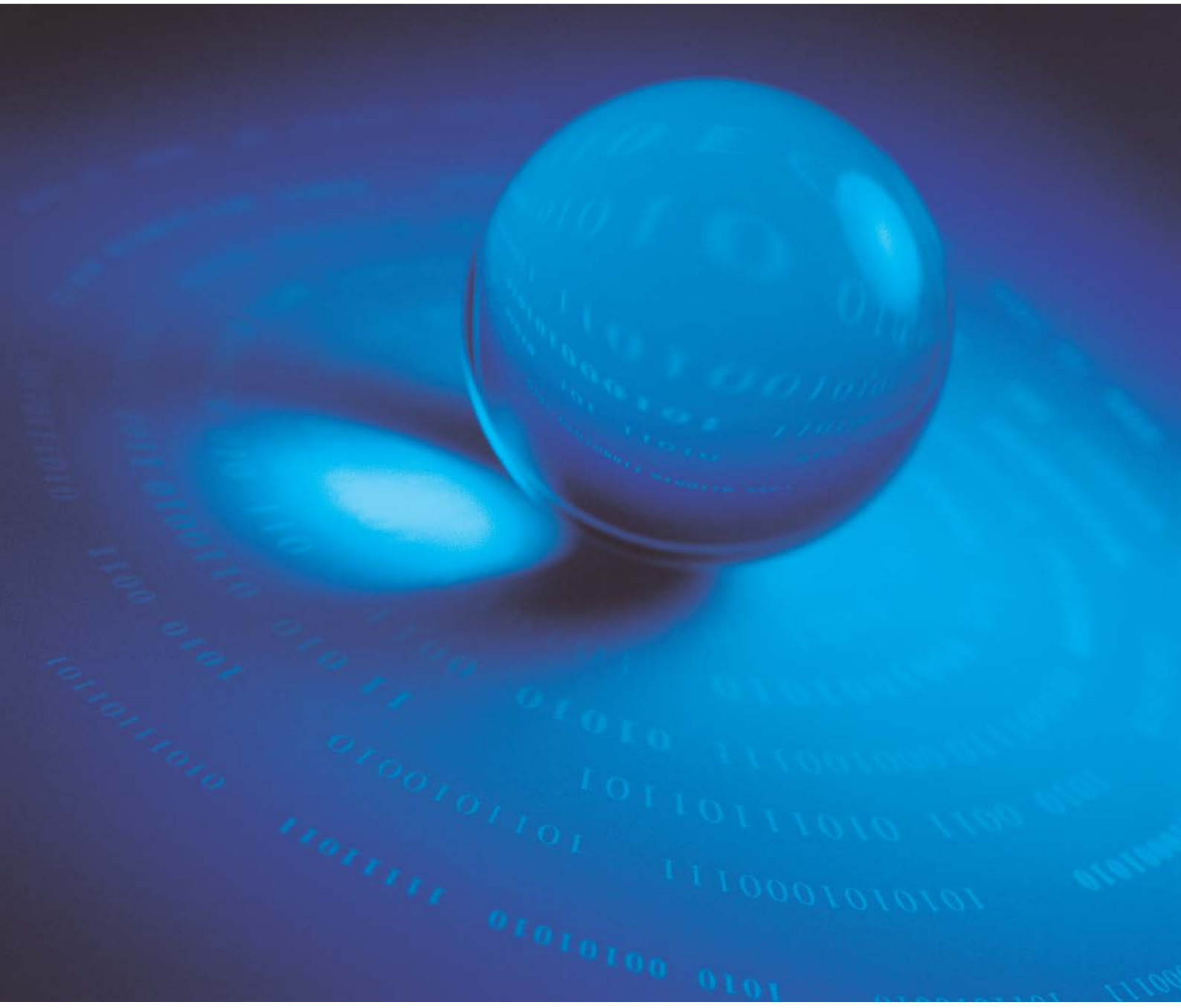
ePass3003 用户手册

1.2 版



http://www.EnterSafe.com

EnterSafe 尽最大努力使这篇文档中的内容完善且正确。EnterSafe 对于由这篇文档导致的任何形式的直接或间接损失不负有责任。这篇文档的内容会跟随产品的升级而有所变化。

修改记录：

日期	版本	说明
2007 年 1 月	1.0	第一版
2008 年 1 月	1.1	第一版第一次修订
2009 年 5 月	1.2	第一版第二次修订

EnterSafe
软件开发协议

本《软件开发协议》（以下简称《协议》）是用户（个人或者单一机构团体）与 EnterSafe 之间有关随附本《协议》的 EnterSafe 软件产品的法律协议。本软件产品包括计算机软件，并且还可能包括电子文档、相关媒体和印刷材料（以下简称“软件产品”）。您一旦安装、复制或以其他方式使用本“软件产品”，即表示您同意接受本《协议》中的条款的约束。如果您不同意本《协议》中的条款，则您不得安装、复制或以其他方式使用本“软件产品”；您可以将本“软件产品”退还原购买处并取得全额退款。

1.软件产品使用许可

如果您遵守本协议的条款，EnterSafe 将授予您协议中所述的权利。

1.1 EnterSafe 授予您作为个人的、非独家性的许可证，仅供您为用于设计、开发及测试您的设计以及与任何 EnterSafe 产品一起运行的软件产品。您可在无数量限制的计算机上安装本“软件产品”的副本，但您必须是本“软件产品”的唯一使用者。如果您为一个机构团体，EnterSafe 授予您指定您组织内一位人员依以上所规定的方式使用本“软件产品”的权力。

1.2 EnterSafe 允许您将本软件合并或链接到您的计算机程序中，但本软件产品中被合并或链接的部分仍受本协议的约束。

1.3 您可以以存档为目的复制合理数量本软件产品的副本;但如果 Entersafe 通过公开声明或发布新闻的形式终止软件副本的使用，您必须马上遵守这个要求。

2.反向工程、反向编译、反汇编的限制

您不可以对本“软件产品”的部分或全部进行反向工程、反向编译或反汇编；尽管有这项限制，如果适用法律明示允许上述活动，则不在此限制范围。

3.禁止租借、传播或商业主办服务

您不可出租、租赁或出借本“软件产品”；或将本“软件产品”放在服务器上传播；或利用本“软件产品”提供商业主办服务。

4.责任限制和补救措施

无论任何原因（包括但不限于上述所有直接规定或一般性的合同规定或其它情况）发生的损害，EnterSafe 与其供应商在本协议条款下的所承担的全部责任以及全部损害的唯一补偿，不超出您购买本“软件产品”所支付的款额。

5.免责声明

在适用法律所允许的最大范围内，EnterSafe 或其供应商按“现有状况且包含所有错误”提供本“软件产品”或支持服务（如果有），并声明不承担所有其他明示、隐含或法定的担保、责任和条件。其中包括但不限于下列任何担保、责任或条件（如果有）：适销性、对于特定目的的适用性、可靠性或可用

性、回应的准确性或完整性、结果或工艺的精良性、无病毒以及无疏忽；还包括通过本“软件产品”或因使用本“软件产品”而提供或未提供支持服务或其他服务、信息、软件和相关内容。用户对本“软件产品”没有所有权、不受干扰的使用权、不受干扰的占有权、与说明一致或不侵权的任何保证或条件。

6.版权所有

EnterSafe 保留所有本《协议》中未明确授予您的权利，本“软件产品”受版权和其它知识产权法及相关条款的保护。EnterSafe 拥有本“软件产品”的所有权、版权和其他知识产权。

7.协议终止

本《协议》在终止前有效。若您违反本《协议》的任何条款，使用本“软件产品”的权利将自动终止。本“软件产品”必须被销毁或返回 EnterSafe。您可以销毁本“软件产品”及其所有副本以终止协议。但条款 2，3，4，5，6 将继续有效。

CE Attestation of Conformity

The equipment complies with the principal protection requirement of the EMC Directive (Directive 89/336/EEC relating to electromagnetic compatibility) based on a voluntary test.

This attestation applies only to the particular sample of the product and its technical documentation provided for testing and certification. The detailed test results and all standards used as well as the operation mode are listed in

Test standards: EN 55022/1998 EN 55024/1998

After preparation of the necessary technical documentation as well as the conformity declaration the CE marking as shown below can be affixed on the equipment as stipulated in Article 10.1 of the Directive. Other relevant Directives have to be observed.

FCC certificate of approval

This Device is conformance with Part 15 of the FCC Rules and Regulations for Information Technology Equipment.

USB

This equipment is USB based.

WEEE

Dispose in separate collection.

