ePass3000 的智能卡登录

1.1 版

www.FTsafe.com

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
2007 年 11 月 23 日	1.0	第一版
2009 年 6 月 2 日	1.1	第一版第一次修订

北京飞天诚信科技有限公司

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。禁止对软件和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(www.rsasecurity.com)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。
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。

目 录

第一章 ePass3000 的智能卡登录

Windows2000 操作系统以及微软后续的操作系统都内置了对智能卡用户认证的支持，计算机用户可以选择使用传统的用户名、口令验证方式进行域用户身份验证，也可以使用智能卡来自动完成用户身份验证。智能卡用户身份验证的优势是更加安全和易于使用。用户只需记住智能卡的用户 PIN 码就可利用智能卡自动进行安全身份认证。

本章主要讲述如何配置智能卡证书管理、申请智能卡证书、使用 ePass3000 进行本地和远程智能卡登录。

- 颁发智能卡证书管理
- 申请智能卡证书
- 使用 ePass3000 进行本地智能卡登录
- 使用 ePass3000 进行远程智能卡登录
- 锁定工作站

1.1 颁发智能卡证书管理

要在 Windows 的工作站上进行智能卡用户登录，首先工作站需要颁发智能卡证书给用户。智能卡证书是存储在用户智能卡内的数字证书。设置为用户颁发智能卡证书的具体步骤如下：

