EPP 命令集

密码键盘

技术手册（C50）

深圳市证通电子有限公司

信息安全技术应用研究所

2009 年 6 月 8 日起草

固件(Firmware)版本说明

修改日期	版本号	修改内容
2002-10-08	V4 .1	建立版本： 内置 DES 64bit 和 MAC 64bit 密码算法，16 个主密钥，对应 2 个工作密钥。断电后主密钥不丢，工作密钥丢失。PIN 密码不够 8 字节，在右边补“FF”。加密时发送“*”，满长度不加发送“CR”。可作普通键盘用。
2003-3-08	V7 .0	选择 IBM3624/ISO9564 标准格式。选择 DES/3DES 密码算法。下载键盘值，屏蔽/解除任意键盘值。
2003-4-18	V7 .1	可选主密钥加密下载。
2003-6-30	V7 .2	为了兼容 X9.9，MAC 运算如果整 8 字节不进行补偿。
2003-06-19	V7.23	程序和密钥存放 SRAM/EPROM 中，开盖不但是丢失密钥而且会丢失程序
2003-10-05	V7.32	可选认证功能和一次性编程
2003-10-30	V7.33	把 SN 放到 EEPROM 中
2003-11-15	V7.35	确定 MAC 的为 247 个字节
2003-12-05	V7.42	仅配合客户需求的键盘面，修改键盘值分布。
2004-03-31	V7.45	修改 IBM3624 的填充值为 0~F。
2004-07-15	C40	根据印尼客户需求，增加 3KEY 的 TDES 运算。
2004-09-09	C41	移植到 ZT579 上使用，提供给清华同方公司。
	C46	将 ZT598 固件 C44 移植到 ZT579 上,增加显示和 IC 卡命令,保留 ZT579 的 100 个汉字库.
	C47	修改发送启动密码输入命令后不清除第二行,增加默认显示修改命令，增加背光控制，增加和修改字库，增加最小 PIN 长度设置,增加输入 PIN 达到最大长度后处理方式设定。
2009-6-8	C50	集成所有 EPP 命令集的功能，并完善

目　　录

一、 命令简介：

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，可选设置是否加尾标志。用[内容]表示可选项。

<>--表示里面的数据必须拆分。

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

16h——密钥校验值错

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 主密钥失效或不存在 X=7 杂项错

二、 命令明细：

1. 取产品版本号

命令：02h+<01h>+<30h>+<BCC>+[03h]

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

描述：DATA=Ver+SN+BACKUP 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），BACKUP 表示 2 个备用字节。

2. 程序复位自检

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

描述：键盘进行自检并复位，前者只进行键盘复位动作，相当于键盘重新上电，31h+38h 会清除所有密钥并参数复位，复位后如果主密钥有效（将 16 个主密钥用 BCC 校验），则蜂鸣器响一声；无效则蜂鸣器响三声，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。

3．下载主密钥

命令：02h+<Ln>+<32h>+<M>+<TMK>+[<KCV>]+<BCC>+[03h]

描述：

[<KCV>]为 4 个字节可选项，当有该项时，键盘在收到该命令后将计算 TMK 的校验值，并取前 4 个字节与 KCV 做比较，如果相等则保存密钥并返回，否则报 16h 错。

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 8/16/24 字节(对应 DES/3DES/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 8/16/24 字节(对应 DES/3DES/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。注意必须设定下载密钥返回要验证才能有返回验证。验证返回的数据就是用下载后的密钥，对 8 个字节 0x00 进行加密后的结果的前 4 个字节。如果需要返回验证数据，在执行该指令之前，如果主密钥是 8 字节，请先设置下载工作密钥的方式为 DES（P=00，F=20），如果主密钥是 16 或 24 字节，请先设置下载工作密钥的方式为 TDES（P=00，F=30）。

不验证返回：02h+<01h>+<ST>+<BCC>+[03h]。ST 可能是 04h、15h、16h、F6h、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用。ST 可能是 04h、15h、16h、F6h、E0。

注： ECB 方式是指把数据按照 8 字节分组，对每组分别进行加密，最后把每组加密结果连接成最终加密结果的方式。

4．下载工作密钥

命令： 02h+<Ln>+<33h>+<M>+<N>+<WP>+[<KCV>]+<BCC>+[03h]

描述：

[<KCV>]为 4 个字节可选项，当有该项时，键盘在收到该命令后将先解密得到工作密钥明文，然后用该密钥计算校验值，取前 4 个字节与 KCV 做比较，如果相等则保存密钥并返回，否则报 16h 错。

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 N(00～3Fh)中，如果设置了算法参数为下载密钥返回要验证，此时以验证方式返回信息。返回信息后关闭加密状态。验证返回的数据就是用下载后的密钥，对 8 个字节 0x0

0 进行加密后的结果的前 4 个字节。在执行该指令之前，如果主密钥是 8 字节，请先设置下载工作密钥的方式为 DES（P=00，F=20），如果主密钥是 16 或 24 字节，请先设置下载工作密钥的方式为 TDES（P=00，F=30）。如果需要返回验证数据，在执行该指令之前，如果工作密钥是 8 字节，请先设置算法参数为 DES（P=01，F=20），如果工作密钥是 16 或 24 字节，请先设置算法参数为 TDES（P=01，F=30）。

返回：02h+<01h>+<ST>+<BCC>+[03h]。ST 可能是 04h、15h、16h、A4h、B5h、C4h、D5h、E0h。

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

5. 设置帐号

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 10 个字节则是传输码，用于 ISO9564 格式 1。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。

6. 启动密码键盘加密

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

描述：

变量	描述	可选值
PIN-L	**密码长度** PIN-L 为 1 字节：00h～0Ch 表示键盘输入密码 PIN 的长度为 0 至 12 个。	00～0Ch
DISP-MD	**显示模式** DISP-MD 为 1 字节：01＝显示或返回串口“*”,	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,01=您好，请输入密码。02=请再输一次。）	00～02
TIMEOUT	**超时时间** TIMEOUT 为 1 字节（1～255 秒），超出此时间无按键，则退出 PIN 输入模式。如果设置为 0，则无超时时间。	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。根据 JM-MD 加密模式，如果 JM-MD=0 不进行加密处理，原码放在键盘缓冲区，等待取键

