

ePass3000 的 CAPI 应用

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(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 CAPI 应用	1
1.1 使用 ePass3000 的 CAPI 进行客户证书申请	1
1.2 使用 ePass3000 的 CAPI 访问 SSL 加密站点	4
1.3 使用 ePass3000 的 CAPI 收发签名与加密邮件	5
1.3.1 获取数字证书	5
1.3.2 设置 Email 帐号的安全性	10
1.3.3 使用 Outlook Express 发送附加数字签名的邮件	14
1.3.4 获取收件人的公钥和证书	15
1.3.5 使用 Outlook Express 发送属性加密的邮件	15

第一章 ePass3000 的CAPI应用

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 CAPI 应用，主要包括 IE 申请证书，访问 SSL 加密站点，Outlook 发送签名、加密邮件等。

- 使用 ePass3000 的 CAPI 申请数字证书
- 使用 ePass3000 的 CAPI 访问 SSL 加密站点
- 使用 ePass3000 的 CAPI 收发签名与加密邮件

1.1 使用ePass3000 的CAPI进行客户证书申请

1. 确认插入了一支已经完成PKI初始化的ePass3000。然后通过IE打开证书颁发机构的网页，如图 1所示：



图 1 申请用户证书

2. 选择“申请一个证书”，再选择“高级证书申请”选项。在证书模板中选择“ES用户”或其它包含客户端验证的模板，在“CSP”（加密服务提供程序）选项中选择“FEITIAN ePassNG RSA Cryptographic Service Provider”，如图 2所示：

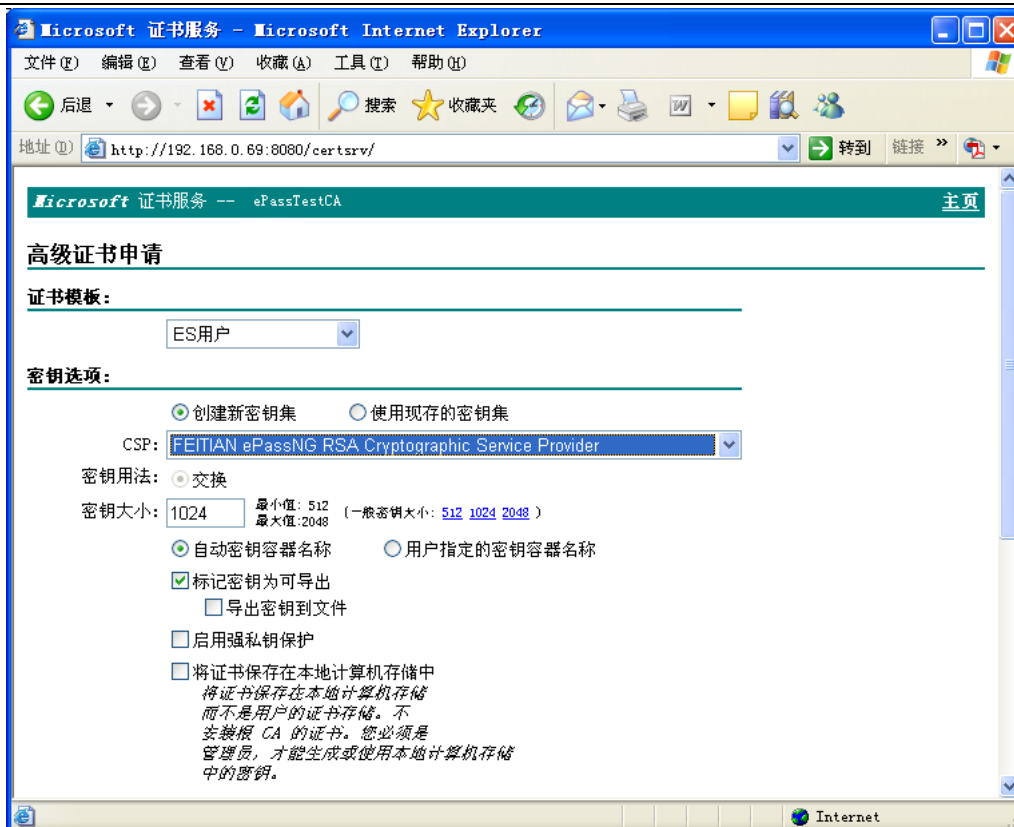


图 2 用户信息

3. 完成上述设置后，单击“提交”按钮，如果您的计算机上连接了多个Token，会显示选择Token的提示框，并且ePass3000 已经被列入其中了，选择您要保存证书的ePass3000，点击“确定”按钮，系统弹出提示输入用户PIN码的对话框，如果只有一个ePass3000 则直接弹出PIN码输入框，如图 3所示：

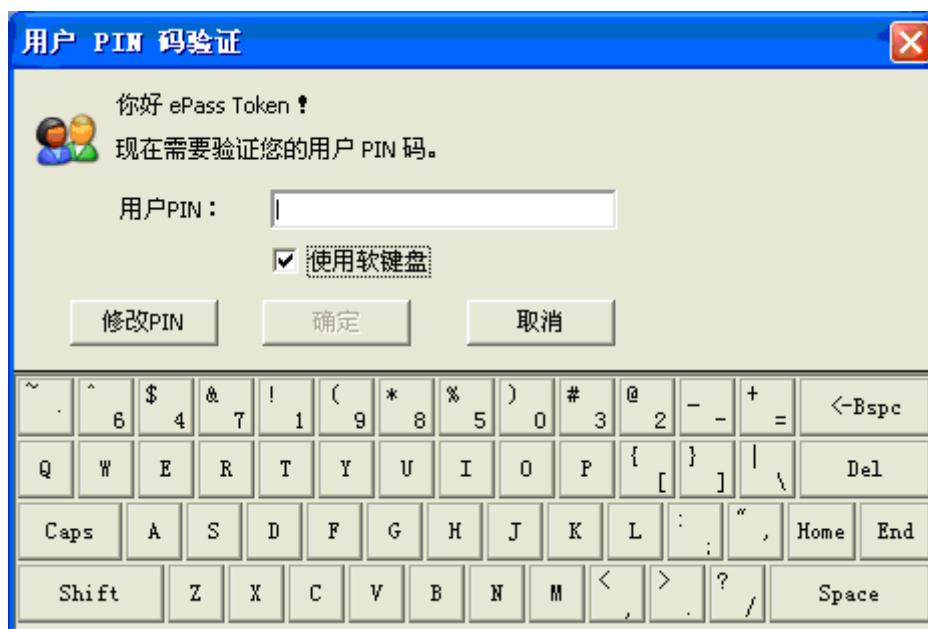


图 3 PIN 码输入框

注意：上图显示的是使用软键盘输入用户 PIN 码的情况，用户也可以不选择“使用软键盘”选项，但是建议您选择“使用软键盘”登录到 Token，这样才能保证您的 PIN 码的安全。选择“使用软键盘”后，物理键盘被禁用。

