金诚信加密键盘技术

使用手册

北京金诚信齐通科技有限公司发布

变 更 记 录

序号	修改条款	修改内容	页号	修改人/日期	批准人/日期	实施日期
1	所有	排版	所有	骆中南 2017/03/10	宁俊强 2017/03/10	2017/03/10
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
11						
12						

注：对该文件内容增加、删除或修改均需填写此变更记录，详细记载变更信息，以保证其可追溯性。

目录

1 概述

本产品是一种多功能密码小键盘。由于本产品的特殊性，要求在使用前，充分阅读该说明书。本产品具有独特的设计理念，不需要硬件开关设置参数，仅采用加电时一次设置键盘的各种参数，以后可以不设置。为了密钥安全，建议键盘工作之前必须使用特别的命令进行初始化处理确保键盘主密钥安全。对工作密钥进行分区管理，以提高密码键盘抗攻击强度。

2 产品分类

密码键盘按界面的尺寸分为 3501A,3501B 和 3503 三种型号。产品型号只标识了界面类型，与内部硬件和软件无关。

3 性能指标

3.1 通讯参数

标准 RS232 串行通讯接口。数据格式可选:N，8，1。1 位起始位，1 位停止位。
通讯速率:9600，可预选 4800、2400、1200 bps。

3.2 通讯参数

十六个按键:0 、1 、2 、3 、4 、5 、6 、7 、8 、9 、更正、确认、取消、和 3 个备用键“*#.”，以 4×4 方式扫描。键值可定义。功能键 8 个按键:分左右两组（有图形而无字符），以 4×1 扫描键盘。
符合 CAS 标准及符合 ISO 9564-1 标准附件 E。

3.3 规范与运算速度

符合中国人民银行规范。
符合 GB/T 15277-1994（等效 ISO8731-1、等效 ANSI X3.92)标准。符合 ISO 9564-1/2（等效 ANSI X9.8）标准。
符合 ISO8731-2（等效 ANSI X9.9）标准。符合 ISO13492-1 标准。
符合 IBM3624 标准。加解密速度<1 秒。

3.4 电气参数

3.4.1 供电要求

DC+5V 直流电源。

3.4.2 功率

工作状态 1W 以下，非工作状态 300mW 以下。

3.4.3 断电密钥保存

电源瞬间及长时间断电时，内存密钥数据不丢失。程序保持 5 年以上有效。

3.5 机械性能

3.5.1 按键寿命

500,000 次以上。

3.5.2 按键压力

3N（牛顿）。

3.5.3 按键行程

0.45mm。

3.5.4 按键材料

不锈钢。

3.5.5 面板材料

不锈钢。

3.5.6 按键表面字符

激光刻字，并涂强漆。

3.6 环境适应性

3.6.1 工作温度

－10℃～+40℃ 相对湿度:40～90%(正常条件下)。

3.6.2 储存温度

－30℃～+55℃ 相对湿度:20～95%(无凝结露)。

3.6.3 大气压力

60～106 Kpa 。

3.7 可靠性

MTBF >20000h，MTTR<30min。

3.8 外形尺寸

长×宽×高:140 mm×94mm×33mm。

3.9 产品重量

0.6kg

4 安装说明

本产品出厂时由深圳市凯明杨公司工厂、各个分公司经过专业训练的技术人员，根据用户实际需要进行必要的设置，银行客户是不需要进行设置。以一般客户在正常使用情况时禁止拆卸，是因为拆卸都会破坏密码键盘内部程序和所有参数，包括破坏用户主密钥和用户工作密钥。

金属密钥键盘主要选择件有:RS-232 电缆、USB 电缆、固定压条、固定螺母等，根据客户安装情况定做。

4.1 密码键盘安装

该产品在正式使用前，需要进行必要的软硬件安装。

首先关闭计算机或终端的电源，将金属密钥键盘，从设备表面的键盘开口处往里装，有 4 个固定螺杆用于固定主键盘。 然后将带有电源线的 RS-232 电缆的一端连接到金属密钥键盘的 RJ45 插座上，另一端插入计算机的 RS-232 串口中。检查无误后，重新打开计算机的电源。

4.2 TEST 测试程序

KMY350TST 测试程序只能作测试用，正常或正式工作不允许运行。

5 附录 A:键盘密钥系统和管理

该密码键盘有两种密钥:主密钥和工作密钥。主密钥相当于 ATM 机上的 A、B 密钥（对密钥加密的密钥），工作密钥相当于 ATM 机上的传输密钥、MAC 密钥（对数据加密的密钥）。

主密钥有 16 个，每个主密钥（TMK）有 8/16/24 个字节。16 个主密钥各对应 4 个工作密钥，每个工作密钥 8/16/24 个字节，因此密钥区共有（16×8+16×8×4 或 16×16+16×16×4 或 24×16+24

×16×4）640/1280/1920 个字节。其中主密钥主要用明文方式下载，也可以用密文方式下载，工作密钥只能用主密钥加密的密文方式下载。主密钥主要做下载工作密钥时解密用，密码键盘收到主密钥 TMK 后（如果是密文方式需要解密得到明文），保存到主密钥区，并对每个主密钥作 BCC 校验。此举提供下装工作密钥时，验证主密钥是否有效。如果主密钥无效，就不能正确解密工作密钥。

工作密钥（WK）有 8/16/24 字节是用指定 M 号的主密钥加密下载的，键盘进行解密得到 WK 保存到 SRAM 中。如果有些银行不用工作密钥，可以直接用主密钥解密。注意加解密前必须正确选择工作方式（6.22）“设置算法处理参数”。建议对 4 个工作密钥进行合理分配，提高密钥钥抗攻击能力。如:0=PIN 加密运算，1=MAC 加密运算，2=数据加密运算，3=数据解密运算。

在每次断电后重新加电时，密码键盘首先验证主密钥有效性（对 16 个主密钥用 BCC 校验）。如果某个主密钥无效，就不能用这个主密钥执行“下装工作密钥”命令，更不能执行“启动密码键盘加密”命令，但可以执行其他命令。

加电后的密码键盘处于关闭状态。如果用“设置开关键盘和按键声音”命令打开键盘后，才允许键盘接受按键，每次按键直接发送相应的键盘码值。用“设置开关键盘和按键声音”命令关闭键盘后，此时按任意键不起作用。如果键盘是关闭的，用“启动密码键盘加密”命令能自动打开键盘后，每次按键将 0～9 变为“*”号发送，其它功能键见附录 6.6 中的解释，完成后能自动关闭键盘。

