



# ePassNG 用户手册

## 1.2 版

北京飞天诚信科技有限公司（以下简称“飞天公司”）尽最大努力使这篇文档中的内容完善且正确。飞天公司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	修改
2005 年 6 月 15 日	1.0	第一版
2007 年 8 月 13 日	1.1	第一版第一次修订
2009 年 6 月 2 日	1.2	第一版第二次修订

# 软件开发协议

北京飞天诚信科技有限公司（以下简称“飞天”）的所有产品，包括但不限于：开发工具包，磁盘，光盘，硬件设备和文档，以及未来的所有定单都受本协议的制约。如果您不愿接受这些条款，请在收到后的 7 天内将开发工具包寄回飞天，预付邮资和保险。我们会把货款退还给您，但要扣除运费和适当的手续费。

## 1. 许可使用

您可以将本软件合并、连接到您的计算机程序中，但其目的只是如开发指南中描述的那样保护该程序。您可以以存档为目的复制合理数量的拷贝。

## 2. 禁止使用

除在条款 1 中特别允许的之外，不得复制、反向工程、反汇编、反编译、修改、增加、改进软件、ePass 系列硬件和产品的其它部分。禁止对软件 and 产品的任何部分进行反向工程，或企图推导软件的源代码。禁止使用产品中的磁性或光学介质来传递、存储非本产品的原始程序或由飞天提供的产品升级的任何数据。禁止将软件放在服务器上传播。

## 3. 有限担保

飞天保证在自产品交给您之日起的 12 个月内，在正常的使用情况下，ePass 系列硬件和软件存储介质没有重大的工艺和材料上的缺陷。

## 4. 修理限度

当根据本协议提出索赔时，飞天唯一的责任就是根据飞天的选择，免费进行替换或维修。飞天对更换后的任何产品部件都享有所有权。

保修索赔单必须在担保期内写好，或发生故障 14 天内连同令人信服的证据交给飞天。当将产品返还给飞天或飞天的授权代理商时，须预付运费和保险。

除了在本协议中保证的担保之外，飞天不再提供特别的或隐含的担保，也不再对本协议中所描述的产品负责，包括它们的质量，性能和对某一特定目的的适应性。

## 5. 责任限度

不管因为什么原因，不管是因合同中的规定还是由于刑事的原因，包括疏忽的原因，而使您及任何一方受到了损失，由我方产品所造成的损失或该产品是起诉的原因或与起诉有间接关系，飞天对您及任何一方所承担的全部责任不超出您购买该产品所支付的货款。在任何情况下，飞天对于由于您不履行责任所导致的损失，或对于数据、利润、储蓄或其它的后续的和偶然的损失，即使飞天被建议有这种损失的可能性，或您根据第 3 方的索赔而提出的任何索赔均不负责任。

## 6. 协议终止

当您不能遵守本协议所规定的条款时，将终止您的许可和本协议。但条款 2，3，4，5 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 report No. 70407310011

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.

## 缩略语及术语

缩略语及术语	解释
PKCS#11 接口	由 RSA( <a href="http://www.rsasecurity.com">www.rsasecurity.com</a> )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。
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。
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设备。
USB Token	具有 USB 接口的密码设备, 其携带方便, 操作简单。
ePass3000	飞天公司推出的将智能卡和 USB 接口结合的便携式设备, 具有智能卡的优点, 又有携带方便的好处。支持 PKI 应用。
ePass3000ND (ePass3k Without Driver)	飞天公司推出的一款无驱型 USB Token。其外形和功能与 ePass3000 相似, 但不需要驱动。
ePassNG (ePass Next Generation)	飞天公司推出的新一代的中间件框架产品, 支持 ePass 系列等产品, 并能够非常方便的增加被支持的硬件。支持 PKI 应用。
TSP (Token Service Provider)	ePassNG 架构中的硬件抽象层, 对各种设备提供统一的访问方式, 从一定程度上屏蔽了硬件的差异。

# 目 录

<b>第一章 ePassNG 介绍.....</b>	<b>1</b>
1.1 ePassNG 体系结构.....	1
1.2 ePassNG 的特点.....	2
<b>第二章 ePassNG 管理工具的使用 .....</b>	<b>4</b>
2.1 前提 .....	4
2.2 概貌 .....	4
2.2.1 未插入 Token 的界面 .....	4
2.2.2 插入 Token 的界面 .....	5
2.2.3 管理工具的菜单 .....	5
2.2.4 “令牌操作”菜单 .....	5
2.2.5 “查看”菜单 .....	6
2.2.6 树型控件右键菜单 .....	6
2.2.7 插入 Token 时的详细信息 .....	7
2.2.8 未插入 Token 时的信息 .....	7
2.3 查看令牌插槽列表信息 .....	8
2.4 查看令牌信息 .....	8
2.5 登录 .....	8
2.6 修改用户 PIN 码.....	9
2.7 修改令牌名称 .....	9
2.8 修改管理员 PIN 码.....	10
2.9 令牌解锁 .....	10
2.10 初始化令牌 .....	11
2.11 用户未登录时的数据管理.....	11
2.12 用户登录后的数据管理.....	12
2.13 导入证书 .....	12
2.14 证书导出 .....	13
2.15 数据信息显示 .....	14
2.16 数据删除 .....	15

