



得安密码卡密钥管理 程序 V2.0

操作手册

版权©2006 Datech

版权所有

得安密码卡密钥管理程序 V2.0 操作手册

本版发行日期：2006 年 9 月

本出版物的内容将做不定期性的变动，且不另行通知。更改的内容将会不补充到本出版物。且会在本指南发行新版本时予以付梓印刷。本公司不做任何明示或默许担保，其中包括本使用手册的内容的适售性或符合特定使用目的的默许担保。

本公司依中华人民共和国著作权法，享有及保留一切著作之专属权力，未经济南得安计算机有限公司事先书面同意，不得就本手册有增删、改编、翻印、改造或仿制的行为。

用户指南

为了帮助您更方便的使用密码卡加密系统 ,我们设计了这套得安密码卡密钥管理程序 V2.0 操作手册 ,这份操作手册向您详细介绍了密码卡密钥管理程序 V2.0 的使用 ,请仔细阅读。

要了解更多关于我们的产品 , 服务和支持信息 , 请访问我们的网站
<http://www.datech.com.cn/>

得安密码卡密钥管理程序 V2.0 操作手册

正式使用密码卡加密系统进行各类运算各项业务之前首先要对密码卡做一些必要的设置和管理，为密码卡的运行准备好必备的属性。

对 IC 卡控制类型的密码卡来说，此过程尤为重要，密码卡的加密系统采用了严格的密钥管理机制，保证密码卡在运作过程中的安全性，要认真严密的通过密钥管理软件完成各项管理控制工作；

对 IC 卡无访问控制类型的加密系统来说，此过程可以省略，只要在初次使用前对卡进行彻底的初始化即可。

下面详细介绍 IC 卡控制类型加密系统在 WINDOWS 环境下的控制管理。

下面就得安密码卡密钥管理程序 V2.0 对一代卡与三代卡的操作
作一下详细说明：

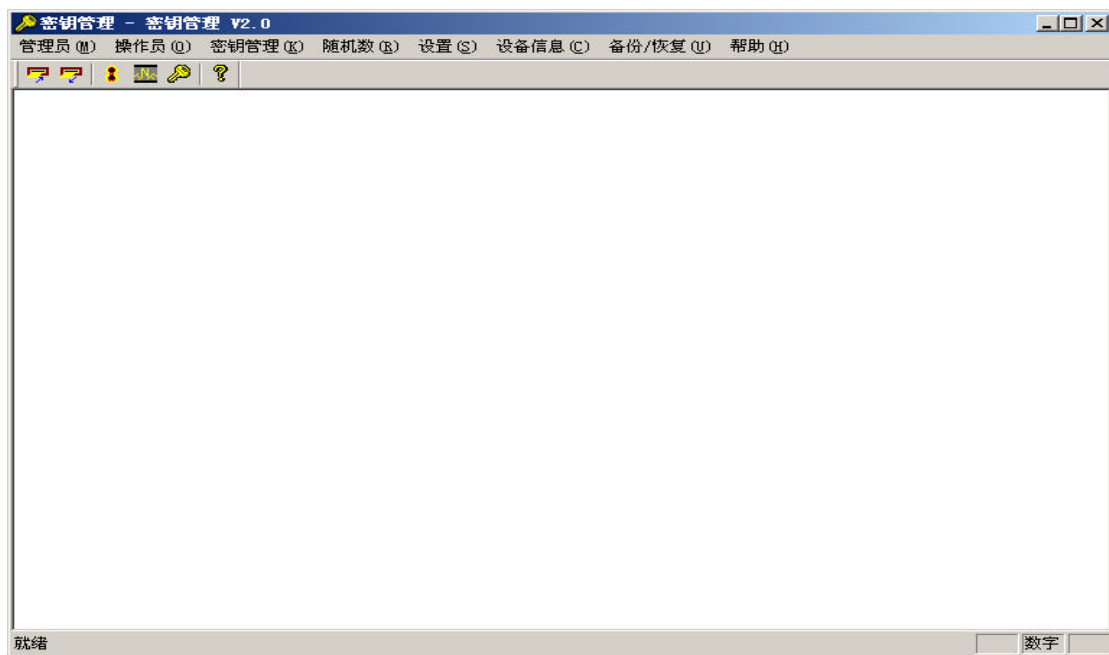
一代卡：

启动密钥管理软件

正确安装密钥管理软件后，点击 开始->程序->得安密码卡密钥管理程序->得安密码卡密钥管理程序 V2.0.exe，启动密钥管理程序。如下显示：

密码卡信息

未对管理员设置前：

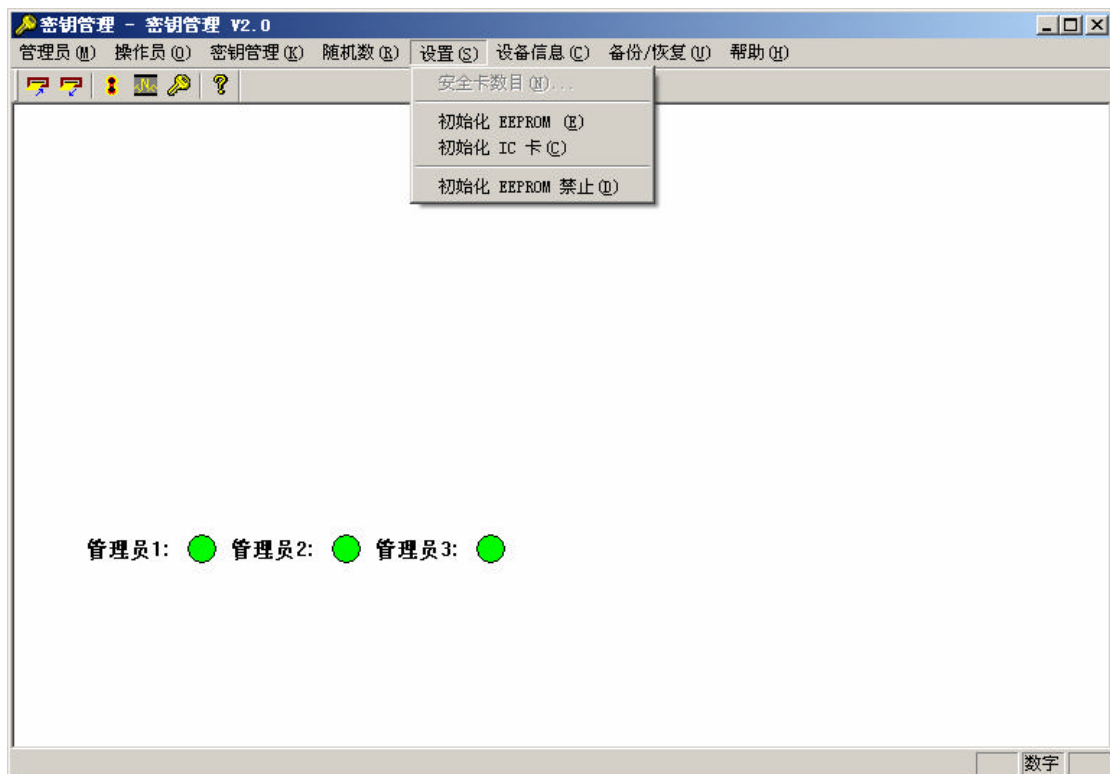


对管理员设置后：



设置

选中“设置”标签项：



本标签项中包含

- ◆ 安全卡数目（一代卡不支持此功能）；
- ◆ 初始化 EEPROM；
- ◆ 初始化 IC 卡；
- ◆ 初始化 EEPROM 禁止（**注意**）。

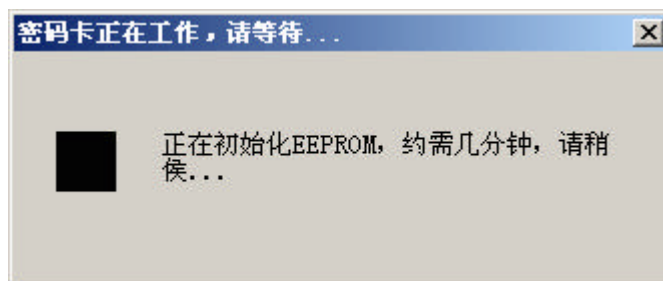
初始化 EEPROM

一块新的密码卡内的 EEPROM 中的内容是不确定的，应该首先对密码卡进行初始化 EEPROM 操作，以保证密码卡内为确定的空状态。

1. 点击选项“初始化 EEPROM”，出现以下信息：



2. 根据需要点击“取消”则取消此次操作，或点击“确定”则出现以下信息：



3. 等待几分钟后出现以下信息：



4. 点击“确定”，初始化 EEPROM 成功。



说明：

- 完成 EEPROM 初始化操作，密码卡内所有信息将被清空，需要重

新进行管理员初始化等操作及密钥设置；EEPROM 的初始化操作并不会影响到基础配置程序所设置的内容。



注意：

- 此项操作一旦执行则会丢失密码卡内所有信息，在正常使用过程中不允许执行此操作；所以对于此项操作，必须由专业维护人员或厂商技术支持人员完成。

初始化 IC 卡

此功能彻底清除 IC 卡上的所有内容。

1. 点击选项“初始化 IC 卡”，出现以下信息：



2. 插入要初始化的 IC 卡，根据需要点击“取消”则取消此次操作，或点击“确定”则几秒钟后出现以下信息：



3. 点击“确定”，初始化 IC 卡成功。

初始化 EEPROM 禁止

注意：请千万不要点击此选项，否则会带来不可估量的损失，后果自负。

管理员

选中“管理员”标签项：



本标签项中包含了对管理员口令 IC 卡的操作：

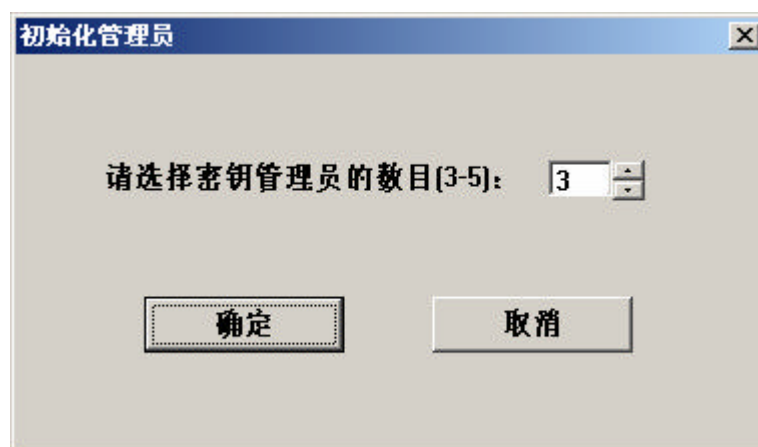
- ◆ 管理员登录：识别验证管理员口令 IC 卡的身份信息；
- ◆ 管理员退出：管理员全部退出；
- ◆ 初始化管理员：设置管理员口令 IC 卡；
- ◆ 增加管理员：增加一个管理员；
- ◆ 删除管理员：删除一个管理员；
- ◆ 备份管理员口令：备份一个管理员的口令；
- ◆ 修改管理员口令：修改一个管理员的口令；
- ◆ 退出：退出程序，管理员退出登录。