章节目录

图目录

第一章 ePass3003 管理工具的使用

1.1 前提

因为管理工具基于 ePass3003 的中间件之上并且要访问硬件 Token，所以在使用 ePass3003 的图形界面管理工具之前，您必须在您的计算机上正确安装了 ePass3003 产品。

在使用 ePass3003 之前必须对其进行 PKI 初始化。默认情况下出厂的 ePass3003 都是经过 PKI 初始化的。

注意：如果您使用的是 ePass3003 Auto 产品，将 ePass3003 Auto 插入您计算机的 USB 接口中，ePass3003 Auto 能够在您的计算机上自动安装运行该 Token 的中间件，无须手动安装。

1.2 概貌

1.2.1 未插入 USBKey 的界面

您可以在“开始”—〉“所有程序”—〉“EnterSafe”—〉“ePass3003”中找到管理工具的快捷方式，点击管理工具的快捷方式启动管理工具，出现界面如图 1 所示：

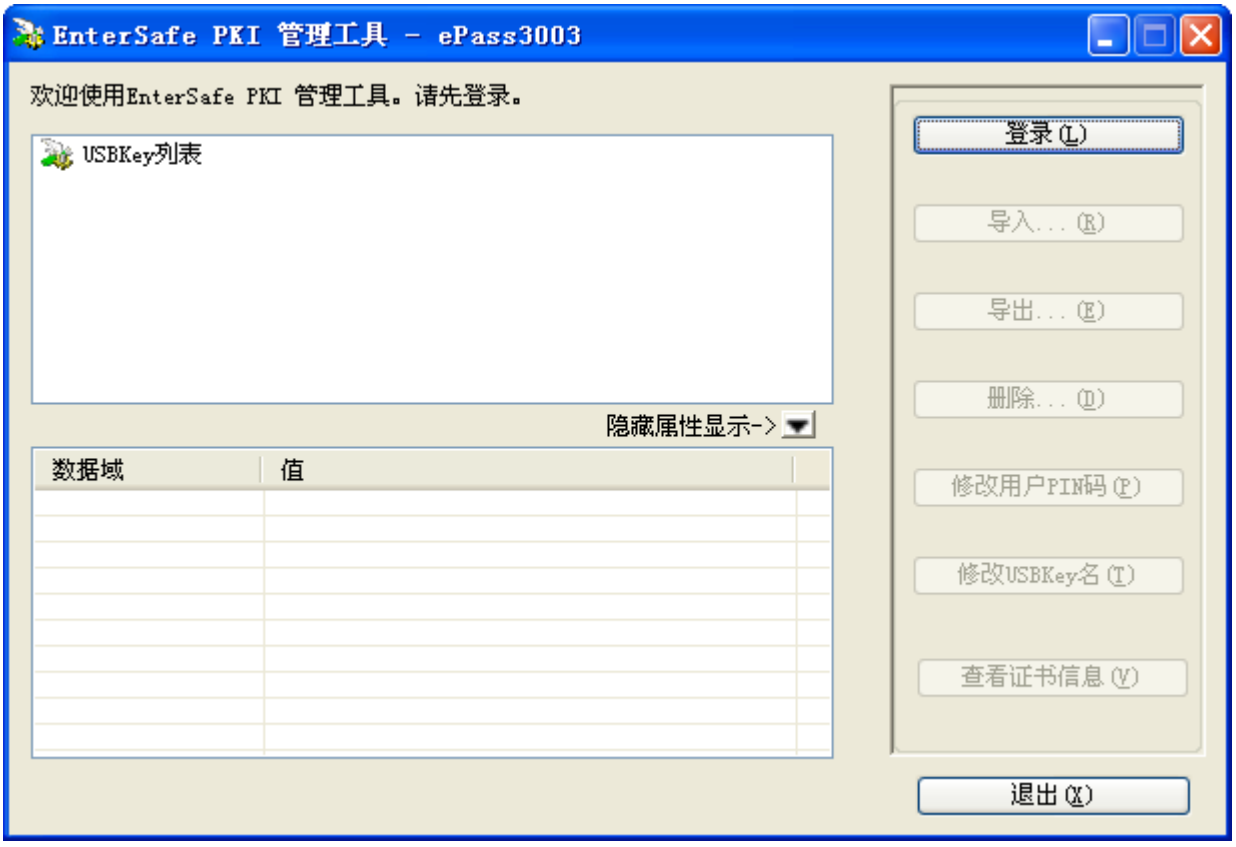


图 1 未插入 USBKey 时管理工具的界面

1.2.2 插入 USBKey 的界面

现在在您计算机的 USB 接口中插入一个名称为“ePass3003”的 USBKey，那么管理工具就能自动识别出这个 USBKey 的基本信息，并且会呈现出如图 2 所示的界面：

图 2 插入 USBKey 时管理工具的界面

1.2.3 管理工具的按钮

管理工具的按钮包括：“登录”、“导入”、“导出”、“删除”、“修改用户 PIN 码”、“修改 USBKey 名”、“查看证书信息”和“退出”，如图 2 右侧所示的按钮。

1.3 登录

在管理工具主界面 USBKey 列表中选择想要登录的 USBKey，然后点击“登录”按钮，弹出 PIN 码输入框，如图 3 所示：

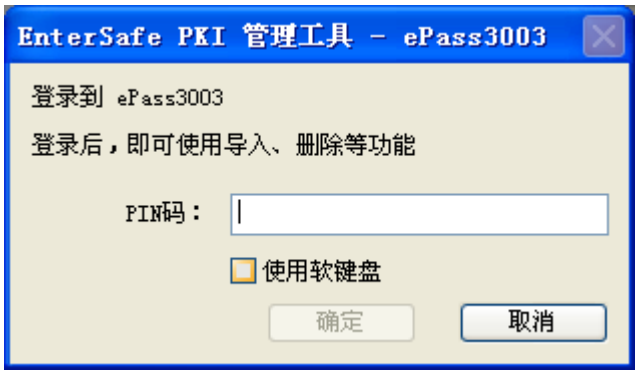


图 3 登录对话框

在此用户可以通过勾选“使用软键盘”复选框来使用软键盘输入 PIN 码以避免木马程序对用户输入的 PIN 码的监控，如图 4 所示：

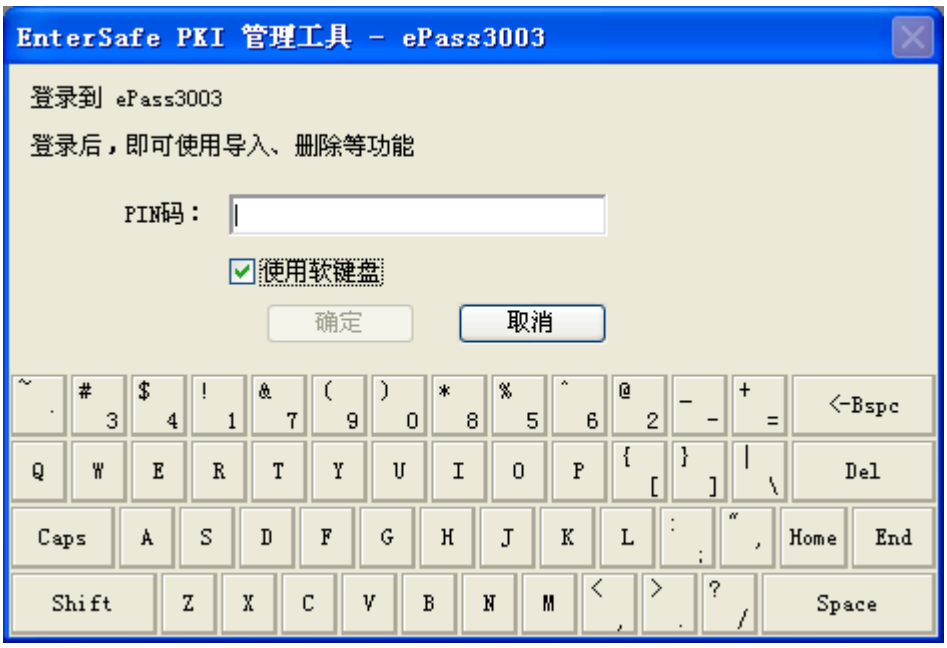


图 4 PIN 码输入框——使用软键盘

注意：选择“使用软键盘”后，物理键盘的键盘输入将被禁用。

用户输入正确的 PIN 码并点击“确定”按钮后，进入如图 5 所示的界面，在界面的上半部显示 USBKey 列表，用户可以点选树型列表内的项目，界面的下部会显示用户点选项目的相应属性值。用户可以通过点击“隐藏属性显示”按钮或“查看属性显示”按钮来隐藏属性显示或展开属性显示。用户登录后，不仅可以查看 USBKey 中的公有数据的信息，还可以查看到 USBKey 里私有数据的信息。用户登录后，“登录”按钮显示为“登出”，您可以点击“登出”按钮，安全登出 ePass3003。

