《NCIE 培培你》

----------商宏图投稿 2004.12.5

◆每周一讲

在 Windows 2000 下利用证书服务实现邮件加密和签名

（NCSE 二级内容）

NCIE 考试管理中心课程策划、教学督导　商宏图（shanght@ncie.gov.cn）

在今天这样一个信息化的时代，人们每天都通过电子邮件进行交流。可是网络中的各种威胁却使人们在发送电子邮件总是没有足够的安全感，人们总是担心诸如“我的邮件是不是会被别人截取”、“别人会不会看到我的信息”等等这样的安全问题。因此如何来实现邮件安全就成为一个非常重要的问题摆在我们面前。

要实现邮件安全可以对邮件进行加密，这样即使邮件被非法用户获取也无法读取其中的数据，这样就实现了邮件的数据安全性。

加密可以分为对称式加密和非对称式加密两种方式。在对称式加密中，加密的算法和解密的算法是相同的。因此只要知道了加密的方法，就可以进行解密，所以这种加密的方法不是很安全。在非称式加密中加密的算法和解密的算法不是相同的，而是采用了密钥对的方式，每个用户都有一个“公钥”和一个“私钥”，其中“公钥”是对所有潜在的用户公开的，而“私钥”只有用户本人才有。这对密钥必须配对使用，如果用某个用户账号的“公钥”加密，则只能用该用户账号的“私钥”进行解密，反之亦然。

举例来说，用户 A 想给用户 B 发送一封 E_mail，则用户 A 可以用 B 的“公钥”对数据进行加密（B 的“公钥”对所有潜在的用户都是公开的），然后传送给 B。当用户 B 收到数据时，如果能用自己的“私钥”进行解密的话，说明这封信的确是发给自己的。其他用户，即使拿到这个数据，由于没有 B 的“私钥”，也无法对数据进行读取。这种“公钥加密”，“私钥解密”的方式，称为“数字信封”，用来确认收件人。同时，当用户 A 发送数据时，除了用 B 的“公钥”对数据进行加密外，还可以用自己的“私钥”进行加密。这样，当用户 B 收到数据时，如果能用 A 的“公钥”进行解密的话（A 的“公钥”对所有潜在的用户都是公开的），说明这封信的确是用户 A 而不是其他用户发的。这种“私钥加密”，“公钥解密”的方式，称为“数字签名”，用来确认发件人。

在 Windows 2000 中使用“证书服务”给用户颁发证书，颁发证书的机构称为 CA。在颁发证书的同时就把“私钥”给了用户，而“公钥”保留在 CA 中。对 CA 来说应该保证用户“私钥”的惟一性（同时也就保证了用户“公钥”的惟一性）。当多个用户从同一个 CA 申请证书时（代表这些用户都信任该 CA），这些用户可以认为自己的私钥是惟一的。

下面讲述一下在 Windows 2000 下利用证书服务的功能实现邮件加密的过程。

- **安装证书服务**

1．首先在网络中的一台 Windows 2000 Server 计算机上安装证书服务。在“控制面板”中选择“添加/删除程序”→“添加/删除 Windows 组件”，在“Windows 组件向导”对话框中选择“证书服务”，如图 1-1 所示。

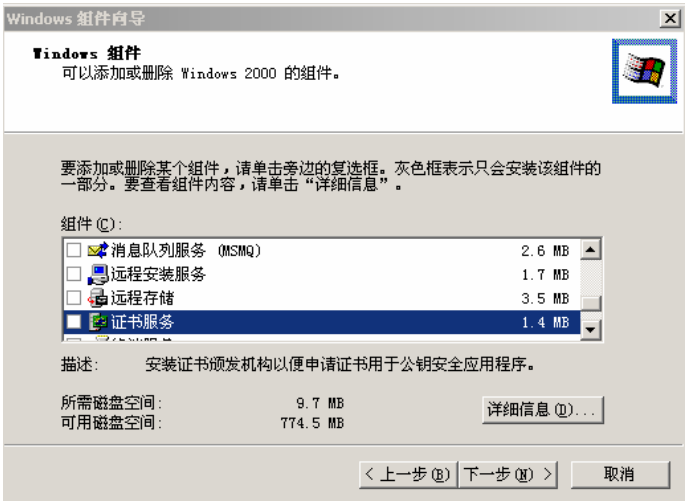

图 1-1 Windows 组件向导对话框

2．选中“证书服务”后单击“下一步”按钮，出现如图 1-2 所示对话框，提示安装证书服务后计算机不能重命名，不能加入域或从域中删除。

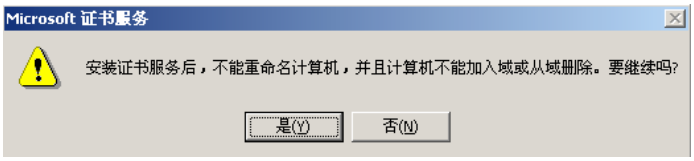

图 1-2　Windows 提示对话框

3．单击“是”按钮，出现如图 1-3 所示对话框，在此选择 CA 的类型。在 Windows 2000 中 CA 可以分为两大类，一种是企业级 CA，另一种是独立的 CA。其中企业级 CA 要依赖活动目录，可以提供更高的功能。独立的 CA 不依赖活动目录。

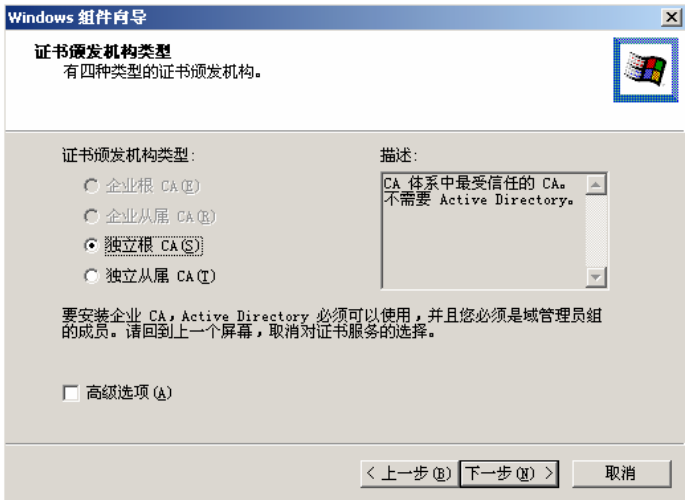

图 1-3 选择证书颁发类型

4．此处选择安装“独立根 CA”，单击“下一步”按钮出现如图 1-4 所示“CA 标识信息”对话框，在此输入标识该 CA 的信息，如图 1-4 所示。

图 1-4　输入 CA 标识信息

5．单击“下一步”按钮，出现如图 1-5 所示“数据存储位置”对话框，在此选择证书数据库和证书数据库日志文件的物理位置。

图 1-5　指定证书数据库和日志位置

6．单击“下一步”按钮，出现如图 1-6 所示对话框，提示如果要安装证书服务，必须停止 Internet 信息服务。

图 1-6　Windows 提示对话框

7．单击“确定”按钮，开始执行安装。安装过程中需要提供 Windows 2000 Server 安装源文件，如图 1-15 所示。

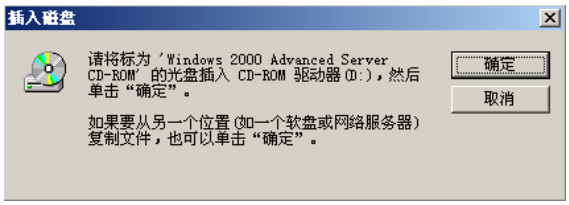

图 1-7 提示提供 Windows 2000 Server 安装源文件

8．单击“确定”按钮完成证书服务安装。

- **安装邮件服务器**

1．邮件传输离不开邮件服务器，此处以利用 MDaemon 为例创建邮件服务器的过程。双击 MDaemon 邮件服务器安装文件“MDaemon pro 6.85 官方简体中文版.exe”执行安装（安装过程略）。