如果用户想修改 PIN 码，可以按照步骤 4 的说明进行操作，如果不需要修改 PIN 码，直接执行步骤 6。

4. 点击图 3 所示界面中的“修改PIN”按钮进行用户PIN码的修改，点击“修改PIN”弹出如图 4 所示的对话框：

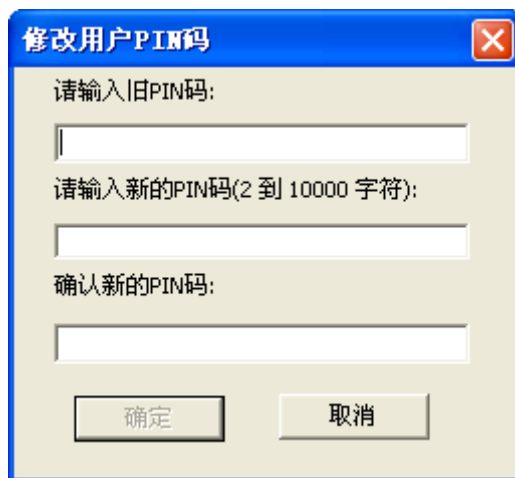
该对话框标题为“修改用户PIN码”，包含三个输入框，分别用于输入旧PIN码、新的PIN码（2到10000字符）以及确认新的PIN码。底部有“确定”和“取消”两个按钮。

图 4 修改 PIN 码对话框

5. 按照界面上的要求输入原PIN码和新PIN码并确认，然后点击“确定”按钮，完成用户PIN码的修改。修改PIN码后ePass3000 自动登录，无须再进行PIN码验证，此时可以看到如图 5 所示的界面。

6. 输入正确的用户PIN码点击“确定”按钮后，稍候会看到证书挂起页面，用户需要等待颁发机构验证身份并颁发证书，如图 5 所示：



图 5 证书挂起

收到证书颁发机构的通知后，用户就可以去领取证书了，在安装证书时，系统同样会让用户选择所需的 Token 并要求输入正确的用户 PIN 码，在完成这些工作之后，系统就会自动将用户证书安装到 ePass3000 里。用户可以通过 ePass3000 管理工具来查看证书是否申请成功。

1.2 使用ePass3000 的CAPI访问SSL加密站点

现在，我们就可以用这支 ePass3000 来访问安全 Web 站点了。

1. 首先，确认已插入这支证书申请成功的ePass3000，然后用IE浏览器通过https: (https://delltest:443) 连接到要访问的Web站点。此时，会看到安全提示对话框，单击“是”按钮后，出现证书列表框供用户选择，如图 6所示：

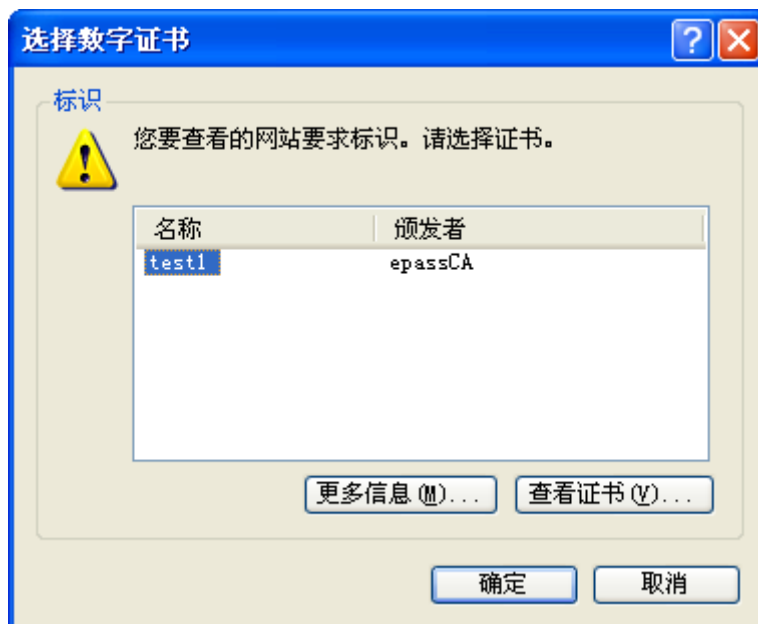


图 6 证书列表框

2. 现在，可以看到用户证书已经列在列表框里了，选中证书，单击“确定”按钮。系统弹出PIN码输入框，如图 3所示，用户输入正确PIN码进行登录之后就能够看到这个安全Web站点的内容了（此安全Web站点为示例站点），如图 7所示：

