名值；该指令仅对数据的摘要值（32 字节）进行 SM2 公钥验证运算，数据摘要的产生由应用系统自行负责。

域	长度&类型	描述

命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	EF
曲线标识	2 N	07 - 国密-256 新曲线，SM2;
签名编码格式	1 N	0 - 签名值数据串（r、s 序列）； 1 - DER 编码格式（r、s 序列编码），整数使用 2 的补码表示法；
签名长度	4 N	待验证的签名长度，字节数(0064-0080)
待验证的签名	n B	待验证的签名
分隔符	1 A	‘;’ 标识签名域的结束
数据块摘要值	32 B	待验证的数据的 SM3 摘要值，必须是 32 字节
密钥索引标识	1 A	取值’K’
SM2 密钥索引号	4 N	SM2 公钥在密码机内存储的索引号。取值：0001 - 0064；9999 标识公钥使用下面域的值。
SM2 公钥	n B	可选项，仅当密钥索引号为 9999 时存在 公钥， ASN.1 格式 DER 编码（x，y）
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	EG
错误码	2 A	00：成功 01：验证失败 15：无效的输入数据（无效的格式/字符或长度错误） 41：无主密钥或加密卡运算单元错误 43：DER 解码失败 45：密钥不存在 54：非法的签名编码格式 55：非法的 SM2 密钥索引 58：非法的曲线标识 80：非法的数据长度

3.5.2.11. 保护密钥（对称）加密导出一对 SM2 密钥（TT）

若保护密钥需分散，则分散因子域为 16 字节的外部组合的数据，使用保护密钥直接 ECB 模式加密该分散因子得到其子密钥；

保护密钥加密被导出的 SM2 私钥时，采用的算法由保护密钥的密钥方案（密钥标识 1A）指定，算法模式由“加密算法模式”域指定。

该指令输出 SM2 公钥和密文私钥分量。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	TT
加密算法模式	2 H	00 - ECB 01 - CBC
保护密钥类型	3 H	用于加密保护被导出密钥的源密钥类型 000 - KEK; 109 - MDK;
保护密钥	K + 4N /	用于加密导出 SM2 密钥的保护密钥索引或密文

	16 H / 1A + 32H / 1A + 48H	
保护密钥分散级数	2 H	分散级数。取值 00 - 08。
保护密钥分散因子	n*32 H	n 个分散因子的串联。每个分散因子必须为 16 个字节。 用于产生卡片传输密钥或卡片的应用主控密钥；
曲线标识	2 N	07 - 国密-256 新曲线，SM2；
SM2 密钥索引号	4 N	SM2 公钥在密码机内存储的索引号。取值：0001 - 0064； 9999 标识私钥使用下面域的值。
公钥	n B	可选域，‘9999’时存在 公钥， ASN.1 格式 DER 编码（公钥 x、y 序列）
私钥长度	4 N	可选域， or ‘9999’时存在。 私钥数据的长度，字节数。
私钥数据	n B	可选域，‘9999’时存在。 LMK 加密的私钥 SM2 私钥分量
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	TU
错误码	2 A	00：成功 03：非法的加密算法模式 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 36：非法的分散级数 41：无主密钥或加密卡运算单元错误 45：密钥不存在 55：非法的 SM2 密钥索引 57：无效的密钥数据 58：非法的曲线标识
公钥	n B	公钥， ASN.1 格式 DER 编码（公钥 x、y 序列）
私钥分量 d 加密后长度	4 N	私钥分量 d 密文长度，字节数
私钥分量 d 密文	n B	私钥分量 d 密文

示例 1. 使用外部密文 KEK 加密保护导出 10 号 SM2 密钥对

```
[
TT
00
000
X801617441513A2F135AB14EAAD1069DF
00
07
0010
|
TU
00
&
3059301306072A8648CE3D020106082A 811CCF5501822D0342000422FC92E664
8C45FF63D9AB23261A5B34F8A2023A0A 5E4568C70DD77BB224B9E051519160A8
38FA154B278DC1277DFED94069A9B695 0EDAD1B7C987253E385128
!
```

```
0040
&
42899D03F76DB809F10300AA5E02A5F7 A3DC1F152A5E5C3E0E4690448F5BEEAD
DC5342DC20124957
!
]
```

3.5.2.12. 保护密钥（对称）加密导入一对 SM2 密钥 (TU)

将对称密钥加密的 SM2 密钥分量密文导入到密码机，可选的支持存储到密码机内某索引和外部密文存储；即，保护密钥加密的 SM2 密钥密文转换为 LMK 下加密。

TT 指令的反向功能。

如果存储到密码机内，需满足主机服务的密钥管理权限。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**TU**
加密算法模式	2 H	00 - ECB 01 - CBC
保护密钥类型	3 H	用于加密保护被导出密钥的源密钥类型 000 - KEK; 109 - MDK;
保护密钥	K + 4N / 16 H / 1A + 32H / 1A + 48H	用于加密导入 SM2 密钥的保护密钥索引或密文
保护密钥分散级数	2 H	分散级数。取值 00 - 08。
保护密钥分散因子	n*32 H	n 个分散因子的串联。每个分散因子必须为 16 个字节。 用于产生卡片传输密钥或卡片的应用主控密钥；
曲线标识	2 N	07 - 国密-256 新曲线，SM2;
SM2 密钥索引号	4 N	SM2 密钥在密码机内存储的索引号。取值：0001 – 0064； 9999 标识密钥不存储于内部
密钥标签长度	2 N	取值：00-16 仅当 SM2 密钥索引号不为 9999 时存在该域
密钥标签	0-16 A	用于标记密钥的标签说明，0-16 个 ASCII 字符 仅当 SM2 密钥索引号不为 9999 时存在该域
公钥	n B	要导入的 SM2 公钥 ASN.1 格式 DER 编码（公钥 x、y 序列）
私钥分量 d 长度	4 N	保护密钥加密的 SM2 私钥分量 d 密文长度，字节数
私钥分量 d	n B	保护密钥加密的 SM2 私钥分量 d 密文
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**TV**
错误码	2 A	00：成功 03：非法的加密算法模式 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 36：非法的分散级数

		41：无主密钥或加密卡运算单元错误 45：密钥不存在 55：非法的 SM2 密钥索引 57：无效的密钥数据 58：非法的曲线标识 70：解密后的密钥数据去 PADDING 失败 96：非法的密钥标签长度
私钥长度	4 N	私钥数据的长度，字节数
私钥数据	n B	LMK加密的私钥（包括私钥d成份）

示例 1. 使用外部密文 KEK 加密保护导入一对 SM2 密钥对，存储到 20 号索引中

```
[
TU
00
000
R4CFCA087C6B43DFB7319746192A53CE0
00
07
0020
06
IMPSM2
&
3059301306072A8648CE3D020106082A 811CCF5501822D0342000422FC92E664
8C45FF63D9AB23261A5B34F8A2023A0A 5E4568C70DD77BB224B9E051519160A8
38FA154B278DC1277DFED94069A9B695 0EDAD1B7C987253E385128
!
0048
&
A3FD185D7AE311EA53F6454707F33310 A92CA047831E642DF2DC213ADF6B30C7
E22C48C2A6BC25BEA6FDC7DE5A490FF0
!
|
TV
00
0040
&
F00C4BE63BD7EE7C531908E26C7FB33B DBC81797FC2719F912F527208874D9BA
33446475BCCB789F
!
]
```

3.5.2.13. SM2 公钥保护导出一条对称密钥（TX）

适用于使用非对称算法完成密钥交换。

A 使用 B 的公钥加密本地的一条对称密钥（通常为传输密钥），导出发送给 B，B 再执行导入命令，以备双方通讯使用。使用 B 的公钥前，需要进行公钥 MAC 认证，以确保公钥所有者是 A 信任的主体；

域	长度&类型	描述
命令报文		

报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**TX**
曲线标识	2 N	07 - 国密-256 新曲线，SM2
被导出密钥类型	3 H	被保护导出的密钥的类型 000 - KEK; 00A - DEK; 109 - MDK;
被导出密钥	K + 4N / 16 H / 1A + 32H / 1A + 48H	被导出密钥的密钥索引或密文
被导出密钥分散级数	2 H	分散级数。取值 00 - 08
被导出密钥分散因子	n*32 H	n 个分散因子的串联。每个分散因子必须为 16 个字节
SM2 密钥索引号	4 N	作为保护密钥的 SM2 公钥在密码机内存储的索引号 取值：0001 - 0064； 9999 标识公钥使用下面域的值。
SM2 公钥	n B	可选域，仅当密钥索引为 9999 时存在； 公钥，ASN.1 格式的 DER 编码（公钥 x、y 序列）；
认证数据	n B	可选域，仅当密钥索引为 9999 时存在； 用于计算公钥 MAC 的额外的数据，不能包含’;’字符。
认证数据分隔符	1 A	可选域，仅当密钥索引为 9999 时存在； ‘;’,用于标识认证数据域的结束。
公钥 MAC	4 B	可选域，仅当密钥索引为 9999 时存在； 公钥 MAC 值，用于验证公钥的合法可信；
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**TY**
错误码	2 A	00：成功 01：公钥 MAC 验证失败 04：非法的密钥类型（或索引内密钥类型不合法） 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 36：非法的分散级数 39：无效的填充模式 41：无主密钥或加密卡运算单元错误 45：密钥不存在 55：非法的 SM2 密钥索引
密文长度	4 H	密钥密文长度
密钥数据块密文	n B	被导出的对称密钥数据块密文
校验值	16 H	被导出密钥的校验值

示例 1. 使用 10 号 SM2 密钥保护导出一条 MDK 密钥

```
[
TX
07
109
X84BE3F9DF32844D77B60C89583EBC6B2
00
0010
|
TY
00
```

```
0070
&
A9EE5D424A62E3E8831DDD2448033457 DF4B81674F110ABB608B1738507007B3
A3057C2A285961E563A7F77A138C0493 C5580B627D110B0519BF2EA94286BE2C
204C4719F77C2369478A6F111B21E06B C7587680B79C0AAA3AC23935AD154752
CC08F599156BB2A02F104CC7FCEE7FAB
!
E98DBE5394BD4943
]
```

