# ePass3000 的 NetScape 应用

## 1.2 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 |
|---|---|---|
| 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 |

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<br>(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Netscape应用指南

ePass3000 的设计目标之一就是与现有的 PKI 体系应用无缝的集成。PKI 应用开发商无需对 ePass3000 进行任何形式的编程开发就能通过配置相关服务而开始将 ePass3000 集成于 PKI 应用当中。

目前支持 PKI 的应用有些使用 PKCS#11 接口，有些使用 Crypto API（简称 CAPI）接口，后者都是微软的 Windows 平台下的应用，而前者在任何平台下都有。

本章主要讲述如何配置 ePass3000 的 Netscape 应用，本手册还讲述了在 Windows 上使用 ePass3000 进行申请数字证书、访问 SSL 加密站点和收发签名、加密邮件。Mozilla 和 Firefox 的使用与 Netscape 一致。在 Netscape 上申请的证书完全可以在 Mozilla、Firefox 和 Internet Explorer 上使用，在 Internet Explorer 上申请的证书也同样可以在 Netscape、Mozilla 和 Firefox 上使用。

- ePass3000 与 Netscape 的集成
- 使用 ePass3000 的 PKCS#11 申请数字证书
- 使用 ePass3000 的 PKCS#11 访问 SSL 加密站点
- 使用 ePass3000 的 PKCS#11 收发签名与加密邮件

## 1.1 Windows平台下Netscape与ePass3000 的应用

Netscape 和 Mozilla 的界面、菜单和操作步骤都极其类似，因此本手册所描述的所有的对 Netscape 的操作都适用于 Mozilla（菜单项的位置有可能不同）。下面以 Netscape7.2 英文版为例进行说明。