初始化管理员

一张新的密码卡初始化之后是没有管理员的，对于 IC 卡控制类型的密码卡此时

应认真设置好它的管理员，才能进一步应用密码卡。

1. 点击选项“初始化管理员”，出现对话框：



2. 请选择您要初始化的管理员的数量，3~5 个，然后点击“确定”：



按照提示，向读卡器中插入将要作为 1 号管理员口令卡的 IC 卡，然后点击“确定”键后重复以上过程。



说明：

- 本步骤将会根据所输入的管理员的数量 n 重复执行 n 次，即把所初始化的管理员口令依次输出到 IC 卡。

3. 初始化管理员成功，完成此操作。



注意：

- 本初始化操作所生成的管理员口令卡对以后密码卡管理非常重要，

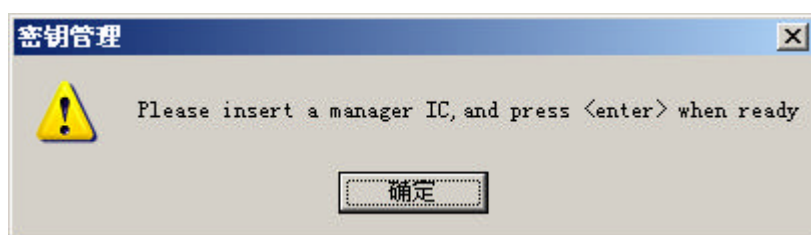
所以需要妥善保管。

- 本初始化操作只能在密码卡初始化之后进行，且不可重复，若要改动，请通过增加、删除管理员的方式完成。

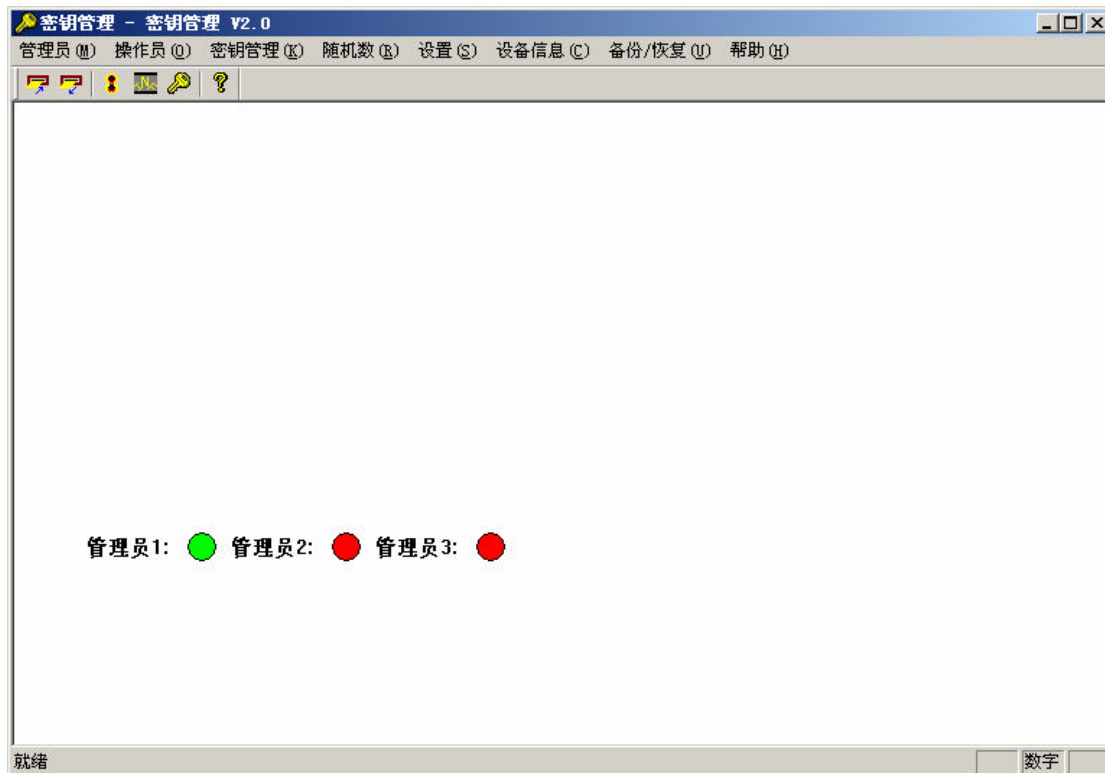
管理员登录

对密码卡的大部分管理操作需要满足管理权限，即半数以上的管理员成功登录方可进行。

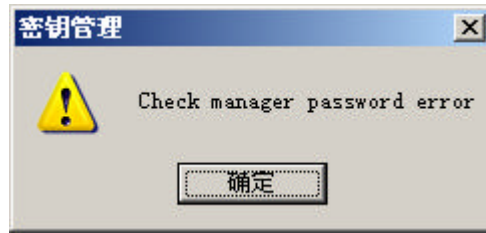
点击选项“管理员登录”，出现提示信息：



按照提示，将管理员口令 IC 卡插入读卡器中，然后点击确定，密码卡识别验证后返回此次操作结果，成功则显示（相应管理员标识由红变绿）：



错误则将显示：



管理员退出

管理员在完成相应的管理职责之后应及时退出登录 ,以防止他人越权误操作或恶意破坏。

点击选项“管理员退出”后，出现管理员退出登录成功信息：



增加管理员

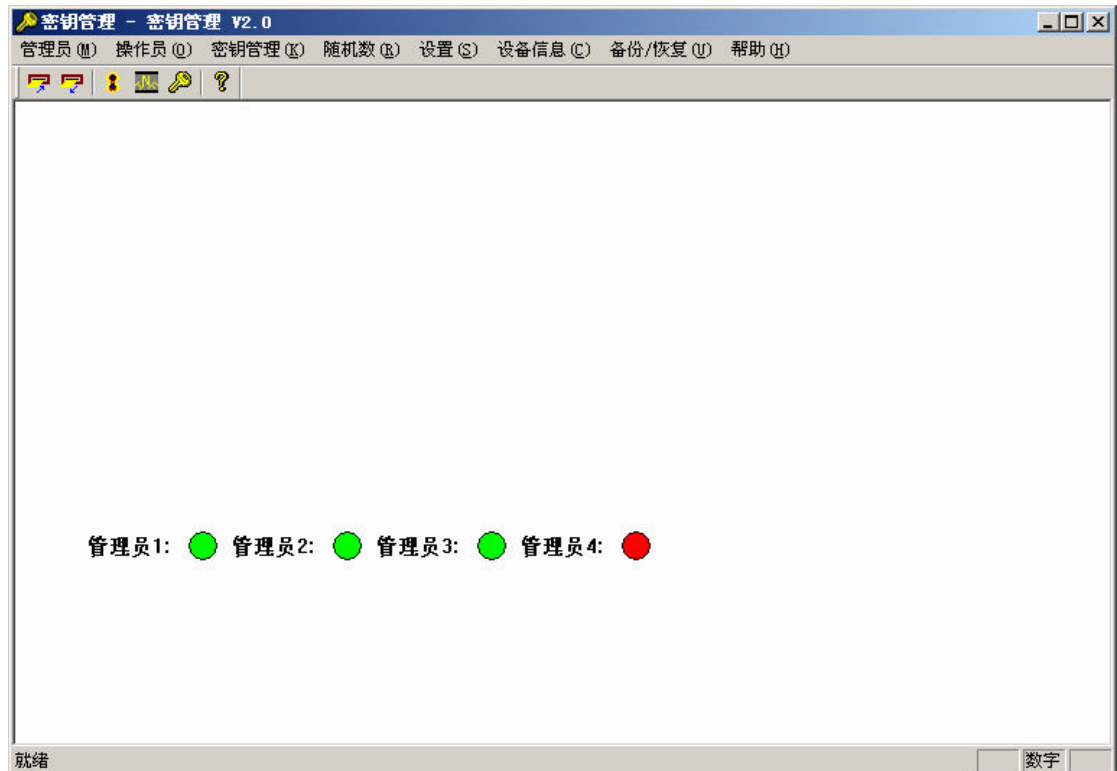
点击选项“增加管理员”，出现如下对话框：

A screenshot of a Windows-style dialog box titled '增加管理员' (Add Administrator). The main text area contains the prompt '请输入需要增加的密钥管理员号(1-5):' followed by a text input field containing the number '4'. At the bottom, there are two buttons: '确定' (OK) on the left and '取消' (Cancel) on the right.

请输入将要增加的管理员号码（1-5），然后点击确定：



向读卡器中插入作为新增管理员口令卡的 IC 卡 ,然后点击“ 确定 ”,成功则弹出 :



说明 :

- 此操作需满足管理权限。
- 增加一个已存在的管理员号码或者管理员数目已经最大 (5 个) 时 , 此操作将错误返回。

删除管理员

点击选项“删除管理员”，出现如下对话框：



输入将要删除的管理员号码，然后点击“确定”，成功则弹出：

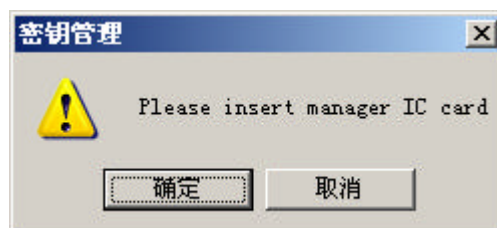


说明：

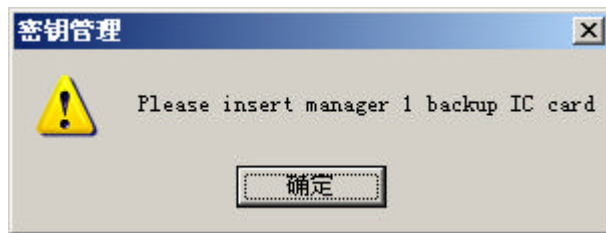
- ☐ 此操作需要满足管理权限。
- ☐ 删除一个不存在的管理员号码时，此操作将错误返回。（另附：密码卡管理员数目等于 3 个时就不能再删除。）

备份管理员口令

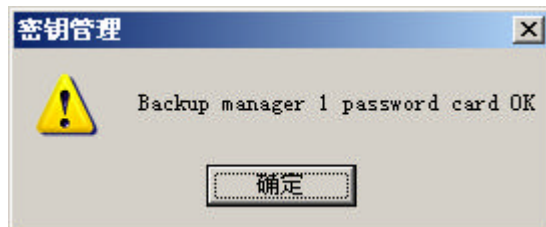
点击选项“备份管理员口令”，出现如下提示：



任意插入一张管理员口令卡后，点击确定：



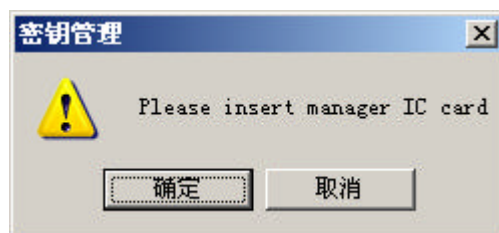
插入一张 IC 卡后，点击确定：



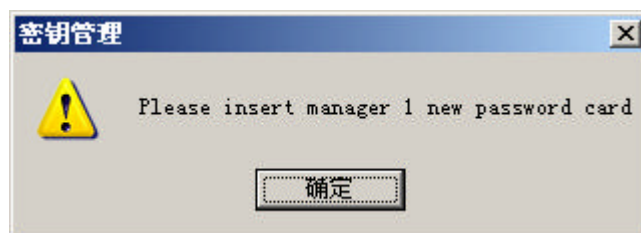
备份管理员口令完成。

修改管理员口令

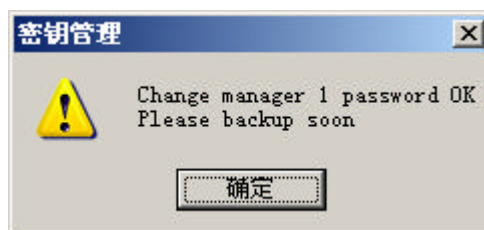
点击选项“修改管理员口令”，出现如下提示：



任意插入一张管理员口令卡后，点击确定：



插入一张 IC 卡后，点击确定：



修改管理员口令完成。

退出

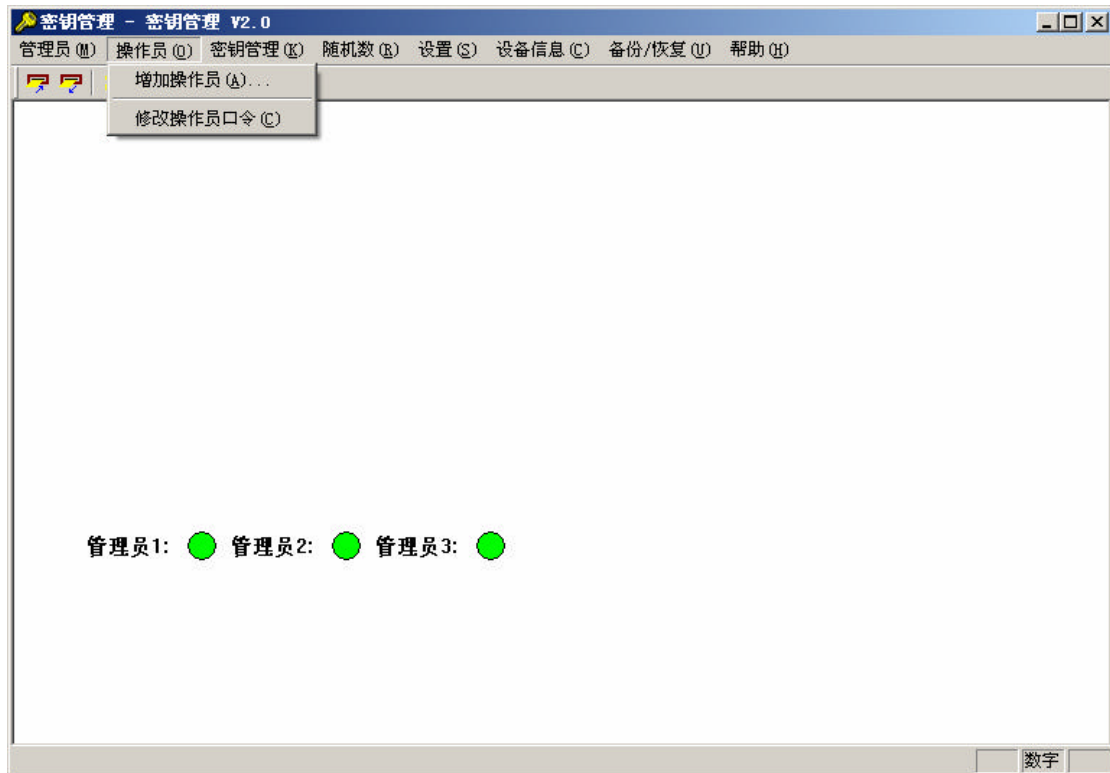
点击选项“退出”，出现如下提示：



管理员退出登录，密钥管理程序关闭。

操作员

选中“操作员”标签项：



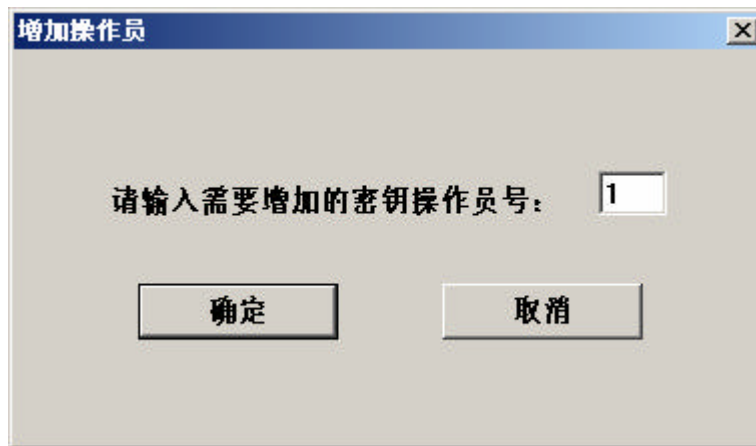
本标签项中包含了对操作员的以下操作：

- ◆ 增加操作员： 增加一个操作员；
- ◆ 修改操作员口令：操作员口令更换。

增加操作员

密码卡更新操作员口令后无操作员，此时需要添加操作员，还有就是密码卡可能要授予更多的人操作权限，此时也需要添加操作员，密码卡最多可以添加 10 个操作员。

点击选项“增加操作员”，系统弹出：



点击确定，出现如下信息：



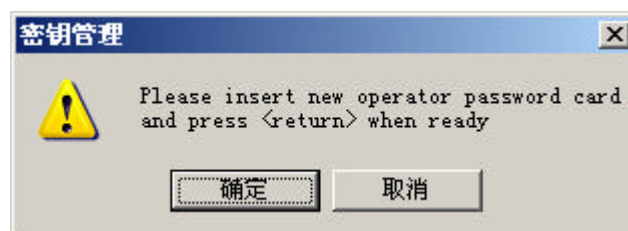
按照提示，向读卡器中插入将要添加的操作员口令 IC 卡，然后点击“确定”，系统返回相应的操作信息：



