旭 子 科 技
SUNSON

# 加密键盘指令说明

# XZ_F10

| | |
|---|---|
| 文档编号 | XZ_F10 |
| 文档版本号 | V1.2 |
| 文档日期 | 2013 年 01 月 28 日 |
| 最后更改日期 | 2015 年 07 月 10 日 |
| 文档作者 | 魏荣 |
| 项目负责人 | 白培基 |
| 审核人 | 张红军 |

# 目录

目录.....2
1、键盘命令解释.....4
1.1 基本参数说明.....4
1.2 取产品版本号.....4
1.3 程序复位自检.....5
1.4 下装主密钥.....5
1.5 下装工作密钥.....5
1.6 设置帐号（用于 ANXIX9.8 加密）/ 传输码（用于 ISO9564-1 格式 1）.....6
1.7 启动密码键盘加密.....6
1.8 数据加密.....7
1.9 数据解密.....7
1.10 读取/设置产品终端号字符串.....7
1.11 显示字符串.....8
1.12 数据 MAC 运算.....8
1.13 取键盘中密码.....8
1.14 激活工作密钥.....9
1.15 发送回送字符.....9
1.16 发送开关键盘和按键声音.....9
1.17 算法处理参数.....10
1.18 访问 COS，取键盘 PIN 加密数据（限于 SAM 卡加密模式）.....11
1.19 访问 COS，原用 APDU.....11
1.20 复位 IC 卡.....12
1.21 设置 IC 卡座及卡类型（所有 IC 卡）.....12
1.22 读取 IC 卡座及卡类型（所有 IC 卡）.....12
1.23 给 CPU 卡座断电.....12
1.24 设置国密模式 （国密键盘有效）.....13
1.25 获取国密模式 （国密键盘有效）.....13
1.26 生成 SM2 密钥 （国密键盘有效）.....13
1.27 sm2 数据加密 （国密键盘有效）.....13
1.28 sm2 数据解密 （国密键盘有效）.....13
1.29 sm2 签名 （国密键盘有效）.....14
1.30 sm2 验签 （国密键盘有效）.....14
1.31 下载 SM2 密钥 （国密键盘有效）.....14
1.32 导出 SM2 公钥 （国密键盘有效）.....14
1.33 SM3 哈希运算 （国密键盘有效）.....15
1.34 HASHID 初始化 （国密键盘有效）.....15
1.35 使能禁止移除和自毁功能 （国密键盘有效）.....15
1.36 键盘双向校验.....15

1.37 使能 EPP 固件下载 （国密键盘有效）.....16
1.38 获取明文或者密文按键值.....16
附录 A 键盘密钥管理.....17
附录 B 键盘值表及功能键说明.....18
附录 C 发送和接收字符的拆分规则.....19

# 1、键盘命令解释

## 1.1 基本参数说明

命令格式：02h+<Ln>+<CMD>+<DATA>+<BCC>

返回格式：02h+<Ln>+<ST>+<DATA>+<BCC>

Ln——表示 CMD 和 DATA 或 ST 和 DATA 的字节数

CMD——命令关键字

DATA——交换的数据信息

BCC——从 Ln 到 DATA 的字节异或校验和

ST——解释如下：

04h——命令成功执行

15h——命令参数错

80h——超时错误

A4h——命令可成功执行，但主密钥无效

B5h——命令无效，且主密钥无效

C4h——命令可成功执行，但电池可能损坏

D5h——命令无效，且电池可能损坏

E0h——无效命令

FXh——自检时出错：

X=0 CPU 错　　X=1 SRAM 错

X=2 键盘有短路错　　X=3 串口电平错

X=4 CPU 卡出错　　X=5 电池可能损坏

X=6 主密钥失效　　X=7 杂项错

## 1.2 取产品版本号

命令：02h+01h+30h+<BCC>

描述：密码键盘将所设置在 E2ROM 芯片的有关参数发送返回。

返回：02h+Ln+<ST>+<DATA>+<BCC>。ST 可能是 04h、15h、E0h、F0h。当 ST=F0h 表示没有安装 E2ROM 芯片。

注：由产品制造公司进行解释 DATA 内容。

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。

## 1.3 程序复位自检

命令：02h+01h+31h+<BCC>+[03h] 或选择 02h+02h+31h+38h+BCC+[03h]

