



# ePass应用介绍

安全电子邮件

北京飞天诚信科技有限公司  
[www.FTsafe.com](http://www.FTsafe.com)

随着电子邮件和电子商务的逐渐普及，在 Internet 上传递的机密信息也在迅速增加。因此，对电子邮件的安全性和非公开性提出了更高的要求。另外，随着 ActiveX 控件、Script 脚本和 Java 小程序的广泛使用，所收电子邮件中 HTML 内容在未经许可的情况下访问或修改计算机中文件的可能性也在不断增强。如何确保自己的个人邮件隐私不会被泄露，邮件在发送后没有被人截获、修改，许多安全专家都正在寻找行之有效的方法。

Windows Outlook Express 包含一些工具，有助于您防止欺骗行为、增强电子邮件的非公开性并防止对计算机进行未授权的访问。这些工具通过安全区域使您能够更安全地发送和接收邮件并控制可能携带有害内容的电子邮件。

要使用 Outlook Express 中的安全电子邮件，您需要数字 ID (也叫数字证书)。提供了一种在 Internet 上验证您身份的方式，与您的身份证、司机驾照或日常生活中的其他身份证的方式相似。数字 ID 允许您给电子邮件签名，这样真正的收件人可确保该邮件确实是由您发来的并且没有受损。另外，数字 ID 允许其他人给您发送加密的邮件，邮件内容只有接收方本人才能解开。

要获得数字 ID，您必须从发证机构获得，那是个负责发布数字证书的组织，并不断地验证数字证书是否持续有效。他们对用户的身份进行审核，并以自身的信用提供对用户身份的担保。然后您可将您的数字证书发送给要给您发送加密邮件的用户，您也可用相同的数字证书发送签名邮件。个人用户可以申请免费的个人证书，这种证书的申请较为简单，也比较容易审核通过。

下面以国内较大的数字证书中心——广东省电子商务认证中心 [www.cnca.net](http://www.cnca.net) 颁发的试用型个人证书为例，来说明证书的整个申请过程，到其他 CA 站点申请证书的操作方式与之类似。

## 第一步 下载根证书

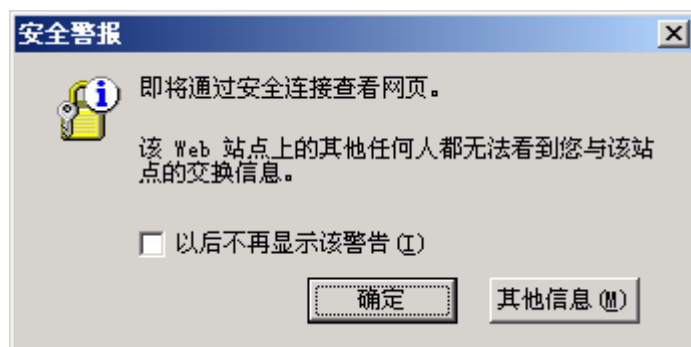
### 登录网站

在浏览器的地址输入 [www.cnca.net](http://www.cnca.net) 进入广东省电子商务认证中心的主页。

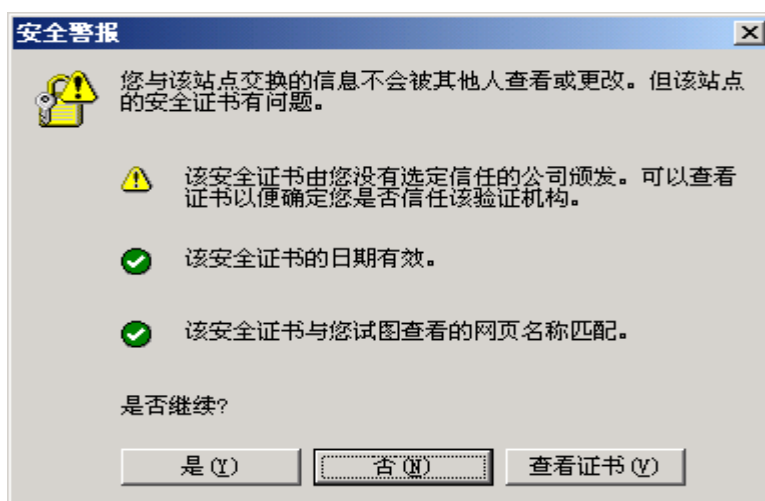
### 下载根证书

如果您以前还没有下载过广东电子商务认证中心的根证书，请先点击主页上"下载根证书"按钮。

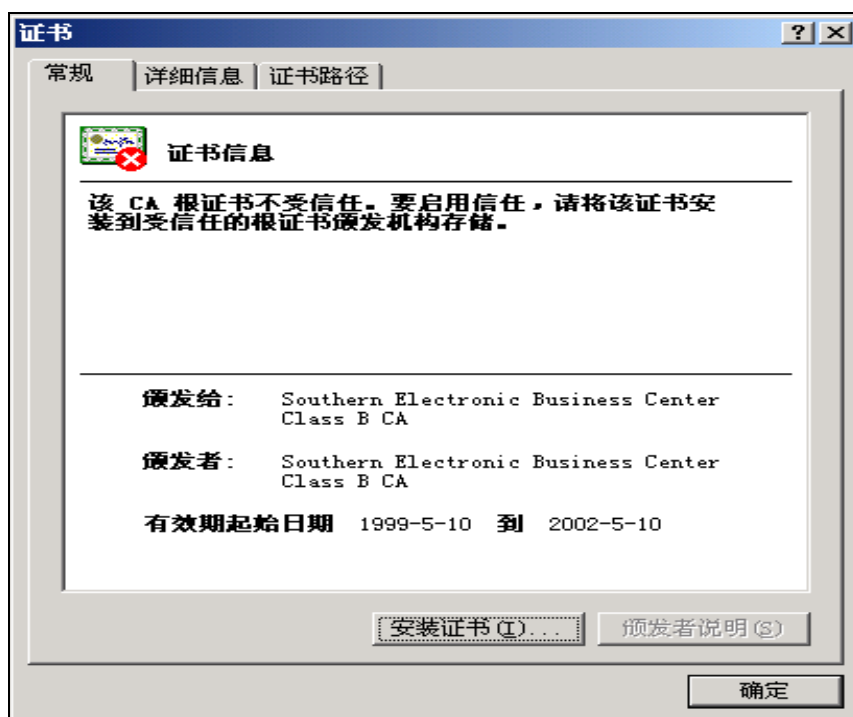
因为该页面是由 SSL 协议保护的页面，所以进入前 IE 浏览器有可能出现如下图所示的安全警报窗口。