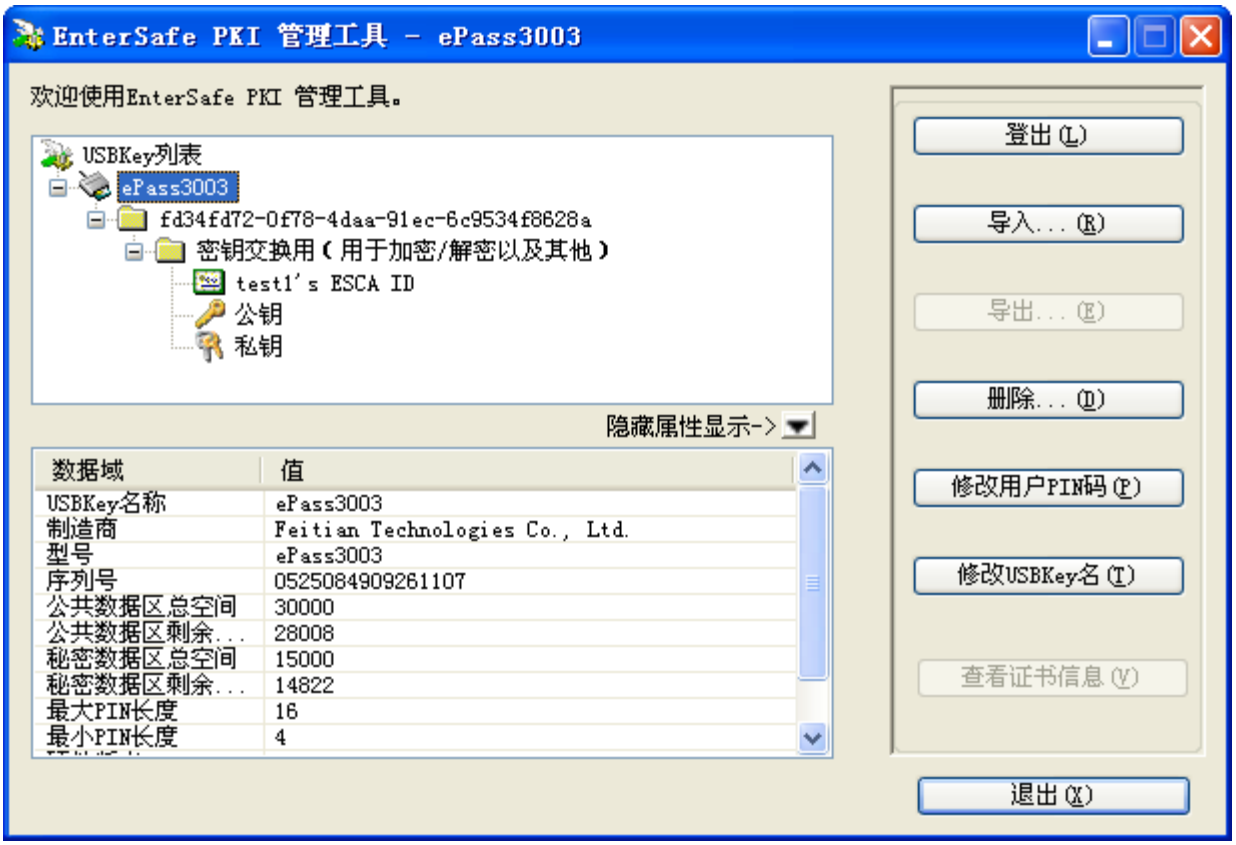


图 5 登录后的界面

如果用户输入的 PIN 码错误，则会弹出图 6 所示的提示框，提示您的 PIN 码输入错误，点击“是”按钮返回图 3 所示的登录对话框，继续登录，点击“否”按钮，退出登录。

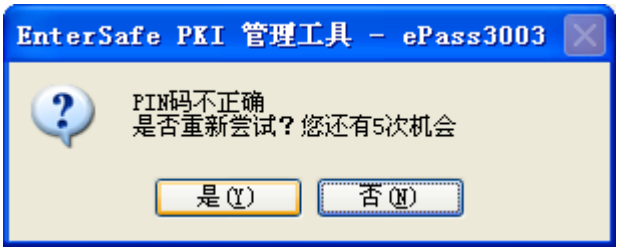


图 6 密码输入错误提示框

注意：ePass3003 对用户 PIN 码的误输入次数有限制，如果您连续累计 6 次错误输入 PIN 码，USBKey 将被锁定，锁定后您将不能对 USBKey 做任何操作。

1.4 证书管理

用户登录到 ePass3003 后就可以对其进行查看证书信息、导入证书、删除证书数据等操作。

1.4.1 查看证书信息

1. 在 USBKey 列表中点击容器（文件夹图标）左侧的“+”或双击图标以显示容器内的内容；点击证书图标左侧的“+”以显示证书包含的公私钥对。选中证书，此时“查看证书信息”按钮变为可用，如图 7 所示：