描述：键盘进行自检完毕，前者不破坏密钥区，后者会预置主密钥和工作密钥（初始所有主密钥为 16 个 38h，工作密钥为 16 个 30h)，如果主密钥有效（将 16 个主密钥用 BCC 校验)，将蜂鸣器响一声；无效蜂鸣器响三声，自检状态在 ST 中。返回信息后，复位所有变量，并关闭键盘及加密状态。

返回：02h+01h+<ST>+<BCC>+[03h]。ST 可能是 04h、15h、E0h、FXh。

## 1.4 下装主密钥

命令：02h+0Ah+32h+<M>+<TMK>+<BCC>+[03h]或 02h+12h+32h+<M>+<TMK>+<BCC>+[03h]

描述：下载不验证方式时，主密钥号 M 为 1 字节（00～0Fh)，16 个主密钥 TMK 为 8/16 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，就不能直接保存，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。

下载有验证方式时，主密钥号 M 为 1 字节（40h～4Fh)，16 个主密钥 TMK 为 8/16 字节(对应 DES/3DES)，当前激活的主密钥号为解密主密钥号，以 ECB 方式解密 TMK，命令中 M 为存放主密钥号来保存主密钥。如果当前激活的主密钥无效，该命令不执行。下载是否需要验证，参考**“设置算法处理参数”**命令说明。返回信息后关闭加密状态。

（国密模式主密钥长度必须 16 字节 非国密模式主密钥长度 8，16，24）

不验证返回：02h+01h+<ST>+<BCC>+[03h]。ST 可能是 04h、15h、C4h、D5h、E0。

有验证返回：02h+05h+ST+<DATA>+<BCC>+[03h]。其中<DATA>为 4 个字节返回码作验证码用。

## 1.5 下装工作密钥

命令： 02h+0Bh+33h+<M>+<N>+<WP>+<BCC>+[03h]

或 02h+13h+33h+<M>+<N>+<WP>+<BCC>+[03h]

描述：工作密钥密文 WP 均为 8/16 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(主密钥号*4+工作密钥号+0x40)，保存到对应的工作密钥号 N(00～3Fh)中，此时以验证方式返回信息。返回信息后关闭加密状态。

（国密模式主密钥长度必须 16 字节 非国密模式主密钥长度 8，16，24）

不验证返回：02h+01h+<ST>+<BCC>+[03h]。ST 可能是 04h、15h、A4h、B5h、C4h、D5h、E0h

有验证返回：02h+05h+ST+<DATA>+<BCC>+[03h]。其中<DATA>4 个字节返回码作验证用

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

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。帐号和传输码是分开保存，互不干涉。

返回：02h+01h+<ST>+<BCC>+[03h]。ST 可能是 04h、15h、C4h、D5h、E0h。

## 1.7 启动密码键盘加密

命令：02h+06h+35h+〈PIN-L〉+<DISP-MD>+<JM-MD>+<TS-MD>+<TIMEOUT>+<BCC>

| 变量 | 描述 | 可选值 |
|---|---|---|
| PIN-L | **密码长度** PIN-L 为 1 字节：04h～0Ch 表示键盘输入密码 PIN 的长度为 4 至 12 个。00 表示把上次 PIN 加密结果重发一次。 | 00/04～0Ch |
| DISP-MD | **显示模式** DISP-MD 为 1 字节：01＝显示或返回串口“*”，不支持显示或返回明文。 | 01 |
| JM-MD | **加密模式** JM-MD 为 1 字节：00=由算法参数决定加密模式， 01＝PIN 与 CARD-NO 进行运算后加密（ISO9564-1 格式 0），02=PIN 不与 CARD-NO 进行运算直接 ASCII 码加密（ASCII 格式）,03==PIN 不与 CARD-NO 进行运算直接 BCD 码加密（IBM3624 格式）。 | 00/01/02/03 |

| | | |
|---|---|---|
| TS-MD | **提示方式** TS-MD 为 1 字节（00=不提示） | 00 |
| TIMEOUT | **超时时间** TIMEOUT 为 1 字节（1～255 秒），超出此时间无按键，退出。 | 01～FF |