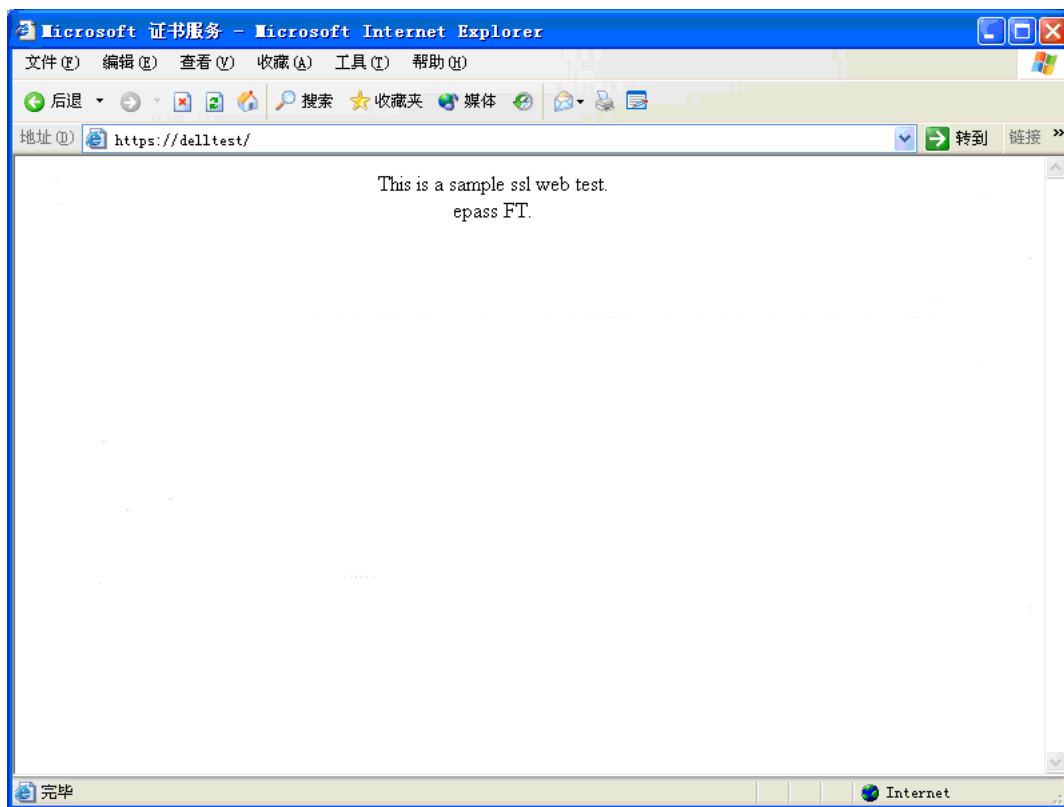


图 7 安全 Web 站点

1.3 使用ePass3000 的CAPI收发签名与加密邮件

在开始设置 Outlook Express 收发签名与加密邮件之前, 假设已经将 Outlook Express 设置好, 可以连接上电子邮件服务器, 换句话说, 用户已经可以使用 Outlook Express 以一般的方式发送/接收电子邮件。要进行 Outlook Express 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(在 Outlook Express 里称为“数字标识”), 当获取用户的数字标识后, 用户才可以发送具有签名的或者信息加密的电子邮件。

1.3.1 获取数字证书

我们先来获取用于证明用户身份的数字标识。由于电子邮件的应用是公开性的, 因此, 用户必须通过专门负责提供证书服务的企业, 来获取适当的证书信息, 以确保该证书的有效性。用户可以采用下列的操作步骤, 连接上企业外部的证书颁发机构, 并获取使用在 Outlook Express 内的数字标识。下面以 <https://digitalid.verisign.com/> 这个公开的CA为例来申请测试用的数字标识(飞天不保证这个CA总是有效)。在确认插入了一支PKI初始化过的ePass3000后:

1. 先以用户帐户登录 Windows 系统。
2. 启动 Internet Explorer。
3. 在地址栏中输入 <https://digitalid.verisign.com/>, 如图 8所示:

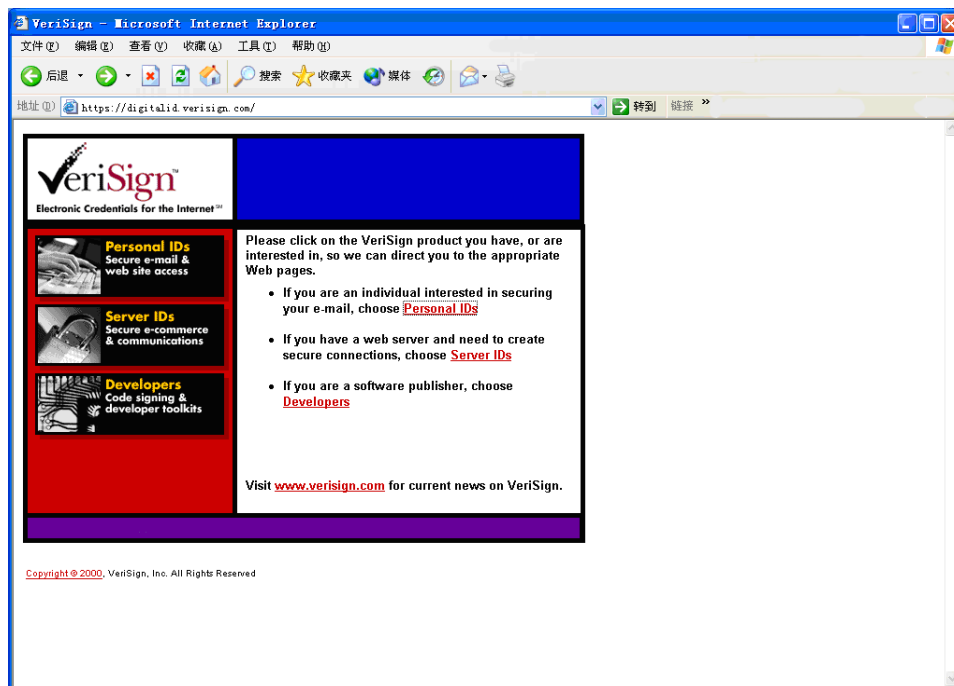


图 8 申请个人数字证书

4. 选择“Personal IDs”后进入图 9所示的界面：

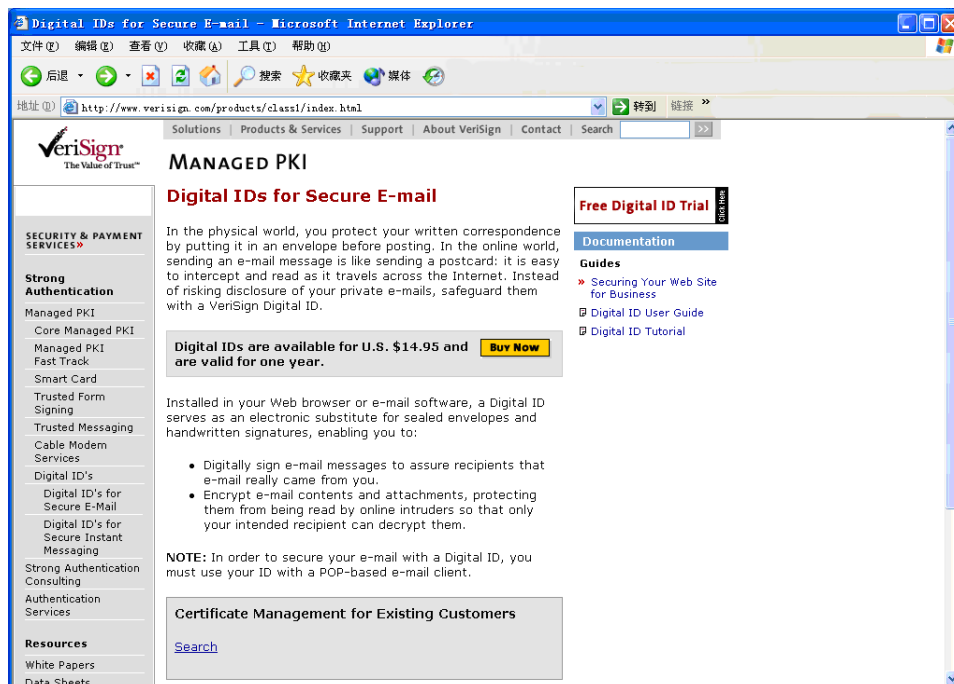


图 9 申请免费数字证书

5. 选择“Free Digital ID Trail”，进入如图 10所示的界面：

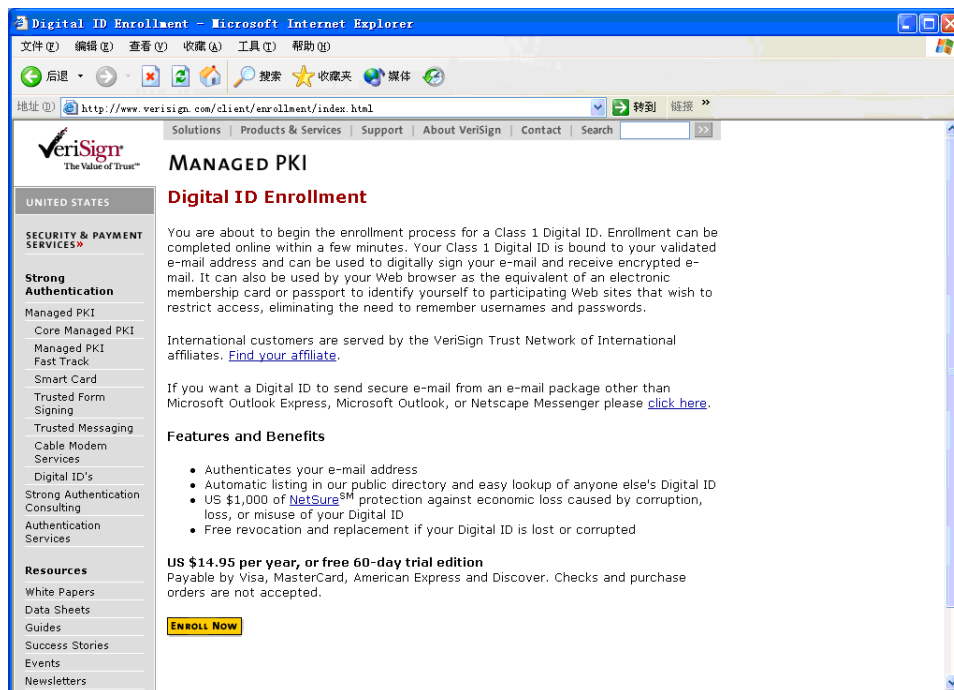


图 10 数字证书代理

6. 选择“Enroll Now”后进入证书申请页面，如图 11所示：

由于各网站所提供的这些提供证书服务的企业申请安全性证书（数字标识）的方式各不相同，用户可以直接通过各 CA 网站的链接连接到提供证书服务的企业，并获取专用的证书（数字标识），然后用户才可以利用获取的数字标识来进行安全性邮件的一些设置。由这些提供证书服务线上登记获取数字标识时，若用户要求获取的证书（数字标识）的用途是使用在安全性邮件方面时，在登记获取数字标识时都会要求输入用户的 Email 帐号的地址，在这里填写的 Email 帐号即是该数字标识的授予对象，若用户有两个以上的 Email 帐号时，请注意填写要进行安全性邮件设置处理的 Email 帐号。

举个例子来说，假设要在 techsup@ftsafes.com 的 Email 帐号上设置使用安全性邮件的功能（在 Outlook Express 上设置），用户必须在向提供证书服务的网站填入要获取证书（数字标识）之签发对象的 Email 信箱地址，即 techsup@ftsafes.com。

以下继续由 Verisign 企业所提供的服务获取数字标识。

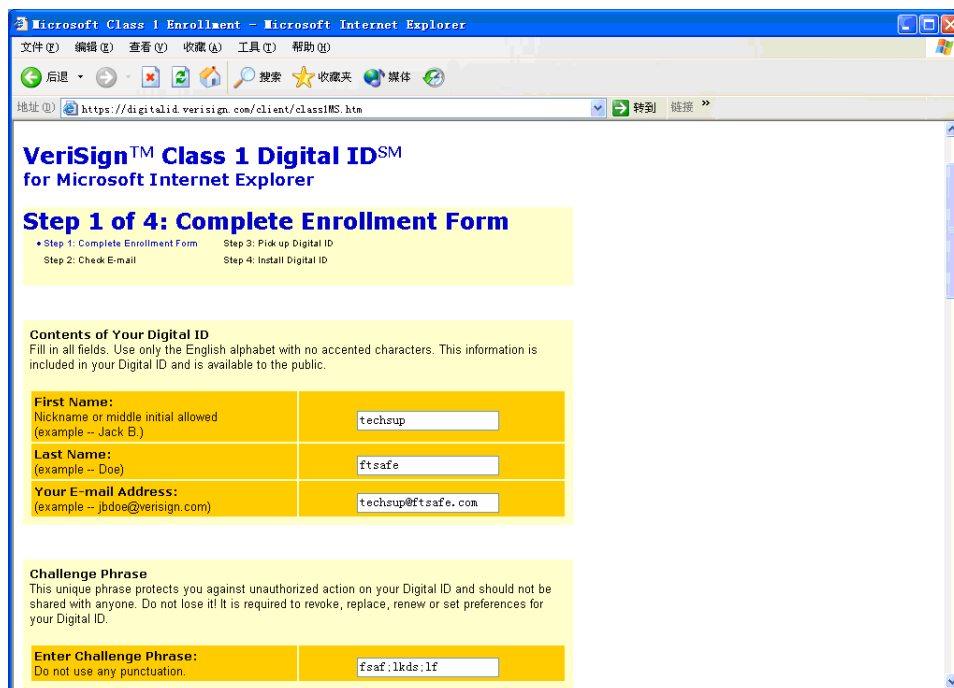


图 11 线上登记获取数字标识

7. 在此需要我们填写一些个人的信息资料，用户可以看到由这个企业线上获取安全性电子邮件的数字标识时，在“Cryptographic Service Provider Name”一项中，选择“FEITIAN ePassNG RSA Cryptographic Service Provider”。

8. 确定填写的一切信息无误后，请按页面最下边的“Accept”按钮，此时，如果在您的计算机上连接了多个Token，会出现“选择令牌”对话框，选定用户要安装证书的这支ePass3000，系统会提示输入用户PIN码，如果只插入了一支ePass3000则直接弹出其PIN码输入框要求用户输入PIN码，如图 3所示。