点击确定后，将出现具体的证书问题提示窗口，选择 "是" 即可。

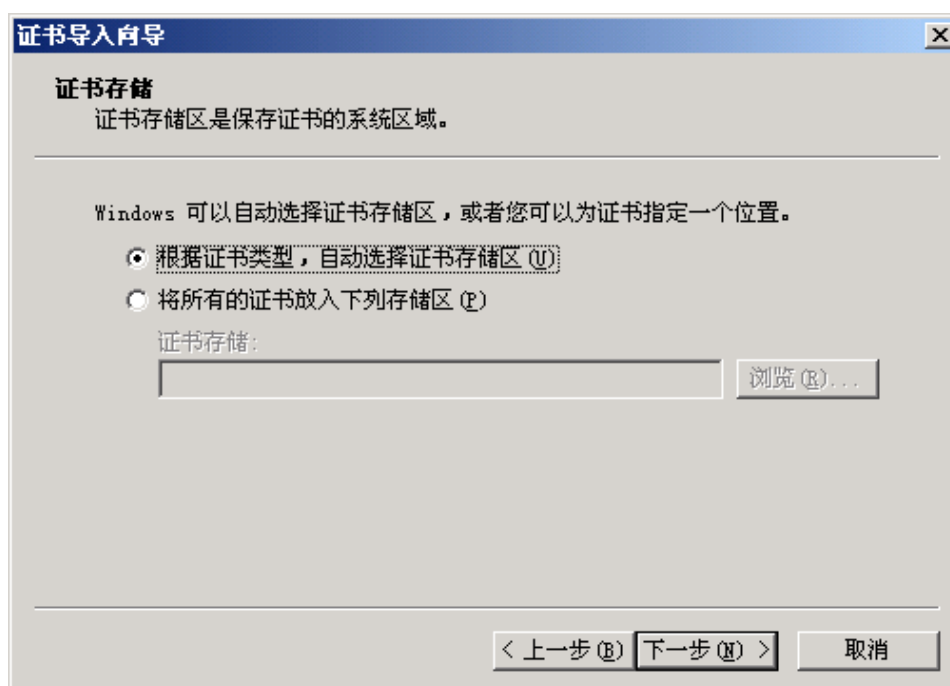


这时将出现"文件下载"对话框，选择"在文件的当前位置打开"，单击"确定"后，出现下一

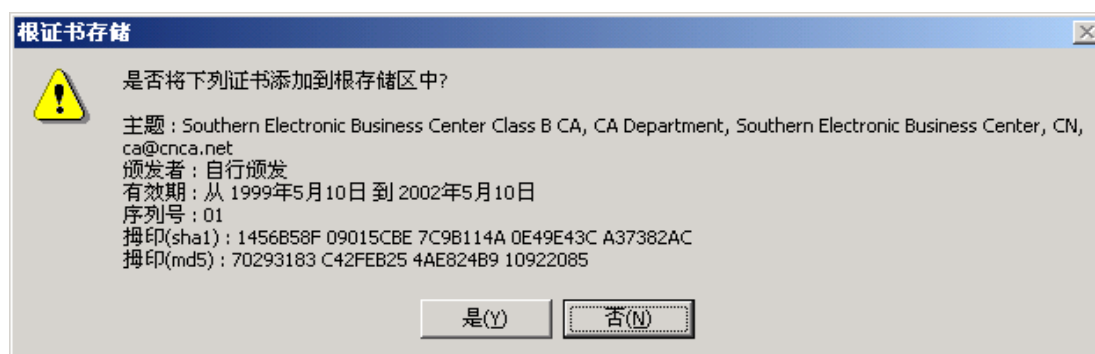


个对话框"证书"。

点击"安装证书"按钮，单击"确定"按钮，屏幕上出现下一个对话框"证书导入向导"，



对接下来弹出的窗口都选择默认选项，最后出现如下"根证书的存储区"窗口，选择"是"按钮，系统将提示导入成功，此时根证书已成功下载完毕并自动装入 IE 浏览器中。



您可以在 IE 浏览器中的"查看"菜单中选择"Internet 选项"，选定"内容"分页中的"证书"，打开"证书管理器"，选择"受信任的根目录证书发行机构分页"，就可以在其中查看我们所有的根目录证书，其中就包括我们刚刚下载的根本目录证书 Southern Electronic Business Center Test Certificate。

## 第二步 填写申请

进入 <https://testca.netca.net>

申请试用型个人数字证书。进入如下界面：



## 申请试用型个人数字证书

**! 特别提示**

只有安装了试用CA证书链的计算机，才能完成后面的申请步骤和正常使用您在本中心申请的数字证书。

请您点击以下“安装证书链”图标，如果您没有安装过本公司的试用型根证书，那么系统将提示您是否将证书添加到根证书存储区，请选择“是”。然后系统将自动将CA证书链安装到您的计算机上，安装完成后系统将提示您证书下载完毕。点击“确定”即可。

在成功安装试用CA证书链后，请您点击“继续”图标，进行下一步操作。

安装证书链
继续

继续 [返回首页](#)