2. 安装成功后启动 MDaemon 服务，设置邮件域名为 sht.com，并创建两个用户账号 simon 和 steven，如图 1-8 所示。

图 1-8 MDaemon 账号管理器

3．邮件服务需要 DNS 服务器的支持，在 DNS 服务器上为邮件域名创建正向搜索区域 sht.com，并在该区域中为邮件服务器创建相应的主机记录（A）和邮件交换器记录（MX），如图 1-9 所示。

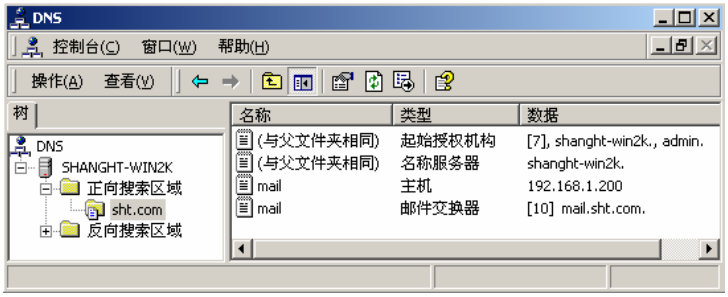

图 1-9 DNS 控制台下新建主机记录和邮件交换器记录

- **设置邮件客户端，测试邮件服务器**

1．本文选择 Windows 系统自带的 Outlook Express 作为邮件客户端。在一台 Windows 计算机上打开 Outlook Express，设置 Outlook Express 的用户名为 simon，如图 1-10 所示。

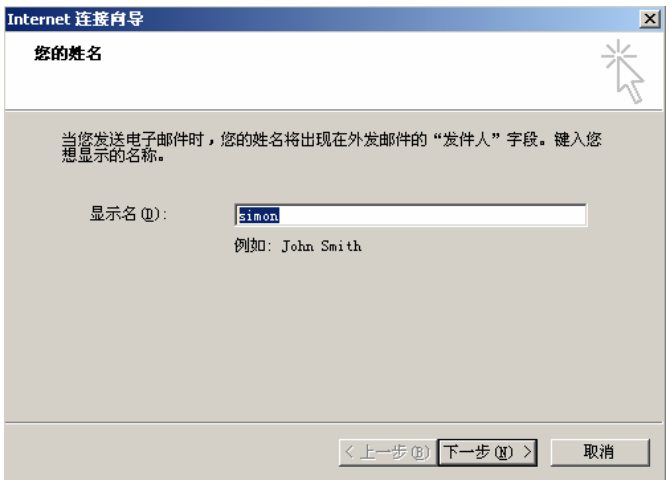

图 1-10 输入邮件客户端用户名

2．单击“下一步”按钮，出现图 1-11 所示对话框，在此指定用户的邮件地址为 simon@sht.com。

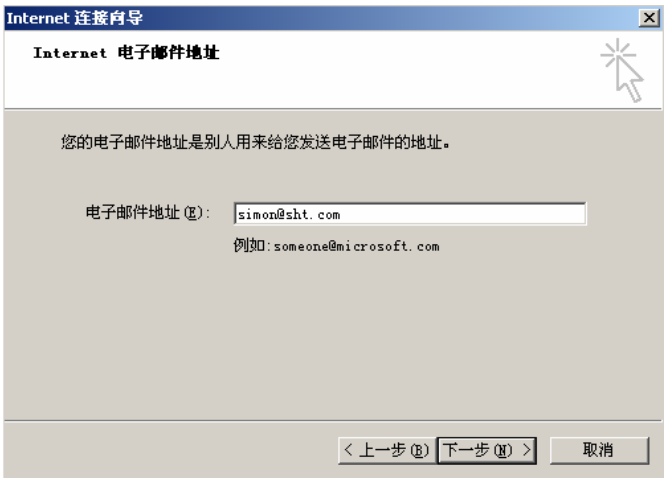

图 1-11 输入邮件地址

3．单击“下一步”按钮，指定电子邮件服务器名，如图 1-12 所示。

图 1-12 指定邮件服务器地址

4．单击“下一步”按钮指定该客户端在邮件服务器上的用户账号名称和密码，如图 1-13 所示。

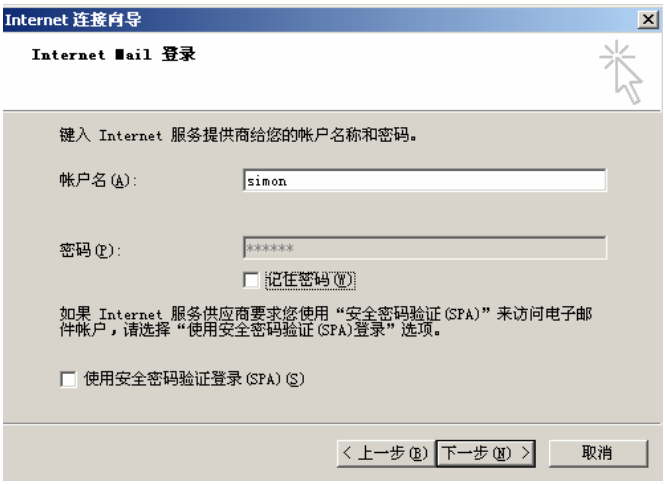

图 1-13 输入用户账号名称和密码

5．单击“下一步”按钮，完成用户账号 simon 的设置，按照同样的步骤设置用户账号 steven。

分别设置两台客户端计算机的 TCP/IP 属性，把 DNS 指向维护区域 sht.com 的计算机。在用户 steven 的计算机上给用户 simon 发送一封电子邮件，在 simon 客户端上接收邮件，可以看到由 steven 发来的邮件，如图 1-14 所示。由于没有采用任何加密措施，这时邮件是以明文的方式发送的。

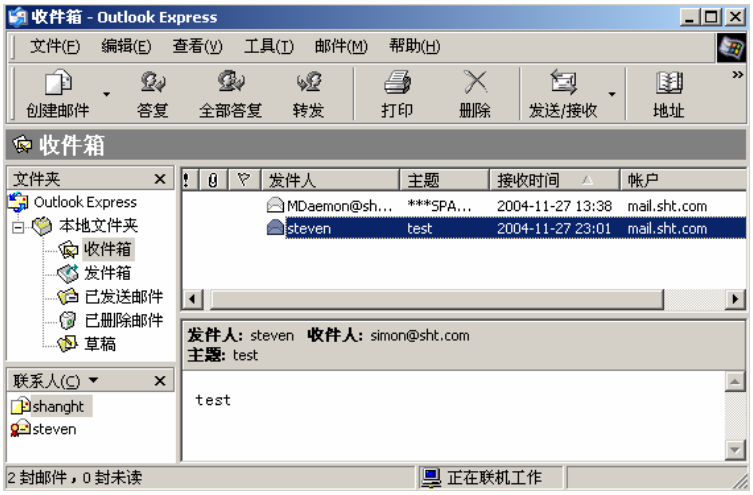

图 1-14 邮件接收测试

- 客户端申请证书以进行邮件加密

1．为了进行邮件加密，用户 simon 和 steven 都要申请证书。此处以 simon 为例说明证书的申请过程。

在用户 simon 的计算机上打开 IE 浏览器，在地址栏中输入“http://CAServer/certsrv”，其中 CAServer 为证书服务器的主机名或 IP 地址，连接成功后出现图 1-15 所示的画面，在此可以看到证书服务器的标识为上面安装的证书颁发机构 NCNE-shanght。