# 第一章 ePassNG 介绍

ePassNG 是完全跨平台的，新一代的数据安全产品架构。

ePassNG 主要用于为上层 PKI 应用提供很好的硬件支持，其证书、密钥及其他个人私密信息都存储在 ePassToken 中。ePassNG 提供标准的 PKCS#11 及 CryptoAPI 接口，支持标准的 PKI 应用，很容易被 PKI 应用的二次开发商或最终用户使用。另外由于 ePassNG 提供简单的框架结构，硬件提供商可以通过实现一个 TSP（Token Service Provider，令牌服务提供者）而将其硬件加入 ePassNG 框架中，很容易地就将其硬件融入到了 PKI 框架。

本章包括如下主题：

- ePassNG 体系结构
- ePassNG 的特点

## 1.1 ePassNG体系结构

ePassNG 为上层的 PKI 应用提供了标准的 PKCS#11 接口和 CryptoAPI 接口，二次开发商可以很好的利用该接口开发出自己的 PKI 应用。同时，ePassNG 还与采用标准接口的 PKI 应用无缝集成，只需安装和少许配置即可配合 PKI 应用进行使用。

ePassNG 的体系结构图如图 1-1 所示：

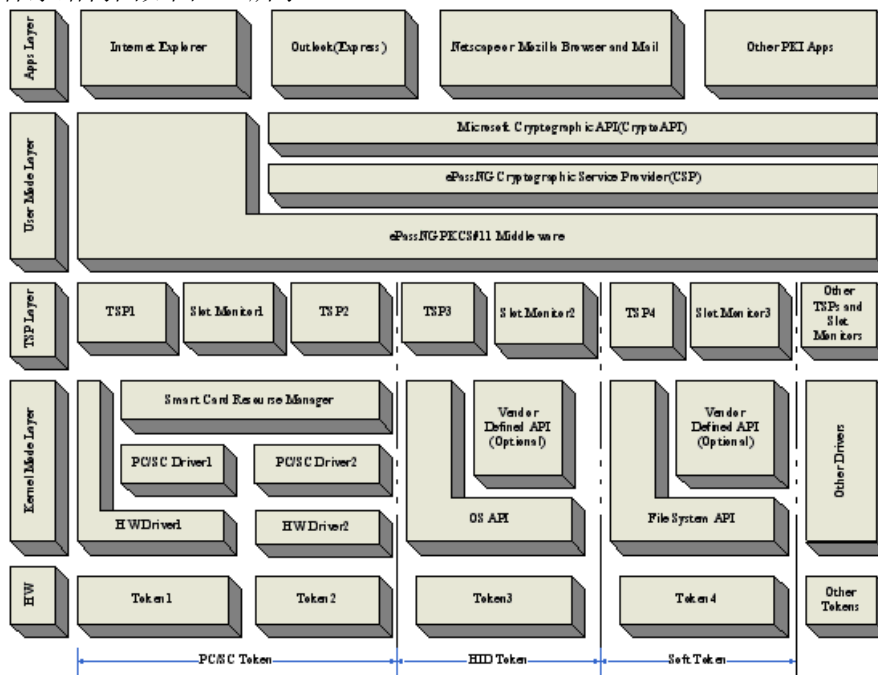


图 1-1

由上图可以看出，ePassNG 的产品构架可以分为五个层次：硬件层、核心驱动层、硬件抽象层、用户接口层和应用层。

### 硬件层

这一层位于整个构架的最底层，它包括各种 Token 及其硬件线路、固件程序和接线。该硬件层的 Token

可以是符合 PC/SC 规范的各种 Token，如 ePass1000、ePass2000、ePass3000、各种读卡器+智能卡的组合或第三方的 USB-Key，它们的共同点是可以通过调用操作系统的智能卡资源管理器(Smart Card Resource Manager)函数进行监测和访问。Token 还可以是各种 HID 设备，如 ePassND（飞天公司推出的无驱型 USB-Key）或优盘，甚至可以是硬盘上的文件。多种类型的 Token 或一种类型的多个 Token 都可以同时共存。