© 2001 北京网证通科技有限公司版权所有

按照上面的提示，如果没有安装过证书链，点击“安装证书链”按钮，系统会安装证书链，然后进入下图界面。如果以前安装过，点击“继续”按钮，进入如下图页面。



## 申请试用型个人数字证书

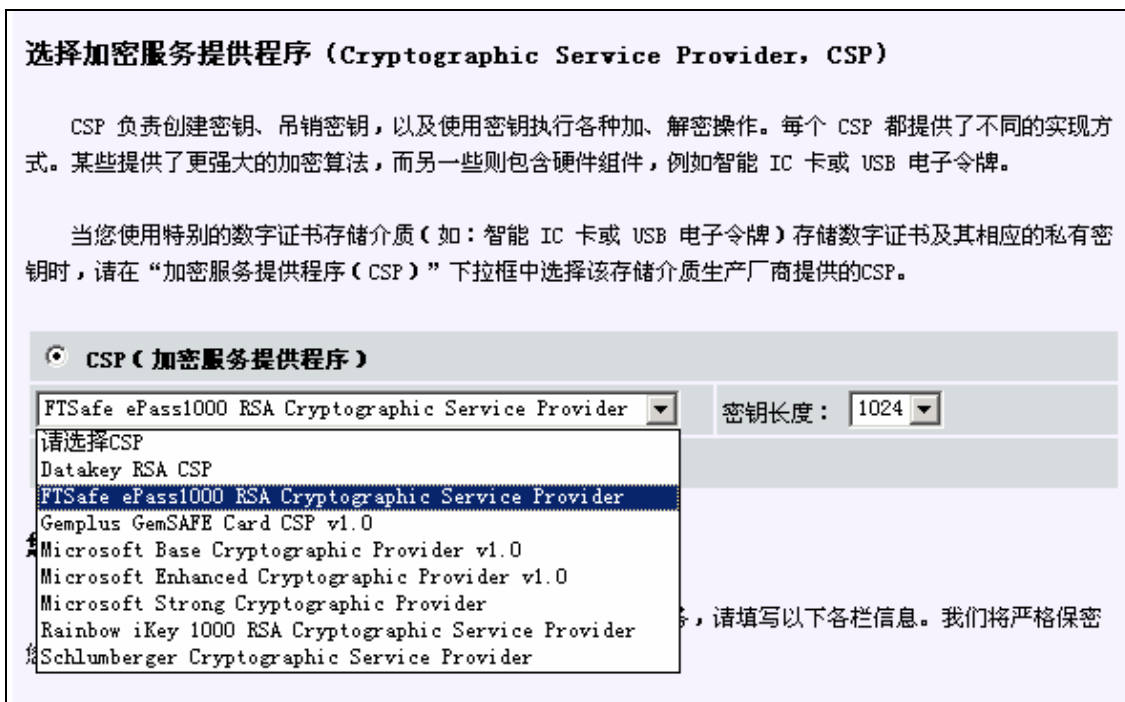
1、填写并提交申请表格
2、下载并安装您的数字证书

**您的基本信息**

请输入以下各栏信息，不可填写特殊字符。所有的信息都需要正确填写，否则将无法完成下面的申请步骤。

请输入您的姓名： (示例：张三)	<input type="text" value="shanghai"/> (必填)
请选择您所在的国家： (示例：中国)	<input type="text" value="中国"/> (必填)
请选择您所在的省份或直辖市： (示例：北京)	<input type="text" value="北京"/> (必填)
请输入您所在的城市： (示例：北京)	<input type="text" value="shanghai"/> (必填)
请输入您的电子邮件地址： (示例：zs@netca.net)	<input type="text" value="shanghai@ftsafes.com"/> (必填)

填写申请人的基本信息。如名称、国家、省市、电子邮件地址。然后选取加密服务 (Cryptographic Service Provider, CSP)。注意：每个公司提供的 CSP 不同，这里我们选择我公司提供的“FTSafe ePass1000 RSA Cryptographic Service Provider”，然后选择加密密钥长度 1024 位。（如下图所示）



所有的信息填好后，按“提交”按钮，提交此请求。此时会产生公钥和私钥。公钥随着表单提交，而私钥直接存储在 ePass1000 中。这时会弹出对话框，要求输入 ePass 的 PIN 码。



注意：在程序把密钥写入或者读出 ePass 过程中不要拔下 ePass，否则会出错。写入过程中，“ePass1000 Monitor” 监控程序会提示相应的信息。

### 第三步 审核通过

由于是测试型数字证书，网下身份审核过程就省略。认证中心会按照申请时使用的邮件信箱发确认邮件，告知业务受理号以及证书查询密码。如下图所示。



点击上图的蓝色字“这里”, 就可以进入数字证书安装页面。

**网证通 NET CA** **安装数字证书**

**安装数字证书身份校验**

在安装我们为您签发的数字证书之前, 需要您提交相应的信息以验证您的身份。请输入您的证书业务受理号和密码, 进入安装数字证书页面。

如果您忘记证书业务受理号及密码, 请从邮件中取回。将证书业务受理号及密码填入后, 点击“确定”按钮, 进入安装证书页面。

您的证书业务受理号:

您的密码:

**网证通 NET CA** **安装数字证书**

**您的数字证书**

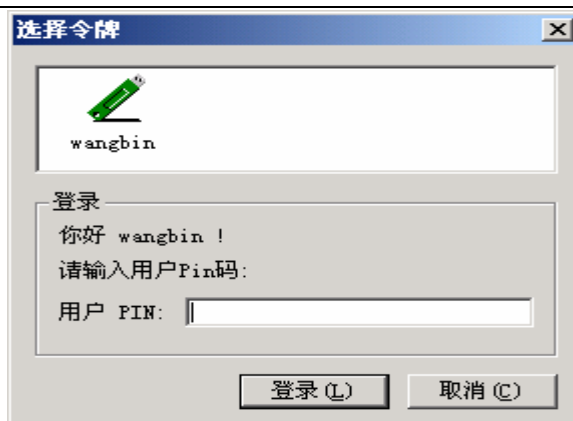
您已经获得北京网证通科技有限公司签发的数字证书, 其包含的基本信息如下:

姓名:	shanghai
国家:	CN
省份:	Beijing
城市:	shanghai
电子邮件:	shanghai@ftsafe.com

请点击“安装证书”图标, 安装您的数字证书

[返回页首](#)

© 2001 北京网证通科技有限公司版权所有

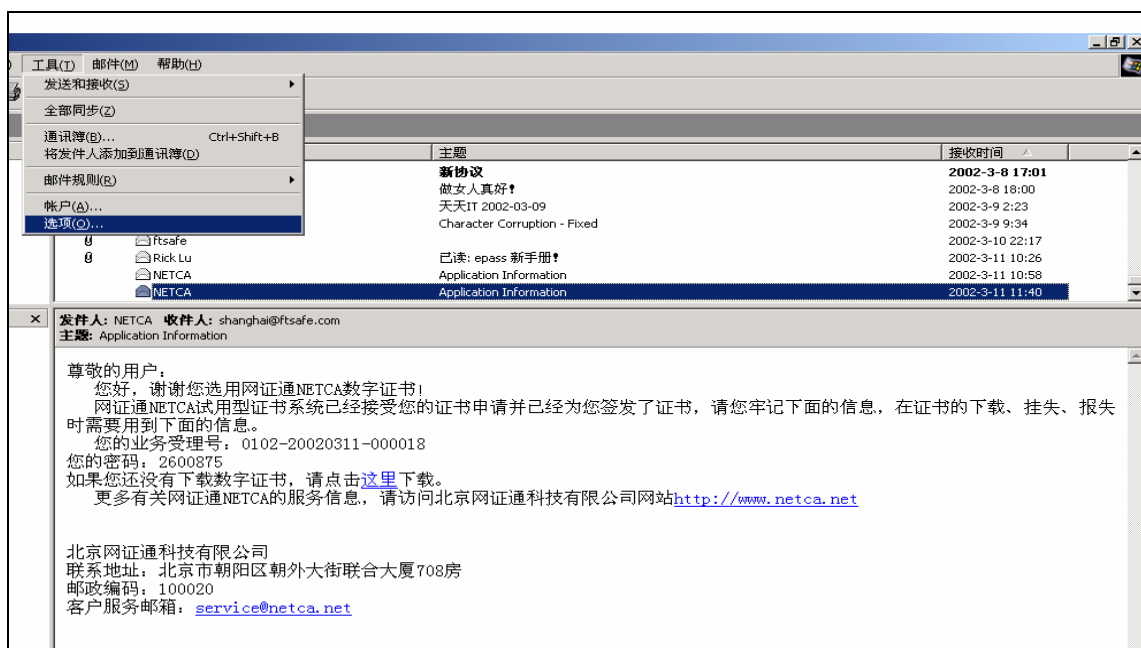


输入 ePass 的 PIN 码，系统会把数字证书写入到 ePass 中。提示证书安装完毕。

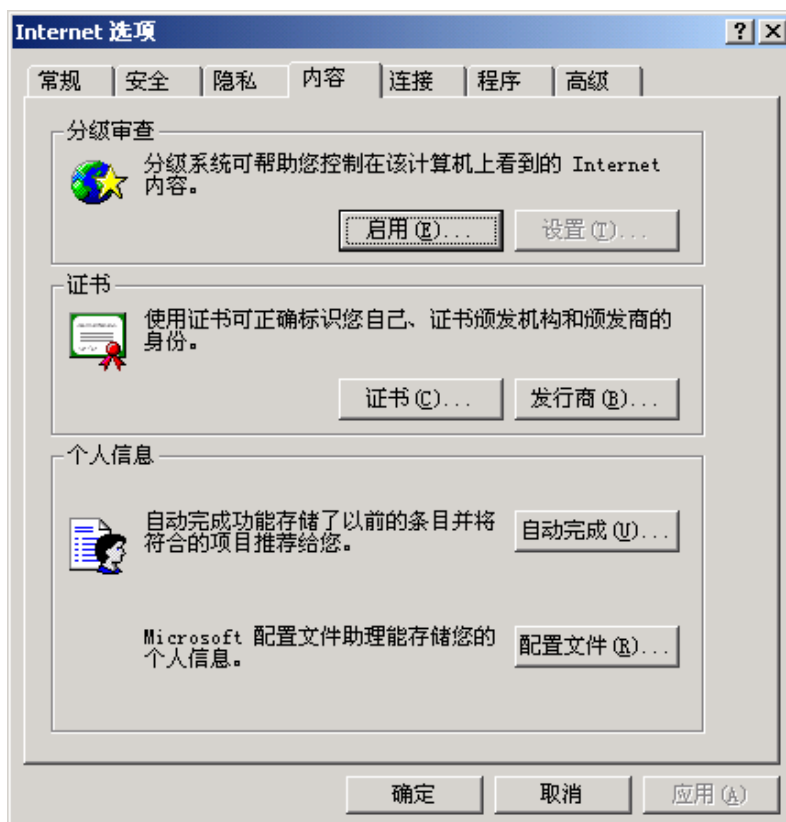


您已经拥有数字证书，可以发送安全电子邮件了。Outlook Express 中的安全电子邮件通过使用数字签名和加密对 Internet 通讯提供保护。使用数字签名，您可以在所发电子邮件上签署独特的标识，这样接收方就可以确认您是邮件的发送者，并且邮件在传送过程中未被篡改。对所发邮件进行加密有助于确保只有预定接受人员才能在传送过程中读取该邮件。

因为 Outlook Express 使用标准 S/MIME，所以其他人可用支持该技术的程序阅读您所撰写的安全电子邮件。同样，您也可用支持 S/MIME 技术的电子邮件程序阅读他人撰写的邮件。