在“启动密码键盘加密”命令打开键盘时，如果达到命令规定的时间（缺省为超过 20 秒）没有按键，自动发送超时返回信息（ST=80h），如果在该命令前是键盘打开的，会继续打开，但送明码（不送*号）。如果在该命令前是键盘关闭的，回到关闭键盘。

键盘码值按附录 C 处理。

6 附录 B:键盘命令解释

注:协议中有部分字段需要以拆分方式发送或者接受，拆分规则请详见附录 D。需要拆分的字段以<…>注明,不需要拆分的字段以[…]注明
注:红色标记部分为定制产品实现。

常规指令格式

命令格式:[02h]+<Ln>+<CMD>+<DATA>+<BCC>+[03h]
返回格式:[02h]+<Ln>+<ST>+<DATA>+<BCC>+[03h]
02h/03h——表示通信识别头/尾标志。尾标志为可选项,默认不需要。[1Byte] Ln——表示 CMD 和 DATA 或 ST 和 DATA 的字节数。[1Byte] CMD——命令关键字。[1Byte] DATA——交换的数据信息。[(Ln-1)Byte] BCC——从 Ln 到 DATA 的字节异或校验和。 [1Byte] ST——见附录 E 解释。[1Byte]

特殊指令格式

说明:该指令格式用于解决 DATA 字段数据超过 256 字节时，常规指令 Ln 字段不支持的问题。适用于该指令格式的指令都会用[BD]标识。
命令格式:[02h]+<Ln=5>+<CMD>+<DATALen>+<BCC>+<Par1>+<Par2>+<DATA>
返回格式:[02h]+<Ln=5>+<ST>+<DATALen>+<BCC>+[DATA]
02h——表示通信识别头标志。
Ln——表示 CMD 和 DATALen 或 ST 和 DATALen 的字节数,恒为 5。[1Byte] CMD——命令关键字。[1Byte] DATALen——DATA 的长度字符串。[4Byte] BCC——从 Ln 到 DATALen 的字节异或校验和。[1Byte] ST——见附录 E 解释。[1 Byte] Par1——参数 1，为指令功能预留。[1 Byte] Par2——参数 2，为指令功能预留。[1 Byte] DATA——交换的数据信息。[DATALen Byte]
注:DATALen 解释，DataLen 表示后续<DATA>的长度字符串，由 4 字节组成。例如<DATA>长度为 10,则 DataLen 值为"0010"

6.1 下载基础密钥(Derivation Key)（20）

命令: 02h+11h+20h+<DK>+<BCC>+ [03h]
描述: 应用在 DUKPT 上，DK 为 16 字节，主要用于生成新的加密密钥（PIN Entry DeviceKey）。
返回: 02h+01h+<ST>+<BCC>+[03h]。

6.2 下载键盘序列编号(Key Serial Number)（21）

命令: 02h+0Bh+21h+<KSN>+<BCC>+ [03h]
描述: 应用在 DUKPT 上， KSN 为 10 字节，主要用于加密密钥。
返回: 02h+01h+<ST>+<BCC>+[03h]。

6.3 控制 DUKPT 算法（22）

命令: 02h+02h+22h+<CTL>+<BCC>+ [03h]
描述: 应用在 DUKPT 上， CTL 为 1 字节，31h 表示 PIN 运算采用 DUKPT 算法，30h 表示取消 DUKPT 算法。
返回: 02h+01h+<ST>+<BCC>+[03h]。

6.4 启动直接从键盘输入主密钥模式（23）

命令: 02h+02h+23h+<M>+<BCC>+ [03h]
描述:主密钥号 M 为 1 字节（00～0Fh），主密钥为 8/16 字节(对应 DES/3DES)。启动这个功能后，直接在键盘上输入工作密钥，按“确认”键结束，并保存密钥。 不足位用 0x00 填补。
返回: 02h+01h+<ST>+<BCC>+[03h]。

6.5 启动直接从键盘输入工作密钥模式（24）

命令: 02h+03h+24h+<M>+<N>+<BCC>+ [03h]
描述:主密钥号 M 为 1 字节（00～0Fh），N 为 1 字节的工作密钥号（00-03），密钥 为 8/16 字节(对应 DES/3DES)启动这个功能后，直接在键盘上输入工作密钥， 按“确认”键结束，并保存密钥。不足位用 0x00 填补。
返回:02h+01h+<ST>+<BCC>+[03h]。

6.6 取产品版本号等参数（30）

命令:02h+01h+30h+<BCC>+ [03h]
返回:02h+Ln+<ST>+<DATA>+<BCC>+[03h]。
描述:DATA=Ver+SN+Rechang 其中 Ver 表示 16 字节（ASCII 码）版本号，SN 前 4 字节（BCD）表示生产序号，后 4 个字节是全为“00”（如果有密码算法芯片，则是其

编号），Rechang 表示 2 字节充电时间（需硬件支持）。返回信息后关闭加密状 态。

6.7 程序复位自检（31）

命令:02h+01h+31h+<BCC>+[03h] 或选择 02h+02h+31h+38h/39h+BCC+[03h]
描述:键盘进行自检。

第一种只做复位和自检。复位成功后，蜂鸣器响一声。

第二种，38H 时会复位和自检，清除所有密钥。39 时会复位和自检，并重置出厂缺省设置但不会重置密钥。复位成功后，蜂鸣器将短响三声。

自检状态在 ST 中，若自检异常蜂鸣器长响一声。返回信息后，复位所有开机缺省设置，并关闭键盘及加密状态。

返回:02h+01h+<ST>+<BCC>+[03h]。

6.8 下载主密钥（32）

命 令 :02h+0Ah+32h+<M>+<TMK>+<BCC>+[03h] 或
02h+12h+32h+<M>+<TMK>+<BCC>+[03h] 或
02h+1Ah+32h+<M>+<TMK>+<BCC>+[03h]
描述:如果主密钥号 M 为 00～0Fh，16 个主密钥 TMK 为 8/16/24 字节(对应 DES/3DES)明文 直接保存。如果主密钥号 M 为 40h～4Fh 那么 TMK 是密文，不能直接保存，必须用对应（00～0Fh）原主密钥作为密钥，以 ECB 方式解密 TMK 后保存。因此下载 TMK 密文是用原主密钥进行加密的。返回信息后关闭加密状态。