## 核心驱动层

这一层负责协调用户主机与硬件层之间的数据交互操作和处理 TSP 层的访问请求。对于 PC/SC Token 来说，这一层就是硬件驱动和 PC/SC 驱动，以及操作系统的 Smart Card Resource Manager。对于 HID Token 来说，这一层就是操作系统中内置的驱动，对于文件系统 Token 来说，这一层就是操作系统中的文件处理部分。

## 硬件抽象层

硬件抽象层为用户接口层提供标准的抽象接口，对各种设备（包括 Token）均提供统一的访问方式，从一定程度上屏蔽了硬件的差异。这一层的软件实现叫 TSP（Token Service Provider）。

## 用户接口层

用户接口层为上层提供 PKCS#11 标准接口及 MS CryptoAPI 接口的实现。

另外，我们提供符合微软 PC/SC 规范的 PC/SC 应用接口。开发者可以选择使用已经非常熟悉的 PC/SC 函数集进行开发。这个接口与平台无关，可以在 ePassNG 所适用的所有平台上调用。

## 应用层

应用层包括已经广泛使用的应用程序和针对 ePassNG 开发的应用程序。由于 ePassNG 提供兼容多种业界标准的接口，既可与现有应用程序兼容也可使开发者针对已经熟悉的编程接口进行开发。

# 1.2 ePassNG的特点

## 1. 跨平台

ePassNG 目前支持 Windows、Redhat Linux、Mandrake Linux、Mac OS X、Knoppix Linux 等平台，核心库文件采用统一代码（而不像其他软件是各平台有各自的实现），是真正的跨平台产品，最大限度的满足用户的需求。而且随着产品线的丰富将支持更多的平台。

## 2. 接口标准

ePassNG 向上层提供标准的 PKI 接口，包括 RSA PKCS#11 和 MS CryptoAPI（此接口只能在 Windows 系列平台上使用）。所有使用标准 PKI 接口的应用程序都可以使用 ePassNG 来保存密钥和证书，并进行密码操作。对于硬件 Token 的扩充来说，我们提供标准的接口给第三方硬件厂商供其实现。

## 3. 兼容性好

ePassNG 完全兼容飞天以前所推出的 ePass3000 和 ePass3000ND 的硬件，因此以前申请的证书和个人密钥仍然可以在 ePassNG 中使用。另外使用 ePassNG 在一个平台上申请的证书完全可以在另一个平台上使用，这给用户提供了不同环境下的统一身份识别的方便性。



#### 4. 支持多种 Token

ePassNG 框架设计的开放性使得它可以支持多种不同的 Token，而且可以同时支持多种 Token 共存。用户在不同的情况下可以选择不同的 Token。在实现 TSP 的前提下，ePassNG 甚至可以支持优盘、磁盘文件、软盘、光盘等虚拟 Token。

#### 5. 容易扩充

第三方 Token 提供商可以通过与飞天签订相关协议，将其 Token 纳入 ePassNG 框架中，根据飞天提供的 TSP 开发接口，第三方 Token 提供商只需要进行极少量的开发工作，甚至根本不需要额外的开发工作。

#### 6. 更加完善

飞天推出的 ePass3000 和 ePass3000ND 产品已经通过了多项国际和国内权威认证，其中包括 CheckPoint、CFCA 等。而 ePassNG 借鉴了它们的优点，比它们更完善、更稳健、更安全。而且 ePassNG 也将继 ePass3000 和 ePass3000ND 之后进行多项国际和国内认证。

## 第二章 ePassNG 管理工具的使用

ePassNG 在各个不同的平台下的界面风格以及功能流程基本相似，以方便用户在不同平台下的使用。另外 ePass1000ND、ePass2000、ePass2000\_FT11、ePass2000\_FT12、ePass3000ND、ePass3000 和 ePass3000OEM 采用同一个管理工具。

ePassNG 的管理工具分为管理员版和最终用户版，二者的区别主要在“管理员版”比“最终用户版”多了“初始化 Token”、“解锁 PIN”和“更改 SO PIN”的功能。

本章将以 Windows 下“管理员版”的 ePassNG 图形界面管理工具为例说明其如下功能的使用方法：

- 初始化 Token（只限于管理员版）
- 解锁用户 PIN（只限于管理员版）
- 更改 SO PIN（只限于管理员版）
- 登录（验证用户 PIN）
- 查看 Token 以及插槽内容
- 更改用户 PIN
- 更改 Token 名称
- Token 数据管理

### 2.1 前提

因为管理工具是基于 ePassNG 的中间件之上并且要访问硬件 Token，所以在使用 ePassNG 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 ePassNG 产品（中间件和硬件驱动）。