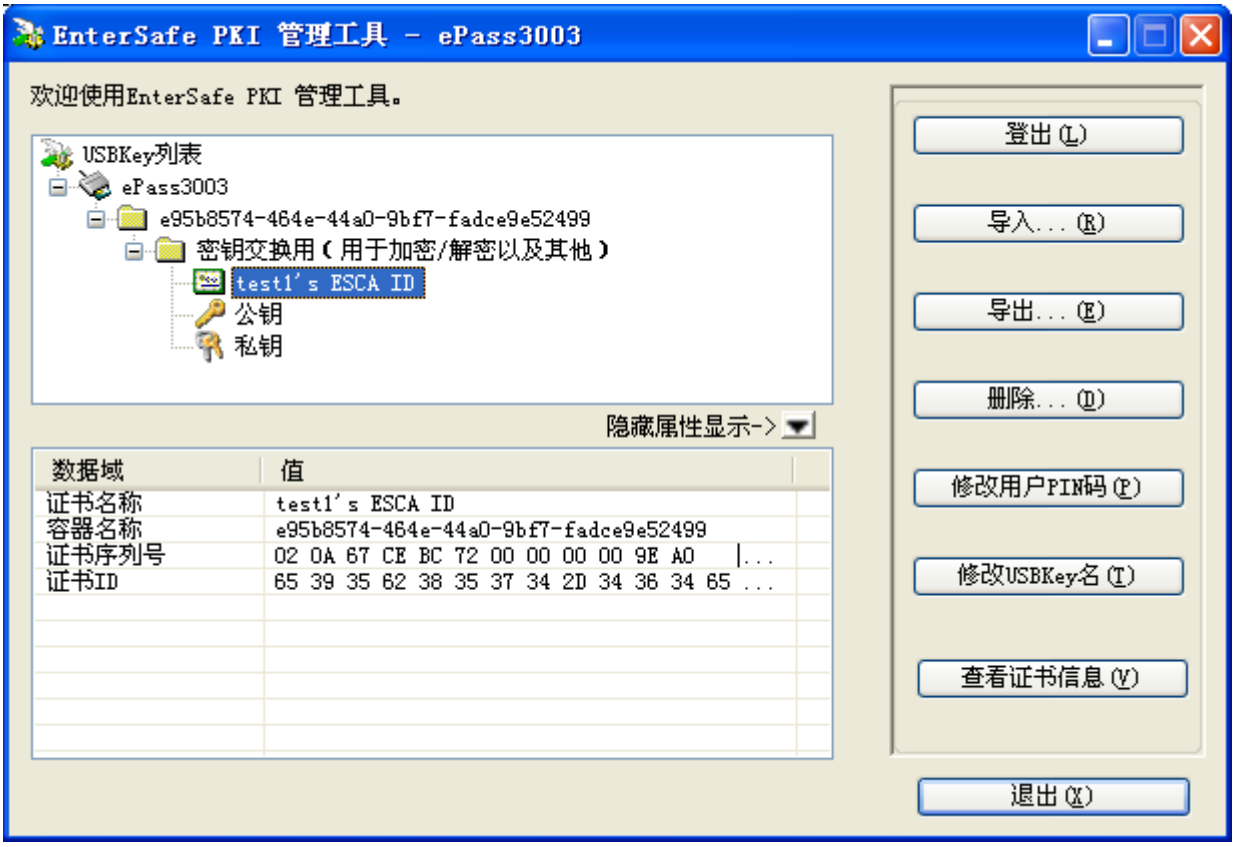


图 7 查看证书信息界面

2. 点击“查看证书信息”按钮或双击证书图标，弹出查看证书信息对话框，用户可以点选“常规”、“详细信息”和“证书路径”选项卡来查看证书的信息，如图 8 所示：

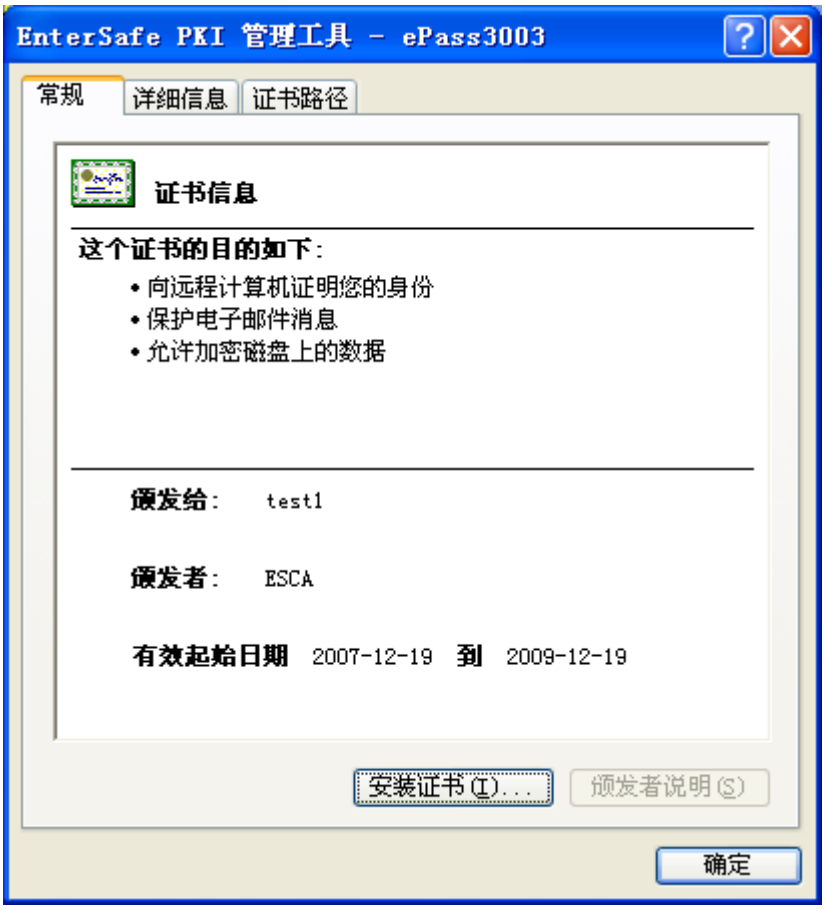


图 8 查看证书信息对话框

1.4.2 导入

目前 ePass3003 支持的证书类型包括：P12、PFX、P7B、CRT 和 CER 五种类型，其中 P12 和 PFX 类型的证书含有公私钥对，P7B、CRT 和 CER 类型的证书不包含公私钥对。下面以导入 PFX 和 CER 类型的证书为例进行说明。

1.4.2.1 导入 PFX 证书

在管理工具主页面点击“导入”按钮，显示如图 9 所示的界面，点击“浏览”按钮，选择要导入的 PFX 证书的路径，如证书设置了访问密码，还需在“证书访问密码”文本框中输入密码，用户可以新建一个容器来存储导入的证书，也可以使用已有容器，由于 PFX 类型的证书含有公私钥对，所以既可以用来交换也可以用于签名，用户选择一个证书的用途，完成上述设置后点击“确定”按钮即可完成证书的导入。

注意：同一个容器中只能同时保存两个不同用途的证书，如果将一个证书导入已经存在的容器内，则管理工具会提示替换原有相同用途的证书，如果原有证书与导入的证书用途相同则原有证书将被替换。

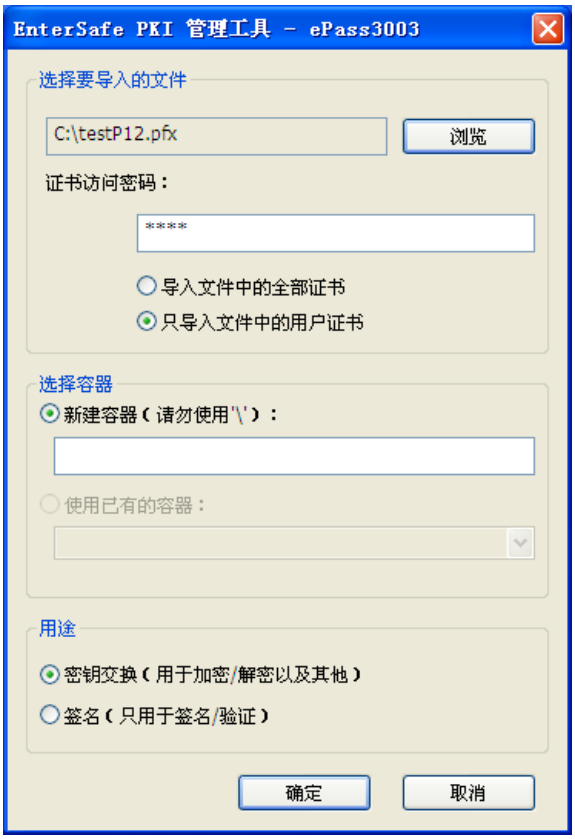


图 9 证书导入界面

1.4.2.2 导入 P7B 证书

在管理工具主页面点击“导入”按钮，显示如图 10 所示的界面，点击“浏览”按钮，选择要导入 P7B 证书的路径，用户需新建一个容器来存储导入的证书，由于 P7B 类型的证书不包含公私钥对，只能用于交换，所以“证书用途”部分的单选按钮为不可选状态，完成上述设置后点击“确定”按钮即可完成证书的导入。

