

ET199 的 CAPI 应用

1.1 版



版权所有©2007-2008 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

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 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.

章节目录

第一章 ET199 的CAPI应用	1
1.1 使用ET199 的CAPI进行客户证书申请.....	1
1.2 使用ET199 的CAPI访问SSL加密站点.....	4
1.3 使用ET199 的CAPI收发签名与加密邮件.....	5
1.3.1 获取数字证书	6
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	15
1.3.4 获取收件人的公钥和证书.....	16
1.3.5 使用Outlook Express发送属性加密的邮件	16
附录 缩略语及术语	18

图目录

图 1 申请用户证书	1
图 2 用户信息	2
图 3 PIN码输入框	3
图 4 证书挂起	4
图 5 证书列表框	5
图 6 安全Web站点	5
图 7 申请个人数字证书	6
图 8 申请免费数字证书	7
图 9 数字证书代理	7
图 10 线上登记获取数字标识	8
图 11 检查Email提示	9
图 12 数字标识服务第三步	9
图 13 安装数字证书	10
图 14 启动帐号设置	11
图 15 设置您电子邮件帐号的属性	11
图 16 检查电子邮件的设置	12
图 17 邮件帐号的安全设置	13
图 18 选择使用在Outlook Express的证书	14
图 19 Outlook Express整体安全设置	14
图 20 高级安全设置选项	15
图 21 选择收件人	17
图 22 加密邮件	17

第一章 ET199 的 CAPI 应用

ET199 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 ET199 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 ET199 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 ET199 的 CAPI 应用，主要包括 IE 申请证书，访问 SSL 加密站点，Outlook 发送加密、签名邮件等。

- 使用 ET199 的 CAPI 申请数字证书
- 使用 ET199 的 CAPI 访问 SSL 加密站点
- 使用 ET199 的 CAPI 收发签名与加密邮件

1.1 使用 ET199 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ET199。然后通过IE打开证书颁发机构的网页，如图 1所示：

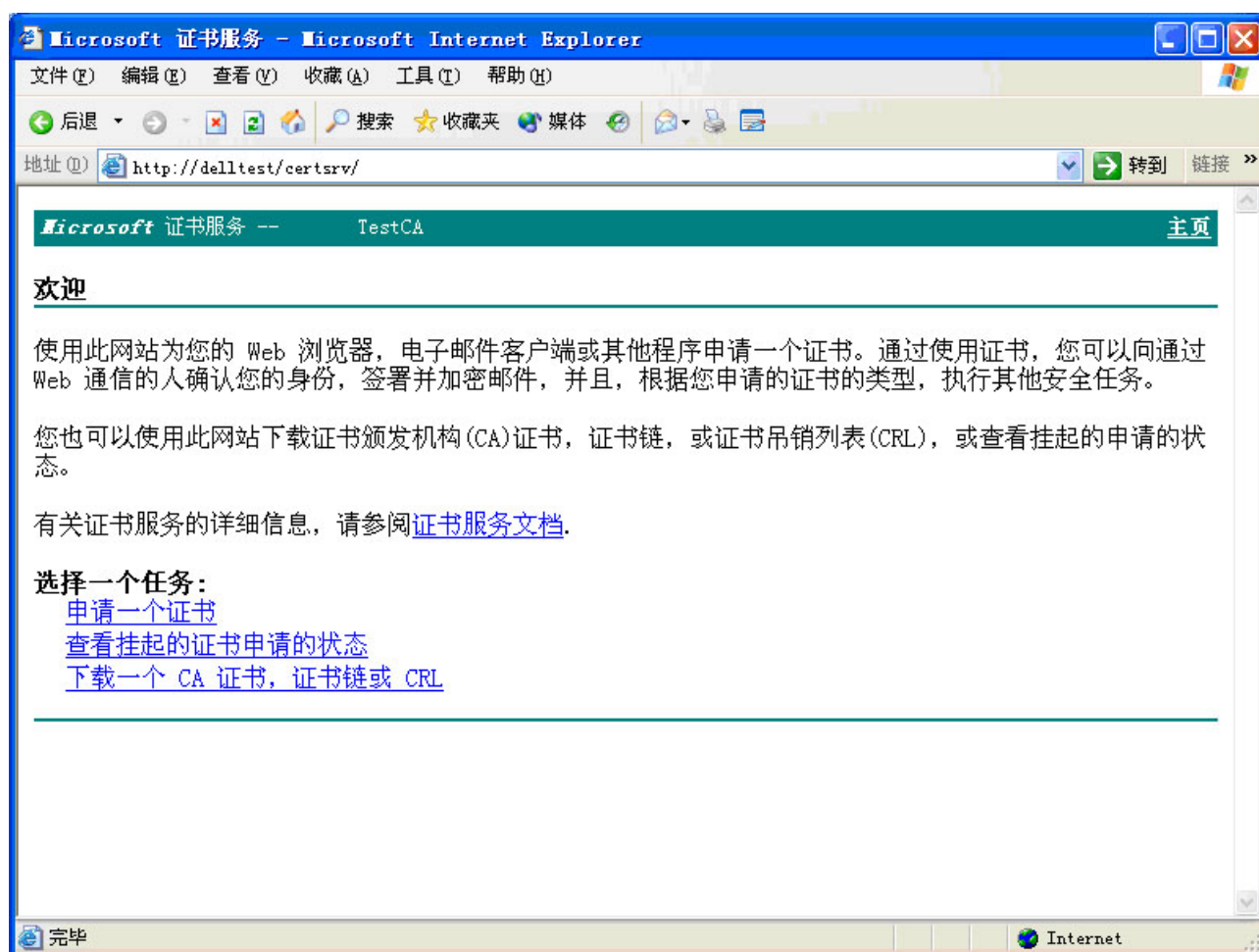


图 1 申请用户证书

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“用户”证书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“EnterSafe ET199 CSP v1.0”，如图 2所示：