在 Windows 平台下为了使 Netscape 能够对 ePass3000 进行操作，必须使 Netscape 集成 ePass3000。

您可以在 Netscape 的“安全设备管理器”中操作 ePass3000 的集成和卸载。具体的操作步骤如下：

**1.** 启动Netscape，选择菜单“Edit”→“Preferences”，如图 1所示：

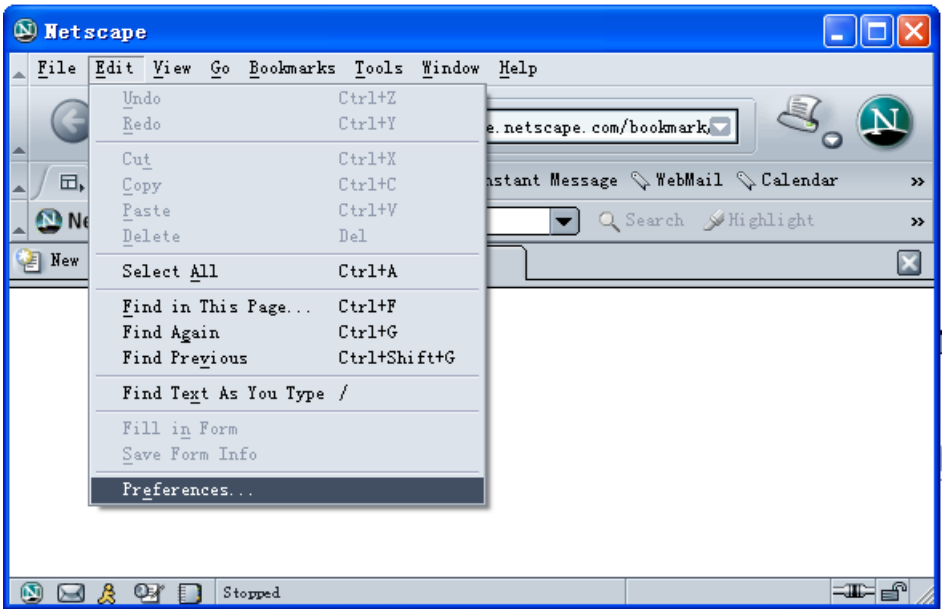


图 1 Preferences 菜单

**2.** Netscape将弹出“Preferences”对话框，选择左侧树状菜单的“Privacy & Security”→“Certificates”，在右侧就会出现“Certificates”配置页面，如图 2所示：

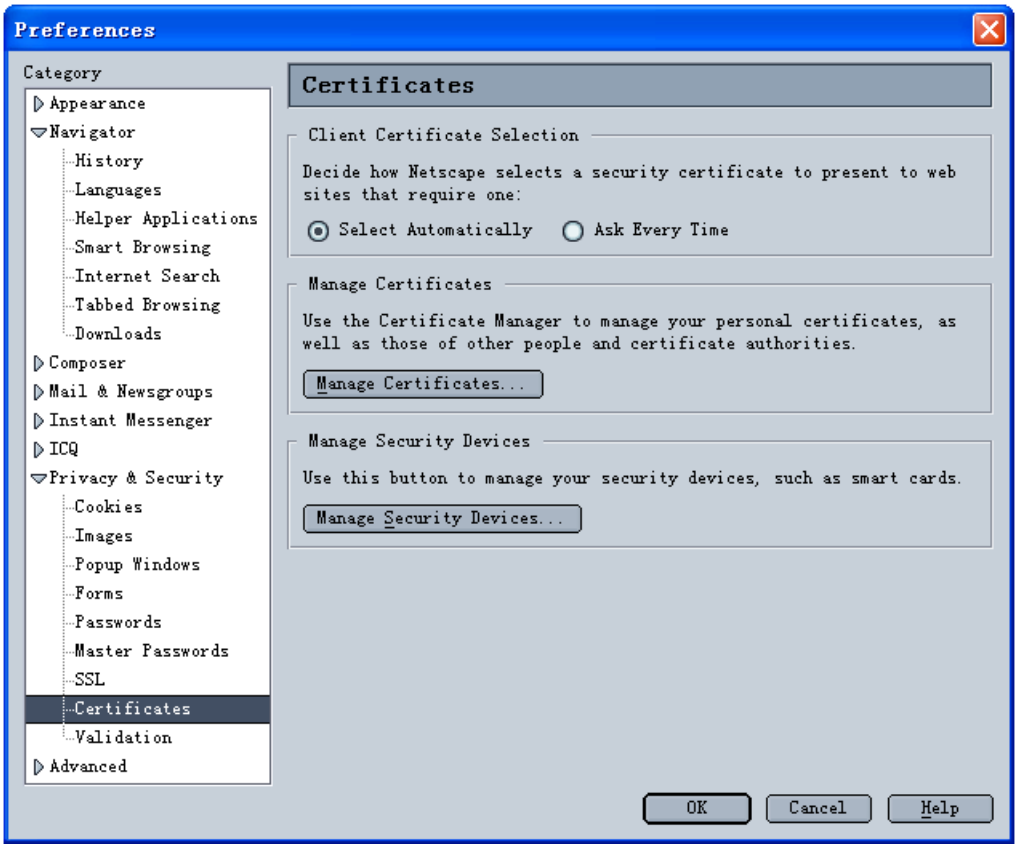


图 2 Certificates 配置页面

**3.** 点击“Manager Security Devices”按钮，Netscape将弹出设备管理器界面，如图 3所示：

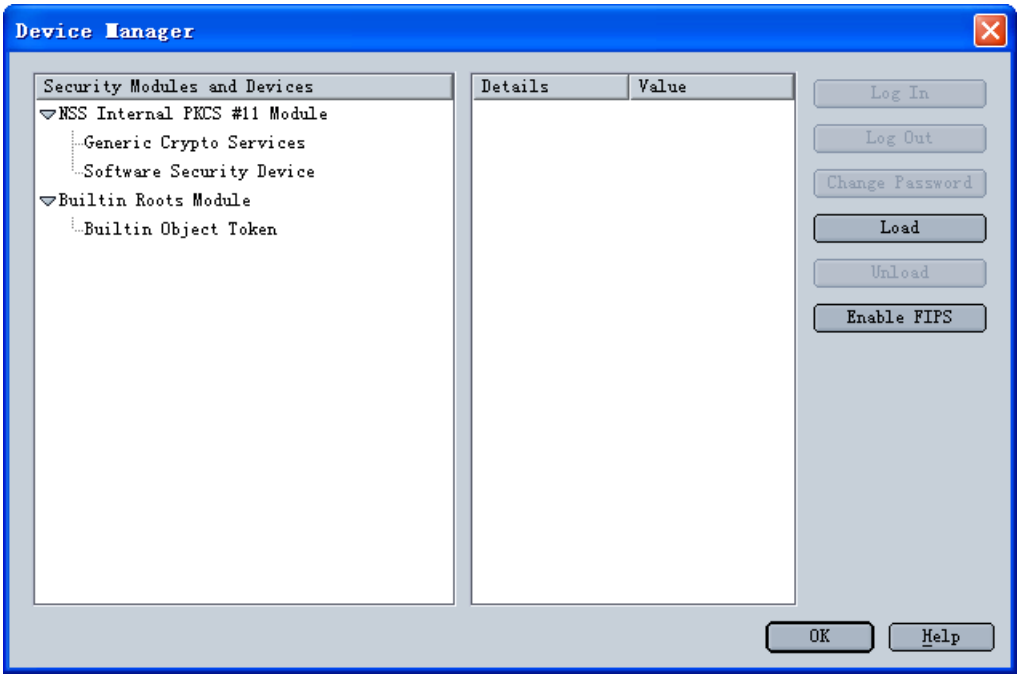


图 3 设备管理器界面

**4.** 按右侧的“Load”按钮，Netscape弹出对话框，请您输入安全模块的名称和路径，路径为C:\WINDOWS\system32\ngp11v211.dll，如图 4所示：

**注意：“Module Name”（模块名）建议不要使用缺省字符串，要输入自己命名的名称。**

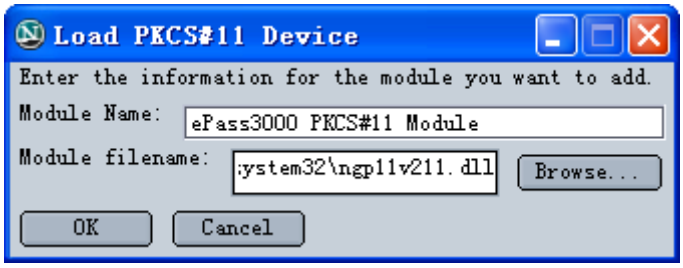


图 4 加载 PKCS#11 设备对话框

**5.** 点击“OK”按钮后，Netscape弹出确认对话框，询问是否确定要安装该安全模块，如图 5所示：

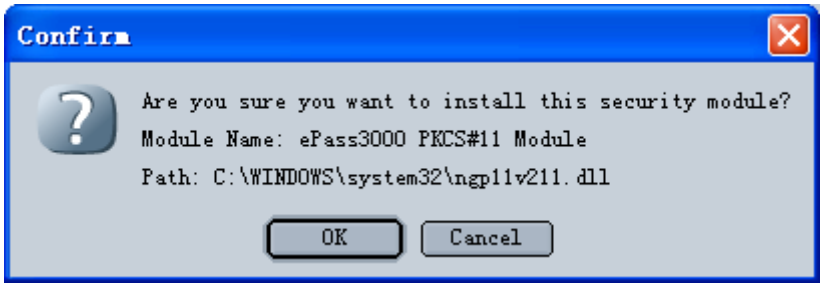


图 5 确认安装 PKCS#11 模块对话框

**6.** 点击“OK”按钮后，Netscape就会进行安装的过程，在此过程中将访问该安全模块的库文件。如果安装正确，Netscape将弹出对话框，告诉用户安装成功，如图 6所示：

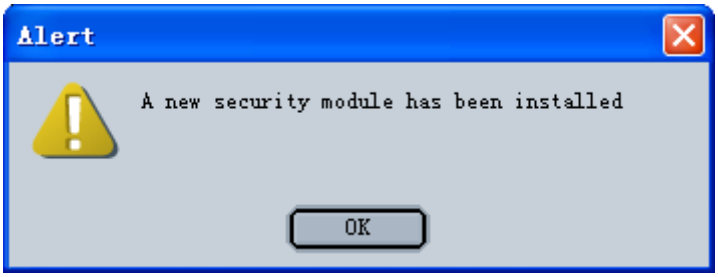


图 6 安装成功确认对话框

**7.** 点击“OK”按钮后，在设备管理器的左侧就会出现ePass3000 模块的信息，其中“ePass3000 PKCS#11 Module”显示有一把名称为“ePass3000”的USB Key插入了计算机的USB接口，如图 7所示：

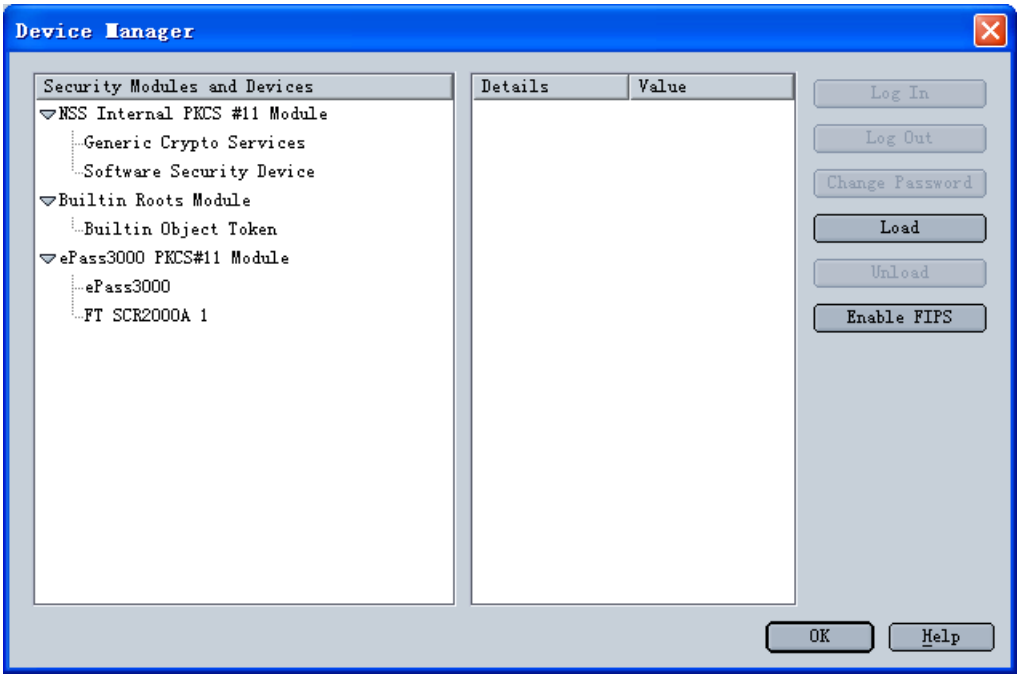


图 7 集成了 ePass3000 的设备管理器

此时您已经成功将 ePass3000 与 Netscape 集成了，您可以对该 ePass3000 进行“登录（Log In）”和“登出（Log Out）”的操作。

