移动数字证书

Linux 版用户手册

版本：F-3.0

适用硬件：F1、F2

深圳证券数字证书认证中心

http://ca.szse.cn

目　　录

1. 物品清单 2
2. 软件安装 2
2.1 适用平台 2
2.2 注意事项 2
2.3 安装过程 3
3. 证书使用 4
3.1 与电脑相连 4
3.2 证书管理工具 4
3.3 软件窗口简介 5
3.3.1 “文件”菜单 6
3.3.2 “查看”菜单 7
3.3.3 “令牌操作”菜单 7
3.4 标准功能 7
3.4.1 查看证书信息 7
3.4.2 登录 8
3.4.3 修改用户 PIN 码 9
3.4.4 修改令牌名 9
3.4.5 数据管理 10
3.4.6 查看详细信息 11
3.4.7 导入证书 13
3.4.8 导出证书 14
3.4.9 删除证书 15
3.5 注意事项 16
4. 软件卸载 17
5. 常见问题 18
6. 软件版本 21
7. 硬件规格 22

1.物品清单

包装盒内物品清单如下：

1. 移动数字证书
2. 安装光盘
3. 用户手册
4. 合格证

2.软件安装

2.1 适用平台

移动数字证书支持下列操作系统：

- ✓ RedHat Linux Advanced Server V3.X（32/64 位）
- ✓ RedHat Linux Advanced Server V4.X（32/64 位）
- ✓ RedHat Linux Advanced Server V5.X（32/64 位）
- ✓ RedHat Linux Advanced Server V6.X（32/64 位）

2.2 注意事项

在开始安装移动数字证书相关软件之前，需保证满足以下要求（本手册中，“UKey”与“移动数字证书”意义相同）：

- ✓ 操作系统为产品支持的版本(请参见“2.1 适用平台”)。
- ✓ 电脑上带有至少一个 USB 接口，并且在 CMOS 设置中将 USB 支持功能打开。
- ✓ 可选用 USB 延长线或 USB Hub。

2.3 安装过程

1、复制 UKey 安装文件到操作系统的任意位置，并解压。

- ✓ 如果是 32 位 Linux 操作系统，请复制并解压光盘中的以下文件：

  /linux/EnterSafe-Shuttle-1.0.100720_32_RHAS.tar.gz

- ✓ 如果是 64 位 Linux 操作系统，请复制并解压光盘中的以下文件：

  /linux/EnterSafe-Shuttle-1.0.100720_64_RHAS.tar.gz

2、如果您的操作系统启用了 SELinux，请执行以下命令：

cd <解压文件所在目录>/redist/

chcon -t texrel_shlib_t libshuttle_p11v220.so.1.0.0

3、如果您需要在非管理员用户下使用 UKey，请运行“sh <解压文件所在目录>/config/config.sh″，配置成功后，非管理员用户即可正常使用。

3. 证书使用

3.1 与电脑相连

可以使用以下两种方式：

1、拔下移动数字证书的帽盖，直接插在电脑的 USB 接口上，移动数字证书尾部的灯亮，表示移动数字证书与电脑的连接正常。

2、将 USB 延长线插在电脑的 USB 接口上，拔下移动数字证书的帽盖，将移动数字证书插在 USB 延长线上，移动数字证书尾部的灯亮，表示移动数字证书与电脑的连接正常。