盘密码命令处理，因此在取键盘中密码命令之前，可以设置算法参数（决定加密模式）和激活工作密钥。如果 JM-MD≠0 需要加密处理，根据 PIN 格式要求，确定 CARD-NO 与 PIN 的运算关系，然后用 DES/3DES 以 ECB 方式进行加密运算 C＝eK(P)，得到密文数据保存在缓冲区，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。如果按键按住不放超时，则返回一个字节 81h，如果超过 TIMEOUT 时间没有按键，则返回一个字节 80h，表示超时。

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

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或者一个字符。并发生（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。

注：执行该指令之前，如果需要按键有声，请设置**发送开关键盘和按键声音**（CTR=02），如果需要按键无声，请设置**发送开关键盘和按键声音**（CTR=00），还可以根据**设置算法处理参数**来设置最小 PIN 长度，PIN 加密方法和处理方式，PIN 输入达到最大长度时的处理方法。

7．数据加密

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 或 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 Ln-1 表示小于等于 248 字节。

在执行该指令之前，如果工作密钥是 8 字节，请先设置算法参数为 DES（P=01，F=20），如果工作密钥是 16 或 24 字节，请先设置算法参数为 TDES（P=01，F=30）。

返回： 02h+<Ln>+<ST>+<密文字串>+<BCC>+[03h]。 ST 可能是 04h、15h、A4h、B5h、C4h、D5h、E0h。

8．数据解密

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 或 CBC 方式进行解密运算 P＝dK(C)，返回明文数据。返回信息后关闭加密状态。要求 Ln-1 表示小于等于 248 字节。

在执行该指令之前，如果工作密钥是 8 字节，请先设置算法参数为 DES（P=01，F=20），如果工作密钥是 16 或 24 字节，请先设置算法参数为 TDES（P=01，F=30）。

返回： 02h+<Ln>+<ST>+<明文字串>+<BCC>+[03h]。ST 可能是 04h、15h、A4h、B5h、C4h、D5h、E0h。

9. 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。

10. 显示字符串

命令：02h+<Ln>+<39h>+<显示方式>+<显示位置>+<字符串>+<BCC>+[03h]。

描述：显示字符如果是 ASCII 字符串则要求值大于 20h（空格），如果是汉字请填入其内码（两个字节）。返回信息后关闭加密状态。注意 ASCII（7F）是人民币符号￥。显示方式为 00h 时一行只能显示 15 个 ASCII 字符或者 7 个汉字，显示方式为 01h 时一行能显示 17 个 ASCII 字符或者 8 个汉字。显示位置为 00 时显示在第一行，为 01 时显示在第二行。

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

11. 数据 MAC 运算

命令：02h+<Ln>+<41h>+<字符串>+<BCC>+[03h]

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**设置算法处理参数**进行加密运算。返回 8 字节 MAC 字串数据。返回 MAC 信息后关闭加密状态。

返回：02h+<09h>+<ST>+<MAC 字串>+<BCC>+[03h]。 ST 可能是 04h、15h、A4h、B5h、C4h、D5h、E0h。

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。CBC 方式指按 8 字节分组后，对第一组加密，结果异或第二组数据，然后加密，加密结果再异或第三组，然后再加密，这样循环进行，到最后整个加密完成。在执行该指令之前，如果工作密钥是 8 字节，请先设置算法参数为 DES（P=01，F=20），如果工作密钥是 16 或 24 字节，请先设置算法参数为 TDES（P=01，F=30）。

12. 取键盘中密码

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。注意该命令

执行后密码将会清除，如果没有再输入新密码将不能再取，否则会返回错误代码 15h。

返回：02h+<0Eh>+<ST>+<密文>+<CN>+<SN>+<BCC>+[03h]。ST 可能是 04h、15h、C4h、D5h、E0h。

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。

13. 激活工作密钥

命令：02h+03h+43h+<M>+<N>+<BCC>+[03h]

描述：如果在**设置算法处理参数**中设置的是主密钥加密方式，则该命令激活的是 M(00～0Fh)号的主密钥，与工作密钥无关。如果在**设置算法处理参数**中设置的是工作密钥加密方式，则指定工作密钥作为当前工作密钥的方案，不会验证主密钥有效性。如果工作密钥号 N=40～7Fh，则与主密钥 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>+[03h]。ST 可能是 04h、15h、A4h、B5h、C4h、D5h、E0h。

14. 测试键盘响应字符

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。如果通信故障就没有返回。返回信息后不关闭加密状态。

返回： 02h+<02h>+<ST>+<CHR>+<BCC>+[03h]。ST 可能是 04h、15h、C4h、D5h。CHR 表示一个 ASCII 字符。

15. 发送开关键盘和按键声音

命令：02h+<02h>+<45h>+<CTL>+<BCC>+[03h]

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]。ST 可能是 04h、15h、C4h、D5h、E0h。

CTL 参数	功能描述	备注
00	表示关闭键盘和关闭按键 BZ 声音，并且清除 PIN 输入状态，屏幕显示恢复默认设置 **	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。	
10～1F	按键不放报错超时时间设置，10 为不报错，11～1F 分别对应超时时间为 1～15 秒。默认参数是 15，即 5 秒超时报错。	十六者选一项
20	表示更正键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。（出厂缺省）*	二者选一项（固化参数）
21	表示更正键是删除已经输入的一个字符。如没有输入字符，也发送 1 个（08H）码。	
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。**	
41～48	表示通信时采用的波特率：41h～48h 分别对应: 1200,2400,4800,9600,19200,38400,57600,115200。默认参数是 44h，即 9600 波特率	八者选一项（固化参数）
50	PS2 通信模式(明文模式键值和密文模式‘*’从 PS2 返回)	二者选一项
51	RS232 通信模式(明文模式键值和密文模式‘*’从 RS232 返回) *	
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（02h+<02h>+<ST>+<DATA>+<BCC>+[03h]），是用于表示键值。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。*为出厂缺省值，**为开机缺省值。返回信息后关闭加密状态。注意该命令设置的参数在键盘复位或重新上电的情况下会恢复初始设置。