3.5.2.14. SM2 公钥保护导入一条对称密钥（TY）

适用于使用非对称算法完成密钥交换。

A 使用 B 的公钥加密本地的一条对称密钥（通常为传输密钥），导出发送给 B，B 执行本命令导入到本地存储，以备双方通讯使用。

TX 指令的反向功能。

如果存储到密码机内，需满足主机服务的密钥管理权限。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**TY**
曲线标识	2 N	07 - 国密-256 新曲线，SM2
导入密钥类型	3 H	SM2 公钥加密导入的对称密钥类型 000 - KEK; 00A - DEK; 109 - MDK;
导入密钥标识(LMK)	1 A	SM2 公钥加密导入的对称密钥算法类型： Z - 8 字节 DES 密钥 X/U - 16 字节 3DES 密钥 Y/T - 24 字节 3DES 密钥 P - 16 字节 SM1 密钥 R - 16 字节 SM4 密钥 L - 16 字节 AES 密钥
导入密钥存储标识	1 A	可选域。取值‘K’； 如存在该标识，则表明被导入的对称密钥存储到 HSM 中某索引，必须存在后续 3 个域。
密钥索引	4 N	可选域。仅当密钥存储标识域’K’存在时存在该域。 存储到密码机内的密钥索引号，0001 - 2048。
导入密钥标签长度	2 N	可选域，仅当导入密钥存储标识域存在时存在该域。 取值：00-16
导入密钥标签	0-16 A	用于标记被导入密钥的标签说明，0-16 个 ASCII 字符。
导入密钥的校验值	16 H	全 0 则不校验，直接完成导入工作； 否则校验通过后，再继续完成导入工作； 若 128 分组算法，则截取前 8 字节进行校验；
导入密钥的密文长度	4 H	密钥密文长度
导入密钥的密文（PK 公钥）	n B	密钥密文，在 SM2 公钥下加密的密钥密文
SM2 密钥索引号	4 N	作为保护密钥的 SM2 密钥的索引号。取值： 0001 - 0064,标识存储到密码机内的目标索引号；

		9999，标识使用后续域的私钥数据
私钥长度	4 N	可选域，仅当密钥索引为 9999 时存在。 私钥数据的长度，字节数。
私钥数据	n B	可选域，仅当密钥索引为 9999 时存在。 LMK 加密的私钥（包括私钥 d 成份）
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	TZ
错误码	2 A	00：成功 01：导入密钥的校验值验证失败 04：非法的密钥类型 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 36：非法的分散级数 39：无效的填充模式 41：无主密钥或加密卡运算单元错误 45：密钥不存在 55：非法的 SM2 密钥索引 70：解密后去 PADDING 失败 96：非法的密钥标签长度
被导入密钥的密文（LMK）	16 H / 1A + 32H / 1A + 48H	被导入密钥的密文，对应 LMK 分组下加密。
校验值	16 H	被导入密钥的校验值

示例 1. 使用 10 号 SM2 密钥保护导入一条 MDK 密钥，不存储

```
[
TY
07
109
X
E98DBE5394BD4943
0070
&
A9EE5D424A62E3E8831DDD2448033457 DF4B81674F110ABB608B1738507007B3
A3057C2A285961E563A7F77A138C0493 C5580B627D110B0519BF2EA94286BE2C
204C4719F77C2369478A6F111B21E06B C7587680B79C0AAA3AC23935AD154752
CC08F599156BB2A02F104CC7FCEE7FAB
!
0010
|
TZ
00
X84BE3F9DF32844D77B60C89583EBC6B2
E98DBE5394BD4943
]
```

3.5.2.15. 为 SM2 公钥产生一个 MAC(TQ)

密码机需满足主机指令的公钥 MAC 授权状态。

主要用于在以非对称机制进行密钥交换时，确保用于加密密钥的公钥是本地信任许可的。该命令就

是为信任的公钥和附加的认证数据计算公钥 MAC。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**TQ**
曲线标识	2 N	07 - 国密-256 新曲线，SM2
公钥	n B	公钥，ASN.1 格式的 DER 编码(包含公钥 x、y 序列)
认证数据	n B	可选域，用于计算公钥 MAC 的额外的数据（不能包含字符';'） 取值的长度范围：0-128 字节
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	**TR**
错误码	2 A	00：成功 15：无效的输入数据（无效的格式/字符或长度错误） 41：无主密钥或加密卡运算单元错误 43：无效的 DER 编码数据 58：非法的曲线标识 80：非法的数据长度（认证数据）
MAC	4 B	使用 LMK 分组对公钥和认证数据计算的 MAC
公钥	n B	公钥， ASN.1 格式 DER 编码(包含公钥 x、y 序列)

3.5.3. 其他功能报文

3.5.3.1. 计算/校验 MAC(3D)

私钥解密公钥加密的 MAC 数据块，得到 MAC 明文后，使用 MAC 密钥计算 MAC

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	**3D**
公钥算法标识	2 N	标识公钥加密 MAC 数据块时采用的非对称算法 01 - RSA 07 - SM2
私钥索引	4 N	用于解密(公钥加密的)MAC 数据块密文的私钥索引号，0001-0064 9999 标识使用私钥使用下面两个域的值。
私钥长度	4 N	下个域的长度，仅当私钥索引号为 9999 时存在；
私钥	n B	LMK 加密的私钥密文，仅当私钥索引号为 9999 时存在；
公钥加密 MAC 块组成格式	2 N	标识公钥加密的 MAC 数据块组成格式 00 -2 字节 MAC 数据长度（2H）+MAC 数据+随机数据
公钥加密的填充模式	2 N	标识公钥加密 PIN 数据块时采用的填充模式，仅当公钥算法标识为 01 时存在； 01 - PKCS#1 v1.5 填充方式 07 -在 MAC 数据块前面补 0x00，以使数据长度等于 RSA 密钥模长
公钥加密的 MAC 数据密文数据块长度	4 N	标识公钥加密的 MAC 数据数据块密文的长度，字节数

公钥加密的 MAC 数据密文	n B	经公钥加密的 MAC 数据密文
MAK 密钥类型	1 N	0 - TAK 1 - ZAK
TAK/ZAK 密钥	K + 4N / 16 H / 1 A + 32 H / 1 A + 48 H	TAK/ZAK 密钥索引或 LMK 下加密的 TAK/ZAK 密文
MAC 算法标识	2 N	01 - ISO9797-1 MAC 算法模式 1 使用 MAC 密钥 CBC 模式加密数据，取最后一段密文；
MAC 计算模式	2N	01 - 计算 MAC 02 - 验证 MAC
待验证的 MAC	16H/32H	可选域，仅当 MAC 计算模式为 02 时存在 当密钥标识为 Z/X/U 时，该域为 16H 当密钥标识为 R/P/L 时，该域为 32H
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	3E
错误码	2 A	00：成功 01：验证失败 04：非法的密钥类型（或索引内密钥类型不合法） 05：非法的密钥长度 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的密钥索引 26：非法的密钥标识 32：无效的报文块标识或数据类型 35：无效的输出 MAC 长度 41：无主密钥或加密卡运算单元错误 45：密钥不存在 80：非法的数据长度
MAC	16 H / 32 H	仅当 MAC 计算模式为 01 时存在 当密钥标识为 Z/X/U 时，该域为 16H 当密钥标识为 R/P/L 时，该域为 32H

3.5.3.2. 数据转加密 – 非对称转对称(S8)

将 RSA 或 ECC 算法下公钥加密的数据密文转换到对称密钥下加密，输出。

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	S8
公钥算法标识	2N	标识公钥加密数据时采用的非对称算法 01 - RSA 07 - SM2
索引标识	1A	取值 K
私钥索引	4N	私钥在密码机内存储的索引号。取值：1-64； 9999 标识私钥使用下面两个域的值。
私钥长度	4N	下个域的长度，仅当索引号为 9999 时存在；

		取值：0-1968；
私钥密文	nB	LMK 加密的私钥密文，仅当索引号为 9999 时存在；
填充模式	2H	仅当公钥算法标识为 01 时存在 01 - PKCS#1 v1.5 填充方式
加密算法模式	2H	标识密钥加密数据时的算法模式 00 - ECB 01 - CBC 02 - CFB 03 - OFB
目标密钥类型	3H	用于加密数据的目标密钥类型 000 - KEK; 109 - MDK; 309 - MK-SMC; 00A - ZEK/DEK; 00B - TEK; 011 - KMC;
目标密钥	K + 4N/ 1A + 16H/ 1A + 32H/ 1A + 48H	用于加密数据的目标密钥索引或密文
目标密钥分散级数	2H	分散级数。取值 00 - 08。
目标密钥分散因子	n*32H	n 个分散因子的串联。每个分散因子必须为 16 个字节。
目标密钥会话密钥模式	2H	会话密钥的产生模式： 00 - 不产生会话密钥； 01 - ECB 模式加密 8 字节会话密钥因子，得 8 字节会话密钥； 02 - ECB 模式加密 16 字节会话密钥因子，得 16 字节会话密钥； 03 - 密钥的左右 8 字节异或，得 8 字节会话密钥； 04 - 取密钥的左 8 字节作为会话密钥； 05 - CBC 模式加密 16 字节会话密钥因子，得 16 字节会话密钥；
目标密钥会话密钥因子	16H/32H	仅当目标会话密钥模式取值为 01/02/05 时存在 • 会话密钥模式为 01 时，该域为 8 字节（16H），适用于产生 PBOC 规范的单长度会话密钥，取值：6 字节 0x00||2 字节 ATC； • 会话密钥模式为 02 时，该域为 16 字节（32H），适用于产生 PBOC 规范的双长度会话密钥，取值：6 字节 0x00||2 字节 ATC||6 字节 0x00||2 字节 ATC 的非； 会话密钥模式为 05 时，该域为 16 字节（32H），适用于产生 GP 规范 SCP02 的卡片会话密钥，取值：2 字节密钥类型||2 字节卡计数器||12 字节 0x00；
目标密钥加密时的数据 PAD 标识	2H	标识加密前数据的填充规则 取值范围：00 - 05 或 10 - 11，详细规则参见 4.1
目标密钥加密时的 IV	16H/32H	仅当加密算法模式为 01/02/03 时存在。 若密钥算法为 128 分组，该域为 16 字节（32H）； 若密钥算法为 64 分组，该域为 8 字节（16H）；
输入数据长度	4H	转对称加密的密文长度，字节数 取值 0000-07C0（即 0 - 1984 字节）
输入数据	n B	转对称加密的密文
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	S9
错误码	2 A	00：成功

		03：非法的算法标识 04：非法的密钥类型 10：密钥不符合奇校验 15：无效的输入数据（无效的格式/字符或长度错误） 21：非法的对称密钥索引 36：非法的分散级数 37：非法的会话密钥产生方式 39：非法的数据填充方式 41：无主密钥或加密卡运算单元错误 45：密钥不存在 55：非法的私有密钥索引 58：非法的曲线标识 70：无效的密文数据，数据解密去 padding 失败 80：非法的数据长度
密文长度	4H	数据密文长度
密文	n B	数据块密文

3.6. OTP 动态口令主机命令

本部分指令支持 GM/T 0021-2012《动态口令密码应用技术规范》中定义的密钥管理和动态口令运算算法。

3.6.1. 产生令牌种子（F3）

产生指定长度的随机令牌种子，再分别使用 Ks 及 Kps 加密并计算密文 MAC，输出两个密文及密文 MAC 值。

将保护该种子的根密钥 Km，按两个不同的分散因子分散成两个不同的保护密钥 Ks 及 Kps，对随机产生的令牌种子分别加密并计算 MAC（加密时采用 ECB 模式，MAC 计算采用 CBC MAC 模式），输出。

