C200系列PCI-E密码卡用户手册

（版本：1.0.0.0）

中国金融认证中心

2019年09月16日

版权声明：本文档的版权属于中国金融认证中心任何人或组织未经许可，

不得擅自修改、拷贝或以其它方式使用本文档中的内容

文档修订记录

本文档会随时保持更新，请与中国金融认证中心索要最新版本

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版本 | 内容 | 日期 | 编写 | 审核 |
| 1.0.0.0 | 创建文档 | 2019/09/16 | 简志栋 |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

注：对该文件内容增加、删除或修改须填写此修订记录，详细记载变更信息，以保证其可追溯性。

目录

[1 产品介绍 1](#_Toc19525648)

[1.1 产品简介 1](#_Toc19525649)

[1.2 产品功能 1](#_Toc19525650)

[1.2.1 密钥生成与管理 1](#_Toc19525651)

[1.2.2 数字签名产生和验证 1](#_Toc19525652)

[1.2.3 数据加密和解密 2](#_Toc19525653)

[1.2.4 消息鉴别码功能 2](#_Toc19525654)

[1.2.5 物理随机数产生 2](#_Toc19525655)

[1.2.6 用户访问权限控制 2](#_Toc19525656)

[1.2.7 密钥备份及恢复 2](#_Toc19525657)

[1.2.8 密钥导入及导出 2](#_Toc19525658)

[1.2.9 文件管理 3](#_Toc19525659)

[2 准备工作 4](#_Toc19525660)

[2.1 运行环境 4](#_Toc19525661)

[2.2 安全要求 4](#_Toc19525662)

[3 安装密码卡 5](#_Toc19525663)

[3.1 安装驱动 5](#_Toc19525664)

[3.2 启动管理程序 5](#_Toc19525665)

[3.3 安装向导 6](#_Toc19525666)

[4 用户登录 8](#_Toc19525667)

[5 设备管理 9](#_Toc19525668)

[6 权限管理 10](#_Toc19525669)

[6.1 查看注册信息 10](#_Toc19525670)

[6.2 查看登录状态 10](#_Toc19525671)

[6.3 修改用户口令 11](#_Toc19525672)

[6.4 管理员管理 12](#_Toc19525673)

[6.4.1 增加管理员 12](#_Toc19525674)

[6.4.2 删除管理员 13](#_Toc19525675)

[6.5 操作员管理 13](#_Toc19525676)

[6.5.1 增加操作员 13](#_Toc19525677)

[6.5.2 删除操作员 14](#_Toc19525678)

[6.6 用户注销 14](#_Toc19525679)

[6.7 查看权限设置表 15](#_Toc19525680)

[7 密钥管理 16](#_Toc19525681)

[7.1 密钥初始化 16](#_Toc19525682)

[7.2 非对称密钥管理 16](#_Toc19525683)

[7.2.1 RSA密钥管理 16](#_Toc19525684)

[7.2.1.1 产生RSA密钥对 16](#_Toc19525685)

[7.2.1.2 删除RSA密钥对 17](#_Toc19525686)

[7.2.1.3 查看RSA密钥状态 18](#_Toc19525687)

[7.2.1.4 查看RSA公钥 18](#_Toc19525688)

[7.2.2 ECC密钥管理 18](#_Toc19525689)

[7.2.2.1 产生ECC密钥对 18](#_Toc19525690)

[7.2.2.2 删除ECC密钥对 19](#_Toc19525691)

[7.2.2.3 查看ECC密钥状态 20](#_Toc19525692)

[7.2.2.4 查看ECC公钥 20](#_Toc19525693)

[7.3 对称密钥管理 21](#_Toc19525694)

[7.3.1 DES密钥管理 21](#_Toc19525695)

[7.3.1.1 产生DES密钥 22](#_Toc19525696)

[7.3.1.2 删除DES密钥 22](#_Toc19525697)

[7.3.1.3 查看DES密钥状态 23](#_Toc19525698)

[7.3.2 SM4密钥管理 24](#_Toc19525699)

[7.3.2.1 产生SM4密钥 25](#_Toc19525700)

[7.3.2.2 删除SM4密钥 25](#_Toc19525701)

[7.3.2.3 查看SM4密钥状态 26](#_Toc19525702)

[7.4 密钥备份恢复 27](#_Toc19525703)

[7.4.1 密钥备份 27](#_Toc19525704)

[7.4.2 密钥恢复 28](#_Toc19525705)

[7.5 密钥导入导出 29](#_Toc19525706)

[7.5.1 密钥导出 29](#_Toc19525707)

[7.5.2 密钥导入 31](#_Toc19525708)

[8 功能自检 32](#_Toc19525709)

[9 文件管理 33](#_Toc19525710)

[9.1 查看文件状态 33](#_Toc19525711)

[9.2 创建文件 33](#_Toc19525712)

[9.3 写文件 33](#_Toc19525713)

[9.4 读文件 33](#_Toc19525714)

[9.5 删除文件 34](#_Toc19525715)

[附录 A 35](#_Toc19525716)

[常见问题 35](#_Toc19525717)

[附录 B 36](#_Toc19525718)

[权限设置表 36](#_Toc19525719)

[附录 C 38](#_Toc19525720)

[错误码定义 38](#_Toc19525721)

# 产品介绍

## 产品简介

C200系列PCI-E密码卡是由北京中金国信科技有限公司自主研发的高性能密码卡，能够适用于各类密码应用系统进行高速的、多任务并行处理的密码运算，可以满足应用系统数据的签名/验证、加密/解密的要求，同时提供安全、完善的密钥管理机制。

密码卡应用接口对上层应用透明，应用开发商能够快速的使用密码卡所提供的安全功能。密码卡应用接口符合国家密码管理局发布的《GM/T 0028-2014 密码设备应用接口规范》中标准接口规范。本产品支持RSA1024/1152/1408/1984/2048/4096和DES/TDES密码算法，兼容C200型PCI-E密码卡的使用，能够平滑接入各种系统平台，满足大多数应用系统的要求，在应用系统安全方面具有广泛的应用前景。

## 产品功能

### 密钥生成与管理

可以生成RSA非对称密钥对和对称密钥，使用由国家密码管理局认证通过的物理噪声源产生器芯片生成的随机数。

### 数字签名产生和验证

支持利用内部生成的RSA密钥对或外部导入的RSA密钥对对请求数据进行数字签名和验证签名。

### 数据加密和解密

支持DES/TDES算法的ECB、CBC、OFB、CFB模式的数据加密和解密运算。

### 消息鉴别码功能

支持DES/TDES算法的MAC产生。

### 物理随机数产生

使用由国家密码管理局认证通过的噪声源产生器芯片生成的随机数。

### 用户访问权限控制

通过读卡器实现IC卡数据读写，IC卡分为操作员、管理员和备份卡。

### 密钥备份及恢复

支持密钥的备份和恢复功能，保证了安全应用系统的安全性和可靠性。

### 密钥导入及导出

支持密钥的导入和导出功能，保证了安全应用系统的安全性和可靠性。

### 文件管理

支持最大3个文件、最大字节为8K Byte的创建，以及读取、写入和删除功能。

# 准备工作

## 运行环境

硬件环境：具有PCI Express 8x接口的计算机设备，需预留读卡器安装位置，具体尺寸请联系技术支持。

操作系统：Linux 32/64位系统，内核版本2.6.32及更高版本。

## 安全要求

重要用户密钥对一定要通过管理程序在设备内产生；

导入密钥操作需要使用专用的工具，并在网络隔离的情况下进行；

使用更安全的口令或密码；

使用国家密码主管部门的批准的密码算法。

# 安装密码卡

## 安装驱动

进入驱动目录，请先确认load\_driver.sh拥有可执行权限，如没有权限应当先执行chmod 777 load\_driver.sh指令；然后执行. load\_driver.sh。若不出现提示语，则表示驱动已安装成功。

## 启动管理程序

将安装包解压至用户目录，请先确认ManagementTool\_Mix是否拥有可执行权限，如没有应当先执行chmod 777 ManagementTool\_Mix指令。

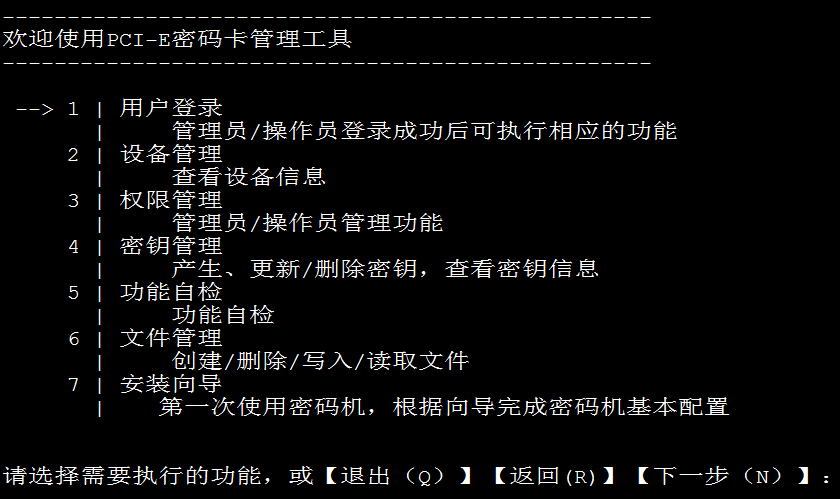
工具默认为英文显示，如需要显示中文界面，可按以下步骤操作：

系统安装中文语言支持（如已支持中文，可忽略此步）；

1、将Management.mo拷贝至“/usr/share/locale/zh\_CN/LC\_MESSAGES”目录；

2、设置终端的显示语言为简体中文。在Linux终端执行”export LANGUAGE=zh\_CN:zh”或”export LC\_MESSAGES=zh\_CN.UTF-8”；该设置仅在当前终端生效。