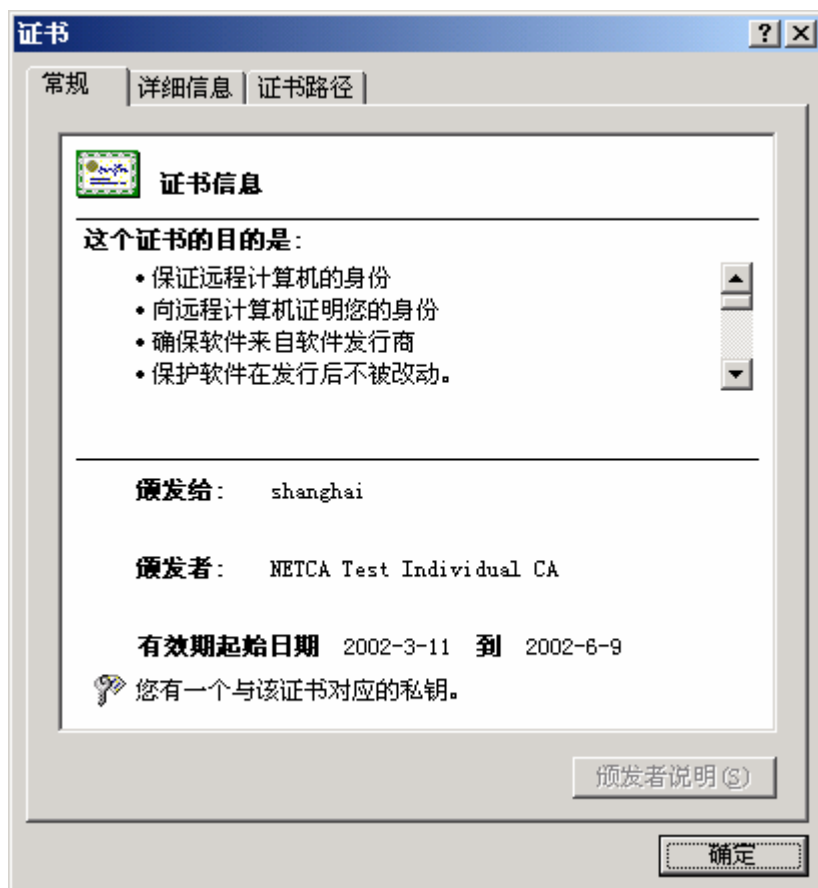
在 outlook express 中，选择“工具— 选项”菜单，显示如下“Internet 选项”。如下图。