### 2.2 概貌

#### 2.2.1 未插入Token的界面

启动管理工具，出现界面如图 2-1：

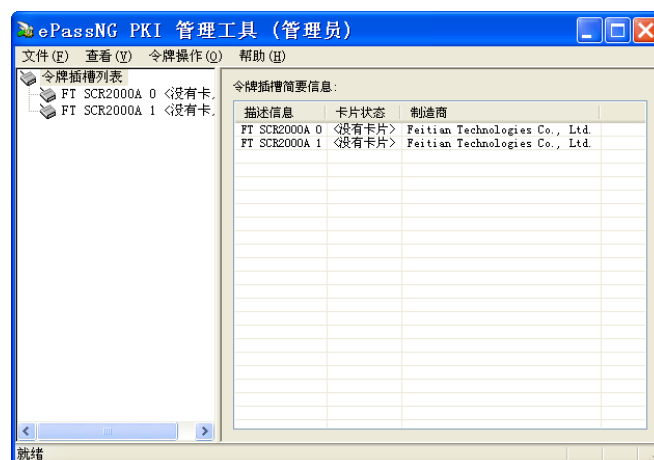


图 2-1 未插入 Token 时管理工具的界面

左边列出令牌插槽所能支持的全部插槽，右边列出这些插槽系列的简要信息。

### 2.2.2 插入Token的界面

在 USB 接口中插入一个名称为“ePass Token 3000”的 Token，那么管理工具就能自动识别出这个 Token 的基本信息，并且界面如图 2-2:



图 2-2 插入 Token 的管理工具界面

### 2.2.3 管理工具的菜单

在图 2-3 中用红色圈出:

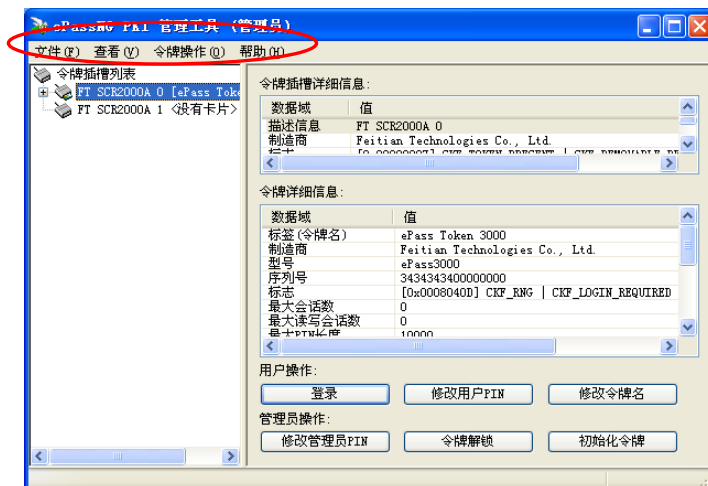


图 2-3 管理工具的菜单

主菜单主要包括，文件：程序退出；查看：查看令牌插槽系列信息；令牌操作：关于令牌的各种操作；以及帮助：版本信息。

### 2.2.4 “令牌操作”菜单

详细功能如图 2-4:



图 2-4 令牌操作菜单下的具体操作菜单信息

2.2.5 “查看”菜单

详细功能如图 2-5:



图 2-5 查看操作菜单下的具体操作信息

2.2.6 树型控件右键菜单

选中左侧某个令牌，点击鼠标右键，弹出详细菜单如图 2-6:



图 2-6 令牌右键菜单操作

其中包括登录令牌、修改用户 PIN 码、修改令牌名、初始化令牌、令牌解锁以及修改管理员 PIN 码。

## 2.2.7 插入Token时的详细信息

点击管理工具左边某个插入令牌的插槽，右边将显示出该令牌的相应信息以及可以操作的界面，如图 2-7：

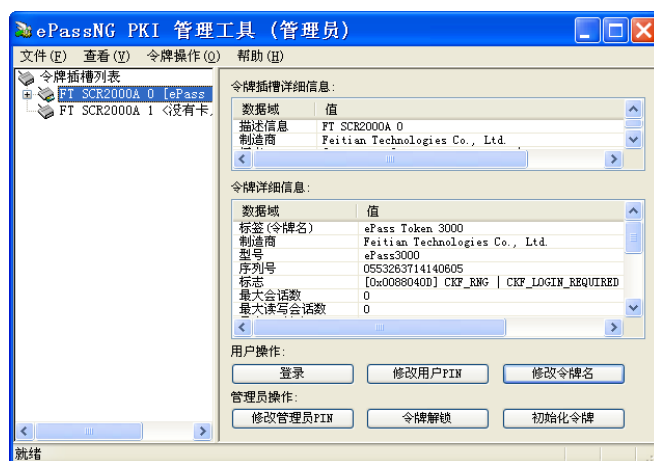


图 2-7 插入令牌后的令牌详细信息

右边显示的信息包括令牌插槽详细信息以及令牌详细信息。同时，和该令牌相关的各种操作将显示出来，当前不可用的操作会置灰。

## 2.2.8 未插入Token时的信息

点击左边某个未插入令牌的插槽时，显示的信息如图 2-8：



图 2-8 未插入令牌时的信息

没有插入令牌的时候，点击令牌插槽，右边显示令牌插槽详细信息。

## 2.3 查看令牌插槽列表信息

点击左边的令牌插槽或者选中查看菜单的查看令牌插槽列表，将显示如图 2-1 所示的令牌插槽列表的具体信息。

## 2.4 查看令牌信息

点击左边令牌插槽列表，右边将显示相应令牌插槽的具体信息。假如此时已经插入了令牌，显示的信息将包括令牌插槽详细信息、令牌详细信息以及令牌的各种操作如图 2-7；假如没有插入令牌仅仅显示令牌插槽详细信息如图 2-8。

## 2.5 登录

用户未登录的时候只能看到令牌上的公有对象，其他私有对象只有在验证用户的 PIN 码以后才能看到。点击用户操作下面的“登录”按钮，管理工具会弹出如图 2-9 的登录对话框：

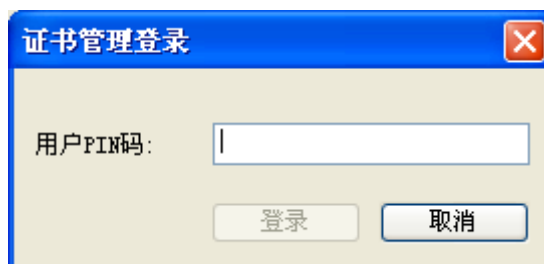


图 2-9 证书管理登录界面

在输入正确的 PIN 码后，点击“登录”按钮登录到令牌。

## 2.6 修改用户PIN码

如果您的 Token 是直接从天购买的，则出厂用户 PIN 码为 1234，否则，请咨询您的运营商。用户购买 Token 后建议及时修改 PIN 码，以保证 PIN 码的私密性。点击用户操作下面的“修改用户 PIN”弹出对话框如图 2-10：

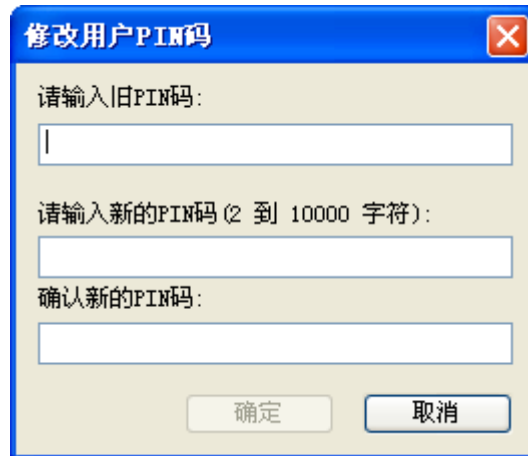
A screenshot of a Windows-style dialog box titled "修改用户PIN码" (Modify User PIN Code). The dialog has a blue title bar with a close button (X) in the top right corner. The main area is light gray and contains three input fields. The first field is labeled "请输入旧PIN码:" (Please enter the old PIN code:). The second field is labeled "请输入新的PIN码 (2 到 10000 字符):" (Please enter the new PIN code (2 to 10000 characters):). The third field is labeled "确认新的PIN码:" (Confirm the new PIN code:). At the bottom, there are two buttons: "确定" (OK) and "取消" (Cancel).

图 2-10 修改用户 PIN 码界面

修改用户 PIN 码时，您要先输入旧 PIN 码，能后输入新的 PIN 码，以及再次输入以确认新 PIN 码，点击“确定”就完成了用户 PIN 码的修改。

## 2.7 修改令牌名称

一般情况令牌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，所以我们以令牌名称来标记令牌。令牌名可以根据自己的喜好任意命名。

点击“修改令牌名”按钮，弹出对话框如图 2-11：

A screenshot of a Windows-style dialog box titled "修改令牌名" (Modify Token Name). The dialog has a blue title bar with a close button (X) in the top right corner. The main area is light gray. It shows "当前令牌名:" (Current token name:) followed by "ePass Token 3000". Below this, it says "请输入令牌新名 (最大32字符，不能以空格结尾):" (Please enter the new token name (maximum 32 characters, cannot end with a space)). There is a text input field containing "ePass Token 3000". At the bottom, there are two buttons: "确定" (OK) and "取消" (Cancel).