启动管理程序，显示页面如下：

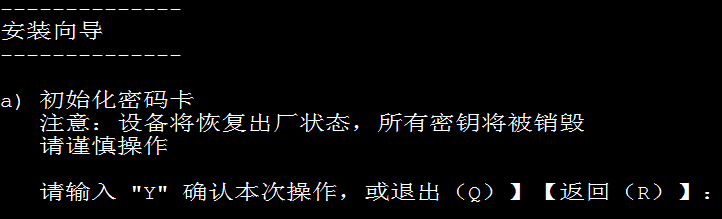


## 安装向导

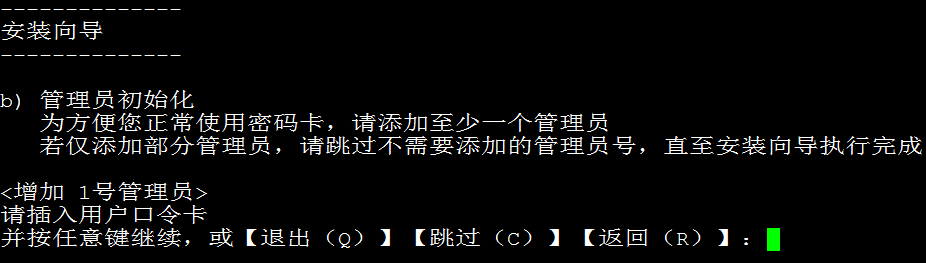
在第一次使用C200系列PCI-E密码卡，或者已获取超级管理员权限，可以使用管理程序的安装向导功能，逐步完成对C200系列PCI-E密码卡的基本配置。如果需要使用其他配置功能，可参考其他章节的管理操作说明。

安装向导提供以下主要配置功能：

a)初始化密码卡：清空所有密钥及管理信息。



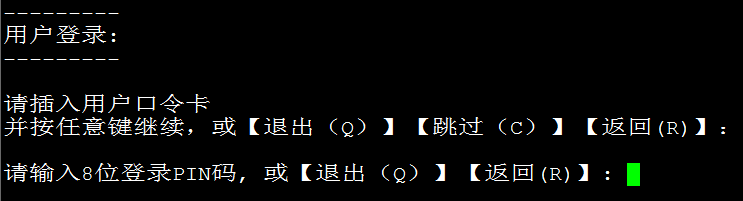
b)管理员初始化：为保证设备的安全性、可靠性，及正常使用所有功能，建议设置3个管理员（标准配置）。



<!>提示：管理员初始化最多可增加5个管理员，若注册成功3个管理员后，后续可输入“c”进行跳过，直至安装向导执行完成。

# 用户登录

选择“用户登录”界面登录管理员或者登录操作员。

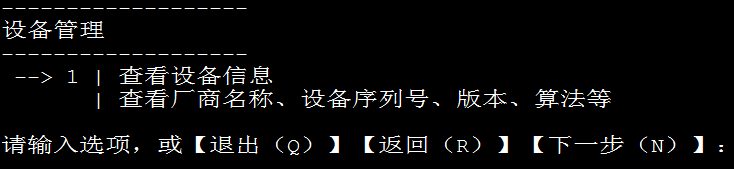


在登录时请根据卡片标示的方向插入管理员或者操作员IC卡并输入IC卡保护口令（PIN）。

<!>安全提示：在出厂时所有用户IC卡的保护口令均被初始化为“abcd1234”，为保证系统的安全性，请及时通过“权限管理”界面中“修改用户口令”功能修改该口令。

# 设备管理

可查看厂商信息、设备编号、系统版本、支持算法等信息。

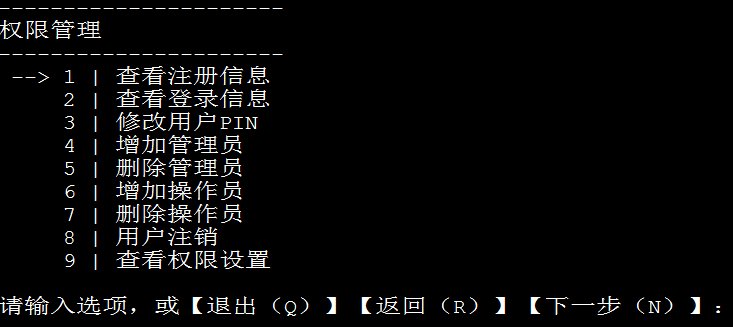


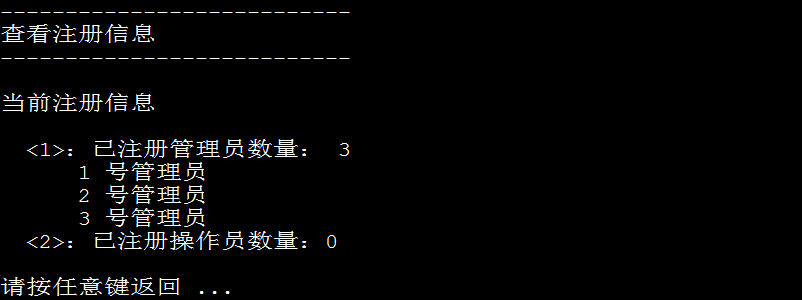
<!>提示：使用密码卡过程中遇到问题需要技术支持时，提供以上信息将会帮助我们更快解决问题。