16. 设置算法处理参数

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 参数	F 参数	功能描述	
00	10	下载主密钥采用 SAM 卡解密	可选
	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 卡解密	
	50	下载工作密钥采用 CHIP 内密码算法，主密钥解密	
01	20	键盘输入 PIN 采用内置 DES 密码算法，工作密钥加密*	七者选一项
	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	00	键盘输入 PIN 处理方式为 ASCII 格式。PIN Block =P1P2P3P4P5P6P7P8 直接 ASCII 码加密。F=填充为 00～FF。	十五者选一项
	10	键盘输入PIN处理方式为ISO9564-1格式0(ANSI9.8格式) *。 P1 = CLPPPPffffffffFF P2 = ZZZZAAAAAAAAAAAA （从帐号右边取12位，去校验） PIN Block = P1 XOR P2 where C = 0x0 L= 0x4 to 0xC	
	11	键盘输入PIN处理方式为ISO9564-1格式1。 PIN Block = CLPPPPrrrrrrrrRR where C = 0x1 L= 0x4 to 0xC	
	12	键盘输入 PIN 处理方式为 ISO9564-1 格式 2 （IC 卡用） PIN Block = CLPPPPffffffffFF where C = 0x2 L= 0x4 to 0xC	

	13	键盘输入 PIN 处理方式为 ISO9564-1 格式 3 P1 = CLPPPPffffffffFF P2 = ZZZZAAAAAAAAAAAA PIN Block = P1 XOR P2 where C = 0x3 L= 0x4 to 0xC	
	14	键盘输入 PIN 处理方式为 IBM3621 格式 PIN Block = SSSSPPPPxxxxxxxx	
	15	键盘输入 PIN 处理方式为 IBM4704 格式 PIN Block = LPPPPffffffffFSS where L= 0x4 to 0xC	
	20	键盘输入 PIN 处理方式为 IBM3624 格式 PIN Block = PPPPxxxxxxxxXXXX	
	21	键盘输入 PIN 处理方式为 NCR 格式（China） PIN=TTTTT000000PPPPP，直接加密。其中 T=为终端号。 或 PIN=TTTTTzzzzzzYYYYY YYYYY=PPPPP-NNNNN （不够减增加 100000）	
	22	键盘输入 PIN 处理方式为 NCR 格式（HK） PIN Block = TTTTYYYYYYYYYYYY YYYYYYYYYYYY=KKKKKKKKKKKK⊕489624461835 KKKKKKKKKKKK=J_1J_2×947124×1000+ $J_3J_4J_5$×947124 $J_1J_2J_3J_4J_5$=PPPPP-NNNNN （同 NCR-China 计算）	
	23	键盘输入 PIN 处理方式为 VISA 格式 2 PIN Block = LPPPPzzDDDDDDDDD where L= 0x4 to 0x6	
	24	键盘输入 PIN 处理方式为 VISA 格式 3 PIN Block = PPPPPPFXXXXXXXXX where L= 0x4 to 0xC	
	25	键盘输入 PIN 处理方式为 ECI 格式 2 PIN Block = PPPPRRRRRRRRRRR where L= 0x4	
	26	键盘输入 PIN 处理方式为 ECI 格式 3 PIN Block = LPPPPzzRRRRRRRRR where L= 0x4 to 0x6	
05	00	在加密状态，输入到约定长度时不加送回车键值	二者选一项
	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*	二者选一项
	03	在加密状态，期间允许送出功能键值	
	04	下载密钥返回不验证	二者选一项
	05	下载密钥返回要验证 *	
	06	输入 PIN 达到最大长度自动关闭键盘返回 *	二者选一项

	07	输入 PIN 达到最大长度后必须按确认键才关闭键盘返回	
06	01	MAC 采用 ASNI X9.9/X9.19 算法 * （如果设置算法参数为 DES 加解密，则 TDES 密钥只取前 8 字节密钥按 DES 计算）	五者选一项
	02	MAC 采用 PBOC SAM 卡算法	
	03	MAC 采用银联的算法	
	04	MAC 采用 CBC 算法（密钥加解密都采用全密钥加解密）	
07	10	数据 ECB 解密算法*	四者选一项
	11	数据 CBC 解密算法	
08	00-0C	PIN 输入最小长度。（默认长度为 4）	
09	00	按键键值或‘*’号直接返回 *	两者选一项
	01	按键键值或‘*’号必须用命令才能取得。	

返回： 02h+<01h>+<ST>+<BCC>+[03h]。ST 可能是 04h、15h、C4h、D5h、E0h。*为出厂缺省值。

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。

PIN BLOCK 格式中的解释：

C=格式标志码；L=PIN 长度码；PPPP=从 EPP 上输入的 PIN 码；ffffffff=可以是 P 也可以是填充为 F；FF=固定填充 FF；rrrrrrrr=可以是 P 也可以是随机数；RR=固定随机数；ZZZZ=固定填充为 0000；AAAAAAAAAAAA=银行帐号；zz=可以是 P 也可以是 00；DDDDDDDDD=填充相同的数字；XXXXXXXXX=填充相同的十六制数；TTTT=终端号；NNNNN=PIN Offset；SSSS=串号或流水号。

标准 3DES 加密算法是：如果是 16 字节密钥分为前后两部分：L 密钥和 R 密钥。以 ECB 方式加密算法过程是采用 L 密钥进行 DES，R 密钥进行 UnDES，L 密钥进行 DES 得密文。 而以 ECB 方式解密算法过程用 L 密钥进行 UnDES，R 密钥进行 DES，L 密钥进行 UnDES 得明文。

如果是 24 字节密钥分为 3 部分：K1 密钥、K2 密钥和 K3 密钥。以 ECB 方式加密算法过程是采用 K1 密钥进行 DES，K2 密钥进行 UnDES，K3 密钥进行 DES 得密文。 而以 ECB 方式解密算法过程用 K3 密钥进行 UnDES，K2 密钥进行 DES，K1 密钥进行 UnDES 得明文。