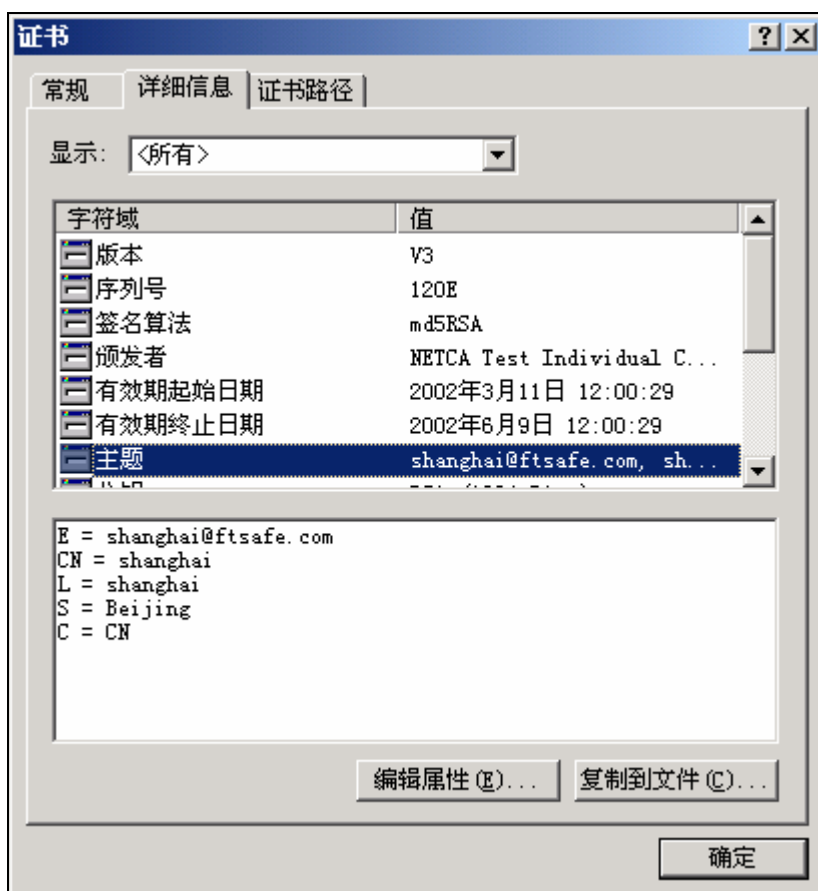
点击“证书...”按钮。



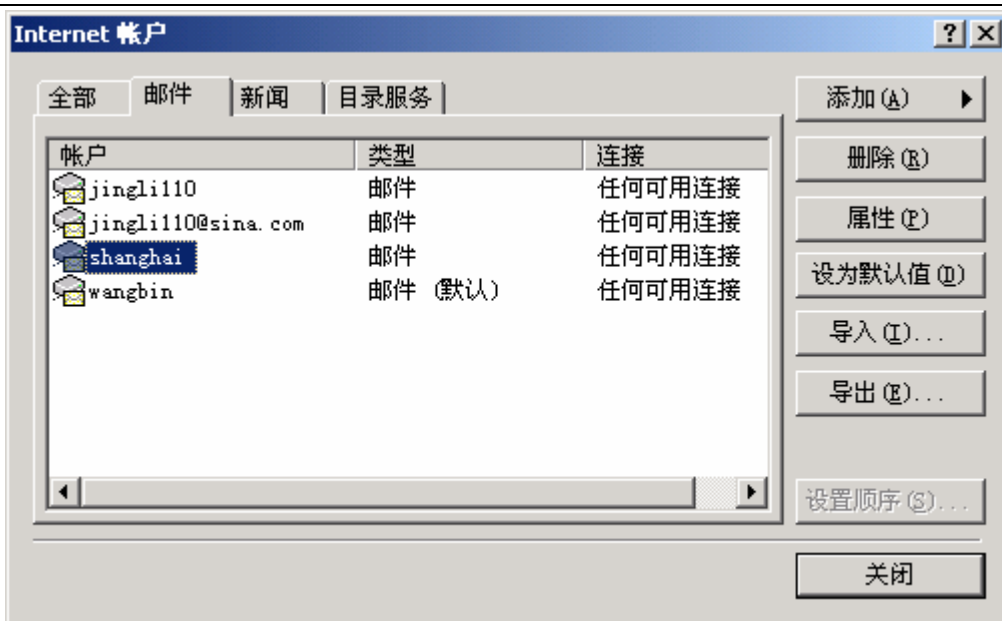
上图显示了此时系统中安装了的个人证书。其中由“NETCA Test Individual CA”颁发给“shanghai”的证书为我们演示中申请到的证书。双击或者点“查看”按钮就可看到此证书的详细信息。



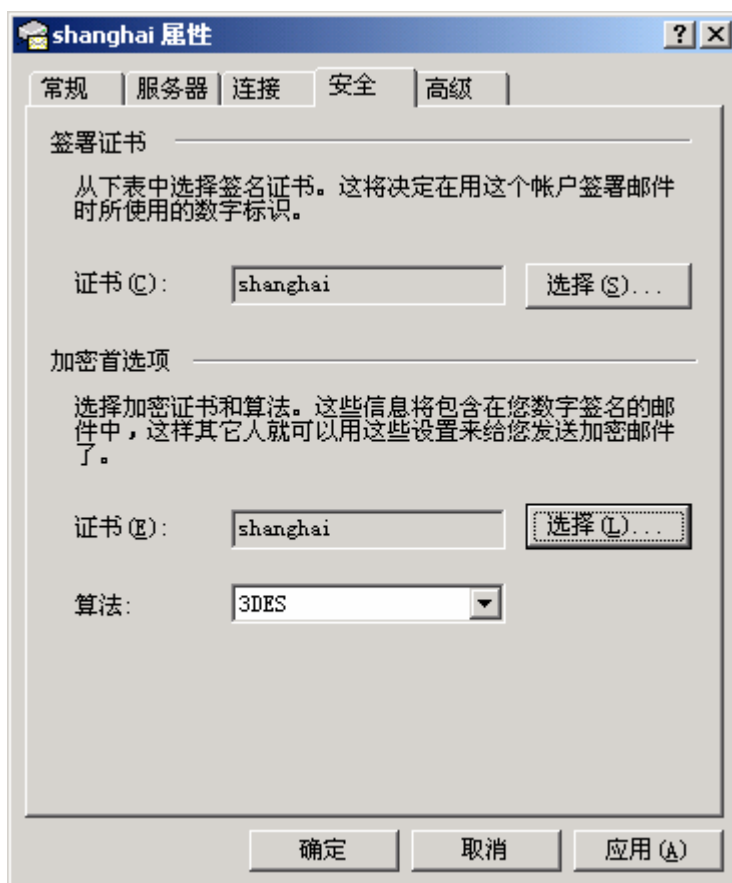
主题中显示的信息就是申请时所填入或者选择的信息。



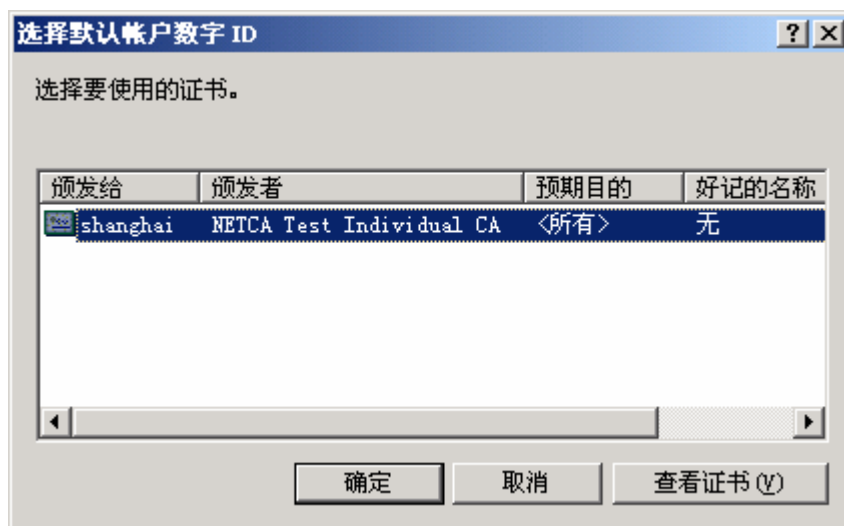
选择“工具— 帐户”，我们查看 shanghai@ftsafe.com 的信息。