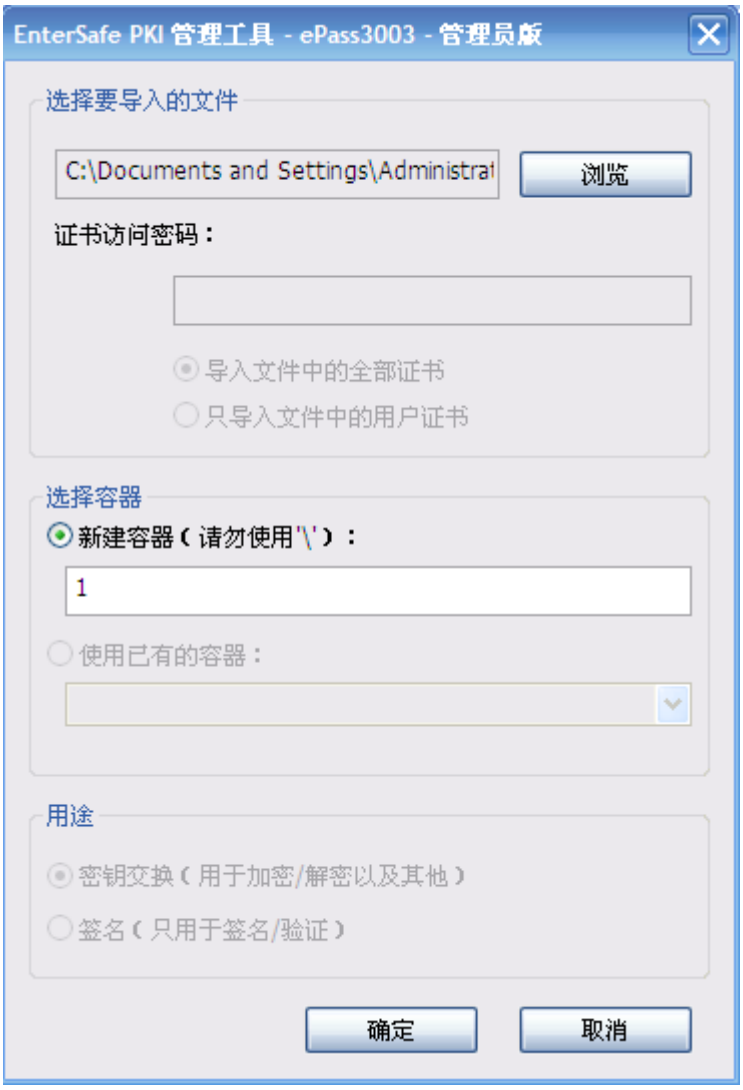


图 10 证书导入界面

1.4.3 导出

用户可以使用管理工具将 USBKey 中的证书导出并保存成文件，导出证书的方法如下：

在管理工具主页面的树形列表中选择要导出的证书，并点击“导出”按钮，弹出选择导出路径对话框，选择要保存证书文件的路径并设置证书文件的名称，如图 11 所示：

图 11 选择证书导出路径对话框

点击“保存”按钮，如果导出成功则弹出如图 12 所示的对话框：

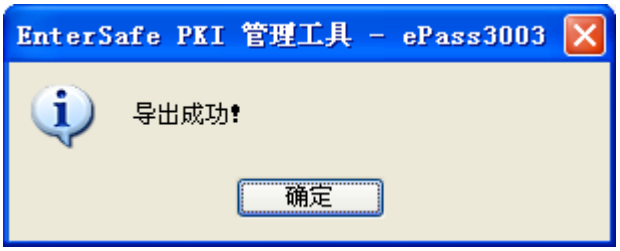


图 12 导出成功对话框

注意：管理工具只能导出证书，证书对应的公私钥对无法导出。

1.4.4 删除

1. 在管理工具主页面的树形列表中选择要删除的证书，并点击“删除”按钮，弹出如图 13 所示的对话框：

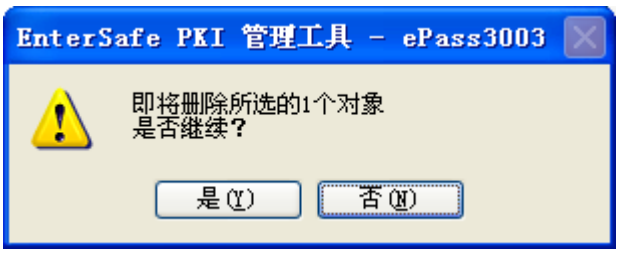


图 13 删除证书

2. 点击“是”按钮，确认删除所选的证书。

用户可以用同样的方法删除 ePass3003 内的密钥或容器，您只需将鼠标点击在树形列表中您要删除的密钥或容器上，再点击“删除”按钮就可删除相应的密钥或容器。如果您点击树形列表中的“ePass3003” USBKey 名，再点击“删除”按钮，您将删除 ePass3003 中所有容器及容器内的证书和密钥。

1.5 修改 USBKey 名

一般情况下 USBKey 都是以序列号来相互区分的，但是序列号不直观而且不容易记，所以在 ePass3003 中以 USBKey 名称来标记 USBKey。USBKey 名可以根据自己的喜好任意命名。

1. 在管理工具主页面点击“修改 USBKey 名”按钮，弹出如图 14 所示的对话框：

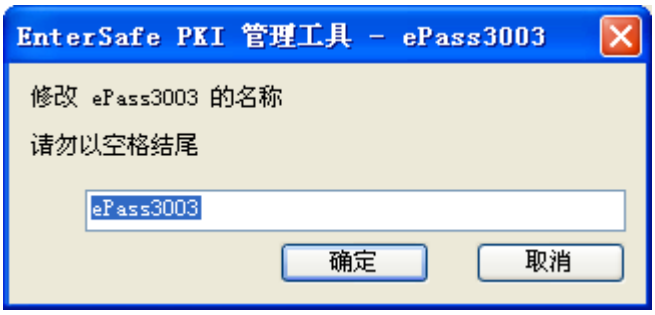


图 14 修改 USBKey 名

2. 在文本框内输入 USBKey 的名称后点击“确定”按钮，完成 USBKey 名的修改。

注意：USBKey 名称最大不能超过 32 个字符。

1.6 修改用户 PIN 码

您还可以对 USBKey 的 PIN 码进行修改，插入 USBKey 后点击管理工具主页面上的“修改用户 PIN 码”按钮，弹出如图 15 所示修改 PIN 码对话框，分别输入原 PIN 码和新 PIN 码并确认新 PIN 码后点击“确定”按钮，即可完成用户 PIN 码的修改。

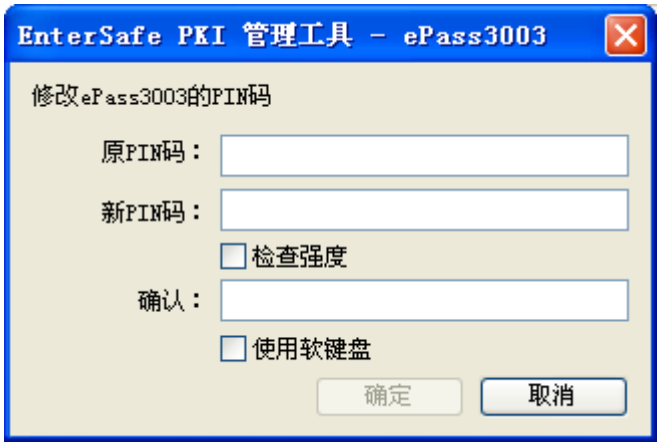


图 15 修改用户 PIN 码对话框

用户可以通过选择使用软键盘来避免木马程序对用户设置的 PIN 码的监控，如果用户选择 “使用软键盘”，修改用户 PIN 码对话框如图 16 所示：

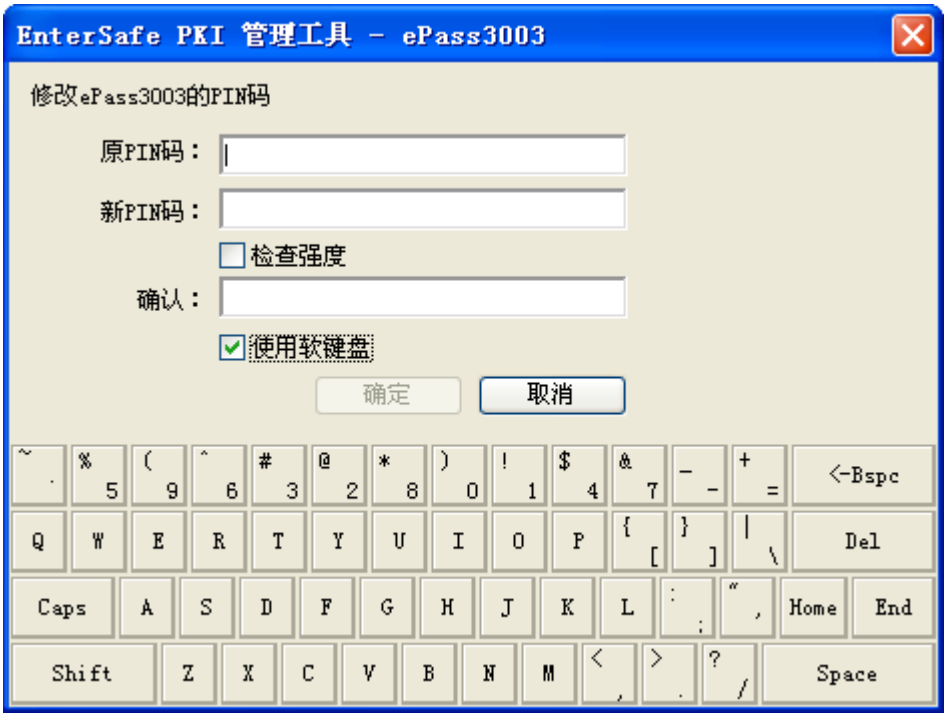


图 16 使用软键盘修改用户 PIN 码

用户还可以选择“检查强度”来检查设置的 PIN 码的安全强度，当设置的 PIN 码强度较低时管理工具会进行提示，如图 17 所示的红色圆点，其内有“低”字表示设置的 PIN 码强度较低。