3.2 证书管理工具

运行“<解压文件所在目录>/redist/pkimanager”，没有插入 UKey 时显示的管理工具如图 3-1 所示：

图 3-1

插入 UKey 后，管理工具将识别到 UKey 的基本信息，显示的信息如图 3-2 所示：

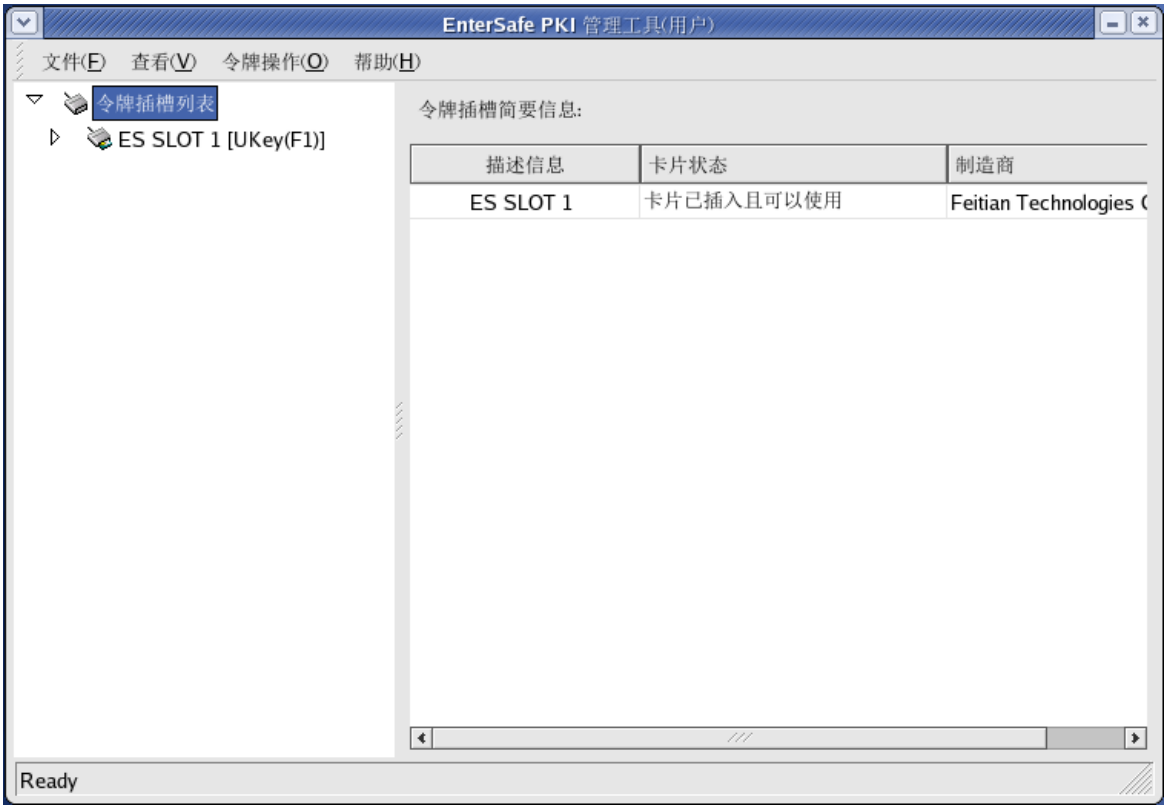

图 3-2

3.3 软件窗口简介

工具菜单如图 3-3 所示：

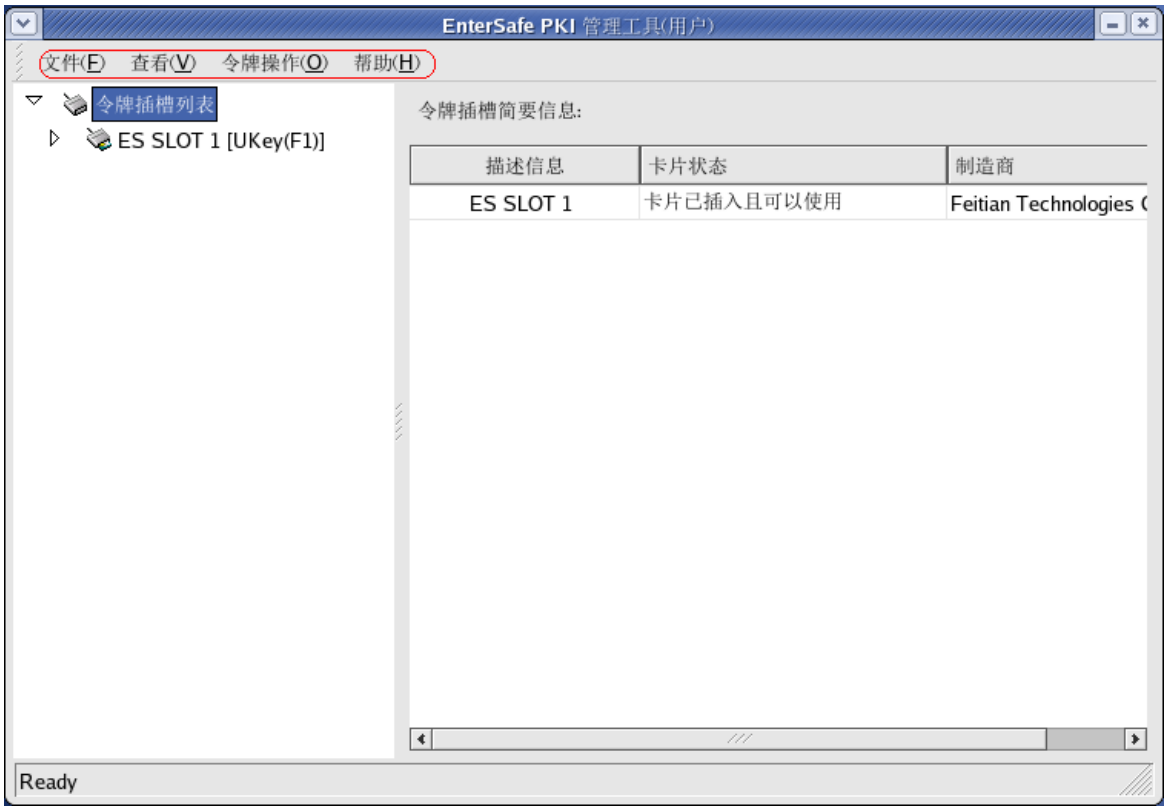

图 3-3

工具菜单包括：文件（更改语言和退出）、查看（查看令牌插槽列表和隐藏空的读卡器）、令牌操作（操作 UKey 的相关功能）和帮助（版权信息）。

3.3.1 “文件”菜单

该菜单详细的选项如图 3-4 所示：

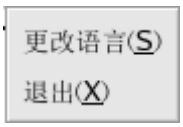

图 3-4

点击“更改语言”按钮，可以设置工具的显示语言为“简体中文”或者“英文”，如图 3-5 所示：