## 1.2 使用ePass3000 的PKCS#11 申请数字证书

我们以在 Windows 平台下的 Netscape 为例来说明使用 PKCS#11 的证书申请过程。

**1.** 确认已经插入了一支已经初始化过的ePass3000，启动Netscape，打开证书颁发机构的网页，选择“申请证书”单选按钮，如图 8所示：

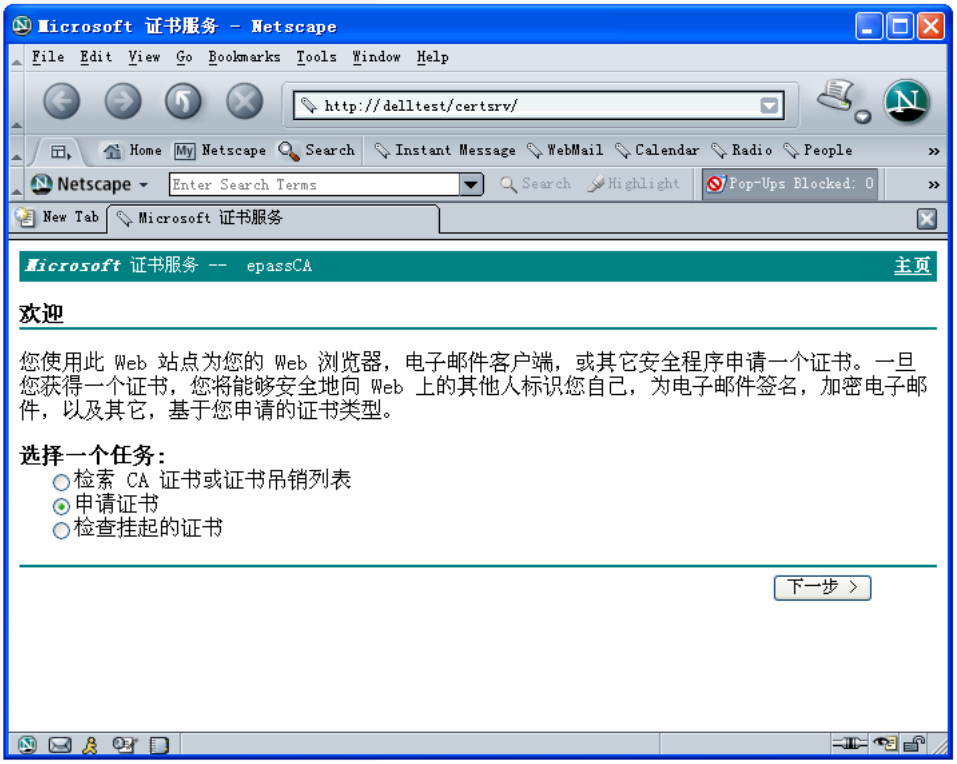


图 8 证书服务器界面

**2.** 点击“下一步”按钮进入“选择申请类型”界面，选择“用户证书申请”单选按钮，如图 9所示：

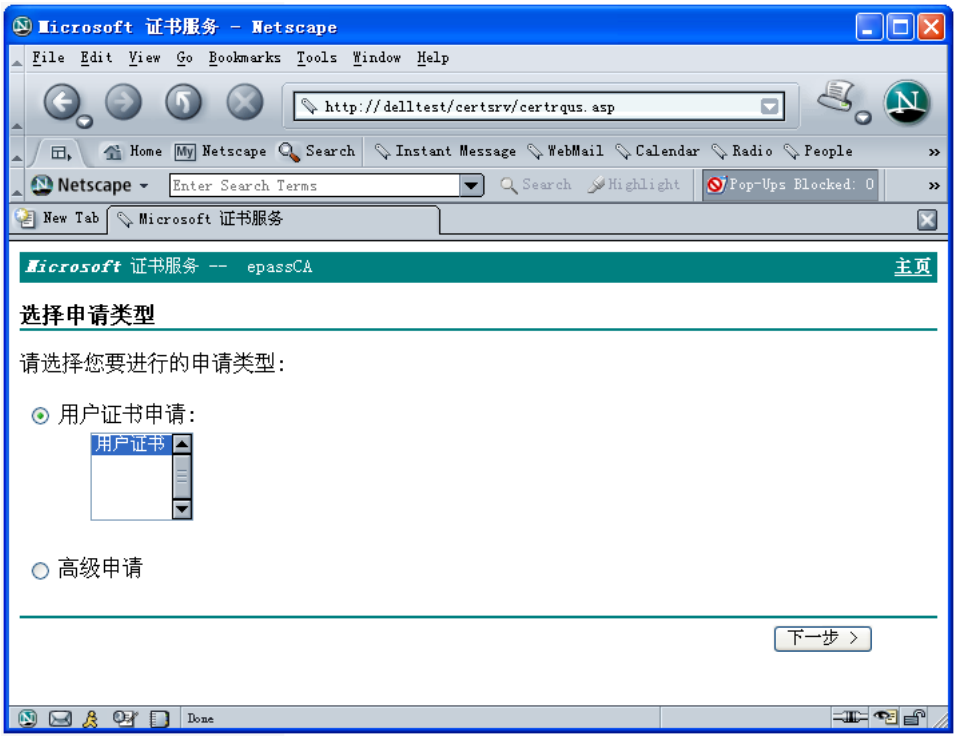


图 9 选择申请证书类型界面

**3.** 点击“下一步”按钮，进入选择密钥长度的页面，在下拉框中选择合适的密钥长度，如图 10所示：


图 10 选择密钥长度

**4.** 点击“提交”按钮后，Netscape弹出Token列表，要求选择所要产生密钥对的安全设备，从中选择ePass3000，然后按“OK”按钮，如图 11所示：

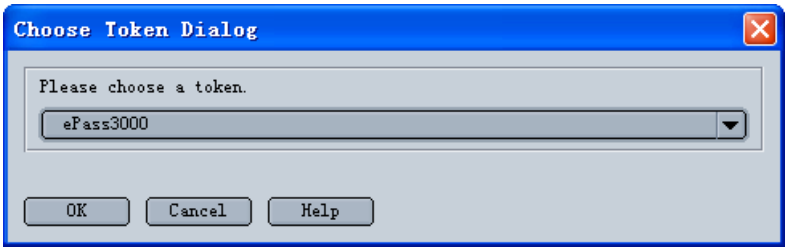


图 11 选择 Token 对话框

**5.** 这时，Netscape弹出对话框要求用户输入PIN码，如图 12所示：


图 12 输入 PIN 码对话框

**注意：如果您在1.1的最后一步中已经登录了，那么此处就不会出现PIN码框而直接产生密钥对。**

**6.** 输入ePass3000 的PIN码后点击“OK”按钮，Netscape开始产生密钥对，如图 13所示：

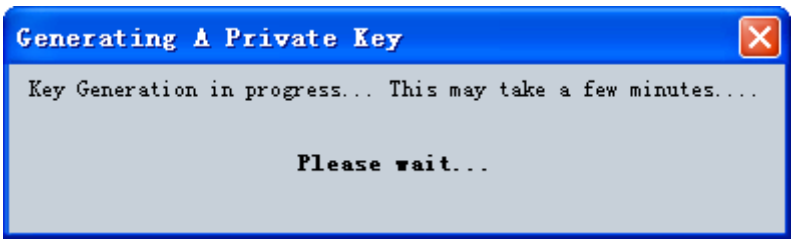


图 13 产生密钥对界面

**7.** 密钥对产生完成后，Netscape将密钥信息及个人信息发送给证书颁发机构，由证书颁发机构颁发证书，成功后转向如图 14所示的页面：

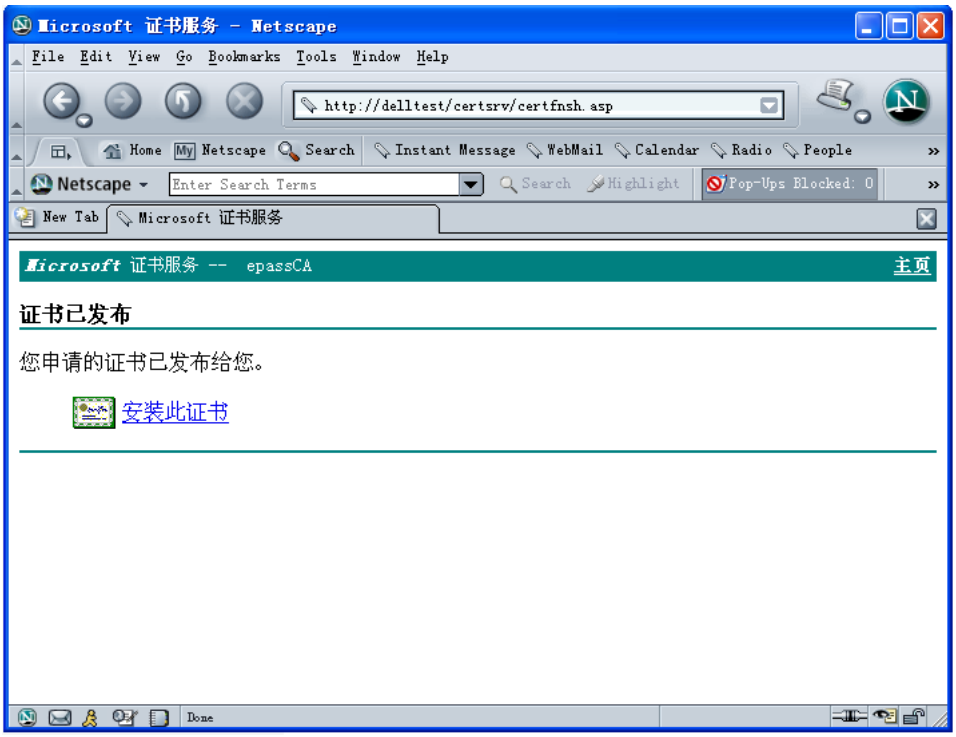


图 14 证书已发布界面

**8.** 点击图 14所示页面的“安装此证书”链接，Netscape将该证书安装到ePass3000 中。

至此，整个证书申请流程完成，您可以通过 ePass3000 管理工具查看申请的证书。

## 1.3 使用ePass3000 的PKCS#11 访问SSL加密站点

**1.** 确认已经在计算机的 USB 接口上插入含有证书的 ePass3000。启动 Netscape，用 https 协议访问 SSL 站点（本例中为 https://delltest）。

**2.** 如果一切正常，Netscape将陆续弹出所有和计算机连接的安全设备的密码框，此处只有ePass3000和计算机连接，其PIN码输入框如图 15所示：


图 15 PIN 码输入框