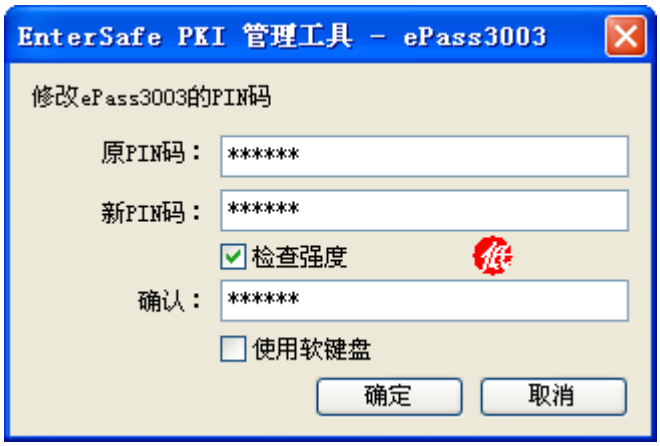


图 17 提示设置的 PIN 码强度低

当设置的 PIN 码强度较强时，会显示如图 18 所示的提示：

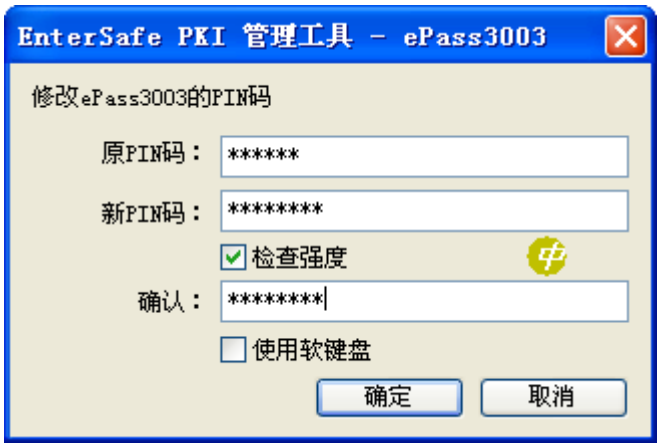


图 18 提示设置的 PIN 码强度为中等

建议您在设置时，PIN 码中尽量同时包含大小写字母、数字和特殊符号，并且在容易记忆的前提下尽量设置较长的 PIN 码，如图 19 所示：

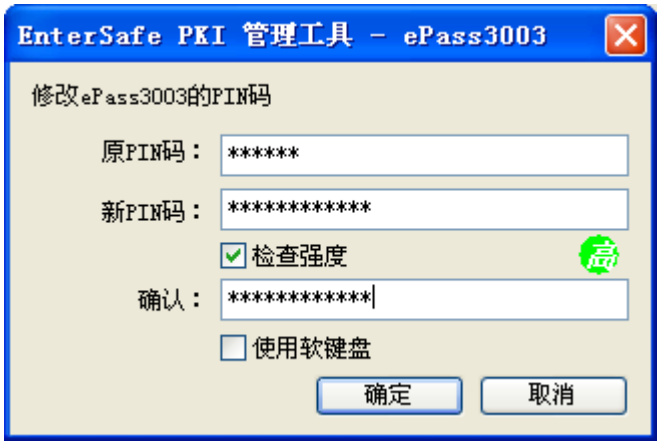


图 19 提示设置的 PIN 码强度高

在“原 PIN 码”栏内和“新 PIN 码”以及“确认”栏内输入相应的 PIN 码，点击“确定”按钮，弹出如图 20 所示的 PIN 码修改成功对话框，点击“确定”按钮，完成用户 PIN 的修改。

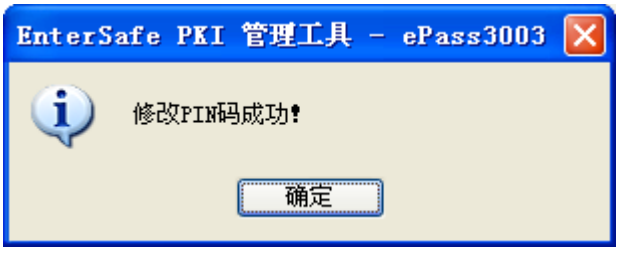


图 20 PIN 码修改成功

以上是以用户版管理工具为例对 ePass3003 管理工具使用方法进行的介绍，管理员版管理工具相应功能的使用方法与用户版管理工具的使用方法相同。下面将继续介绍管理员版管理工具的特殊功能。

管理员版管理工具的界面与用户版管理工具的界面稍有不同，在管理工具主界面的右侧按钮区有一个翻页按钮，点击这个翻页按钮能够使按钮进行前后换页，在图 21 中用红色圈出：