图 3-5

3.3.2 “查看”菜单

该菜单详细的选项如图 3-6 所示：

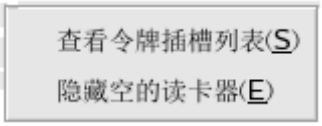

图 3-6

3.3.3 “令牌操作”菜单

该菜单详细的选项如图 3-7 所示：

图 3-7

3.4 标准功能

3.4.1 查看证书信息

选中工具右边“令牌插槽列表”下的 UKey，可以查看对应 UKey 的相关信息，如图 3-8 所示：

图 3-8

3.4.2 登录

点击“登录”按钮，将弹出图 3-9 所示的密码输入窗口，验证 UKey 的用户 PIN 码：

图 3-9

在输入正确的“用户 PIN 码”后，点击“确定”按钮，即完成登录。

3.4.3 修改用户 PIN 码

默认的用户 PIN 码是“111111”。第一次使用 UKey 时，强烈建议您立即修改用户 PIN 码，并定期修改。

点击“修改用户 PIN”按钮，会弹出如图 3-10 所示窗口：

图 3-10

请输入旧的用户 PIN，然后再输入“新的 PIN 码”和“确认新的 PIN 码”，最后点击“确定”按钮完成该操作。

3.4.4 修改令牌名

令牌名(UKey 名称)可以用来区分不同的令牌，您可以修改 UKey 的名称，点击“修改令牌名”，会弹出图 3-11 所示窗口：

图 3-11

输入不超过 32 位的任意内容后点击“确定”按钮，管理工具将会显示 UKey 的新名称。

3.4.5 数据管理

在没有“登录”的情况下，点击令牌的“数据管理”会出现如图 3-12 所示窗口，显示证书信息和证书的公钥信息：

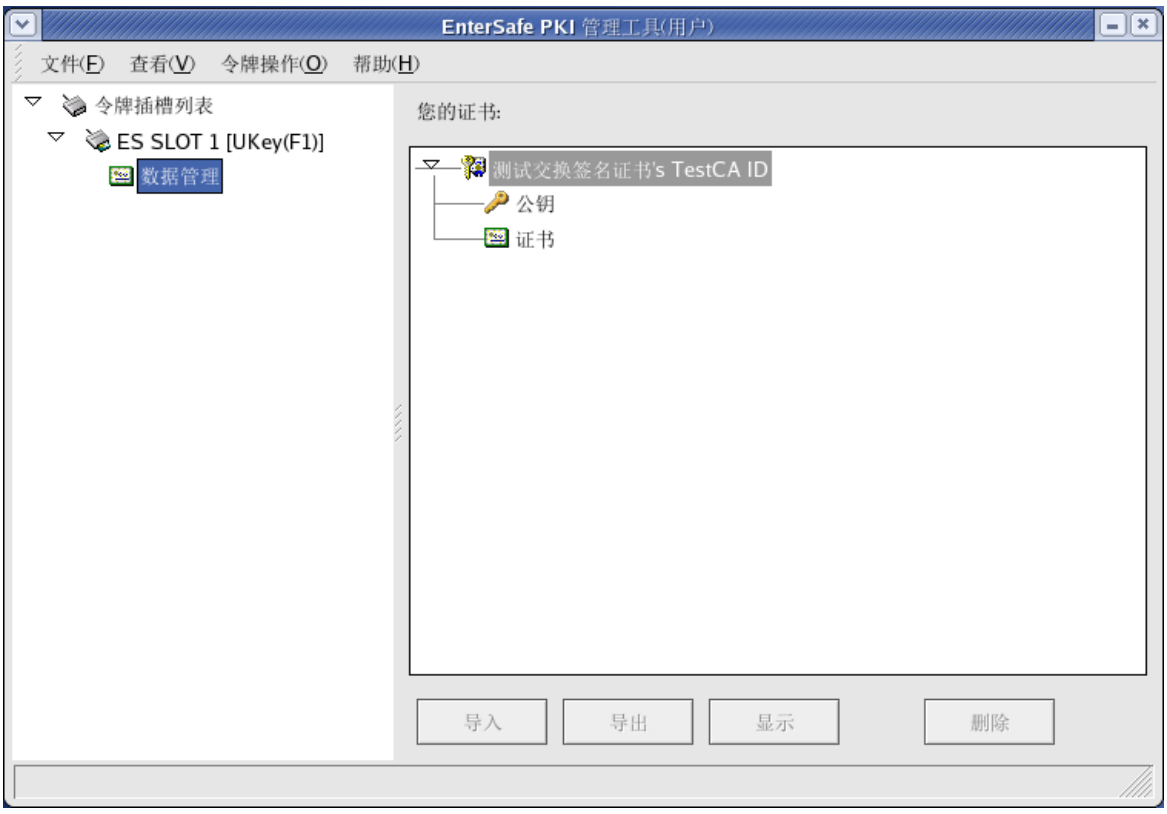

图 3-12

在“登录”的情况下，点击令牌的“数据管理”会出现如图 3-13 所示窗口，显示 UKey 的所有信息，导入证书功能的“导入”按钮也会变为可点击的状态：

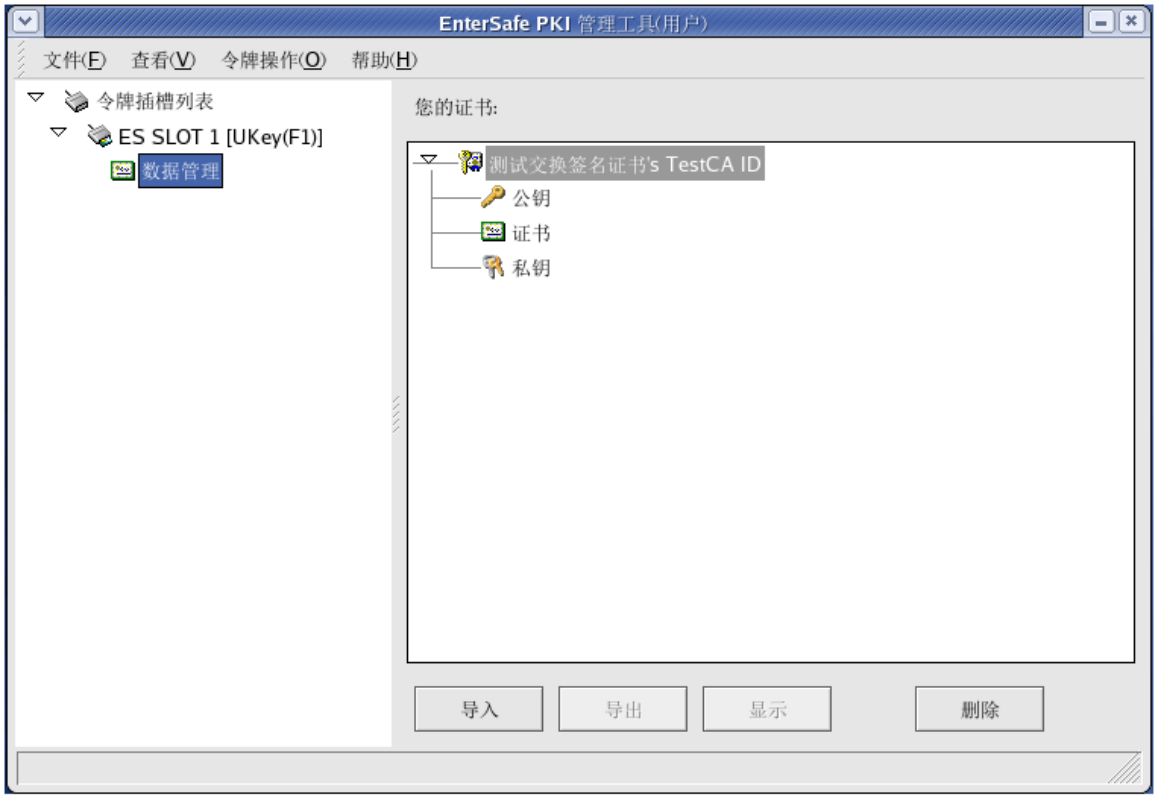

图 3-13

3.4.6 查看详细信息

