

ePass3003 的 Netscape 应用

1.2 版



版权所有© 2007-2012 EnterSafe

<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以任何 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

第一章	ePass3003 的 Netscape 应用.....	1
1.1	Windows 平台下 Netscape 与 ePass3003 的应用	1
1.2	使用 ePass3003 的 PKCS#11 申请数字证书.....	4
1.3	使用 ePass3003 的 PKCS#11 访问 SSL 加密站点.....	7
1.4	使用 ePass3003 的 PKCS#11 收发签名与加密邮件.....	9
1.4.1	获取安全邮件数字证书.....	9
1.4.2	设置 E-mail 帐号的安全性.....	9
1.4.3	使用 Netscape Mail 发送附加数字签名的邮件	12
1.4.4	获取收件人的公钥和证书.....	14
1.4.5	使用 Netscape Mail 发送加密邮件.....	16
1.4.6	使用 Netscape Mail 发送签名加密邮件.....	17
附录	缩略语及术语	19

图目录

图 1 Preferences 菜单.....	1
图 2 Certificates 配置页面.....	2
图 3 设备管理器界面.....	2
图 4 加载 PKCS#11 设备对话框.....	3
图 5 确认安装 PKCS#11 模块对话框.....	3
图 6 安装成功确认对话框.....	3
图 7 集成了 ePass3003 的设备管理器.....	4
图 8 证书服务器界面.....	5
图 9 选择申请证书类型界面.....	5
图 10 选择密钥长度.....	6
图 11 选择 Token 对话框.....	6
图 12 输入 PIN 码对话框.....	6
图 13 产生密钥对界面.....	7
图 14 证书已发布界面.....	7
图 15 PIN 码输入框.....	8
图 16 证书列表.....	8
图 17 访问 SSL 站点成功.....	9
图 18 帐号设置菜单.....	10
图 19 帐号安全设置界面.....	10
图 20 签名证书对话框.....	11
图 21 提示指定加密证书对话框.....	11
图 22 指定完签名加密证书界面.....	12
图 23 书写新邮件界面.....	13
图 24 签名邮件菜单.....	13
图 25 签名邮件菜单.....	14
图 26 查看邮件签名对话框.....	15
图 27 地址菜单.....	15
图 28 Netscape Address Book 菜单.....	17
图 29 Netscape 地址簿.....	17

第一章 ePass3003 的 Netscape 应用

ePass3003 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 ePass3003 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 ePass3003 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 CryptoAPI（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 ePass3003 的 Netscape 应用，本手册还讲述了在 Windows 上使用 ePass3003 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。

- ePass3003 与 Netscape 的集成
- 使用 ePass3003 的 PKCS#11 申请数字证书
- 使用 ePass3003 的 PKCS#11 访问 SSL 加密站点
- 使用 ePass3003 的 PKCS#11 收发签名与加密邮件

1.1 Windows 平台下 Netscape 与 ePass3003 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 ePass3003 进行操作，必须使 Netscape 集成 ePass3003。您可以在 Netscape 的“安全设备管理器”中操作 ePass3003 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：