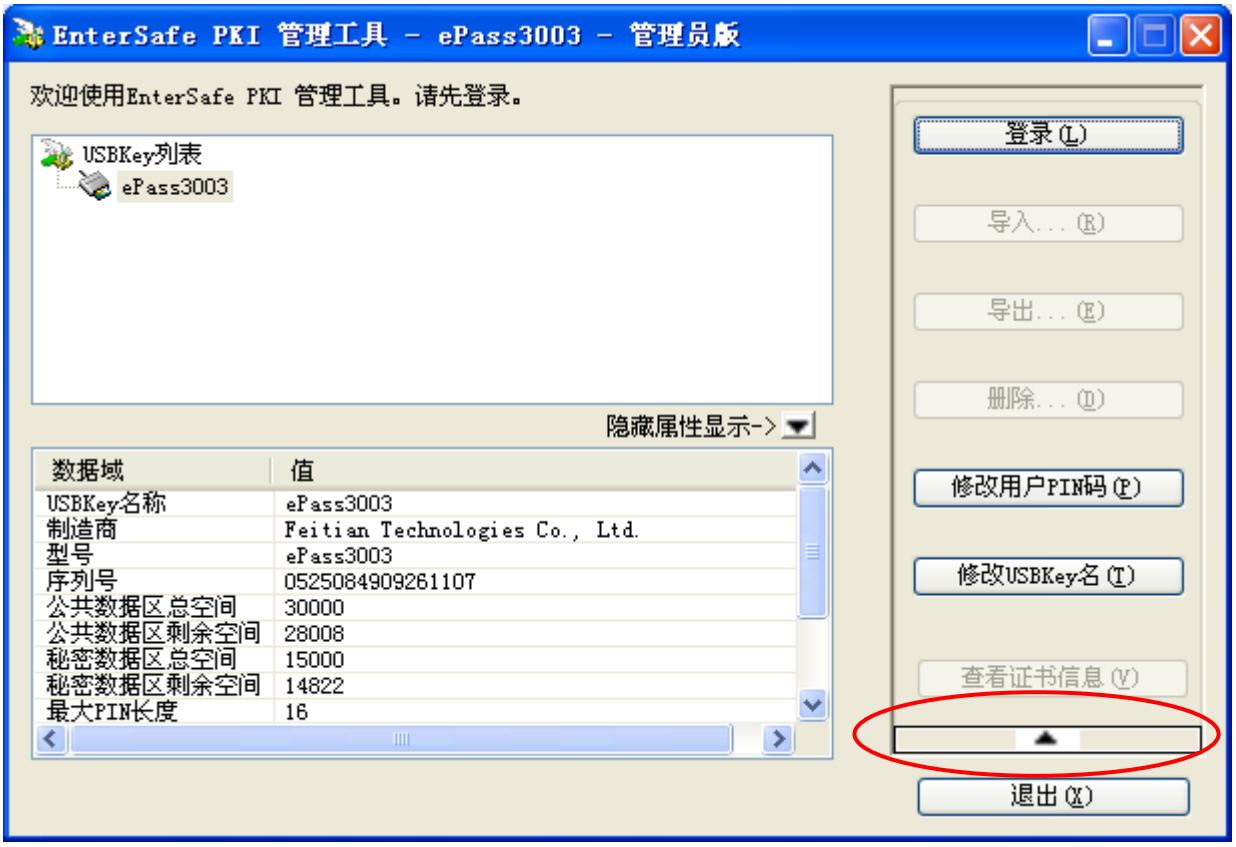


图 21 管理员版管理工具主页面 I

点击翻页按钮，以显示按钮的第二页，如图 22 所示：

图 22 管理员版管理工具主页面 II

1.7 解锁（仅限管理员版）

利用管理员版管理工具可以对由于误操作而锁定的 USBKey 进行解锁，解锁的方法如下：

在图 22 所示的管理工具主界面上点击“解锁”按钮，将弹出解锁对话框，如图 23 所示：

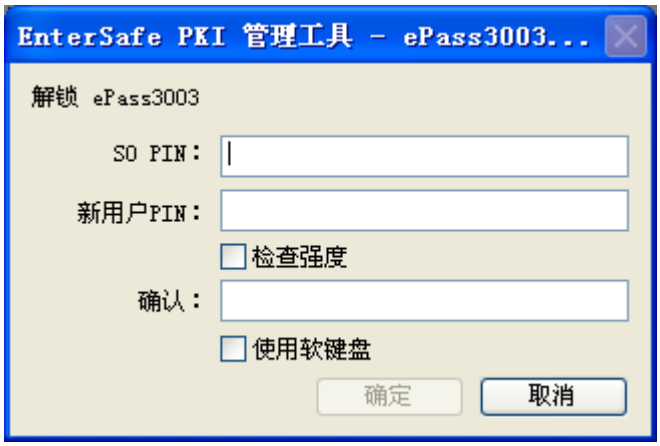


图 23 解锁对话框

用户可以通过选择“使用软键盘”来避免木马程序对用户输入和设置的 PIN 码的监控，如果用户选择 “使用软键盘”，解锁 USBKey 的对话框如图 24 所示：

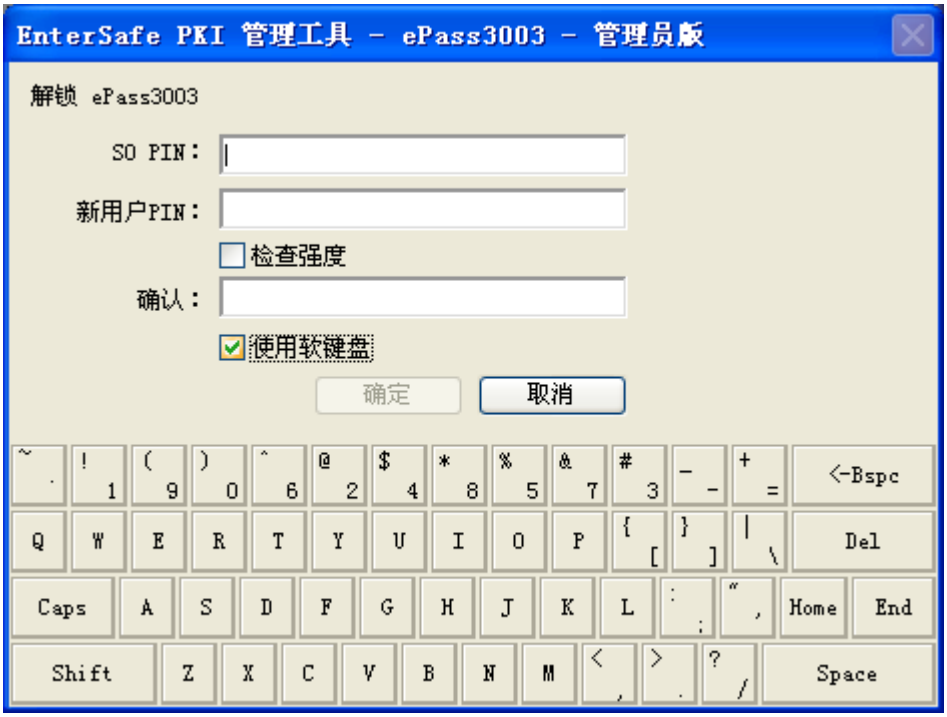


图 24 解锁对话框——使用软键盘

用户还可以选择“检查强度”来检查设置的 PIN 码的安全强度，具体使用方法与 1.6 修改用户 PIN 码中的“检查强度”相同。

输入 SO PIN，设置新用户 PIN 并确认，然后点击“确定”按钮，解锁成功将弹出如图 25 所示的对话框：

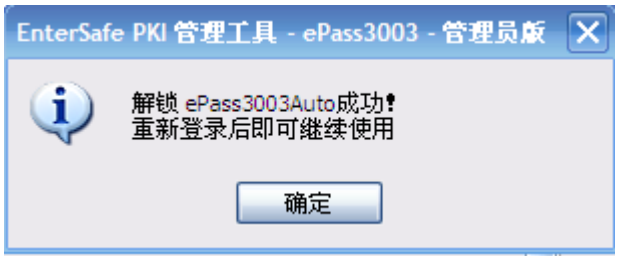


图 25 解锁成功对话框

1.8 初始化（仅限管理员版）

在图 22 所示的管理工具主界面上点击“初始化”按钮，将弹出初始化 USBKey 对话框，如图 26 所示：

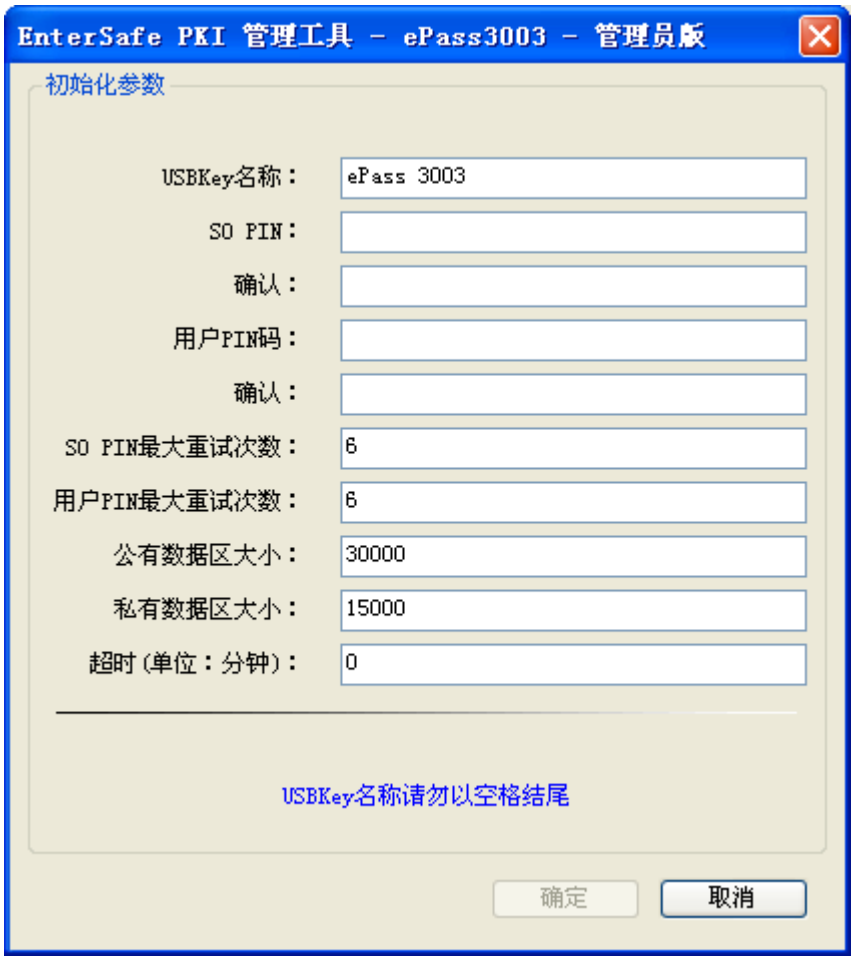


图 26 初始化对话框

注意：当“超时”设置为“0”时，表明不对操作进行超时限制。

设置好各初始化参数后，点击“确定”按钮，此时会弹出提示对话框，让用户确认进行初始化操作，如图 27 所示：

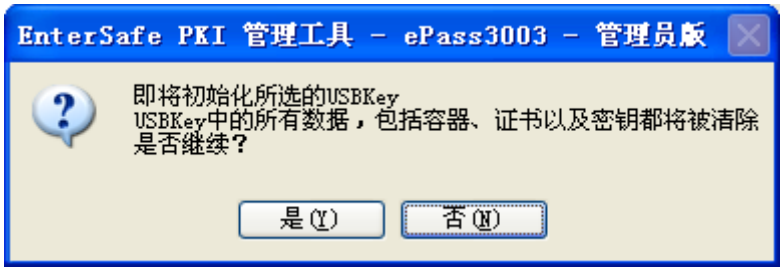


图 27 确认初始化对话框

点击“是”按钮，开始对 USBKey 的初始化操作，初始化成功后会弹出初始化成功对话框，如图 28 所示：

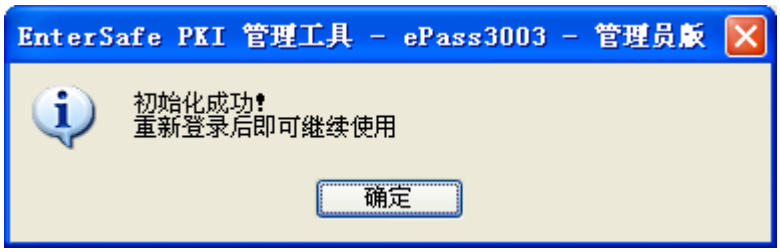


图 28 初始化成功对话框

1.9 修改 SOPIN（仅限管理员版）

在图 22 所示的管理工具主界面上点击“修改 SO PIN”按钮，将弹出修改 SO PIN 对话框，如图 29 所示：

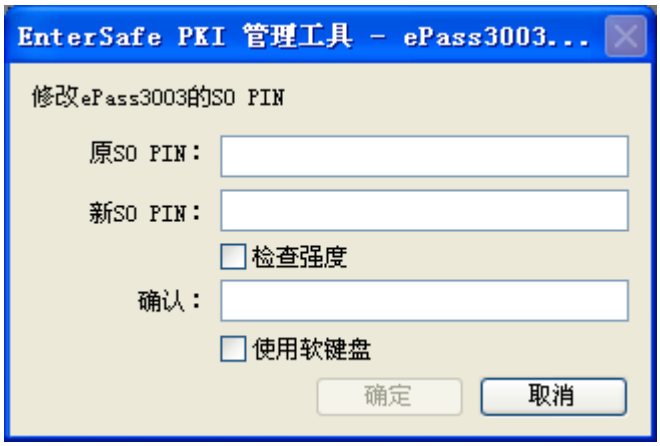


图 29 修改 SO PIN 对话框

用户可以通过选择使用“软键盘”来避免木马程序对用户设置的 SO PIN 的监控，如果用户选择 “使用软键盘”，修改 SO PIN 对话框如图 30 所示：