图 2-11 修改令牌名界面

输入您想要的令牌名，然后点击“确定”按钮。令牌名修改成功后，管理工具就会进行自动刷新，以新的令牌名显示令牌。

## 2.8 修改管理员PIN码

如果您的 Token 是直接从天购买的，则出厂管理员 PIN 码为 “rockey”，否则，请咨询您的运营商。点击管理员操作下的“修改管理员 PIN”按钮，弹出对话框如图 2-12：

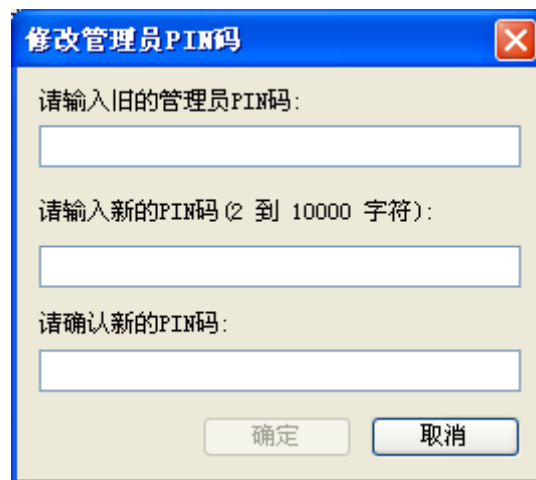
A Windows-style dialog box titled "修改管理员PIN码" (Modify Admin PIN). It contains three input fields: "请输入旧的管理员PIN码:" (Enter old admin PIN), "请输入新的PIN码 (2 到 10000 字符):" (Enter new PIN, 2 to 10000 characters), and "请确认新的PIN码:" (Confirm new PIN). At the bottom are "确定" (OK) and "取消" (Cancel) buttons.

图 2-12 修改管理员 PIN 码界面

修改管理员 PIN 码时，先输入旧的管理员 PIN 码，然后输入新的 PIN 码，以及再次输入新 PIN 码确认，点击“确定”完成修改。

## 2.9 令牌解锁

当用户 PIN 码连续多次输入错误以后，PIN 码会被锁死，Token 将无法使用，这时候需要管理员来对 Token 进行解锁。点击管理员操作下的“令牌解锁”按钮，弹出对话框如图 2-13：

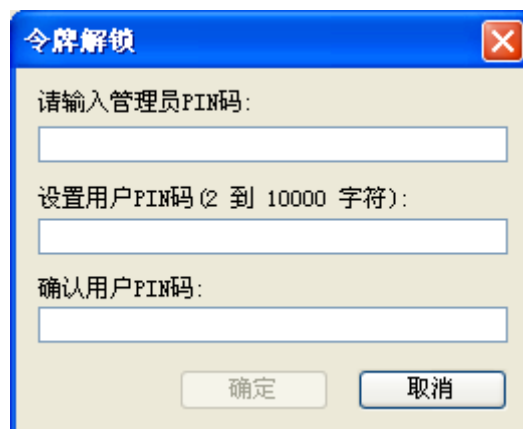
A Windows-style dialog box titled "令牌解锁" (Token Unlock). It contains three input fields: "请输入管理员PIN码:" (Enter admin PIN), "设置用户PIN码 (2 到 10000 字符):" (Set user PIN, 2 to 10000 characters), and "确认用户PIN码:" (Confirm user PIN). At the bottom are "确定" (OK) and "取消" (Cancel) buttons.

图 2-13 用户令牌解锁界面

要对用户 PIN 码进行解锁，您必须知道管理员 PIN 码，用户 PIN 码必须重新设置。点击“确定”按钮就完成了 Token 解锁。令牌解锁成功后，管理工具自动进入已登录状态。



## 2.10 初始化令牌

该功能清除 Token 上所有的内容，并将 Token 初始化成能进行 PKI 操作的硬件 Token。

**注意：**执行该功能后，Token 上所有的 PKI 内容（包括证书、公私钥、用户数据等）将被全部删除。

点击管理员操作下面的“初始化令牌”按钮，弹出对话框如图 2-14：

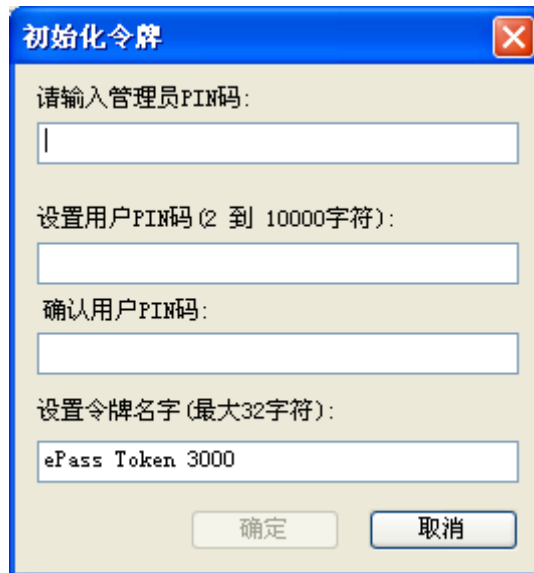


图 2-14 令牌初始化界面

初始化令牌需要输入管理员 PIN 码，设定用户 PIN 码和令牌名。在初始化成功后，管理工具自动刷新界面上的令牌信息，同时令牌将进入已登录状态。

## 2.11 用户未登录时的数据管理

在管理工具的左边，每个令牌下都有一个数据管理功能，在未登录的情况下点击数据管理，右边将显示出 Token 中的公有数据信息，以及它们的相对应的各种操作如图 2-15：