描述：密码长度 PIN-L 为 1 字节（1～16，0 表示把上次的结果重发一次）；显示模式 DISP-MD 为 1 字节(1＝显示“*”)；加密模式 JM-MD 为 1 字节（1＝与 CARD-NO 进行运算后加密，2=不与 CARD-NO 进行运算直接加密）；提示方式 TS-MD 为 1 字节（=0）；超时时间 TIMEOUT 为 1 字节（1～255 秒），超出此时间无输入，退出输入。

功能：自动打开键盘，提示后允许输入，输入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，需要用 00/FFh 补齐到 PIN-L 长度，或等于 PIN-L，根据加密模式，是否需要进行 CARD-NO 与 PIN 的身份信息运算（在 PIN_BLOCK 运算时，根据 ANSIX9.8 或 ISO 9564 或 IBM3624 要求，把 PIN 用 FFh 补足 8 字节），然后进行密码加密运算，最后将返回数据保存在缓冲区，等到取密码命令。如果超时退出，只返回状态没有密文。等待 PIN 输入时，可选择功能键输出或禁止输出。

返回：02h+01h+<ST>+<BCC>。ST 可能是 04h、15h、A4h、B5h、C4h、D5h、E0h。

## 1.8 数据加密

命令：02h+Ln+36h+<字符串>+<BCC>

描述：将(Ln-1)字节明文字符串用当前工作密钥（DES/3DES）加密。进行密码加密运算，返回密文数据。国密模式如果不为 16 的倍数 后面补 0

返回：02h+ln+<ST>+<密文字串>+<BCC>。 ST 可能是 04h、15h、A4h、B5h、C4h、D5h、E0h。

## 1.9 数据解密

命令：02h+Ln+37h+<密文字串>+<BCC>

描述：将(Ln-1)字节密文字符串用当前工作密钥（DES/3DES）解密。进行密码解密运算，返回明文数据。国密模式如果不为 16 的倍数 后面补 0

返回：02h+Ln+<ST>+明文字串+<BCC>。ST 可能是 04h、15h、A4h、B5h、C4h、D5h、E0h。

## 1.10 读取/设置产品终端号字符串

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

返回： 02h+09h+<ST>+<终端号字串>+<BCC>+[03h] 或 02h+01h+<ST>+<BCC>+[03h]。ST 可能是 04h、15h

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。

## 1.11 显示字符串

命令：02h+<Ln>+39h+<字符串>+<BCC>。

描述：不支持。

返回：02h+01h+<ST>+<BCC>。ST 可能是 04h、15h、E0h。

注意：汉字码是根据密码键盘字库编码的，符数码必须是密码键盘能显示的。如果无字符串部分表清除显示屏。

## 1.12 数据 MAC 运算

命令：02h+<Ln>+41h+<字符串>+<BCC>

描述：将 Ln（5～247）个字节明文字符串，用当前的工作密钥（DES/3DES）以 CBC 方式进行加密运算 C1＝eK(P1)及 Ci＝eK(Pi⊕C i-1)i=2,3, …,n。返回 8 字节 MAC 字串数据。返回 MAC 信息后关闭加密状态。国密模式如果不为 16 的倍数 后面补 0

返回：02h+Ln+<ST>+<MAC 字串>+<BCC>+[03h]。 ST 可能是 04h、15h、A4h、B5h、C4h、D5h、E0h。国密模式 Ln 17 字节 非国密模式 9 字节

## 1.13 取键盘中密码

命令：02h+01h+42h+<BCC>

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，按算法参数决定的加密模式，用当前的工作密钥对键盘中的数据，以 ECB 方式进行加密运算 C＝eK(P)，获得返回密文数据，然后关闭加密状态。

返回：02h+len+<ST>+<密文>+<CN>+<SN>+<BCC>+[03h]。ST 可能是 04h、15h、C4h、D5h、E0h。国密模式 len 22 字节 非国密模式 14 字节