如需要查看证书、证书公钥、证书私钥或者其他对象的详细信息，可以选中该对象，如果选择的是证书，然后点击“显示”按钮，会弹出如图 3-14 所示窗口：

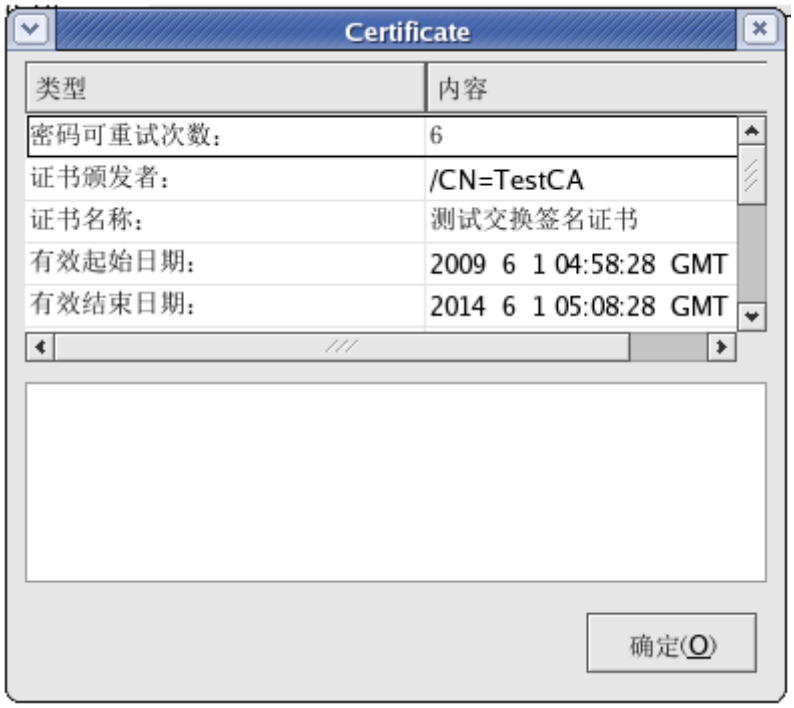

图 3-14

如果选择的是其它对象（如证书的公钥或者证书的私钥），则会弹出图 3-15 所示窗口：

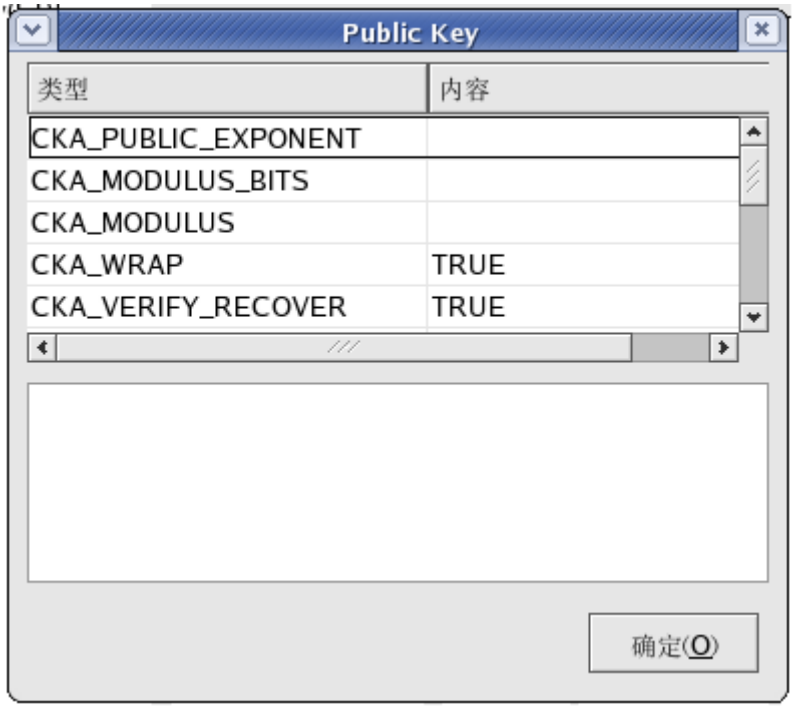

图 3-15

3.4.7 导入证书

当您需要导入证书时（支持 PFX、P12、P7B、CER、CRT 格式的证书），点击“导入”按钮，会弹出如图 3-16 所示窗口：

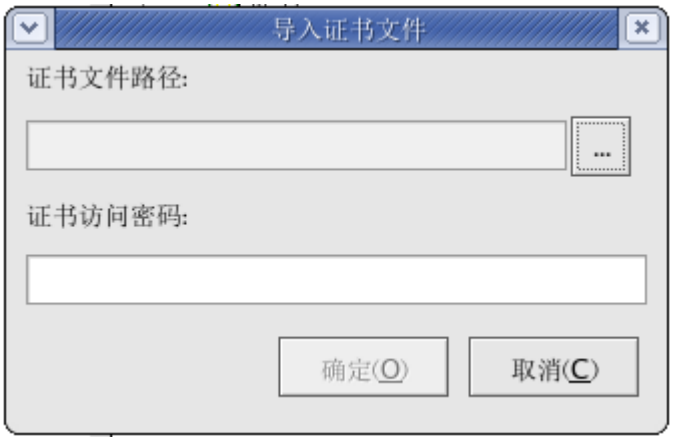

图 3-16

证书为 PFX 或者 P12 格式时才需要输入“证书访问密码”，导入其他格式的证书时管理工具会忽略该输入参数，点击 ... 按钮选择您需要导入的证书，并输入正确的“证书访问密码”，再点击“确定”按钮，管理工具会导入证书并显示新证书的信息，如图 3-17 和图 3-18 所示：