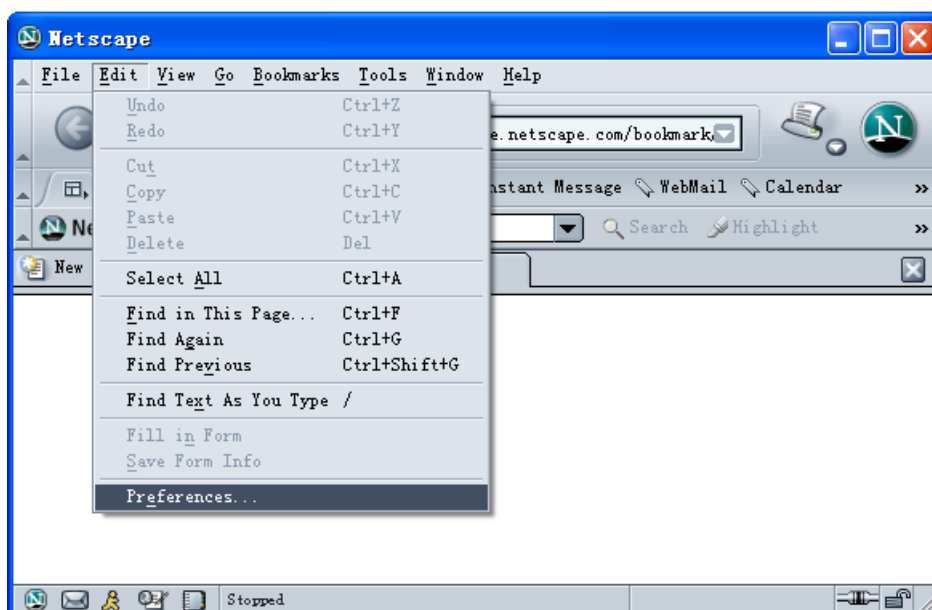


图 1 Preferences 菜单

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：

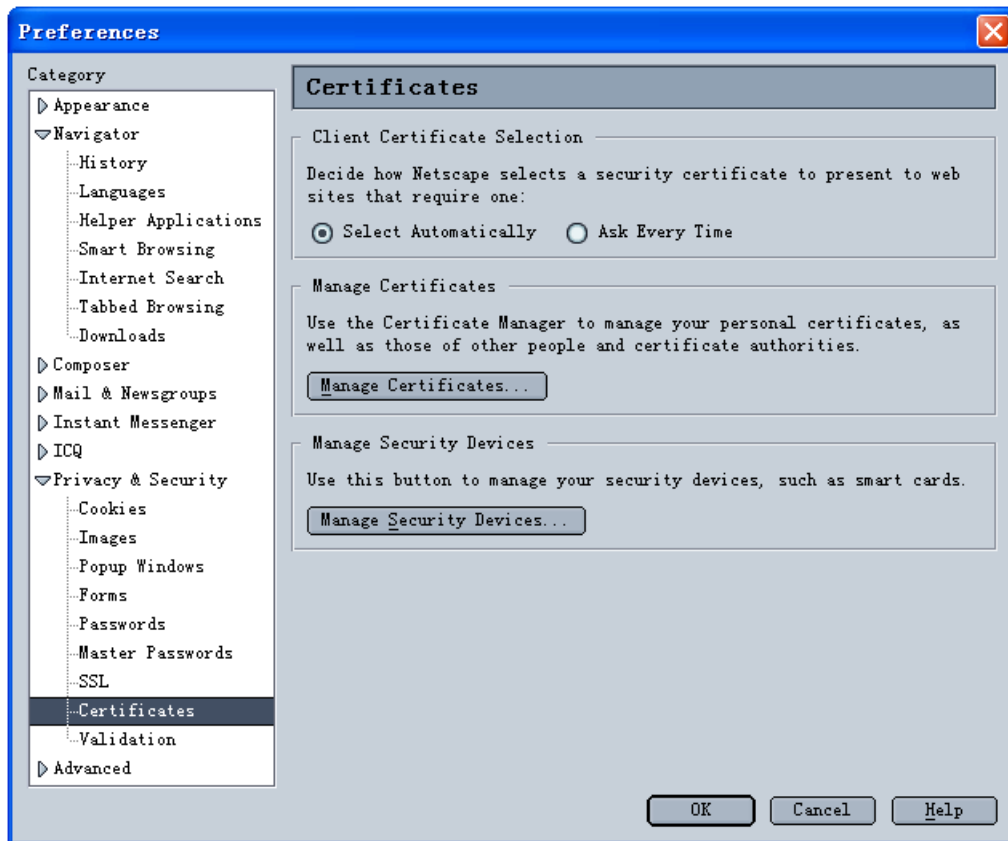


图 2 Certificates 配置页面

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

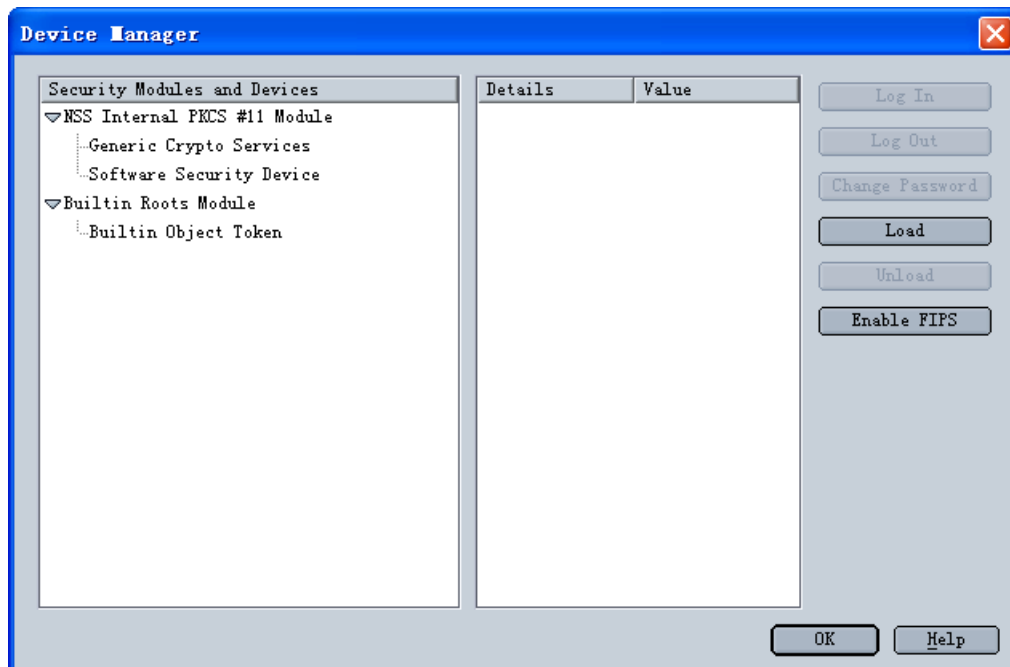


图 3 设备管理器界面

4. 按右侧的“Load”按钮，Netscape 弹出对话框，请您输入或选择安全模块的名称和路径，路径为 C:\WINDOWS\system32\ShuttleCsp11_3003.dll（C 盘为系统所在的盘符），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。

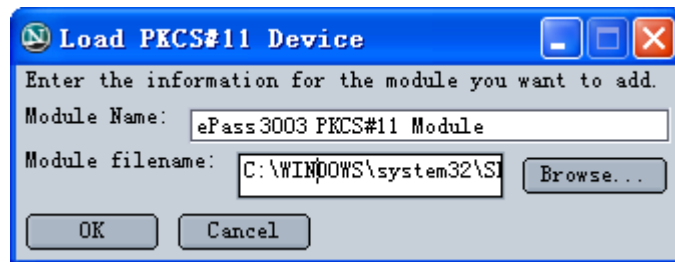


图 4 加载 PKCS#11 设备对话框

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：

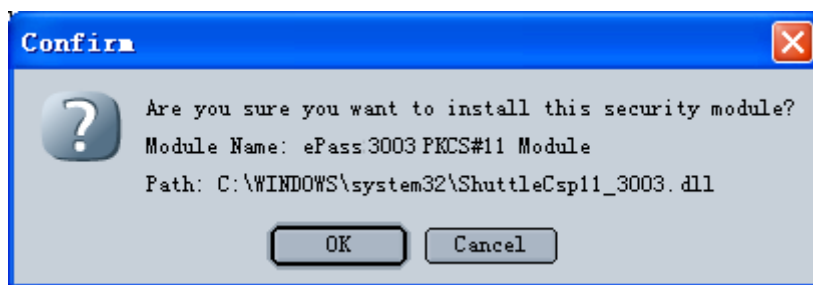


图 5 确认安装 PKCS#11 模块对话框

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：

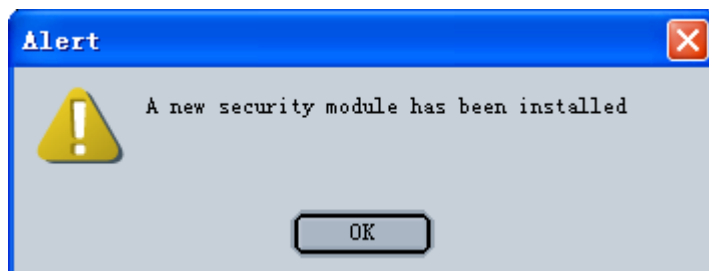


图 6 安装成功确认对话框

7. 点击“OK”按钮后，在设备管理器的左侧就会出现 ePass3003 模块的信息，其中“ePass3003 PKCS#11 Module”显示有一把名称为“ePass3003”的 USB Key 插入了计算机的 USB 接口，如图 7 所示：

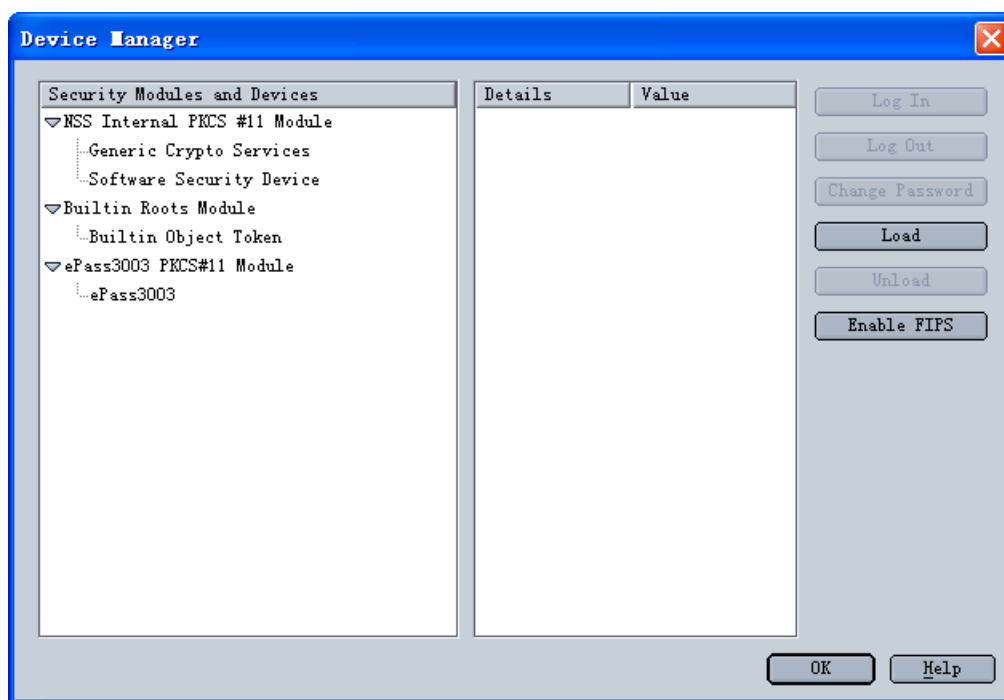


图 7 集成了 ePass3003 的设备管理器

此时您已经成功将 ePass3003 与 Netscape 集成了，您可以对该 ePass3003 进行“登录 (Log In)”和“登出 (Log Out)”的操作。