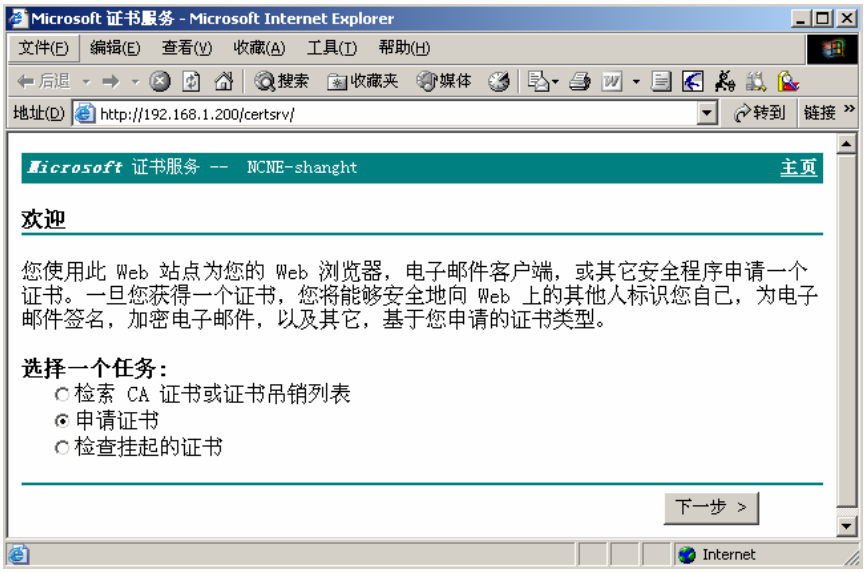

图 1-15 在 IE 浏览器中申请证书

2．选择“申请证书”，单击“下一步”按钮，出现如图 1-16 所示画面，在此选择证书类型。

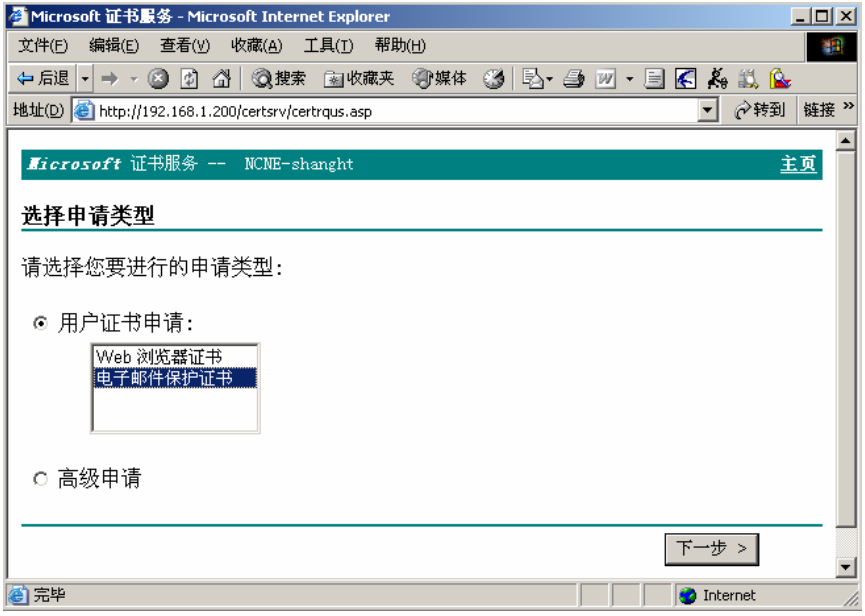

图 1-16 选择申请证书的类型

3．选择“电子邮件保护证书”，单击“下一步”按钮，出现如图 1-17 所示画面，在此输入用户账号的名称“simon”和邮件地址“simon@sht.com”。

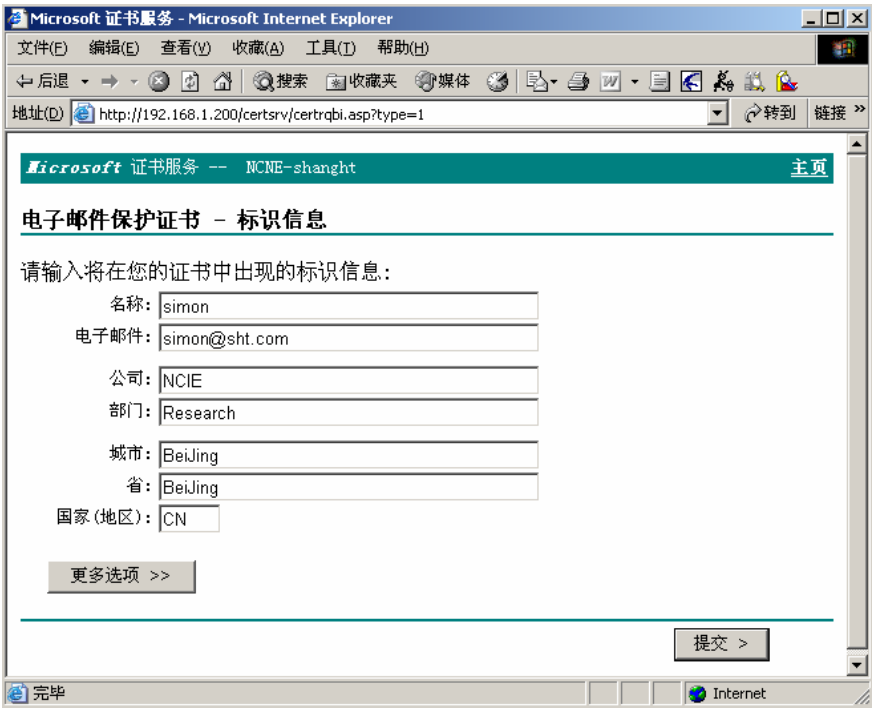

图 1-17 输入用户名称和电子邮件地址

4．单击“提交”按钮，出现图 1-18 所示对话框。

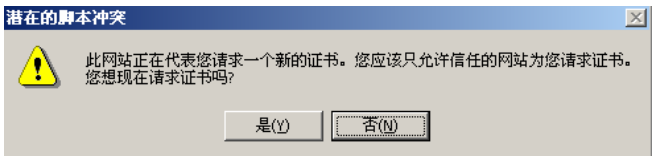

图 1-18 Windows 提示信息

5．单击“是”按钮提交申请，出现如图 1-19 所示画面，显示证书申请已经收到。

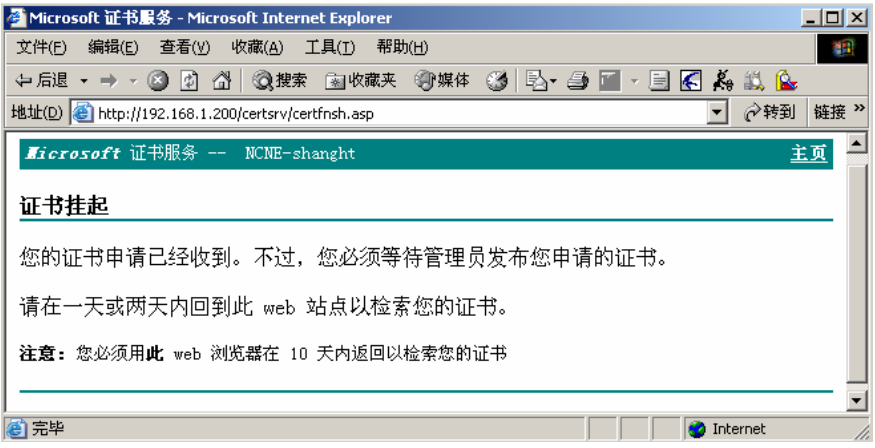

图 1-19 证书挂起

6．在证书服务器上单击“开始”→“程序”→“管理工具”→“证书颁发机构”，打开“证书颁发机构”控制台，在控制台下单击“待定申请”，在右边的窗口中可以看到用户的申请。右键单击客户申请选择“所有任务”，选择“颁发”，给用户颁发证书。