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	F3
根密钥类型	3 H	用于保护令牌种子的根密钥 Km 类型： 000 - ZMK/KEK;　　109 - MK-AC/MDK; 209 - MK-SMI;　　309 - MK-SMC; 409 - MK-DAK;　　509 - MK-DN;
根密钥	K + 4N / 1A + 16H / 1A + 32H / 1A + 48H	用于保护令牌种子的根密钥索引或密文
密钥分散级数 1	2 H	第一个子密钥的分散级数。取值 00 - 08
密钥分散因子 1	n*32 H	第一个子密钥的分散因子串。

		n 个分散因子的串联。每个分散因子必须为 16 个字节
MAC 算法模式 1	2 H	对第一个子密钥加密的种子密文的 MAC 计算方式： 00 - 不计算密文 MAC 01 - ISO9797-1 MAC 算法模式 1 使用 MAC 密钥 CBC 模式加密数据，取最后一段密文；
密钥分散级数 2	2 H	第二个子密钥的分散级数。取值 00 - 08
密钥分散因子 2	n*32 H	第二个子密钥的分散因子串。 n 个分散因子的串联。每个分散因子必须为 16 个字节
MAC 算法模式 2	2 H	对第二个子密钥加密的种子密文的 MAC 计算方式： 00 - 不计算密文 MAC 01 - ISO9797-1 MAC 算法模式 1 使用 MAC 密钥 CBC 模式加密数据，取最后一段密文；
IV 产生方式	1 N	若两个密文 MAC 均不计算，则该域存在但无效。 0：外部送入 1：内部随机生成
IV	32 H	仅当 IV 产生方式为 0 时存在。 其作为上面二个密文计算 MAC 的共同使用的 IV； 若两个密文 MAC 均不计算，则该域无效
种子长度	3 N	指定要产生的随机种子长度，最小 12 字节
PAD 标识	2 H	标识随机种子被保护密钥加密前数据的填充规则 取值范围：00－05 或 10 - 11，详细规则参见 4.1
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	F4
错误码	2 A	00：成功 04：非法的根密钥类型 15：无效的输入数据（无效的格式/字符或长度错误）
IV	32 H	若两个密文 MAC 均不计算，则该域存在但无效 CBC MAC 计算时使用的 IV
第一子密钥加密的种子密文长度	3 N	第一子密钥加密的种子密文长度
第一子密钥加密的种子密文	2*n H	第一子密钥加密后数据密文(ECB 方式加密)
第一密文 MAC 值	32 H	第一子密钥对第一种子密文计算的 CBC MAC 不计算第一密文 MAC 时该域返回全 0
第二子密钥加密的种子密文长度	3 N	第二子密钥加密的种子密文长度
第二子密钥加密的种子密文	2*n H	第二子密钥加密后数据密文(ECB 方式加密)
第二子密钥 MAC 值	32 H	第二子密钥对第二种子密文计算的 CBC MAC 不计算第二密文 MAC 时该域返回全 0

3.6.2. 解密种子密文（F4）

该指令实际为一条安全报文解密功能的指令。

将保护种子的根密钥，按分散因子分散成子密钥，对种子密文 MAC 进行验证，然后解密出种子输出。

域	长度&类型	描述
命令报文		

报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	F4
根密钥类型	3 H	用于保护令牌种子的根密钥类型： 000 - ZMK/KEK; 109 - MK-AC/MDK; 209 - MK-SMI; 309 - MK-SMC; 409 - MK-DAK; 509 - MK-DN;
根密钥	K + 4N / 1A + 16H / 1A + 32H / 1A + 48H	用于保护令牌种子的根密钥索引或密文
密钥分散级数	2 H	子密钥的分散级数。取值 00 - 08
密钥分散因子	n*32 H	子密钥的分散因子串。 n 个分散因子的串联。每个分散因子必须为 16 个字节
MAC 算法模式	2 H	对子密钥加密的种子密文的 MAC 验证方式： 00 - 不验证密文 MAC 01 - ISO9797-1 MAC 算法模式 1 使用 MAC 密钥 CBC 模式加密数据,取最后一段密文；
IV	32 H	仅当“MAC 算法模式”为 1 时存在该域 验证密文 MAC 时使用的 IV；
密文种子长度	3 N	子密钥加密的种子密文的长度，字节数
种子密文	n*2 H	子密钥加密的种子密文
密文 MAC	32 H	待验证的种子密文 MAC 如果 MAC 不满 32H，则左对齐后右补字符‘0’；MAC 校验时忽略右边为 0 的位。
PAD 标识	2 H	标识随机种子被保护密钥加密前数据的填充规则 取值范围：00－05 或 10 - 11，详细规则参见 4.1
明文种子 MAC 算法模式	2 H	对解密后的种子明文的 MAC 产生方式： 00 - 不产生明文 MAC 01 - ISO9797-1 MAC 算法模式 1 使用子密钥 CBC 模式加密数据，取最后一段密文；
IV	32 H	仅当“明文种子 MAC 算法模式”为 1 时存在该域
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	F5
错误码	2 A	00：成功 01：种子密文 MAC 验证失败 04：非法的根密钥类型 15：无效的输入数据（无效的格式/字符或长度错误）
明文种子长度	3 N	明文种子长度
明文种子	2*n H	令牌明文种子
MAC 值	32 H	使用子密钥对明文种子计算的 CBC MAC 仅当“明文种子 MAC 算法模式”为 1 时存在该域

3.6.3. 生成 OTP 动态口令（F5）

将保护种子的根密钥，按分散因子分散成子密钥，对种子密文 MAC 进行验证，解密出种子后根据规范计算出 OTP 动态口令输出。

域	长度&类型	描述

命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	F5
根密钥类型	3 H	用于保护令牌种子的根密钥类型： 000 - ZMK/KEK; 109 - MK-AC/MDK; 209 - MK-SMI; 309 - MK-SMC; 409 - MK-DAK; 509 - MK-DN;
根密钥	K + 4N / 1A + 16H / 1A + 32H / 1A + 48H	用于保护令牌种子的根密钥索引或密文
密钥分散级数	2 H	子密钥的分散级数。取值 00 - 08
密钥分散因子	n*32 H	子密钥的分散因子串。 n 个分散因子的串联。每个分散因子必须为 16 个字节
MAC 算法模式	2 H	对子密钥加密的种子密文的 MAC 验证方式： 00 - 不验证密文 MAC 01 - ISO9797-1 MAC 算法模式 1 使用 MAC 密钥 CBC 模式加密数据，取最后一段密文；
IV	32 H	仅当“MAC 算法模式”为 1 时存在该域 验证密文 MAC 时使用的 IV；
密文种子长度	3 N	子密钥加密的种子密文的长度，字节数
种子密文	n*2 H	子密钥加密的种子密文
密文 MAC	32 H	待验证的种子密文 MAC 如果 MAC 不满 32H，则左对齐后右补字符‘0’；MAC 校验时忽略右边为 0 的位。
PAD 标识	2 H	标识随机种子被保护密钥加密前数据的填充规则 取值范围：00－05 或 10 - 11，详细规则参见 4.1
ID 长度	3 N	输入 ID 的长度
ID 值	2*n H	ID 值
OTP 杂凑算法标识	2 N	01 : SHA-1 02 : MD5 20 : SM3-256
输出 OTP 长度	2 N	指定输出的 OTP 长度（4-10）
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	F6
错误码	2 A	00：成功 01：种子密文 MAC 验证失败 04：非法的根密钥类型 15：无效的输入数据（无效的格式/字符或长度错误） …
OTP 长度	2 N	输出的 OTP 长度
OTP 值	n N	输出的 OTP 值
杂凑结果	40 H / 32 H / 64 H	杂凑算法输出结果

3.6.4.产生新种子并生成 OTP 动态口令（F6）

域	长度&类型	描述
		命令报文
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	F6
根密钥类型	3 H	用于保护令牌种子的根密钥类型： 000 - ZMK/KEK; 109 - MK-AC/MDK; 209 - MK-SMI; 309 - MK-SMC; 409 - MK-DAK; 509 - MK-DN;
根密钥	K + 4N / 1A + 16H / 1A + 32H / 1A + 48H	用于保护令牌种子的根密钥索引或密文
密钥分散级数	2 H	子密钥的分散级数。取值 00 - 08
密钥分散因子	n*32 H	子密钥的分散因子串。 n 个分散因子的串联。每个分散因子必须为 16 个字节
MAC 算法模式	2 H	对子密钥加密的种子密文的 MAC 验证方式： 00 - 不验证密文 MAC 01 - ISO9797-1 MAC 算法模式 1 使用 MAC 密钥 CBC 模式加密数据,取最后一段密文；
IV	32 H/16H	仅当“MAC 算法模式”为 1 时存在该域 验证密文 MAC 时使用的 IV；
密文种子长度	3 N	子密钥加密的种子密文的长度，字节数
种子密文	n*2 H	子密钥加密的种子密文
密文 MAC	32 H	待验证的种子密文 MAC 如果 MAC 不满 32H，则左对齐后右补字符‘0’；MAC 校验时忽略右边为 0 的位。
PAD 标识	2 H	标识随机种子被保护密钥加密前数据的填充规则 取值范围：00－05 或 10 - 11，详细规则参见 4.1
激活挑战码长度	2 N	输入激活挑战码的长度(1-16)
激活挑战码	n N	激活挑战码
新种子 MAC 算法模式	2 H	对子密钥加密的新种子密文的 MAC 验证方式： 00 - 不计算密文 MAC 01 - ISO9797-1 MAC 算法模式 1 使用 MAC 密钥 CBC 模式加密数据,取最后一段密文；
新种子 IV 产生方式	1 N	若新种子密文 MAC 不计算，则该域存在但无效。 0：外部送入 1：内部随机生成
新种子 IV	32 H/16H	仅当新种子 IV 产生方式为 0 时存在。 若新种子密文 MAC 不计算，则该域无效
OTP 杂凑算法标识	2 N	01 ： SHA-1 02 ： MD5 20 ： SM3-256
输出 OTP 长度	2 N	指定输出的 OTP 长度（4-10）
		响应报文
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	F6
错误码	2 A	00：成功 01：种子密文 MAC 验证失败 04：非法的根密钥类型

		15：无效的输入数据（无效的格式/字符或长度错误） …
OTP 长度	2 N	输出的 OTP 长度
OTP 值	n N	输出的 OTP 值
杂凑结果	40 H / 32 H / 64 H	杂凑算法输出结果
激活码长度	2N	输出的激活码长度
激活码	n N	激活码是激活挑战码||OTP
IV	32 H/16H	若新种子密文 MAC 不计算，则该域存在但无效 CBC MAC 计算时使用的 IV
新种子密文长度	3 N	新种子密文长度
新种子密文	2*n H	新种子密文(ECB 方式加密)
新种子 MAC 值	32 H	新种子密文计算的 CBC MAC 不计算新种子密文 MAC 时该域返回全 0