1.2 使用 ePass3003 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 ePass3003，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：

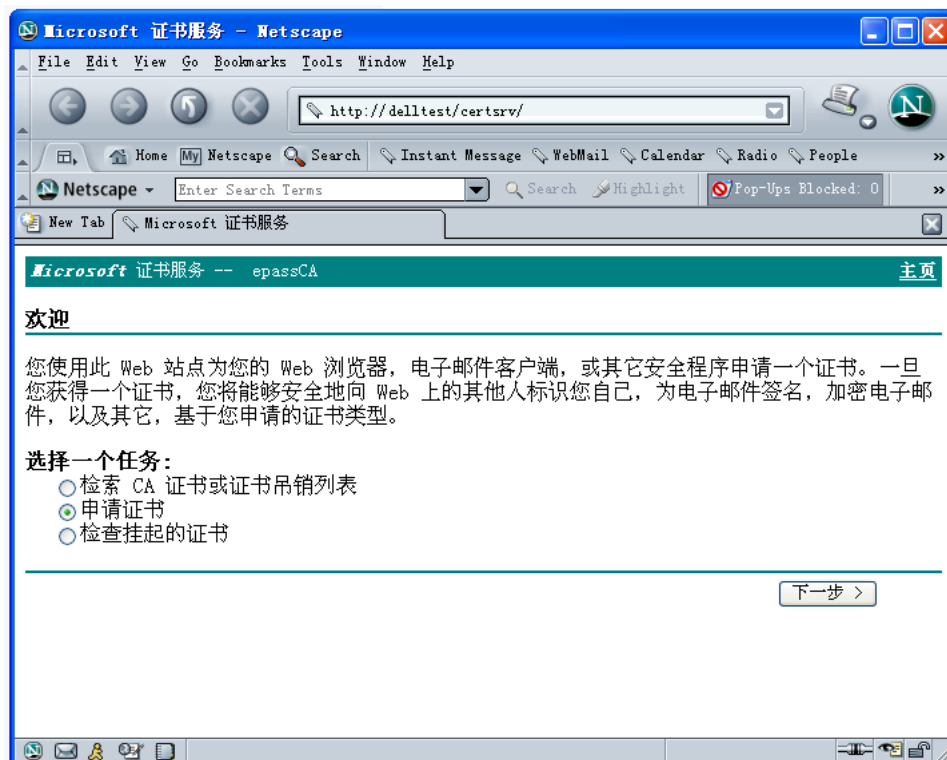


图 8 证书服务器界面

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：

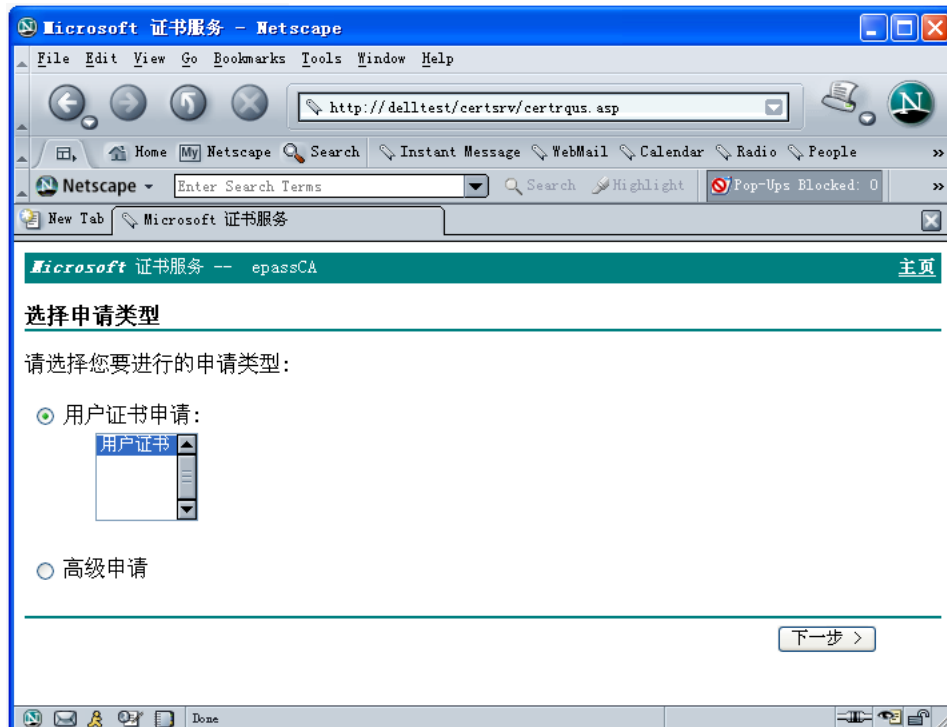


图 9 选择申请证书类型界面

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：

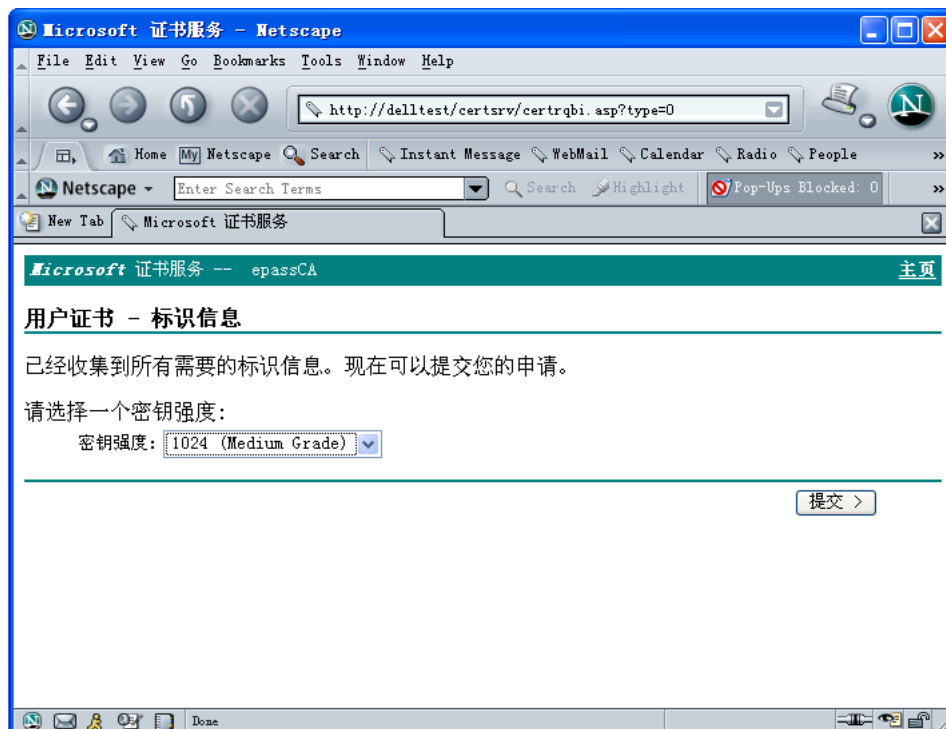


图 10 选择密钥长度

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 ePass3003，然后按“OK”按钮，如图 11 所示：