# 权限管理

## 查看注册信息

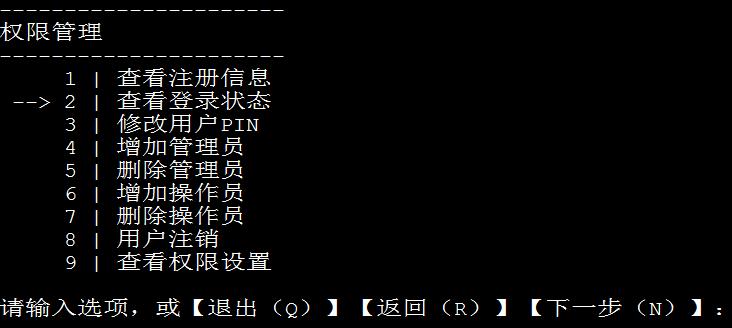
选择“查看注册信息”，即可查看当前管理员或操作员的注册信息。

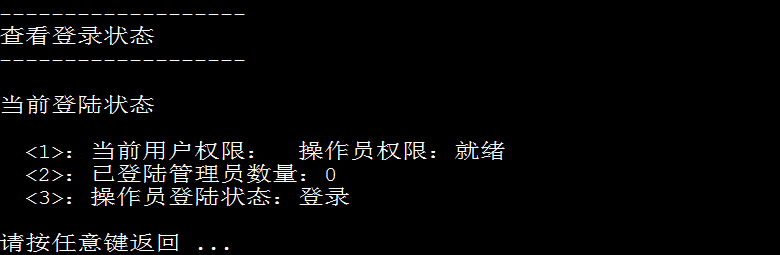




## 查看登录状态

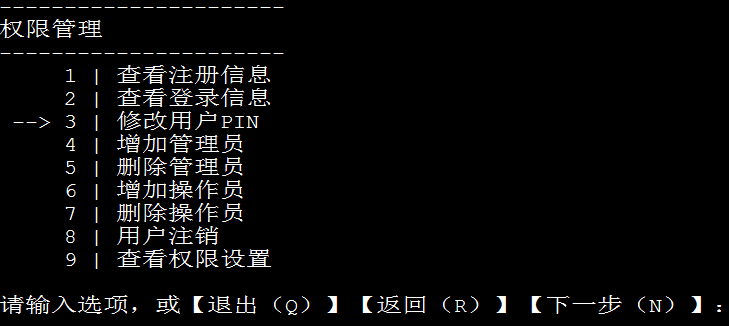
选择“查看登录状态”，即可查看当前管理员或操作员的登录状态。

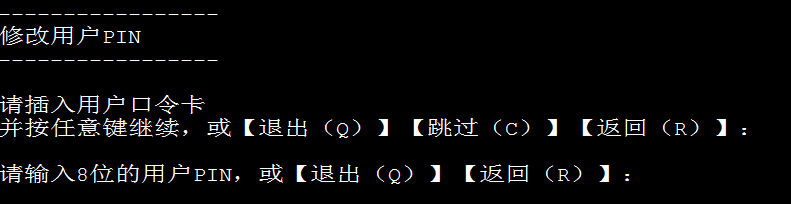




## 修改用户口令

根据卡片标示的方向插入IC卡，选择“修改用户口令”，输入IC卡原保护口令和新口令，即可完成修改。





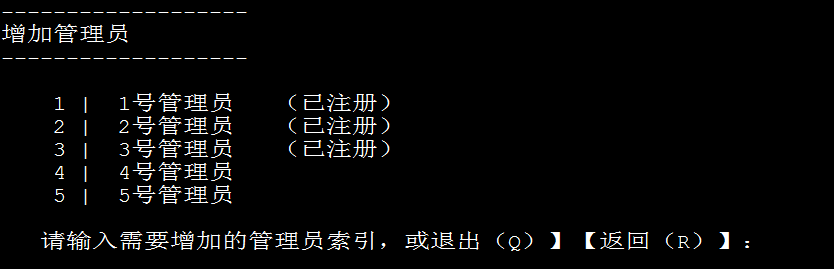
## 管理员管理

### 增加管理员

根据卡片标示的方向插入IC卡，选择“修改用户口令”，输入IC卡原保护口令和新口令，即可完成修改。

a)选择“权限管理”中的“增加管理员”功能。

b)根据卡片标示的方向插入管理员IC卡，输入要增加的管理员索引号，点击“Enter”操作。



c)输入管理员IC卡保护口令（PIN），才能获得对IC卡的访问权限。

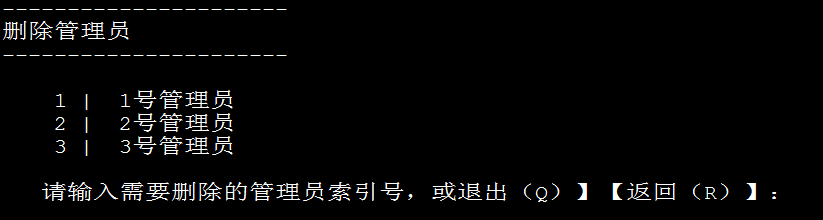
d)输入正确的口令后，即可完成新增管理员功能。

<!>安全提示：该密码卡在设计时支持1到5个管理员，为保证密码卡的安全性及可靠性,建议设置3个管理员。

<!>安全提示：在出厂时所有用户卡的保护口令均被初始化为“abcd1234”，为保证系统的安全性，请及时通过“修改用户口令”功能修改该口令。

### 删除管理员

在“权限管理”中选择“删除管理员”功能，即可完成管理员删除。

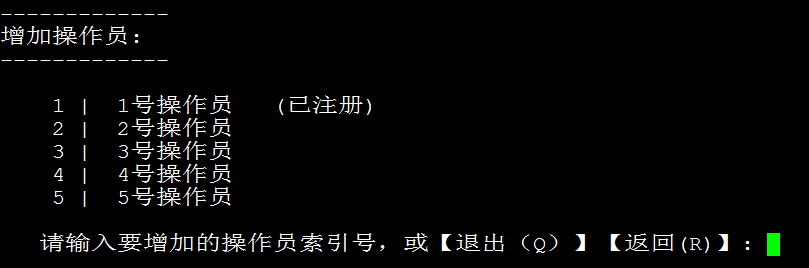


<!>安全提示：当某张管理员IC卡丢失或认为其安全性存在隐患时，可通过“删除管理员”及“增加管理员”功能更新管理员。

## 操作员管理

### 增加操作员

根据IC卡标识的方向插入操作员IC卡，并输入IC卡保护口令（PIN），即可完成新增操作员功能。

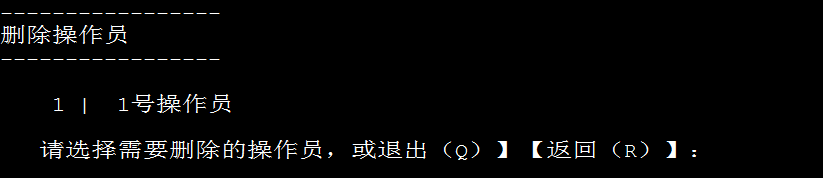


<!>安全提示：为保证设备的可扩展性，本密码卡支持1到5个操作员，但标准配置为1个操作员。

<!>安全提示：在出厂时所有用户卡的保护口令均被初始化为“abcd1234”，为保证系统的安全性，请及时通过“修改用户口令”功能修改该口令。

### 删除操作员

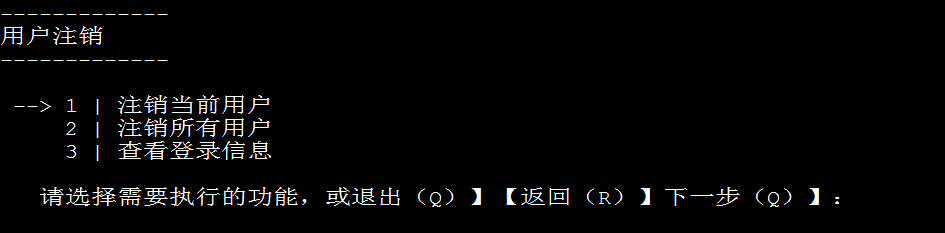
在“权限管理”中选择“删除操作员”功能，即可完成操作员删除。



<!>安全提示：如果出现操作员IC卡丢失的情况，为保证安全性，可通过“删除操作员”及“增加操作员”功能更新操作员。

## 用户注销

在“权限管理”中有“用户注销”的选项，可以通过执行该功能释放管理员或操作员权限。



<!>安全提示：在完成管理操作后，建议及时注销管理员，仅保留操作员登录状态即可正常使用密码卡的密码运算功能。

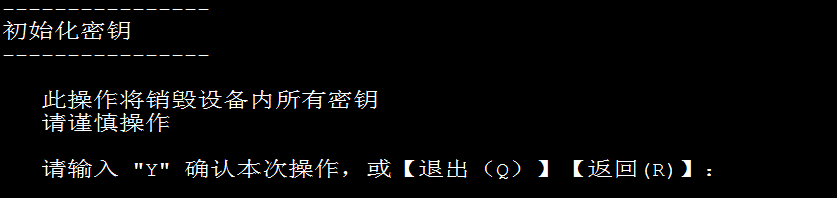
## 查看权限设置表

为方便使用，可以查看各项管理操作所需要的权限对应表。详细的权限表参考“附录 权限设置表”部分。

# 密钥管理

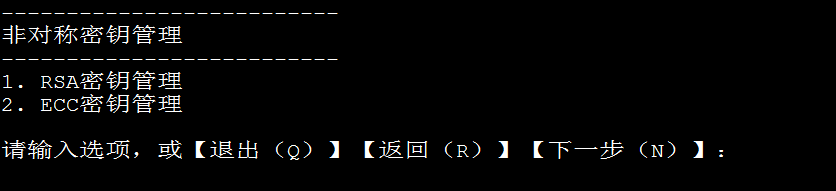
## 密钥初始化

该操作会销毁密码卡设备内的所有密钥信息。



<!>安全提示：该功能不仅用于销毁密码卡内的所有密钥信息，还可以用于复位密码卡的初始状态。

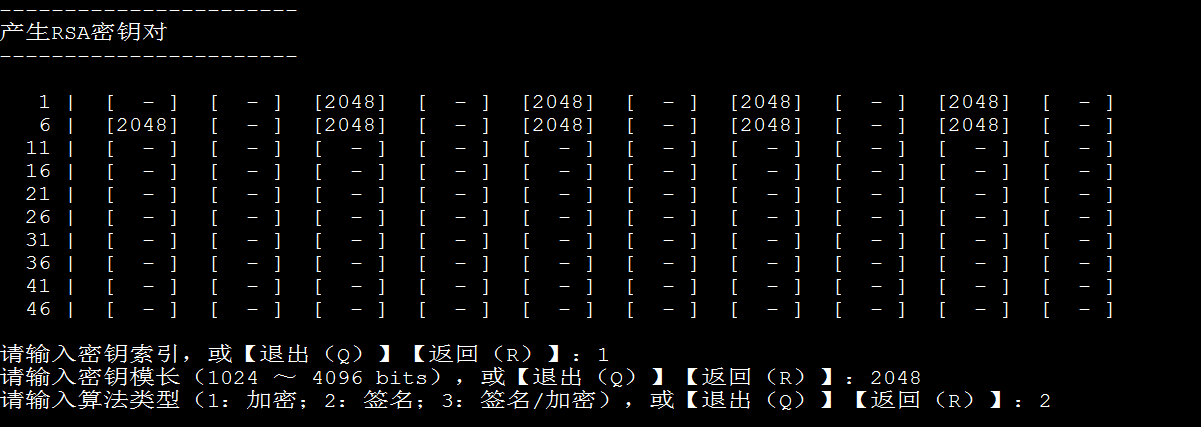
## 非对称密钥管理



### RSA密钥管理

#### 产生RSA密钥对

本密码卡支持双密钥体制，每个索引位置对应两对RSA密钥对，分别是签名密钥对和加密密钥对，签名密钥对主要用于数字签名，加密密钥对一般用于数字信封或保护会话密钥的安全。支持1024bit~4096bit的密钥模长的RSA密钥对生成。

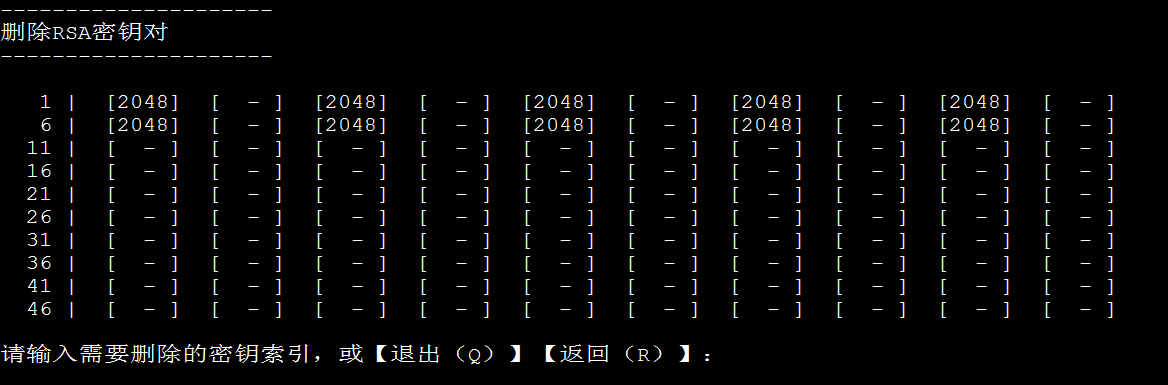


<!>提示：批量产生RSA密钥对的时候，可通过“索引n：索引m”指令来操作，例如，批量产生索引1到12的RSA密钥对，输入“1:12”即可批量产生该索引范围的RSA密钥对。