3.6.5.生成 OTP（F7）

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	F7
根密钥类型	3 H	用于保护令牌种子的根密钥类型： 000 - ZMK/KEK; 109 - MK-AC/MDK; 209 - MK-SMI; 309 - MK-SMC; 409 - MK-DAK; 509 - MK-DN;
根密钥	K + 4N / 1A + 16H / 1A + 32H / 1A + 48H	用于保护令牌种子的根密钥索引或密文
密钥分散级数	2 H	子密钥的分散级数。取值 00 - 08
密钥分散因子	n*32 H	子密钥的分散因子串。 n 个分散因子的串联。每个分散因子必须为 16 个字节
变形算法	1H	0x09： 表示不变形（选择该值，无下边 3 项） TA_SM3 0x00：SM3 TA_SHA1 0x01：SHA1 TA_SHA256 0x02：SHA256 TA_HMAC_SM3 0x03：HMAC-SM3 TA_HMAC_SHA1 0x04：HMAC-SHA1 TA_HMAC_SHA256 0x05：HMAC-SHA256 TA_SM4_CBC_MAC 0x06：SM4-CBC-MAC 如果由于散列算法的原因产生的结果数据大于变形前种子密钥的长度，舍弃掉后面多余的数据。 变形的处理方式,H 为 sm3/sha1/sha256 H（种子密钥|变形因子） HMAC-H（种子密钥，变形因子） SM4-CBC-MAC(种子密钥，变形因子，IV)， （说明:暂不支持 0x03 HMAC-SM3 和 0x06:SM4-CBC-MAC。

		HMAC-SM3 默认不变形 SM4-CBC-MAC 目前实现的方法为：种子明文长度必须为 16 字节，且对变形因子非强制填充 0x00 计算 MAC，ISO9797-1 MAC 算法模式 1，产生 mac 长度 16 字节。）
变形因子长度	4N	长度范围为 1-1024
变形因子	nB	用于变换种子密钥的变形因子
初始向量	32H	仅当变形算法为 SM4-CBC-MAC 时存在， 恒为 16 字节长
动态口令类型	1H	DPT_SM3 0x01：SM3 DPT_SM4 0x02：SM4
因子组合类型	1H	FCT_T 0x01：T FCT_C 0x02：C 以及三者的组合： FCT_T|FCT_C 0x03：T|C FCT_T|FCT_Q 0x04：T|Q FCT_C|FCT_Q 0x05：C|Q FCT_T|FCT_C|FCT_Q 0x06：T|C|Q 至少包含 T/C 的其中一个参数，Q 为可选参数。 只有在因子组合类型中含 T 时，下面关于时间因子的项存在; 且只有在因子组合类型中含 C 时，下面关于事件因子的项存在; 只有在因子组合类型中含 Q 时，下面关于挑战因子的项存在。
时间因子输入方式	1N	0 – 输入 T 的方式，直接输入时间因子 T 1 – 输入 T0 和 Tc 的方式。T=T0/Tc。 可选，由因子组合类型决定，仅当含 T 输入时存在
T0	16H	T0 是以 UTC 时间或用户选择的时间标准为计量标准的一个 8 字节整数。 16 进制数输入，如 1313655030 为 000000004E4CC8F6 仅当时间因子输入方式为 1 时存在 可选，由因子组合类型决定，仅当含 T 输入时存在
Tc	2N	Tc 是以秒为单位的口令变化周期，最大为 60s.即取值为 1-60. 仅当时间因子输入方式为 1 时存在 可选，由因子组合类型决定，仅当含 T 输入时存在
时间因子 T	16H	时间因子，恒为 8 字节长 仅当时间因子输入方式为 0 时存在 16 进制数输入 可选，由因子组合类型决定，仅当含 T 输入时存在
事件因子	8H	事件因子，恒为 4 字节长 16 进制数输入 可选，由因子组合类型决定，仅当含 C 输入时存在
挑战因子长度	4N	挑战因子长度，长度范围为 4-255 字节 可选，由因子组合类型决定，仅当含 Q 输入时存在
挑战因子	nA	挑战因子，参与到动态口令生成过程中的一种数据。 可选，由因子组合类型决定，仅当含 Q 输入时存在
种子密文 MAC 算法模式	2H	对子密钥加密的种子密文的 MAC 验证方式： 00 - 不验证密文 MAC 01 - ISO9797-1 MAC 算法模式 1 使用 MAC 密钥 CBC 模式加密数据， 取最后一段密文；
IV	32H	仅当种子密文 MAC 算法模式为 1 时存在该域 验证密文 MAC 时使用的 IV
种子密文 MAC	32H	仅当种子密文 MAC 算法模式为 1 时存在该域 待验证的种子密文 MAC 如果 MAC 不满 32H，则左对齐后右补字符‘0’；MAC 校验时忽略右边为 0 的位。
种子密文长度	3N	子密钥加密的种子密文的长度，字节数
种子密文	n*2 H	子密钥加密的种子密文
PAD 标识	2H	标识随机种子被保护密钥加密前数据的填充规则

		取值范围：00－05 或 10 － 11，详细规则参见 4.1
输出 OTP 长度	2 N	指定输出的 OTP 长度（4-10）
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	F8
错误码	2 A	00：成功 01：种子密文 MAC 验证失败 04：非法的根密钥类型 15：无效的输入数据（无效的格式/字符或长度错误） …
OTP 长度	2 N	输出的 OTP 长度
OTP 值	n N	输出的 OTP 值
杂凑结果	32 H / 64 H	杂凑算法输出结果

3.6.6.验证 OTP（F8）

域	长度&类型	描述
命令报文		
报文头	n A	不做任何修改直接返回给主机
命令代码	2 A	F8
根密钥类型	3 H	用于保护令牌种子的根密钥类型： 000 － ZMK/KEK;　　109 － MK-AC/MDK; 209 － MK-SMI;　　309 － MK-SMC; 409 － MK-DAK;　　509 － MK-DN;
根密钥	K + 4N / 1A + 16H / 1A + 32H / 1A + 48H	用于保护令牌种子的根密钥索引或密文
密钥分散级数	2 H	子密钥的分散级数。取值 00 － 08
密钥分散因子	n*32 H	子密钥的分散因子串。 n 个分散因子的串联。每个分散因子必须为 16 个字节
变形算法	1H	0x09： 表示不变形（选择该值，无下边 3 项） TA_SM3　　0x00：SM3 TA_SHA1　　0x01：SHA1 TA_SHA256　　0x02：SHA256 TA_HMAC_SM3　　0x03：HMAC-SM3 TA_HMAC_SHA1　　0x04：HMAC-SHA1 TA_HMAC_SHA256　　0x05：HMAC-SHA256 TA_SM4_CBC_MAC　　0x06：SM4-CBC-MAC （说明:暂不支持 0x03 HMAC-SM3 和 0x06:SM4-CBC-MAC。 HMAC-SM3 默认不变形 SM4-CBC-MAC 目前实现的方法为：种子明文长度必须为 16 字节，且对变形因子非强制填充 0x00 计算 MAC， ISO9797-1 MAC 算法模式 1，产生 mac 长度 16 字节。）
变形因子长度	4N	长度范围为 1-1024
变形因子	nB	用于变换种子密钥的变形因子
初始向量	32H	仅当变形算法为 SM4-CBC-MAC 时存在， 恒为 16 字节长
动态口令类型	1H	DPT_SM3　　0x01：SM3

		DPT_SM4 0x02：SM4
因子组合类型	1H	FCT_T 0x01：T FCT_C 0x02：C 以及三者的组合： FCT_T|FCT_C 0x03：T|C FCT_T|FCT_Q 0x04：T|Q FCT_C|FCT_Q 0x05：C|Q FCT_T|FCT_C|FCT_Q 0x06：T|C|Q 至少包含 T/C 的其中一个参数，Q 为可选参数。 只有在因子组合类型中含 T 时，下面关于时间因子的项存在; 且只有在因子组合类型中含 C 时,下面关于事件因子的项存在; 只有在因子组合类型中含 Q 时，下面关于挑战因子的项存在。
时间窗口	3N	用于验证 OTP 的时间浮动范围，浮动范围 000-127,一般选择 000-010 范围。
时间因子输入方式	1N	0 – 输入 T 的方式，直接输入时间因子 T 1 – 输入 T0 和 Tc 的方式。T=T0/Tc。 可选，由因子组合类型决定，仅当含 T 输入时存在
T0	16H	T0 是以 UTC 时间或用户选择的时间标准为计量标准的一个 8 字节整数。 仅当时间因子输入方式为 1 时存在 可选，由因子组合类型决定，仅当含 T 输入时存在
Tc	2N	Tc 是以秒为单位的口令变化周期，最大为 60s.即取值为 1-60. 仅当时间因子输入方式为 1 时存在 可选，由因子组合类型决定，仅当含 T 输入时存在
时间因子 T	16H	时间因子，恒为 8 字节长 仅当时间因子输入方式为 0 时存在 可选，由因子组合类型决定，仅当含 T 输入时存在
时间偏移方向	1N	0 – 不偏移 1 – 取正，当前 T 加上偏移量 2 – 取负，当前 T 减去偏移量 不偏移时，选其一，下一个域取 000，当为 0 时下一域只能为 000 可选，由因子组合类型决定，仅当含 T 输入时存在
时间偏移值	3N	时间偏移值，用于得到时间窗口对应的基准时间，针对时间因子 T 而言。 可选，由因子组合类型决定，仅当含 T 输入时存在
事件窗口	3N	用于验证 OTP 的事件变化范围，浮动范围 000-010 可选，由因子组合类型决定，仅当含 C 输入时存在
事件因子	8H	事件因子，恒为 4 字节长 可选，由因子组合类型决定，仅当含 C 输入时存在
挑战因子长度	4N	挑战因子长度，长度范围为 4-255 字节 可选，由因子组合类型决定，仅当含 Q 输入时存在
挑战因子	nA	挑战因子，参与到动态口令生成过程中的一种数据。 可选，由因子组合类型决定，仅当含 Q 输入时存在
种子密文 MAC 算法模式	2H	对子密钥加密的种子密文的 MAC 验证方式： 00 - 不验证密文 MAC 01 - ISO9797-1 MAC 算法模式 1 使用 MAC 密钥 CBC 模式加密数据， 取最后一段密文；
IV	32H	仅当种子密文 MAC 算法模式为 1 时存在该域 验证密文 MAC 时使用的 IV
种子密文 MAC	32H	仅当种子密文 MAC 算法模式为 1 时存在该域 待验证的种子密文 MAC 如果 MAC 不满 32H，则左对齐后右补字符‘0’；MAC 校验时忽略右边为 0 的位。
种子密文长度	3N	子密钥加密的种子密文的长度，字节数
种子密文	n*2 H	子密钥加密的种子密文
PAD 标识	2H	标识随机种子被保护密钥加密前数据的填充规则