从上述看出 3DES 中如果 K1=K3，就是 16 字节的 3DES 一样了。

注：该命令设置的参数会保存在内存中，重新上电或复位不会影响这些参数。

17. 客户信息命令

命令：02h+<33h>+<3Eh>+<DATA>+<BCC>+[03h] or 02h+<01h>+<3Eh>+<BCC>+[03h]

返回：02h+<01h>+<ST>+<BCC>+[03h] or 02h+<33h>+<ST>+<DATA>+<BCC>+[03h] ST 可能是 04h、15h。

描述：设置客户信息 DATA 只能是 50 个 ASCII 码。如果命令中无 DATA，表示读取客户信息。

18. 默认显示命令

命令：02h+<Ln>+<7Fh>+<DATA>+<BCC>+[03h]

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

描述：<Ln>不大于 30（0x1E），<DATA>为默认显示信息。

19. 认证命令

命令：02h+<12h>+<40h>+<FLAG>+<DATA>+<BCC>+[03h]

返回：02h+<11h>+<ST>+<DATA>+<BCC>+[03h]。ST 可能是 04h、15h、A4h、B5h、C4h、D5h、E0h。

描述：该命令是作为识别认证用途。

FLAG=10h 时，表示进行初始（个人）化键盘。将 16 字节 DATA 客户信息（明文 ASCII 码）设置到密码键盘中。键盘出厂是不设置的，一旦客户设置后，不能再设置。除非重新下载控制程序后，才可以一次性设置。

FLAG=00h～0Fh 及 40h～7Fh 时，表示启用 16 字节客户信息作为密钥。对命令带入的随机数 DATA 进行 3DES 加密。结果作为返回信息的 DATA，作为客户认证之用。

FLAG=20h 时，将上次得到的客户认证之用信息，用原来初始化的客户信息(16 字节)作为左右密钥，进行 3DES 加密。结果作为命令中的 DATA 发送给键盘，作为 PINpad 对客户认证。返回的 DATA 是无关的随机数。

FLAG=30h 时，如果 SAM 卡模式下，仅仅需要 FLAG=30h 认证命令，过程如下：

1、 上电复位.

2、 从 SAM 卡中选择文件。APDU=00A40000023F00。

3、 从 SAM 中取 8 字节随机数。APDU=0084000008。

4、 用命令带进的 DATA 作为密钥，对从 SAM 中取出的随机数，进行 TDES 运算。

将 TDES 运算的结果，发送给 SAM 卡鉴别认证。APDU=0082000008（DATA）

注意：客户认证命令和 PINpad 认证命令必须接着使用，中间不能发送其他的命令。否则会造成认证失败。如果对键盘进行过(FLAG=10)初始化后，每次加电后，只有且必须通过双方认证，才能保证“启动键盘加密”命令执行。中途随时可以认证，如果认证失败会立即禁止“启动键盘加密”命令执行。

如果没有对键盘进行过(FLAG=10)初始化，“启动键盘加密”命令不受限制。

原始客户识别信息，象密钥一样，由客户妥善保存。

20. 访问 COS，取键盘 PIN 加密数据

命令：02h+<Ln>+<47h>+<APDU>+<BCC>

返回：02h+<Ln>+<ST>+<COS-DATA>+<BCC>。ST 可能是 04,11h,12h,13h,14h,21h,22h,23h,24h,41h。

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“ZT598E00”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。

21. 访问 COS

命令：02h+<Ln>+<48h>+<APDU>+<BCC>

返回：02h+<Ln>+<ST>+<COS-DATA>+<BCC>。ST 可能是 04,11h,12h,13h,14h,21h,22h,23h,24h,41h。

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。

22. 上电复位 IC 卡

命令：02h+<01h>+<49h>+<BCC>

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

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。

23. 设置 IC 卡座及卡类型

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

返回：02h+<Ln>+<ST>+<DATA>+<BCC>。ST 可能是 04,11h,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。

24. 读取 IC 卡座及卡类型

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：

88h 表示 CPU 智能卡，如 SAM 卡等。

25. 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。

26. 用户信息处理

命令：02h+<02h>+<5Ch>+<BLOCK-SET>+<BCC>+[03h] 或者 02h+<88h>+<5Ch>+<BLOCK-SET>+<USER-DATA>+<USER-PASSWORD>+<BCC>+[03h]

返回：02h+<81h>+<ST>+<USER-DATA>+<BCC>+[03h] 或者等待按键后返回 02h+<01h>+<ST>+<BCC>+[03h]。ST 可能是 04,15h,80h。

描述：读取或写入用户数据，每次写入 128 字节，总共可以写入 4 块共 512 个字节数据。该数据断电后不丢失。写数据时需要在键盘上输入与命令中一致的 6 位口令。<BLOCK-SET>是数据块选择，值为 00h～03h。

27. SAM 卡认证命令

命令：02h+<06h>+<50h>+<Key Index>+<Password>+<BCC>+[03h]

返回：02h+<01h>+<ST>+<BCC>+[03h]。ST 可能是 04，11h,12h,13h,14h,15h，21h,22h,23h,24h。

描述：该命令用于选择 SAM 内的主密钥并进行认证操作。Key Index 为一个字节，表示密钥号，取值范围为 00～1F。Password 为认证密码，为 4 个字节，由 8 个密码合成。

28. 设置初始向量命令

命令：02h+<09h>+<60h>+<IV data>+<BCC>+[03h]

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

描述：该命令用于设置 CBC 运算中初始向量数据。

29. 加密主密钥下载命令

命令：02h+<Ln>+<61h>+<M1>+<M2>+<TMK>+[<KCV>]+<BCC>+[03h]

描述：

[<KCV>]为 4 个字节可选项，当有该项时，键盘在收到该命令后将在得到主密钥的明文后计算该密钥的校验值，并取前 4 个字节与 KCV 做比较，如果相等则保存密钥并返回，否则报 16h 错。