增加一操作员成功，此 IC 卡应有某操作员妥善保管好，需要时行使相应的职责。

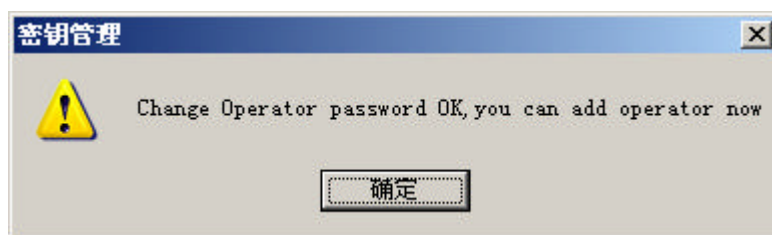
修改操作员口令

点击按钮“修改操作员口令”，弹出：



然后根据需求，点击“确定”执行此操作或“取消”撤销此次选择。

向读卡器中插入操作员口令 IC 卡点击确定后，出现如下信息：

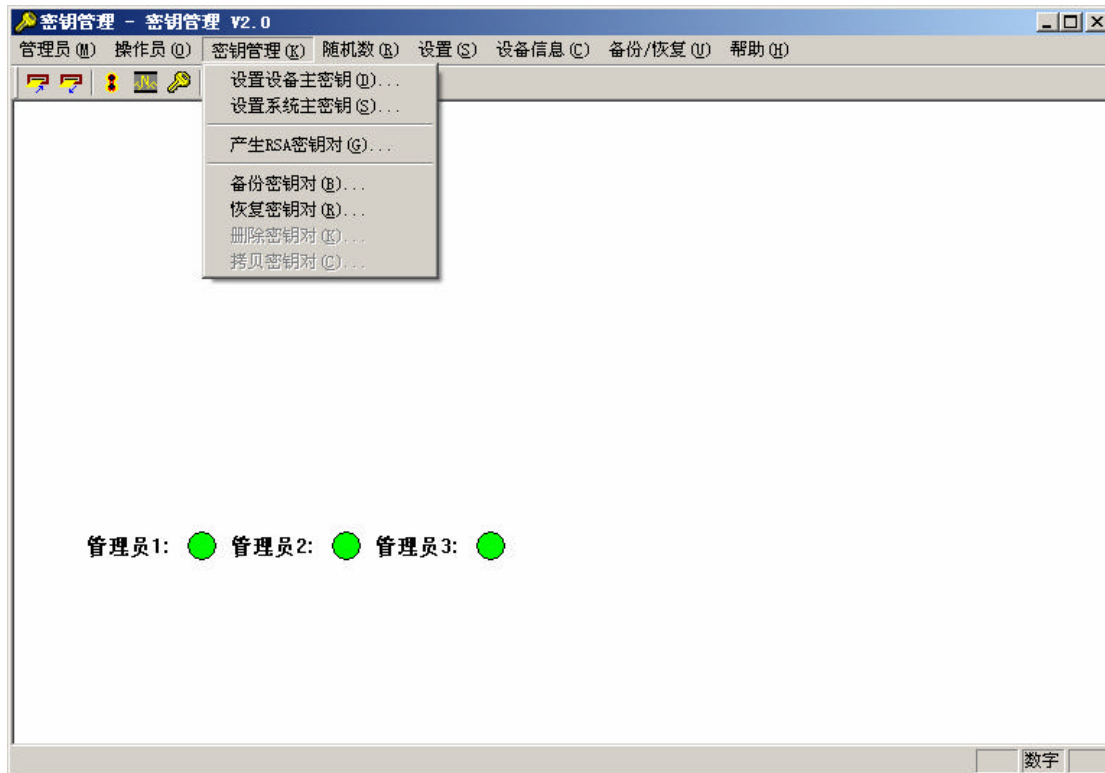


说明：

- 此操作需要满足管理权限；

密钥管理

选中“密钥管理”标签项：



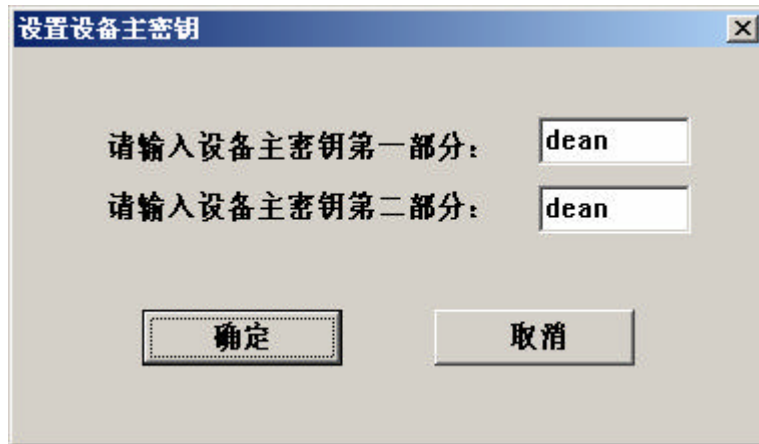
本标签项中包含

- ◆ 设置设备主密钥；
- ◆ 设置系统主密钥；
- ◆ 产生 RSA 密钥对；
- ◆ 备份密钥对；
- ◆ 恢复密钥对；
- ◆ 删除密钥对（一代卡不支持此功能）；
- ◆ 拷贝密钥对（一代卡不支持此功能）。

设置设备主密钥

设备主密钥是用于单机上多卡配置时同步密码卡信息的主密钥，不提供给用户。它由两部分组成。

1. 点击选项“设置设备主密钥”，弹出对话框：



2. 请依次输入设备主密钥第一、第二部分，然后根据需求点击“取消”则取消此次操作，或点击“确定”则

等待生成设备主密钥。

设置设备主密钥成功：



点击确定设置设备主密钥成功。

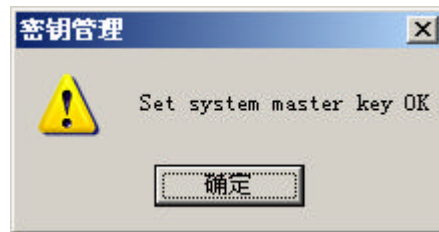


注意：

- 设备主密钥应当在初始化管理员之后就完成此设置。

设置系统主密钥

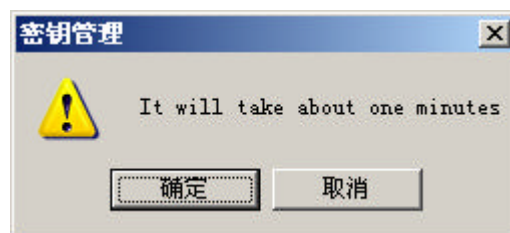
新的密码卡中不存在系统主密钥，需要生成新的以供加解密用户数据；当认为当前系统主密钥不够安全时，可在满足管理权限的情况下更新此系统主密钥，相应的用户数据应随之更新。点击选项“设置系统主密钥”，等待一会出现如下设置系统主密钥成功信息：



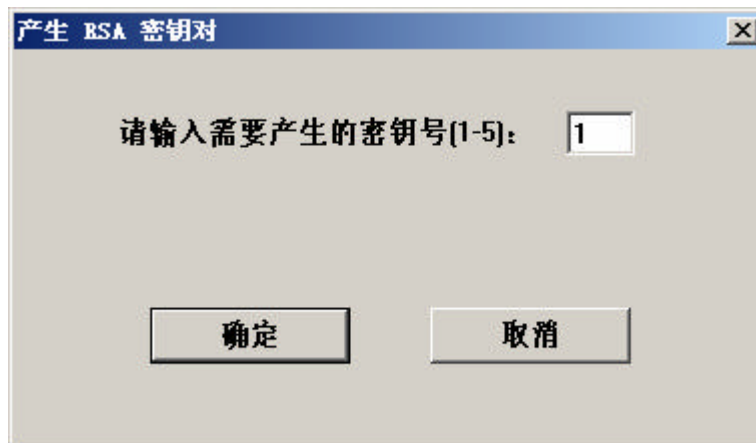
点击确定设置系统主密钥成功。

产生 RSA 密钥对

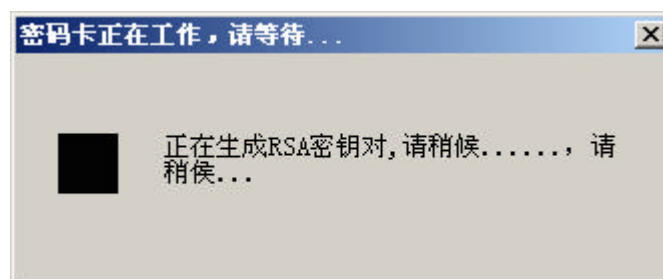
1. 点击选项“产生 RSA 密钥对”，出现以下信息：



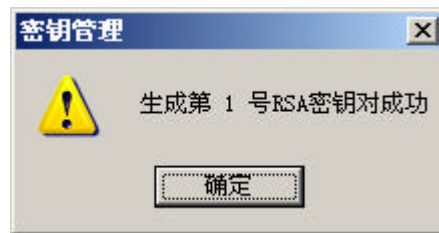
2. 根据需要点击“取消”则取消此次操作，或点击“确定”则出现以下的对话框：



3. 输入密钥号（1-5）后，点击确定：



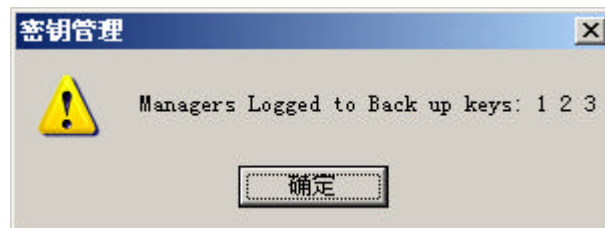
4. 等待约一分钟后出现以下信息：



5. 点击“确定”生成 RSA 密钥对成功。

备份密钥对

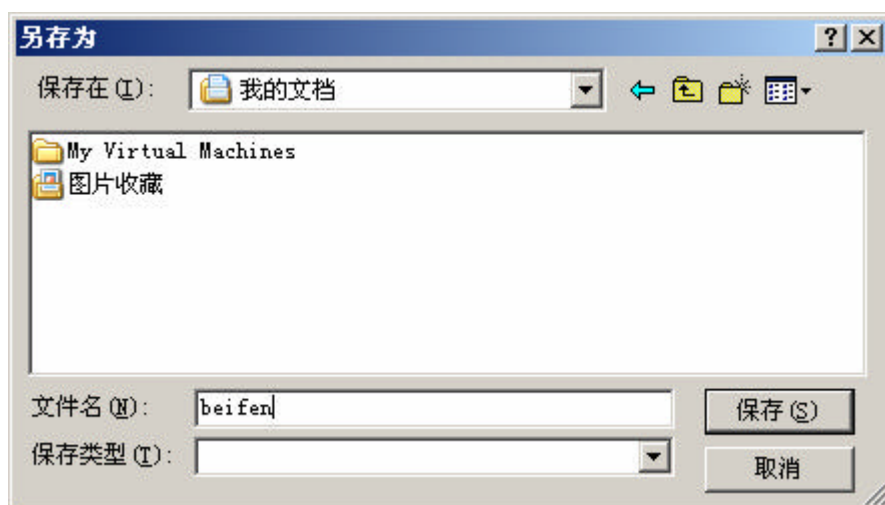
1. 点击选项“备份密钥对”，出现以下信息：



2. 点击“确定”则出现以下信息：



3. 点击“确定”等待一分钟后，出现另存为文件对话框，请选择将要保存的文件目录及文件名（保存类型不用设置）：



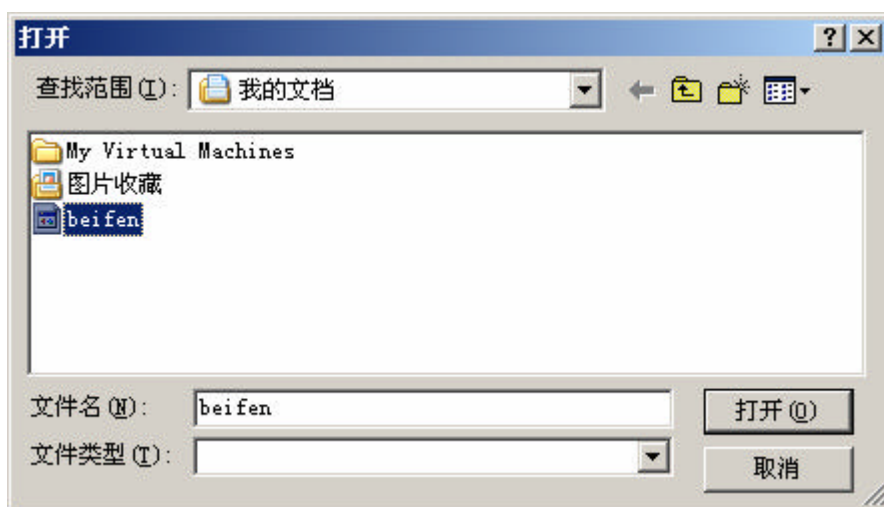
4. 点击“保存”后，显示以下信息：



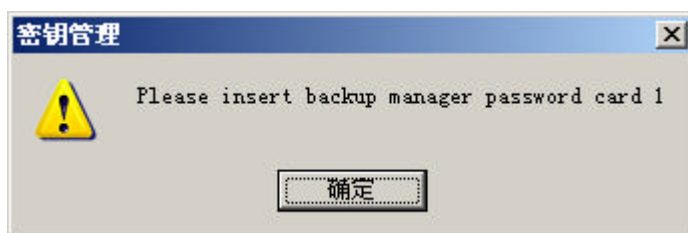
5. 点击“确定”备份密钥对成功。

恢复密钥对

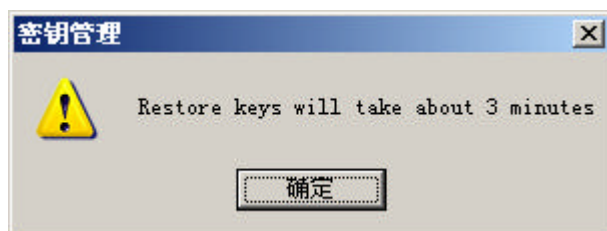
1. 点击选项“恢复密钥对”，出现以下打开对话框（在恢复密钥对时，要重新登陆管理员满足管理权限）：