**3.** 输入PIN码并点击“OK”按钮后Netscape将访问ePass3000 的PKCS#11 接口，加载ePass3000 上的密钥和证书信息，然后弹出所有符合要求的证书列表请用户选择其中一个作为用户的身份信息，如图 16所示：

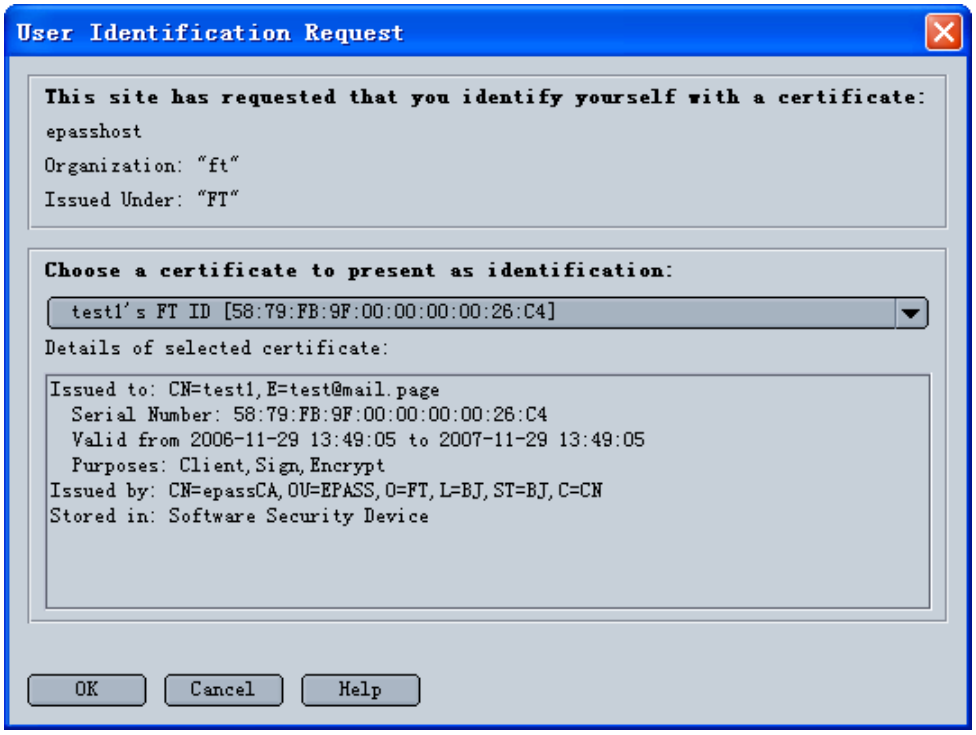


图 16 证书列表

**注意：如果在图 2所示的属性设置窗口中的“Client Certificate Selection”栏中选择“Select Automatically”单选按钮，Netscape会自动选择证书，则不会弹出图 16所示的选择证书对话框，如果选择“Ask Every Time”单选按钮，才会弹出图 16所示的对话框。**

**4.** 选择相应的用户证书后按“OK”按钮，Netscape就会和该SSL网站交换信息，并进行一系列的认证过程。如果一切都符合要求，则所访问的页面就会显现出来，如图 17所示（此安全Web站点为示例站点）：

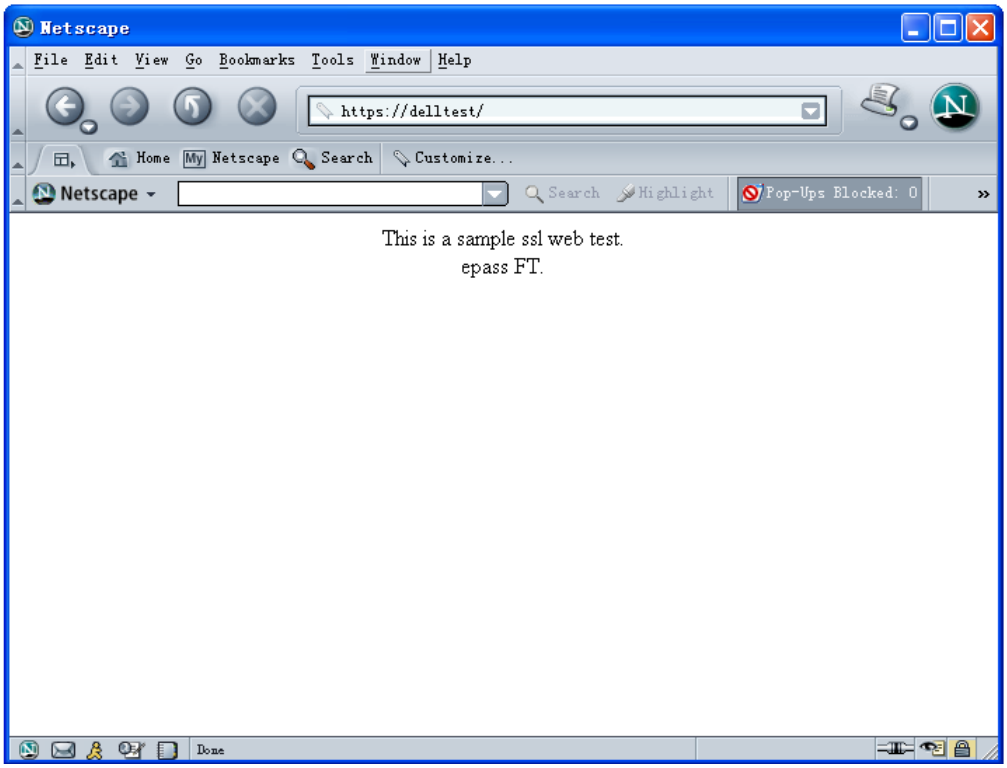


图 17 访问 SSL 站点成功

## 1.4 使用ePass3000 的PKCS#11 收发签名与加密邮件

本节以 Windows 平台下的 Netscape Mail 为例来说明使用 PKCS#11 获取安全邮件证书以及收发签名与加密邮件的过程。

在开始设置 Netscape Mail 收发签名与加密邮件之前，假设已经将 Netscape Mail 设置好，可以连接上电子邮件服务器以及电子邮件帐号的相关设置，换句话说，用户已经可以使用一般的方式发送/接收电子邮件。要设置 Netscape Mail 的安全设置，必须先获取具有电子邮件安全处理能力的证书，当获取用户的安全邮件证书后，用户才可以发送具有数字签名或者信息加密的电子邮件。

### 1.4.1 获取安全邮件数字证书

获取安全邮件数字证书的方法与1.2节中使用ePass3000 的PKCS#11 申请数字证书的方法大致相同，具体申请方法与CA服务器的设置和选项相关，申请的数字证书必须是具有邮件属性的数字证书。当获取数字证书后，用户就可以开始设置Netscape Mail中的Email帐号，让Email帐号能够具有安全性邮件的处理能力。

### 1.4.2 设置E-mail帐号的安全性

设置 Netscape 中的 Email 帐号中的安全性功能，按照下列的操作步骤依序进行操作：

**1.** 启动Netscape Mail（在Netscape主界面左下角第二个图标或菜单项的“Windows”→“Mail & Newsgroups”），用户需首先确定已经获取了使用在安全性邮件的数字证书。选择菜单“Edit”→“Mail & Newsgroups Account Settings…”，如图 18所示：