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。

## 1.14 激活工作密钥

命令：02h+03h+43h+<M>+<N>+<BCC>

描述：如果在 1.16 命令中，指定主密钥作为当前工作密钥的方案，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 1.16 命令中，指定工作密钥作为当前工作密钥的方案，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。但是这种情况下，如果工作密钥号 N=40～7Fh，与主密钥 M 无关，不验证主密钥有效性。

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>。ST 可能是 04h、15h、A4h、B5h、C4h、D5h、E0h。

## 1.15 发送回送字符

命令：02h+02h+44h+<CHR>+<BCC>

描述：密码键盘将收到的字符立即返回。

返回：02h+02h+<ST>+<CHR>+<BCC>。ST 可能是 04h、15h、C4h、D5h、E0。CHR 表示一个 ASCII 字符。

## 1.16 发送开关键盘和按键声音

命令：02h+02h+45h+<CTL>+<BCC>

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，一旦有压键会主动送出键值码。如果按键（BZ）声音也是打开的，按键时还会发出声音。还有通信参数设置。

返回：02h+01h+<ST>+<BCC>。ST 可能是 04h、15h、C4h、D5h、E0。

| CTL 参数 | 功能描述 | 备注 |
|---|---|---|
| 00 | 表示关闭键盘和关闭按键 BZ 声音** | 四者选一项（非固化参数） |
| 01 | 表示打开键盘但关闭按键 BZ 声音 | |
| 02 | 表示关闭键盘但打开按键 BZ 声音 | |
| 03 | 表示打开键盘且打开按键 BZ 声音 | |
| 04 | 表示 IC 卡使用 02 头命令（开机缺省）* | 二者选一项（固化参数） |
| 05 | 表示 IC 卡选用 ESC（1B）头命令，并对 IC 卡断电，等待上电命令才能上电。 | |
| 06 | 表示打开夜视灯(仅当硬件支持时) | 二者选一项（非固化参数） |
| 07 | 表示关闭夜视灯(仅当硬件支持时)** | |

| | | |
|---|---|---|
| 08 | 命令尾不加 03h。* | 二者选一项（固化参数） |
| 09 | 命令尾增加 03h。 | |
| 0a | 打开系统键盘打开按键 BZ 声音 | （USB 键盘选项） |
| 0b | 打开系统键盘关闭按键 BZ 声音 | （USB 键盘选项） |
| 30 | 表示通信时采用拆分全加 30H | 二者选一项（固化参数） |
| 37 | 表示通信时采用拆分 0～9 加 30H，A～F 加 37H。** | |
| 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） | （非固化参数） |

注意：8X 命令的返回多一个字节，是用于表示键值。如果与命令中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。*为出厂缺省值，**为开机缺省值。

## 1.17 算法处理参数

命令：02h+03h+46h+<P>+<F>+<BCC>

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 参数 | F 参数 | 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 | 下载工作密钥采用 SAM 卡内密码算法，主密钥解密 | |
| | 50 | 下载工作密钥采用 CHIP 内密码算法，主密钥解密 | |
| 01 | 10 | 键盘输入 PIN 采用密码算法，输出明码 | 七者选一项 |
| | 20 | 键盘输入 PIN 采用内置 DES 密码算法，工作密钥加密* | |
| | 30 | 键盘输入 PIN 采用内置 3DES 密码算法，工作密钥加密 | |
| | 40 | 键盘输入 PIN 采用内置 SAM 卡内密码算法，工作密钥加密 | |
| | 50 | 键盘输入 PIN 采用内置 CHIP 内密码算法，工作密钥加密 | |
| | 60 | 键盘输入 PIN 采用 DES 密码算法，主密钥加密 | |
| | 70 | 键盘输入 PIN 采用 3DES 密码算法，主密钥加密 | |
| 02 | 00-FF | 键盘输入 PIN 短时，用<F>值填充 PIN 右边直至 8 字节* | 二者选一项 |