下载密钥时，可选择设置是否返回校验码， 若果选择返回验证码，将用下载的密钥对 8 字节 0x00 加密，并将结果作为验证返回。

返回:无验证码:02h+01h+<ST>+<BCC>+[03h]。

有验证码:02h+05h+ST+<DATA>+<BCC>+[03h]。其中<DATA>为 4 个字节验证码，验 证码为用密钥明文对 8 字节 0x00 做加密运算返回的结果。

6.9 下载工作密钥（33）

命 令 :02h+0Bh+33h+<M>+<N>+<WP>+<BCC>+[03h] 或
02h+13h+33h+<M>+<N>+<WP>+<BCC>+[03h] 或
02h+1Bh+33h+<M>+<N>+<WP>+<BCC>+[03h]
描述:工作密钥密文 WP 均为 8/16/24 字节(对应 DES/3DES)。用主密钥号为 M 的主密钥(DES/3DES) ，

以 ECB 方式解密得到工作密钥 WK，保存到指定的工作密钥号 N（00～03h）中。如 果命令中工作密钥号 N=40h～7Fh，保存到对应的工作密钥号中（计算公式为 M=M,N=N-0x40-M*4），此时返回信息将带有校验码。返回信息后关闭加密状态。

返回: 02h+01h+<ST>+<BCC>+[03h]。
注: 带校验码返回 02h+05h+ST+<DATA>+<BCC>+[03h]。其中<DATA>为 4 个字节校验码，校 验码为用密钥明文对 8 字节 0x00 做加密运算返回的结果。

6.10 下载工作密钥(限于 SAM 卡操作)（71）

命令:s02h+0Ch+71h+<M>+<N>+<SLOT>+<PWD>+<WP>+<BCC>+[03h]

描述:M 对应主密钥号，N 对应工作密钥号，SLOT 对应 SAM 卡的卡槽(1-4)，PWD 对应 SAM 卡验证密钥, 工作密钥密文 WP 为 8 字节(对应 DES)。

选择 SAM 卡座失败	返回 ST=0xE1
给 SAM 卡座上电失败	返回 ST=0xE2
验证 SAM 卡密码失败	返回 ST=0xE3
SAM 选择 DF01 目录失败	返回 ST=0xE4
SAM 卡解密初始化失败	返回 ST=0xE5
SAM 卡解密工作密钥失败	返回 ST=0xE6
保存工作密钥失败	返回 ST=0xE7
SAM 卡座下电失败 S	返回 ST=0xE8

返回:02h+01h+<ST>+<BCC>+[03h]。

6.11 设置帐号(用于 ANXIX9.8 加密)/ 传输码 (用于 ISO9564-1 格式 1)（34）

命 令 :02h+0Dh+34h+<CARD-NO>+<BCC>+[03h] 或 02h+0Bh+34h+<TRANS-Code>+<BCC>+[03h]

描述:卡号或帐号 CARD-NO 为 12 个字节 ASCII 的数字码（必须按 ANXIX9.8 规范截取帐号）。如果 TRANS-Code 是为 10 个字节是传输码，用于 ISO9564 格式 1，是因为不需要帐号。返回信息后不关闭加密状态。帐号 s 和传输码是分开保存，互不干涉。

返回: 02h+01h+<ST>+<BCC>+[03h]。

6.12 启动密码键盘加密（35）

命
令 :02h+06h+35h+<PIN-L>+<DISP-MD>+<JM-MD>+<TS-MD>+<TIMEOUT>+<BCC>+[03h]
或

02h+0Eh+35h+<PIN-L>+<DISP-MD>+<JM-MD>+<TS-MD>+<TIMEOUT>+<DATA>+<BCC>+[03h]

描述:

变量	描述	字节数	可选值（十六进制）
PIN-L	键盘输入密码 PIN 的最大长度，因兼容性问题，最小长度可由 6.22 节参数设置，该值不能小于最小长度	1	04-0C

DISP-MD	显示模式。 01=显示或返回串口“*” 00=显示或返回明文,不支持。	1	1
JM-MD	加密模式。 00:由算法参数决定加密模式，后加密模式，可在 PIN 输入完成后再设置加密模式。 01:PIN 与 CARD-NO 进行运算后加密（ISO9564-1 格式 0 或 ANSI X9.8） 02:PIN 不与 CARD-NO 进行运算，使用 PIN ASCII 码加密。(ASCII 格式) 03: PIN 不与 CARD-NO 进行运算，使用 PIN BCD 码加密。(IBM3624 格式)	1	00/01/02/03
TS-MD	提示方式 00:不提示	1	0
TIMEOUT	超时时间 1~255 秒，超出此时间，退出 PIN 输入。	1	01~FF
DATA	随机密钥密文。 由当前主密钥解密后，作为当前工作密钥。	8	00~FF

功能:如果键盘是关闭的，自动打开键盘，允许输入并进入加密状态，输入 PIN 时要 求判断输入密码长度与 PIN-L 比较，如是小于 PIN-L 但有确认键，或等于 PIN- L，根据 PIN 格式要求（如用 00/FFh）补齐到 8 字节长度。

区，等到取键盘密码命令。如果按键超时退出，只返回超时状态没有密文。

返回:02h+01h+<ST>+<BCC>+[03h]。

注意:在 PIN 码只允许 0～9 数字键，键值以“*”发送，除下面 3 个功能键外，其它 功能键应视为无效(但键值可选择是否需要发送，见“设置算法处理参数”命 令)。

取消:相当于 ESC 键，是取消当前的启动密码键盘加密命令执行。也可以用其他命令 取消当前的启动密码键盘加密命令执行，即关闭加密状态。

更正:是删除已经输入的所有字符。如已经输入了 5 个字符，就连续发送 5 个 （08H）码。

确认:是确认 PIN 密码的输入结束。或者监视“*”的个数达到长度，必须延迟 50mS 以上等待 DES 运算完成，如果是 TDES 需要 3 倍等待时间。

6.13 数据加密（36）

命令:02h+<Ln>+36h+<字符串>+<BCC>+[03h]

描述:将(Ln-1=)8 倍字节明文字符串用当前工作密钥（DES/3DES）以 ECB/CBC 方式进行加 密运算 C＝eK(P)，返回密文数据。要求 Ln-1 小于等于 240 字节，否则请参考 6.35 节。返回信息后关闭加密状态。