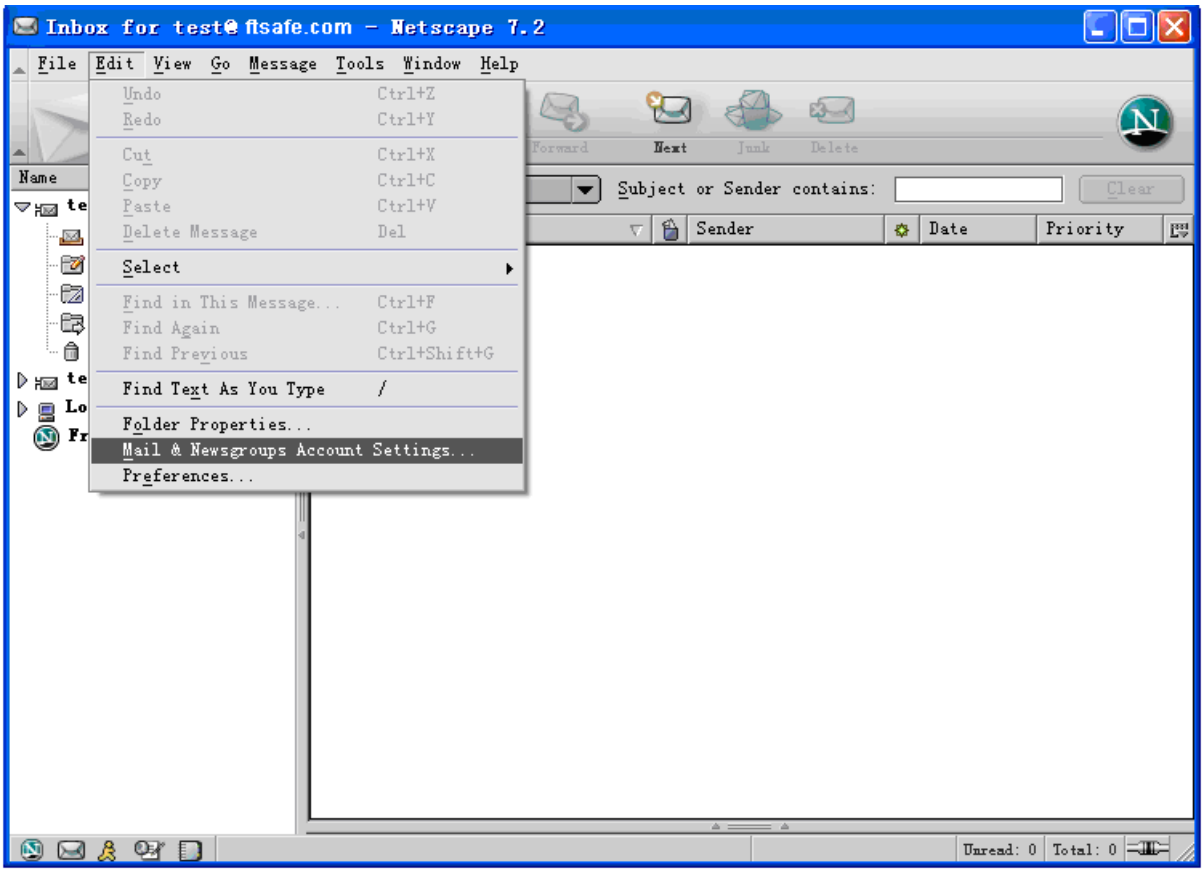


图 18 帐号设置菜单

**2.** 系统弹出帐号设置对话框，在左侧树状列表中选择test@ftsafe.com 帐号下面的“Security”菜单项，右侧出现安全配置界面，如图 19所示：

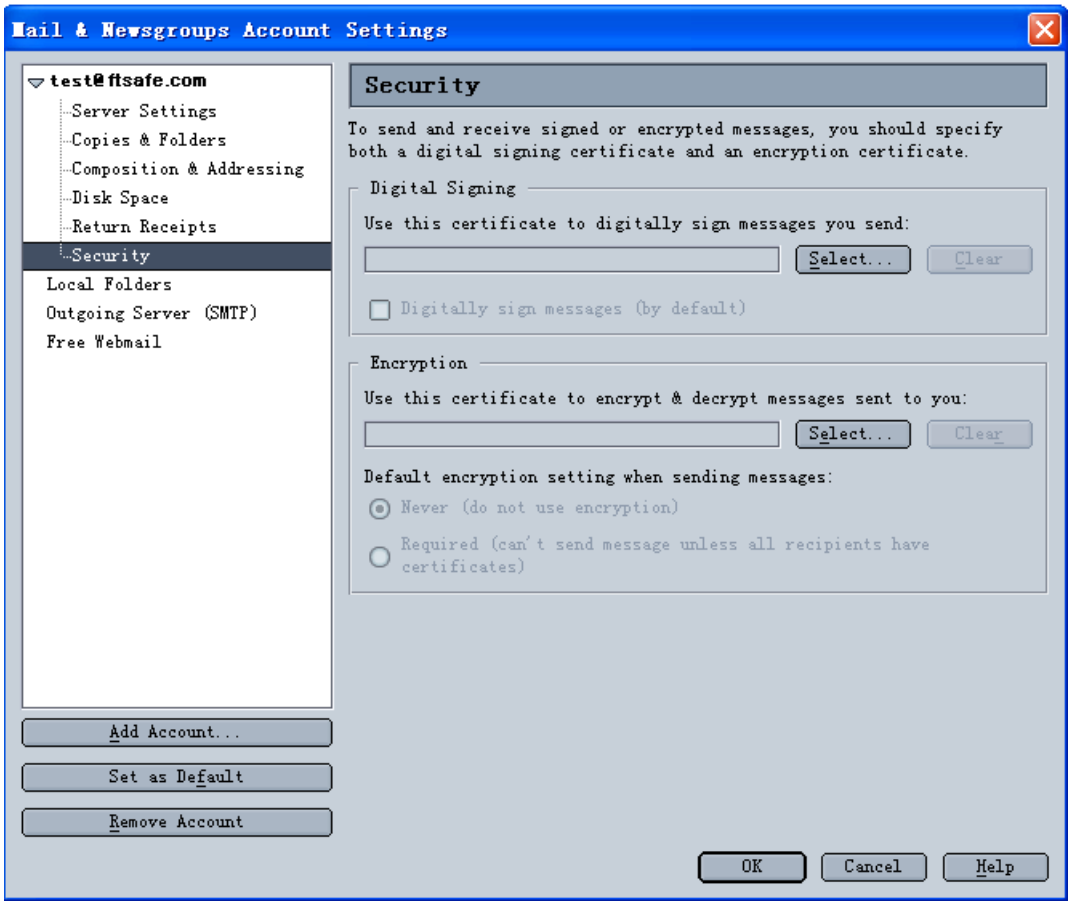


图 19 帐号安全设置界面

**3.** 选择右侧上面的“Select”按钮，Netscape就将系统（ePass3000）中test@ftsafe.com帐号的签名证书列出，供用户选择，如图 20所示：

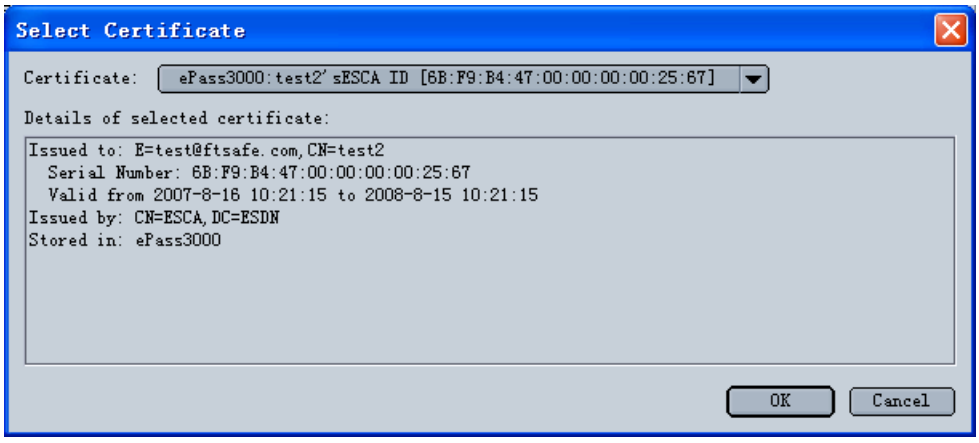


图 20 签名证书对话框

**4.** 选择具有邮件属性的数字证书，点击“OK”按钮后，签名证书就出现在上面的“Select”按钮前面的空白栏中。然后Netscape又弹出对话框提示用户指定一个加密证书由其他人给test@ftsafe.com发送加密邮件时使用，如图 21所示：