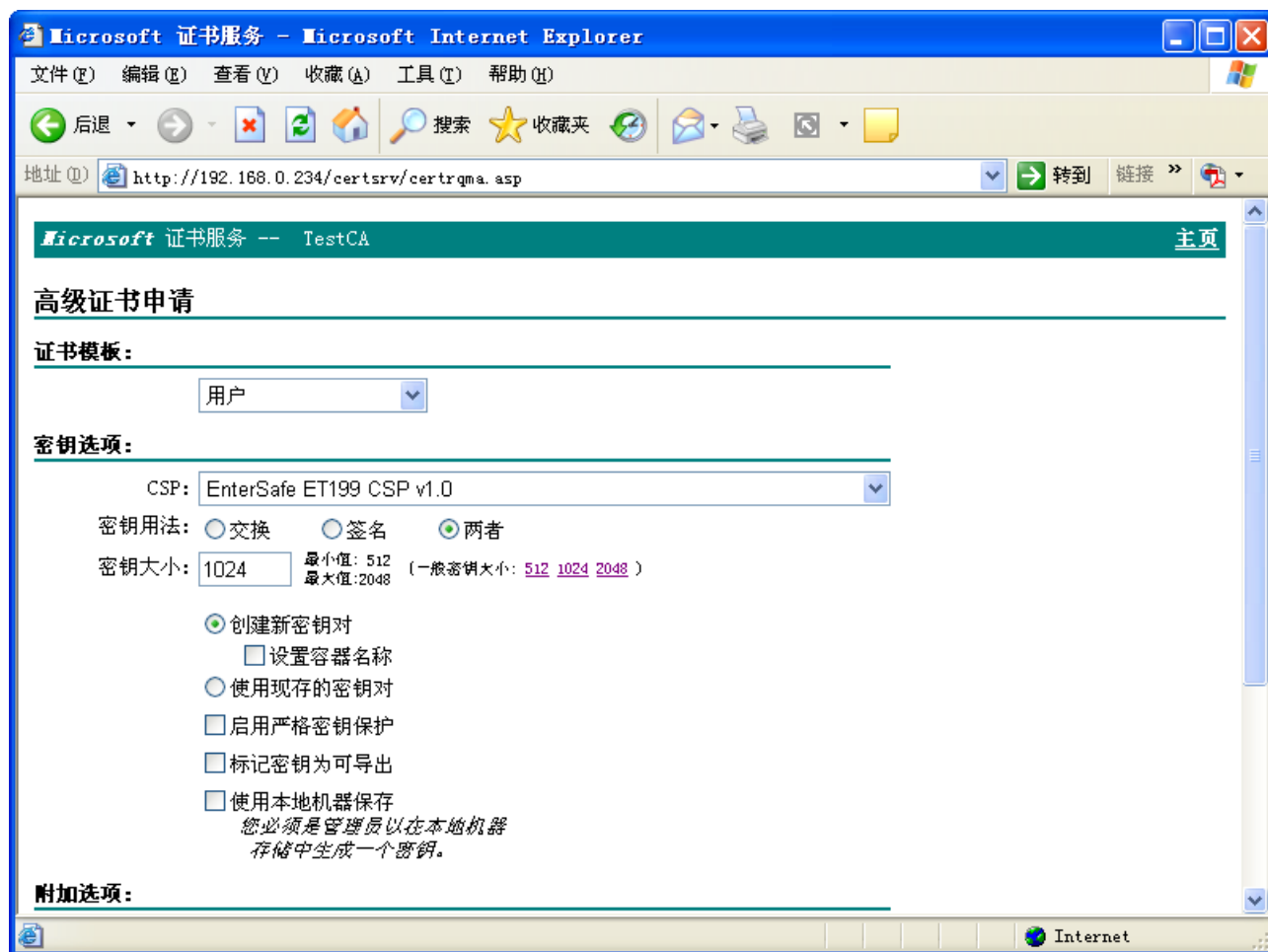


图 2 用户信息

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ET199 已经被列入其中了，选择您要保存证书的ET199，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ET199 则直接弹出PIN码输入框，如图 3所示：

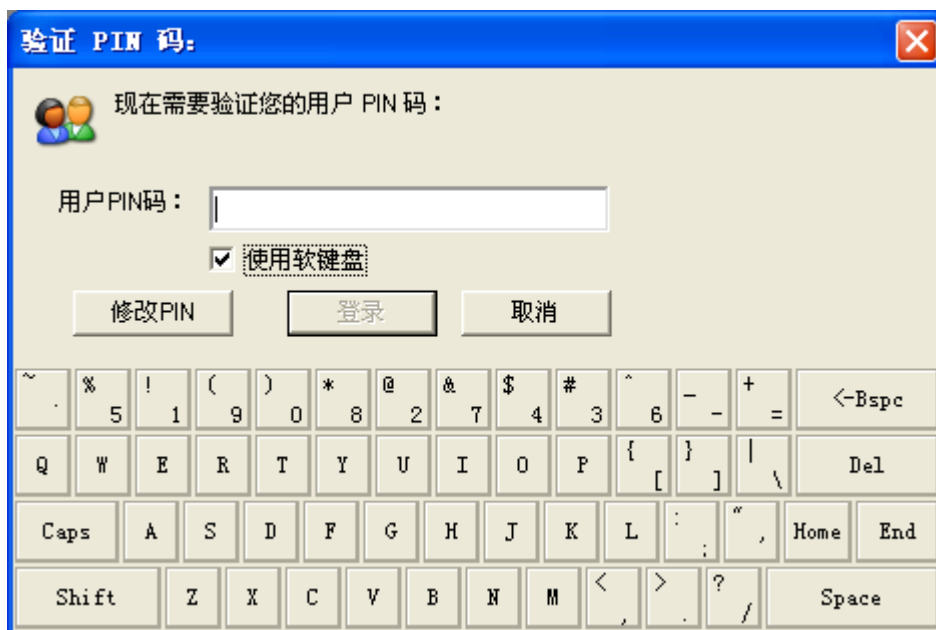


图 3 PIN 码输入框

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，物理键盘的键盘输入将被禁用。另外，只有 Windows2000 以上的操作系统支持软键盘功能，Windows Me 和 Windows98 没有此功能。