1. 使用管理员身份登录到用来颁发智能卡证书的证书颁发机构(CA)，并打开证书颁发机构管理工具，如下图：

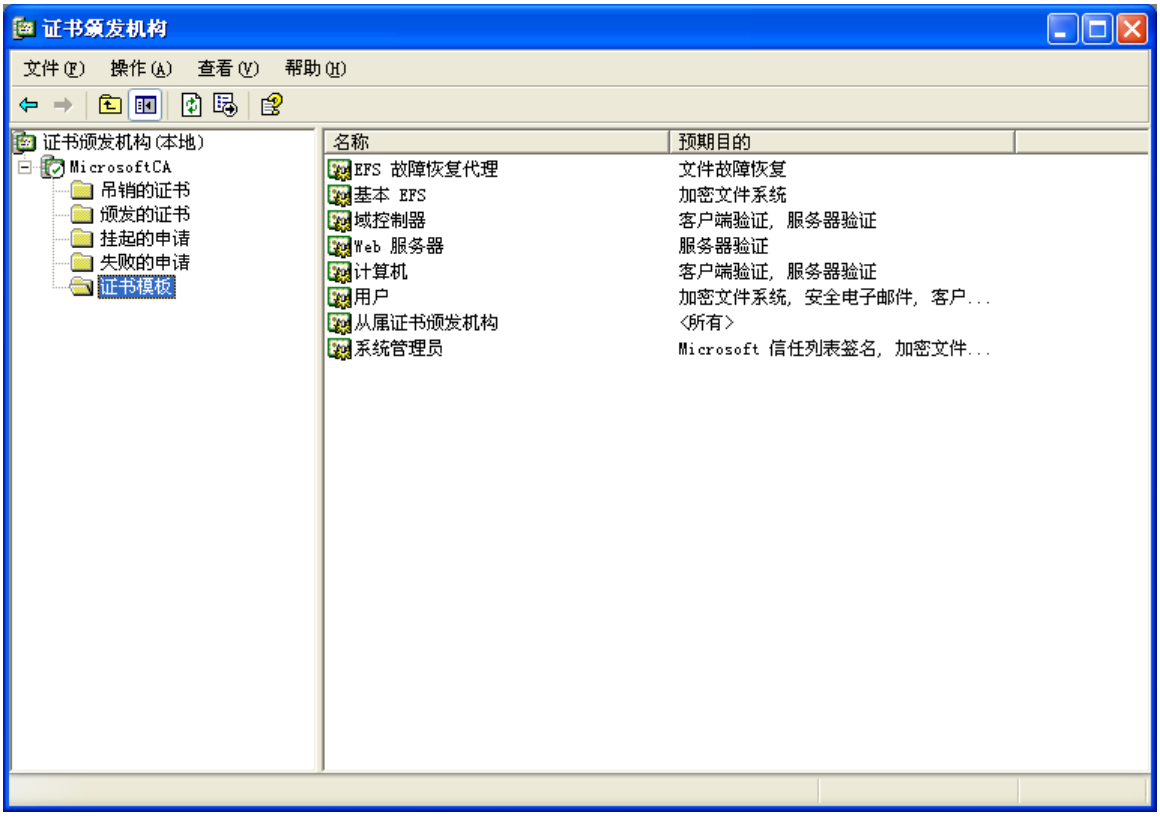

图 1 证书颁发机构管理工具

2. 在控制台的证书颁发机构树图中选择：证书颁发机构（计算机名）—>CA 名称—>证书模板。右

边的列表显示了当前可颁发证书的类型模板。

3. 在“操作”菜单上选择“新建”菜单的子菜单“要颁发的证书模板”，接下来将显示下面的窗口：

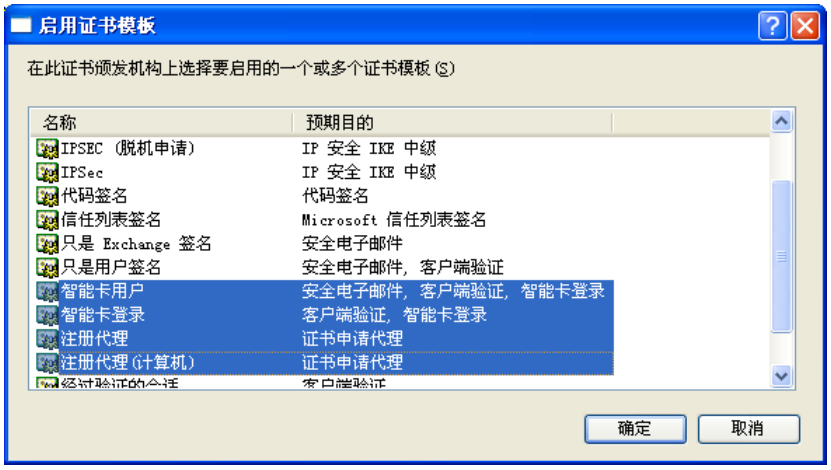

图 2 选择证书模板窗口