下载不验证方式时，密钥号 M1 为 1 字节（00～0Fh），为解密用主密钥号，密钥号 M2 为 1 字节（00～0Fh），为解密后保存的主密钥号。16 个主密钥 TMK 为 8/16/24 字节(对应 DES/3DES/3DES)密文。返回信息后关闭加密状态。

下载有验证方式时，密钥号 M1 为 1 字节（00～0Fh），为解密用主密钥号，密钥号 M2 为 1 字节（00～0Fh），为解密后保存的主密钥号。，以 ECB 方式解密 TMK，命令中 M1 为解密用主密钥。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。注意必须设定下载密钥返回要验证才能有返回验证。验证返回的数据就是用下载后的密钥，对 8 个字节 0x00 进行加密后的结果的前 4 个字节。如果需要返回验证数据，在执行该指令之前，如果主密钥是 8 字节，请先设置下载工作密钥的方式为 DES（P=00，F=20），如果主密钥是 16 或 24 字节，请先设置下载工作密钥的方式为 TDES（P=00，F=30）。

不验证返回：02h+<01h>+<ST>+<BCC>+[03h]。ST 可能是 04h、15h、16h、F6h、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用。ST 可能是 04h、15h、16h、F6h、E0。

注： ECB 方式是指把数据按照 8 字节分组，对每组分别进行加密，最后把每组加密结果连接成最终加密结果的方式。

30. 删除密钥命令

命令：02h+<02h>+<62h>+<密钥号>+[03h]
返回：02h+<01h>+<ST>+<BCC>+[03h]。ST 可能是 04，15。
描述：该命令删除键盘中的密钥。
密钥号：00～0F 时为删除主密钥，40～7F 时为删除工作密钥（00～3F）。

31. 虚拟按键命令

命令：02h+<02h>+<63h>+<按键位置>+[03h]
返回：02h+<01h>+<ST>+<BCC>+[03h]。ST 可能是 04，15。
描述：该命令用于仿真按键的动作，当发了该命令后，就相当于真实按了该位置的按键一样。
按键位置：键盘主界面从左到右，从上到下依次为 00h～0Fh。然后是左功能键从上至下为 10h～13h，右功能键从上至下为 14h～17h。

32. 手工输入密钥命令

命令：02h+<04h>+<64h>+<管理员代码>+<密钥号>+<密钥长度>+[03h]
返回：02h+<01h>+<ST>+<BCC>+[03h] 或者 02h+<05h>+<ST>+<DATA>+<BCC>+[03h]。其中<DATA>为 4 个字节返回码作验证用。ST 可能是 04h、15h、16h、F6h、E0。
描述：该命令用于手工输入密钥。当设置为密钥校验值返回时，在最后合成密钥时将返回密钥的校验值。当进入手工输入密钥时，键盘将自动打开，等待输入密钥，当输入完成后，按确认键退出。
管理员代码：30h—管理员 A 输入密钥
31h—管理员 B 输入密钥
33h—管理员 C 输入密钥
41h—管理员 A，B 输入的密钥进行异或合成。此时密钥号和密钥长度没有意义。
42h—管理员 A,B,C 输入的密钥进行异或合成。此时密钥号和密钥长度没有意义。
密钥号：00～0F 为主密钥，40～7F 为工作密钥（00～3F）。
密钥长度： 00h—8 字节密钥
01h—16 字节密钥
02h—24 字节密钥

33. 取密钥校验值命令

命令：02h+<02h>+<65h>+<密钥号>+[03h]
返回：02h+<05h>+<ST>+<DATA>+<BCC>+[03h]。其中<DATA>为 4 个字节密钥校验值。ST 可能是 04h、15h。
描述：当密钥号为 00～0F 时为返回主密钥的校验值，
当密钥号为 40～7F 时，为返回工作密钥 00～3F 的校验值。
当密钥号为 30 时，为返回管理员 A 输入的密钥的校验值，
当密钥号为 31 时，为返回管理员 B 输入的密钥的校验值，
当密钥号为 32 时，为返回管理员 B 输入的密钥的校验值，

34. PIN OFFSET 命令

命令：02h+<22h>+<66h>+<OFFSET 模式>+< Validation data >+< Decimalization table>+ [03h]
返回：02h+<Ln>+<ST>+<DATA>+<BCC>+[03h]。其中<DATA>为最小 PIN 长度个字节 PVV。ST 可能是 04h、15h。
描述：OFFSET = 30h 时为 IBM_PIN OFFSET 模式。
= 31h 时为 VISA_PIN OFFSET 模式。

35. 取随机数命令

命令：02h+<01h>+<67h>+ [03h]
返回：02h+<09h>+<ST>+<8 字节随机数>+<BCC>+[03h]。ST 可能是 04h、15h。
描述：该命令用于从键盘取 8 字节长度的随机数。

36. 取键值命令

命令：02h+<01h>+<68h>+ [03h]
返回：02h+<05h>+<ST>+<按键键值>+<BCC>+[03h]。ST 可能是 04h、15h。
描述：该命令用于从键盘按键缓冲中取出前 4 字节长度的键值。该命令只有在**设置算法参数** P=09，F=01

的情况下才能正常使用，否则报 15 错。

37. 设置键值命令

命令：02h+<21h>+<7Eh>+<按键键值>+[03h]
返回：02h+<01h>+<ST>+<BCC>+[03h]。
描述：该命令用于设置键盘的键值。按键键值总共 32 个字节，按照 16 字节主界面键值+4 字节左功能键键值+4 字节右功能键键值+8 字节备用键键值组成。主界面键值的顺序为从左到右，从上到下，功能键的顺序为从上到下。

38. 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，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，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。

三、 键盘值表及功能键说明

键位	表一	
	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
删除	-	1BH
确认	-	0DH
F1（备用）	A	41H
F2（备用）	B	42H