图 1-20 为客户端颁发证书

7．在客户端 simon 的计算机上再次打开 IE 浏览器，如图 1-21 所示。

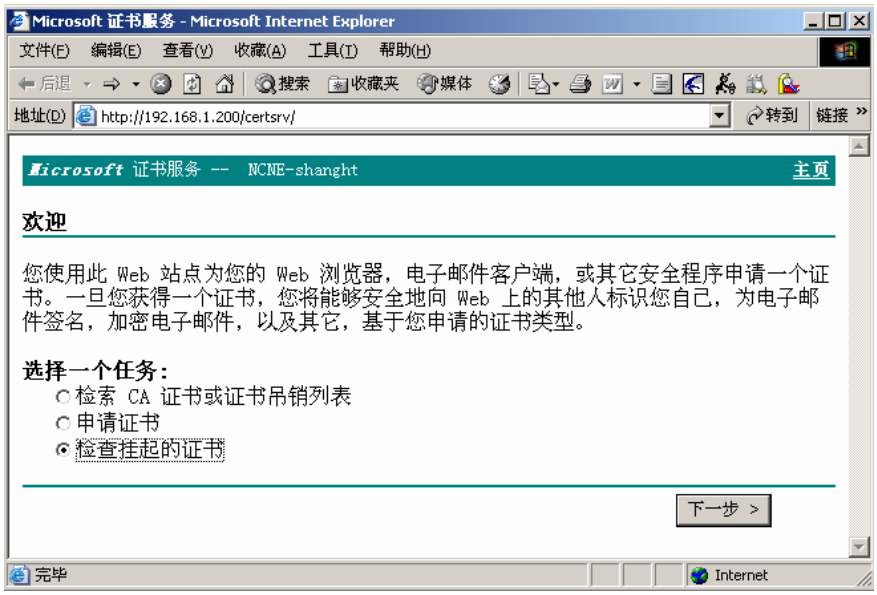

图 1-21 检查挂起的证书

8．选择“检查挂起的证书”，单击“下一步”按钮，出现如图 1-22 所示画面。

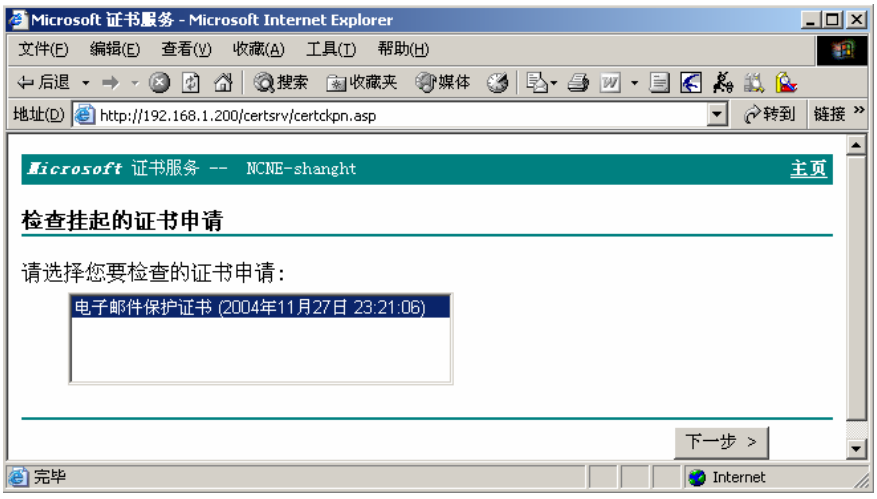

图 1-22 检查挂起的证书申请

9．单击“下一步”按钮，出现如图 1-23 所示画面，显示证书已经颁发。

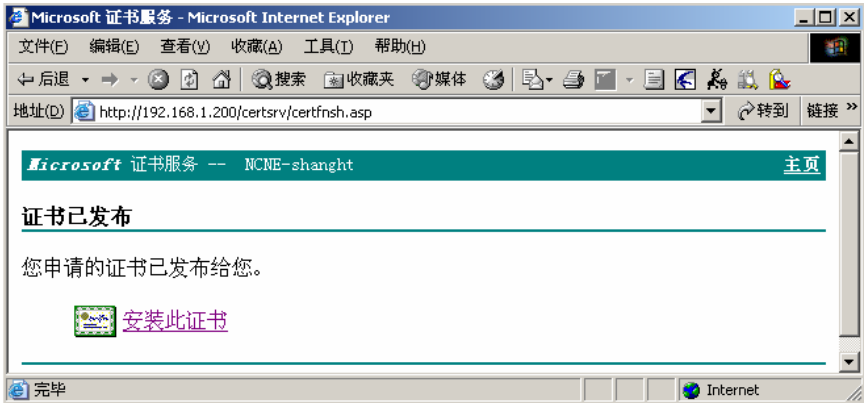

图 1-23 提示证书已发布

10．单击“安装此证书”，出现如图 1-24 所示的 Windows 提示信息。

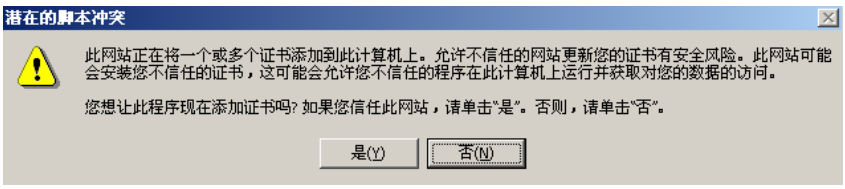

图 1-24 Windows 信息提示

11．单击“是”按钮，安装此证书，如图 1-24 所示。

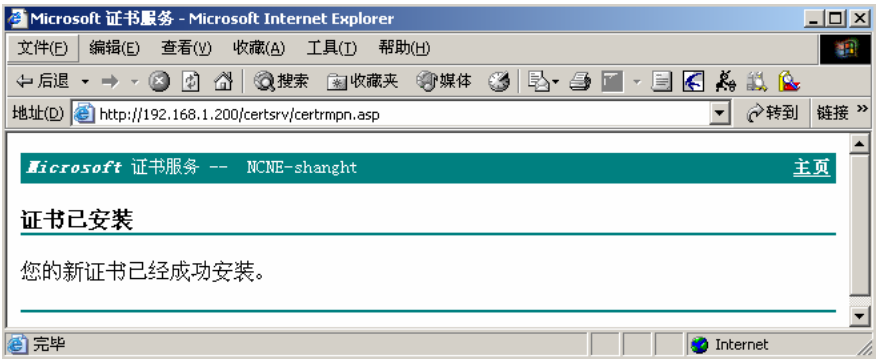

图 1-25 证书安装成功

12．要对邮件进行加密用户彼此之间必需拥有对方的公钥，因此需要把证书导出。在证书导出的过程中就把用户的公钥导出了。

在用户 simon 的计算机上打开 IE 浏览器，选择“工具”→“Internet 选项”，在“Internet 选项”对话框中选择“内容”标签，如图 1-26 所示。