4. 选择“注册代理”，然后按“确定”按钮。接下来重复前面的步骤，将“智能卡用户”和“智能卡登录”两个证书模板类型也加入到证书模板中。完成后，如下图所示：

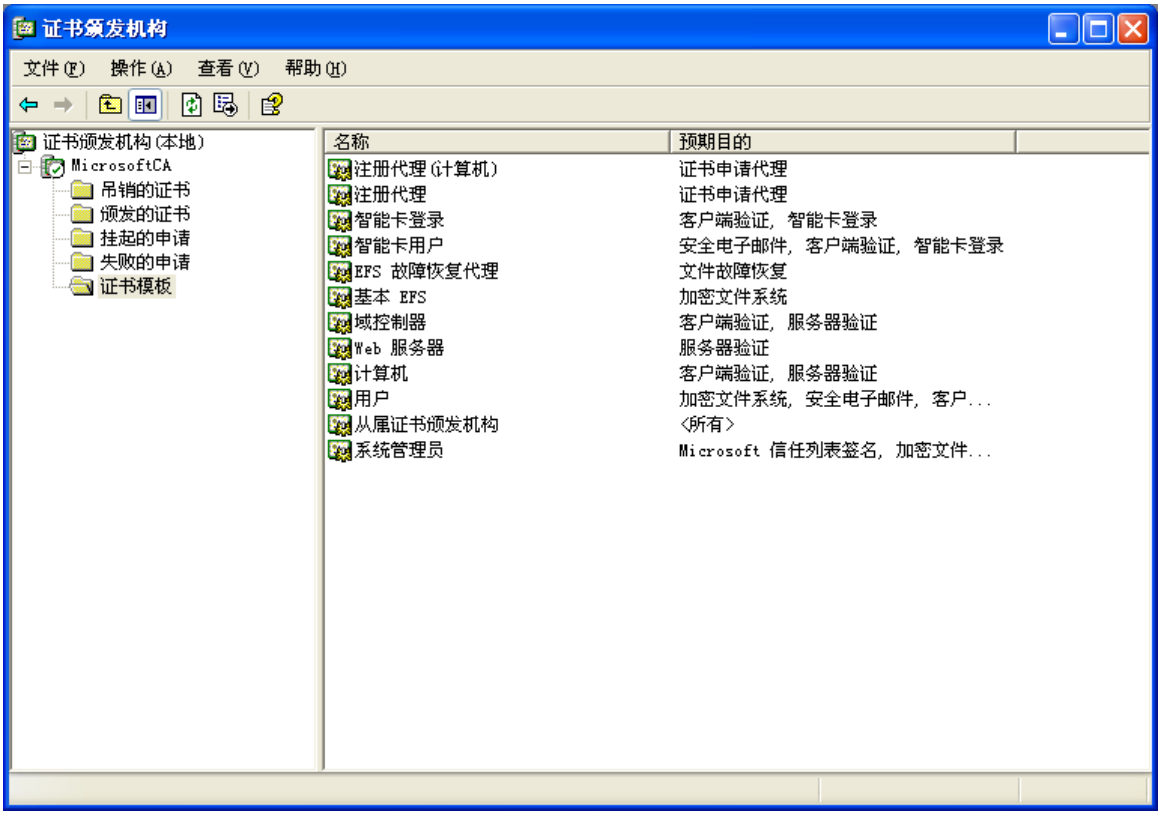

图 3 证书模板类型操作

另外，注册代理证书可以由不同于颁发智能卡证书的 CA 颁发，前提条件是颁发注册代理证书的 CA 必须是域内被信任的企业 CA。

有了注册代理证书就可以开始建立智能卡证书注册站点了。

5. 以管理员身份登录 Windows Server 2003，单击“开始”菜单并选择“运行”，键入“mmc”然后回车。