用户可以点击“修改 PIN”按钮弹出修改 PIN 码对话框，进行 PIN 码修改。

4. 输入正确的用户PIN码点击“登录”按钮后，稍候会看到证书挂起页面，需要等待颁发机构验证身份并颁发证书，如图 4所示：

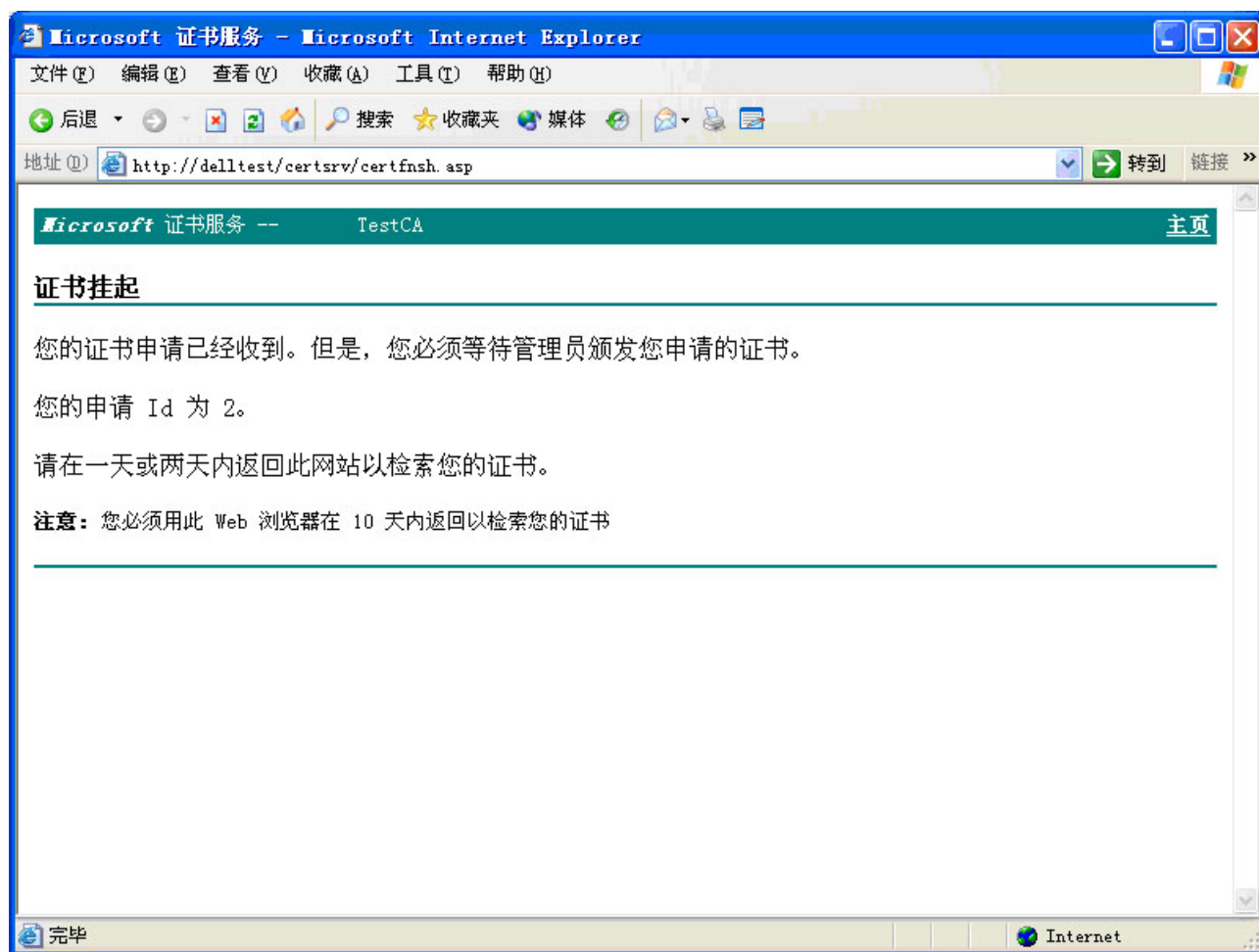


图 4 证书挂起

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 ET199 里。用户可以通过 ET199 管理工具来查看证书是否申请成功。

1.2 使用 ET199 的 CAPI 访问 SSL 加密站点

现在，我们就可以用这支 ET199 来访问安全 Web 站点了。

1. 首先，确认已插入这支申请证书成功的 ET199，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 5 所示：



图 5 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，如图 6所示（此安全Web站点为示例站点）：

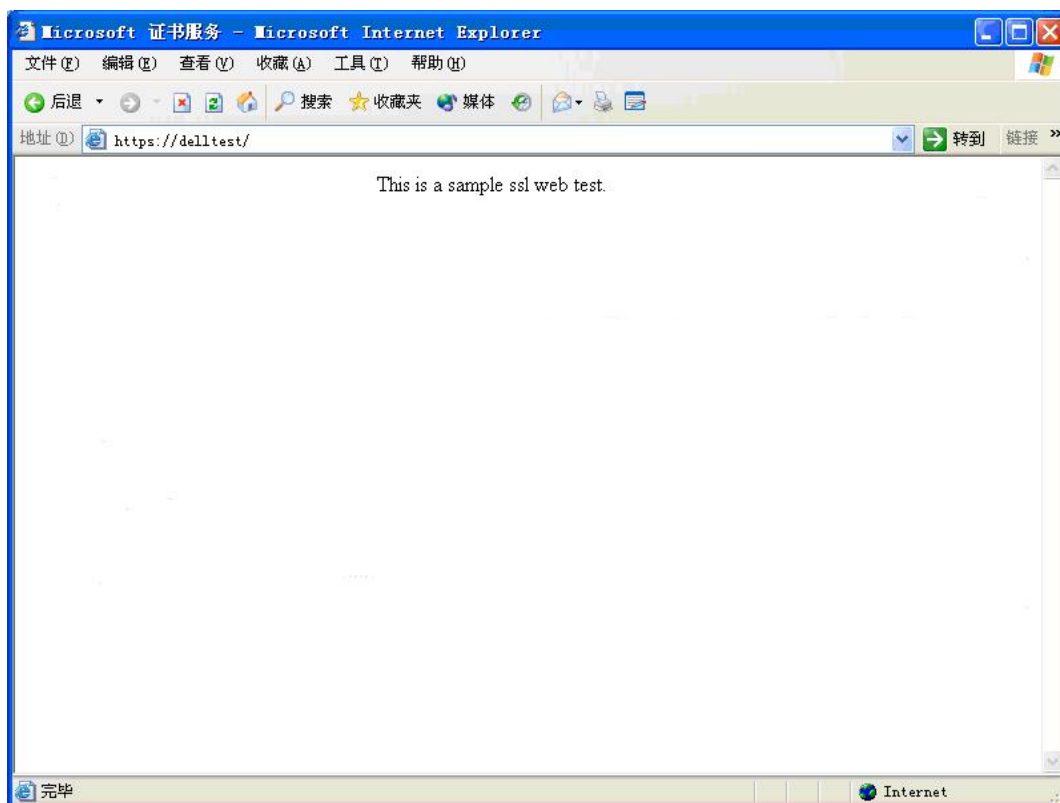


图 6 安全 Web 站点

1.3 使用 ET199 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 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 获取数字标识