返回: 02h+<Ln>+<ST>+<密文字串>+<BCC>+[03h]。

6.14 数据解密（37）

命令:02h+<Ln>+37h+<密文字串>+<BCC>+[03h]

描述:将(Ln-1=)8 倍字节密文字符串用当前工作密钥（DES/3DES）以 ECB 方式进行解密运算 P＝dK(C)，返回明文数据。要求 Ln-1 小于等于 240 字节，否则请参考 6.36 节。返回信息后关闭加密状态。

返回:02h+<Ln>+<ST>+<明文字串>+<BCC>+[03h]。

6.15 读取/设置产品终端号字符串（38）

命令:02h+01h+38h+<BCC>+[03h] 或 02h+09h+38h+<终端号字串>+<BCC>+[03h]

描述:终端号字符串为 8 个字节。如果是选择 NCR 的格式，取最后的 5 个 ASCII 码则表示 终端号。如果客户没有设置终端号，返回的是产品序列号（保证兼容原来命令）。返回信息后关闭加密状态。

返回:02h+09h+<ST>+<终端号字串>+<BCC>+[03h] 或 02h+01h+<ST>+<BCC>+[03h]。

6.16 显示字符串（39）

命令:02h+<Ln>+39h+<字符串>+<BCC>+[03h]。

描述:不带 LCD 屏的产品不支持。返回信息后关闭加密状态。

返回:02h+01h+<ST>+<BCC>+[03h]。

6.17 数据 MAC 运算（41）

命令:02h+<Ln>+41h+<字符串>+<BCC>+[03h]

描述:将 Ln（1～240）个字节明文字符串，用当前的工作密钥（DES/3DES）以指定算法进 回 MAC 信息后关闭加密状态。 MAC 算法可由 6.22 设置。

返回:02h+09h+<ST>+<MAC 字串>+<BCC>+[03h]。注意:MAC 是按 8 字节进行分组，每组需 要 25/75mS 等待 DES/3DES 运算，根据此确立等待返回时间。

6.18 取键盘中密码（42）

命令:02h+01h+42h+<BCC>+[03h]

描述:启动密码键盘加密命令中，如果 JM-MD≠0，将已经加密在缓冲区的密文返回，并且 键盘关闭加密状 态。启动密码键盘加密命令中，如果 JM-MD=0，按算法参数决定获得返回密文数据，然后关闭加密状态。

返回:02h+0Eh+<ST>+<密文>+<CN>+<SN>+<BCC>+[03h]。

返回:02h+19h+<ST>+<密文>+<CN>+<SN>+<BCC>+[03h]。（DUKPT）

注意:CN 是 1 字节是键盘中 PIN 密码运算流水号，每运算一次 CN 加一。SN 是 4 字节

“00”，如果装有密码芯片，是其唯一序列号。

6.19 激活工作密钥（43）

命令:02h+03h+43h+<M>+<N>+<BCC>+[03h]

描述:如果在 6.12 命令中，指定主密钥作为加/解密运算密钥的方案，激活的是 M(00～0Fh)号的主密钥，与 工作密钥无关，但会验证主密钥有效性。

如果在 6.12 命令中，指定工作密钥作为加/解密运算密钥的方案，将主密钥号为 M 所属工作密钥号为 N 激活为当前工作密钥，也会验证主密钥有效性。

总之一旦激活了当前工作密钥，以后所有密码运算用都是指定该当前工作密钥。

返回信息后不关闭加密状态。

返回:02h+01h+<ST>+<BCC>+[03h]。

6.20 测试键盘响应字符（44）

命令:02h+02h+44h+<CHR>+<BCC>+[03h]

描述:密码键盘将收到的字符（不论 ST 状态如何）立即返回，用于验证串口通信。 如果信故障就没

有返回。返回信息后不关闭加密状态。返回: 02h+02h+<ST>+<CHR>+<BCC>+[03h]。

6.21 键盘功能控制（45）

命令:02h+02h/09h+45h+<CTL>+<BCC>+[03h]

CTL 参数	功能描述	备注
01	输入时打开按键声音**	二者选一项
02	输入时关闭按键声音	
00	关闭键盘输入**	三者选一项
03	打开键盘输入	
14	切换成 PS/2 键盘	
04	表示 IC 卡使用 02 头命令（开机缺省）*	二者选一项
05	表示 IC 卡选用 ESC（1B）头命令，并对 IC 卡断电，等待上电命令才	

06	打开夜视灯 关闭夜视灯 **	二者选一项
08	命令结尾不加 03H *	二者
09	命令结尾加 03H	
20	清除键做 clear 使用，清除所有输入	二者
21	清除键做 Backspace 使用，只清除最新一个输入	选一项
30	通讯时，拆分规则为全加 30H	二者
37	通讯时，拆分规则为按照 ASCII 码表转换*	选一项
40	设置键盘上电后为正常模式，即无法输入状态*	
41	设置键盘上电后为明文输入模式，即串口输入状态	三者
42	设置键盘上电后为 PS/2 模式，即 PS/2 输入状态(只对双通道键盘 有效)	
43	使能自毁功能，若设备不支持该功能，将返回错误	二者
44	失能自毁功能，若设备不支持该功能，将返回错误	选一项
8X	表示用作暂时屏蔽/开放某键（键值必须是定义的，否则无效），返 回多一个字节键码。（开机按键均开放） 快捷激活/屏蔽按键. 用 4 个字节表示 ActiveFK，再用 4 个字节表示 ActiveFDK(保留).高位字节在前.	ActiveFDK 做保留，目前不表示任何按键。 未列出的按键通过
ActiveFK	每一位代表一个按键，0 为屏蔽，1 为激活。按键顺序从第 0	8X 方式控制。

ActiveFDK	位向上依次为： 0~9(0x30~0x39)、确认(0x0D)、退出(0x1b)、清除(0x08) 退格 (0x08) 、空格 (0x20) 、点 (0x2E) 、双 0(0x7F) 、 A~F(0x41~0x46)	清除与退格同时只能激活一个，若都激活则为清除功能激活。

描述:打开/关闭密码键盘，打开/关闭按键(BZ)声音。在键盘打开时，一旦有按键会 主动发送键值码(如附件 C 中的 ASCII 码)。如果打开了按键声音，按键时还会 发 出 声音。设置还有通信参数如下:

返回: 02h+01h+<ST>+<BCC>+[03h]。

注意: 8X 命令的返回多一个字节（02h+02h+<ST>+<DATA>+<BCC>+[03h]），是用于表示激活或屏蔽状态键值。如果与命令中 CTL 值一样表示接受屏蔽该键，如果是键值本身，则去掉屏蔽或称已经激活。开机后所有键值都打开。快捷激活按键示 例：

ActiveFK = 0x0000001 只激活 0 键，其它按键屏蔽。

ActiveFK = 0x0001FFF 激活 0~9/确认/取消/清除键，其它按键屏蔽

*为出厂缺省值，**为开机缺省值。返回信息后关闭加密状态。

6.22 设置算法处理参数（46）

命令:02h+03h+46h+<P>+<F>+<BCC>+[03h]

描述:定义密码键盘主参数码<P>和辅助参数码<F>。这些是与密码有关的固化参数，断电也不丢失。

P	F	功能描述	备注
00	20	下载工作密钥采用 DES 密码算法，主密钥解密*	四者选一项
	30	下载工作密钥采用 3DES 密码算法，主密钥解密	
	40	下载密钥采用 SAM 卡内密码算法，主密钥解密	
	50	下载密钥采用 CHIP 内密码算法，主密钥解密	
01	10	键盘不采用密码算法，PIN 将输出明码	七者选一项
	20	键盘采用内置 DES 算法，工作密钥加密*	
	30	键盘采用内置 3DES 算法，工作密钥加密	
	80	键盘采用 SM4 算法，工作密钥加密	

	40	键盘输入采用内置 sam 卡内密码算法，工作密钥加密	
	50	键盘输入采用内置 CHIP 内密码算法，工作密钥加密	
	60	键盘采用 DES 密码算法，主密钥加密	
	70	键盘采用 3DES 密码算法，主密钥加密	
	90	键盘采用 SM4 算法，主密钥加密	
02	0x00-0xFF	键盘输入 PIN 长度不足时，用<F>值填充 PIN 右边直至达到 8 字节*	二者选一项
03	0x00-0xFF	键盘输入 PIN 长度不足时，用<F>值填充 PIN 左边直至达到 8 字节	
04	0	PIN 加密方式为 ASCII 格式	七者选一项
	10	PIN 加密方式为 ISO9564-1	
	11	PIN 加密方式为 ISO9564-1	
	12	PIN 加密方式为 ISO9564-1	
	13	PIN 加密方式为 ISO9564-1	
	20	PIN 加密方式为 IBM3624 格式(BCD 直接加密)	
	21	PIN 加密方式为 NCR 格式。	
05	0	在 PIN 输入时，达到指定长度时不加送回车键值*	二者选一项
	1	在 PIN 输入时，达到指定长度时自动加送回车键值	
	2	在 PIN 输入时，不允许送出功能键*	二者选一项
	3	在 PIN 输入时，允许送出功能键	
	4	下载密钥不返回验证码*	二者选一项
	5	下载密钥返回验证码	
06	1	MAC 算法采用 X9.19/x9.19 算法*	三者选一项
	2	MAC 算法采用 SAM 卡算法	
	3	MAC 算法采用银联 POS 算法	

07	10	数据加/解算法采用 ECB*	二者选一项
	11	数据加/解算法采用 CBC	
	20	数据加/解算法采用 TDES ECB(为兼容性而保留)	
	21	数据加/解算法采用 TDES CBC(为兼容性而保留)	
08	1	签名时 Hash 算法为 SM3*	四者选一项
	2	签名时 Hash 算法为 MD5	
	3	签名时 Hash 算法为 SHA1	
	4	签名时 Hash 算法为 SHA256	
09	1	非对称算法使用 RSA 算法	二者选一项
	2	非对称算法使用 SM2 算法*	
0A	00-0C	PIN 输入的最小长度,上电后都将重置为 04(**). PIN 输入时小于该长度“确认”将不起作用	

返回: 02h+01h+<ST>+<BCC>+[03h]。ST 可能是 04h、15h、C4h、D5h、E0h。
*为出厂缺省值，**为上电缺省值。
注意:上表中的备用参数不得使用，否则有不良结果。返回信息后不关闭加密状态。

6.23 访问 COS，取键盘 PIN 加密数据（限于 SAM 卡加密模式)（47）

命令:02h+<Ln>+47h+<APDU>+<BCC>
返回:02h+<Ln>+<ST>+<COS-DATA>+<BCC>。
描述: <Ln>代表<APDU>的长度加 1， APDU 必须带 8 字节缓冲数据（任意，建议为 8 字节 0x00），用该缓冲区做 PIN_block 的存储区，送 SAM 卡进行加密。CPU 卡 SW1SW2 状态是包含在返回的
COS-DATA 中。
注意:APDU 的数据部分必须是 8 个字节，没有 MAC 的模式。

6.24 访问 COS，原用 APDU（限于 CPU 卡）（48）

命令:02h+<Ln>+48h+<APDU>+<BCC>
返回:02h+<Ln>+<ST>+<COS-DATA>+<BCC>。
描述: <Ln>代表<APDU>的长度加 1。CPU 卡 SW1SW2 状态是包含在返回的 COS-DATA 中。有关 CPU 卡标准是按 ISO7816 标准命令做，详细资料请参考 CPU 卡厂商提供的说 明书。书中有解释 APDU 及 SW1SW2 格式。

6.25 上电复位 IC 卡（所有 IC 卡）（49）

命令:02h+01h+49h+<BCC>
返回:02h+<Ln>+<ST>+<DATA>+<BCC>。
描述:DATA 是反馈复位数据，根据不同的 IC 卡说明，返回不同的数据信息。

6.26 设置 IC 卡座及卡类型（所有 IC 卡）（59）

命令:02h+03h+59h+<IC-SET>+<IC-TYPE>+<BCC>
返回:02h+<Ln>+<ST>+<DATA>+<BCC>。
描述:IC-SET 是卡座号，IC-TYPE 是卡类型数据。卡座号:
01h～04h 表示 SAM 卡座卡类型数据: 00 表示自动识别卡类型。
88h 表示 CPU 智能卡，如 SAM 卡等。

6.27 读取 IC 卡座及卡类型（所有 IC 卡）（5A）

命令:02h+02h+5Ah+<IC-SET>+<BCC>
返回:02h+03h+<ST>+<IC-SET>+<IC-TYPE>+<BCC>。
描述:IC-SET 是卡座号,0=当前卡座，IC-TYPE 是卡类型数据。卡座号:
01h～04h 表示 SAM 卡座卡类型数据:
00 表示自动识别卡类型。
88h 表示 CPU 智能卡，如 SAM 卡等。