6. 在弹出的控制台“文件”菜单上，单击“添加/删除管理单元”，然后单击“添加”。

7. 在“添加独立管理单元”的对话框中，双击“证书”。如果以用户身份登录，证书管理单元将自

动加载。如果作为管理员登录，则应当选择“我的用户帐户”，如下图所示：

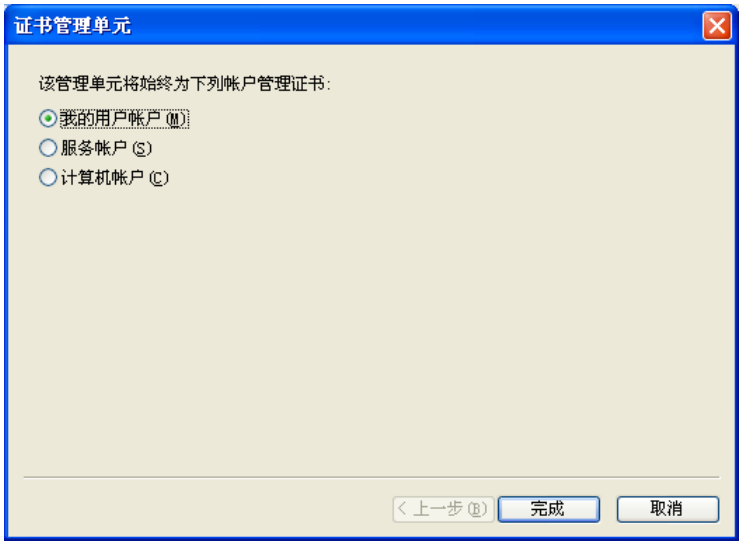

图 4 独立管理单元操作

8. 关闭“添加/删除独立管理单元”对话框。双击“证书 – 当前用户”，在控制台树中选择“个人”。然后鼠标右键单击，在弹出菜单中选择“所有任务”下的“申请新证书”，如下图：