图 3-17

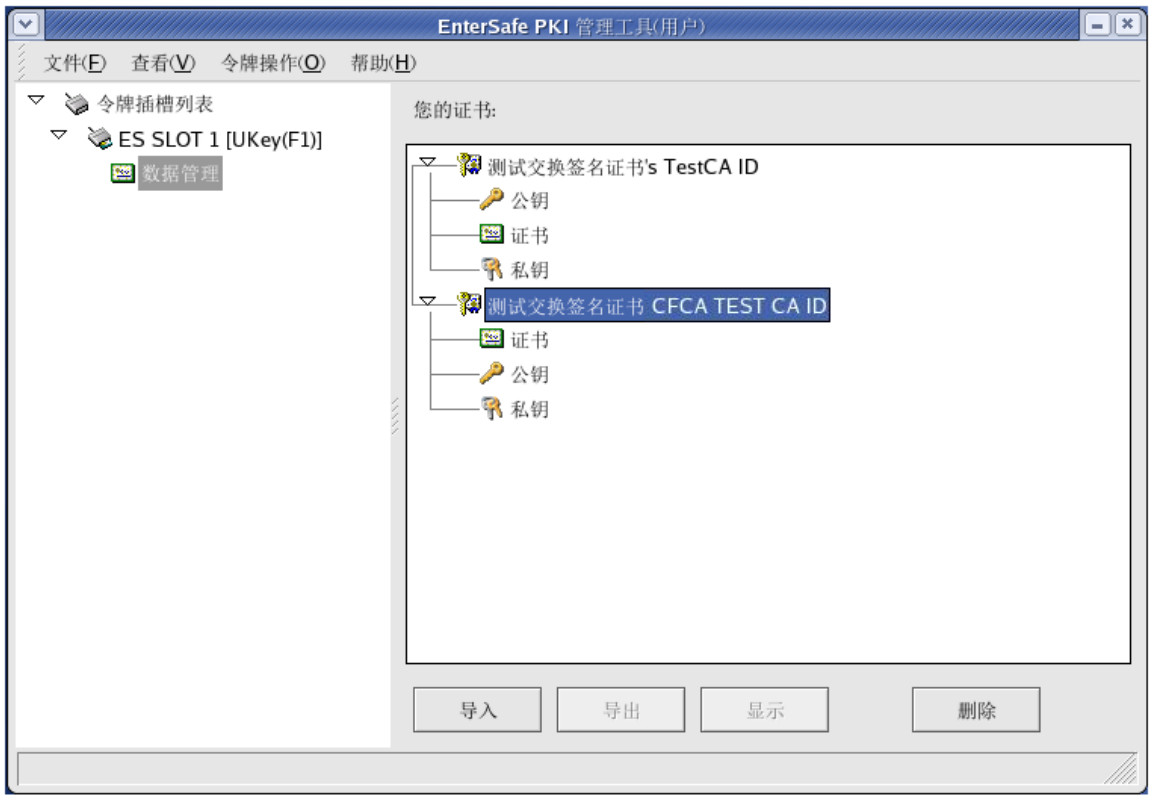

图 3-18

3.4.8 导出证书

但需要导出证书时，请选中需要导出的证书，然后点击“导出”按钮，会出现如图 3-19 所示窗口：

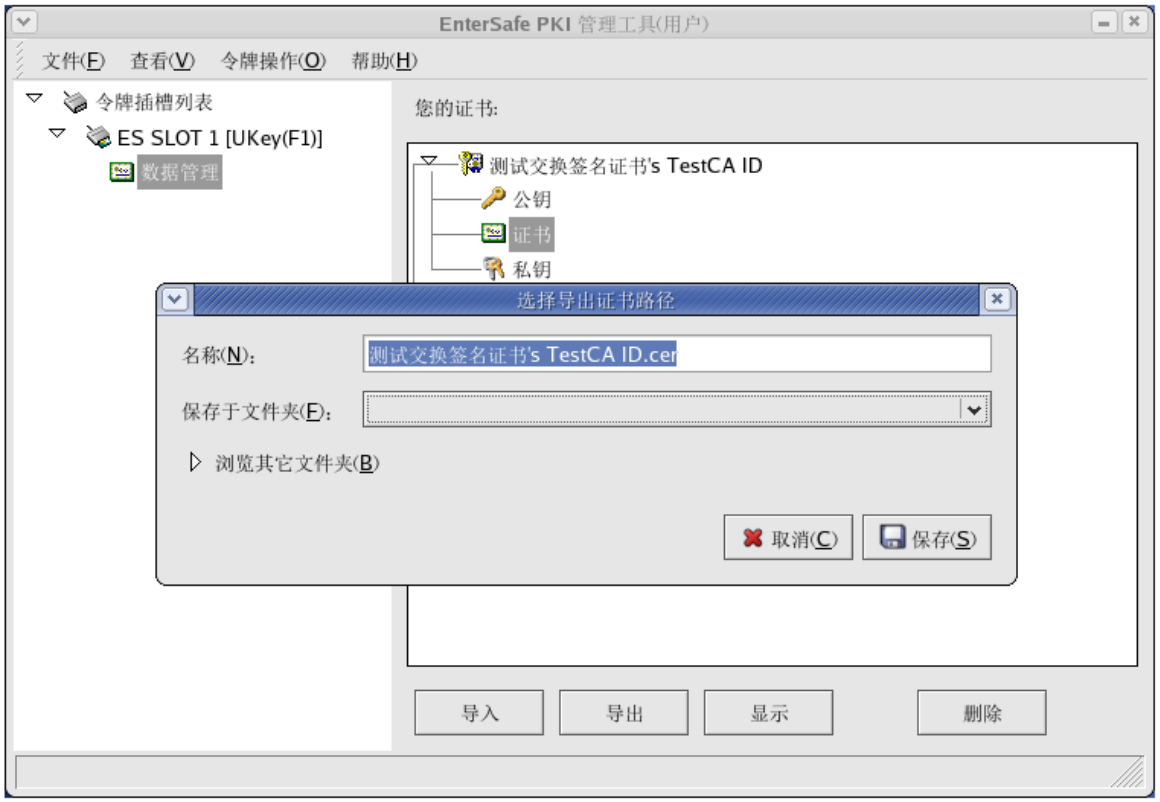

图 3-19

在设置完导出证书的保存路径和文件名称后，点击“保存”按钮完成该操作。

3.4.9 删除证书

当需要删除 UKey 中存储的数据时，在“登录”后进入“数据管理”界面，选择需要删除的对象，然后点击“删除”按钮，工具将弹出图 3-20 所示窗口：

图 3-20

选择“是”会删除指定的数据对象，数据对象删除后无法恢复，请谨慎操作。

3.5 注意事项

- ✓ 第一次使用移动数字证书时，请立即修改用户密码，不要使用默认密码。
- ✓ 请牢记您的移动数字证书密码，不要透露给其他人。
- ✓ 每次使用完移动数字证书后，请从电脑上拔下来，并及时收妥。
- ✓ 请妥善保管好您的移动数字证书，勿借给他人使用；如有遗失，请立即与移动数字证书颁发机构联系。

4. 软件卸载

- ✓ 如果您是在管理员用户下使用 UKey，并且没有运行过“sh <解压文件所在目录>/config/config.sh”，则无需进行卸载，直接删除“<解压文件所在目录>”即可。