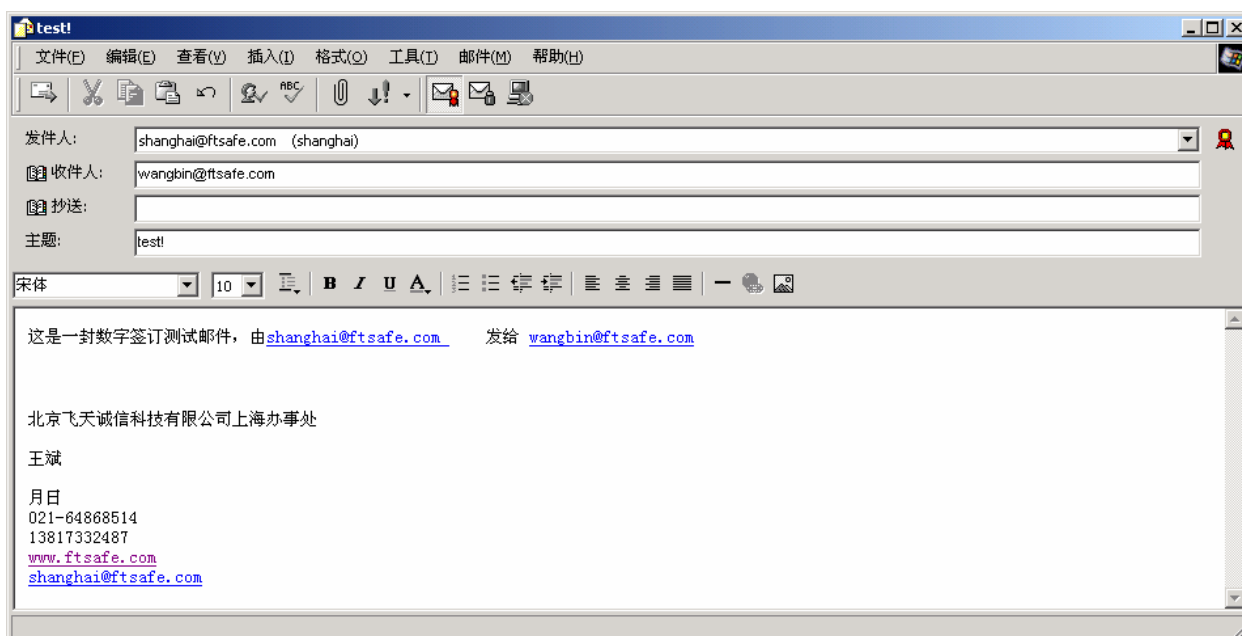
用鼠标双击“shanghai”或者选中后点击“属性”按钮查看shanghai帐户的属性。如下图



选择“安全”选项，“签署证书”为签名的证书。“加密首选项”为加密证书以及算法。点击“选择”按钮显示如下。



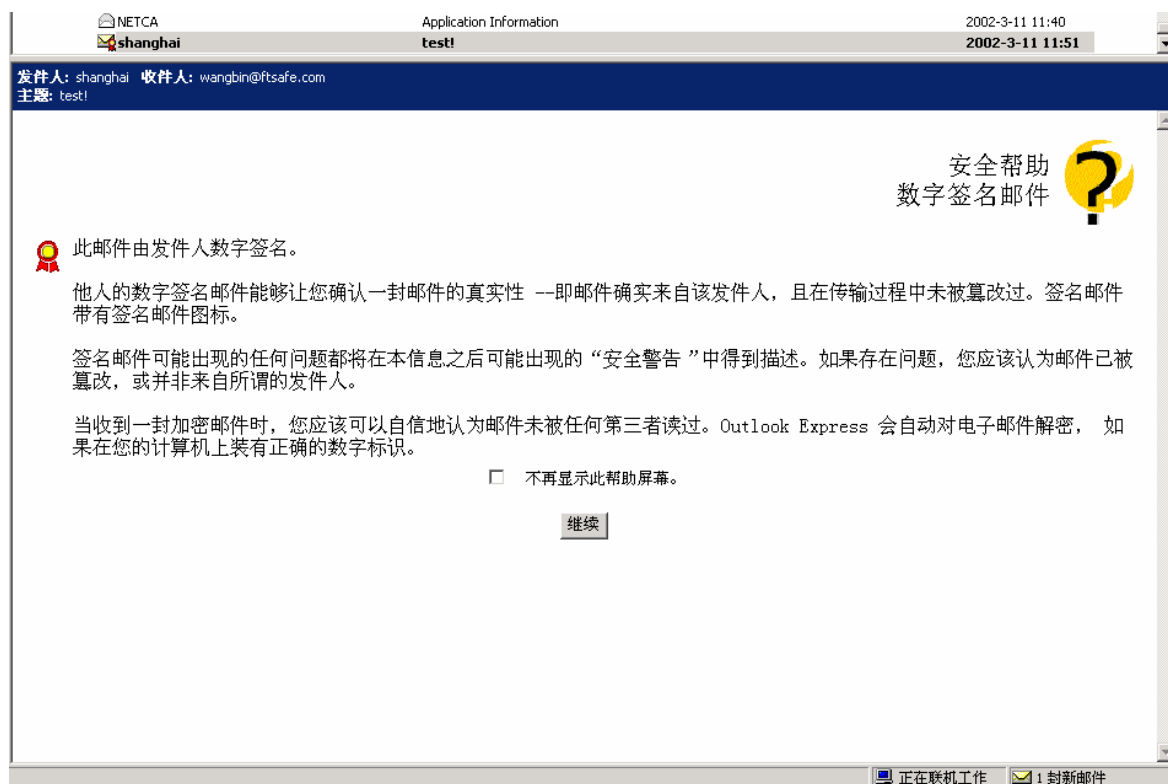
## 发签名邮件



本例中我们先用申请下来的证书发签名邮件。[shanghai@ftsafe.com](mailto:shanghai@ftsafe.com) 发给 [wangbin@ftsafe.com](mailto:wangbin@ftsafe.com)。写完邮件内容后，点击数字签名按钮，在发件人后面就会显示一个红色的图标表示此为签名邮件。点击发送后，系统会提示输入 PIN 码，以读取 ePass1000 中的数字证书。