-表示不可见字符。

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）。

四、 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。

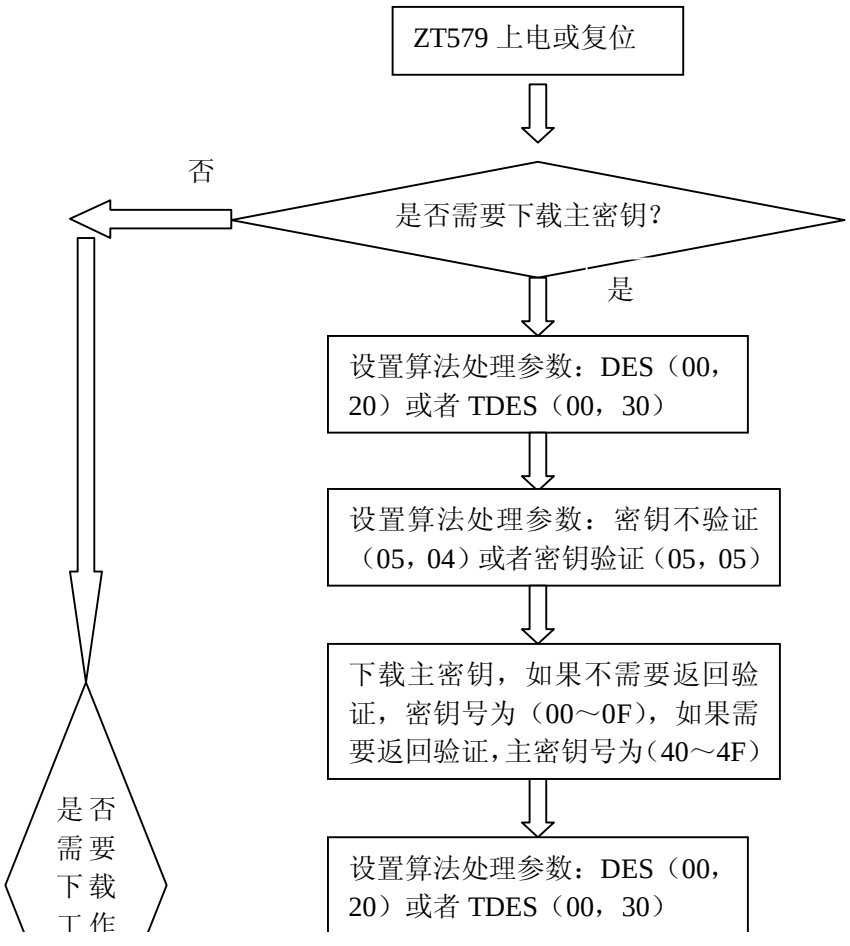
接收时将 2 字节转换为 1 字节：把第一个 ASCII 字符减去 30h(或 37h)做为高半字节，把第二个 ASCII 字符减去 30h(或 37h)做为低半字节，再把高低半字节合成一个十六进制字节。