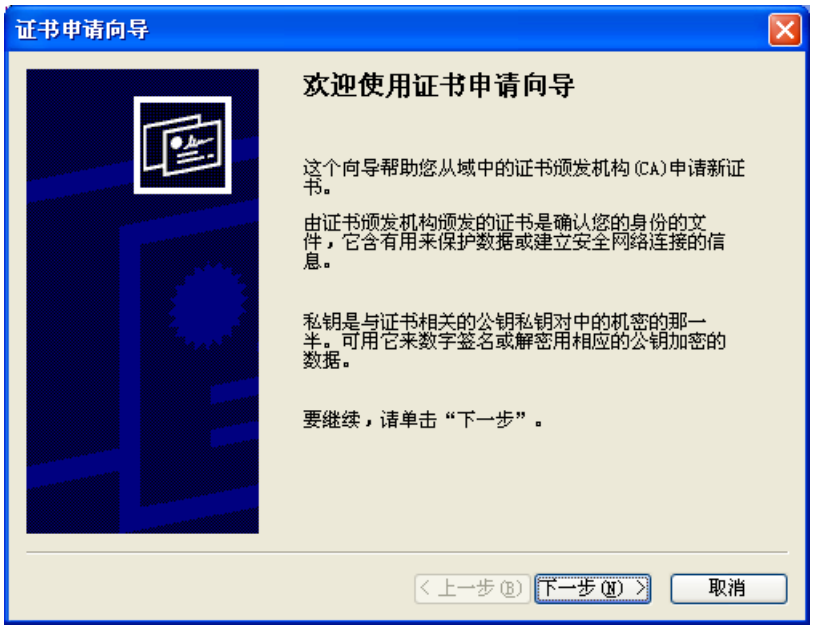

图 5 个人证书申请操作

9. 单击“下一步”按钮，选择证书模板“注册代理”，如下图：

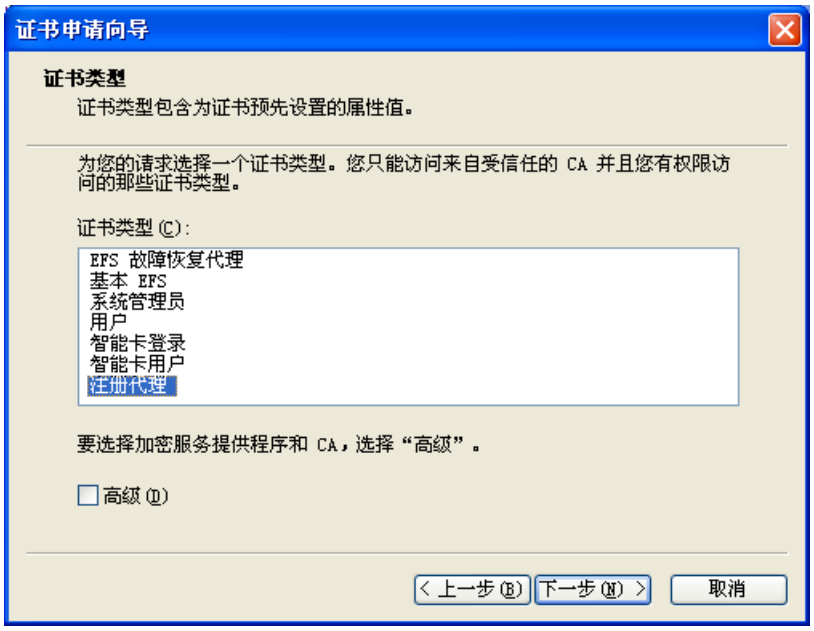

图 6 证书申请向导窗口之一

10. 单击“下一步”按钮，在编辑框中输入证书的好记的名称。输入完毕后，继续单击“下一步”完成智能卡代理注册证书的申请。

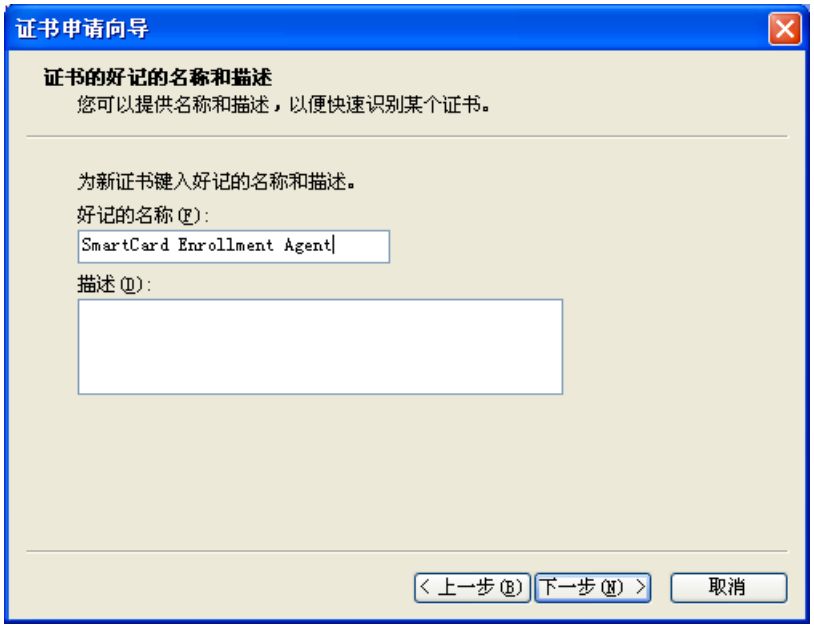

图 7 证书申请向导窗口之二

在为域内用户申请智能卡登录证书之前，智能卡管理员必须有可用的注册代理证书，用来代表域用户生成智能卡证书申请。这就是上述操作的目的。要执行这一操作，必须拥有访问注册代理证书模板的安全权限。有关注册代理证书和注册智能卡证书的详细信息，请参阅相关的 Windows 在线帮助。

1.2 申请智能卡证书

完成1.1的步骤之后，就可以正式进行智能卡证书的申请操作了。

1. 以管理员身份登录 Windows。

2. 打开 Internet Explorer，在地址栏中输入用来颁发智能卡证书的证书颁发中心的地址，然后按 Enter 键。

3. 在显示的网页中选择“申请一个证书”。

4. 在显示的网页中选择“高级证书申请”。

5. 插入 ePass3000（也可提前插入，但必须是初始化过的 ePass3000）。

6. 选择“通过使用智能卡证书注册站来为另一用户申请一个智能卡证书”，然后单击“下一步”。（如果是第一次申请证书，浏览器会自动下载两个 ActiveX 控件）。新的页面显示效果如下图所示：