		取值范围：00－05 或 10 － 11，详细规则参见 4.1
待验证 OTP 长度	2 N	指定输出的 OTP 长度（4-10）
OTP	nN	待验证 OTP 值
响应报文		
报文头	n A	不做任何修改直接返回给主机
响应代码	2 A	F9
错误码	2 A	00：成功 01：种子密文 MAC 验证失败 04：非法的根密钥类型 15：无效的输入数据（无效的格式/字符或长度错误） …
时间窗口偏移方向	1N	0 – 不偏移 1 – 取正 (时间因子 T 加上窗口偏移值) 2 – 取负 (时间因子 T 减去窗口偏移值) 验证成功时存在，仅当因子组合方式中含 T 时有意义，不含 T 时默认不偏移取 0 （注意：时间窗口偏移值是建立在“时间因子 T +/- 输入的时间偏移值”的基础之上的。即此时窗口对应的时间因子 T 由输入时间因子 T 和时间偏移值决定。）
时间窗口偏移值	3N	时间窗口实际偏移值(为 000 时不偏移) 最大值取决于时间窗口输入值 验证成功时存在，仅当因子组合方式中含 T 时有意义，不含 T 时默认不偏移取 000
事件窗口偏移方向	1N	0 – 不偏移 1 – 取正 （事件因子 C 加上窗口偏移值） 2 – 取负 （事件因子 C 减去窗口偏移值） 验证成功时存在，仅当因子组合方式中含 C 时有意义，不含 C 时默认不偏移取 0
事件窗口偏移值	3N	事件窗口实际偏移值（为 000 时不偏移） 最大值取决于事件窗口输入值 验证成功时存在，仅当因子组合方式中含 C 时有意义，不含 C 时默认不偏移取 000

4. 安全机制

下述算法及填充均依据 PBOC2.0 的标准规范。

【表示约定】：

- Y = DES(K)[X]，表明对数据块X使用单长度密钥K进行DES加密运算，得到密文Y；
- X = DES^{-1}(K)[Y]，表明使用单长度密钥K进行DES解密数据Y，得明文X；

4.1. 分组对称算法的数据填充模式

密码机支持的 DES/3DES/AES/SM1/SM4 对称算法，均为分组加密算法，被加密的数据长度必须是分组长度的整数倍。针对不定长的明文数据，在加密前需按照一定的规则进行填充，以使其长度符合加密的要求，解密后再进行还原去除填充的数据。

DES/3DES 算法，分组长度 N 为 8 字节；

AES/SM1/SM4 算法，分组长度 N 为 16 字节；

4.1.1. 模式 0

遵循 PBOC 2.0 的加解密数据填充规范。

如果输入数据 MSG 的长度不是分组长度 N 的整数倍，在 MSG 的右端加上一个字节的 0x80，然后在右边加上最少的 0x00 字节，使得结果报文 MSG':= (MSG||'80'||'00'||…||'00')的长度是分组长度 N 的整数倍；

如果输入数据 MSG 的长度是分组长度 N 的整数倍，则不填充；

【注意】若原始数据的最末字节可能是 0x80，则加解密运算不建议使用此模式。

4.1.2. 模式 1

遵循 ISO/IEC 9797-1 的 PADDING 模式 2 标准。等同于 PBOC 2.0 的 MAC 运算数据填充规范。

对输入数据 MSG，在 MSG 的右端强制加上一个字节的 0x80，然后在右边加上最少的 0x00 字节，使得结果报文 MSG':= (MSG||'80'||'00'||…||'00')的长度是分组长度 N 的整数倍。

4.1.3. 模式 2

遵循 ISO/IEC 9797-1 的 PADDING 模式 1 标准。等同于 ANSI X9.19 中定义的规范，符合银联规范应用中的 MAC 运算填充模式。

如果输入数据 MSG 的长度不是分组长度 N 的整数倍，在 MSG 的右端加上最少的 0x00 字节，使得结果报文 MSG':= (MSG||'00'||'00'||…||'00')的长度是分组长度 N 的整数倍；

如果输入数据 MSG 的长度是分组长度 N 的整数倍，则不填充；

【注意】若原始数据的最末字节可能是 0x00，则加解密运算不建议使用此模式。

4.1.4. 模式 3

遵循 ANSI X9.23 中定义的规范。

对输入数据 MSG，在 MSG 的右端强制加上一个字节的填充字符，然后在右边加上最少的 0x00 字节，且添加的最后一个字节标识添加的 PAD 的字节数，使得结果报文 MSG':= (MSG||'00'||'00'||…||'0X')的长度是分组长度 N 的整数倍，最末字节 X 取值为 0x01 – 0x10。

4.1.5. 模式 4

遵循 PKCS#5 中定义的规范。

对输入数据 MSG，在 MSG 的右端添加 N-(||MSG|| % N)个 PAD 字符，每个字符取值为 N-(||MSG|| % N)；也就是说，对 MSG，最右端数据块，缺 m 个字节则补充 m 个数值 m，最少补 1 个 0x01，最多补 16 个 0x10（当 MSG 长度为分组长度 N 字节的整数倍时）。

4.1.6. 模式 5

密码机不处理数据的 PADDING，外部应用系统将数据填充到加密算法的分组长度 N 的整数倍。

4.1.7. 模式 10

PBOC3.0 规范的加解密数据填充模式；

对输入数据 MSG，先在 MSG 的左端填充 1-3 个字节的数据长度（ASN.1 编码对象的长度域），然后进行类同模式 0 的填充处理：若满足分组长度 N 的整数倍则不再填充，否则填充'80'||'00'||…||'00'。

4.1.8. 模式 11

对输入数据 MSG，先在 MSG 的左端填充 1-3 个字节的数据长度（ASN.1 编码对象的长度域），然后进行类同模式 1 的填充处理：在添加了长度域的数据块的右端强制加上一个字节的 0x80，然后在右边加上最少的 0x00 字节。

4.2. 对称加解密运算模式

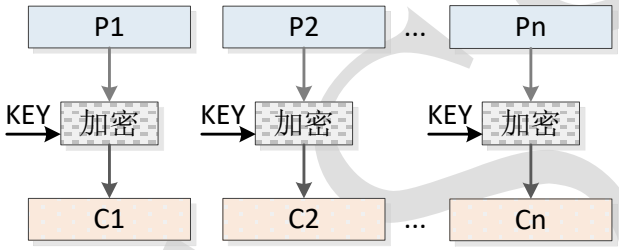
约定：X_1，X_2，. . . , X_k 为明文数据块，Y_1, Y_2, . . . , Y_k 为密文数据块，每块的长度与分组算法的数据块长度一致；

4.2.1. ECB 模式

Electronic Code Book，电子密码本模式。

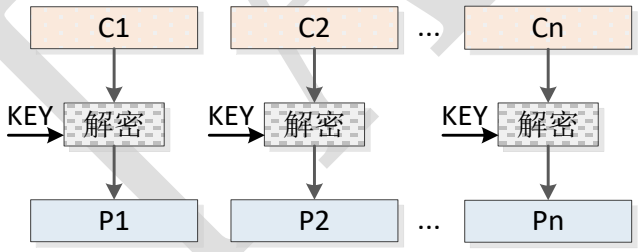
a) 加密

用加密密钥 KEY 以 ECB 模式的分组加密算法将明文块 P_1，P_2，. . . , P_n 加密为密文块 C_1, C_2, . . . , C_n



ECB模式加密

b) 解密



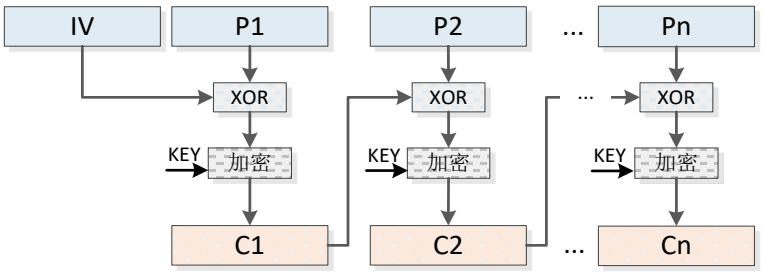
ECB模式解密

4.2.2. CBC 模式

Cipher Block Chaining，密码分组链接模式。

a) 加密

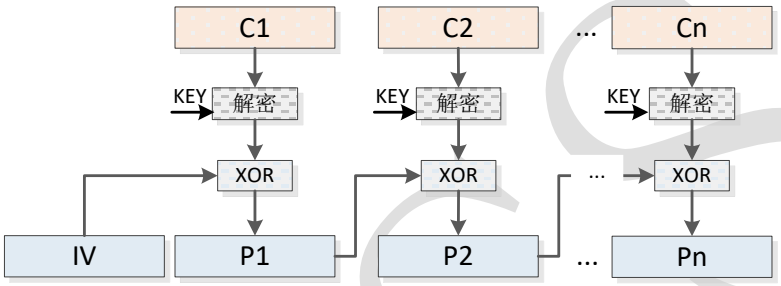
用加密密钥 K 以 CBC 模式的分组加密算法将块 P_1，P_2，. . . , P_n 加密为密文块 C_1, C_2, . . . , C_n



CBC模式加密

IV，为一个分组长度的初始向量数据块；

b) 解密



CBC模式解密

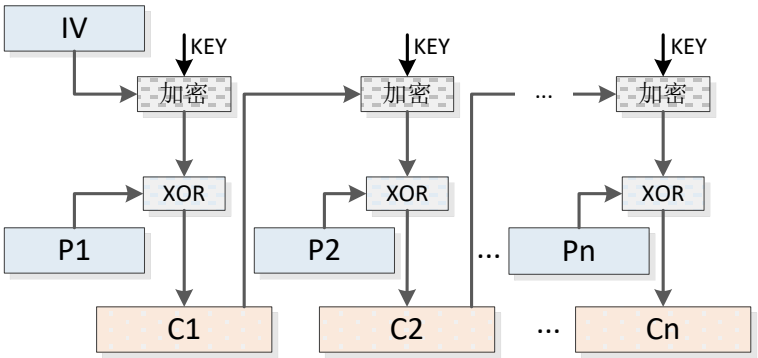
其中 IV，需与加密时的 IV 一致；

4.2.3. CFB 模式

Cipher FeedBack，密码反馈模式。SJJ1310 金融数据密码机按一个分组长度的反馈进行加密解密运算。

a) 加密

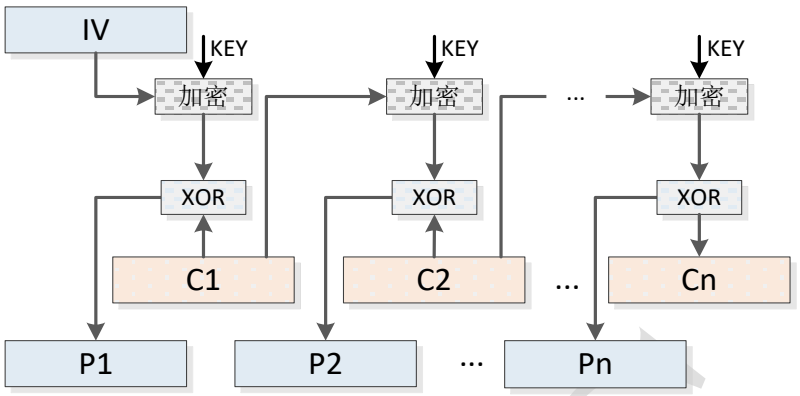
用加密密钥 K 以 CFB 模式的分组加密算法将块 P_1，P_2，. . . , P_n 加密为密文块 C_1, C_2, . . . , C_n