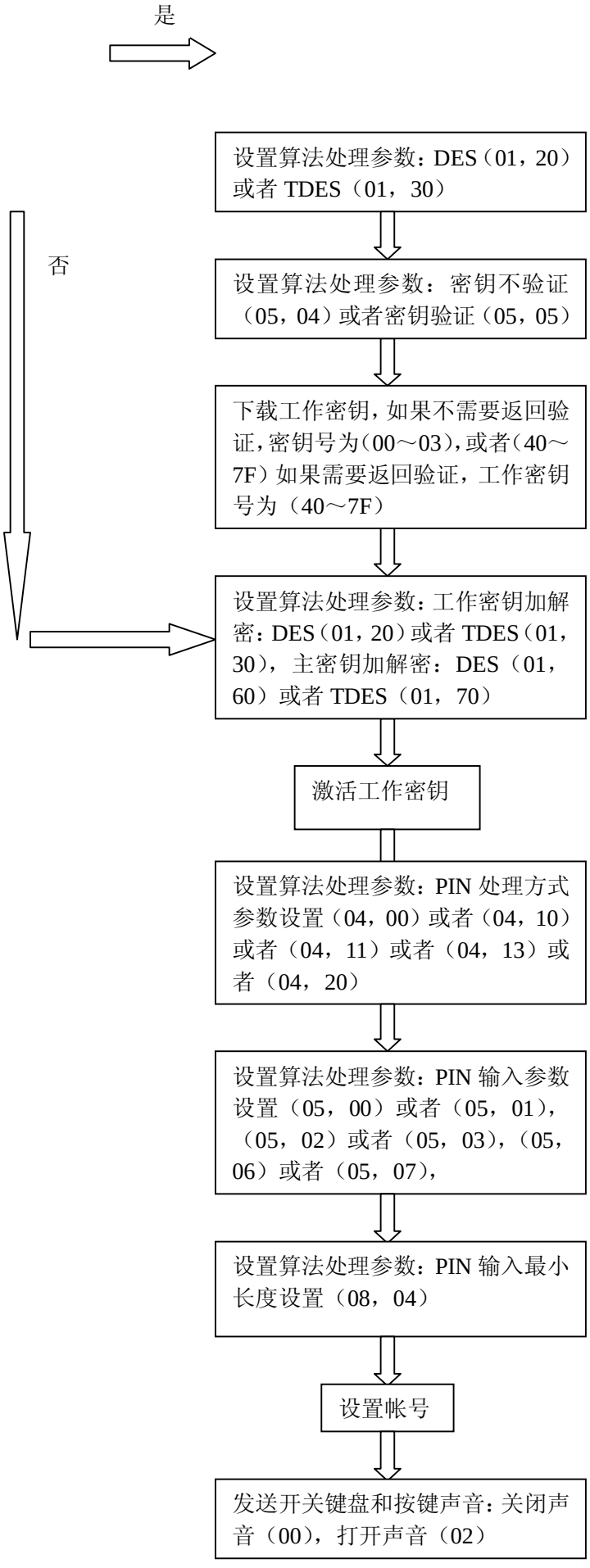
附录 A：命令字对应表

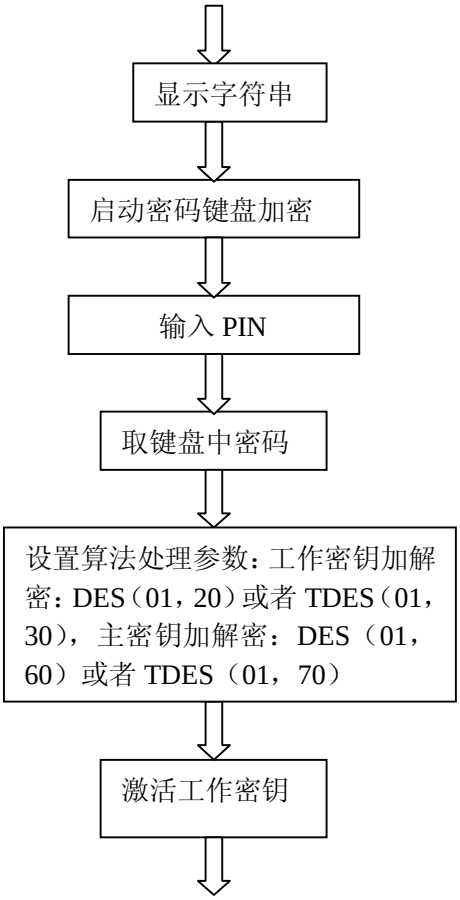
命令名称	命令字
取产品版本号	30h
程序复位自检	31h
下载主密钥	32h
下载工作密钥	33h
设置帐号	34h
启动密码键盘加密	35h
数据加密	36h
数据解密	37h
读取/设置产品终端号字符串	38h
显示字符串	39h
客户信息命令	3Eh
认证命令	40h
数据 MAC 运算	41h

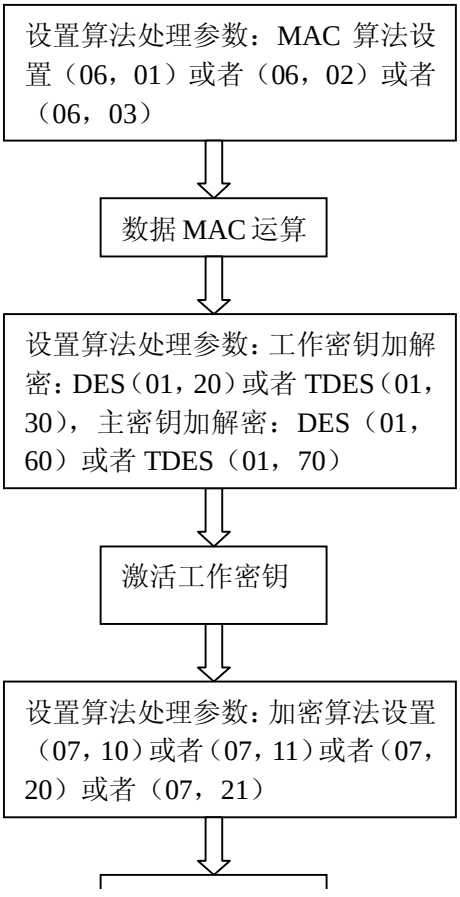
取键盘中密码	42h
激活工作密钥	43h
测试键盘响应字符	44h
发送开关键盘和按键声音	45h
设置算法处理参数	46h
访问 COS，取键盘 PIN 加密数据	47h
访问 COS	48h
上电复位 IC 卡	49h
变换计算 MAC 值	4Ah
SAM 卡认证命令	50h
设置 IC 卡座及卡类型	59h
读取 IC 卡座及卡类型	5Ah
给 CPU 卡座断电	5Bh
用户信息处理	5Ch
设置初始向量命令	60h
加密主密钥下载命令	61h
删除密钥命令	62h
虚拟按键命令	63h
手工输入密钥命令	64h
取密钥校验值命令	65h
PIN OFFSET 命令	66h
取随机数命令	67h
取键值命令	68h
取设备状态命令	7Dh
设置键值命令	7Eh
默认显示命令	7Fh

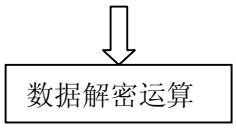
附录 B：EPP 标准使用流程：




是
否
设置算法处理参数：DES（01，20）或者 TDES（01，30）
设置算法处理参数：密钥不验证（05，04）或者密钥验证（05，05）
下载工作密钥，如果不需要返回验证，密钥号为（00～03），或者（40～7F）如果需要返回验证，工作密钥号为（40～7F）
设置算法处理参数：工作密钥加解密：DES（01，20）或者 TDES（01，30），主密钥加解密：DES（01，60）或者 TDES（01，70）
激活工作密钥
设置算法处理参数：PIN 处理方式参数设置（04，00）或者（04，10）或者（04，11）或者（04，13）或者（04，20）
设置算法处理参数：PIN 输入参数设置（05，00）或者（05，01），（05，02）或者（05，03），（05，06）或者（05，07），
设置算法处理参数：PIN 输入最小长度设置（08，04）
设置帐号
发送开关键盘和按键声音：关闭声音（00），打开声音（02）


显示字符串
启动密码键盘加密
输入 PIN
取键盘中密码
设置算法处理参数：工作密钥加解密：DES（01，20）或者 TDES（01，30），主密钥加解密：DES（01，60）或者 TDES（01，70）
激活工作密钥


设置算法处理参数：MAC 算法设置（06，01）或者（06，02）或者（06，03）
数据 MAC 运算
设置算法处理参数：工作密钥加解密：DES（01，20）或者 TDES（01，30），主密钥加解密：DES（01，60）或者 TDES（01，70）
激活工作密钥
设置算法处理参数：加密算法设置（07，10）或者（07，11）或者（07，20）或者（07，21）