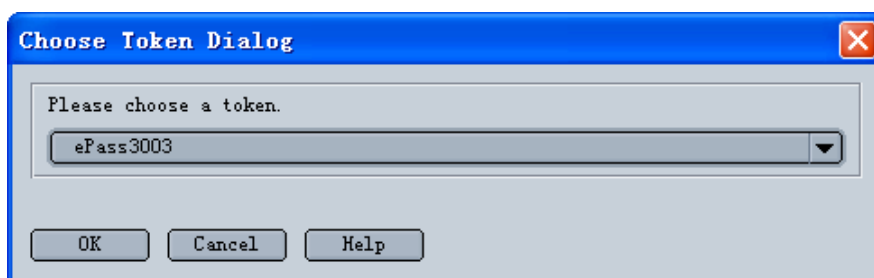


图 11 选择 Token 对话框

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

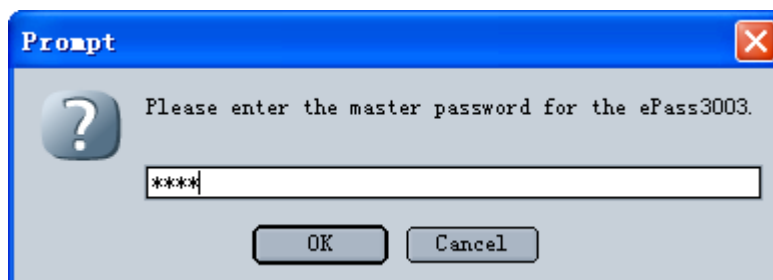


图 12 输入 PIN 码对话框

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 ePass3003 的 PIN 码后点击“OK”按钮，Netscape 开始产生密钥对，如图 13 所示：

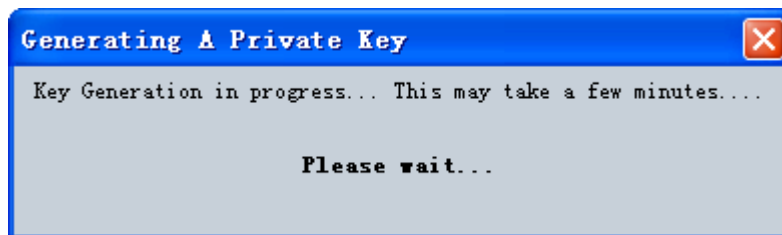


图 13 产生密钥对界面

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：

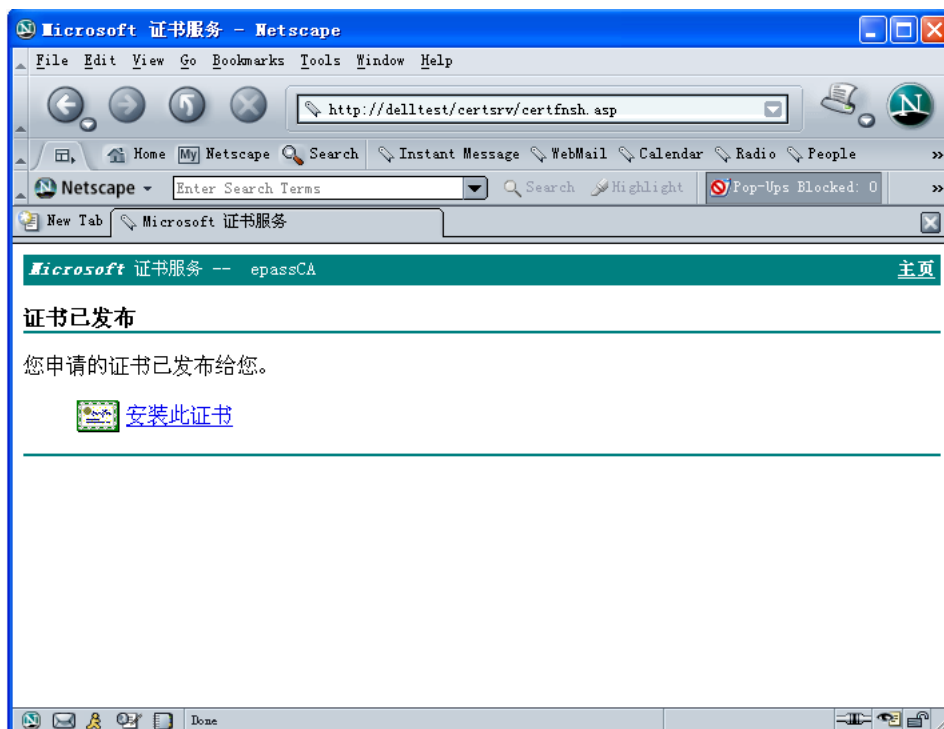


图 14 证书已发布界面

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 ePass3003 中。至此，整个证书申请流程完成。

1.3 使用 ePass3003 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 ePass3003。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 ePass3003 和计算机连接，其 PIN 码输入框如图 15 所示：

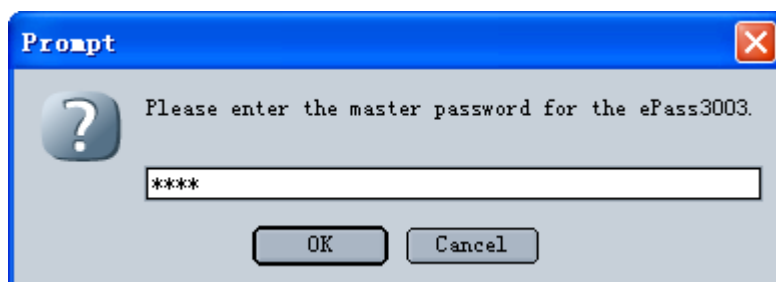


图 15 PIN 码输入框

3. 输入 PIN 码并点击“OK”按钮后 Netscape 将访问 ePass3003 的 PKCS#11 接口，加载 ePass3003 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：