6.28 给 CPU 卡座断电（58）

命令:02h+01h+5Bh+<BCC>+[03h]
返回:02h+01h+<ST>+<BCC>+[03h]。
描述:操作完成后的断电。

6.29 安全输入密钥（62）

命令：02h+01h+62h+<MKIndex>+<BCC>+[03h]
返回：02h+01h+<ST>+<BCC>+[03h]。
描述：由键盘输入主密钥内容。指令成功启动后，键盘将进入输入状态，要求输入 32 位 密钥内容。
<MKIndex>: 主密钥号，0-15。

6.30 安装/移除键盘（60）

命令：02h+02h+60h+<Operation>+<BCC>+[03h]
返回：02h+01h+<ST>+<BCC>+[03h]。
描述：安装/移除键盘，命令成功执行后，将要求输入管理员 A 和管理员 B 的密码，两个密码校验成功后方能完成指定操作。
<Operation> 0x01: 安装键盘 0x02: 移除键盘

6.31 修改管理员密码（61）

命令：02h+01h+61h+<ManagerID>+<BCC>+[03h]
返回：02h+01h+<ST>+<BCC>+[03h]。
描述：修改管理员密码。管理员分为管理员 A 和管理员 B。
<ManagerID> 0x01:管理员 A 0x02: 管理员 B
启动该指令后，键盘将进入输入状态，先输入原始密码，再输入 2 遍新的密码完成修改管理员密码修改。

6.32 下载 RSA 密钥对模[BD]（A1）

命令:02h+05h+A1h+<模数据长度>+03h+<密钥号>+00h+<DATA>
描述:下载 RSA 密钥对模数据，用于 RSA 运算。<DATA>为对模数据。若为 RSA 算法时，即为 RSA->n,目前只支持 1024 位模数。
返回: 02h+05h+<ST>+”0000”+<BCC>。

6.33 下载私钥[BD]（A2）

命令:02h+05h+A2h+<私钥数据长度>+03h+<密钥号>+00h+<DATA>
描述:下载非对称算法私钥数据。若为 RSA 算法时，即为 RSA->d。
返回: 02h+05h+<ST>+”0000”+<BCC>。

6.34 下载公钥[BD]（A3）

命令:02h+05h+A3h+<公钥数据长度>+03h+<密钥号>+00h+<DATA>
描述:下载非对称算法公钥数据。若为 RSA 算法时，即为 RSA->e,受硬件限制，该值一直为 0x10001，下载公钥指令无效(也无需下载公钥,下载模数即可)。
返回: 02h+05h+<ST>+”0000”+<BCC>。

6.35 公钥加密[BD]（A4）

命令:02h+05h+A4h+<数据长度>+03h+<密钥号>+00h+<DATA>

描述:RSA 或 SM2 公钥加密。<DATA>是要加密的数据。若为 RSA 算法时，加密数据必须为 128byte；若长度不足，由用户自己决定填充(建议 PKSC#7 或全填 0x00)。
返回: 02h+05h+<ST>+<数据长度>+<BCC>+<DATA>。
<DATA>为加密返回的结果。

6.36 私钥解密[BD]（A5）

命令:02h+05h+A5h+<数据长度>+03h+<密钥号>+00h+<DATA>
描述:RSA 或 SM2 私钥解密。<DATA>是要解密的数据。若为 RSA 算法时，解密数据必须为 128byte。
返回: 02h+05h+<ST>+<数据长度>+<BCC>+<DATA>。
<DATA>为解密返回的结果。

6.37 非对称算法签名[BD]（A6）

命令:02h+05h+A6h+<数据长度>+03h+<密钥号>+<HashFlag>+<DATA>
描述:RSA 或 SM2 签名。
<DATA>是要进行签名的数据。签名时使用的 hash 算法由 6.22 进行设置。
RSA:
<DATA>结构: <MH>+<ML>+<MSG>
<MH>:摘要数据长度高字节，1 字节
<ML>:摘要数据长度低字节，1 字节
<MSG>:摘要数据，MH<<8+ML 字节<0x00>:ID 恒为 0 <0x00>:ID 恒为 0
MH<<8+ML 恒为 128
SM2: <DATA>结构:<MH>+<ML>+<MSG>+<IH>+<IL>+<ID> <MH>:摘要数据长度高字节，1 字节<ML>:摘要数据长度低字节，1 字节
<MSG>:摘要数据，MH<<8+ML 字节<IH>:ID 长度高字节，1 字节<IL>:ID 长度低字节，1 字节<ID>:ID 数据，IH<<8+IL 字节<HashFlag>是否需要对数据做 Hash。

	值	描述
HashFlag	0	不需要做 Hash
	1	需要做 Hash

返回: 02h+05h+<ST>+<数据长度>+<BCC>+<DATA>。<DATA>为签名返回的结果。

6.38 非对称算法验签[BD]（A7）

命令:02h+05h+A7h+<数据长度>+03h+<密钥号>+00h+<DATA>描述:RSA 或 SM2 验签。
RSA:

<DATA>结构:<SH>+<SL>+<Sign>+<MH>+<ML>+<MSG> <SH>:签名数据长度高字节，1 字 节<SL>:签名数据长度低字节，1 字节

<Sign>:签名数据，SH<<8+SL 字节
<MH>:摘要数据长度高字节，1 字节
<ML>:摘要数据长度低字节，1 字节
<MSG>:摘要数据，MH<<8+ML 字节<0x00>:ID 恒为 0 <0x00>:ID 恒为 0
MH<<8+ML 恒为 128
SH<<8+SL 恒为 128
SM2:
<DATA>结构:<SH>+<SL>+<Sign>+<MH>+<ML>+<MSG>+<IH>+<IL>+<ID> <SH>:签名数据 长度高字节，1 字节<SL>:签名数据长度低字节，1 字节
<Sign>:签名数据，SH<<8+SL 字节
<MH>:摘要数据长度高字节，1 字节
<ML>:摘要数据长度低字节，1 字节
<MSG>:摘要数据，MH<<8+ML 字节<IH>:ID 长度高字节，1 字节<IL>:ID 长度低字节，1 字节<ID>:ID 数据，IH<<8+IL 字节验签时使用的 hash 算法由 6.22 进行设置。
返回: 02h+05h+<ST>+<数据长度>+<BCC>+<DATA>。<DATA>为签名反解的结果。返回其它或无数据返回则失败。
<DATA>结构： <VerifyFlag>+<UnSignData>
<VerifyFlag> 如果为 0，返回验签结果，此时，<UnSignData>为 0 验签失败，非 0 成功。
<VerifyFlag> 如果为 1，返回验签数据，键盘不做验证。此时，<UnSignData>为签 名反解数据。
<VerifyFlag>由硬件功能决定。