| | | | |
|---|---|---|---|
| 03 | 00-FF | 键盘输入 PIN 短时，用<F>值填充 PIN 左边直至 8 字节 | |
| 04 | 10 | 键盘输入 PIN 处理方式为 ISO9564 格式* | 二者选一项 |
| | 20 | 键盘输入 PIN 处理方式为 IBM3624 格式 | |
| 05 | 00 | 在加密状态，输入到约定长度时不加送回车键值， | 二选一项 |
| | 01 | 在加密状态，输入到约定长度时自动加送回车键值，* | |
| | 02 | 在加密状态，期间不允许送出功能键值* | 二选一项 |
| | 03 | 在加密状态，期间允许送出功能键值 | |
| 06 | 01 | MAC 采用 ASNI X9.9 算法 * | 三者选一项 |
| | 02 | MAC 采用 SAM 卡算法 | |
| | 03 | MAC 采用银联的算法 | |
| 08 | 04~0C | 设置最小密码长度，密码长度范围从 4~12 位 | 固化参数 |
| 09 | 04~0C | 设定最大密码长度，密码长度范围从 4~12 位 | 非固化参数 |

返回：02h+01h+<ST>+<BCC>。ST 可能是 04h、15h、C4h、D5h、E0。

注意：在发送激活工作密钥命令时，要考虑工作模式，如 DES 的主密钥和工作密钥都采用 8 字节，而 3DES 的主密钥和工作密钥都采用 16 字节。CHIP 的主密钥 16 字节，工作密钥采用 24 字节。

标准 3DES 加密算法是：采用 0#KEY 进行 DES，1#KEY 进行 UnDES,0#KEY 进行 DES。其解密算法为：0#KEY 进行 UnDES，1#KEY 进行 DES,0#KEY 进行 UnDES。*为出厂缺省值。

下载加密工作密钥受到该命令控制解密还原。主密钥可以通信下载，也可以手工输入。

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

命令：02h+<Ln>+47h+<APDU>+<BCC>

返回：02h+<Lln>+<ST>+<COS DATA>+<BCC>。ST 可能是 04h、15h、A4h、B5h、C4h、D5h、E0h。

描述：<Ln> 代表<APDU>的长度加 1，键盘必须判断 APDU 带 8 字节数据为"\x00\x00\x00\x00\x00\x00\x00\x00"标志，但是不用它，而从缓冲区取得 PIN_block 替代之，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。

## 1.19 访问 COS，原用 APDU

命令：02h+<Ln>+48h+<APDU>+<BCC>

返回：02h+<Ln>+<ST>+<COS DATA>+<BCC>。ST 可能是 04h、15h、A4h、B5h、C4h、D5h、E0h。

注意：<Ln>代表<APDU>的长度加 1。CPU 卡 SW1SW2 状态是包含在返回 COS-DATA 中。

## 1.20 复位 IC 卡

命令：02h+01h+49h+<BCC>

返回：02h+<Ln>+<ST>+<DATA>+<BCC>。ST 可能是 04h、15h、A4h、B5h、C4h、D5h、E0h。

注意：DATA 是反馈复位数据。

## 1.21 设置 IC 卡座及卡类型（所有 IC 卡）

命令：02h+03h+59h+<IC-SET>+<IC-TYPE>+<BCC>

返回：02h+<Ln>+<ST>+<DATA>+<BCC>。ST 可能是 04h，11h, 12h, 13h, 14h, 21h, 22h, 23h, 24h。

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。

## 1.22 读取 IC 卡座及卡类型（所有 IC 卡）

命令：02h+02h+5Ah+<IC-SET>+<BCC>

返回：02h+03h+<ST>+<IC-SET>+<IC-TYPE>+<BCC>。ST 可能是 04, 11h, 12h, 13h, 14h。

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。

## 1.23 给 CPU 卡座断电

命令：02h+01h+5Bh+<BCC>+[03h]

返回：02h+01h+<ST>+<BCC>+[03h]。ST 可能是 04, 11h, 12h, 13h, 14h, 25h。

描述：操作完成后的断电。

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。

CPU 卡的 ST 错误码：

| 错误码 | 错误代码含义 | 错误码 | 错误代码含义 |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 11h | 命令 BCC 校验错 | 31h | 密码错或没校验密码 |
| 12h | 命令格式错 | 32h | 写错误 |
| 13h | 命令关键字错 | 33h | 密码校验封锁（只读卡） |
| 14h | 命令长度错 | 41h | 访问 COS 出错 |
| 21h | 无卡 | 04h | 命令执行正确 |
| 22h | 非标准卡 | 24h | 卡类型不支持 |
| 23h | 卡没上电 | 25h | 弹卡不成功 |