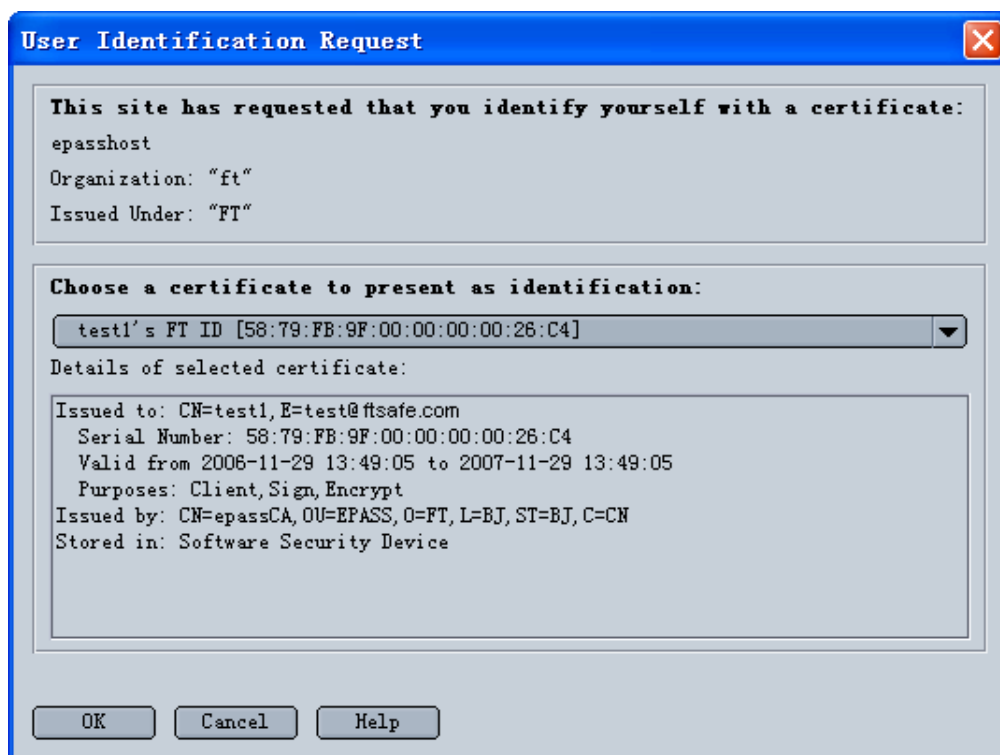


图 16 证书列表

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）：

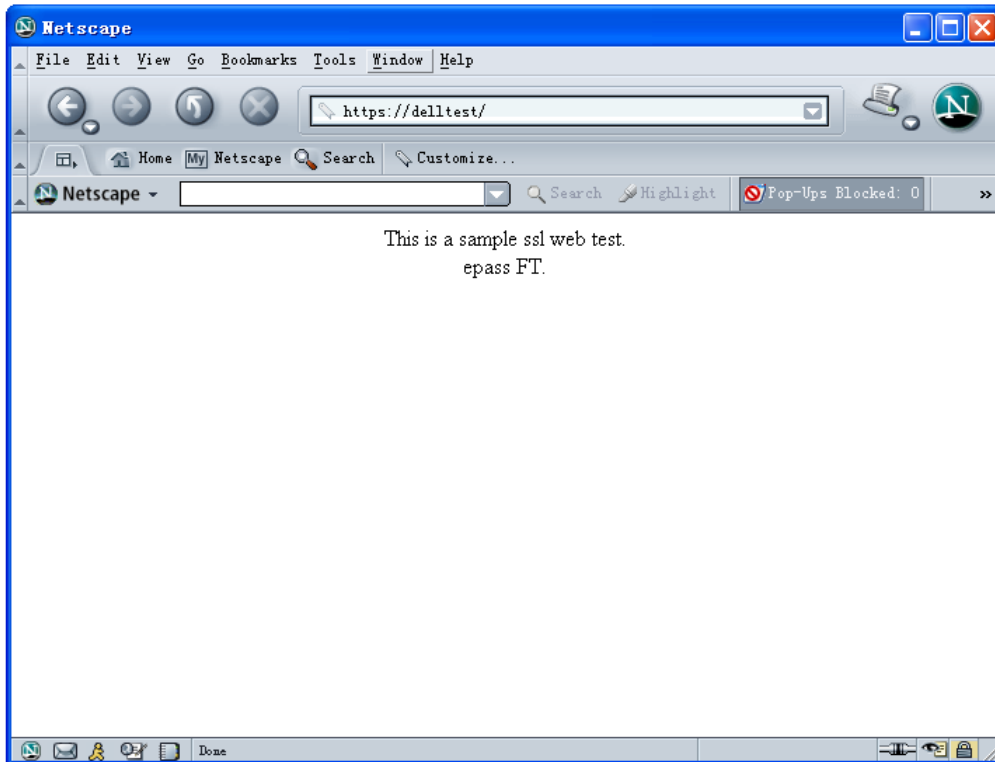


图 17 访问 SSL 站点成功

1.4 使用 ePass3003 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 ePass3003 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：