2. 请选择将要打开的文件目录及文件名（保存类型不用设置）：
然后点击“打开”，出现下列信息：



3. 按顺序依次插入备份密钥对时登陆的管理员口令卡（备份密钥对时有几个管理员登陆则此过程循环几次），循环完毕后出现下列信息：



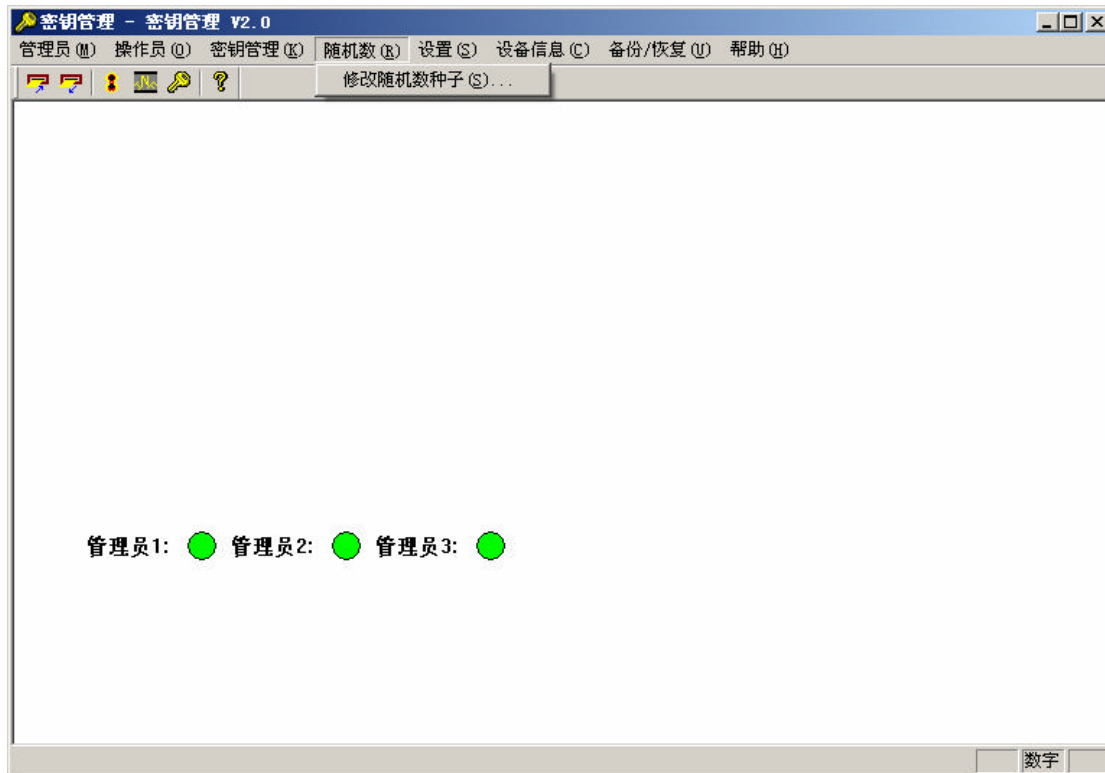
4. 点击确定后，等待约三分钟后出现以下信息：



5. 点击“确定”恢复密钥对成功。

随机数

选中“随机数”标签项：



本标签项中包含

- ◆ 修改随机数种子。

修改随机数种子

修改随机数种子以用于产生随机数。

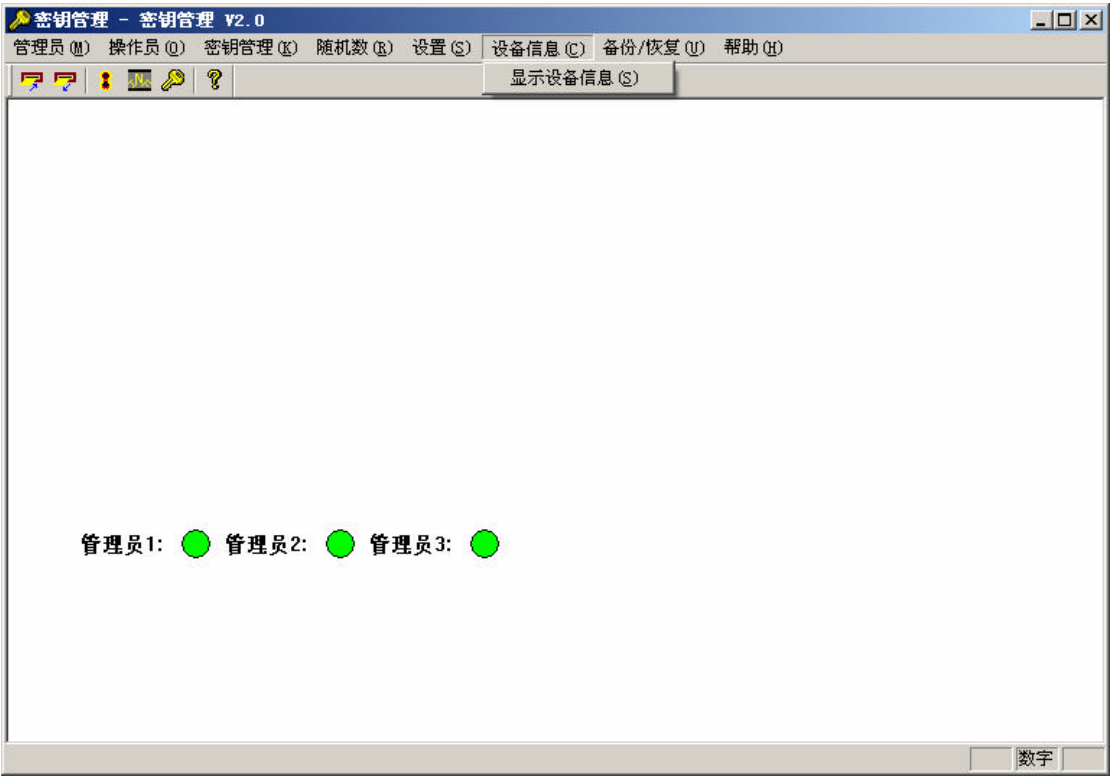
1. 点击选项“修改随机数种子”，出现以下信息：



2. 点击“确定”修改随机数种子成功。

设备信息

选中“设备信息”标签项：



本标签项中包含

- ◆ 显示设备信息。

显示设备信息

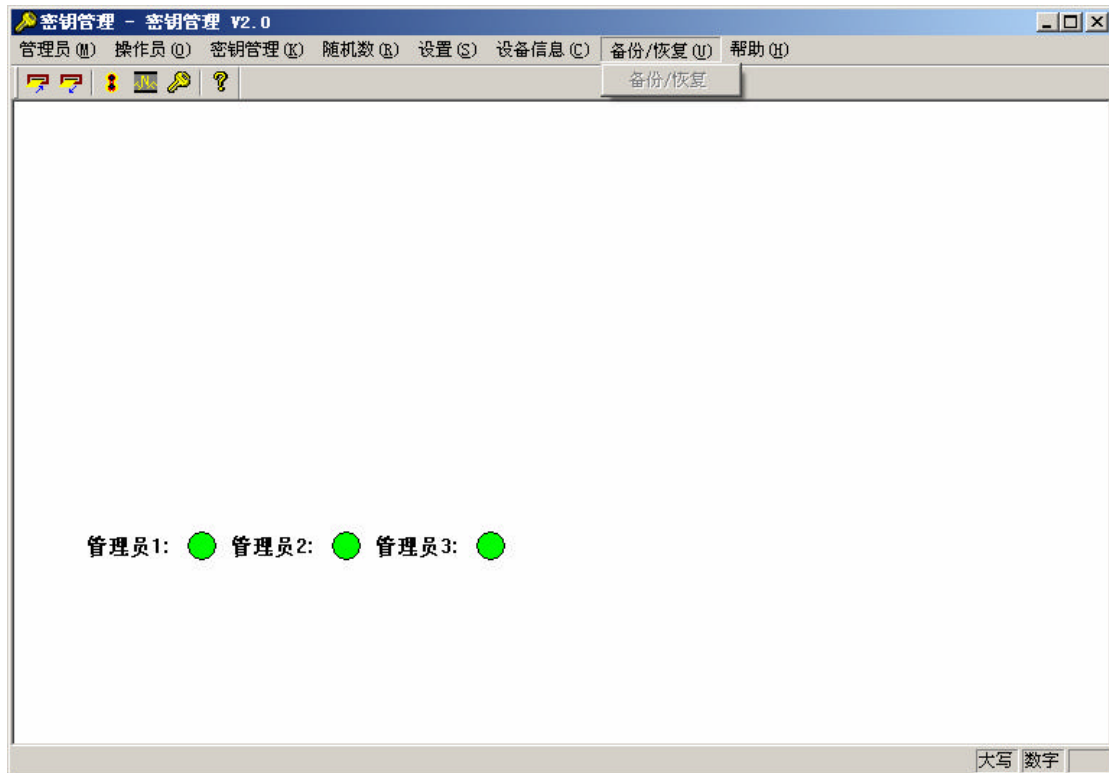
点击选项“显示设备信息”，出现以下信息（包括管理员初始化情况、管理员使用情况、管理员登陆情况、RSA 密钥使用情况）：