### 1.24 设置国密模式 （国密键盘有效）

命令：02h+02h+90h+mode+<BCC>

返回：02h+01h+<ST>+<BCC>

描述：设置当前模式 非国密 0， 国密 1 。改变当前工作模式会清除所有密钥

### 1.25 获取国密模式 （国密键盘有效）

命令：02h+01h+91h+<BCC>

返回：02h+02h+<ST>+mode+<BCC>

描述：获取当前模式 mode 非国密 0， 国密 1

### 1.26 生成 SM2 密钥 （国密键盘有效）

命令：02h+03h+92h+keyid+attr+<BCC>

返回：02h+01h+<ST> +<BCC>

描述：keyid: 密钥号 0~11

Attt ： 0x01 加密 0x02 解密 0x03 签名 0x04 验签

### 1.27 sm2 数据加密 （国密键盘有效）

命令：02h+ len+93h+keyid+datalen+data+<BCC>

返回：02h+Len+data+<ST> +<BCC>

描述：keyid 密钥号 0~11

Len = 2 + datalen

Datalen 1~136字节

### 1.28 sm2 数据解密 （国密键盘有效）

命令：02h+ len+94h+keyid+datalen+data+<BCC>

返回：02h+Len+data+<ST> +<BCC>

描述：keyid 密钥号 0~11

Len = 2 + datalen

Datalen 1~232字节

### 1.29 sm2 签名 （国密键盘有效）

命令：02h+ len+95h+keyid+datalen+data+<BCC>

返回：02h+Len+data+<ST> +<BCC>

描述：keyid 密钥号 0~11

datalen 32字节

data 32字节的E值

返回数据 64字节的签名值

### 1.30 sm2 验签 （国密键盘有效）

命令：02h+ len+96h+keyid+datalen+data+<BCC>

返回：02h+01h+<ST> +<BCC>

描述：keyid 密钥号 0~11

datalen 96字节

data 64字节的验签值和32字节的密码杂凑函数值

### 1.31 下载 SM2 密钥 （国密键盘有效）

命令：02h+ len+97h+keyid+attt+datalen+data+<BCC>

返回：02h+01h+<ST> +<BCC>

描述：keyid ： 密钥号 0~11

Attt ： 0x01 加密 0x02 解密 0x03 签名 0x04 验签

Datalen： 96 字节 64 字节公钥+32 字节私钥

64 字节 64 字节公钥

32 字节 32 字节私钥

data ： 64字节的验签值和32字节的密码杂凑函数值

### 1.32 导出 SM2 公钥 （国密键盘有效）

命令：02h+ 02h+98h+keyid +<BCC>

返回：02h+len+<ST>+data +<BCC>

描述：keyid ： 密钥号 0~11

返回数据 64字节的公钥

### 1.33 SM3 哈希运算 （国密键盘有效）

命令：02h+ len+99h+hashtype+hashlen+hashdata +<BCC>

返回：02h+len+<ST>+data +<BCC>

描述：Hashtype: 0x01:hash 初始化 不带数据运算
0x02:hash 数据运算 最大传输数据 1024 字节
0x04: hash 运算结束不带数据运算， 产生 32 字节的结果
0x06:hash 数据运算+运算结束 产生 32 字节的结果
0x08:hash 初始化+数据运算+运算结束产生 32 字节的结果