附录 C：参数设置和下载密钥的长度之间的关系：

下载工作密钥：

原先下载的主密钥是 8 字节：

参数设置为（00，20），工作密钥将会以 DES 解密存储。

参数设置为（00，30），工作密钥将会以 3DES 解密存储，原先主密钥的后 8 字节将作为右密钥（此时不确定）参与运算。

原先下载的主密钥是 16 字节：

参数设置为（00，20），工作密钥将会以 DES 解密存储。此时只用到主密钥的左密钥。

参数设置为（00，30），工作密钥将会以 3DES 解密存储。

PIN 运算，MAC 运算，数据加解密运算：

原先下载的工作密钥是 8 字节：

参数设置为（01，20），数据将会进行 DES 运算。

参数设置为（01，30），数据将会进行 3DES 运算，原先工作密钥的后 8 字节将作为右密钥（此时不确定）参与运算。

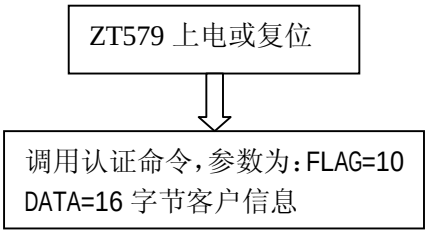
原先下载的工作密钥是 16 字节：

参数设置为（01，20），数据将会进行 DES 运算。此时只用到工作密钥的左密钥。

参数设置为（01，30），数据将会进行 3DES 运算。

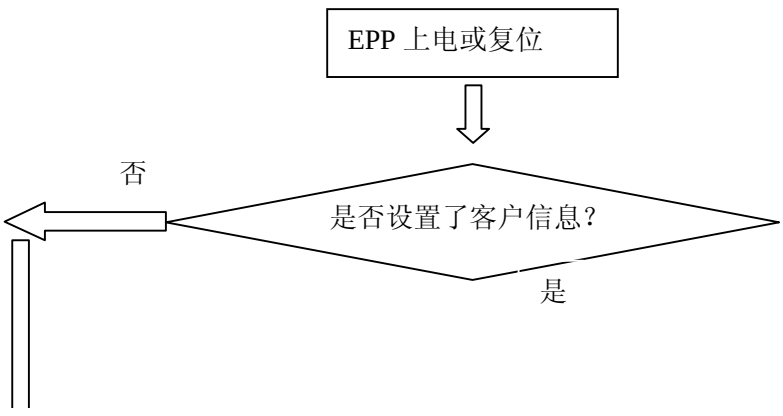
附录 D：EPP 认证使用流程：

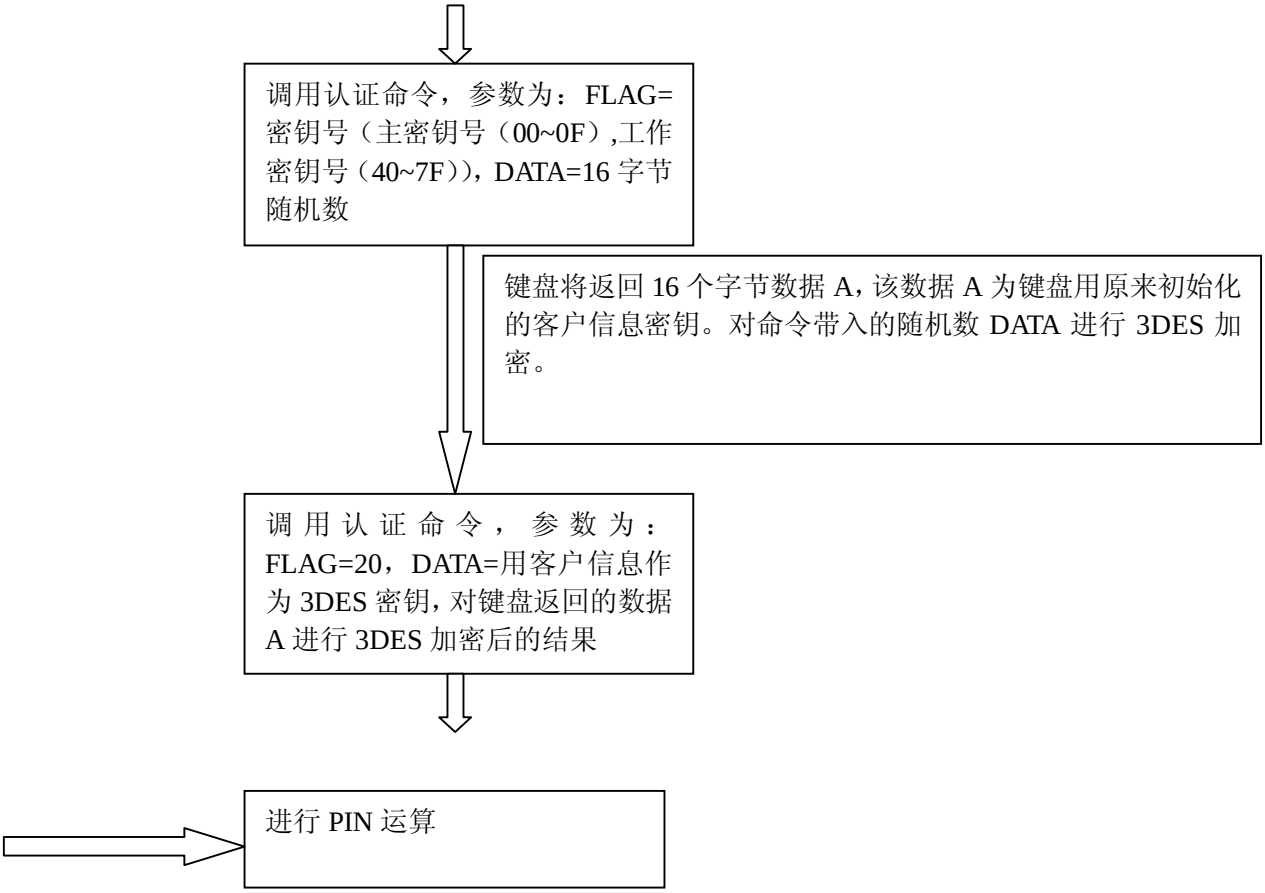
1、设置用户信息：



注意：用户信息只能设置一次。

2、进行 PIN 运算：




调用认证命令，参数为：FLAG=密钥号（主密钥号（00~0F）,工作密钥号（40~7F）），DATA=16 字节随机数
键盘将返回 16 个字节数据 A，该数据 A 为键盘用原来初始化的客户信息密钥。对命令带入的随机数 DATA 进行 3DES 加密。
调用认证命令，参数为：FLAG=20，DATA=用客户信息作为 3DES 密钥，对键盘返回的数据 A 进行 3DES 加密后的结果
进行 PIN 运算