9. 输入正确的用户PIN码后，稍候会看到如图 12所示的页面，提示用户去查看Email信箱。

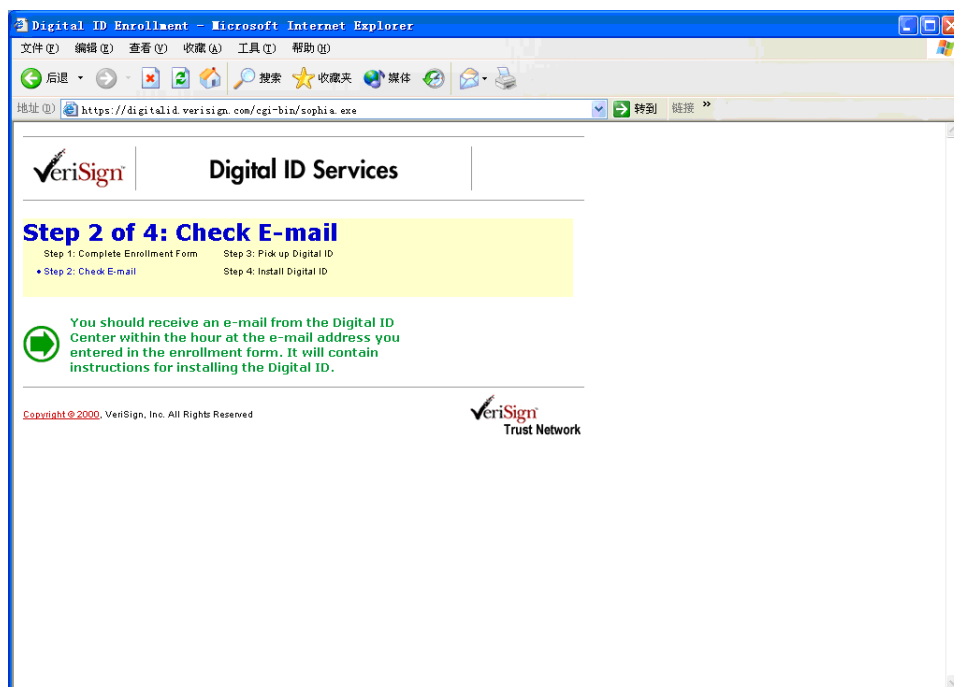


图 12 检查 Email 提示

10. 打开 Verisign 发的 Email，可以看到用户提供的相关信息和一个 Internet 链接

<https://digitalid.verisign.com/enrollment/mspickup.htm>, 以及“PIN number”。在Internet Explorer中打开这个链接, 来到“数字标识服务”的第三步, 如图 13所示:

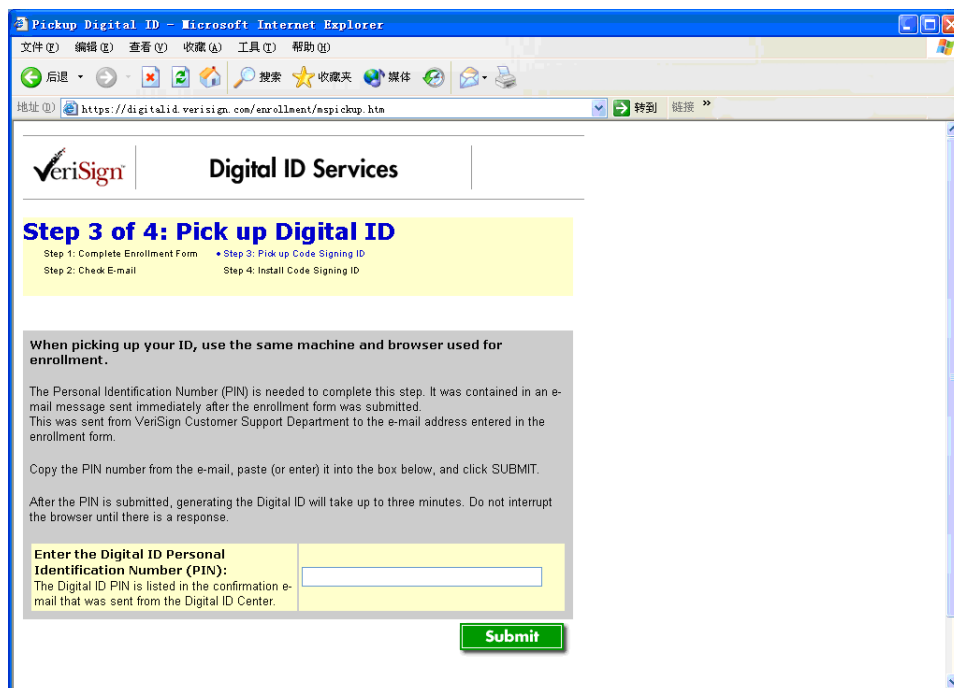


图 13 数字标识服务第三步

11. 将Email中的“PIN number”填入到文本框中, 然后按“Submit”按钮。来到“数字标识服务”的第四步——“安装数字证书”, 如图 14所示:

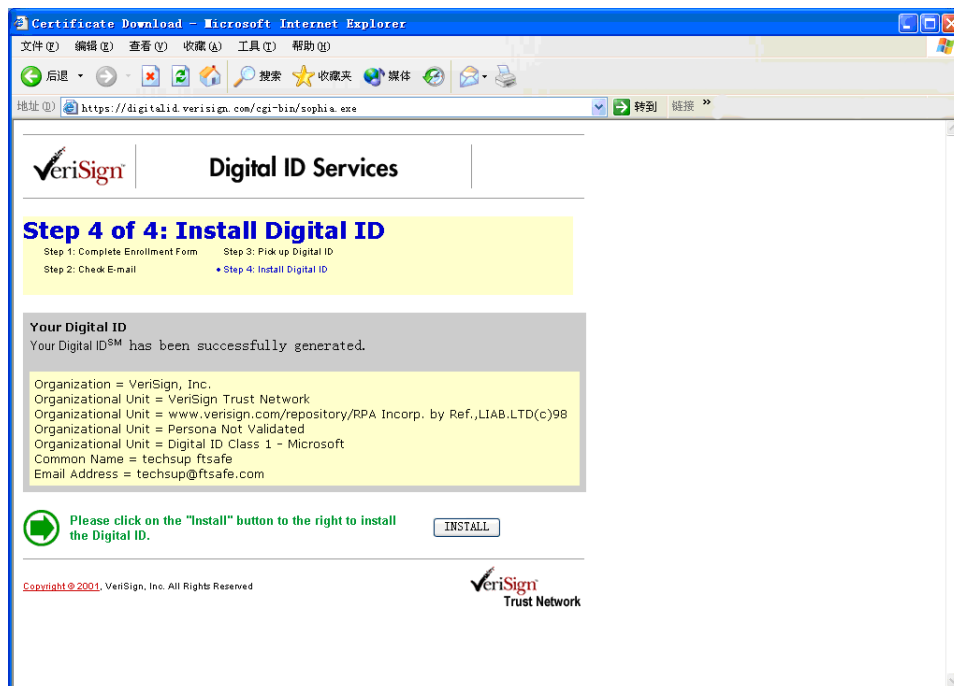


图 14 安装数字证书

12. 按下“Install”按钮, 此时, 如果计算机上连接了多个 Token, 又会有“选择 Token”对话框出现, 仍然是选择要装入证书的 ePass3000, 如果只连接一个 ePass3000, 则直接要求输入用户 PIN 码, 输入正确的用户 PIN 码, 稍候 Verisign 会提示证书已经成功安装。用户可以通过 ePass3000 管理工具来查看安