#### 删除RSA密钥对

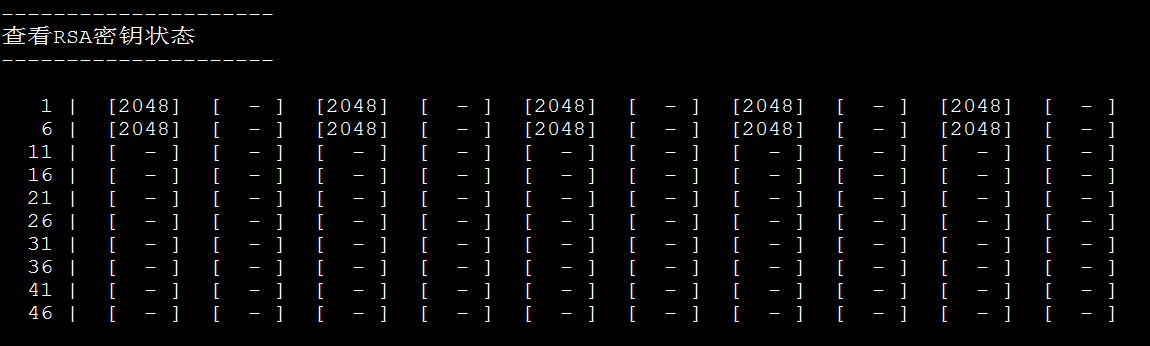
选择“删除RSA密钥对”即可删除指定密钥索引位置的RSA密钥对。

<!>提示：批量删除RSA密钥对的时候，通过“索引n：索引m”指令来操作，例如，批量删除索引1到5的RSA密钥对，输入“1:5”即可批量删除该索引范围的RSA密钥对。



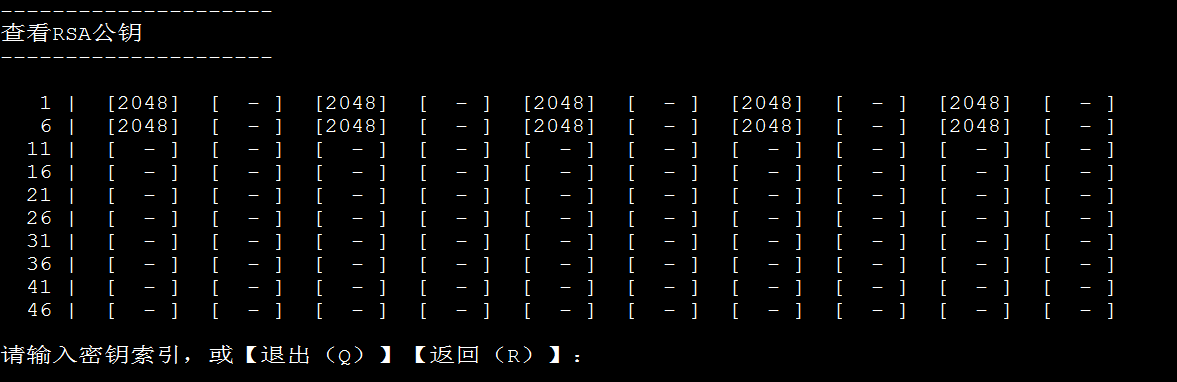
#### 查看RSA密钥状态

可通过选择“查看RSA密钥状态”来查看当前密码卡内已有的RSA密钥对。



#### 查看RSA公钥

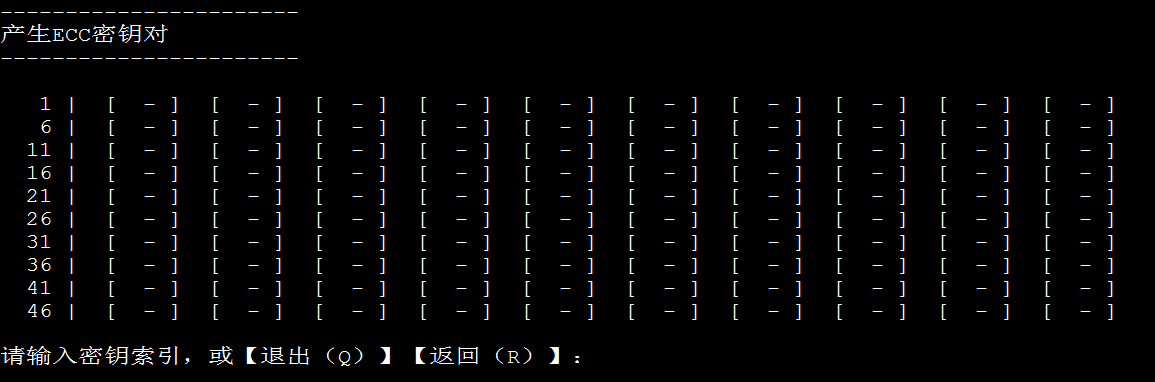
可通过选择“查看RSA公钥”来查看对应密钥对的签名和加密公钥。



### ECC密钥管理

#### 产生ECC密钥对

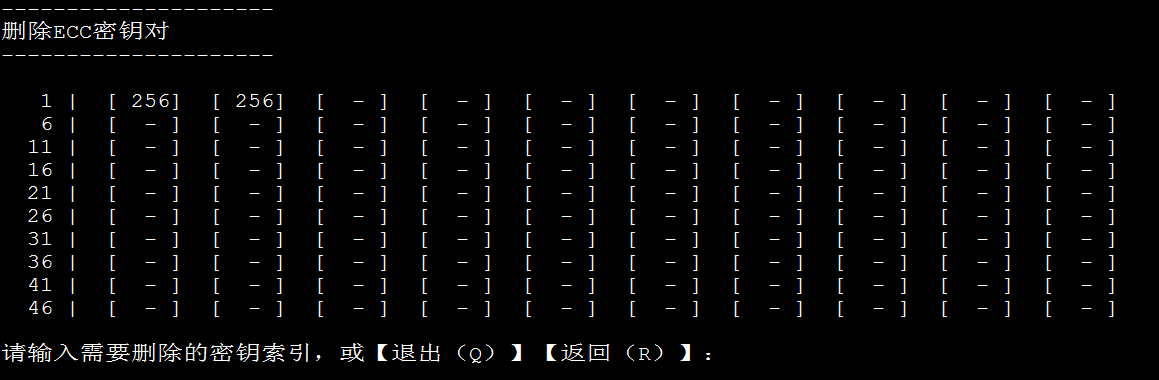
本密码卡支持双密钥体制，每个索引位置对应两对ECC密钥对，分别是签名密钥对和加密密钥对，签名密钥对主要用于数字签名，加密密钥对一般用于数字信封或保护会话密钥的安全。



<!>提示：批量产生ECC密钥对的时候，可通过“索引n：索引m”指令来操作，例如，批量产生索引1到12的ECC密钥对，输入“1:12”即可批量产生该索引范围的ECC密钥对。