CFB模式加密

IV，为一个分组长度的初始向量数据块；

b) 解密



CFB模式解密

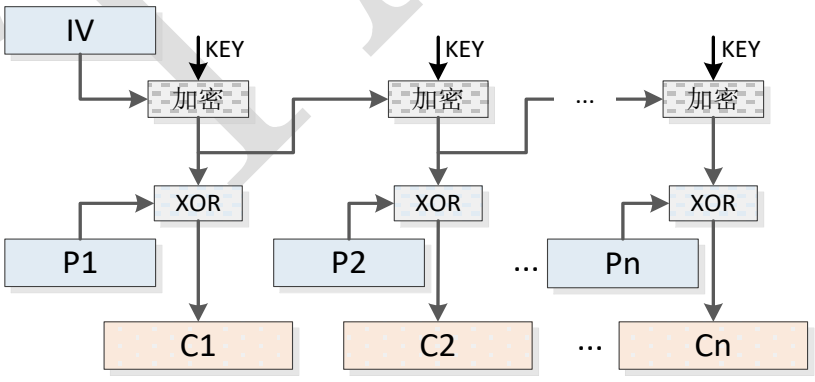
其中 IV，需与加密时的 IV 一致；

4.2.4. OFB 模式

Output FeedBack，输出反馈模式。SJJ1310 金融数据密码机按一个分组长度的反馈进行加密解密运算。

a) 加密

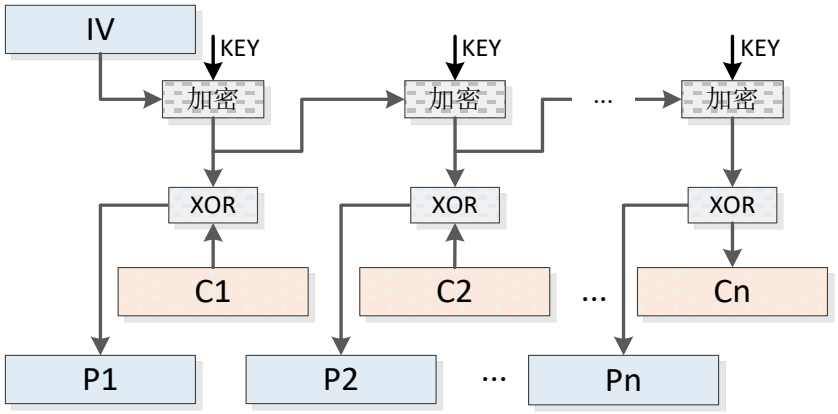
用加密密钥 K 以 OFB 模式的分组加密算法将块 P_1，P_2，. . . , P_n 加密为密文块 C_1, C_2, . . . , C_n



OFB模式加密

IV，为一个分组长度的初始向量数据块；

b) 解密



OFB模式解密

其中 IV，需与加密时的 IV 一致；

4.3. MAC 运算模式

4.3.1. 模式 01

ISO/IEC 9797-1 MAC 算法 1，支持 SM1/SM4/DES/3DES/AES 算法类型的密钥。当密钥为单长度 DES 算法时等同于 ANSI X9.9 标准的 MAC 算法，当密钥为 128 位分组算法时等同于 PBOC 2.0 规范的 128 位分组 MAC 运算模式。

以一个分组长度 0x00 为初始 IV，使用密钥 K 对数据进行 MAC 运算，步骤：

1) 使用密钥 K 对数据进行 CBC 模式加密运算；

2) 取最后一组密文 H_k 得到最终的数据 MAC。

4.3.2. 模式 03

ISO/IEC 9797-1 MAC 算法 3，仅支持双长度 DES 密钥，等同于 ANSI X9.19 标准的 MAC 算法。

以 8 字节 0x00 为初始 IV，使用密钥 $K=(K_L||K_R)$ 对数据计算 MAC，步骤：

1) 使用 K_L 对数据分组 $X_1,X_2,\ldots X_k$ 进行单 DES CBC 模式加密，如下表示：

$$H_i = DES(K_L)[X_i \oplus H_{i-1}]$$

其中 H_0 为初始 8 字节全 0x00 的 IV；最后一组密文为 H_k。

2) 使用 KR 解密 H_k，得 H_{k+1}；

3) 再用 KL 加密 H_{k+1}，得到最终的数据 MAC；

4.4. 子密钥分散算法

用于使用一个 16 字节的发行商主密钥 IMK 分散得到 IC 卡卡片子密钥。

分散因子 D，以主账号和主账号序列号组成，8 字节数据块。

分散算法，使用 K 加密（D || D 的非）得到子密钥：

Z := ALG(IMK)[D || D⊕(‘FF’||’FF’||’FF’||’FF’||’FF’||’FF’||’FF’||’FF’)];

4.5. 会话密钥产生算法

基于 64/128 位分组加密算法的会话密钥分散方法。

MAC 和数据加密过程密钥的产生如下所述，本接口依据用户需求，采用第二种算法产生双长度 DES 过程密钥。

4.5.1. PBOC 8 字节会话密钥

会话密钥模式 01。仅适用于源密钥为双长度 3DES 密钥算法类型，产生的 8 字节会话密钥为单 DES 密钥。

第一步：卡片/发卡行决定是使用 MAC 密钥 A 和 B 还是数据加密密钥 A 和 B 来进行所选择的算法处理。(以后统称为“Key A”和“Key B”)

第二步：将当前的 ATC 在其左边用十六进制数字’0’填充到 8 个字节，用 Key A 和 Key B 对该数据作如图 9 所示的 3-DES 运算产生会话密钥 A。

Z := 3-DES(Key)[‘00’ || ‘00’ || ‘00’ || ‘00’ || ‘00’ || ‘00’ || ATC]

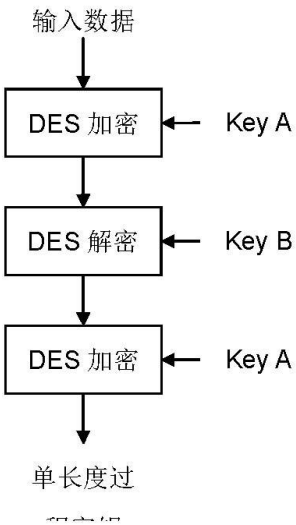


图1 单长度会话密钥的产生

4.5.2. PBOC 16 字节会话密钥

会话密钥模式 02。

第一步：卡片/发卡行决定是使用 MAC 密钥还是数据加密密钥来进行所选择的算法处理；

第二步：将当前的 ATC 在其左边用十六进制数字'0'填充到 8 个字节记为数据源 A，将当前的 ATC 异或十六进制值 FFFF 后在其左边用十六进制数字'0'填充到 8 个字节记为数据源 B，将数据源 A 和数据源 B 串连，用选定的密钥对该数据作 ECB 模式加密运算产生会话密钥；

Z := Alg-EncECB(Key)['00' || '00' || '00' || '00' || '00' || '00' || ATC ||'00' || '00' || '00' || '00' || '00' || '00' || (ATC ⊕ 'FFFF')]

若密钥算法为 3DES，为了符合对 DES 密钥奇校验的要求，DES 密钥每个字节的最低位应被设成能够保证密钥的 8 个或 16 个字节的每一个都有奇数个非 0 位。

4.5.3. 异或产生单长度 DES 会话密钥

会话密钥模式 03。仅适用于源密钥为双长度 3DES 密钥算法类型，产生的 8 字节会话密钥为单 DES 密钥。

$Z := K_L \oplus K_R$；

4.5.4. GP SCP02 安全通道的会话密钥

会话密钥模式 05。用于由 Kenc/Kmac/Kdek 分散产生卡片与主机间安全通道的会话密钥：Senc/Scmac/Srmac/Sdek。

会话密钥因子数据 D := [2 字节密钥类型||2 字节卡计数器||12 字节 0x00]；

会话密钥 Z := Alg-EncCBC(Key)[D]；

a) 2 字节密钥类型

Senc: ‘0182’

Scmac: ‘0101’

Srmac: ‘0102’

Sdek: ‘0181’

b) 2 字节卡计数器

由卡片送出的一个操作计数器

c) 加密算法

由源密钥 Kenc/Kmac/Kdek，采用 3DES-CBC 模式加密会话密钥因子得到会话密钥；

4.6. 密钥校验值产生

使用密钥 K 对一个分组长度的全 0 数据块进行加密运算，得到的密文就是密钥 K 的校验值 KCV，部分指令取密文的前 3 字节或前 8 字节作为 KCV；

4.7. 附加说明

密码机在产生或导入 DES/3DES 密钥时，将对密钥进行强制奇校验；使用 DES/3DES 密钥时，将进行奇校验检查，不符合则返回 10 错。

5. PINBLOCK(数字)格式

下述 PINBLOCK 格式均支持 64 位分组算法和 128 位分组算法加密时的 PIN 块组成格式。

5.1. 格式 01

ANSI X9.8 格式，同时又是国际标准组织（ISO）支持的两种格式之一（ISO 9564 1 – 格式 0），银联规范应用中带主账号信息的格式。

1) 采用 64 位分组算法加密时，该 PINBLOCK 格式将客户 PIN 及帐号按以下方式结合：

- 由数字 0，PIN 的长度，PIN 及填充字符（十六进制数 F）组成 16 个字节的数字块。例如，对 5 个数字的 PIN 92389，则该数字块为：

  0592 389F FFFF FFFF

- 另一 16 个数字块是由 4 个零及帐号的最右 12 个字节不包含校验字节组成。例如，对 13 个数字帐号 4000 0012 3456 2，其中校验字节为 2，则该数字块为：