图 2-15 用户未登录数据管理界面

2.12 用户登录后的数据管理

用户登录后的数据管理界面如图 2-16 所示：



图 2-16 用户登录后的数据管理界面

用户登录后，不仅可以查看 Token 中公有数据的信息，还可以查看到 Token 里私有数据的信息。其中“导入”功能只有在登录以后才有效，“导出”功能只是针对证书有效。“显示”功能除了 Token 名称外都有效，“删除”功能在登录后总是有效。

在处于已登录状态时，令牌信息的界面上“登录”按钮变灰，表明令牌为已登录状态，如图 2-17：



图 2-17 已登录 Token 时的管理工具界面

2.13 导入证书

当用户想导入 P12、P7B、CER、CRT 和 PFX 证书到 Token 时，点击“导入”按钮，弹出对话框如图 2-18：

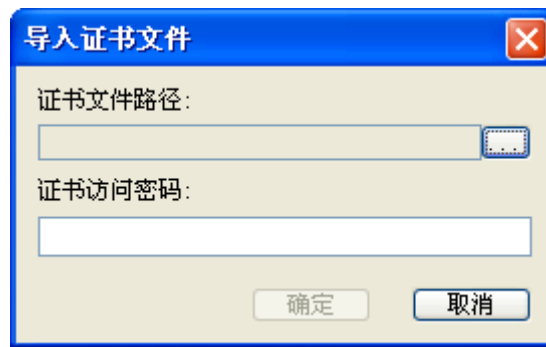


图 2-18 证书导入界面 1

只有 PKCS#12 格式的证书（扩展名为 pfx, p12）需要访问密码。导入其他证书的时候，系统将隐藏密码相关的信息。点击“...”按钮，选择您想要导入的证书，输入证书访问密码，点击“确定”按钮，就可以把证书信息导入到 Token 中，管理工具将自动进行更新，如图 2-19、2-20 所示：