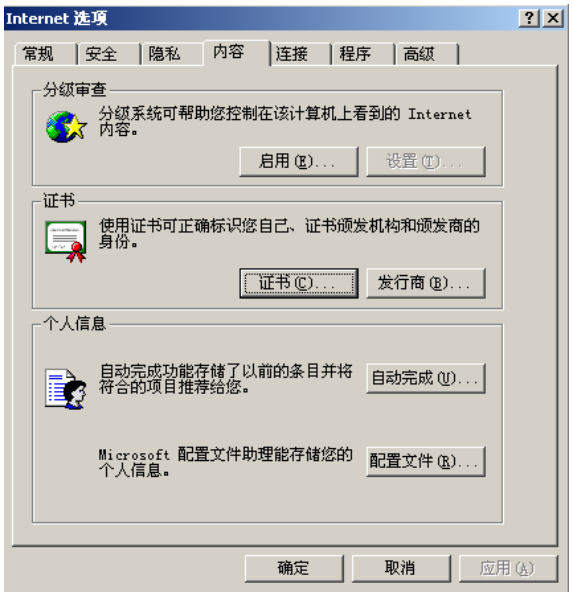

图 1-26 Internet 选项“内容”标签

13．单击“证书”按钮，在证书对话框的“个人”标签中可以看到上面申请的证书。如图 1-27 所示。

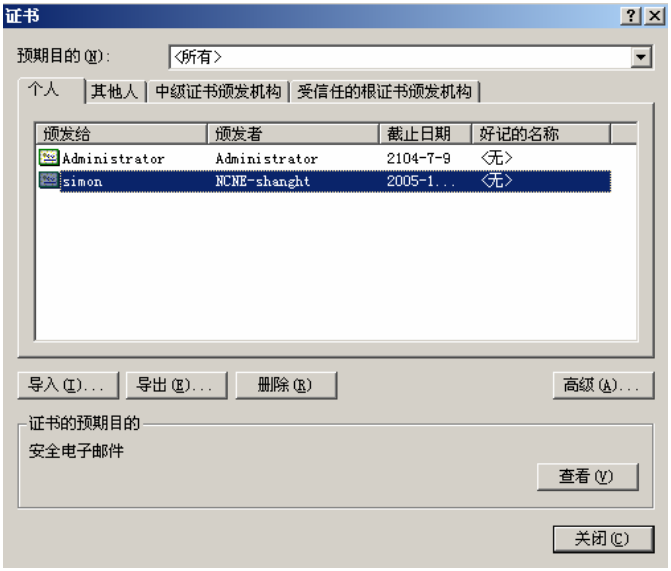

图 1-27 证书对话框

14．选中证书“simon”，单击“导出”按钮，出现“证书导出向导”对话框，如图 1-28 所示。

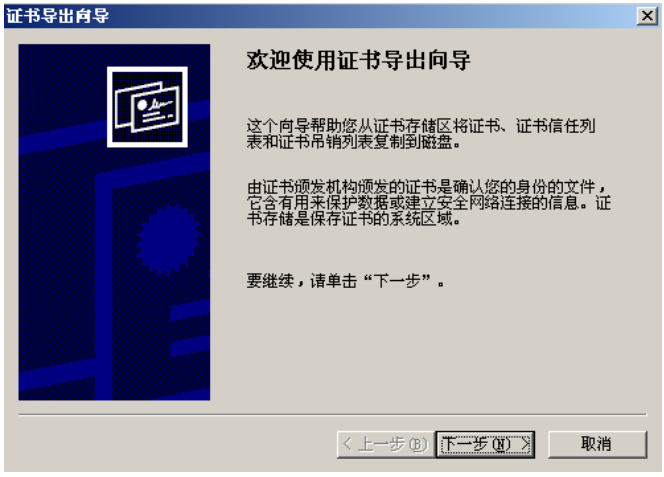

图 1-28 证书导出向导

15．单击“下一步”按钮，出现如图 1-29 所示对话框。

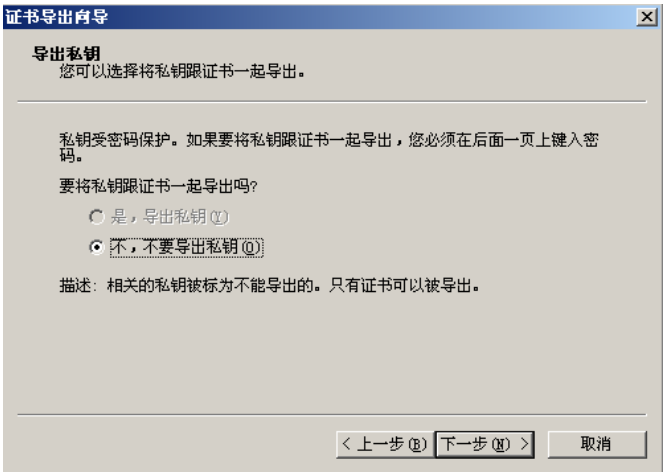

图 1-29 证书导出

16．选择“不，不要导出私钥”，单击“下一步”按钮，出现如图 1-30 所示对话框，在此选择证书导出的格式。

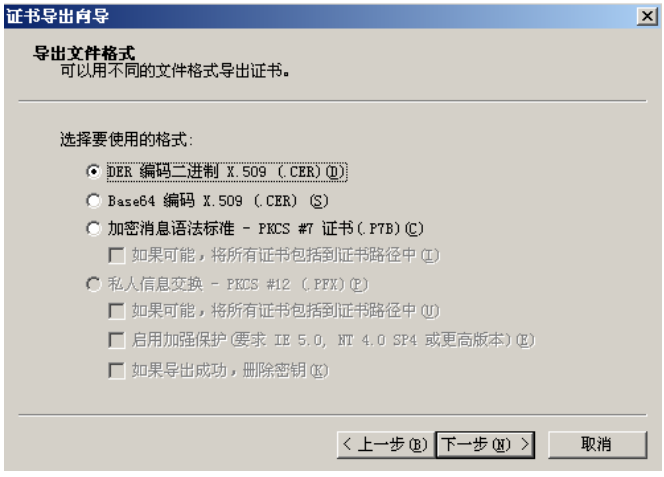

图 1-30 导出文件格式

17．选择默认的文件导出格式，单击“下一步”按钮，指定导出的文件名，如图 1-31 所示。

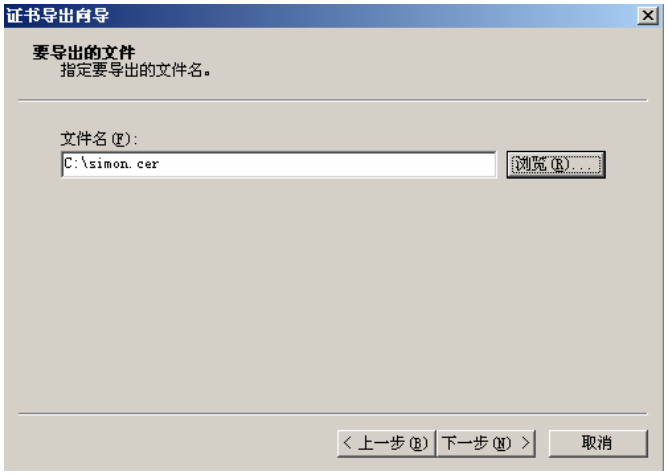

图 1-31 指定导出的文件位置

18．指定文件的导出位置，单击“下一步”按钮，出现如图 1-32 所示对话框。

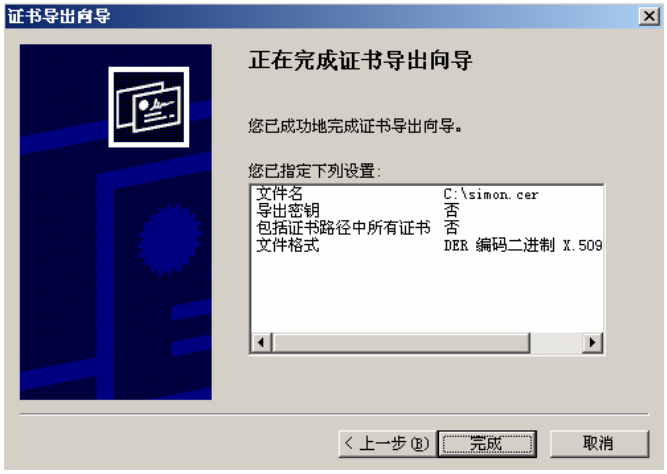

图 1-32 完成证书导出向导

19．单击“完成”按钮，导出证书，出现如图 1-33 所示导出成功对话框。

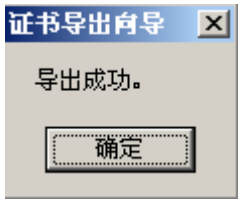

图 1-33 导出成功

20．在用户 steven 的计算机上按照同样的步骤从该 CA 申请用于电子邮件加密的证书，在标识信息处输入用户名称为“steven”，电子邮件地址为“steven@sht.com”。如图 1-34 所示。