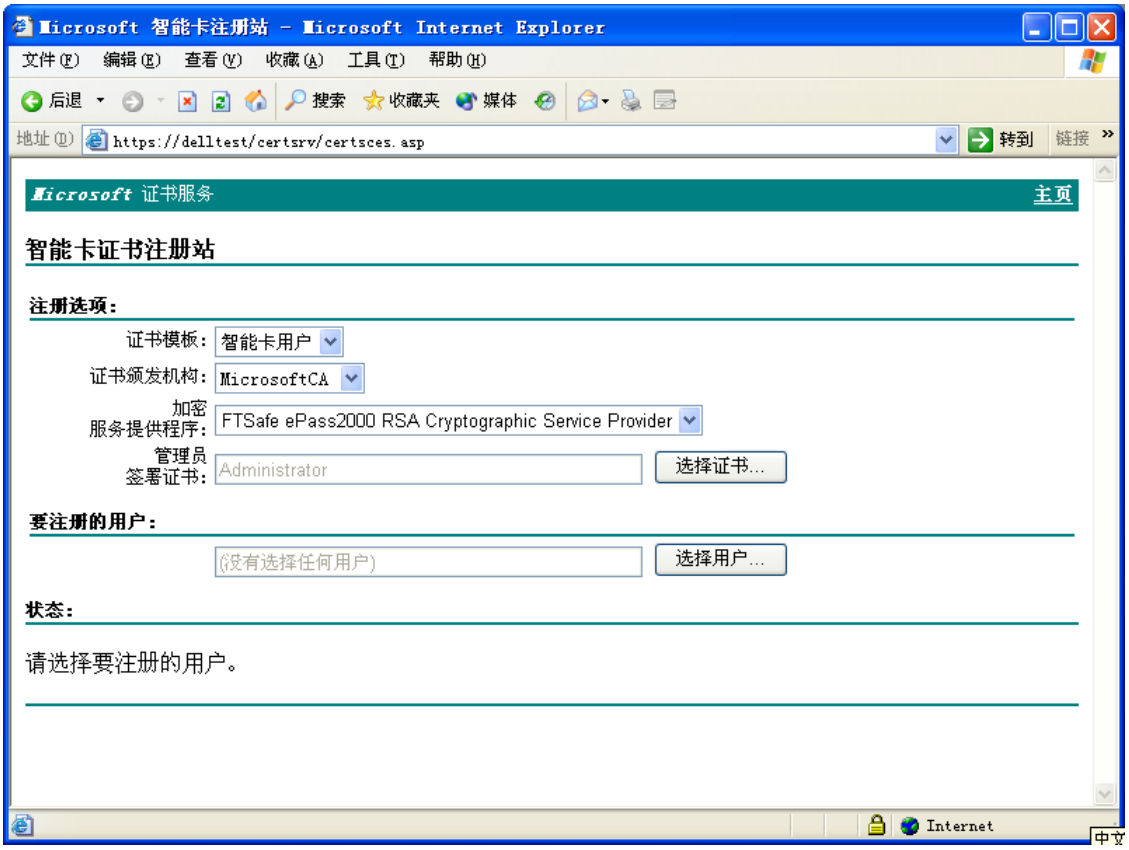

图 8 智能卡用户申请证书操作

7. 选择证书模板为“智能卡用户”。

8. 在“加密服务提供程序”中选择“FEITIAN ePassNG RSA Cryptographic Service Provider”。

9. 在“管理员签署证书”中选择我们先前申请的注册代理证书。

10. 在“要注册的用户”中，选择适当的域用户。

11. 在接下来弹出的验证用户 PIN 码对话框中输入正确的 ePass3000 用户 PIN 码，然后等待证书生成。

当证书下载完成之后，可以选择查看证书或者申请新的智能卡证书。用户智能卡证书申请完成之后，就可以使用智能卡进行域用户登录了。

1.3 使用ePass3000 进行本地智能卡登录

使用 ePass3000 进行本地智能卡登录之前，您需要将计算机加入到域（本文档以 Windows XP 为例说明将计算机加入到域的方法，如果您的计算机已经加入到域，您可以省去步骤 1 和步骤 2）。