点击“确定”后，此信息框消失。

备份/恢复

选中标签项“备份/恢复”：

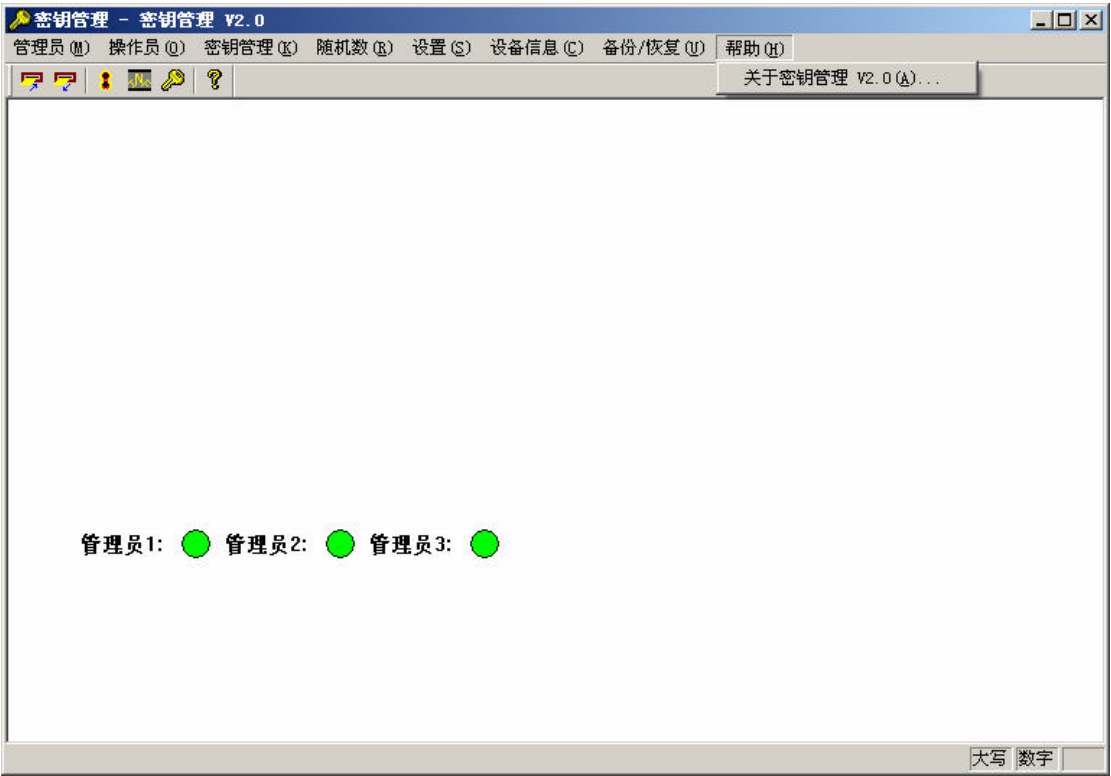


本标签项中包含

- ◆ 备份/恢复（一代卡不支持此功能）。

帮助

选中标签项 “ 帮助 ”：



本标签项中包含

- ◆ 关于密钥管理 V2.0。

关于密钥管理 V2.0

点击选项 “ 关于密钥管理 V 2.0 ”，出现以下信息（有关此密钥管理程序的说明）：



附加说明

本密码卡密钥管理程序除了可以使用菜单栏操作以外 ,还可以使用菜单栏下面的部分工具栏操作。

工具栏中共有六项：

从左到右依次是：管理员登陆、管理员退出、修改随机数种子、显示设备信息、产生 RSA 密钥对、关于密钥管理 V2.0。

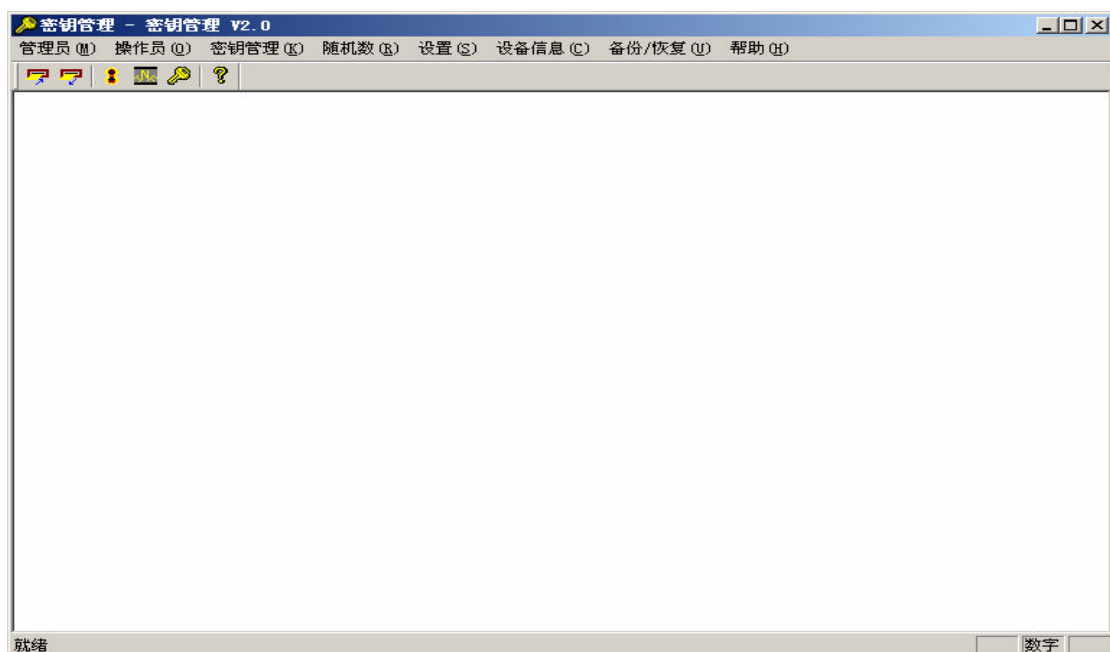
三代卡：

启动密钥管理软件

正确安装密钥管理软件后，点击 开始->程序->得安密码卡密钥管理程序->得安密码卡密钥管理程序 V2.0.exe，启动密钥管理程序。如下显示：

密码卡信息

未对管理员设置前：

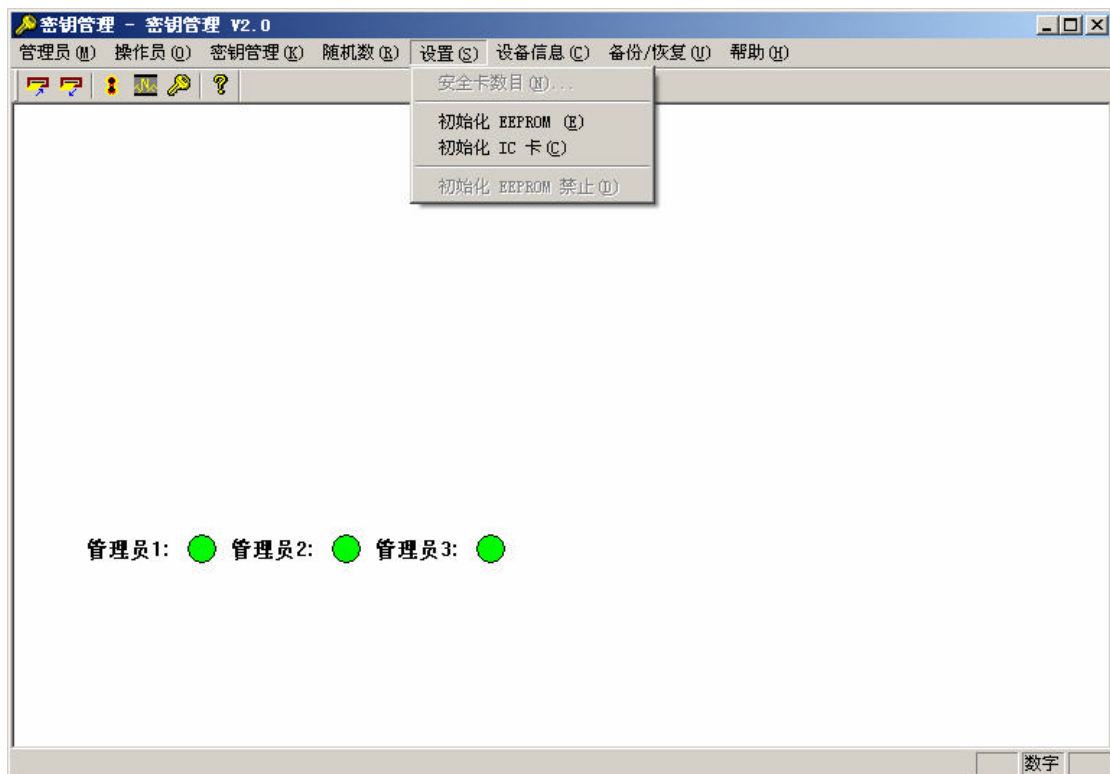


对管理员设置后：



设置

选中“设置”标签项：



本标签项中包含

- ◆ 安全卡数目（三代卡不支持此功能）；
- ◆ 初始化 EEPROM；
- ◆ 初始化 IC 卡；
- ◆ 初始化 EEPROM 禁止（三代卡不支持此功能）。

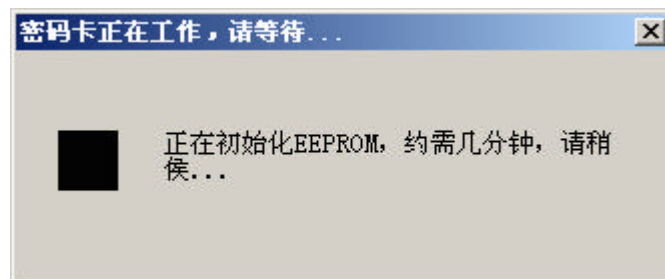
初始化 EEPROM

一块新的密码卡内的 EEPROM 中的内容是不确定的，应该首先对密码卡进行初始化 EEPROM 操作，以保证密码卡内为确定的空状态。

1. 点击选项“初始化 EEPROM”，出现以下信息：



2. 根据需要点击“否”则取消此次操作，或点击“是”则出现以下信息：



3. 等待几十秒钟后出现以下信息：



4. 点击“确定”，初始化 EEPROM 成功。



说明：

- 完成 EEPROM 初始化操作，密码卡内所有信息将被清空，需要重

新进行管理员初始化等操作及密钥设置；EEPROM 的初始化操作并不会影响到基础配置程序所设置的内容。



注意：

- 此项操作一旦执行则会丢失密码卡内所有信息，在正常使用过程中不允许执行此操作；所以对于此项操作，必须由专业维护人员或厂商技术支持人员完成。

初始化 IC 卡

此功能彻底清除 IC 卡上的所有内容。

1. 点击选项“初始化 IC 卡”，出现以下信息：



2. 插入要初始化的 IC 卡，根据需要点击“取消”则取消此次操作，或点击“确定”则几秒钟后出现以下信息：



3. 点击“确定”，初始化 IC 卡成功。

管理员

选中“管理员”标签项：



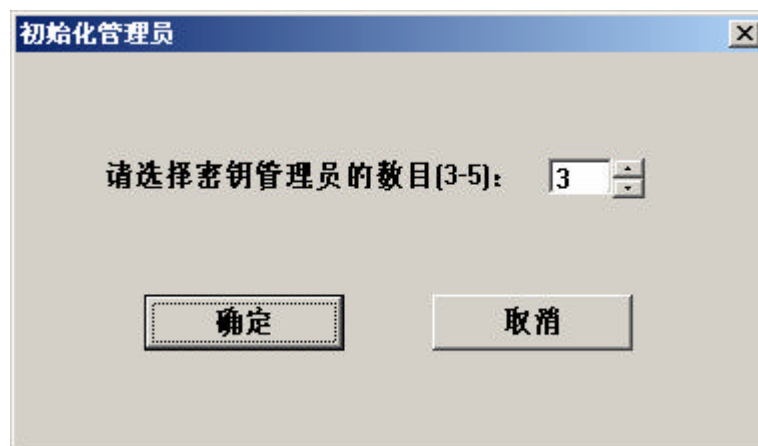
本标签项中包含了对管理员口令 IC 卡的操作：

- ◆ 管理员登录：识别验证管理员口令 IC 卡的身份信息；
- ◆ 管理员退出：管理员全部退出；
- ◆ 初始化管理员：设置管理员口令 IC 卡；
- ◆ 增加管理员：增加一个管理员；
- ◆ 删除管理员：删除一个管理员；
- ◆ 备份管理员口令：备份一个管理员的口令（三代卡不支持此功能）；
- ◆ 修改管理员口令：修改一个管理员的口令（三代卡不支持此功能）；
- ◆ 退出：退出程序，管理员退出登录。

初始化管理员

一张新的密码卡初始化之后是没有管理员的，对于 IC 卡控制类型的密码卡此时应认真设置好它的管理员，才能进一步应用密码卡。

1. 点击选项“初始化管理员”，出现对话框：



2. 请选择您要初始化的管理员的数量，3~5 个，然后点击“确定”：



按照提示，向读卡器中插入将要作为 1 号管理员口令卡的 IC 卡，然后点击“确定”键后重复以上过程。



说明：

- 本步骤将会根据所输入的管理员的数量 n 重复执行 n 次，即把所初始化的管理员口令依次输出到 IC 卡。

3. 初始化管理员成功，完成此操作。





注意：

- 本初始化操作所生成的管理员口令卡对以后密码卡管理非常重要，所以需要妥善保管。
- 本初始化操作只能在密码卡初始化之后进行，且不可重复，若要改动，请通过增加、删除管理员的方式完成。