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 内的证书。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（坚石诚信不保证这个 CA 总是有效）。在确认插入了一支 PKI 初始化过的 ET199 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 7 所示：

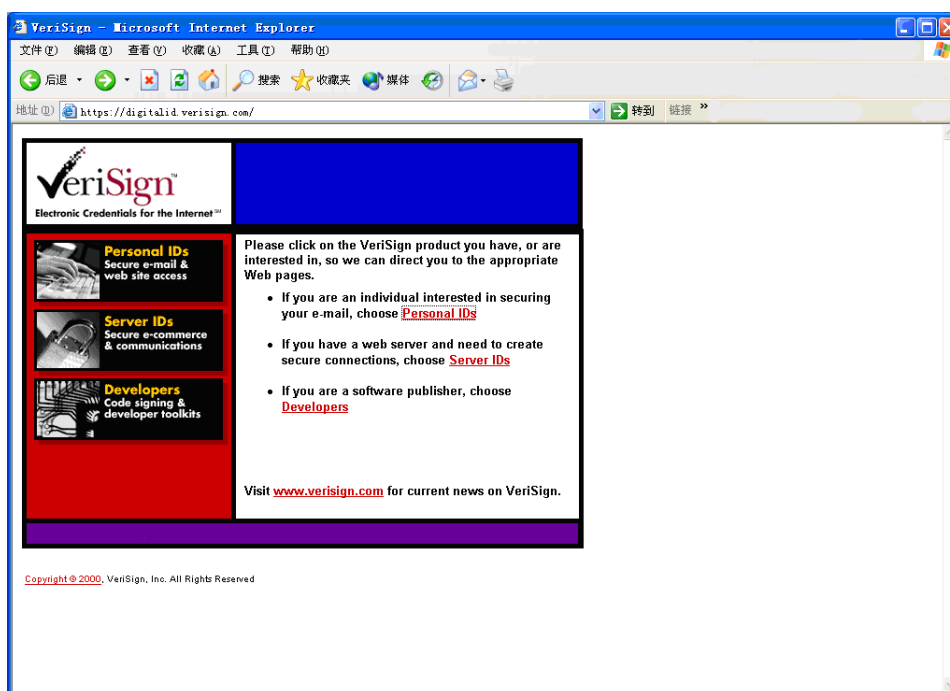


图 7 申请个人数字证书

4. 选择“Personal IDs”后进入图 8 所示的界面：

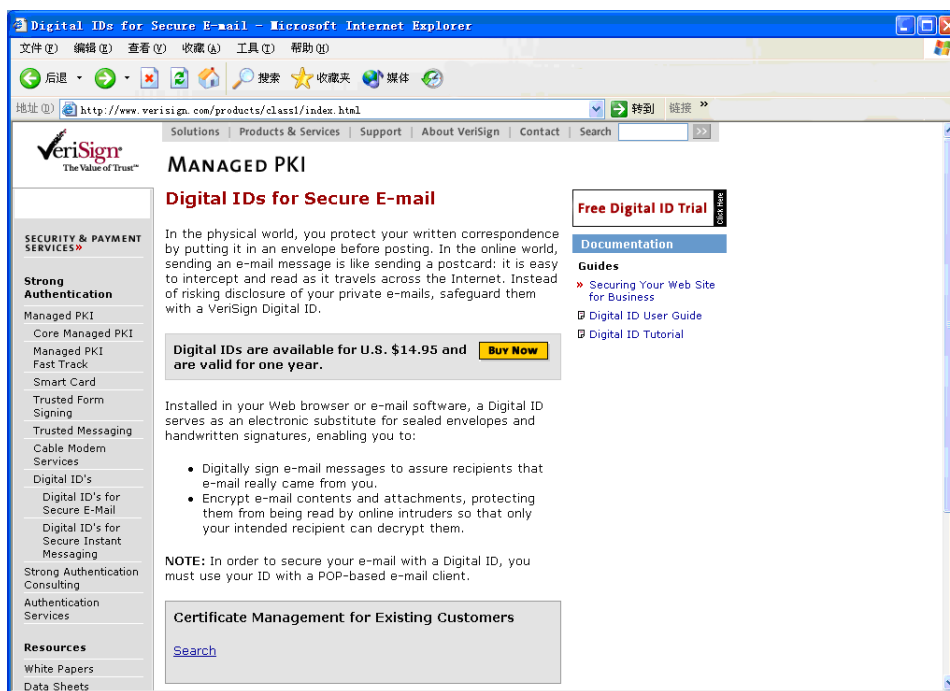


图 8 申请免费数字证书

5. 选择“Free Digital ID Trail”，进入如图 9所示的界面：

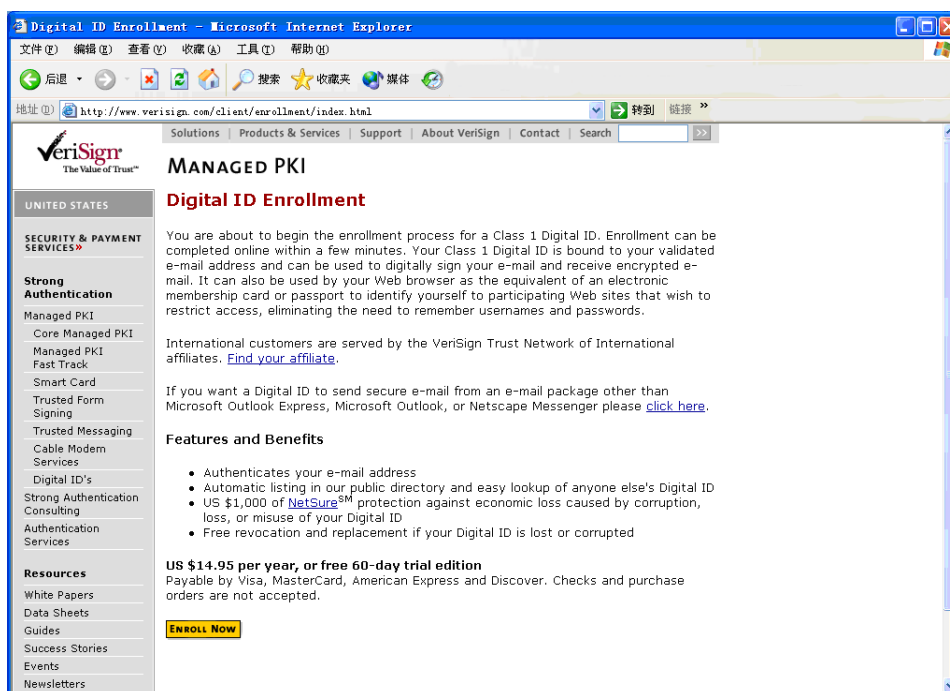


图 9 数字证书代理

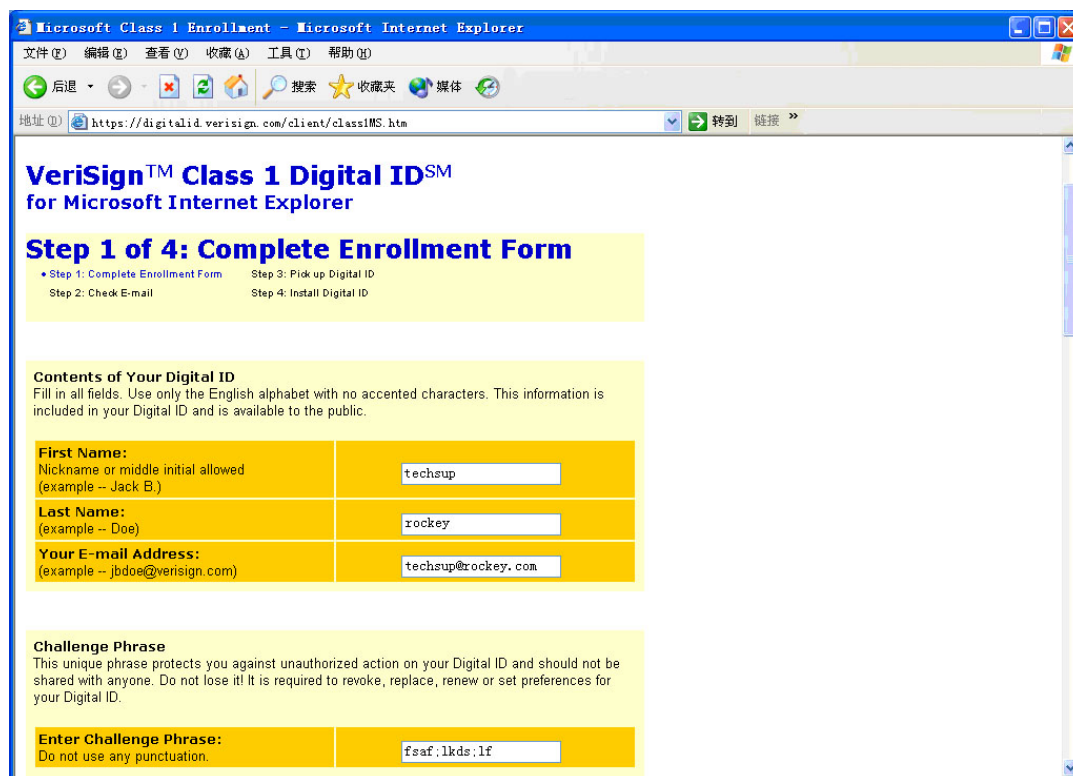
6. 选择“Enroll Now”后进入证书申请页面，如图 10所示：

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，然后用户才可以利用获取的证书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证书时，若用户要求获取的证书的用途是使用在安全性邮件方面时，在登记获取数字证书时都会要求输入用户的 Email 帐号的地址，在这里填写的 Email 帐号即是该数字证书的授予对象，若用户有两个以上的 Email 帐号，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@rockey.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之签发对象的 Email 信箱地址,即 techsup@rockey.com。

以下继续由 Verisign 企业所提供的服务获取数字标识。



Microsoft Class 1 Enrollment - Microsoft Internet Explorer

文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)

后退 前进 刷新 地址 搜索 收藏夹 媒体

地址: https://digitalid.verisign.com/client/class1MS.htm

Verisign™ Class 1 Digital ID™
for Microsoft Internet Explorer