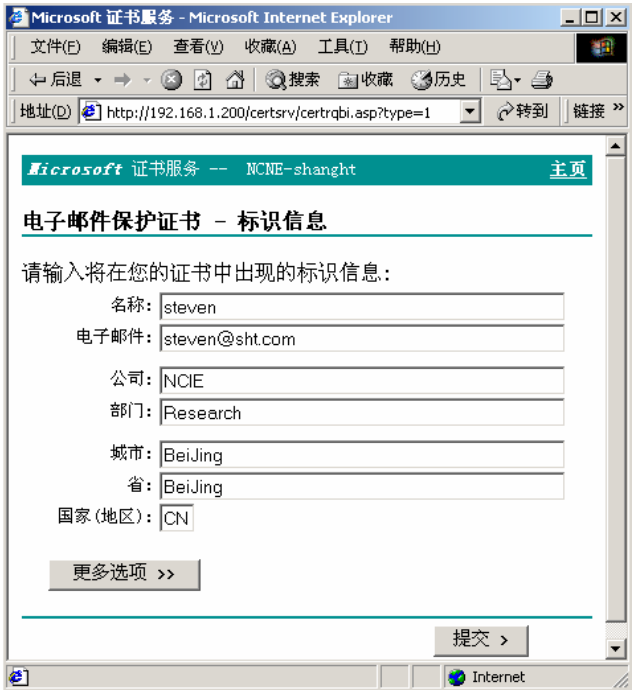

图 1-34 证书标识信息

21．证书申请完成后在 CA 服务器颁发证书，然后在客户端 steven 的计算机上安装证书并把证书导出成文件 steven.cer。

- **在客户端导入对方证书进行邮件加密**

1．要进行邮件加密必须在客户端的邮件工具中导入对方的证书。因此首先把用户 steven 导出的证书 steven.cer 复制到用户 simon 的计算机。

2．在用户 simon 的计算机上打开 Outlook Express，单击“工具”→“选项”，如图 1-35 所示。

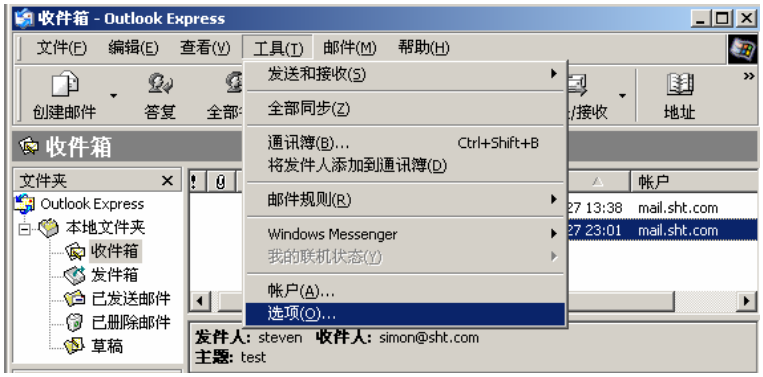

图 1-35 设置 Outlook Express

3．在出现的“选项”对话框中选择“安全”标签，如图 1-36 所示。

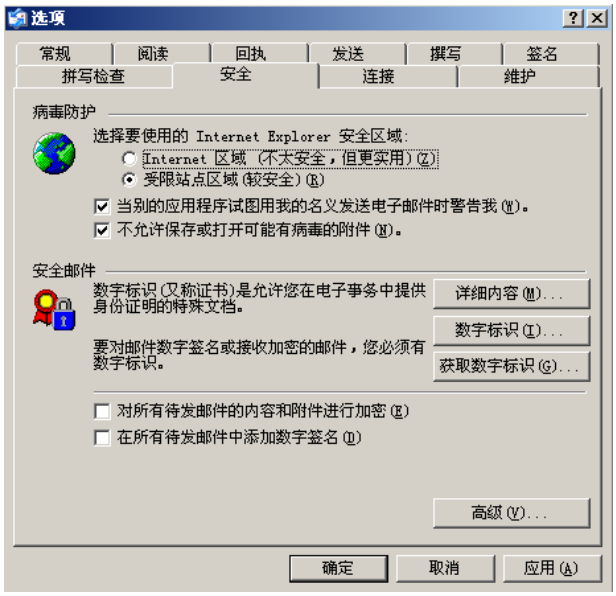

图 1-36 “选项”对话框“安全”标签

4．单击“数字标识”按钮，出现“证书”对话框，如图 1-37 所示。

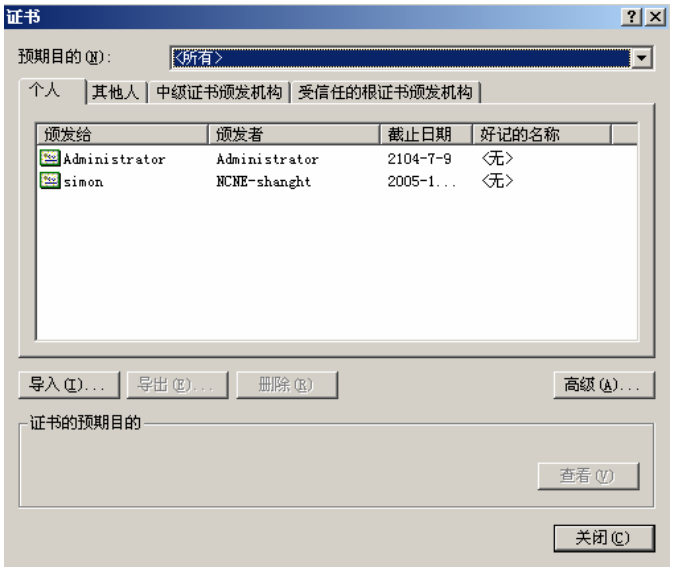

图 1-37 证书对话框

5．单击“导入”按钮，出现“证书导入向导”对话框，如图 1-38 所示。

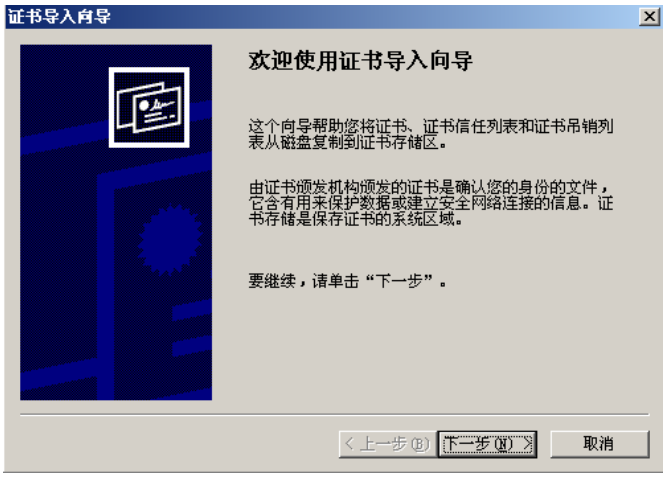

图 1-38 证书导入向导

6．单击“下一步”按钮，指定要导入的文件，如图 1-39 所示。

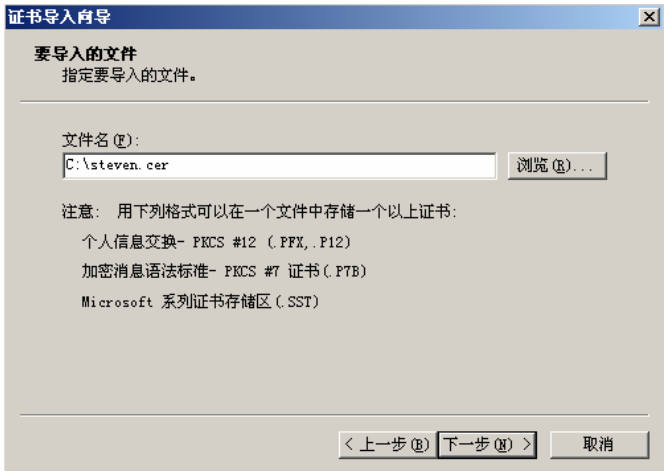

图 1-39 指定要导入的证书文件

7．单击“浏览”按钮指定要导入的证书文件 steven.cer，然后单击“下一步”按钮，出现如图 1-40 所示“证书存储”对话框。

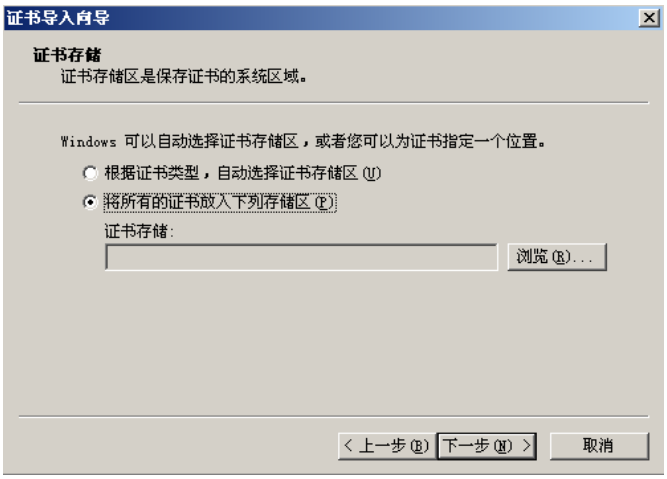