6.39 生成密钥对[BD]（A8）

命令:02h+05h+A8h+”0000”+<BCC>+<密钥号>+00h

描述:生成非对称算法的密钥对。

返回： 02h+05h+<ST>+<数据长度>+<BCC>+<DATA> 。 ST 可能是 04,11h,12h,13h,14h,25h。<DATA>结构：

<PUBKH>+<PUBKL>+<PRIKL>+<PRIKH>+<PUBKEY>+<PRIKEY>

<PUBKH>:公钥长度高字节，1 字节

<PUBKL>:公钥长度低字节，1 字节

<PRIKH>:私钥长度高字节，1 字节

<PRIKL>:私钥长度低字节，1 字节

<PUBKEY>:公钥数据，PUBKH<<8 + PUBKL 字节

<PRIKEY>:私钥数据，PRIKH<<8 + PRIKL 字节若为 RSA 运算时，PUBKEY 指的是 RSA->n, RSA->e 的值固定为 0x10001。PRIKEY 指的是 RSA->d。

6.40 大字节 MAC 运算[BD]（B1）

命令:02h+05h+B1h+<MAC 数据长度>+<BCC>+<当前块数>+<总块数>+<MAC 块数据>

描述:将 Ln（1~1024）个字节明文字符串，用当前的工作密钥（DES/3DES）以指定算法进行 MAC 运算。返回 8 字节 MAC 字串数据。返回 MAC 信息后关闭加密状态。MAC 算法可由 6.XX 设置。该指令可用于 MAC 字节大于 256 字节时使用。

<MAC 数据长度>：当前块的数据长度，以十进制字符表示，例如 1024 则表示为“1024”。占 4 字节。<当前块数>当前块数，十六进制 BCD 码表示，第一块从 1 开始计数。若为 0 表示仅有一个数据块，<总块数>将无效。占 1 字节。

<总块数>数据总块数，十六进制 BCD 码表示，占 1 字节。

返回: 02h+05h+<ST>+<数据长度>+<BCC>+<DATA>。注意:MAC 是按 8 字节进行分组， 每组需要 25/75mS

等待 DES/3DES 运算，根据此确立等待返回时间。

注意: 该指令支持的一次运算的最大数据为 1024 字节,当 MAC 数据大于 1024 字节时，需要将数据按 8 的整数倍(比如 1024 或 800)拆分成若干(N)数据块，然后循环使用该指令进行运算。当<当前块数>等于<总块数>时，运算结束。

<MAC 数据长度>为当前块的数据长度，而非总的 MAC 数据大小。

6.41 大字节加密运算[BD]（B2）

命令:02h+05h+B2h+<运算数据长度字符串>+<BCC>+<当前块数>+<总块数>+<数据>

描述:将(Ln-1=)8 倍字节明文字符串用当前工作密钥（DES/3DES）以 ECB/CBC 方式进行加密运算 C＝eK(P),返回密文数据。返回信息后关闭加密状态。要求运算长度小于等于 1024 字节。<运算数据长度字符串>：当前运算块的数据长度，以十进制字符表示，例如 1024 则表示为

“1024”。占 4 字节。

<当前块数>记录当前运算到第几块,十六进制 BCD 码表示,第一块从 1 开始计数。若为 0 表示为第一块且后续无数据块，<总块数>将无效。占 1 字节。<总块数>记录拆分后的总块数，十六进制 BCD 码表示，占 1 字节。

返回: 02h+05h+<ST>+<数据长度>+<BCC>+<DATA>。

注意: <当前块数>与<总块数>应恒为 1。

6.42 大字节解密运算[BD]（B3）

命令:02h+05h+B3h+<运算数据长度字符串>+<BCC>+<当前块数>+<总块数>+<数据>
描述:将(Ln-1=)8 倍字节明文字符串用当前工作密钥（DES/3DES）以 ECB/CBC 方式进行加 密运算 C＝eK(P)，返回密文数据。返回信息后关闭加密状态。要求运算长度小于等于 1024 字节。<运算数据长度字符串>：当前运算块的数据长度，以十进制字符表示，例如 1024 则表示为“1024”。占 4 字节。

<当前块数>记录当前运算到第几块，十六进制 BCD 码表示，第一块从 1 开始计数。若为 0 表示为第一块且后续无数据块，<总块数>将无效。占 1 字节。<总块数>记录拆分后的总块数，十六进制 BCD 码表示，占 1 字节。

返回: 02h+05h+<ST>+<数据长度>+<BCC>+<DATA>。
注意: <当前块数>与<总块数>应恒为 1。

6.43 产生随机数[BD]（C3）

命令:02h+05h+C3h+”0000”+<BCC>+<LH>+<LL>
描述: 生成指定长度字节的随机数.
<LH> 随机数长度高字节,1 字节。
<LL> 随机数长度低字节，1 字节。
随机数长度<RNL> = LH<<8+LL，最大值为 1024 字节。
返回: 02h+05h+<ST>+<数据长度>+<BCC>+<DATA>。

6.44 Hash 运算[BD]（c4）

命令:02h+05h+C4h+<数据长度>+<BCC>+<Step>+00h+<DATA>
描述: <数据长度> 当前块数的数据长度
<Step> Hash 运算的阶段
00: Init 初始化
01：Update 更新数据块
02: Final 取结果
注意：Init 会清除缓冲区，将 Update 阶段的数据清空。设置 Hash 算法也会清空 Update 阶段的数据。
<DATA> 当前块数据，若不为末尾块，长度必须为 64 字节的整数倍，最大为 1024 字节。
返回: 02h+05h+<ST>+<数据长度>+<BCC>+<DATA>。
注意: Hash 运算需要按三个步骤执行，分别为 Init，Update，Final。其中 Init 和 Final 阶段没有数据下发，Update 阶段可循环执行传入需要进行运算的所有数 据，除末尾块外，数据长度必须都是 64 字节的整数倍。执行 Final 取回最终 hash 结果。