Step 1 of 4: Complete Enrollment Form

- Step 1: Complete Enrollment Form
- Step 2: Check E-mail
- Step 3: Pick up Digital ID
- Step 4: Install Digital ID

Contents of Your Digital ID
Fill in all fields. Use only the English alphabet with no accented characters. This information is included in your Digital ID and is available to the public.

First Name: Nickname or middle initial allowed (example -- Jack B.)	techsup
Last Name: (example -- Doe)	rockey
Your E-mail Address: (example -- jbdoe@verisign.com)	techsup@rockey.com

Challenge Phrase
This unique phrase protects you against unauthorized action on your Digital ID and should not be shared with anyone. Do not lose it! It is required to revoke, replace, renew or set preferences for your Digital ID.

Enter Challenge Phrase: Do not use any punctuation.	fsaf:lkds:lf
---	--------------

图 10 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“EnterSafe ET199 CSP v1.0”。

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ET199,系统会提示输入用户PIN码,如果只插入了一支ET199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 11所示的页面,提示用户去查看Email信箱。

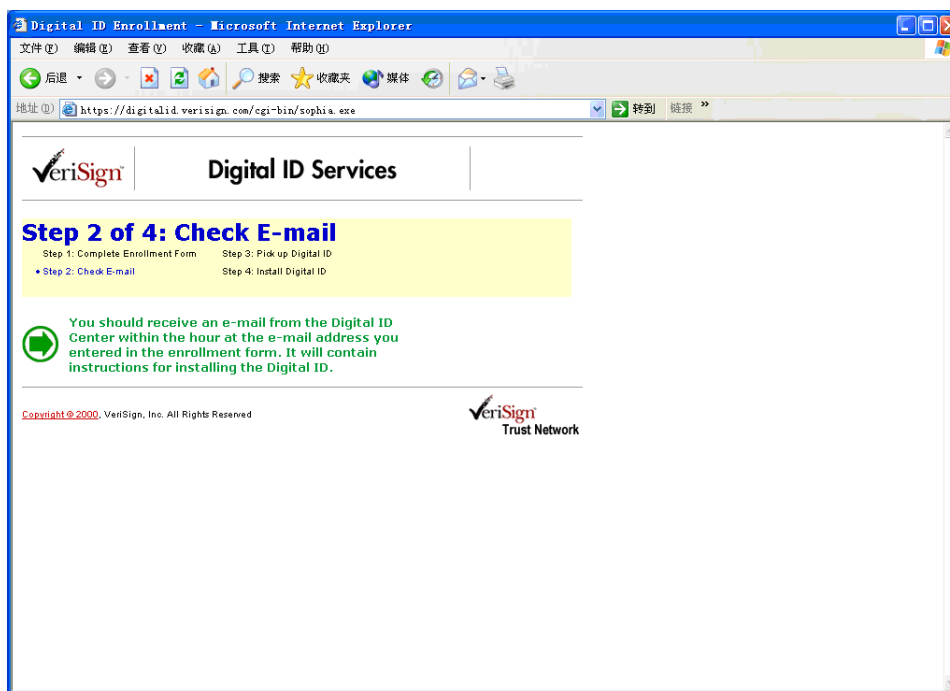


图 11 检查 Email 提示

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 Explore 中打开这个链接，来到“数字标识服务”的第三步，如图 12 所示：

