# Command

Load key method---验证OK 根据开发文档—43页说明。

Review Serial Number—设备SN号的唯一性 已验证，不可更改

Send External Authenticate Command 使用指令产生8位随机数，并把随机数加密发送到上位机，上位机解密之后，再发回加密磁头。验证OK

Encryption Settings----OK

Review KSN (DUKPT Key management only)----SN的前7位+自定义三位（0x10 0x00 0x00）

Review Security Level

Encryption Output Format Setting----根据是否选择普通加密和强加密。普通加密固定格式：02+数据长度高低位+卡类型+三个轨道是否有数据+三个轨道数据长度+轨道1掩码+轨道2掩码+轨道3明文+三个轨道加密数据+1、2轨道哈希值+FIX(SN)/DUKPT(KSN)—来自开发手册32页（4.3. DUKPT Key Management Level 3 Data Output Format）

强制加密输出格式---根据开发手册34页输出格式

Encryption Option Setting: (for enhanced encryption format only)

Hash Option Setting---只有在强加密模式下可以选择某个轨道发送/不发送该轨道哈希值

Mask Option Setting: (for enhanced encryption format only)--- 只有在强加密模式下使用，可以进行某轨道进行掩码，若把某轨道掩码不设置，则该轨道没有掩码数据和明文数据，只有加密数据。

Activate Authentication Mode Command—在该指令下会产生Challegnge 1和 Challenge 2,Challenge 1是有6位随机数+KSN最后两位，组合成的8bit加密数据，DUKPT KEY使用\xF0\xF0\xF0\xF0\xF0\xF0\xF0\xF0\xF0\xF0\xF0\xF0\xF0\xF0\xF0\xF0。Challgenge 2是直接产生8位随机数，也进行加密。\xF0\xF0\xF0\xF0\xF0\xF0\xF0\xF0\xF0\xF0\xF0\xF0\xF0\xF0\xF0\xF0作为当前加密密钥。这是第一次认证，两个Challenge分别使用全局数组保存。

Activation Challenge Reply Command----由于Activate Authentication Mode Command已经返回Challenge 1和Challenge 2给上位机，认证通过需要把Challenge 1的前6个字节+两位延时时间，发送给下位机，验证成功返回06，并且加密等级变成4，加密模式变成DUKPT。在加密等级设置为4的时候，必须先进行验证，否则无法读卡。若是在发送Challenge 1进行二次认证错误，则需重新进行Activate Authentication Mode Command该步骤。否则无法进行验证

Deactivate Authenticated Mode Command-----退出等级4加密认证，需要把Challenge 2发送给下位机进行验证。若成功，则退出，否则依然留在等级4加密模式。当退出加密等级4的时候，并且验证退出成功，加密等级4变成加密等级0.明文传输状态。

Get Reader Status Command----按照客户测试文档以及英文说明文档，已验证功能OK。是根据当前读卡器状态读取。当前读卡器状态分别有--》等待认证。认证失败，认证成功，取消认证模式，等待刷卡等等。此认证模式并不是读卡器状态设置值。

# Encryption

TDES-DUKPT

# HID USB mode

HID MSR mode

HID KB mode—目前无法和IDTECH上位机根据通信

# Output format

Magnetic Track Basic Decoded Data Format

USB HID Data Format

Level 1 and level 2 POS Mode Data Output Format---该模式下输出的格式，从ICTECH文档描述很复杂，请客户给出参考格式。

DUKPT Key Management Level 3 Data Output Format

DUKPT Key Management Level 3 Data Output Format—可自行设置强制加密/普通加密。

DUKPT Enhanced Level 3 Data Output Format

DUKPT Level 4 Data Output Format