#### 删除ECC密钥对

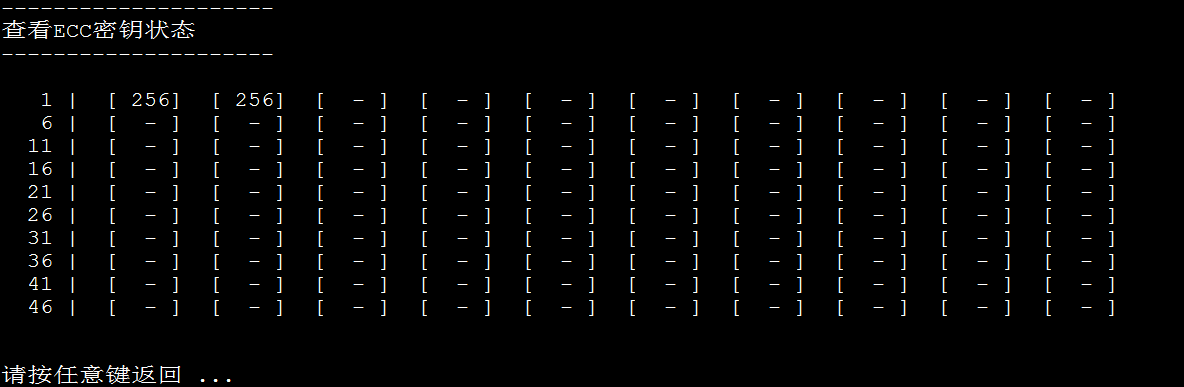
选择“删除ECC密钥对”即可删除指定密钥索引位置的ECC密钥对。



<!>提示：批量删除密钥对的时候，通过“索引n：索引m”指令来操作，例如，批量删除索引1到5的ECC密钥对，输入“1:5”即可批量删除该索引范围的ECC密钥对。

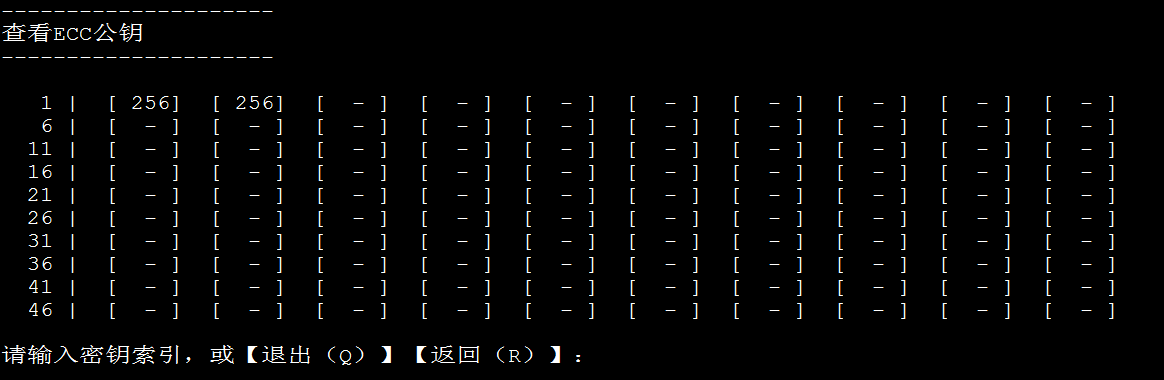
#### 查看ECC密钥状态

可通过选择“查看ECC密钥状态”来查看当前密码卡内已有的ECC密钥对。

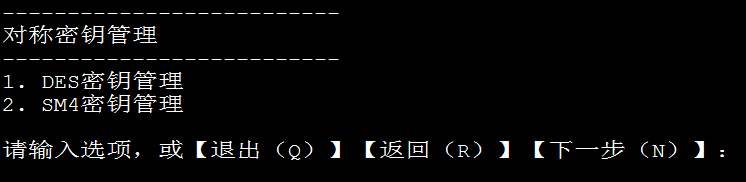


#### 查看ECC公钥

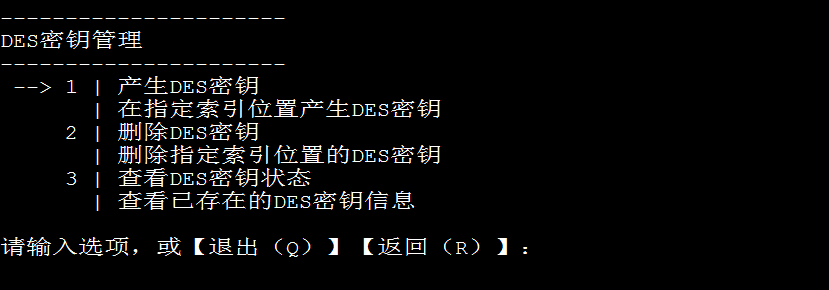
可通过选择“查看ECC公钥”来查看对应密钥对的签名和加密公钥。



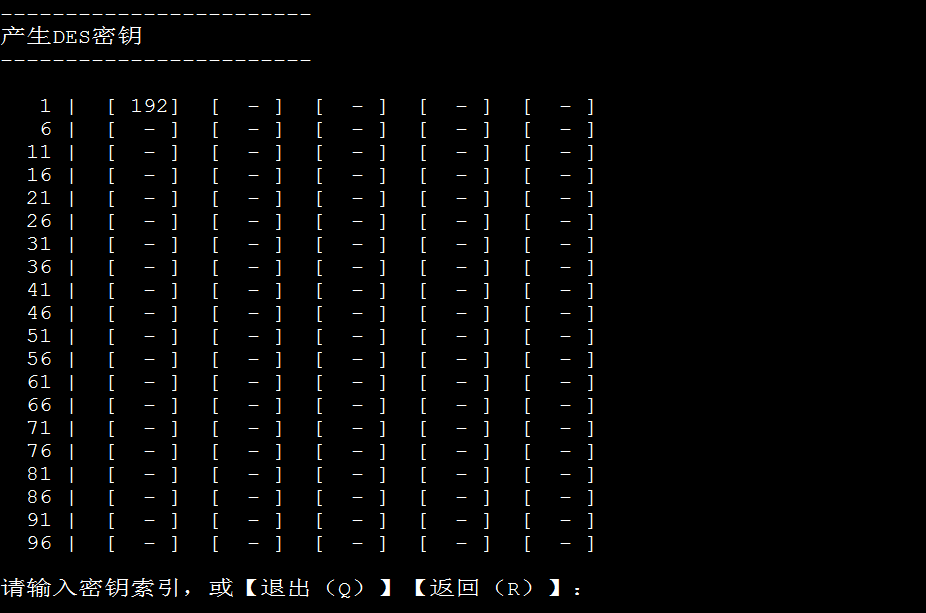
## 对称密钥管理



### DES密钥管理



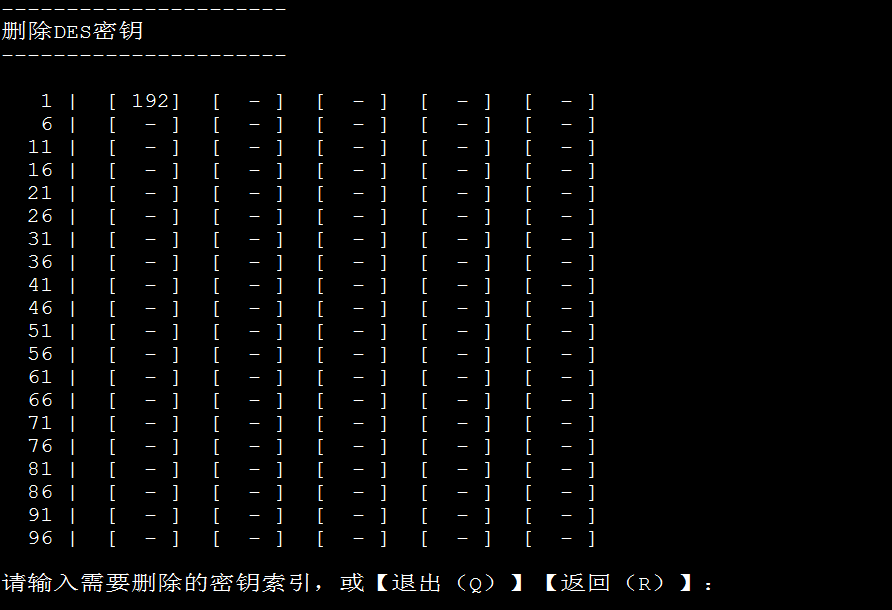
#### 产生DES密钥



<!>提示：批量产生DES密钥的时候，可通过“索引n：索引m”指令来操作，例如，批量产生索引1到12的DES密钥，输入“1:12”即可批量产生该索引范围的DES密钥。

#### 删除DES密钥

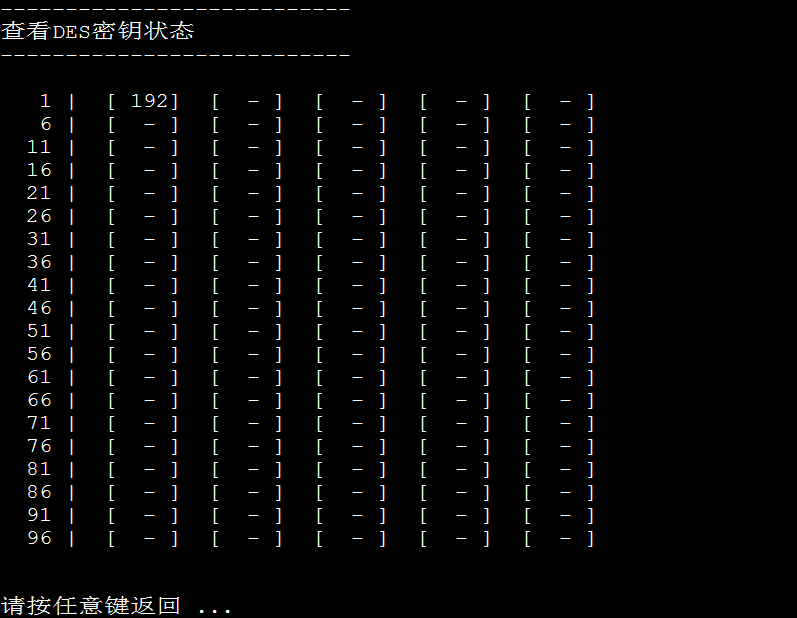
选择“删除DES密钥”即可删除指定密钥索引位置的DES密钥。



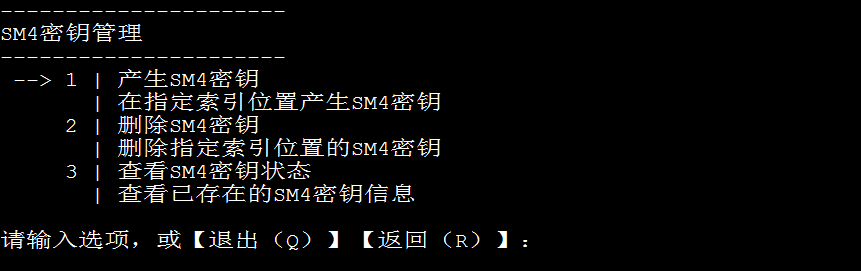
<!>提示：批量删除DES密钥的时候，通过“索引n：索引m”指令来操作，例如，批量删除索引1到5的DES密钥，输入“1:5”即可批量删除该索引范围的DES密钥。