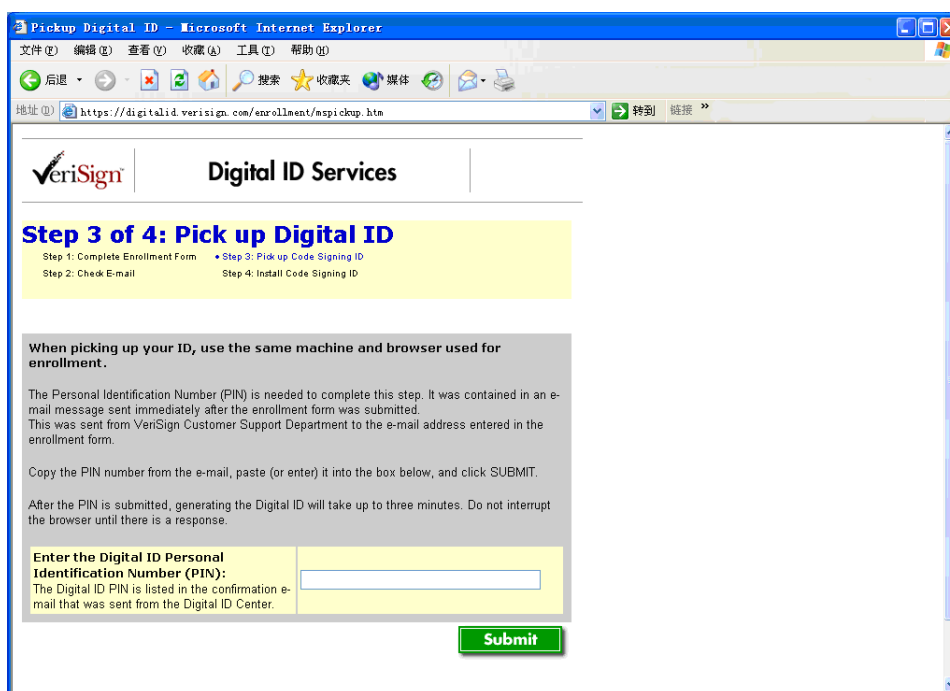


图 12 数字标识服务第三步

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——“安装数字标识”，如图 13 所示：

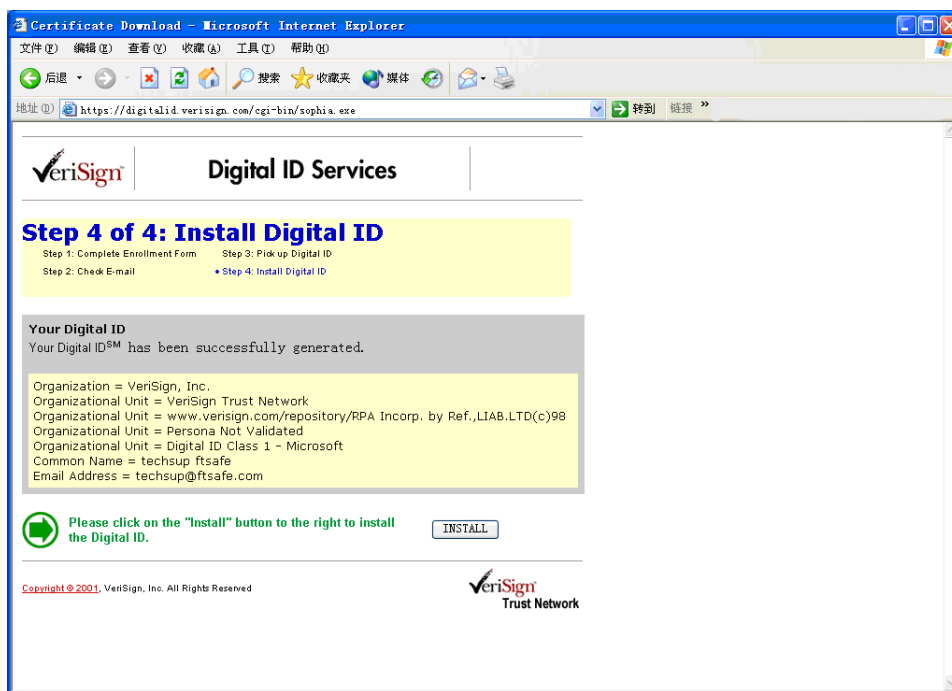


图 13 安装数字证书

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 ET199，如果只连接一个 ET199，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 ET199 管理工具来查看安装的证书。

以上是获取数字标识的操作过程，获取数字标识后，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数字标识，也可以由 Windows Server 2003 证书服务器获取数字标识，要获取数字标识，请按照 1.3.1 中说明的方式进行操作。
- 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 14 所示：