- ✓ 如果您是在非管理员用户下使用 UKey，并且运行过“sh <解压文件所在目录>/config/config.sh”，则需运行“sh <解压文件所在目录>/config/unconfig.sh”进行卸载，然后再删除“<解压文件所在目录>”。

5.常见问题

1. 什么是移动数字证书(UKey)？为什么要使用移动数字证书？

移动数字证书(UKey)是一种智能存储设备，可存储数字证书；证书硬件内有 CPU 芯片，可进行密码运算；外形小巧，可插在电脑的 USB 接口中使用。

数字证书如果存储在电脑硬盘中，则证书私钥很容易被复制、窃取，安全性差；数字证书如果存储在移动数字证书中，则证书私钥无法复制、导出，即使电脑中了木马病毒，也不会被窃取，安全性非常高。

2. 移动数字证书有什么优点？

（1）安全性高：

- 可有效防止黑客或他人盗取证书。证书一旦下载到移动数字证书中，证书私钥无法复制、导出，因此黑客无法窃取。
- 移动数字证书有密码保护机机制且密码连续输错次数超过 6 次，移动数字证书会自动锁死，必须要解锁后方可继续使用。
- 证书存放在移动数字证书中，不受电脑硬盘格式化、重装系统等的影响，可有效防止证书损毁和丢失。