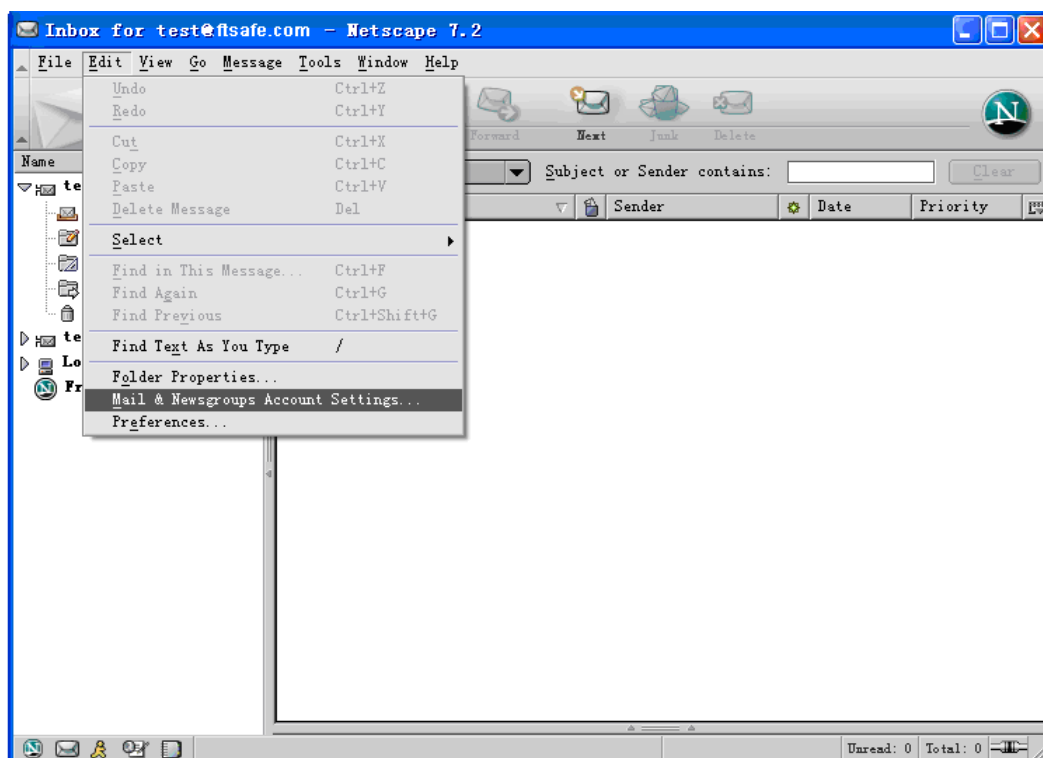


图 18 帐号设置菜单

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：

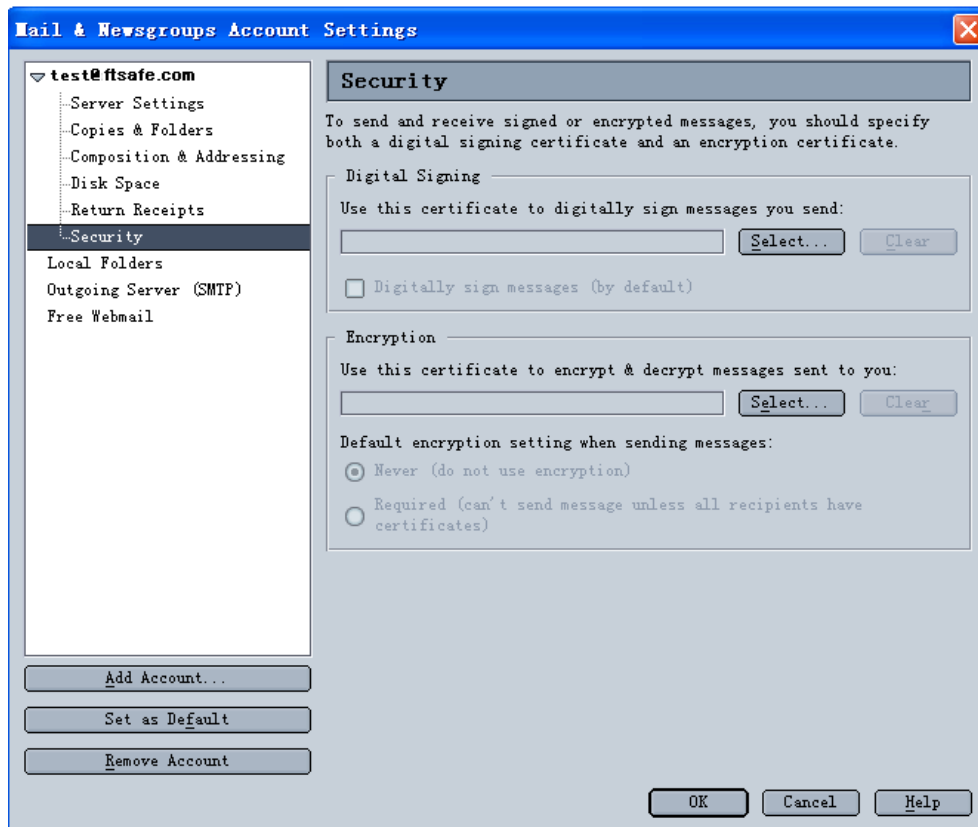


图 19 帐号安全设置界面

3. 选择右侧上面的“Select”按钮，Netscape 就将系统（ePass3003）中 test@ftsafes.com 帐号的签名证书列出，供用户选择，如图 20 所示：

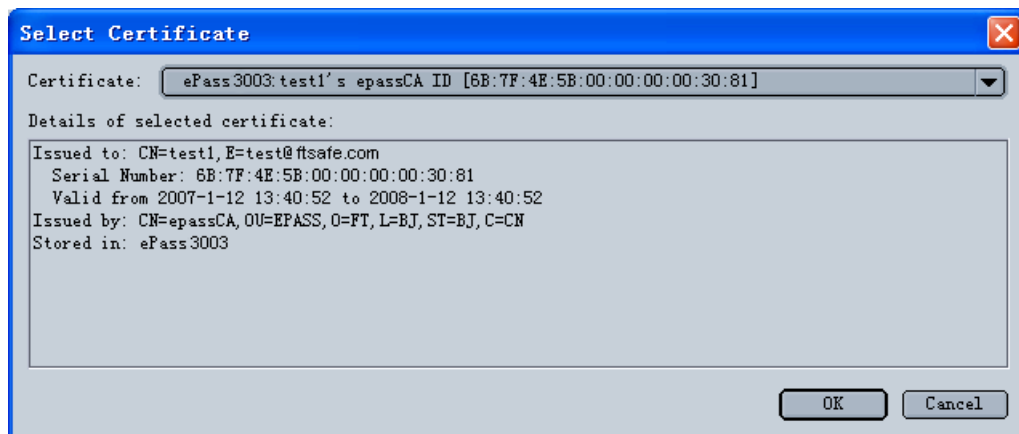


图 20 签名证书对话框

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@ftsafes.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，这样加密证书就出现在下面的“Select”之前的空白处，如图 22 所示：

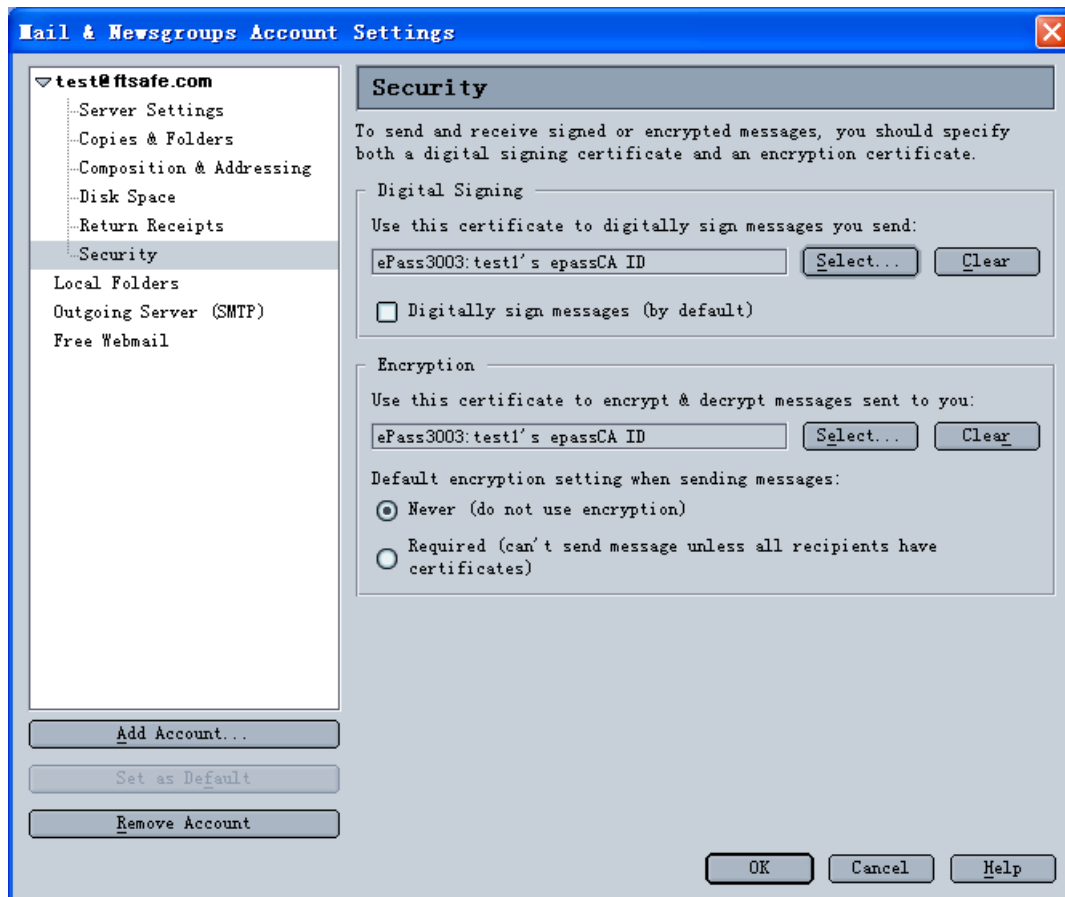


图 22 指定完签名加密证书界面

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@ftsafes.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：