管理员登录

对密码卡的大部分管理操作需要满足管理权限，即半数以上的管理员成功登录方可进行。

点击选项“管理员登录”，出现提示信息：



按照提示，将管理员口令 IC 卡插入读卡器中，然后点击确定，密码卡识别验证后返回此次操作结果，成功则显示（相应管理员标识由红变绿）：





错误则将显示：



相应的错误码，请参看密码卡加密系统 DTCSP 编程手册错误码。

管理员退出

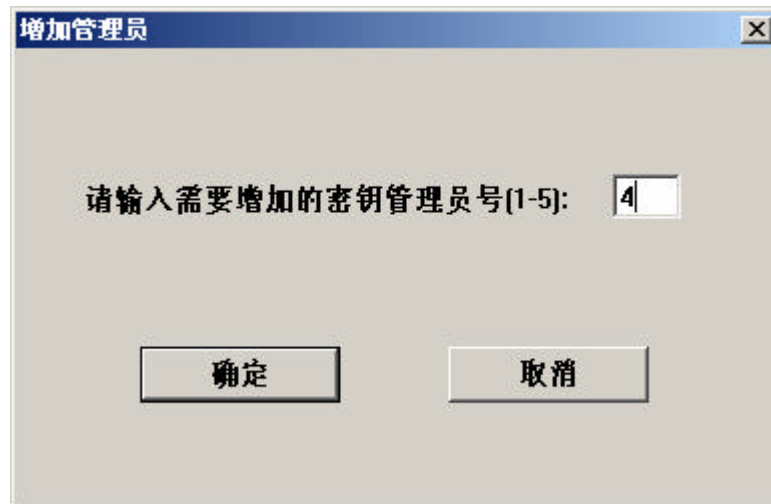
管理员在完成相应的管理职责之后应及时退出登录,以防止他人越权误操作或恶意破坏。

点击选项“管理员退出”后，出现管理员退出登录成功信息：



增加管理员

点击选项“增加管理员”，出现如下对话框：



请输入将要增加的管理员号码，向读卡器中插入作为新增管理员口令卡的 IC 卡，然后点击“确定”，成功则弹出：





说明：

- ☐ 此操作需满足管理权限。
- ☐ 增加一个已存在的管理员号码或者管理员数目已经最大（5个）时，此操作将错误返回。

删除管理员

点击选项“删除管理员”，出现如下对话框：



输入将要删除的管理员号码，然后点击“确定”，成功则弹出：



说明：

- 此操作需要满足管理权限。
- 删除一个不存在的管理员号码时，此操作将错误返回。（另附：密码卡管理员数目等于 1 个时就不能再删除。）

退出

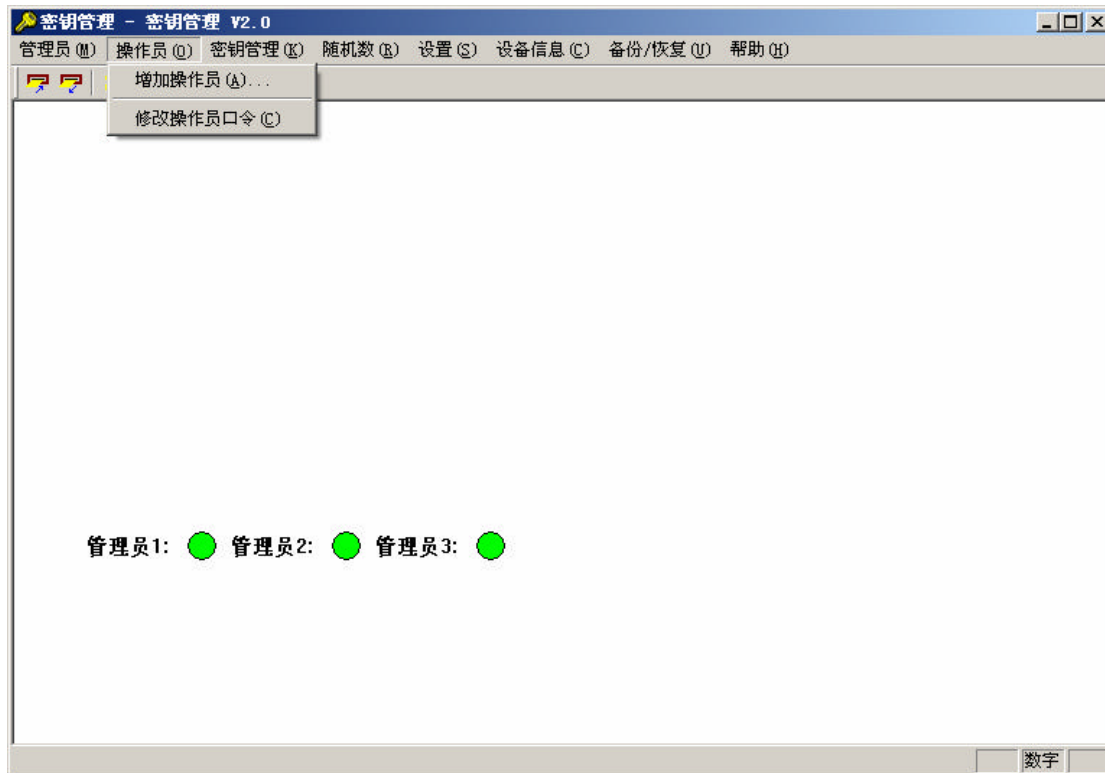
点击选项“退出”，出现如下提示：



管理员退出登录，密钥管理程序关闭。

操作员

选中“操作员”标签项：



本标签项中包含了对操作员的以下操作：

- ◆ 增加操作员：增加一个操作员；
- ◆ 修改操作员口令：操作员口令更换。

增加操作员

密码卡更新操作员口令后无操作员，此时需要添加操作员，还有就是密码卡可能要授予更多的人操作权限，此时也需要添加操作员。

点击选项“增加操作员”，系统弹出：



按照提示，向读卡器中插入将要添加的操作员口令 IC 卡，然后点击“确定”，系统返回相应的操作信息：



增加一操作员成功，此 IC 卡应有某操作员妥善保管好，需要时行使相应的职责。

修改操作员口令

新的密码卡中没有操作员口令，应该运行此操作以对操作员口令进行初始化，然后添加操作员等；当有操作员卡遗失或被盗时，为防止他人误操作或恶意破坏，也应及时做修改操作员口令操作。

点击按钮“修改操作员口令”，弹出：



然后根据需求，点击“确定”执行此操作或“取消”撤销此次选择。

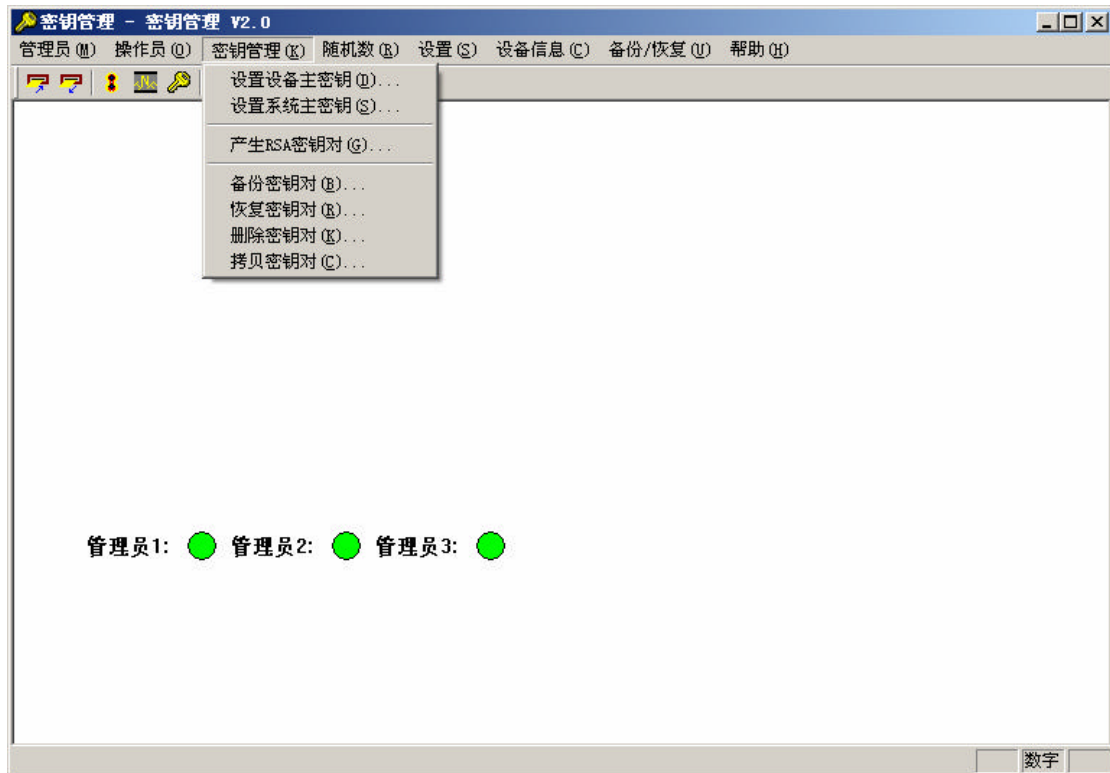


说明：

- 此操作需要满足管理权限；
- 此操作成功后，此前的所有操作员口令 IC 卡均失效，需要重新执行增加操作员操作。

密钥管理

选中“密钥管理”标签项：



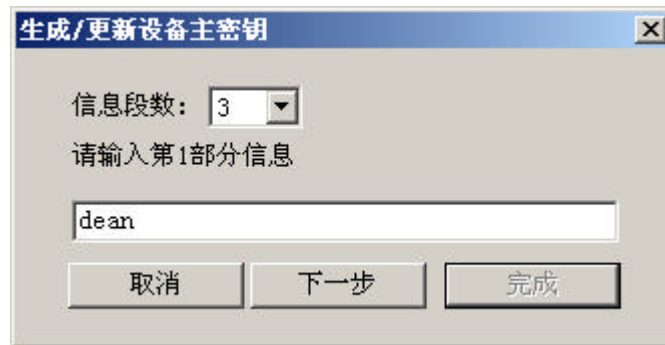
本标签项中包含

- ◆ 设置设备主密钥；
- ◆ 设置系统主密钥；
- ◆ 产生 RSA 密钥对；
- ◆ 备份密钥对；
- ◆ 恢复密钥对；
- ◆ 删除密钥对；
- ◆ 拷贝密钥对。

设置设备主密钥

设备主密钥是用于单机上多卡配置时同步密码卡信息的主密钥，不提供给用户。它由（1~6）部分组成。

3. 点击选项“设置设备主密钥”，弹出对话框：



2. 首先选择需要的信息段数（1~6），然后按系统提示输入信息（选择的信息段数大于1时，要循环选择的信息段数次），然后根据需求点击“取消”则取消此次操作，或点击“完成”则系统提示设置设备主密钥成功：



点击确定设置设备主密钥成功。



注意：

- 设备主密钥应当在初始化管理员之后就完成此设置。

设置系统主密钥

新的密码卡中不存在系统主密钥，需要生成新的以供加解密用户数据；当认为当前系统主密钥不够安全时，可在满足管理权限的情况下更新此系统主密钥，相应的用户数据应随之更新。点击选项“设置系统主密钥”后：