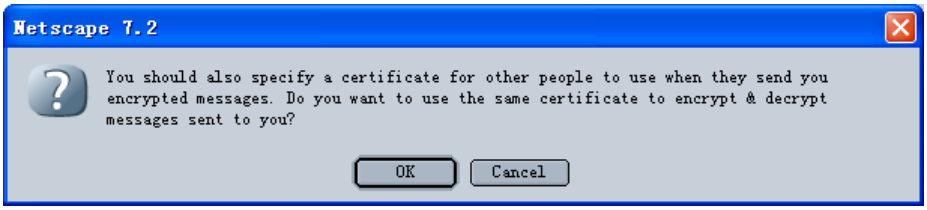


图 21 提示指定加密证书对话框

**5.** 点击“OK”按钮后Netscape自动将指定的签名证书作为加密证书使用，这样加密证书栏中就出现了相应的证书路径，如图 22所示：

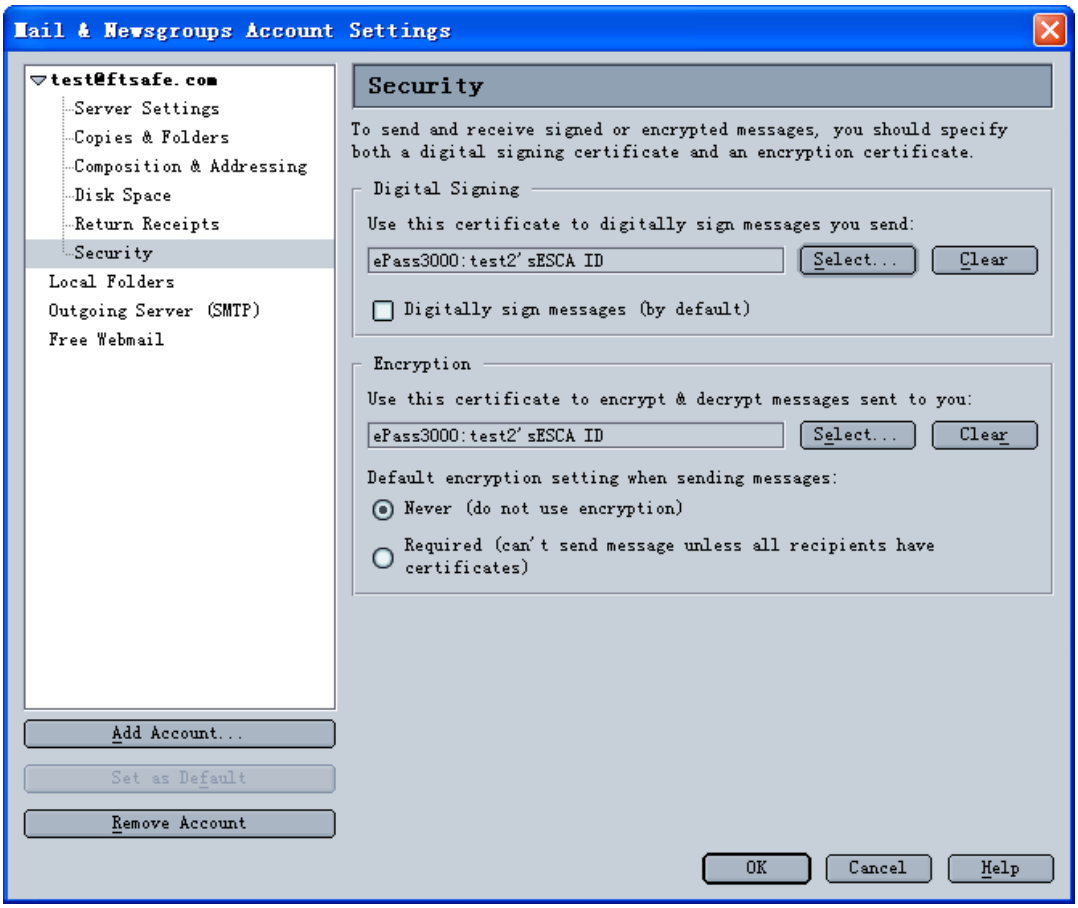


图 22 指定完签名加密证书界面

在上图中，您可以勾选“Digitally sign messages(by default)”的选项来指定在缺省情况下对发出去的邮件进行签名，同时也可以勾选“Required(can’t sent message unless all recipients have certificates)”指定在需要情况下对发出去的邮件进行加密。你也可以采用下面几小节的方法来对发出去的邮件进行签名或加密。

至此，已经将 test@ftsafe.com 帐号的签名证书和加密证书设置完成，可以发送签名和加密的邮件了。

### 1.4.3 使用Netscape Mail发送附加数字签名的邮件

当设置好 Netscape Mail 里的安全设置选项后，用户就可以开始发送具有安全性质的电子邮件。现在，我们就来看看如何在发送出去的邮件中附加数字签名。按照下列的步骤进行操作：

**1.** 启动Netscape Mail，点击工具栏上的“Compose”按钮，打开书写新邮件的编辑器，如图 23所示：

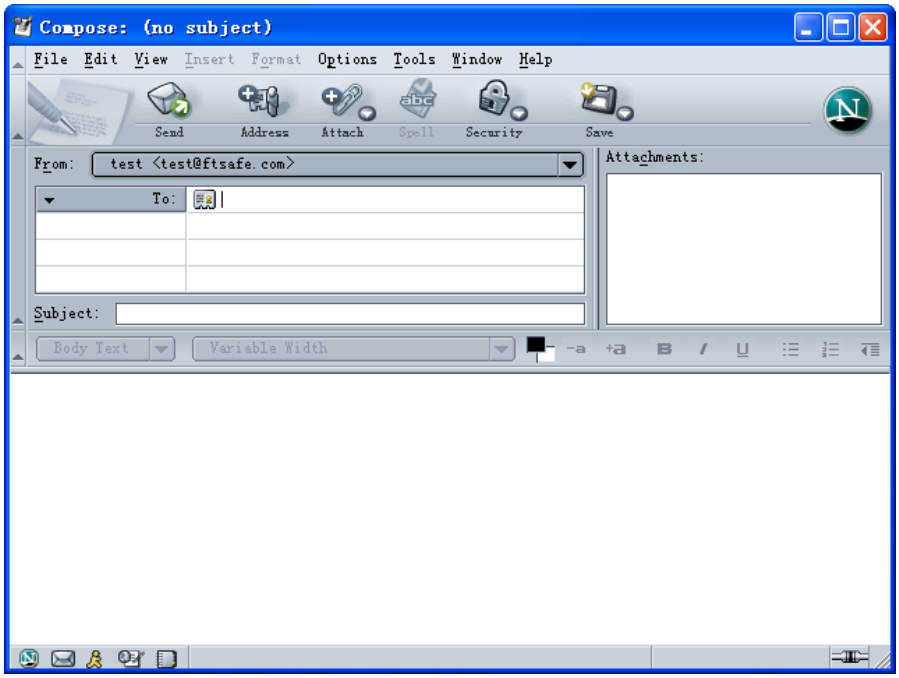


图 23 书写新邮件界面

**2.** 所有内容书写完毕后，点击工具栏上的“Security”按钮，在弹出菜单中选择“Digitally Sign This Message”（如图 24所示），或者选择Netscape Mail的菜单“Options” →“Security” →“Digitally Sign This Message”（如图 25所示），将该邮件签名。