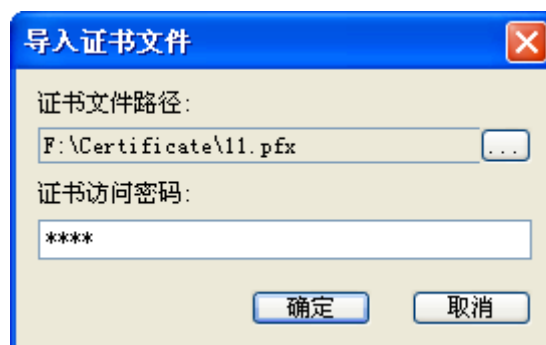


图 2-19 证书导入界面 2

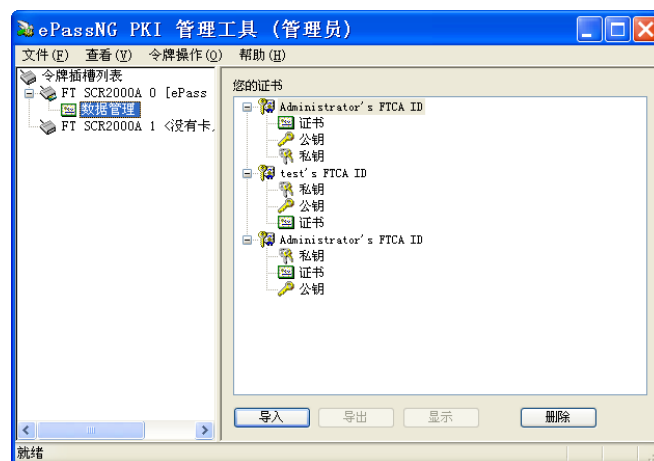


图 2-20 导入后的数据管理界面

## 2.14 证书导出

当用户想导出证书时，只要选中想要导出的证书，点击“导出”按钮，出现对话框如图 2-21：

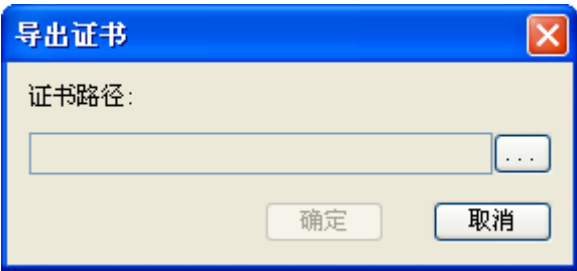


图 2-21 证书导出界面

点击 “...” 按钮，选择相应的文件路径，然后点击 “确定” 按钮就可以导出证书。

2. 15 数据信息显示

当用户想查看证书、公钥、私钥和其他数据的具体信息时，选中某个证书项，点击 “显示” 按钮，出现对话框如图 2-22：

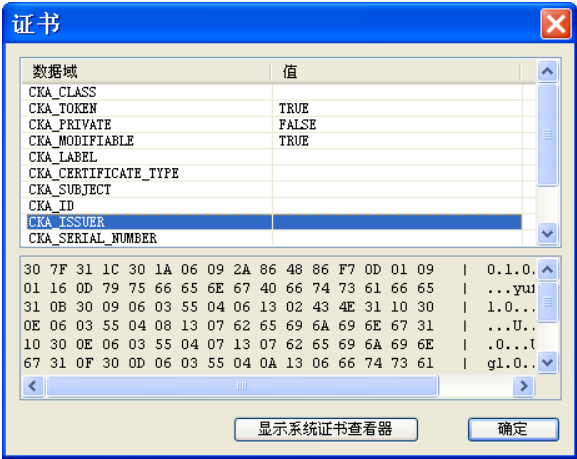


图 2-22 显示证书信息界面

显示证书内容的时候，对话框出现 “显示系统证书查看器” 按钮，点击 “显示系统证书查看器” 出现如图 2-23：

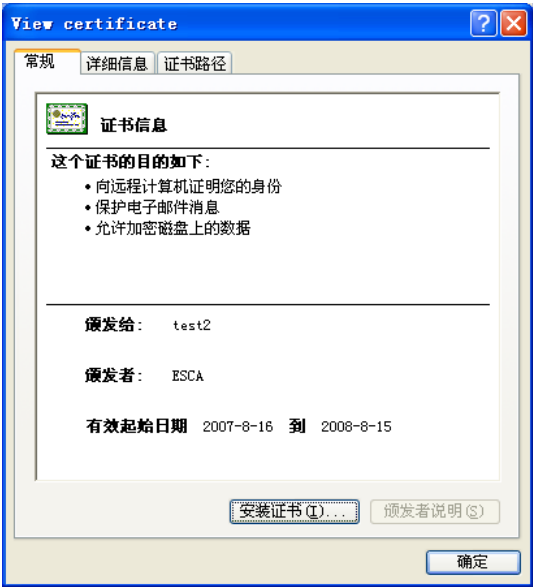


图 2-23 查看证书信息对话框

查看其他数据信息（比如公钥、私钥和其他数据）的时候出现的对话框如图 2-24：

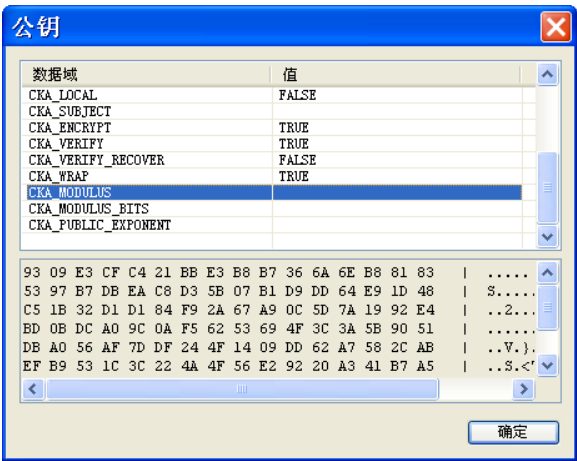


图 2-24 显示公钥信息界面

单击某个属性项，下面将列出该属性的详细信息。

2. 16 数据删除

用户想删除 Token 里面的信息时，用户登录后，选中您要删除的信息，点击“删除”按钮，弹出对话框如图 2-25：

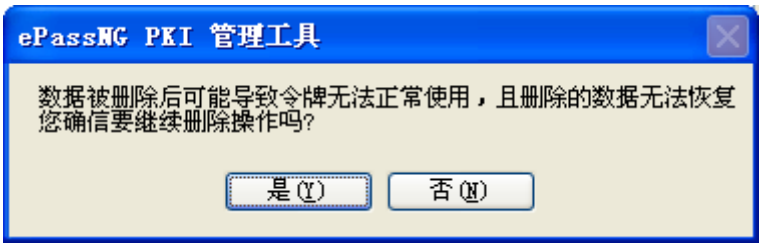


图 2-25 数据删除界面

注意：数据被删除以后将无法恢复。