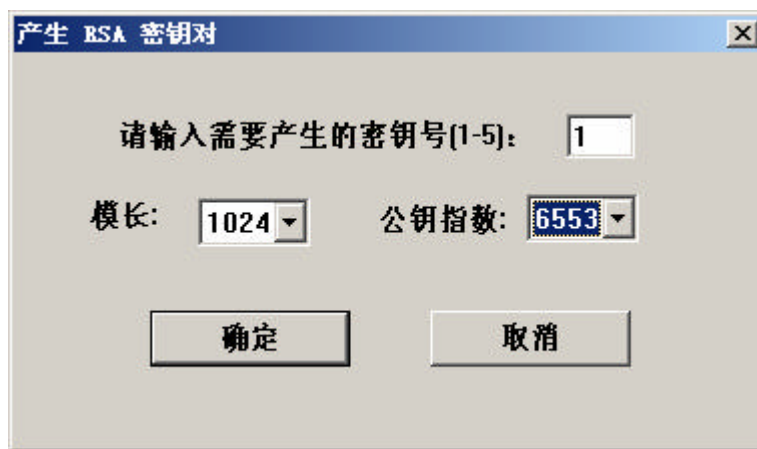
点击“是”等待一会会出现如下设置系统主密钥成功信息：



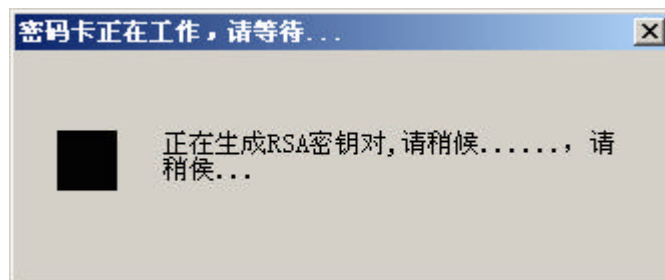
点击确定设置系统主密钥成功。

产生 RSA 密钥对

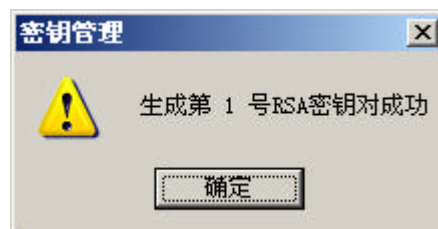
1. 点击选项“产生 RSA 密钥对”，出现以下信息：



4. 输入密钥号（1-5），模长（1024 或 2048）公钥指数（3 或 65537）后，根据需要点击“取消”则取消此次操作，或点击“确定”则出现下列信息：



3. 等待几秒钟后出现以下信息：



4. 点击“确定”生成 RSA 密钥对成功。

备份密钥对

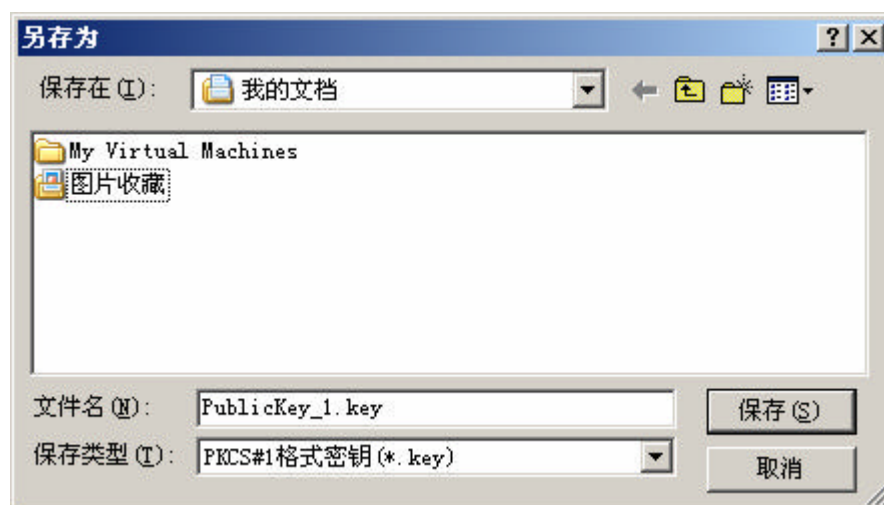
4. 点击选项“备份密钥对”，出现以下信息：



5. 选择要备份的密钥号（1-5），点击“确定”则出现以下信息：



6. 点击“是”等待几秒钟后，出现另存为文件对话框，请选择将要保存的文件目录及文件名和保存类型：



7. 点击“保存”后，显示以下信息：



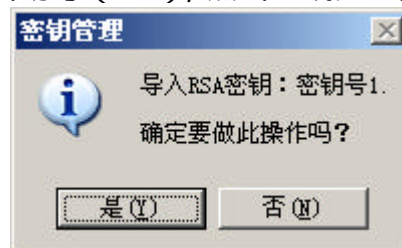
5. 点击“确定”备份密钥对成功。

恢复密钥对

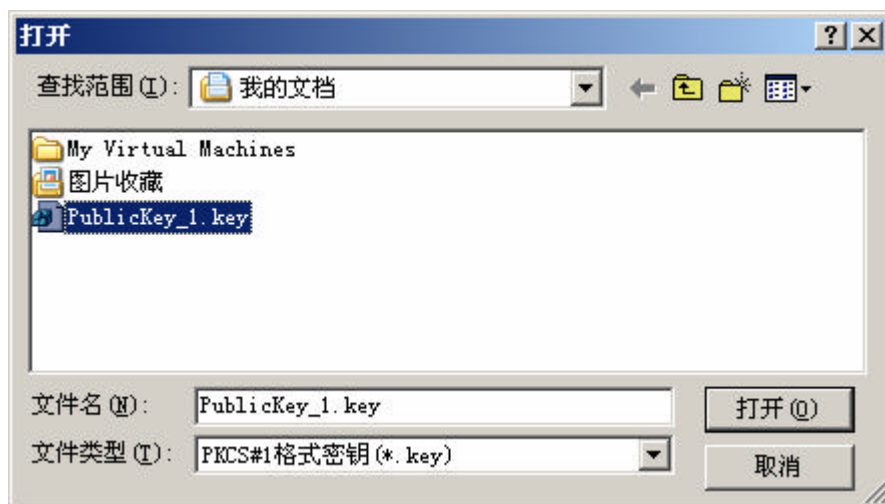
4. 点击选项“恢复密钥对”，出现以下打开对话框：



2. 选择要恢复的密钥号（1-5），点击“确定”则出现以下信息：



3. 点击“是”等待几秒钟后，出现打开文件对话框，请选择将要打开的文件目录及文件名和文件类型：



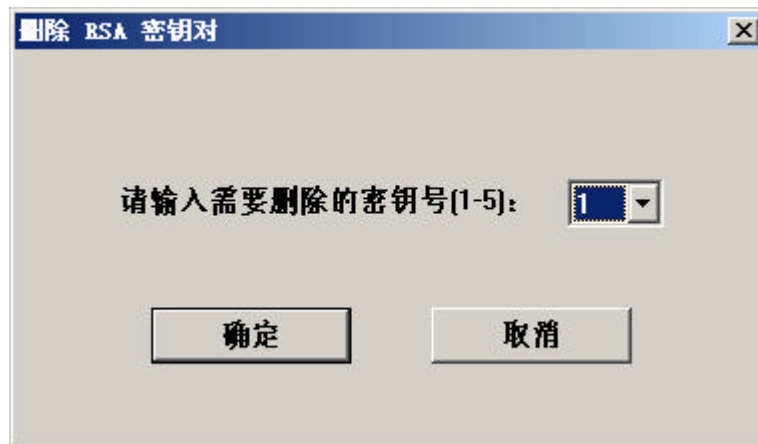
4. 点击“打开”后，显示以下信息：



5. 点击“确定”恢复密钥对成功。

删除密钥对

1. 点击选项“删除密钥对”，出现以下打开对话框：



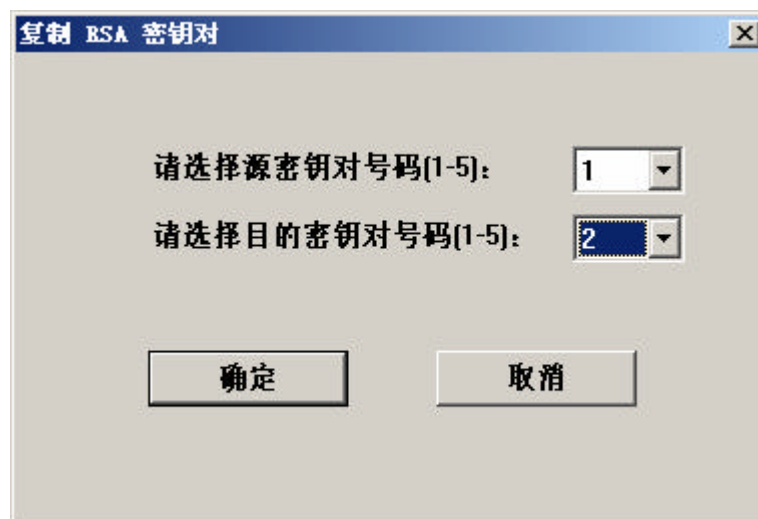
2. 选择要删除的密钥号（1-5），点击“确定”则出现以下信息：



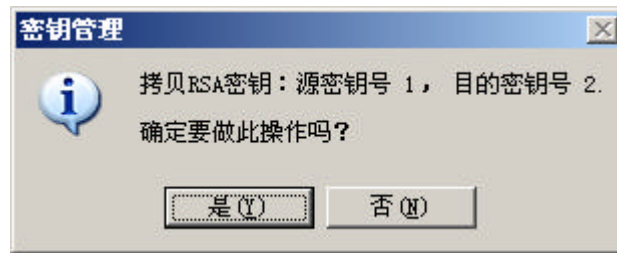
3. 点击“确定”恢复密钥对成功。

拷贝密钥对

1. 点击选项“拷贝密钥对”，出现以下打开对话框：



2. 选择源密钥对号码（1-5），选择目的密钥对号码（1-5），点击“确定”则出现以下信息：



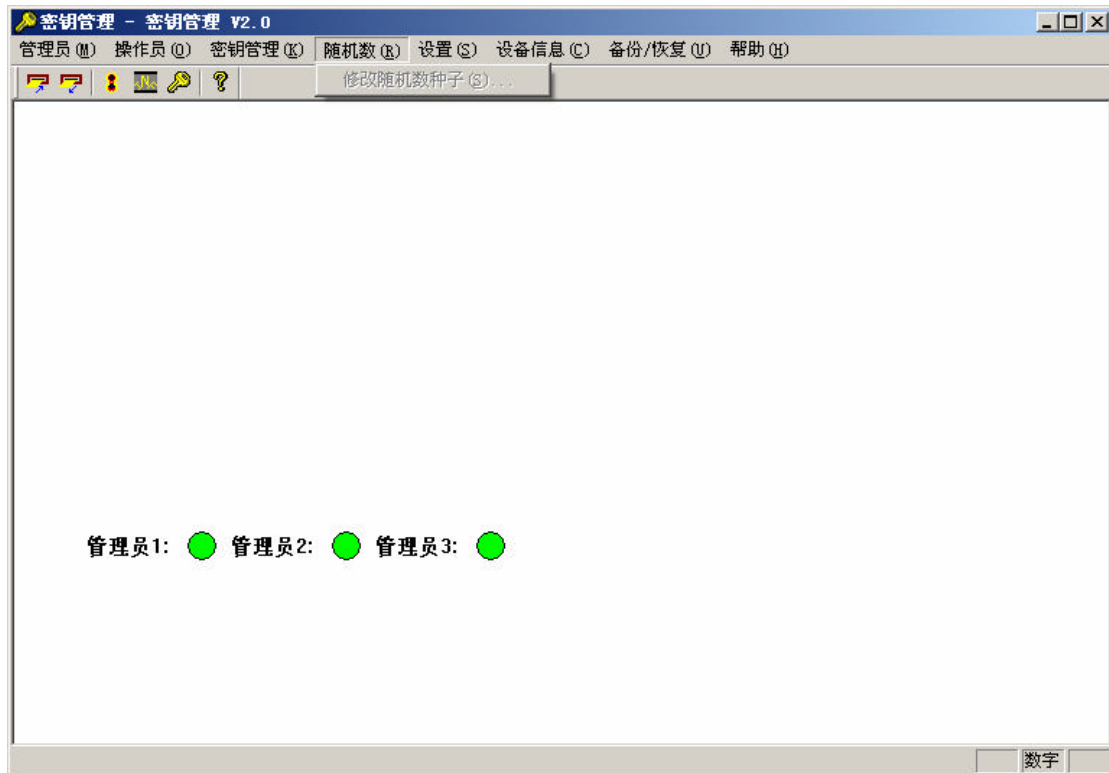
3. 点击“是”出现下列信息：



3. 点击“确定”拷贝密钥对成功。

随机数

选中“随机数”标签项：

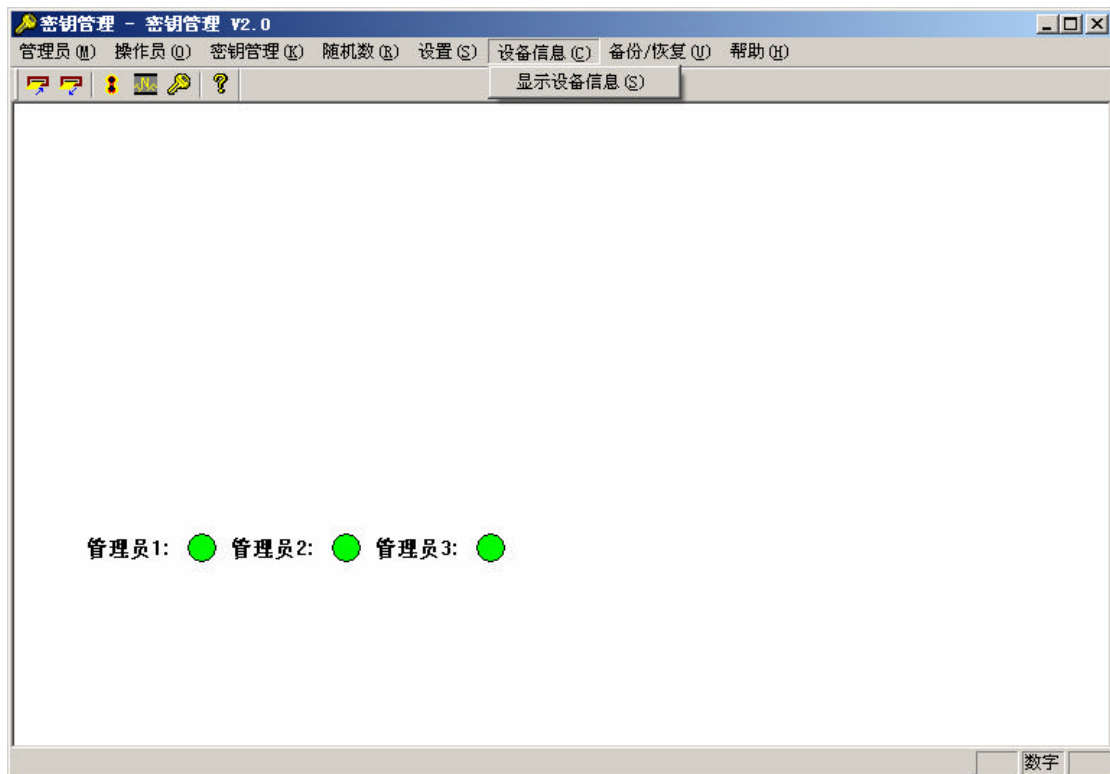


本标签项中包含

- ◆ 修改随机数种子（三代卡不支持此功能）。

设备信息

选中“设备信息”标签项：



本标签项中包含

- ◆ 显示设备信息。

显示设备信息

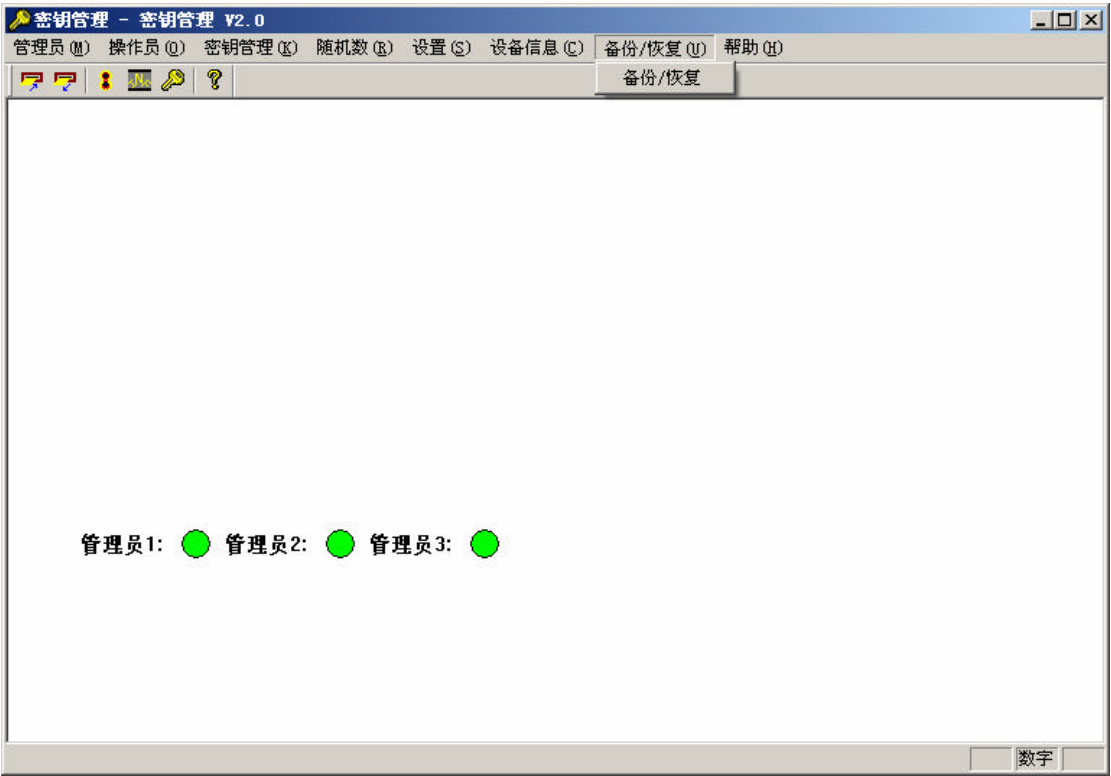
点击选项“显示设备信息”，出现以下信息（包括管理员初始化情况、管理员使用情况、RSA 密钥使用情况等）：