图 1-40 证书存储

8．单击“浏览”按钮出现如图 1-41 所示对话框，在此选择证书存储位置。

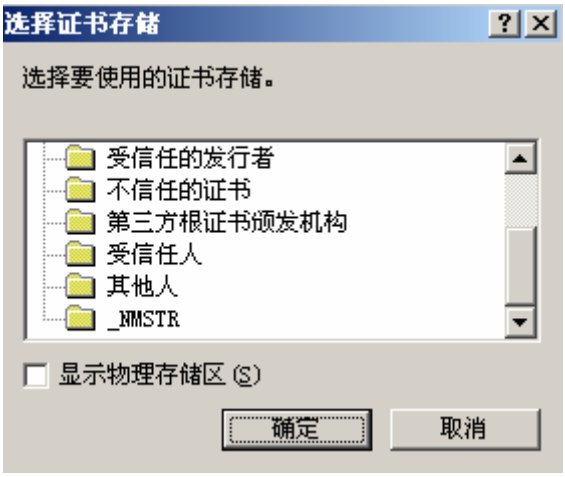

图 1-41 指定导入证书的存储位置

9．选择“其他人”，单击“确定”按钮，出现如图 1-42 所示对话框。

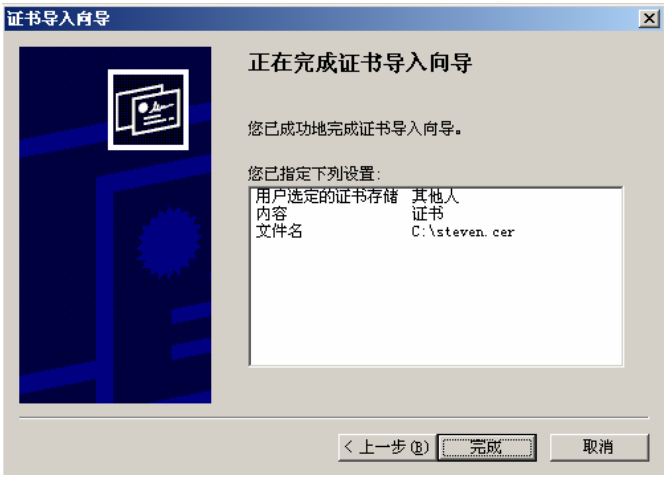

图 1-42 完成证书导入向导

10．单击“完成”按钮，出现如图 1-43 所示对话框，显示证书导入成功。

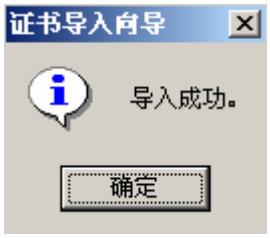

图 1-43 证书导入成功

11．返回“证书”对话框，单击“其他人”标签可以看到刚刚导入的证书。

图 1-44 查看导入的证书

12．如果只希望对用户 simon 发给 steven 的邮件进行加密，那么只在 simon 的计算机上导入 steven 的证书就可以了。如果希望用户 steven 发给 simon 的邮件也进行加密，则要在 steven 的计算机上导入 simon 的证书，过程同上（略）。

- **在 Outlook Express 中对邮件进行加密和签名**

1．在用户 simon 的计算机上打开 Outlook Express，创建新邮件，收件人为 steven@sht.com。在工具栏上单击“加密”按钮，如图 1-45 所示。

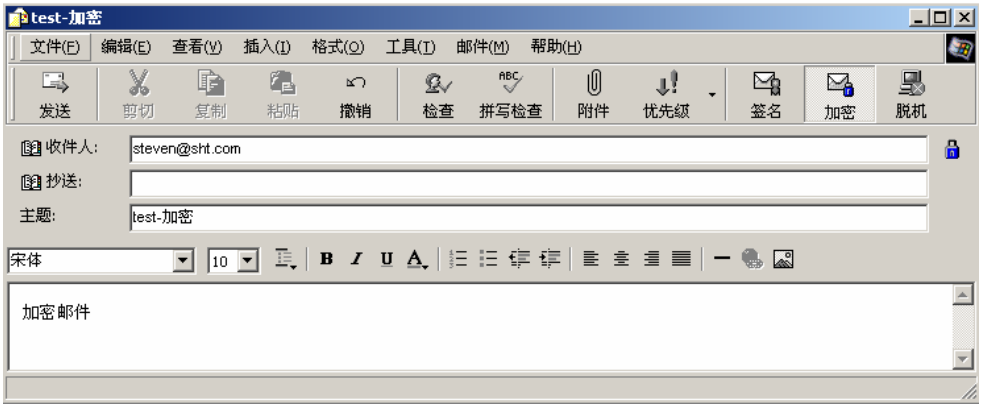

图 1-45 在 Outlook Express 中加密邮件

2．单击“发送”按钮发送该邮件。在用户 steven 的计算机上打开 Outlook Express，单击“发送/按收”按钮接收邮件，可以收到由 simon 发来的邮件。双击该邮件可以看到如图 1-46 所示画面，显示这是一个经过加密的邮件。