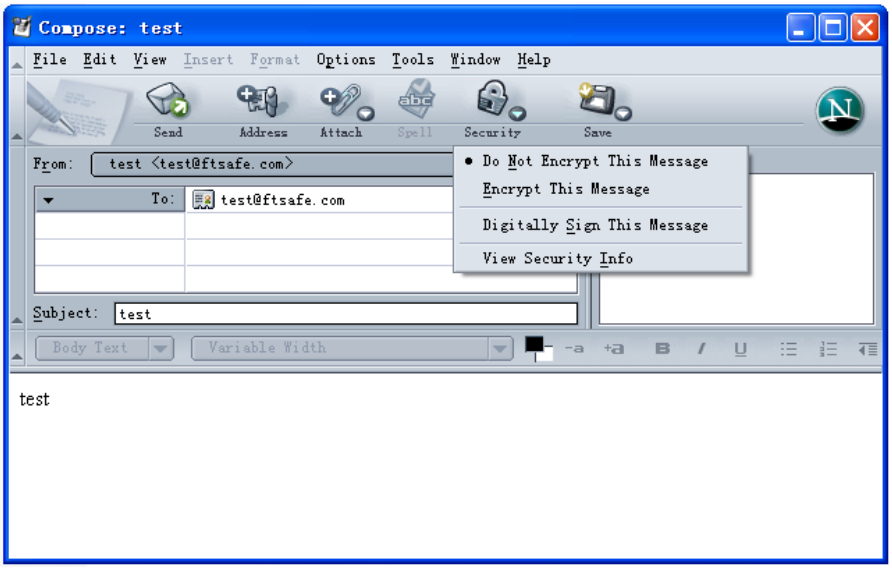


图 24 签名邮件菜单

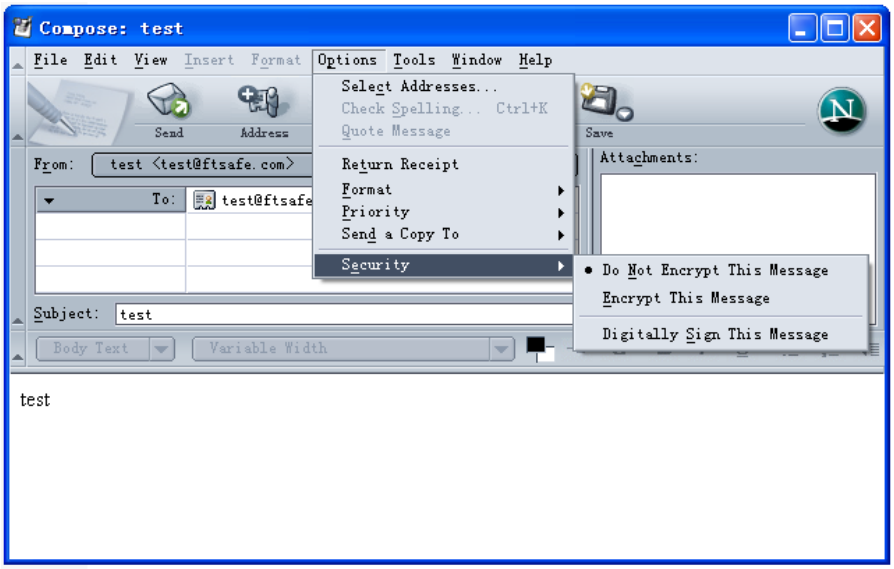


图 25 签名邮件菜单

**3.** 然后点击工具栏上的“Send”按钮，发出该邮件。如果以前没有输入过 ePass3000 的 PIN 码，则 Netscape Mail 会弹出 PIN 码输入框，请求输入用户 PIN 码，用户输入正确的 PIN 码后即可将邮件发送出去。

### 1.4.4 获取收件人的公钥和证书

若要发送加密的电子邮件，用户必须先获取对方的公钥或者证书，再利用对方的公钥对用户信件进行加密处理（也就是使用收件人的公钥来进行加密），这时候，只有此公钥映射的私钥（此私钥只有收件人持有）才能够对此加密过的信件进行解密的处理，因此，只有持有该私钥的人，才能够阅读该信件。

用户要获取对方的公钥或者证书，必须要求对方发送一封带有数字签名的信件，用户将此带有数字签名信息的邮件中的证书存储下来，这时候用户就拥有了对方的证书以及公钥的信息。

若要存储证书或公钥，请按照下列的步骤进行操作：

**1.** 先要求对方以上一个小节的方式发送一份夹带有数字签名的电子邮件给您。

**2.** 启动Netscape Mail，接收并打开对方发送过来的带有数字签名的电子邮件，鼠标点击该邮件右侧的钢笔模样（如图 26所示的红色圆形区域）的图标，Netscape弹出一窗口显示发送者的信息及签名证书，以供用户检查该数字签名的正确性，如图 26所示：

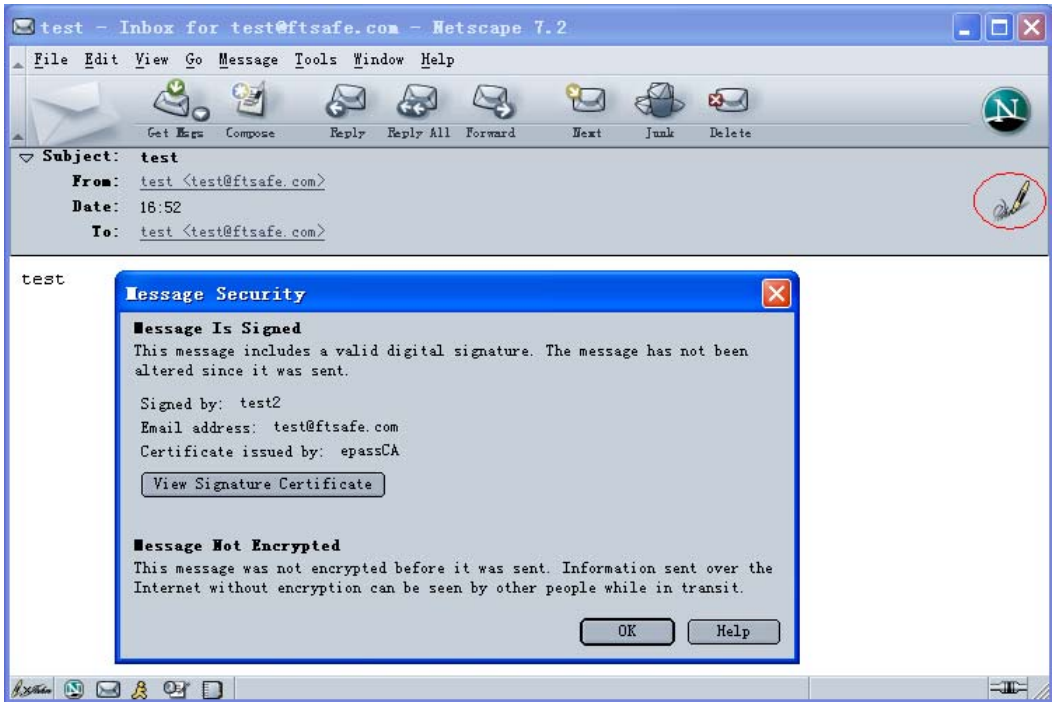


图 26 查看邮件签名对话框

**3.** 点击“OK”按钮关闭查看签名的窗口，在图 26中左侧的From栏后面的邮件地址上鼠标单击，则出现如图 27所示的菜单：

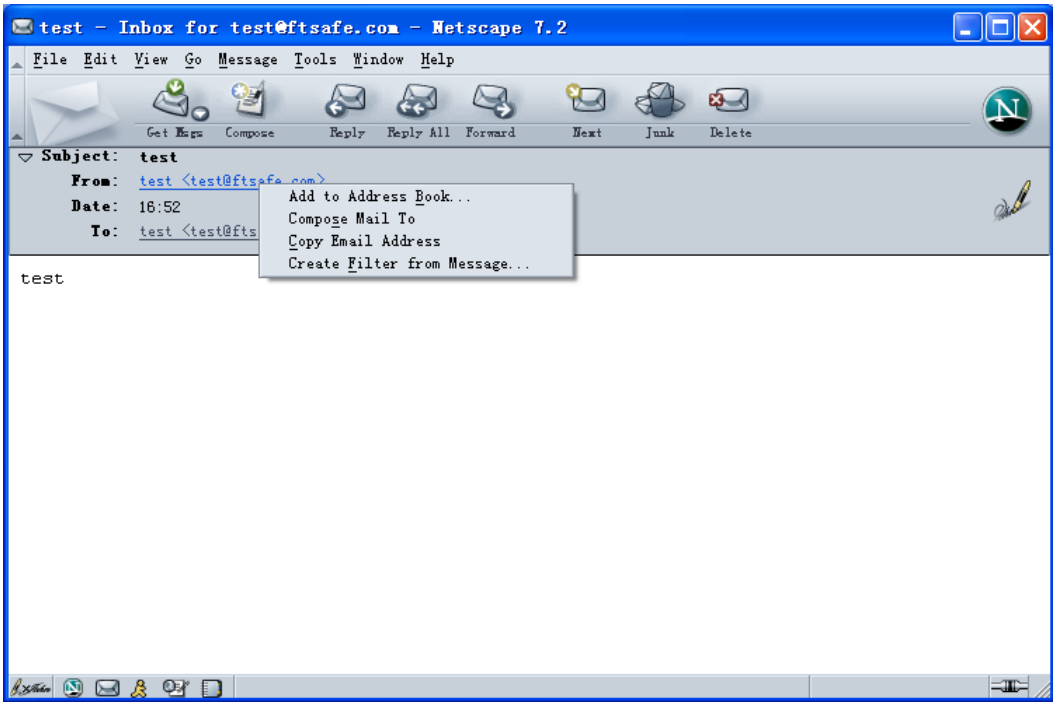


图 27 地址菜单

**4.** 选择“Add to Address Book”，将对方的姓名及地址加入到地址簿中。这样对方的证书已经和其邮件地址关联起来了。

实际上如果收到过对方的签名邮件，那么该邮件地址和其证书已经被自动关联起来并被 Netscape Mail 记录下来。以后发送加密邮件时只要在收件人栏中写入该邮件地址，Netscape Mail 会自动使用其关联的证书。