1. 右键单击“我的电脑”，在弹出的菜单中选择“属性”，然后选择“计算机名”选项卡，点击“更改”按钮，弹出“计算机名称更改”对话框，如下图所示：

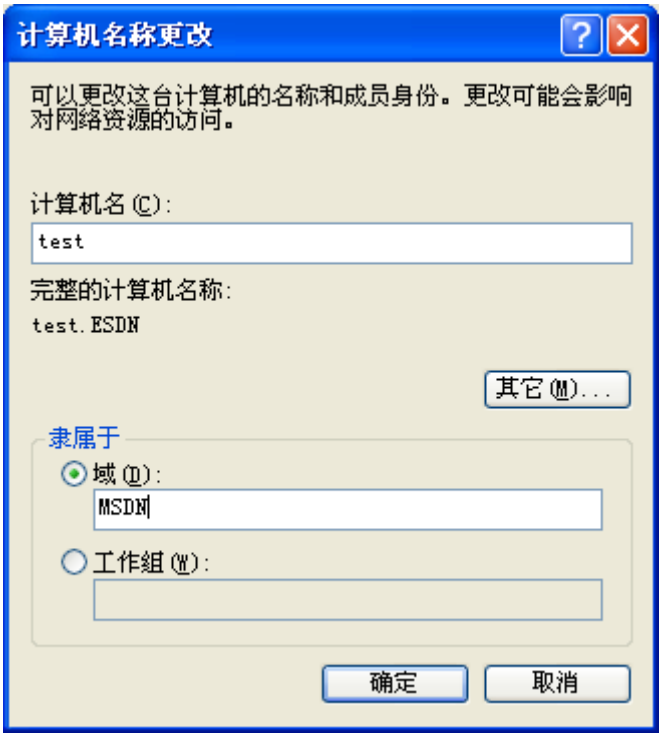

图 9 计算机加入域

2. 在“隶属于”栏中选择域，并在文本框中写入要加入的域名称，点击“确定”按钮，在弹出的对话框中输入域用户的用户名和密码，根据提示重新启动。

3. 再次进入登录界面时，插入申请过智能卡证书的 ePass3000，登录界面如下图所示：

图 10 智能卡登录界面

4. 输入 ePass3000 的 PIN 码即可登录到系统。

1.4 使用ePass3000 进行远程智能卡登录（远程桌面连接）

1.4.1 关于远程桌面

远程桌面是微软公司为了方便网络管理员管理维护而推出的一项服务。从 windows 2000 server 开始引入，网络管理员使用远程桌面连接程序连接到网络任意一台开启了远程桌面控制功能的计算机上，就好比自己操作该计算机一样运行程序，维护数据库等。

远程桌面连接属于 C/S（客户/服务器）模式，所以在建立连接前需要配置好连接的服务器端和客户端。

服务器端是指接受远程桌面连接的一方；客户端是发起桌面连接的一方。

因为“远程桌面连接”远程管理模式是属于 Windows Server 2003 服务器（还可以是 Windows XP 系统）管理远程工作站（或成员服务器）计算机的，所以发起远程桌面连接的当前就是 Windows Server 2003 服务器。作为远程桌面连接的服务器端，必须安装“远程桌面连接”的服务器端程序，而目前只有 Windows XP、Windows Server 2003、Windows Vista 系统，以及安装了“终端服务器”程序的 Windows 2000 Server 系统才具有服务器端程序。

1.4.2 远程桌面连接的权限设置

在进行远程桌面连接前还需为用于远程连接的用户配置远程连接权限。默认情况下，Administrators 组的成员可远程连接到服务器，除此之外还有“Remote Desktop Users”组具有远程连接的权限。但在默认情况下，“Remote Desktop Users”组未添加成员，所以如果想添加其他用户，而又不想赋予他系统管理员那么高权限，则您必须把他添加到这个组中。“Remote Desktop Users”组除了允许与 Users 组相同的访问权限外，还具备远程连接的其他能力。通过使用该组，可以在无需分别为每个用户设置这些权利的情况下保存管理资源。

1.4.3 使用ePass3000 建立远程桌面连接

1. 选择“开始”—〉“所有程序”—〉“附件”—〉“通讯”—〉“远程桌面连接”，弹出远程桌面连接对话框，如下图所示：

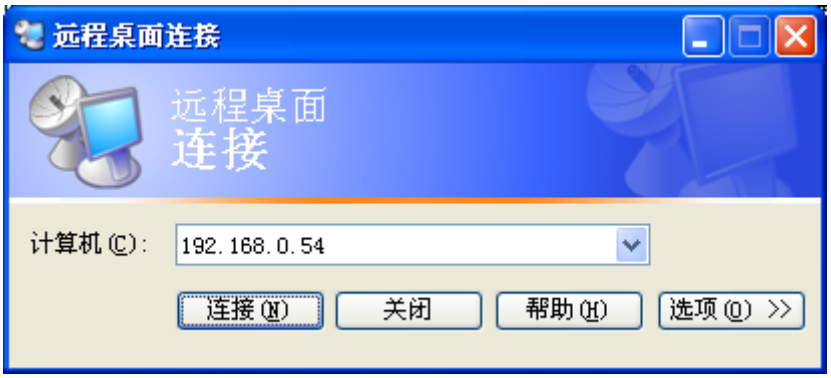

图 11 远程桌面连接对话框

2. 在“计算机”后的文本框内输入远程服务端的地址，点击连接，弹除远程登录界面，插入申请过智能卡证书的 ePass3000，输入其 PIN 码，即可登录到远程计算机。