6.45 预存 APDU（5c）

命令:02h+05h+5Ch+<数据长度>+<BCC>+<n>+00+<APDU1>#+<APDU2>#+…+<APDUn>#
描述: 通过该指令存储 10 条以内的 APDU。
如果需要用 PSAM 卡加密键盘内的 PIN(即 PIN 算法为 PSAM 卡),当执行获取 PINBLOCK 指令时，会逐条发送存储的 APDU 到 PSAM 卡，从而实现从 PSAM 卡内获 取 PINBLOCK。
<n> 预存储的 APDU 的条数，不大于 10,1 字节
<APDUx># APDU 内容，以’#’结束，<APUDx>为十六进制字符串，如”00A40000023F00”#

如果 APDU 数据部分需要 PIN 值的，用”PINBLOCK”字符代 替，例如:” 80FA000008PINBLOCK#”
返回: 02h+05h+<ST>+”0000”+<BCC>

6.46 注意事项

在启动密码键盘加密命令之后，到取键盘中密码命令之前，可以并且只能使用设置算法处理参数命令、激活工作密钥命令、下载卡号或帐号命令和测试键盘响应字符命令，不会影响键盘的加密状态。
若等待或判断键盘操作是否输入完毕，除了用接收*号（可选包括回车）之外，可以用取键盘中密码命令，不能用其他命令，是因为其他命令都会终止键盘的加密状态。
如果在启动密码键盘加密命令中 JM-MD≠0（前加密），在接收到最后一个*号（可选包括回车）之时，立即进行加密处理，因此需要等待加密运算时间（DES/3DES——25/75ms）才能用取键盘中密码命令。如果 JM-MD=0(后加密)，在接收到最后一个*号（可选包括回车）时，不进行加密处理，而 在 取 键 盘 中 密 码 命 令 时 进 行 加 密 处 理 ， 因 此 该 命 令 需 要 等 待 加 密 运 算 时 间（DES/3DES——25/75mS）才能返回信息。
关于 Pin-Block 标准格式简要介绍

格式	PIN_BLOCK 简要描述详见 ISO5964-1B
ISO9564-1 格式 0	PIN=0NPPPPPPFFFFFFFF PAN=0000AAAAAAAAAAAA PIN
(ANSI X9.8 格式)	与 PAN 进行异或后加密。
ISO9564-1 格式 1	PIN=1NPPPPPPTTTTTTTT 直接加密
ISO9564-1 格式 2	不支持，是分配给 IC 卡用的
ISO9564-1 格式 3	PIN=3NPPPPPPFFFFFFFF PAN=0000AAAAAAAAAAAA PIN 与 PAN 进行异或后加密。进行异或后加密。
IBM2624	PIN=PPPPPPFFFFFFFFFF，直接加密。其中 F=填充为 F。
NCR 格式	PIN=TTTTT000000PPPPP，直接加密。其中 T=为终端号
ASCII 格式	PIN=’PPPPPP’FFFF 直接加密

7 附录:键值表及功能键说明

键位	码值	
	ASC II 码	HEX 码
1	1	31H
2	2	32H
3	3	33H
4	4	34H
5	5	35H
6	6	36H
7	7	37H
8	8	38H
9	9	39H
0	0	30H
取消	-	1BH
确认	-	0DH
清除	-	08H
可选键	*	2AH
可选键	#	23H
可选键	.	2Eh
可选键	0	7FH
- 表示该键不能显示		
功能键描述		
键位	码值	
	ASC II 码	HEX 码
左上	G	47H
左中上	E	45H

左中下	C	43H
左下	A	41H
右上	H	48H
右中上	F	46H
右中下	D	44H
右下	B	42H

说明:原则上所有的键值和位置都可以由工厂或一级代理给以重新设置。特定“00h”为无键值，而特定“7Fh”为“0”
连“0”键，之外为可设置任意 ASCII 码(01~7Eh)。

8 附录:发送和接收字符的拆分规则

终端与设备之间进行数据交换时，命令字符串与响应字符串除第一个字节 0x02h 和最后一个字节 0x03h 用十六进制传送外，其它字节均要转换为 ASCⅡ码格式传送。

转换方法 1:

发送时将 1 字节转换为 2 字节:将一个字节拆成高低四位两部分，再把高低两部分，如在 0～9 和 A～F 前加上前缀码 30h 合成 ASCII 码传送。

接收时将 2 字节转换为 1 字节:把第一个 ASCII 字符减去 30h 做为高半字节，把第二个 ASCII 字符减去 30h 做为低半字节，再把高低半字节合成一个十六进制字节。

转换方法 2:

发送时将 1 字节转换为 2 字节:将一个字节拆成高低四位两部分，再把高低两部分，如在 0～9 前加上 30h，若在 A～F 前加上 37h 合成 ASCII 码传送。

接收时将 2 字节转换为 1 字节:把第一个 ASCII 字符减去 30h(或 37h)做为高半字节，把第二个 ASCII 字符减去 30h(或 37h)做为低半字节，再把高低半字节合成一个十六进制字节。

注意:原则上只使用转换方法 2，不建议使用转换方法 1。

9 附录:键盘返回状态码解释

返回值	说明
0x04	指令执行成功
0x15	命令参数错
0x80	超时错误
0xA4	命令执行成功，但主密
0xB5	命令无效且主密钥无效
0xC4	命令可执行，但电池可
0xD5	命令无效且电池可能
0xE0	无效命令
0xE1	不支持的操作
0xE2	内存不足
0xE3	无 PIN
0xF0	CPU 错
0xF1	SAM 卡错
0xF2	键盘有短路
0xF4	CPU 卡出错
0xF5	电池可能损坏
0xF6	主密钥无效
0xF7	其他错
0xA1	国密芯片读写失败
0x68	国密执行失败
0x67	P3 错误
0x6B	P1/P2 错误
0x6E	CLA 错误
0x6A	异或值错误
0x6C	验证失败
0x86	主动取消输入
0x87	输入超时
0x88	口令验证失败
0x8B	两次口令输入不一致
0x8F	口令未修改过
0xA0	密钥验证失败
0x84	输入管理员 A 口令
0x85	输入管理员 B 口令
0x8A	输入新口令
0x8D	再次输入新口令

0x97	输入分量 A
0x98	输入分量 B
0x99	输入 KCV