点击“确定”后，此信息框消失。

备份/恢复

选中标签项 “ 备份/恢复 ”：

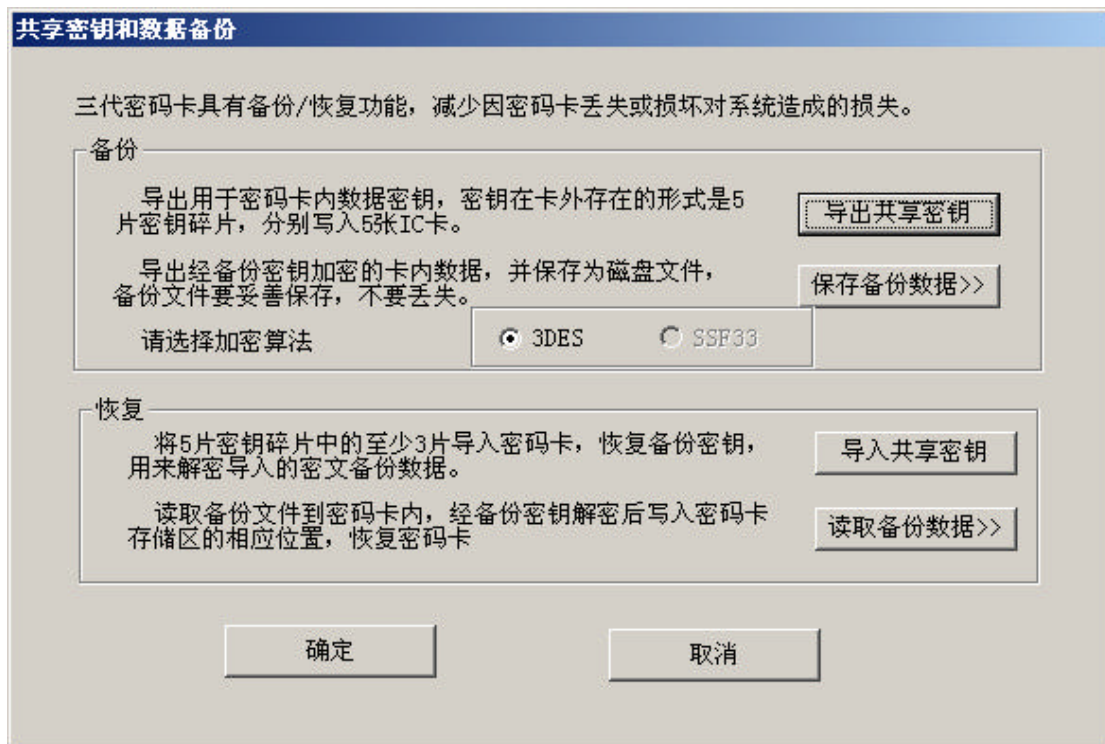


本标签项中包含

- ◆ 备份/恢复。

备份/恢复

点击选项 “ 备份/恢复 ”，出现以下信息：



此信息框中包含对密码卡信息的备份及恢复操作：

- ◆ 备份；
- ◆ 恢复。

备份

在半数以上管理员登录通过的情况下，可以将密码卡的所有信息备份到异地（本地硬盘），在密码卡受到恶意破坏时可以及时恢复密码卡损坏之前的各种状态及密钥信息，选择加密算法（三代底端卡仅支持 3DES 算法）。

1. 准备好 5 张保存此密码卡备份信息的备份 IC 卡，然后点击按钮“导出共享密钥”：



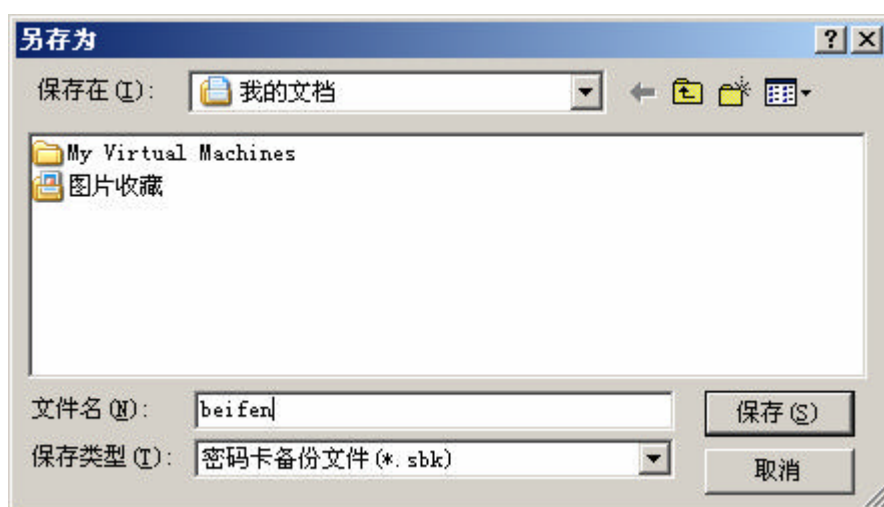
按照提示向读卡器中插入相应的备份 IC 卡，然后点击“确定”；读卡器的指示灯闪过之后，系统将重复此步骤，请按照提示完成此步骤的 5 次循环；

2. 第 5 次循环后弹出信息框：

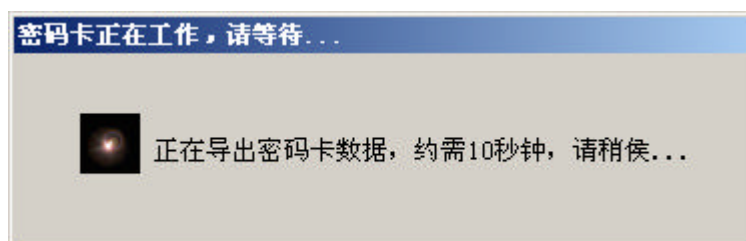


点击“确定”则导出共享密钥完成。

3. 点击按钮“保存备份数据”，弹出另存为文件对话框：



请选择备份文件的保存路径及文件名和保存类型，然后点击保存，等待密码卡备份数据写入选定的备份文件。



此过程中：

失败，返回相应的错误信息，请参看密码卡加密系统 DTCSP 编程手册错误码；

成功，完成：



注意：

- 所生成的 5 张备份卡将会在数据恢复时作为输入口令，所以需要妥善保管。
- 完成备份后的密文备份文件切勿随意篡改，应妥善保存好。

恢复

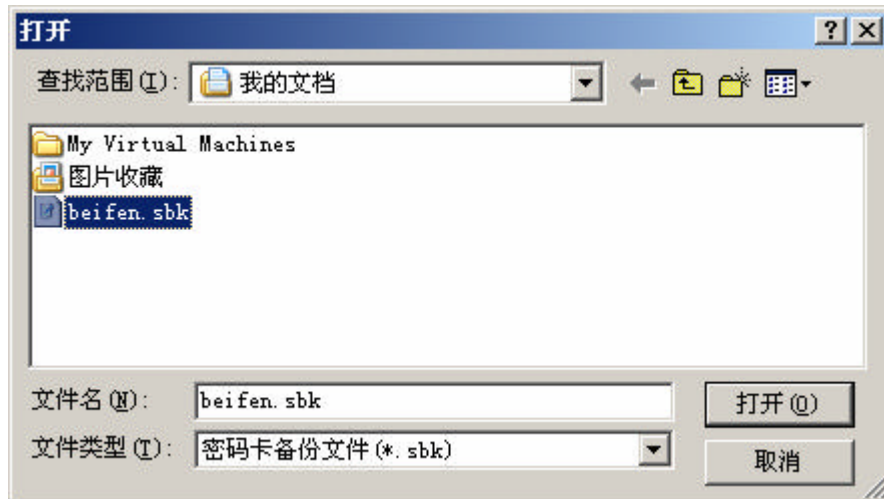
在密码卡受到恶意破坏时，可以根据需要恢复密码卡受损前的状态信息。

准备至少三张备份时存放导出信息的备份 IC 卡，然后点击按钮“ 导入共享密钥 ”，弹出提示对话框：

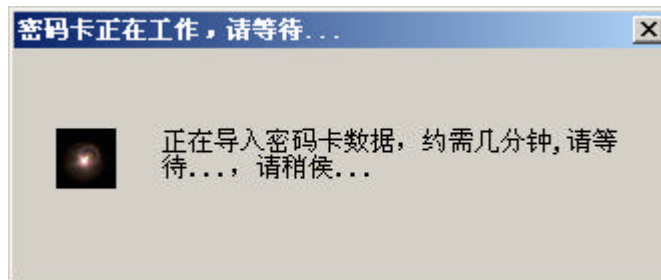


请按照提示向读卡器中插入一张备份 IC 卡，然后点击“ 确定 ”，请按照提示循环三次插入三张不同的备份 IC 卡；

1. 点击按钮“ 读取备份数据 ”，弹出打开文件对话框：



2. 请选择将要恢复的备份文件的路径及文件名和文件类型，点击“打开”，然后等待密码卡执行此操作：



此过程中：

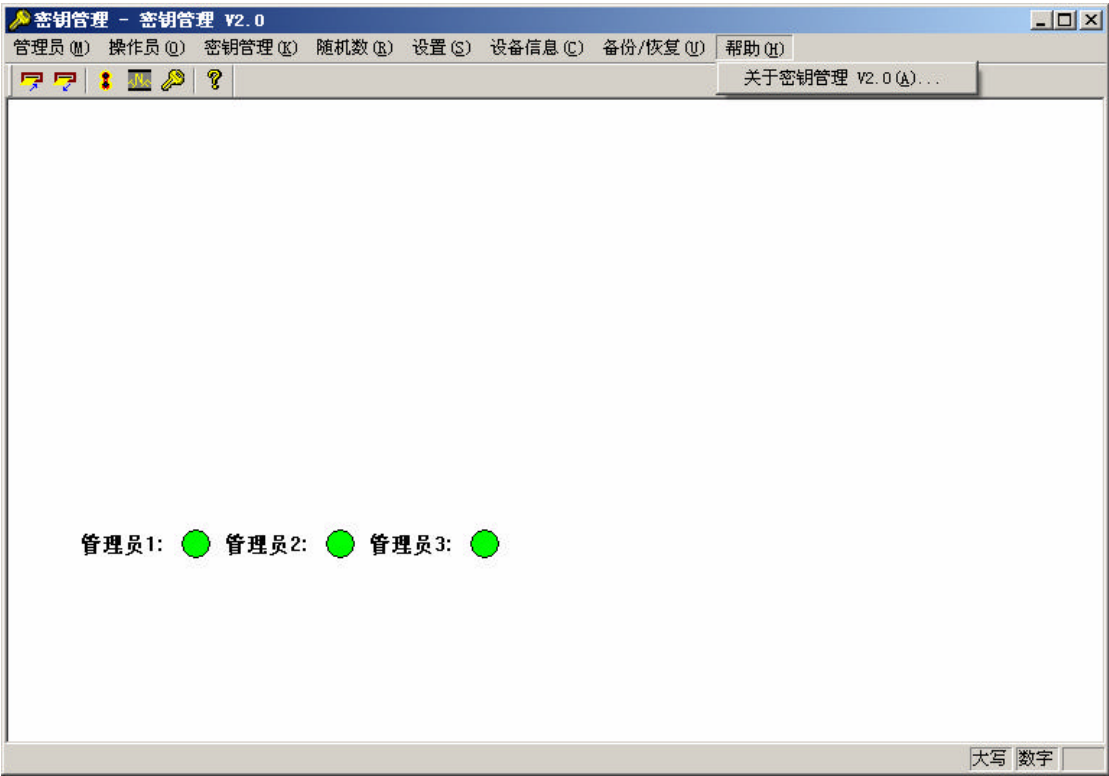
失败，返回相应的错误信息，请参看密码卡加密系统 DTCSP 编程手册错误码；

成功，完成：



帮助

选中标签项 “ 帮助 ”：

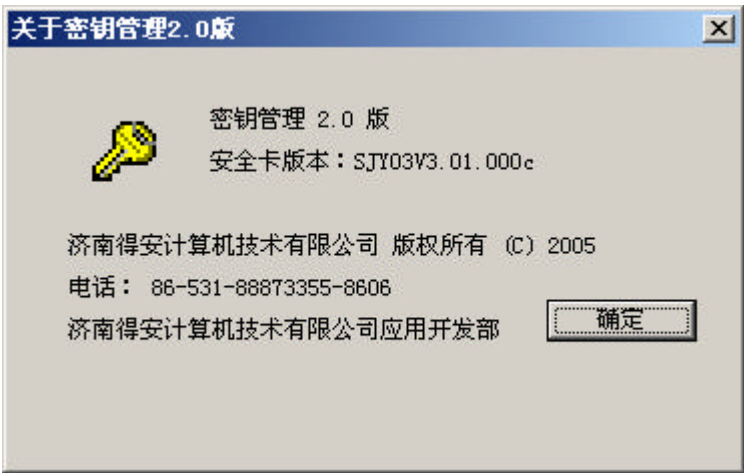


本标签项中包含

- ◆ 关于密钥管理 V2.0。

关于密钥管理 V2.0

点击选项 “ 关于密钥管理 V 2.0 ”，出现以下信息（有关此密钥管理程序的说明）：



附加说明

本密码卡密钥管理程序除了可以使用菜单栏操作以外 ,还可以使用菜单栏下面的部分工具栏操作。

工具栏中共有六项：

从左到右依次是：管理员登陆、管理员退出、修改随机数种子、显示设备信息、产生 RSA 密钥对、关于密钥管理 V2.0。

得安密码卡密钥管理程序 V2.0 对一代卡与三代卡的操作的不同点：

1. 一代卡支持备份管理员口令和修改管理员口令功能，三代卡不支持。
2. 一代卡管理员数目等于 3 个时不能再删除，三代卡管理员数目等于 1 个时不能再删除。
3. 一代卡最多可以添加 10 个操作员，三代卡没有限定。
4. 一代卡增加操作员时要给操作员确定号码，三代卡不需要。
5. 一代卡“修改操作员口令”操作时仅修改一个操作员的，三代卡则全部修改。
6. 一代卡不支持删除密钥对和拷贝密钥对功能，三代卡支持。
7. 一代卡设置设备主密钥时确定输入两部分信息，三代卡可以选择输入 1~6 部分信息。
8. 一代卡产生 RSA 密钥对时仅需输入密钥号（1-5），三代卡产生 RSA 密钥对时则需输入密钥号（1-5） 模长（1024 或 2048） 公钥指数（3 或 65537）。
9. 一代卡与三代卡在备份密钥对和恢复密钥对时由于机制不同具体操作时有很大的区别，请仔细阅读得安密码卡密钥管理程序 V2.0 操作手册中相对应的部分。
10. 一代卡可以修改随机数种子以用于产生随机数，三代卡不可以。
11. 一代卡“初始化 EEPROM 禁止”选项没有禁止（**请千万不要点击此选项，否则会带来不可估量的损失，后果自负。**），三代卡“初始化 EEPROM 禁止”选项则禁止了。
12. 一代卡不支持备份/恢复功能，三代卡支持。