1.5 锁定工作站

用户还可以使用 ePass3000 进行工作站的锁定操作。也就是说，当用户从计算机上拔下 ePass3000 时，系统会锁定工作站，或者强制注销用户。要解除锁定，需要再次插入 ePass3000，并进行 PIN 码校验。设定锁定工作站的操作步骤如下：

1. 打开控制面板中的“管理工具”，双击“域安全策略”图标，在左侧的树形列表中选择“安全设置”—〉“本地策略”—〉“安全选项”，如下图所示：

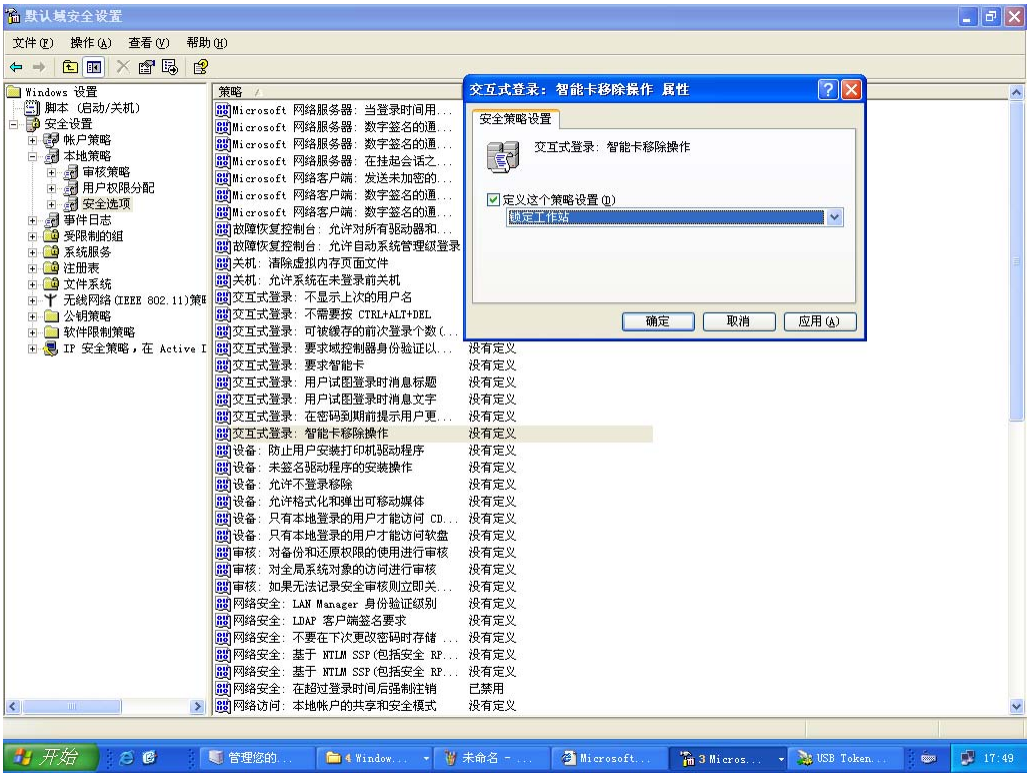

图 12 本地安全策略设置

3. 双击“智能卡移除操作”，弹出如上图所示的对话框，然后选择相应的智能卡移除操作。

这样在进行本地或远程智能卡登录时，当您拔出 ePass3000 时，系统将自动响应相应的拔出事件，例如锁定工作站。

注意：Vista 系统还需要启动 Smart Card Removal Policy 服务。