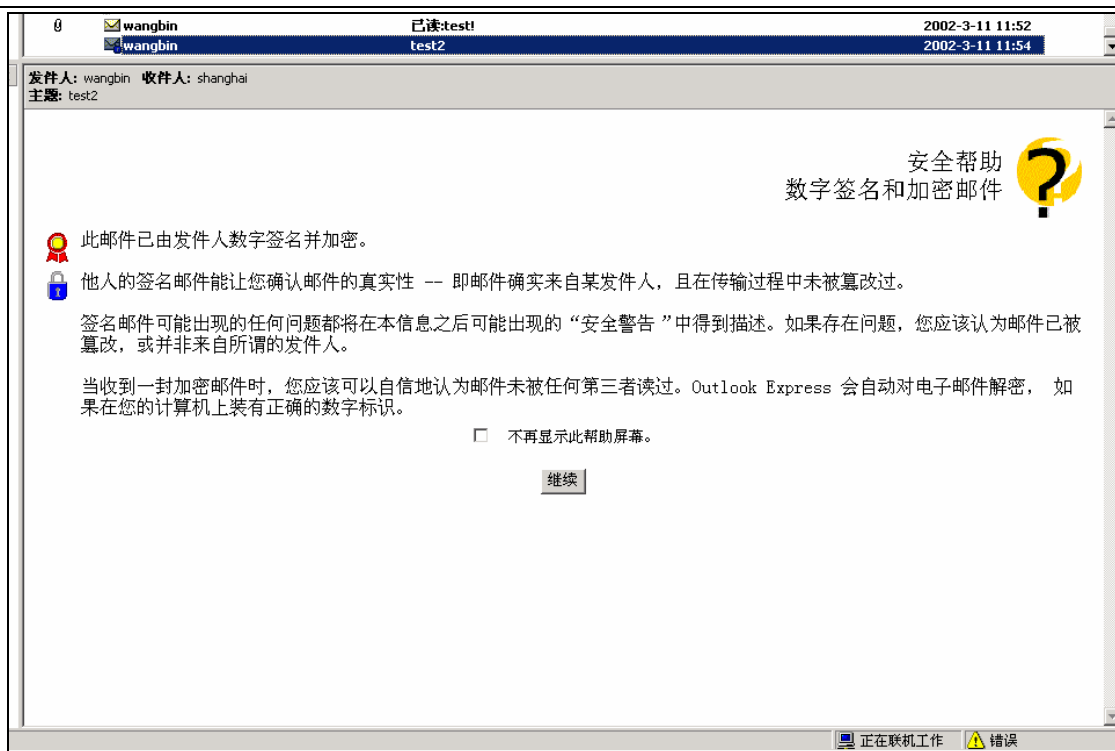
## 接收



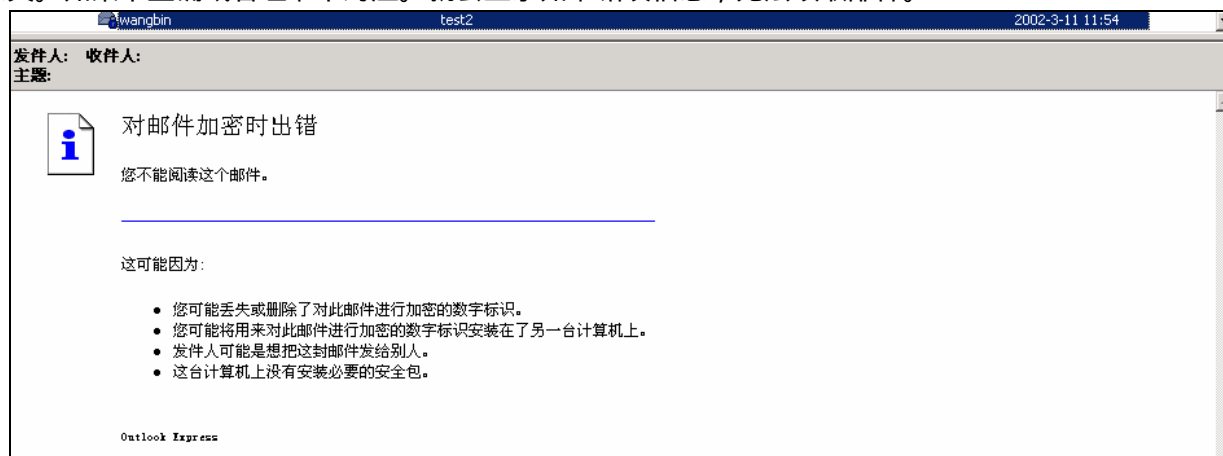
wangbin@ftsaf.com 收到此邮件后显示提示“此邮件由发件人数字签名”，点击“继续”就可看到其中的内容。

## 发签名加密邮件

由于签名邮件中已经包含了发件人认证公钥，因此收件人如果现在也有数字证书，那么他就可以给对方发签名加密邮件。发加密邮件过程与上述发签名邮件相同，在此忽略。接收方在收到此邮件后显示信息如下。



点击“继续”按钮会弹出输入 ePass 的 PIN 码对话框。在此不再复述。若 PIN 码正确就会显示正确的邮件原文。如果不正确或者证书不对应。就会显示如下错误信息，无法读取邮件。



注意：证书申请过程和证书安装过程在实际的应用中是不连续的，而且一般中间有一个网下身份资质认证过程，这个因应用而异。对于我们的产品保证申请过程和安装过程不在同一台电脑上时，证书与私钥均安装在 ePass 中，电脑上不存在证书的备份，但需要电脑上都安装了 ePass 客户端软件，因此满足移动上网而又随时使用数字证书的需求。

在安全电子邮件中，使用电子证书对邮件进行签名、加密，保证了发送方的合法身份确认，接收方的信息完整可靠，使得在网络中发送敏感信息、个人资料得到安全体系保障，而使用 ePass 这种硬件加密证书载体，可以确保证书始终携带在自己身上，保证物理安全。而且，由于不需要专门的读卡器，且小巧便于携带，ePass 本身还带有硬件 PIN 码保护功能这些优点。因此，基于 ePass 的安全电子邮件解决方案不失为目前一个切实可行的方法，可以有效的解决在邮件安全中的一些问题。