装的证书。

以上是获取证书(数字标识)的操作过程,获取证书(数字标识)后,用户就可以开始进行 Outlook Express 中 Email 帐号的安全性设置了,使得 Email 帐号能够具有安全性邮件的处理能力。

1.3.2 设置Email帐号的安全性

设置 Outlook Express 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. 请先以用户帐户登录 Windows 系统。
2. 用户需先确定已经获取了使用在安全性邮件的数字标识。用户可以由企业外专门提供证书服务的企业网站获取证书,也可以由Windows Server 2003 证书服务器获取证书,要获取证书,请按照1.3.1中说明的方式,以此获取需要的数字标识。
3. 启动 Outlook Express。
4. 接着,请由Outlook Express上方的菜单中选择“工具”→“帐户”,如图 15所示:



图 15 启动帐号设置

5. 当打开“Internet帐户”窗口后,请点选“邮件”页面。我们假设用户已经设置好电子邮件信箱了,请选择想设置安全性的电子邮件帐号,接着,请按下旁边的“属性”按钮,如图 16所示:

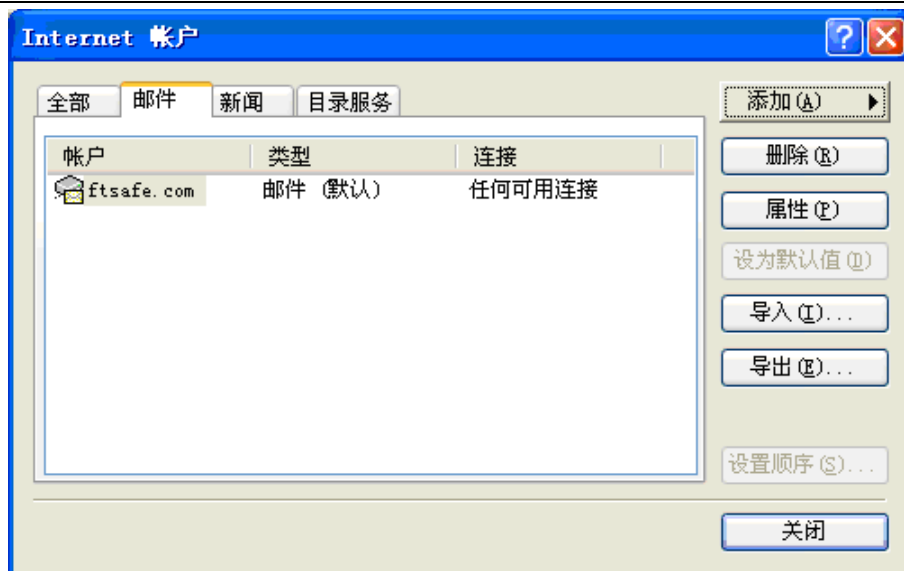


图 16 设置您电子邮件帐号的属性

6. 当打开此电子邮件帐号的属性设置窗口后，先选择“常规”页面，检查目前的电子邮件地址是否有设置错误，如图 17所示：



图 17 检查电子邮件的设置

7. 选择“安全”页面，以显示关于此电子邮件帐号的安全性相关设置，如图 18所示：

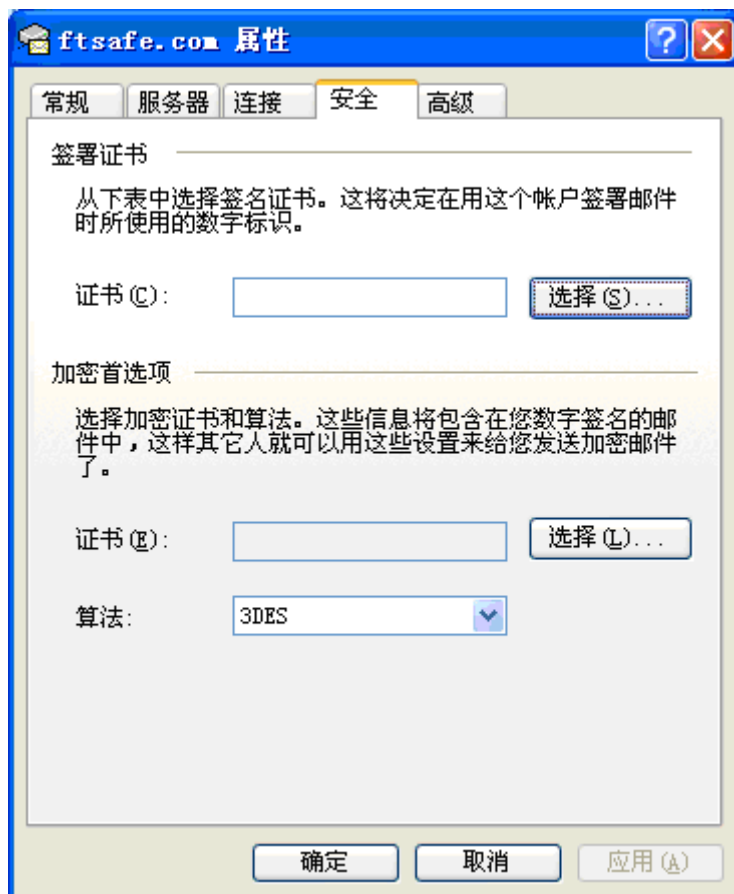


图 18 邮件帐号的安全设置

8. 若让此 Email 帐号能够具有数字签名的能力，在“签署证书”的部分里，按下“选择”按钮，并选择一个刚刚获取的证书（数字标识）。若要此 Email 帐号能够具有电子邮件加密的能力，在“加密首选项”的部分里按下“选择”按钮，并选择一个刚刚获取的证书（数字标识），以便让 Email 帐号具有处理电子邮件加密的功能，用户还可以在算法下拉菜单中选择想使用算法的规则。