  0000 4000 0012 3456

- 以上两个数字块异或：

  05 92 38 9F FF FF FF FF

  00 00 40 00 00 12 34 56

  PIN 数据块： 05 92 78 9F FF ED CB A9

  转换成 8 字节 BCD 码：X’05 X’92 X’78 X’9F X’FF X’ED X’CB X’A9

2) 采用 128 位分组算法加密时，该 PINBLOCK 数据块计算：

  05 92 38 9F FF FF FF FF FF FF FF FF FF FF FF FF

  00 00 00 00 00 00 00 00 00 00 40 00 00 12 34 56

  PIN 数据块： 05 92 38 9F FF FF FF FF FF FF BF FF FF ED CB A9

转换成 16 字节 BCD 码：X’05 X’92 X’38 X’9F X’FF X’FF X’FF X’FF X’FF X’FF X’BF X’FF X’FF X’ED X’CB X’A9

5.2. 格式 02

支持 Docutel ATMs 应用，PIN 长度限制 4-6。无需账号信息。由 PIN 长度、6 位数字 PIN 和用户定义的数字填充串组成。

如果 PIN 少于 6 个数字，则左对齐后右边填充’0’。

PIN BLOCK 数据块为：

1 位 PIN 长度 || n 位 PIN || 用户定义的填充数字

例如，对 5 位数字的 PIN 92389，则

64 位分组算法下 PIN 块：5923 8909 8765 4321

128 位分组算法下 PIN 块：5923 8909 8765 4321 87654321 87654321

5.3. 格式 03

支持 Diebold 和 IBM ATMs 应用。它也可应用在不含 PIN 长度的 Docutel 格式。PIN 块由客户 PIN 和填充字符’F’组成。

例如，对 5 个数字的 PIN 92389，则

64 位分组算法下 PIN 块：9238 9FFF FFFF FFFF

128 位分组算法下 PIN 块：9238 9FFF FFFF FFFF FFFF FFFF FFFF FFFF

5.4. 格式 04

PLUS网络采用的PIN块格式。

1) 采用 64 位分组算法加密时，该 PINBLOCK 格式将客户 PIN 及帐号按以下方式结合：

- 由数字 0，PIN 的长度，PIN 及填充字符（十六进制数 F）组成 16 个字节的数字块。例如，对 5 个数字的 PIN 92389，则该数字块为：

  0592 389F FFFF FFFF

- 另一 16 个数字块是由 4 个零及帐号的最左 12 个字节组成。例如，对 16 个数字帐号 2283 4000 0012 3456，其中校验字节为 6，则该数字块为：

  0000 2283 4000 0012

- 以上两个数字块异或：

  05 92 38 9F FF FF FF FF
  00 00 22 83 40 00 00 12

  PIN块：05 92 1A 1C BF FF FF ED

2) 采用 128 位分组算法加密时，该 PINBLOCK 数据块计算：

  05 92 38 9F FF FF FF FF FF FF FF FF FF FF FF FF
  00 00 00 00 00 00 00 00 00 00 22 83 40 00 00 12

  PIN 块：05 92 38 9F FF FF FF FF FF FF DD 7C BF FF FF ED

  转换成 16 字节 BCD 码：X’05 X’92 X’38 X’9F X’FF X’FF X’FF X’FF X’FF X’FF X’DD X’7C X’BF X’FF X’FF X’ED

注意： 当PIN块采用格式04时，它的帐号域长度必须为18字节。

对PIN转换CA和CC命令，存在两个格式域。如果哪一个正好为格式04，则该帐号域必须为18个字符。若该帐号域少于18个数字，则必须右对齐并左填充X’F。

以下命令可以使用格式04：

BC，BE，CA，CC，CG，DA，DC，EA，EC，EG，JC，JE。当浏览这些命令的细则时，应考虑对应该格式时相应帐号域需做的改变（注意：只要命令中出现格式04，则帐号域应由原来的12位变为18位）。

5.5. 格式 05

格式05为ISO 9564-1 格式1。由以下十六进制数值表示的PIN格式：

1N P_1…P_NR…R

其中

N为PIN的长度（4—C）

P_1…P_N为N个数字的PIN

R…R为随机填充数，填充至分组长度

当输入PIN格式为格式05时必须执行以下有效性校验：

- PIN块第一个字符必须为值1，否则返回错误码20。
- PIN块第二个字符(N)取值范围必须为十六进制数4-C，否则返回错误码24。
- PIN数字（位置3—(N+2)）取值范围必须为0-9，否则返回错误码20。

5.6. 格式 06

格式06为ISO 9564-1 Format 2，等同于格式34。由以下十六进制数值表示的PIN格式：

2N P_1…P_NF…F

其中

N为PIN的长度（4—C）

P_1…P_N为N个数字的PIN

F…F为填充字符，填充至分组长度

当输入PIN格式为格式06时必须执行以下有效性校验：

- PIN块第一个字符必须为值2，否则返回错误码20。
- PIN块第二个字符(N)取值范围必须为十六进制数4-C，否则返回错误码24。
- PIN数字（位置3—(N+2)）取值范围必须为0-9，否则返回错误码20。

5.7. 格式 07

银联规范应用中不带主账号信息的PIN格式，支持64位和128位分组算法。由以下十六进制数值表示的PIN格式：

0N P_1…P_NF…F

其中

N为PIN的长度（4—C）

P_1…P_N为N个数字的PIN

F…F为填充字符，填充至分组长度

5.8. 格式 11

扩展的 ANSI X9.8 格式。

1) 采用 64 位分组算法加密时，与格式 01 相同。该 PINBLOCK 格式将客户 PIN 及帐号按以下方式结合：

- 由数字 0，PIN 的长度，PIN 及填充字符（十六进制数 F）组成 16 个字节的数字块。例如，对 5 个数字的 PIN 92389，则该数字块为：

  0592 389F FFFF FFFF

- 另一 16 个数字块是由 4 个零及帐号的最右 12 个字节不包含校验字节组成。例如，对 13 个数字帐号 4000 0012 3456 2，其中校验字节为 2，则该数字块为：

  0000 4000 0012 3456

- 以上两个数字块异或：

  05 92 38 9F FF FF FF FF

  00 00 40 00 00 12 34 56

  ———————————————————

PIN 数据块： 05 92 78 9F FF ED CB A9

转换成 8 字节 BCD 码：X’05 X’92 X’78 X’9F X’FF X’ED X’CB X’A9

2) 采用 128 位分组算法加密时，该 PINBLOCK 数据块计算：

05 92 38 9F FF FF FF FF FF FF FF FF FF FF FF FF

00 00 40 00 00 12 34 56 00 00 00 00 00 00 00 00

———————————————————————————————

PIN 数据块： 05 92 78 9F FF ED CB A9 FF FF FF FF FF FF FF FF

即在 64 位分组 PIN 数据块的后面填充 8 字节 0XFF。

5.9. 格式 34

EMV PIN数据块格式，等同于ISO 9564-1 Format 2。由以下十六进制数值表示的PIN格式：

2N P_1…P_NF…F

其中

N为PIN的长度（4—C）

P_1…P_N为N个数字的PIN

F…F为填充字符，填充至分组长度

5.10.格式 35

Europay/MasterCard for their Pay Now & Pay Later products应用的PIN数据块格式。

1) 采用 64 位分组算法加密时，该 PINBLOCK 格式将客户 PIN 及帐号按以下方式结合：

- 由数字 2，PIN 的长度，PIN 及填充字符（十六进制数 F）组成 16 个字节的数字块。例如，对 5 个数字的 PIN 34567，则该数字块为：

  2534 567F FFFF FFFF

- 另一 16 个数字块是由 4 个零及帐号的最右 12 个字节不包含校验字节组成。例如，对 13 个数字帐号 4000 0012 3456 2，其中校验字节为 2，则该数字块为：

  0000 4000 0012 3456

- 以上两个数字块异或：

  25 34 56 7F FF FF FF FF

  00 00 40 00 00 12 34 56

  ————————————————————

PIN 数据块： 25 34 16 7F FF ED CB A9

2) 采用 128 位分组算法加密时，该 PINBLOCK 数据块计算：

25 34 56 7F FF FF FF FF FF FF FF FF FF FF FF FF

00 00 00 00 00 00 00 00 00 00 40 00 00 12 34 56

PIN 数据块： 25 34 56 7F FF FF FF FF FF FF BF FF FF ED CB A9

转换成 16 字节 BCD 码：X’25 X’34 X’56 X’7F X’FF X’FF X’FF X’FF X’FF X’FF X’BF X’FF X’FF X’ED X’CB X’A9

5.11.格式 41

VISA/PBOC 不使用当前 PIN 进行 PIN 修改的格式。使用新 PIN 和唯一 DEA 密钥的部分生成 PIN 块：

- 提取卡应用唯一 DEA 密钥 A（UDK-A，即*MK-AC 的卡片子密钥的左半部分）的最右 8 位并且用十六进制 0 填充左边，构成 16 个十六进制数字；假设*MK-AC 的卡片子密钥：9726E0803B070497 57D0299BDA7CF42F，则该数据段的组成：

  00000000 3B070497

- 由数字 0，PIN 的长度，PIN 及填充字符（十六进制数 F）组成 16 个十六进制数字块。例如，对 5 个数字的 PIN 92389，则该数字块为：

  0592 389F FFFF FFFF

- 以上两个数字块异或：

  05 92 38 9F FF FF FF FF

  00 00 00 00 3B 07 04 97

PIN 数据块： 05 92 38 9F C4 F8 FB 68

转换成 8 字节 BCD 码：X’05 X’92 X’38 X’9F X’C4 X’F8 X’FB X’68

5.12.格式 42

VISA/PBOC 使用当前 PIN 进行 PIN 修改的格式。使用当前 PIN、新 PIN 和唯一 DEA 密钥的部分生成 PIN 块：

- 提取卡应用唯一 DEA 密钥 A（UDK-A，即*MK-AC 的卡片子密钥的左半部分）的最右 8 位并且用十六进制 0 填充左边，构成 16 个十六进制数字；假设*MK-AC 的卡片子密钥：9726E0803B070497 57D0299BDA7CF42F，则该数据段的组成：

  00000000 3B070497

- 由数字 0，新 PIN 的长度，新 PIN 及填充字符（十六进制数 F）组成 16 个十六进制数字块。例如，对 6 个数字的新 PIN 123456，则该数字块为：

  0612 3456 FFFF FFFF

- 由当前 PIN 及填充字符（十六进制数 0）组成 16 个十六进制数字块。例如，对 6 个数字的当前 PIN 111111，则该数字块为：

  1111 1100 0000 0000

  - 以上三个数字块异或：

    00 00 00 00 3B 07 04 97

    06 12 34 56 FF FF FF FF

    11 11 11 00 00 00 00 00

    ————————————————————

  PIN 数据块： 17 03 25 56 C4 F8 FB 68

  转换成 8 字节 BCD 码：X’17 X’03 X’25 X’56 X’C4 X’F8 X’FB X’68

5.13.格式 47

ISO 9564 1 – 格式 3。

1) 采用 64 位分组算法加密时，该 PINBLOCK 格式将客户 PIN 及帐号按以下方式结合：

- 由数字 3，PIN 的长度，PIN 及填充字符（十六进制数 F）组成 16 个字节的数字块。例如，对 5 个数字的 PIN 92389，则该数字块为：

  3592 389F FFFF FFFF

- 另一 16 个数字块是由 4 个零及帐号的最右 12 个字节不包含校验字节组成。例如，对 13 个数字帐号 4000 0012 3456 2，其中校验字节为 2，则该数字块为：