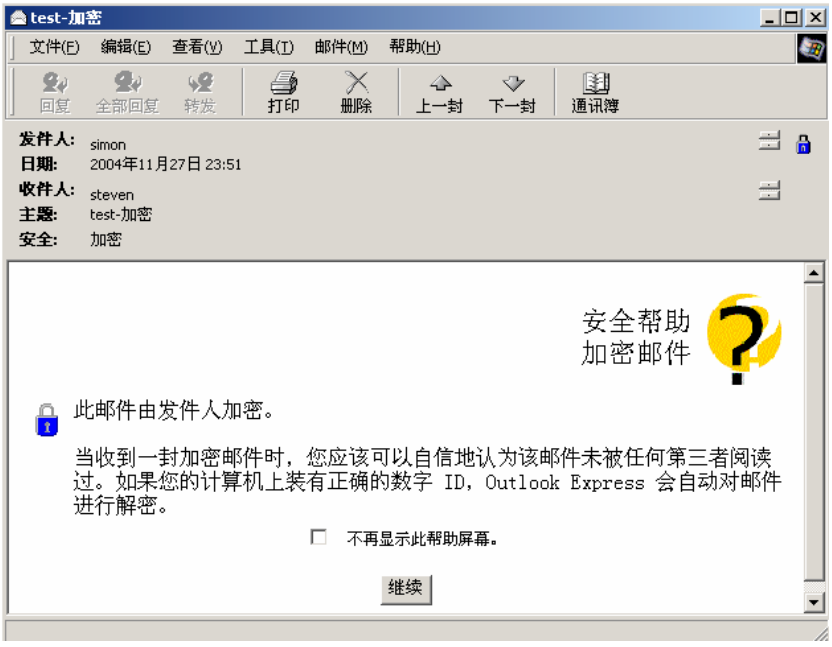

图 1-46 接收到经过加密的邮件

3．单击“继续”按钮可以查看此邮件的内容，如图 1-47 所示。

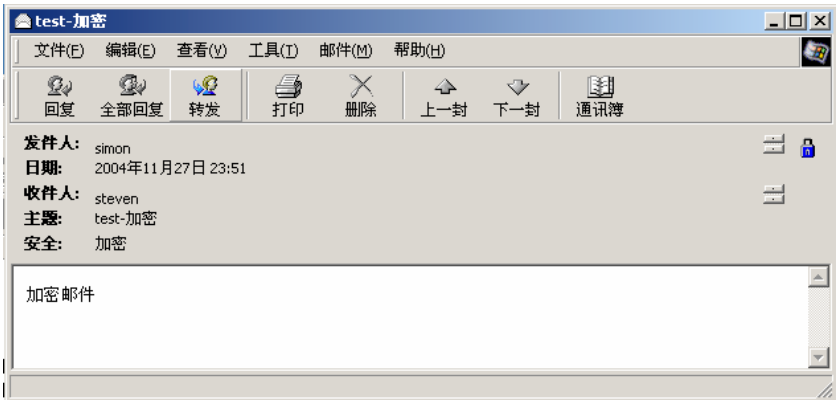

图 1-47 查看加密邮件的内容

4．在用户 simon 的计算机上打开 Outlook Express，创建新邮件，收件人为

steven@sht.com。在工具栏上单击“签名”按钮，如图 1-48 所示。

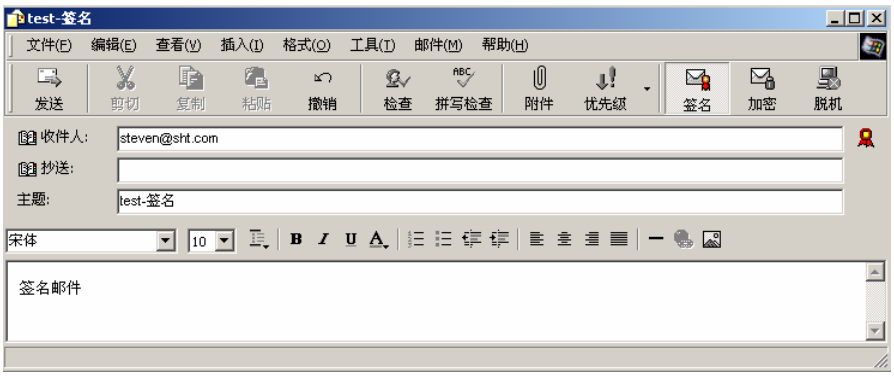

图 1-48 在 Outlook Express 中进行邮件签名

5．单击“发送”按钮发送该邮件。在用户 steven 的计算机上打开 Outlook Express，单击“发送/按收”按钮接收邮件，可以收到由 simon 发来的邮件。双击该邮件可以看到如图 1-49 所示画面，显示这是一个经过签名的邮件。

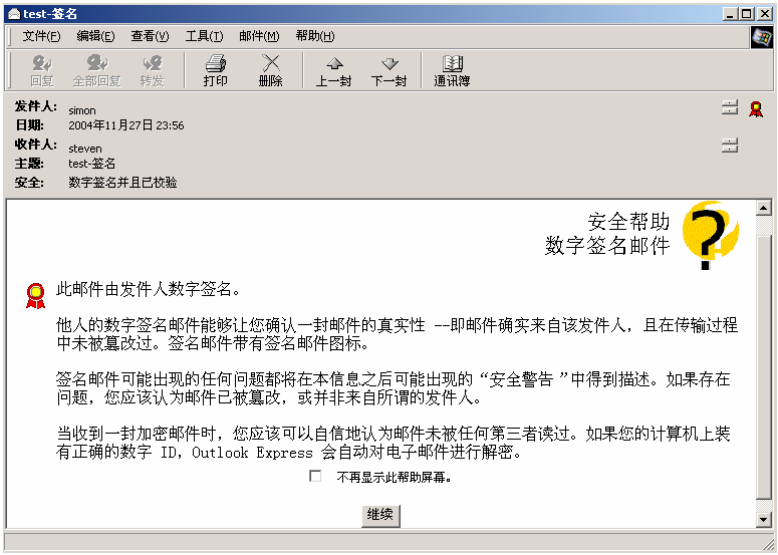

图 1-49 接收到经过签名的邮件

6．单击“继续”按钮可以查看此邮件的内容，如图 1-50 所示。

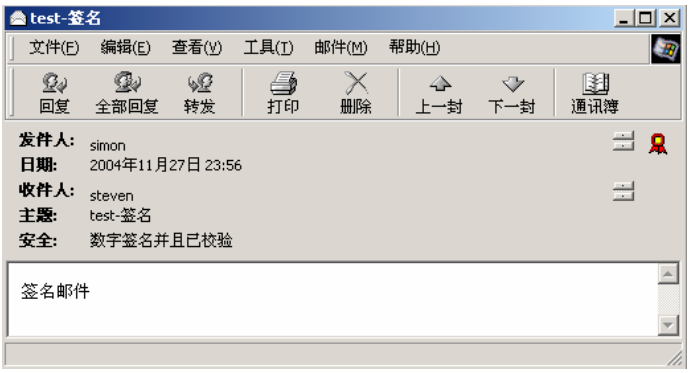

图 1-50 查看经过签名的邮件

以上是利用 Windows 2000 提供的证书实现邮件加密和签名的过程，从而实现了邮件传输的安全性。除了利用证书服务提供邮件加密以外，还可以利用 PGP 实现邮件加密。有关 PGP 加密邮件的过程请读者参阅《每周一讲》的后续内容。