9. 当按下“选择”按钮后，用户会看到如图 19所示的画面，Outlook Express将只使用用户信箱里所设置的证书来辨识S/MIME信件，此证书是记录在Email信箱的证书的主题字段里的证书。这些证书都会显示在图 19所示的选择窗口里，选择一个要使用的证书。用户还可以按下“查看证书”按钮来查看该证书的详细信息。

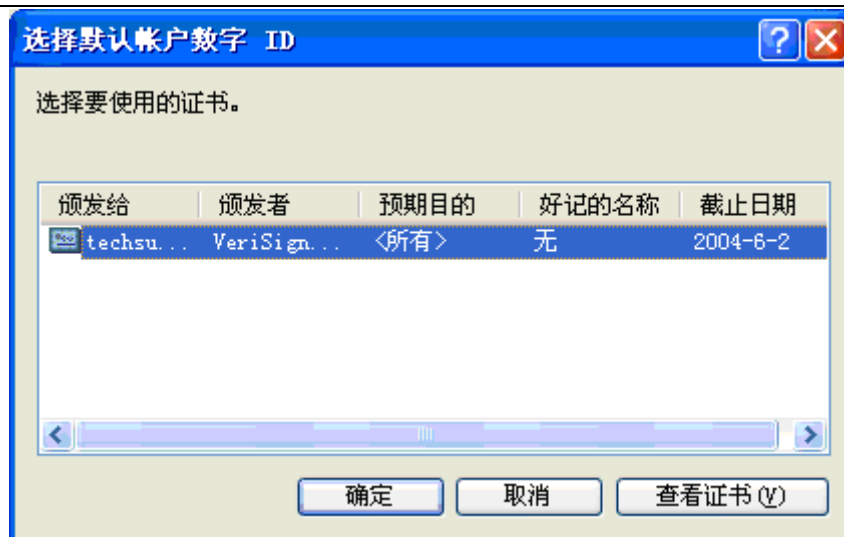


图 19 选择使用在 Outlook Express 的证书

10. 按下“确定”按钮完成设置，并回到 Outlook Express 的主界面。

11. 由下拉式菜单的“工具”里选择“选项”，点选“安全”页面。这时候会显示关于安全设置的一些设置项目，如图 20所示：

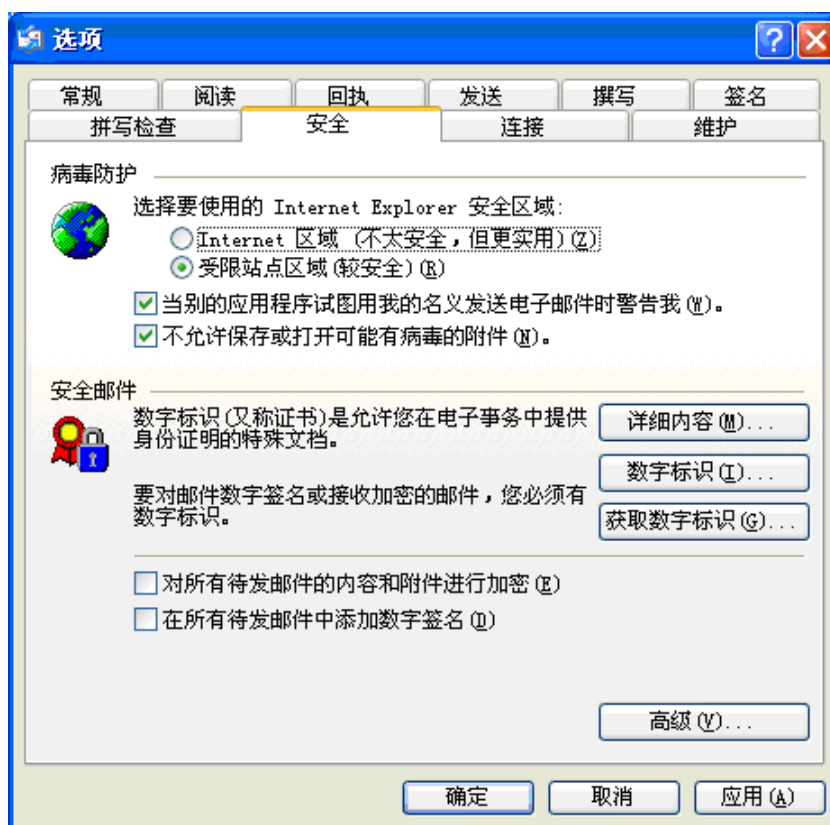


图 20 Outlook Express 整体安全设置

12. 如果想要让发送出去的每一份电子邮件上都附加上数字签名，勾选“在所有待发邮件中添加数字签名”选项，如图 20所示。用户也可以用稍后所说明的方法，在想要发送的电子邮件信息上加上数字签名。

13. 如果要将所发送出去的每一份电子邮件的信息都加密，请勾选“对所有待发邮件的内容和附件进行加密”的选项，如图 20所示。用户也可以用稍后所说明的方式，对想要加密的个别信息进行内容和附件的加密设置。

14. 按下方的“高级”按钮，这时候会启动“高级安全设置”对话框，如图 21所示：

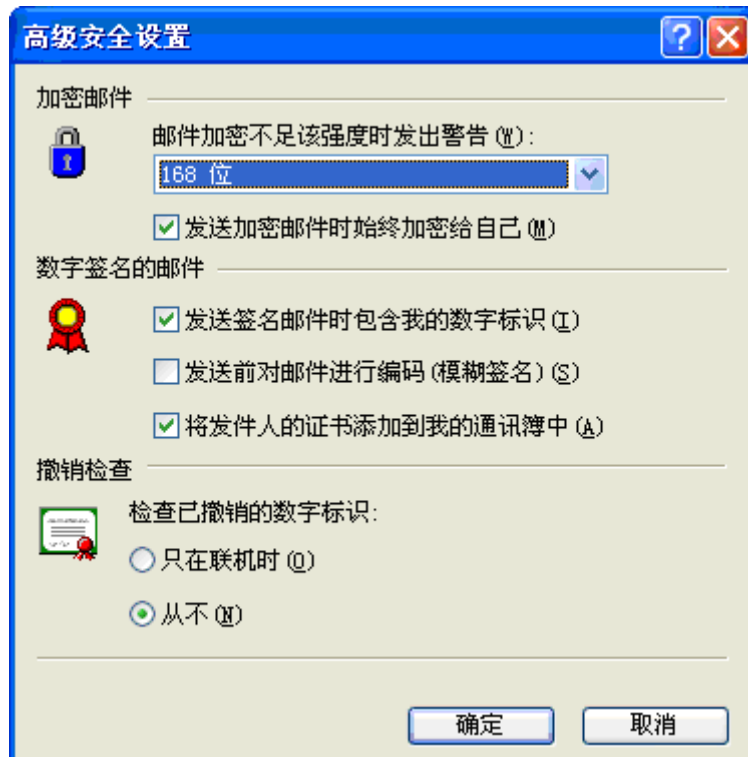


图 21 高级安全设置选项

15. 确定勾选了位于“数字签名的邮件”部分下方的“发送签名邮件时包含我的数字标识”以及“将发件人的证书添加到我的通讯簿中”的选项。因为当发送加密型电子邮件时，发送端的人都必须获取对方的密钥（存储在数字标识中）才可以将邮件加密并发送给接收方，勾选此选项是确保在发送加密邮件时发送端的人能够正确获取加密邮件所使用的对方密钥信息。