#### 查看DES密钥状态

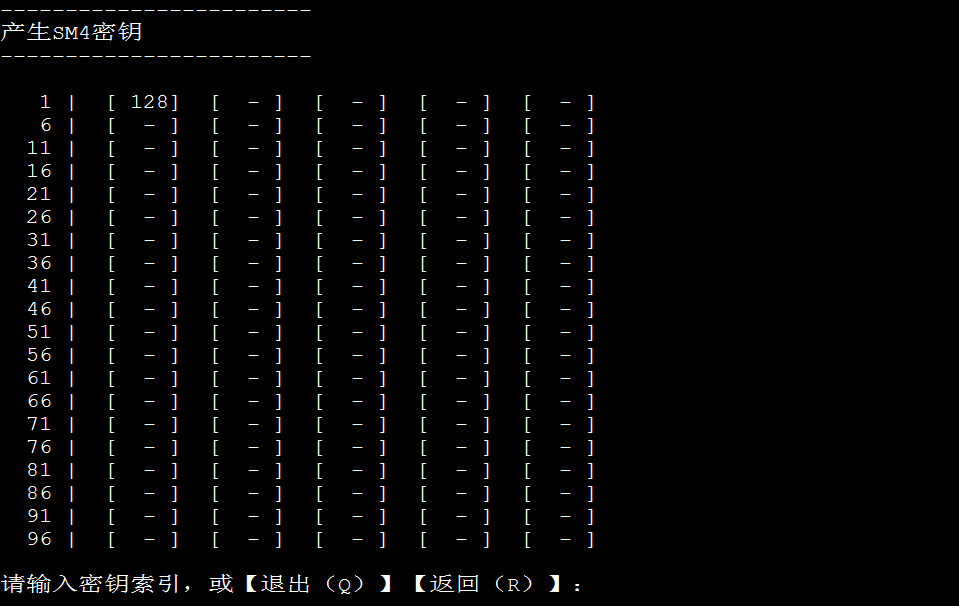
可通过选择“查看DES密钥状态”来查看当前密码卡内已有的DES密钥。



### SM4密钥管理



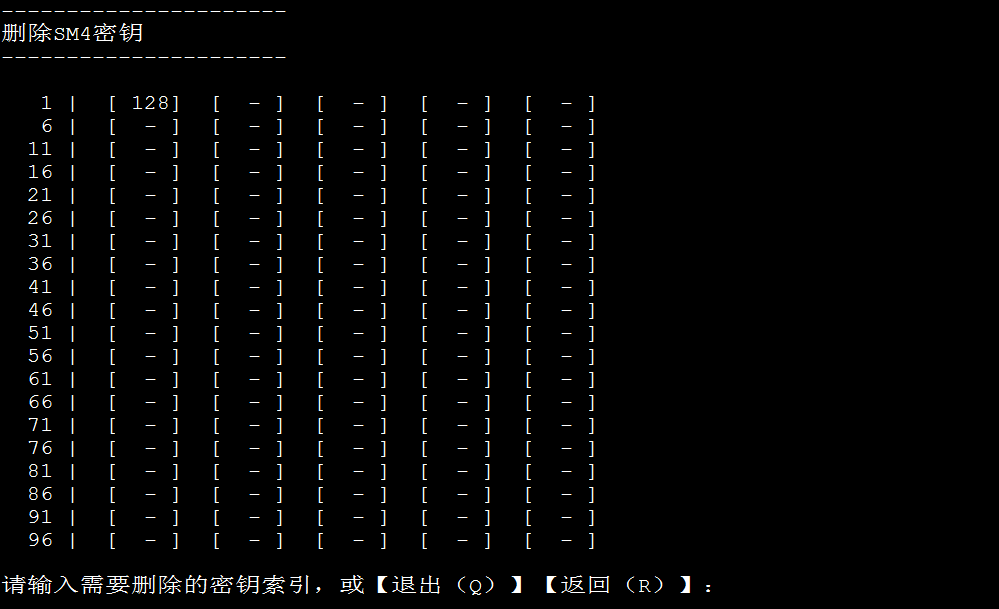
#### 产生SM4密钥



<!>提示：批量产生SM4密钥的时候，可通过“索引n：索引m”指令来操作，例如，批量产生索引1到12的SM4密钥，输入“1:12”即可批量产生该索引范围的SM4密钥。

#### 删除SM4密钥

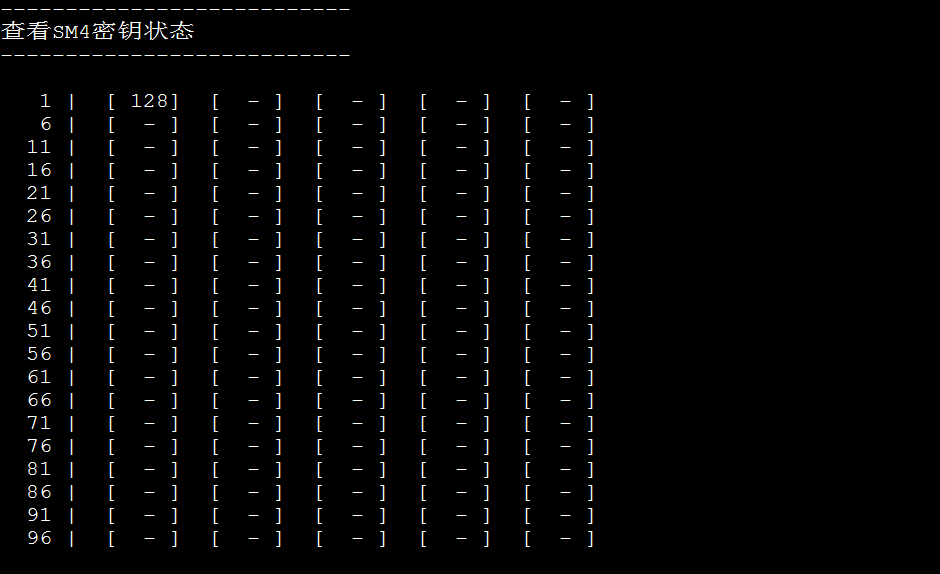
选择“删除SM4密钥”即可删除指定密钥索引位置的SM4密钥。



<!>提示：批量删除SM4密钥的时候，通过“索引n：索引m”指令来操作，例如，批量删除索引1到5的SM4密钥，输入“1:5”即可批量删除该索引范围的SM4密钥。

#### 查看SM4密钥状态

可通过选择“查看SM4密钥状态”来查看当前密码卡内已有的SM4密钥。



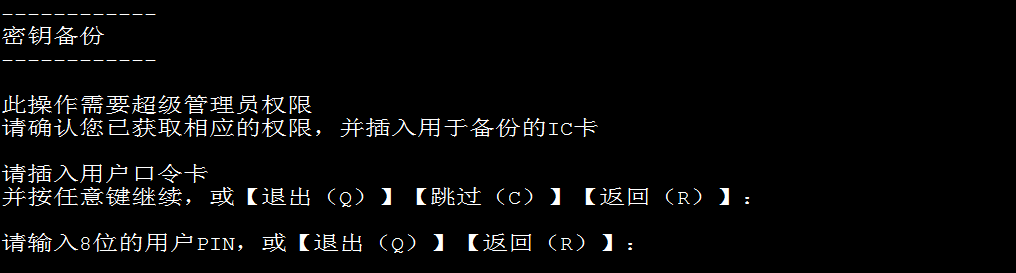
## 密钥备份恢复

### 密钥备份

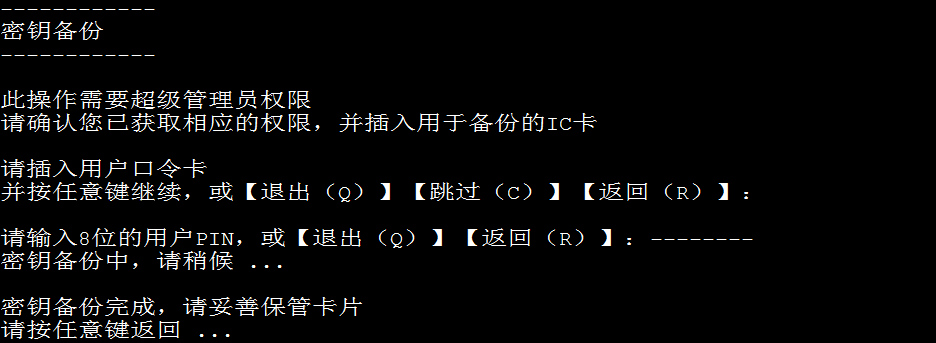
选择“密钥备份”功能后，可对密码卡已有的非对称密钥对、对称密钥保存于备份IC卡中。其中非对称密钥对的私钥、对称密钥是以密文的方式保存到备份IC卡的文件中。具体步骤如下：