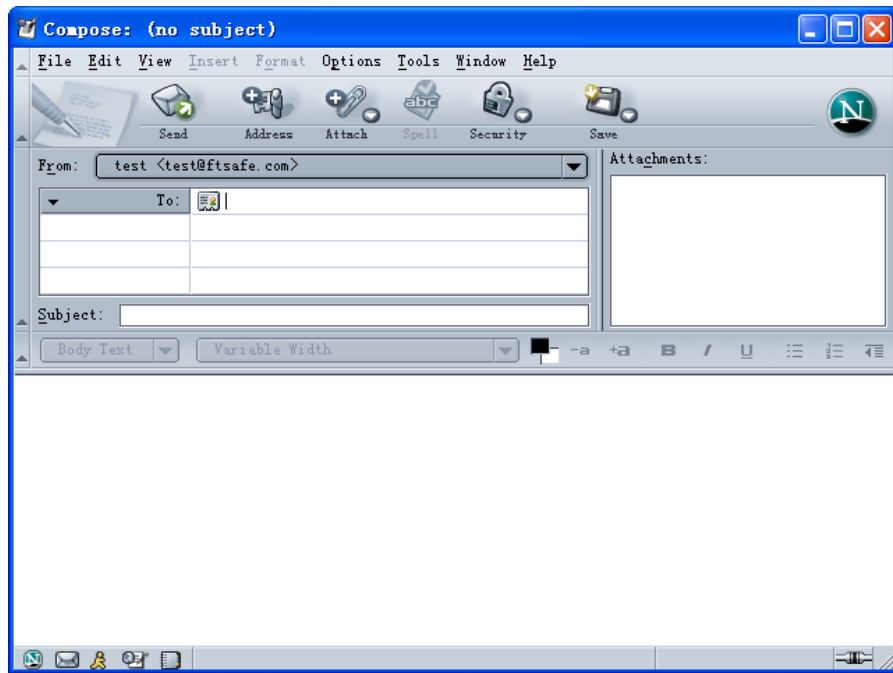


图 23 书写新邮件界面

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。

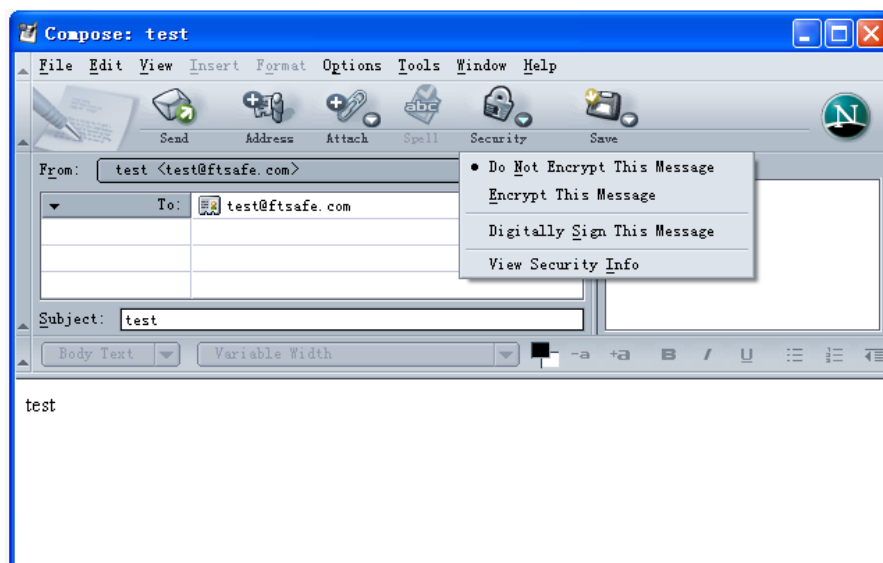


图 24 签名邮件菜单

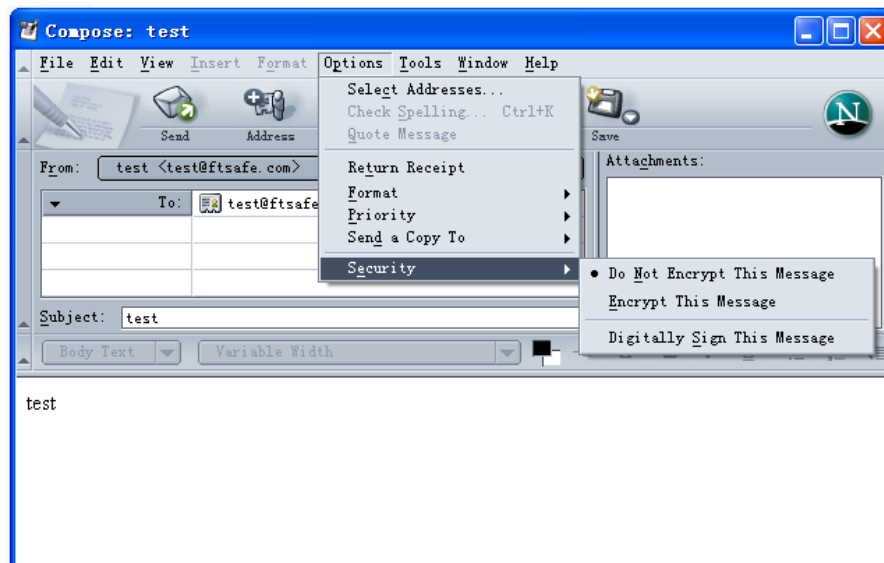


图 25 签名邮件菜单

3. 然后单击工具栏上的“Send”按钮，发出该邮件。如果以前没有输入过 ePass3003 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：