0000 4000 0012 3456

- 以上两个数字块异或：

35 92 38 9F FF FF FF FF

00 00 40 00 00 12 34 56

PIN 数据块： 35 92 38 9F FF ED CB A9

转换成 8 字节 BCD 码：X’35 X’92 X’38 X’9F X’FF X’ED X’CB X’A9

2) 采用 128 位分组算法加密时，该 PINBLOCK 数据块计算：

35 92 38 9F FF FF FF FF FF FF FF FF FF FF FF FF

00 00 00 00 00 00 00 00 00 00 40 00 00 12 34 56

PIN 数据块： 35 92 38 9F FF FF FF FF FF FF BF FF FF ED CB A9

转换成 16 字节 BCD 码：X’35 X’92 X’38 X’9F X’FF X’FF X’FF X’FF X’FF X’FF X’BF X’FF X’FF X’ED X’CB X’A9

6. PINBLOCK(字符)格式

下述字符 PINBLOCK 格式均支持 64 位分组算法和 128 位分组算法加密时的 PIN 块组成格式。字符 PIN 同时包含纯数字的 PIN。

6.1. 格式 00

1) 采用 64 位分组算法加密时，该字符 PINBLOCK 格式将客户字符 PIN 及帐号按以下方式结合：

- 由 PIN 明文扩展 ASCII 码表示的 Expanded Hex 型字符串，如果不足 24 字节（48H），则在后面填补“00”。例如，对 8 个字符的 PIN 123456AB，则该 48H 数据块为：

  313233343536414200000000000000000000000000000000

- 由账号扩展为 ASCII 码表示的 Expanded Hex 型字符串，如果不足 24 字节（48H），则在后面填补“00”。例如，对 12 个数字帐号 4000 0012 3456，则该 48H 数据块为：

  343030303030313233343536000000000000000000000000

- 以上两个数字块异或：

  313233343536414200000000000000000000000000000000

  343030303030313233343536000000000000000000000000

PIN 数据块： 0502 0304 0506 7070 3334 3536 0000 0000 0000 0000 0000 0000

转换成 24 字节 BCD 码：X’05 X’02 X’03 X’04 X’05 X’06 X’70 X’70 X’33 X’34 X’35 X’36 X’00 X’00 X’00 X’00 X’00 X’00 X’00 X’00 X’00 X’00 X’00 X’00

2) 采用 128 位分组算法加密时，该字符 PINBLOCK 数据块为 32 字节（64H），由 PIN 和账号分别扩展并填充到 64H 后，异或计算，如下：

313233343536414200000000000000000000000000000000000000000000000000000000

343030303030313233343536000000000000000000000000000000000000000000000000

PIN 数据块： 0502 0304 0506 7070 3334 3536 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000

转换成 32 字节 BCD 码：X’05 X’02 X’03 X’04 X’05 X’06 X’70 X’70 X’33 X’34 X’35 X’36 X’00 X’00 X’00 X’00 X’00 X’00 X’00 X’00 X’00 X’00 X’00 X’00 X’00 X’00 X’00 X’00

6.2. 格式 01

将 PAN 号与 PIN 明文串联，按照分组长度进行填充，已满足分组长度则不进行填充；若不满足分组长度，则填充至分组长度，填充字符使用需要填充的字符个数对应的字符，例如缺少 6 个字符，则填充 6 个字符'6'；再例如需要填充 15 个字符，则填充 15 个'F'。用 ZPK 对填充后的结果加密，得到 PIN 密文。

例如，对 8 个字符的 PIN 123456AB，和 12 个数字帐号 4000 0012 3456，

1) 在 64 分组算法下的 PINBLOCK 块为，PAN || PIN || 4-byte ‘4’：

34303030303031323334353 6 3132333435364142 34343434

转换成 24 字节 BCD 码：X’34 X’30 X’30 X’30 X’30 X’30 X’31 X’32 X’33 X’34 X’35 X’36 X’31 X’32 X’33 X’34 X’35 X’36 X’41 X’42 X’34 X’34 X’34 X’34

2) 在 128 分组算法下的 PINBLOCK 块为，PAN || PIN || 12-byte ‘C’：

34303030303031323334353 6 3132333435364142 43434343434343434343434343

转换成 32 字节 BCD 码：X’34 X’30 X’30 X’30 X’30 X’30 X’31 X’32 X’33 X’34 X’35 X’36 X’31 X’32 X’33 X’34 X’35 X’36 X’41 X’42 X’43 X’43 X’43 X’43 X’43 X’43 X’43 X’43 X’43 X’43 X’43 X’43

6.3. 格式 02

该格式要求 PIN 及 PAN 都不能超过 16 字节（16 个字符或数字）。

- 由 PIN 明文扩展 ASCII 码表示的 Expanded Hex 型字符串，如果不足 16 字节（32H），则在后面填补“00”。例如，对 8 个字符的 PIN 123456AB，则该 32H 数据块为：

3132333435364142000000000000000

- 由账号扩展为ASCII码表示的Expanded Hex型字符串，如果不足16字节（32H），则在后面填补“00”。例如，对12个数字帐号4000 0012 3456，则该32H数据块为：

  34303030303031323334353600000000

- 以上两个数字块异或：

  3132333435364142000000000000000

  34303030303031323334353600000000

PIN数据块： 0502 0304 0506 7070 3334 3536 0000 0000

转换成16字节BCD码：X’05 X’02 X’03 X’04 X’05 X’06 X’70 X’70 X’33 X’34 X’35 X’36 X’00 X’00 X’00 X’00

6.4. 格式 03

该格式要求 PIN 长度 4-8 字节（4-8 个字符或数字）。

- 国际算法说明：

1. 取帐号（不足 16 位，前补‘0’）；
2. 将处理后的帐号从 16 字节数字为 8 字节二进制。；
3. PIN 明文为 8 字节字符混编，不足 8 字节，后补 0x00 补足；
4. 用 2 步和第三步的结果，进行异或计算；
5. 使用 PIK 密钥，对异或结果采用 DES 算法加密；
6. 把加密后的结果，转换为 16 字节 16 进制字符串；

例子：

帐号：12345678

PIN：Lei_1234

PIK：0x1234567890ABCDEF

则计算过程步骤为：

1. 取帐号 12345678，前补 0 补齐 16 位，处理后的结果为 0000000012345678；
2. 将 0000000012345678 转换为 0X0000000012345678；
3. 取 PINLei_1234，BCD 扩展为 0x4C65695F31323334；
4. 将第 2 步结果和第 3 步异或处理，异或后的结果为 0X4C65695F2306654C;
5. 用 PIK 密钥 DES 加密第 4 步的结果；

- 国密算法说明

1. 取帐号号，前补 0 补齐 32 位；
2. 将处理后的帐号号从 32 字节数字转换为 16 字节二进制；

3. PIN 明文做 BCD 扩展，不足 16 字节的后补 0X00；

4. 第 2 步和第 3 步的结果异或处理；

5. 用 PIK 密钥用 SM4 算法加密第 4 步的结果；

例子:

帐号：12345678

PIN：Lei_1234

PIK：0x1234567890ABCDEF1234567890ABCDEF

则计算步骤为：

1. 取帐号 12345678 前补 0 补齐 32 位，处理后的结果为 00000000000000000000000012345678；

2. 处理后的帐号转换：将 00000000000000000000000012345678 转换为 0X00000000000000000000000012345678；

3. 取 PINLei_1234，BCD 扩展为 0x4C65695F31323334，补位之后为 0x4C65695F3132333400000000000000；

4. 第 2 步和第 3 步异或，异或后的处理结果为 0X4C65695F3132333400000000012345678

5. 用 PIK 密钥用 SM4 算法加密第 4 步结果；

7. 错误码说明

代码	具体描述
00	没有错误
01	验证错误或密钥奇校验错
02	算法的密钥长度不符合/密钥校验值验证失败/pfx内证书和密钥对验证失败
03	无效的算法模式
04	无效的密钥类型代码

05	无效的密钥长度标识/无效的方案ID/无效的对称密钥类型代码/无效的哈希算法标识
06	无效的密钥成份个数或非法的偏移量/无效的加密标识或签名算法标识
07	密钥校验值比对失败/无效的填充模式标识
08	输入数据类型无效
09	导出的密钥个数无效
10	源密钥奇校验错
12	用户存储区内容无效。复位、重启或覆盖
13	LMK 错误
14	LMK组003-005 下加密的PIN无效
15	无效的输入数据 (无效的格式，无效的字符，或输入的数据长度不够)
16	控制台或打印机没有准备好/没有连接
17	加密机没有在授权状态，或不允许输出明文PIN
18	文档格式定义没有加载
19	指定的 Diebold 表无效
20	PIN数据块没有包含有效的值
21	无效的索引值，或索引/数据长度数溢出
22	无效的帐号
23	无效的PIN数据块格式代码
24	PIN 的长度不到4位或超过12位
25	十进制转换表不正确/PIN校验数据非法
26	密钥标识错
27	密钥长度错
28	无效的密钥类型
29	密码功能不允许
30	无效的用户参考号
31	没有足够的请求入口以提供批量处理
32	输入类型无效，RSA算法标识、MAC报文块模式，ICV模式，交易模式/非法的用户ID长度
33	LMK密钥交换存储区有故障
34	mac算法模式无效

35	mac取值方式无效/keycv 取值方式无效
36	密钥分散级数无效
37	会话密钥类型无效
38	会话密钥算法类型错误
39	非法的数据padding类型
40	无效的固件校验值
41	内在的硬件/软件错误。RAM损坏，无效的错误代码等
42	密码运算失败
43	DER解码失败
45	密钥不存在
46	密钥存储区错误，写密钥失败
49	密钥错误，报告给管理员
50	RSA公钥不符合DER编码规则
51	无效的消息头
52	非对称密钥密钥用法（签名、加密）错误
53	非对称密钥长度非法（RSA 512-2048. ECC 256）
54	DER编码类型非法
55	密钥索引超限
56	RSA密钥指数非法/无效的对称密钥标识，长度标识
57	非对称密钥数据非法/非法的密钥校验值类型
58	ECC密钥曲线标识错误
64	无效的PAN长度
65	交易密钥标识设置为NULL
66	标识非法
67	命令码没有授权
68	命令码禁用
69	PINBLOCK禁用
70	无效的密文数据，解密后去PADDING失败；或密钥头验证失败
71	无效的密文数据，数据解密去padding

74	摘要hash模式不支持
75	单长度的密钥用作双长度或三长度
76	公钥长度错误
77	明文数据块错误
78	密文密钥长度错误
79	哈希算法对象标识符错误
80	报文数据长度错误
81	无效的证书头
82	无效的校验值长度
83	密钥格式错误
84	密钥校验值错误
85	无效的OAEP掩码产生算法
86	无效的OAEP掩码产生算法的摘要算法
87	OAEP参数错
90	密码机接受的请求数据校验错误
91	纵向冗余校验(LRC) 字符和通过输入数据计算的值不匹配
92	命令/数据域中的计数值不正确或不在规定的范围内
93	公钥标识验证失败
94	公钥摘要值验证失败
96	密钥标签长度错
97	内部参数错，如会话密钥模式与源密钥类型冲突
98	报文封装错
99	内部运算错误