另外，用户也可以根据需要调整其它的设置，诸如密钥的长度的设置。

至此用户已经完成了 Outlook Express 的设置。当发送电子邮件信息时，邮件会自动进行加密，并加上数字签名信息。

1.3.3 使用Outlook Express发送附加数字签名的邮件

当设置好 Outlook Express 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。因为，Windows Server 2003 操作系统上的证书服务是采用公钥基础技术来建立的，因此，所有架构在 Windows Server 2003 公钥基础的许多应用程序都具有上述的安全性应用功能。在 Windows 操作系统提供的 Outlook Express 也提供了数字签名以及电子邮件加密的基本功能。

现在，我们就来看看如何在邮件上加上证书所签上的数字签名。按照下列的步骤进行操作：

1. 以用户帐号登录 Windows 系统。
2. 启动 Outlook Express。
3. 按下 Outlook Express 上方的“新邮件”按钮，以便打开一个空的邮件写作窗口，开始编辑新的邮件信息。
4. 填上要发送的收件人地址、主题等相关字段的信息，并填写好该邮件的内容。
5. 若要在该邮件上加附数字签名信息，以证明此邮件的正确来源时，按“签名”按钮，再按下“发

送”按钮，此时会弹出 PIN 码输入框，输入正确的 ePass3000 的 PIN 码后将此信息发送出去。如果此信息仍然出现在发件箱里，您可以按“发送/接收”按钮，手动将邮件发送到邮件服务器上。

对方收到签名的邮件后，会显示邮件经过数字签名的提示，点击“继续”按钮，可以查看邮件的内容，点击右侧的签名图标弹出邮件属性信息对话框，在“安全”页面可以查看签名是否有效。

1.3.4 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邮件进行加密处理（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（假设此私钥只有收件人持有）才能够对此加密过的邮件进行解密的处理，因此，只有持有该私钥的人才能够阅读信件属性（加密邮件）。

要获取对方的公钥或者证书的话，必须要求电子邮件的收件人发送一封带有数字签名的邮件，收到带有数字签名信息的邮件后将其内的证书（数字标识）存储下来，这时候用户就保存有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. 先要求发件人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 Outlook Express，接收对方送过来的电子邮件（夹带有数字签名的邮件），并打开签名的邮件。
3. 在“发件人”字段上按下鼠标右键，并选择“添加到通讯簿”选项，按下“确定”按钮，将收件人以及其公钥与证书存储到 Outlook Express 的通讯簿列表里。这时候就完成了存储对方公钥与证书的操作过程。

1.3.5 使用 Outlook Express 发送属性加密的邮件

若要发送加密的邮件给对方时，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，并且已经存储在 Outlook Express 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：

1. 按下 Outlook Express 上方的“新邮件”按钮，开始编辑新的邮件信息。
2. 接着，在“收件人”的字段上，选择该加密邮件的收件人。注意，若 Outlook Express 通讯簿列表里的收件人附带数字标识信息时，其通讯簿列表上的图标会有一个标志（红色的证书标志），您必须选择夹带有证书信息的收件人，如图 22 所示：



图 22 选择收件人

3. 接着，填写电子邮件的主题等相关字段的信息，并填写好该邮件的内容。
4. 按下“加密”按钮，要求将此邮件信息加密，加密信息按钮图标在图 23 中用红色圈出：

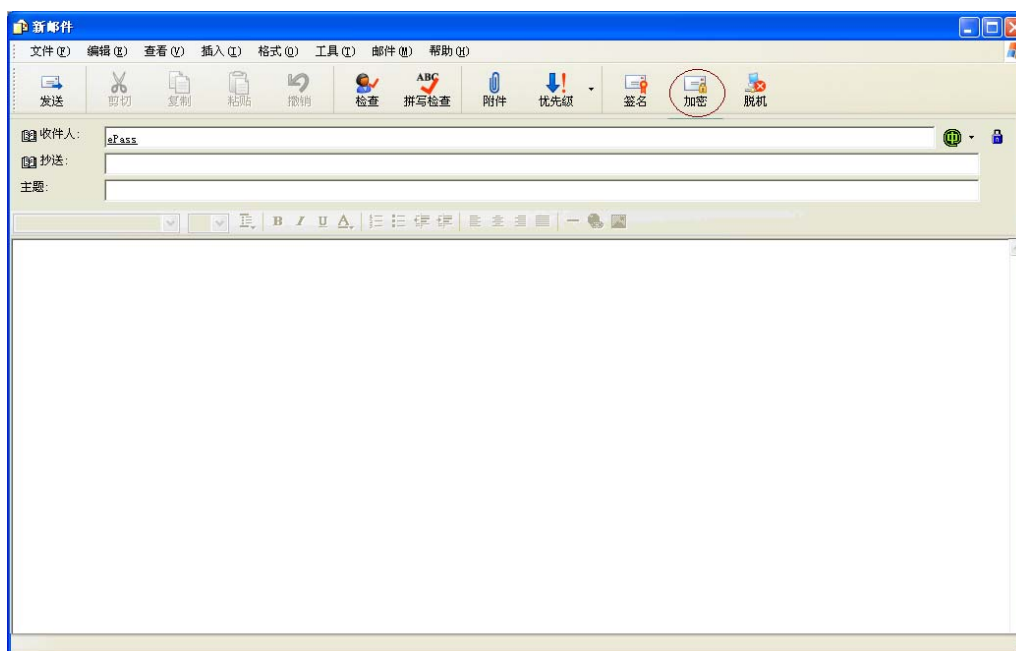


图 23 加密邮件

5. 按“发送”按钮，将邮件发送出去。

至此，已经完成加密邮件的发送。

当对方收到加密的电子邮件后，点击加密的电子邮件会弹出 PIN 码输入框，输入正确的 ePass3000 的 PIN 码即可将电子邮件解密。