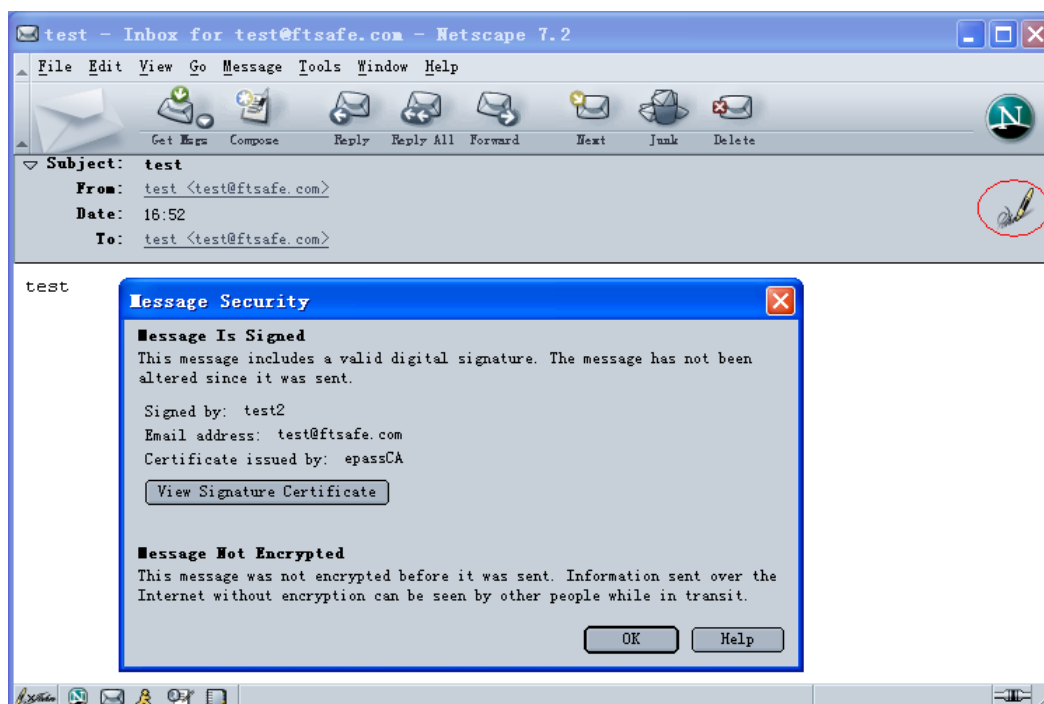


图 26 查看邮件签名对话框

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：

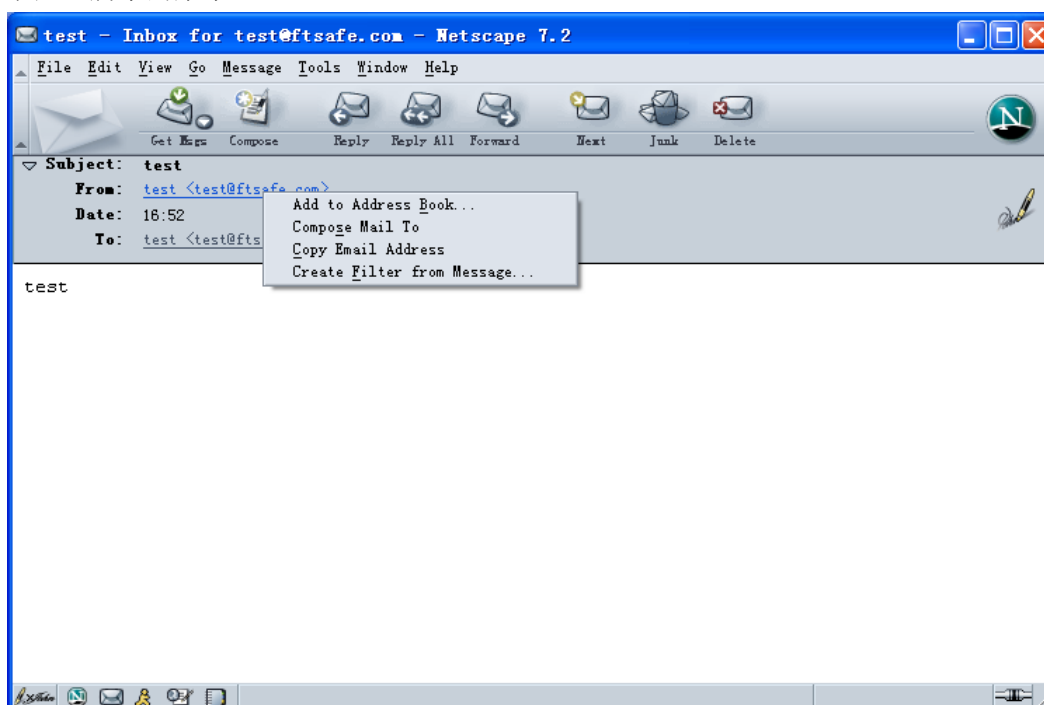


图 27 地址菜单

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 ePass3003 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 ePass3003 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 会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 ePass3003 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 ePass3003 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. 选取菜单中的“Window” → “Address Book”，如图 28 所示：

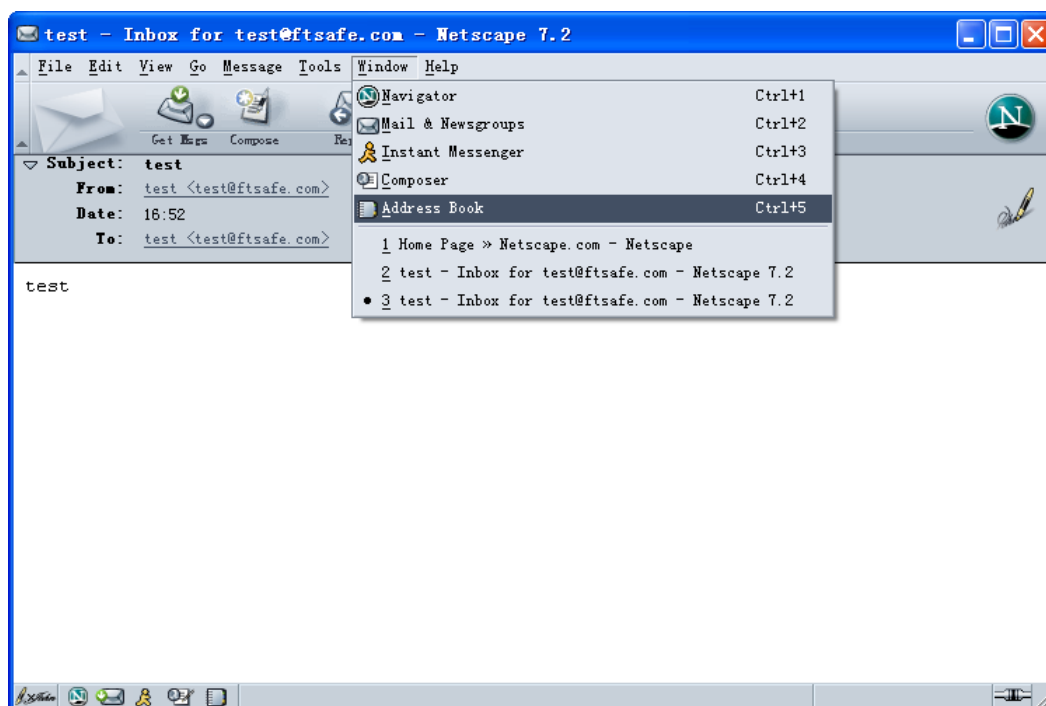


图 28 Netscape Address Book 菜单

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

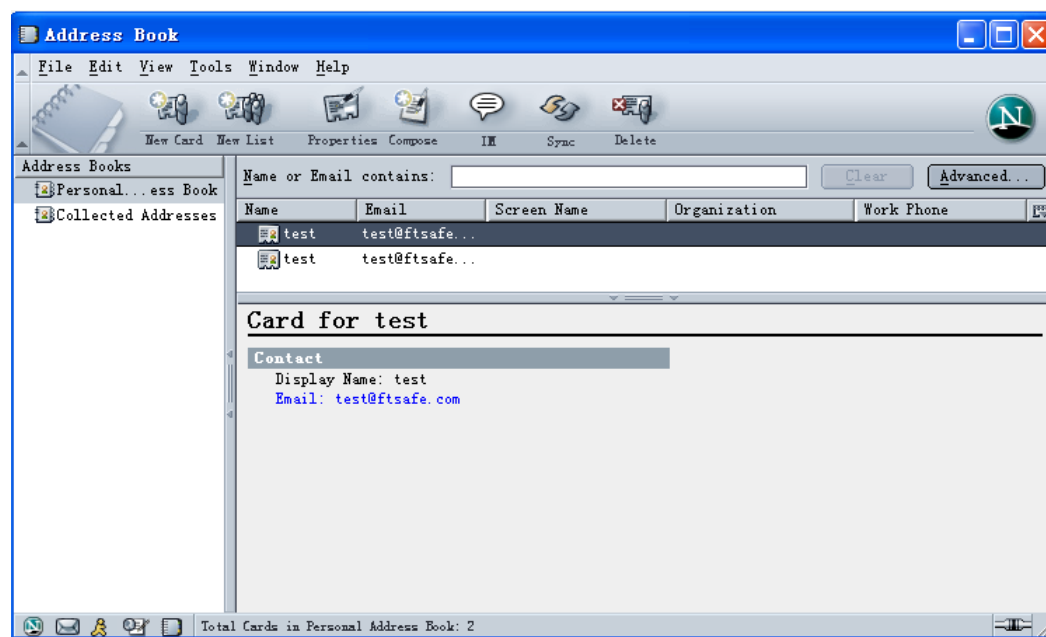


图 29 Netscape 地址簿

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。

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，具有高性能、高安全性、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。