图 14 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 15所示：

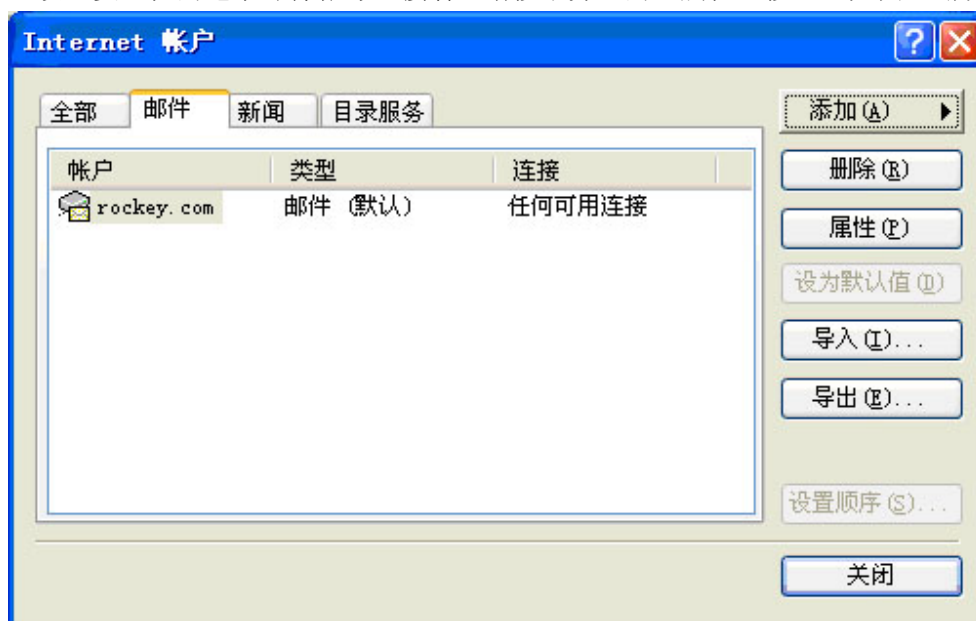


图 15 设置您电子邮件帐号的属性

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 16所示：



图 16 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 17所示：

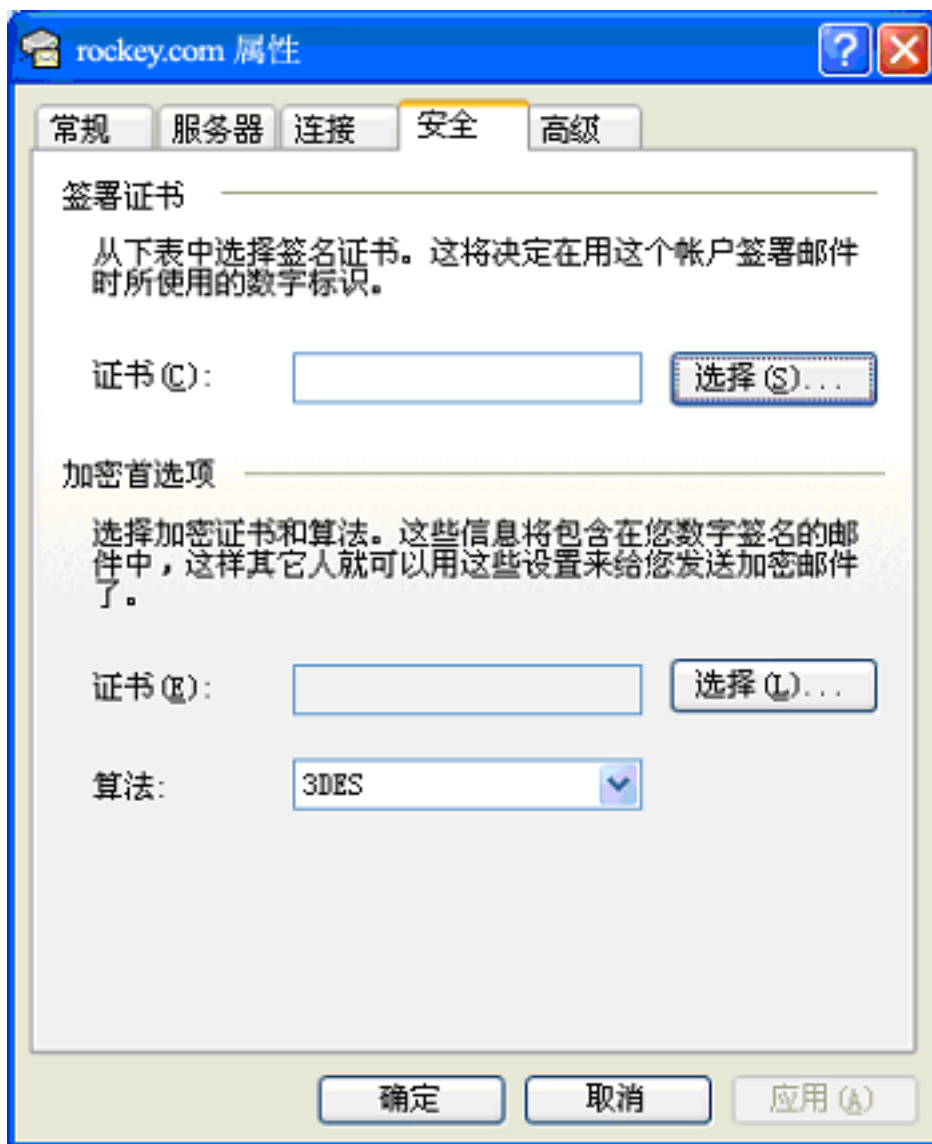


图 17 邮件帐号的安全设置

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数字标识。若要让此 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 18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 18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。