Hashlen 2 字节长度。

Hashtype :0x01 0x02

成功则返回 02h+01h+<ST> +<BCC>

其他：

成功则返回 02h+len+<ST> +32 字节结果+<BCC>

失败则返回 02h+01h+<ST> +<BCC>

### 1.34 HASHID 初始化 （国密键盘有效）

命令：02h+ len+9ah+keyid + useridlen+ userid+<BCC>

返回：02h+01h+<ST> +<BCC>

描述：keyid SM2 密钥号 0~11

Useridlen 用户 ID 长度

Userid 用户 ID 数据

### 1.35 使能禁止移除和自毁功能 （国密键盘有效）

命令：02h + 03h + 74h + mode1 + mode2 +<BCC>

Mode1: 0x01 自毁使能， 0x00 自毁禁止

Mode2: 0x01 移除使能， 0x00 移除禁止

返回：02h+01h+<ST> +<BCC>

### 1.36 键盘双向校验

命令：02h + Len + 71h + data + <BCC>

Data: 需要加密的数据，长度必须为 8 字节或者 16 字节，DES 运算

成功则返回 02h+len+ data +<ST> +<BCC>

失败则返回 02h+01h+<ST> +<BCC>

## 1.37 使能 EPP 固件下载 （国密键盘有效）

命令：02h + 01h + 73h + 〈BCC〉

描述：使能 EPP 固件下载。

返回：02h+01h+〈ST〉+〈BCC〉

## 1.38 获取明文或者密文按键值

命令：02h + 01h + 72h + 〈BCC〉

描述：USB 键盘在明文或者密文模式下通过发此命令主动获取键值，在明文或者密文模式下通过每秒 50 次频率不停采集或者键值。

返回：02h+02h+〈ST〉+键值+〈BCC〉

0xFF 表示没有键值按下，其他表示有键值按下

# 附录 A 键盘密钥管理

该密码键盘有两种密钥：主密钥和工作密钥。主密钥相当于国际 ATM 机上的 A、B 密钥，工作密钥相当于国际 ATM 机上的传输密钥、MAC 密钥。

有 16 个主密钥，每个主密钥有 8 个字节。16 个主密钥个管理 4 个工作密钥，每个工作密钥 8 个字节，因此密钥区共（16×8+16×8×4）640 个字节。其中主密钥明文方式下载，工作密钥用主密钥加密的密文方式下载。主密钥仅做下载工作密钥时解密用，不参加其他运算。

密码键盘收到主密钥 TMK 后，保存到主密钥区，并对 16 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。因无效主密钥时不能正确解密工作密钥。

工作密钥 8 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，因此在没有接到主机后面的下载工作密钥前是不变的。如果像招商银行，不用工作密钥，直接用主密钥解密。注意加解密前必须选择工作方式（1.16）“算法处理参数”。

在每次断电后重新加电时，密码键盘首先验证主密钥，如果主密钥有效（将 16 个主密钥用 BCC 校验），如果主密钥无效，在下载新工作密钥之前，不能进行“带参数取密码”命令，但可以进行其他命令。

重新加电时密码键盘处于关闭状态。只有用命令打开键盘后，才能允许键盘接受按键，每次按键自动发送键码值。但在加密命令时，将 0～9 变为“*”号发送，能自动打开及关闭键盘，备用键或功能键可以选择是否使用。关闭键盘也需要命令控制，关闭键盘后，所有按键不起作用。

在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），回到明码状态。超过时间可用加密命令中的参数进行修改。

键盘值按表 B-1 和表 B-2 处理、

# 附录 B 键盘值表及功能键说明

表 B-1 键盘值表

| 键位 | ASC 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 |
| 删除 | - | 08H |
| 备用键 | * | 2AH |
| 备用键 | # | 23H |
| 备用键 | . | 2Eh |

注：- 表示不可见字符。

在加密命令时，功能键的作用如下：

取消键：相当于 ESC 键，是取消当前命令执行。特别作用是取消启动密码键盘加密命令执行。

确认键：是确认 PIN 密码的输入结束。

删除键：是删除前面输入的所以字符，如前面输入了 5 个字符，当按下删除键时，必须连续发送 5 个（08H）码。

表 B-2 功能键码表

| 键位 | ASC 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 |

# 附录 C 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 0x02 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：**

终端与读写器之间进行数据交换时，命令字符串与响应字符串中，除两个前导字节 Esc=和一个结束字节 03h 用十六进制传送外，其它带<>括号字节均要转换为 ASCⅡ码格式传送。

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。