a)登录半数以上的管理员，获得超级管理员权限。

b)根据卡片标示的方向插入备份IC卡并输入IC卡保护口令（PIN）。



c)完成该备份功能后拔出备份IC卡，按任意键退出。



<!>安全提示：备份IC卡和管理员IC卡一定要妥善保管。

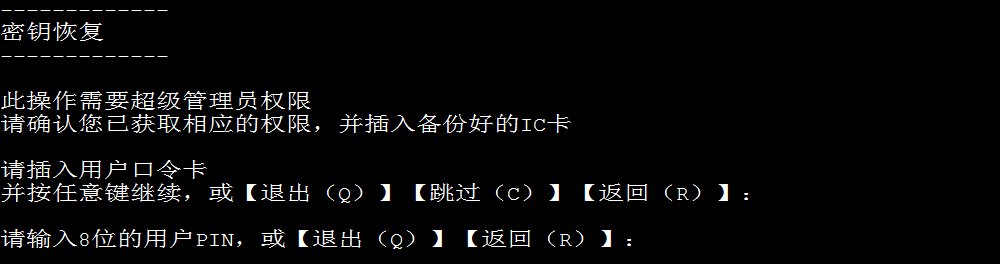
<!>提示：备份过程时间稍长，请耐心等待。

### 密钥恢复

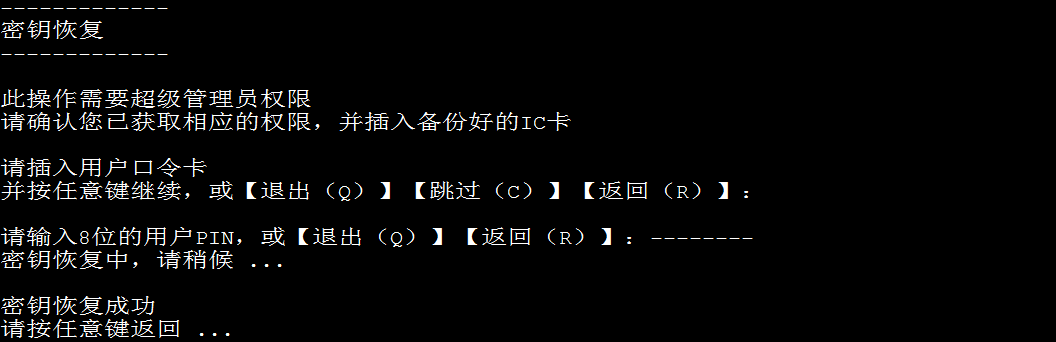
选择“密钥恢复”功能后，可将备份IC卡中备份的RSA密钥对和对称密钥恢复到密码卡中安全存储。具体步骤如下：

a)登录半数以上的管理员，获得超级管理员权限。

b)根据卡片标示的方向插入备份IC卡并输入IC卡保护口令（PIN）。



c)完成该恢复功能后拔出备份IC卡，按任意键退出。



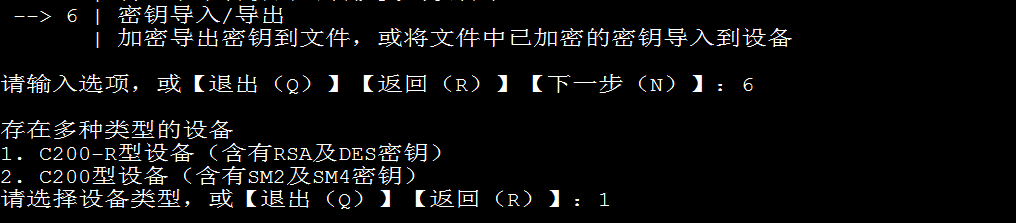
<!>安全提示：密钥恢复过程会破坏当前密码卡内的密钥信息，请确定当前密钥是否继续使用，再决定是否恢复到当前密码卡。

<!>提示：备份IC卡只可执行3次密钥恢复操作，若操作限定恢复次数，请重新执行密钥备份操作。

<!>提示：恢复过程时间稍长，请耐心等待。

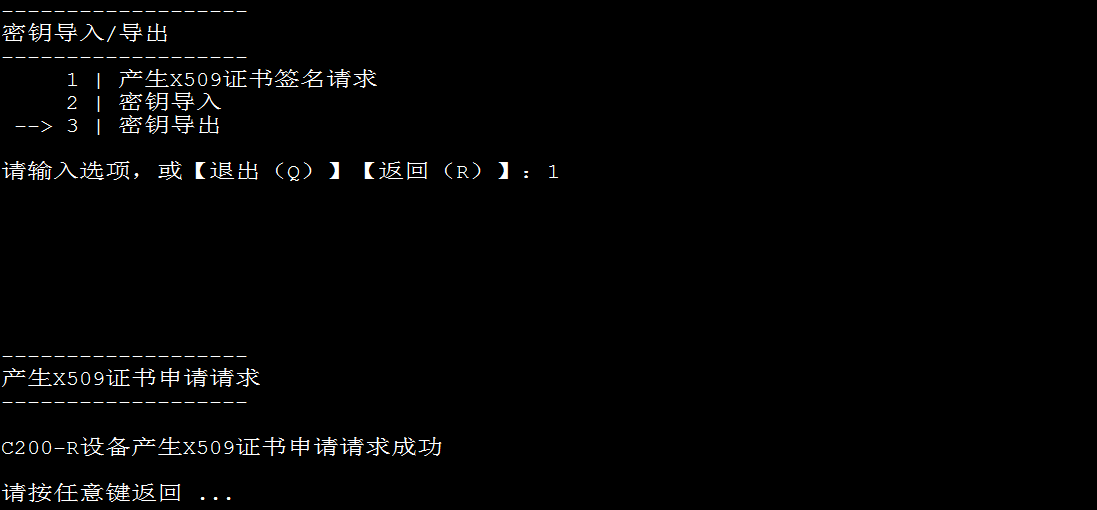
## 密钥导入导出

选择“密钥导入/导出”功能后，可实现两个不同的密码卡之间进行全部密钥或指定索引非对称密钥对、对称密钥之间安全的导入或导出。以下说明以存在两种密码卡为前提，假定密码机A导出C200系列设备密钥至密码机B。

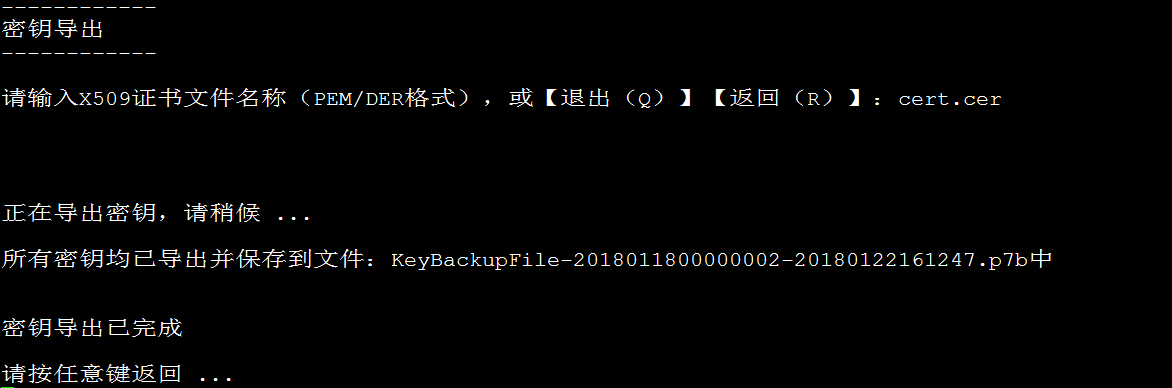


### 密钥导出

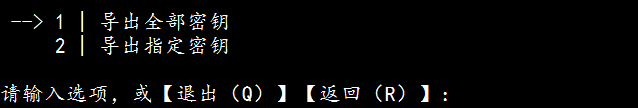
a)密码机B获取当前权限为超级管理员权限后，进入“密钥导入导出”功能，按照提示选择“1 | 生成x509证书申请”，将本地生成的p10请求KeyBackupFile\_r.p10发送至证书服务器生成x509数字证书，最后将数字证书传输到密码机A中。



b)密码机A获取当前权限为超级管理员权限后，按照提示选择“3 | 密钥导出”。



c)可根据需求选择导出全部或者指定索引位置的非对称密钥对和对称密钥。当选择指定索引位置的密钥导出时，依次输入各种类型密钥需导出的密钥索引；如需跳过该种类密钥的导出，直接输入回车键即可。

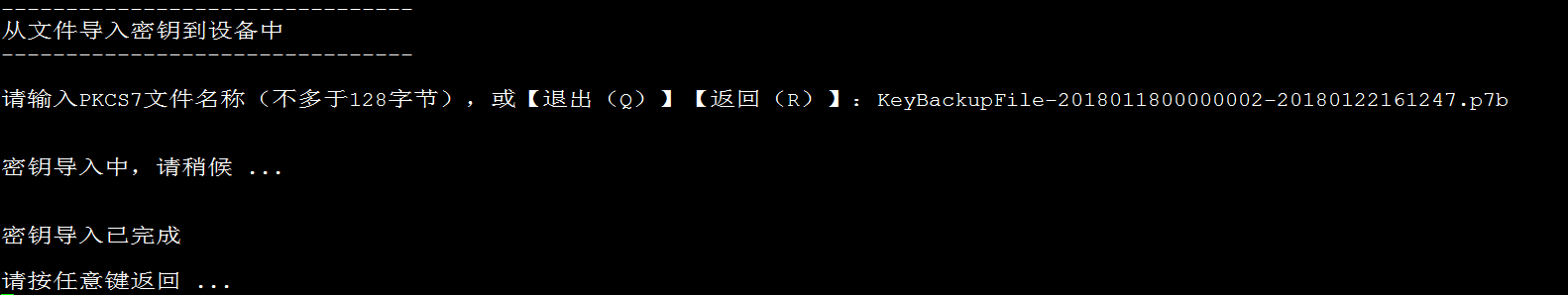


d)导出的密钥是以文件的形式保存在密码机A本地主机上，文件名为：KeyBackupFile-SN-yyyymmdd.p7b，其中SN为C200系列设备的设备序列号，yyyy为年，mm为月，dd为日期；文件路径为当前目录下，将KeyBackupFile-SN-yyyymmdd.p7b文件传输至密码机B中，完成密钥导出操作。