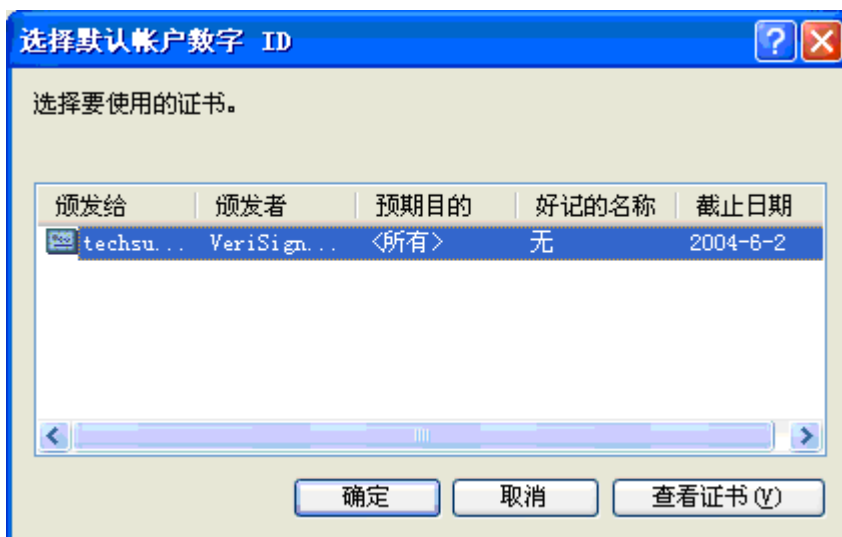


图 18 选择使用在 Outlook Express 的证书

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 19所示：

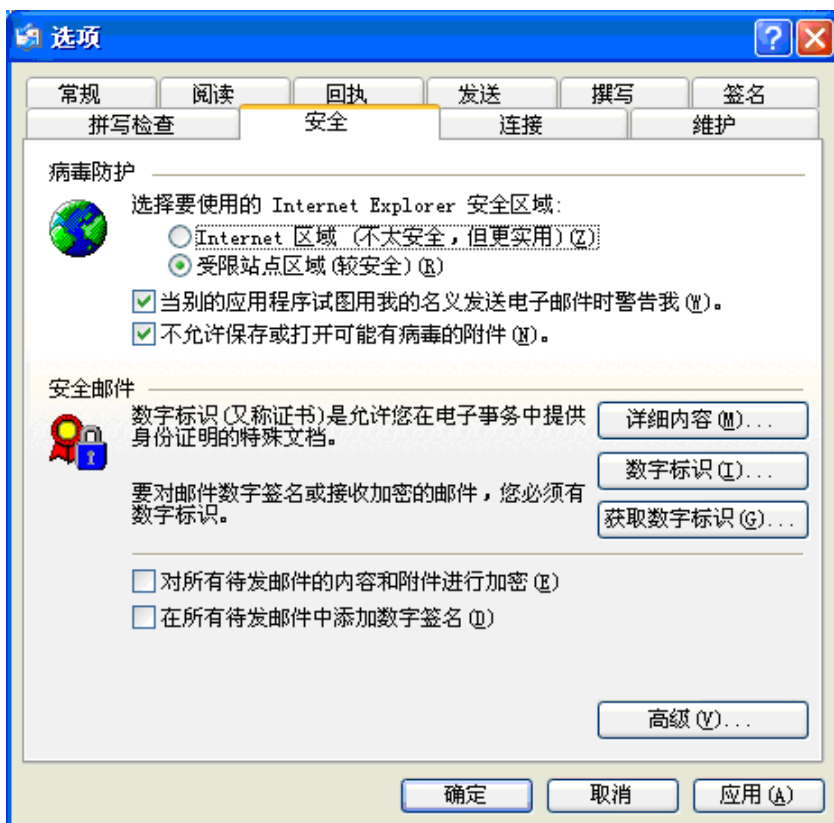


图 19 Outlook Express 整体安全设置

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 19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 19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 20所示：

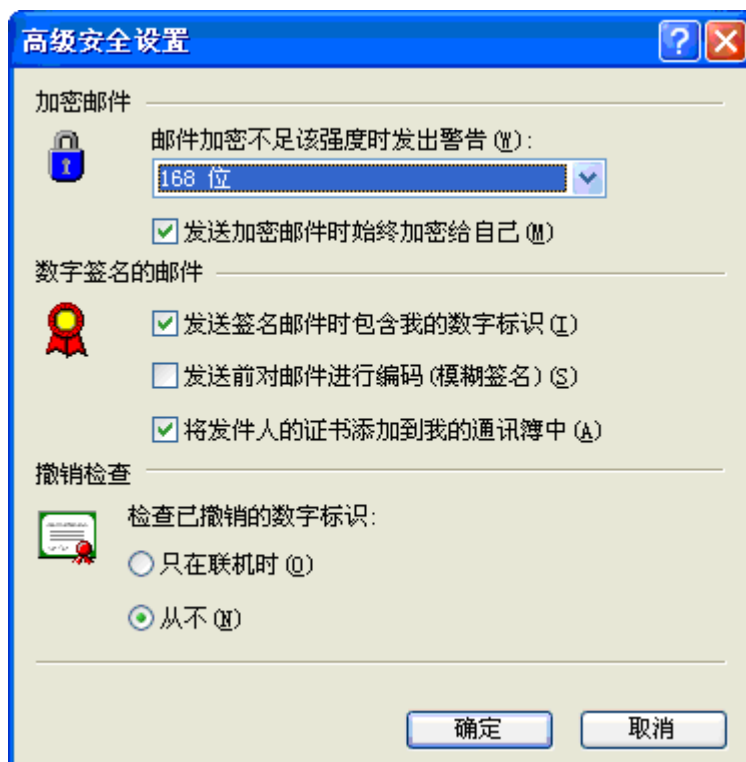


图 20 高级安全设置选项

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将加密邮件发送给接收者，勾选此选项是确保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. 若要在此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 ET199 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（假设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信件，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. 先要求接收者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证书并且已经存储在 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有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 21 所示：



图 21 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 22 中用红色圈出：

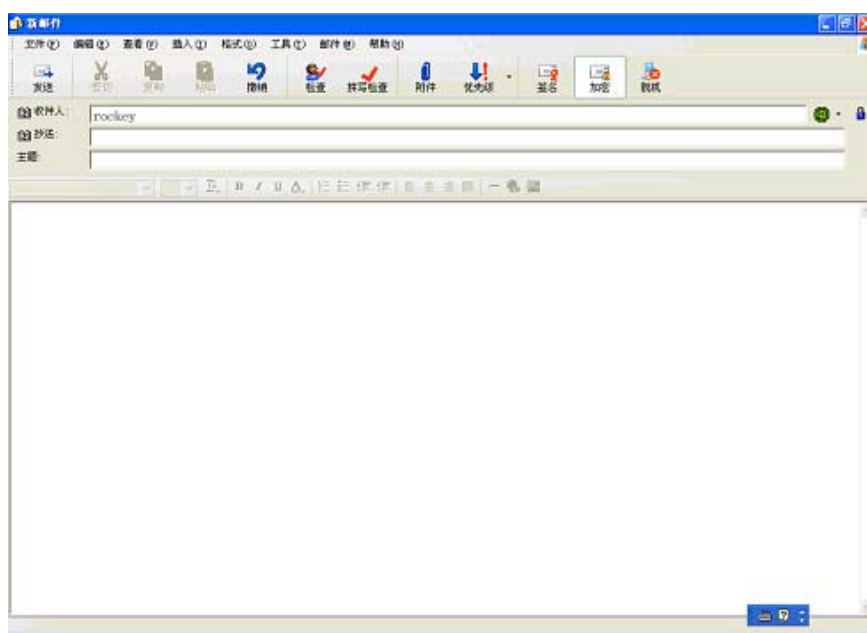


图 22 加密邮件

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 ET199 的 PIN 码即可将电子邮件解密。

附录 缩略语及术语

缩略语及术语	解 释
ET199	坚石诚信推出的 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。
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。ET199 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。