### 1.4.5 使用Netscape Mail发送加密邮件

若要发送加密的邮件给对方，要确定发件人已经使用上一个小节的方式获取对方的公钥或者证书等信息（证书包含了公钥信息）。在这里，假设发件人已经以上一个小节的方式获取对方的公钥证书并且已经存储在 Netscape 的通讯簿列表里了。

要发送一封加密的邮件，按照下列的步骤进行操作：

**方法一：直接回复发件人**

1. 启动 Netscape Mail。
2. 选中对方发过来的邮件，然后选择Mail工具栏中的“Reply”按钮（Netscape Mail的界面及工具栏的布局见图 26），则Netscape打开书写回复邮件的界面窗口。
3. 书写完毕后，选择“Security”按钮，或者选择Netscape Mail的菜单“Options” →“Security”，在弹出的菜单中选中“Encrypt This Message”（见图 24和图 25）。
4. 然后点击工具栏上的“Send”按钮，发出该邮件。如果以前没有输入过 ePass3000 的 PIN 码，则 Netscape Mail 会弹出 PIN 码输入框，请求输入用户 PIN 码，输入正确的 ePass3000 的 PIN 码后点击“OK”按钮即可将邮件发出。

**方法二：直接输入收件人邮件地址**

1. 启动 Netscape Mail。
2. 点击工具栏上的“Compose”按钮（Netscape Mail的界面及工具栏的布局见图 26），打开书写新邮件的编辑器。
3. 在邮件的收件人中填入正确的电子邮件地址，则 Netscape Mail 自动会使用该电子邮件地址所关联的证书作为加密证书。
4. 书写完毕后，选择“Security”按钮，或者选择Netscape Mail的菜单“Options” →“Security”，在弹出的菜单中选中“Encrypt This Message”（见图 24和图 25）。
5. 然后点击工具栏上的“Send”按钮，发出该邮件。如果以前没有输入过 ePass3000 的 PIN 码，则 Netscape Mail 会弹出 PIN 码输入框，请求输入用户 PIN 码，输入正确的 ePass3000 的 PIN 码后点击“OK”按钮即可将邮件发送出去。

**方法三：从地址簿中选择收件人**

1. 启动 Netscape。
2. 选取菜单“Window”→“Address Book”，如图 28所示：

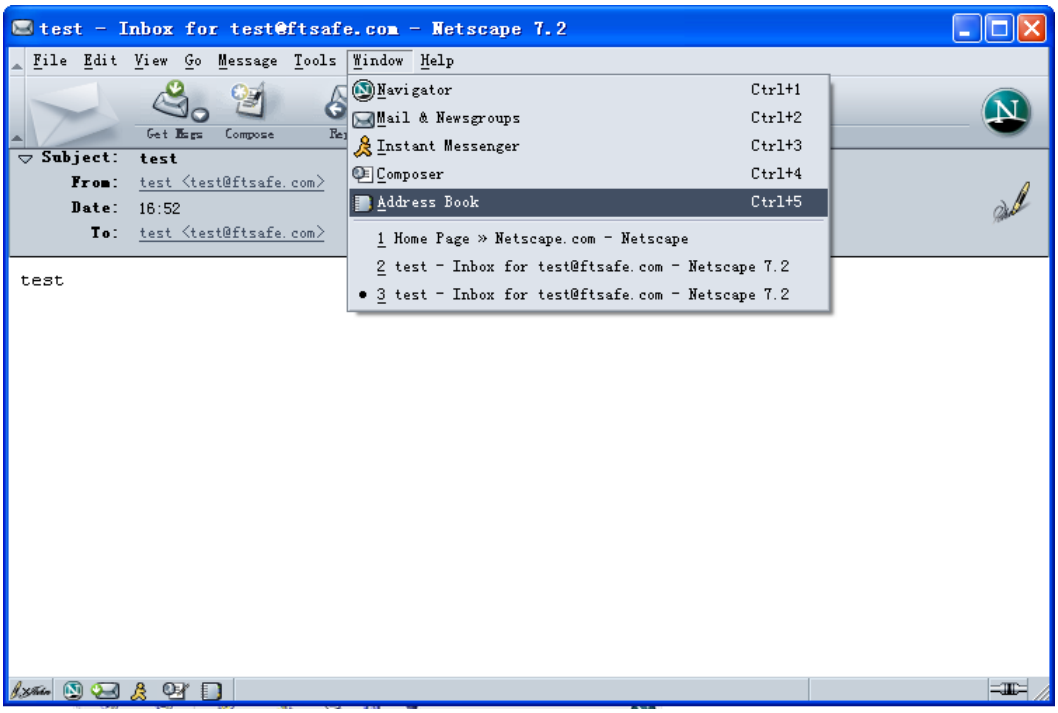


图 28 Netscape Address Book 菜单

**3.** 选取“Address Book”菜单后，Netscape将地址簿窗口打开，如图 29所示：

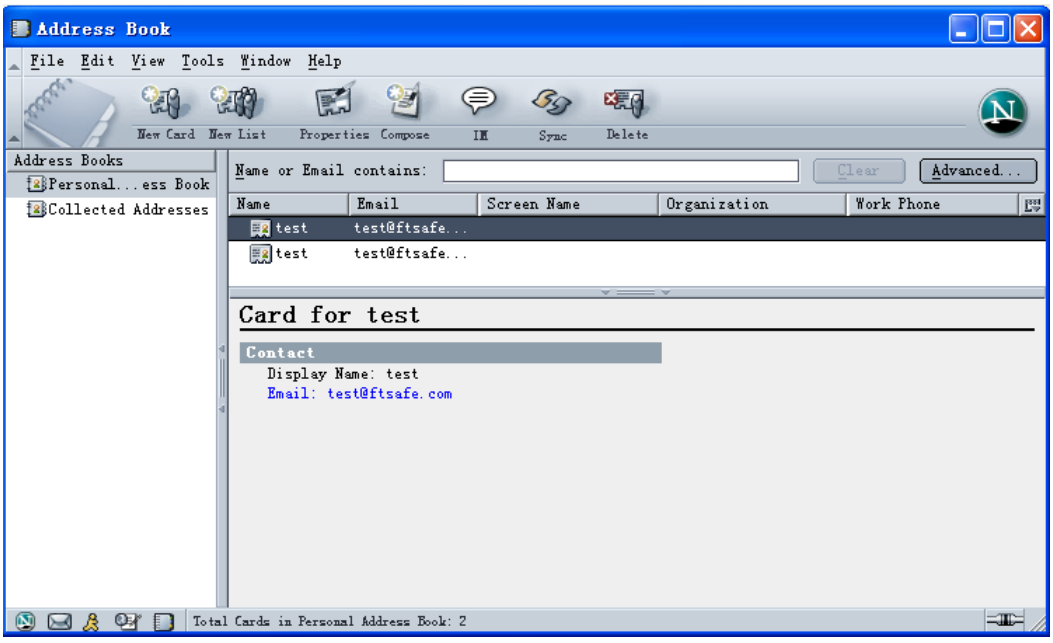


图 29 Netscape 地址簿

**4.** 选择要发送邮件的地址，然后点击工具栏中的“Compose”，则Netscape Mail的书写新邮件的窗口就会打开，如图 23所示。

以后的步骤和方法二的步骤 4 和 5 相同。

## 1.4.6 使用Netscape Mail发送签名加密邮件

这个过程与发送加密或签名邮件的过程相同，只不过在选择安全选项时（见图 24和图 25）将“Encrypt This Message”和“Digitally Sign This Message”同时选中即可。