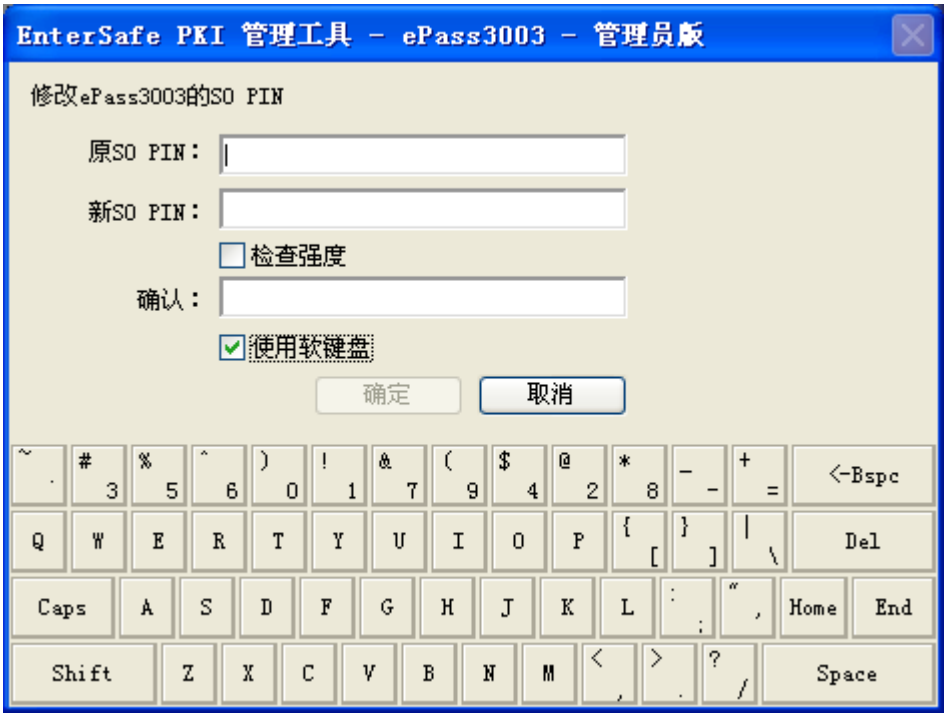


图 30 修改 SO PIN——使用软键盘

用户还可以选择“检查强度”来检查您设置的 SO PIN 的安全强度，具体使用方法与 1.6 修改用户 PIN 码中的“检查强度”相同。

填入原 SO PIN、新 SO PIN，并确认新 SO PIN，然后点击“确定”按钮，修改 SO PIN 成功将弹出修改 SO PIN 成功对话框，如图 31 所示：

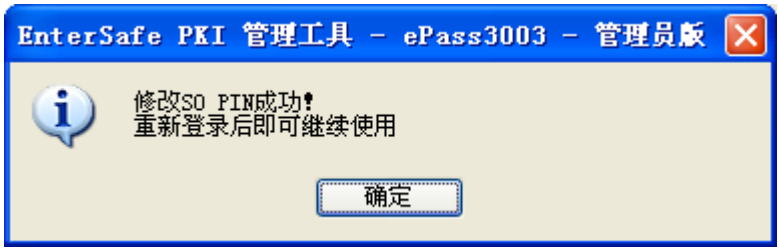


图 31 修改 SO PIN 成功

第二章 ePass3003 配置工具的使用方法

2.1 前提

在使用 ePass3003 的配置工具之前，您必须在您的计算机上正确安装了 ePass3003 产品。

2.2 配置工具的功能

可以在“开始”—〉“所有程序”—〉“EnterSafe”—〉“ePass3003”中找到配置工具的快捷方式，点击配置工具的快捷方式启动配置工具，出现界面如图 32 所示：

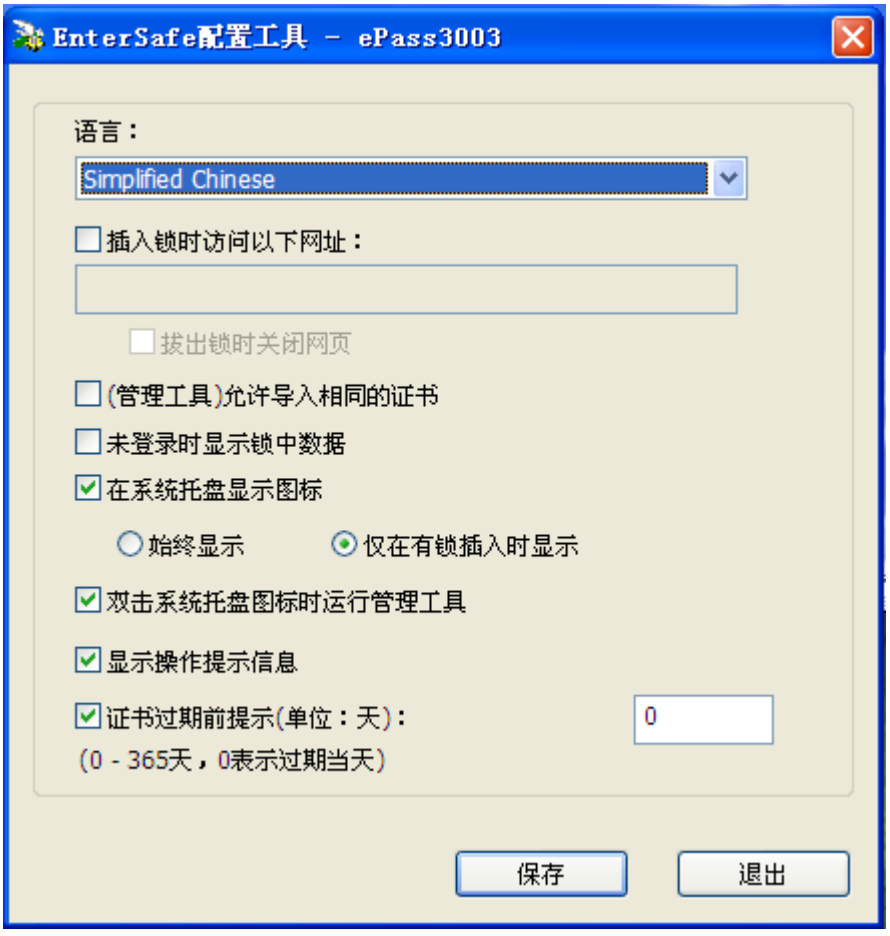


图 32 配置工具的界面

注意：在 Vista、Windows7、Windows2008、Windows8 下的配置工具对话框没有“拔出锁时关闭网页”的选项。

在上图中，您可以看到，通过配置工具可以进行语言、插入锁访问指定网址、托盘图标等多项设置，当您选中某项功能后点击“保存”按钮，会提示您配置成功信息，如图 33 所示：

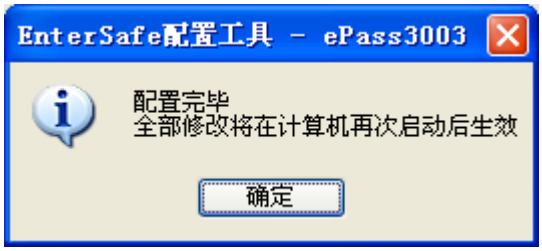


图 33 配置成功对话框

在您使用配置工具进行功能配置后，建议您重新启动计算机，以便使配置生效。

附录 缩略语及术语

缩略语及术语	解　释
ePass3003	飞天推出的 USB 接口的便携式密码设备，具有灵活易用、造价低廉、携带方便等好处。
ePass3003Auto	飞天推出的 USB 接口的便携式密码设备，在 ePass3003 基础上加入自动安装中间件的功能，具有更高的易用性。
Token	密码设备的统称，可以是智能卡，也可以是具有密码和证书存储功能的任何硬件设备。
USB Token	具有 USB 接口的密码设备，其携带方便，操作简单。ePass3003 是其中一种。
CryptoAPI 接口 (简称 CAPI)	由微软公司提供的密码(cryptography)操作接口，提供设备无关的或软件实现的密码算法封装，很容易使开发者能够开发出用于数据加解密、使用数字证书的身份认证、代码签名等的 Windows 平台上的 PKI 应用程序。
PKCS#11 接口	由 RSA 实验室推出的程序设计接口，将密码设备抽象成一种通用的逻辑视图即密码令牌（Cryptographic Token）提供给上层应用，做到设备无关性和资源共享。