### 密钥导入

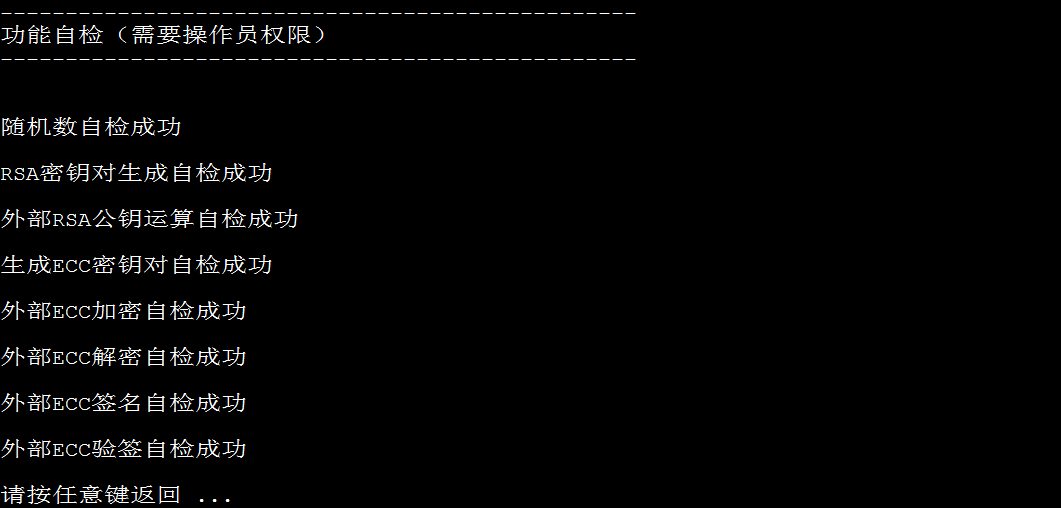
a)密码机B获取当前权限为超级管理员权限后，进入“密钥导入/导出”功能，按照提示选择“2 | 密钥导入”。

b)输入将要导入的pkcs7数字信封文件名，按“Enter”键执行导入操作。



# 功能自检

通过选择“功能自检”功能，可以检测密码卡随机数、算法功能是否正常。



<!>提示：使用“功能自检”功能，需获得操作员权限。

# 文件管理

## 查看文件状态

通过选择“查看文件状态”功能，可以查看当前所有已创建文件的名字和大小。

## 创建文件

通过选择“创建文件”功能，可创建最大8192字节大小的文件。

<!>提示：至多可创建3个文件，每个文件大小最大为8192字节。

## 写文件

进入选择“写文件”功能，选择将要操作的文件索引和起始位置，写入数据至对应索引文件中。

<!>提示：可通过文件输入方式写入至密码卡文件中，输入的文件需放在管理工具同一路径下。

## 读文件

进入选择“读文件”功能，选择文件索引和起始位置，读出索引文件中存储的数据。

<!>提示：读取文件中的数据将以生成文件的方式保存在管理工具同一路径下，名字为File\_xxxx(年)\_xx(月)\_xx(日)。

## 删除文件

通过选择“删除文件”功能，可删除相关文件索引的文件及数据。

# 附录 A

## 常见问题

1.如何判断密码卡功能是否正常

上电后，密码卡首先是红灯亮，装载驱动后，绿灯紧跟着亮，属于密码卡上电自检通过。

2.开机后密码运算功能无法正常进行

a)检查是否成功加载驱动；

b)检查开机时是否插入正确的操作员IC卡；

c)检查是否生成或导入密钥。

3.无法进行备份/恢复操作

a)检查是否是成功注册3张或以上管理员；

b)检查当前权限是否为超级管理员；

c)恢复操作时，备份IC卡至多可执行恢复3次操作，超过3次需重新进行备份操作。

# 附录 B

## 权限设置表

| **管理类别** | **操作项** | **所需权限** |
| --- | --- | --- |
| 设备管理 | 查看设备基本信息 | 无权限 |
| 权限管理 | 查看登录状态 | 无权限 |
| 查看权限设置表 | 无权限 |
| 增加管理员 | 超级管理员权限 |
| 删除管理员 | 超级管理员权限 |
| 增加操作员 | 超级管理员权限 |
| 删除操作员 | 超级管理员权限 |
| 密钥管理 | 查看ECC密钥对状态 | 无权限 |
| 查看RSA密钥对状态 | 无权限 |
| 查看ECC公钥 | 操作员权限 |
| 查看RSA公钥 | 操作员权限 |
| 生成ECC密钥对 | 管理员权限 |
| 生成RSA密钥对 | 管理员权限 |
| 删除ECC密钥对 | 管理员权限 |
| 删除RSA密钥对 | 管理员权限 |
| 导入ECC密钥对 | 管理员权限 |
| 查看DES密钥状态 | 无权限 |
| 查看SM4密钥状态 | 无权限 |
| 生成DES密钥 | 管理员权限 |
| 生成SM4密钥 | 管理员权限 |
| 删除DES密钥 | 管理员权限 |
| 删除SM4密钥 | 管理员权限 |
| 密码运算 | RSA/ECC运算、DES/TDES/SM4运算 | 操作员权限 |
| 备份恢复 | 密钥备份 | 超级管理员权限，前提是成功增加3张管理员 |
| 密钥恢复 | 超级管理员权限，前提是成功增加3张管理员 |
| 导入导出 | 密钥导入 | 超级管理员权限，前提是成功增加3张管理员 |
| 密钥导出 | 超级管理员权限，前提是成功增加3张管理员 |
| 文件管理 | 文件创建 | 无权限 |
| 文件删除 | 无权限 |
| 文件读取 | 无权限 |
| 文件写入 | 无权限 |

# 附录 C

## 错误码定义

|  |  |
| --- | --- |
| 错误码 | 说明描述 |
| 0x0 | 操作成功 |
| 0x0000D001 | C200设备硬件上电自检错误 |
| 0x0000D002 | C200设备未成功验证私访码 |
| 0x0000D003 | C200设备无权限 |
| 0x0000D004 | C200设备索引不在范围错误 |
| 0x0000D005 | C200设备无私钥访问控制码 |
| 0x0000D006 | C200设备无用户密钥对或密钥加密密钥 |
| 0x0000D008 | C200设备不支持的命令类型 |
| 0x0000D009 | C200设备硬件超时 |
| 0x0000D900 | C200-R设备密码卡内部设备打开失败 |
| 0x0000D982 | C200-R设备无权限 |
| 0x0000DA83 | C200-R设备无密钥 |
| 0x0000DA84 | C200-R设备密码卡内部缓存不足 |
| 0x0000DA86 | C200-R设备索引错误 |
| 0x0000DA81 | C200-R设备密码卡内部功能不支持 |
| 0x0000DB00 | C200-R设备密码卡内部算法功能不支持 |
| 0x0000DD00 | C200-R设备密码卡接收的命令不支持 |
| 0x0000D700 | C200-R设备密码卡接收的长度错误 |
| 0x0000DF0F | C200-R设备密码卡硬件自检错误 |
| 0x01000001 | 未知错误 |
| 0x01000002 | 不支持的接口调用 |
| 0x01000003 | 与设备通信失败 |
| 0x01000004 | 运算模块无响应 |
| 0x01000005 | 打开设备失败 |
| 0x01000006 | 创建会话失败 |
| 0x01000007 | 无私钥使用权限 |
| 0x01000008 | 不存在的密钥调用 |
| 0x01000009 | 不支持的算法调用 |
| 0x0100000A | 不支持的算法模式调用 |
| 0x0100000B | 公钥运算失败 |
| 0x0100000C | 私钥运算失败 |
| 0x0100000D | 签名运算失败 |
| 0x0100000E | 验证签名失败 |
| 0x0100000F | 对称算法运算失败 |
| 0x01000010 | 多步运算步骤错误 |
| 0x01000011 | 文件长度超出限制 |
| 0x01000012 | 指定的文件不存在 |
| 0x01000013 | 文件起始位置错误 |
| 0x01000014 | 密钥类型错误 |
| 0x01000015 | 密钥错误 |
| 0x01000016 | 加密数据错误 |
| 0x02000001 | 非法句柄 |
| 0x02000002 | 内存不足 |
| 0x02000003 | 产生随机数错误 |
| 0x02000004 | 验证私钥访问码失败 |
| 0x02000005 | 计算MAC失败 |
| 0x02000006 | 指定文件已经存在 |
| 0x02000007 | 写文件失败 |
| 0x02000008 | 没有足够的空间 |
| 0x02000009 | 输入参数错误 |
| 0x0200000A | 输出参数错误 |
| 0x02001003 | 硬件返回数据错误 |
| 0x02001004 | 数据长度错误 |
| 0x02001005 | 超时错误 |
| 0x02001006 | 进程锁错误 |
| 0x02001007 | 无可用设备 |
| 其它 | 预留 |