（2）使用方便：

- 体积小，重量轻，可随身携带。
- 具有自动打开指定网站功能：每次移动数字证书插入电脑时，将会自动打开 IE 浏览器并且打开设置的网站，无需用户手工输入网址，使用方便、快捷。
- 具有自动提示关闭 IE 浏览器功能：每次移动数字证书拔出电

脑时，如果存在打开的 IE 浏览器窗口，将会自动弹出提示是否关闭 IE 浏览器的窗口，无需用户手工关闭 IE 浏览器窗口，使用方便、快捷。

3. 移动数字证书的初始密码是什么？

移动数字证书的初始密码默认为“111111”。

4. 如何查看移动数字证书内证书？

可以通过移动数字证书的 UKey 管理器查看，具体方法为：打开 UKey 管理器，选择证书，点击“查看证书信息”按钮，就可以查看该证书的详细信息。

5. 移动数字证书是 U 盘吗？

不是。移动数字证书外观虽然和 U 盘差不多，都是插在电脑的 USB 接口中使用，但两者还是有很大区别：

（1）两者的作用不同。U 盘是用来存储数据的，因此容量都比较大，从几百 MB 到几 GB；而移动数字证书属于智能存储设备，主要用于存放数字证书，并可以进行密码运算，一般容量较小，只有几十 KB。

（2）U 盘中的数据可随意进行读写、复制，而数字证书一旦存放在移动数字证书中，则证书私钥无法被复制、导出，可有效防止证书被他人复制窃取，安全性非常高。

（3）移动数字证书中有 CPU 芯片，可进行密码运算，而 U 盘无此功能。

6. 移动数字证书上的灯闪烁，是否说明移动数字证书在工作？

当您把移动数字证书插入电脑后，操作系统会识别硬件。识别后，移动数字证书上的灯应该是常亮的。如果移动数字证书上的灯不亮，说

明系统未识别到硬件，您需要重新插入移动数字证书，如果灯仍然不亮，则可能为移动数字证书损坏。

当您在使用移动数字证书进行证书申请或数据提交等操作时，移动数字证书会进行加密、签名等工作。此时移动数字证书上的灯也会不断闪烁，表明移动数字证书在正常工作；不再闪烁时，表明工作完成。

7. 何种情况下，移动数字证书会被锁定？

用户反复尝试移动数字证书的用户密码，超过次数限制会被锁定。

6. 软件版本

（1）Setup (32 bit) version information

Version No.: 1.0.0 2010-07-20

Version Name: EnterSafe Shuttle SDK For Linux

Release Date: 2010-7-20

File Name: EnterSafe-Shuttle-1.0.100720_32_RHAS.tar.gz

（2）Setup (64 bit) version information

Version No.: 1.0.0 2010-07-20

Version Name: EnterSafe Shuttle SDK For Linux

Release Date: 2010-7-20

File Name: EnterSafe-Shuttle-1.0.100720_64_RHAS.tar.gz

7.硬件规格

硬件型号	SJK1104
型号代码	F2
用户的存储空间	64KB
数据保存期限	≥ 10 年
存储器重写次数	≥ 10 万次
电源	2.7 ～ 5.5 V，支持低功耗模式
工作时钟频率	48M Hz
工作温度	0℃ ～ 70℃
存放温度	-25℃ ～ 85℃
工作湿度	0% ～ 90% （不冷凝）
指示灯	具有 LED 灯，用于电源指示和通讯指示
抗静电特性	ESD ＞ 4000V
连接接口	USB A 型接口，标准 USB 2.0 接口，支持 USB 1.1 接口
传输速率	全速（≥ 12 Mbps）
COS 体系	支持 ISO7816-4/5/6/8/9 标准规范
支持算法	RSA（1024 位/2048 位）、DES/3DES、国密 SM2 算法、SHA-1
支持中间件	CSP 中间件、PKCS#11 中间件

硬件真随机数发生器	支持
数据存取速度(读操作)	≥ 20 Kbps
数据存取速度(写操作)	≥ 10 Kbps
密码算法：非对称加密算法	支持 RSA 1024/2048 算法
RSA1024 公私钥对产生时间	3433ms （平均时间）
RSA1024 解密/签名运算时间	≤ 1887ms（2K 数据）
RSA1024 加密/验证运算时间	≤ 167ms（2K 数据）
RSA2048 公私钥对产生时间	20276ms（平均时间）
RSA2048 解密/签名运算时间	≤ 3668ms（2K 数据）
RSA2048 加密/验证运算时间	≤ 134ms（2K 数据）
密码算法：对称加密算法	支持 DES/3DES 算法（硬件）
DES/3DES 加密/解密速度	≥ 100Kbps
DES/3DES 算法持续工作可用性	≥ 99.99%
RSA 算法持续工作可用性	≥ 99.99%
通电持续工作可用性	≥ 99.99%