

# 计算机密码学与 PKI 体系

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   | 计算机密码学与PKI体系 .....   | 1  |
| 1.1   | 什么是密码学.....          | 1  |
| 1.2   | 密码学的起源.....          | 1  |
| 1.3   | 什么是加密算法 .....        | 1  |
| 1.4   | 对称加密算法与非对称加密算法 ..... | 2  |
| 1.5   | 什么是RSA算法 .....       | 2  |
| 1.6   | 什么是公开密钥体系 .....      | 3  |
| 1.7   | 什么是SSL.....          | 5  |
| 1.8   | 配置证书颁发机构.....        | 7  |
| 1.8.1 | 安装证书颁发机构 .....       | 7  |
| 1.8.2 | 安装根证书 .....          | 15 |
| 1.8.3 | 显示可用的CSP名称 .....     | 20 |
| 1.9   | 配置SSL加密站点.....       | 25 |
| 附录    | 缩略语及术语 .....         | 42 |

## 图目录

|                              |    |
|------------------------------|----|
| 图 1 密钥交换方法 .....             | 4  |
| 图 2 签名方法 .....               | 4  |
| 图 3 SSL握手 .....              | 6  |
| 图 4 添加或删除程序界面 .....          | 8  |
| 图 5 添加或删除Windows组件向导 .....   | 8  |
| 图 6 选择证书颁发机构类型 .....         | 9  |
| 图 7 公钥/私钥对高级设置 .....         | 10 |
| 图 8 证书颁发机构标识信息 .....         | 11 |
| 图 9 证书数据库设置 .....            | 12 |
| 图 10 选择获取证书授权的主要证书颁发机构 ..... | 13 |
| 图 11 要求停止IIS的执行对话框 .....     | 13 |
| 图 12 证书服务器组件安装 .....         | 14 |
| 图 13 证书授权系统管理工具 .....        | 15 |
| 图 14 证书授权网页 .....            | 16 |
| 图 15 证书颁发机构的证书下载安装窗口 .....   | 16 |
| 图 16 自动安装CA证书链 .....         | 17 |
| 图 17 下载CA证书 .....            | 17 |
| 图 18 证书信息对话框 .....           | 18 |
| 图 19 证书导入向导 .....            | 18 |
| 图 20 下载CA证书链 .....           | 19 |
| 图 21 存储CA证书路径文件 .....        | 19 |
| 图 22 下载证书吊销列表 .....          | 20 |
| 图 23 启动证书模板管理单元 .....        | 21 |
| 图 24 证书模板界面 .....            | 21 |
| 图 25 复制模板 .....              | 22 |
| 图 26 设置模板常规信息 .....          | 22 |
| 图 27 设置处理请求 .....            | 23 |
| 图 28 选择CSP .....             | 23 |
| 图 29 模板复制完成 .....            | 24 |
| 图 30 添加证书模板到证书颁发机构中 .....    | 24 |
| 图 31 选择证书模板 .....            | 25 |
| 图 32 显示所有可用的CSP .....        | 25 |
| 图 33 安装IIS .....             | 26 |
| 图 34 IIS管理界面 .....           | 26 |
| 图 35 ASP禁止界面 .....           | 27 |
| 图 36 ASP启动界面 .....           | 27 |
| 图 37 目录安全性设置 .....           | 28 |

|                              |    |
|------------------------------|----|
| 图 38 目录安全性页面 .....           | 29 |
| 图 39 Web服务器证书向导 .....        | 29 |
| 图 40 选择指定服务器证书的来源方式.....     | 30 |
| 图 41 命名及安全设置 .....           | 31 |
| 图 42 组织信息设置 .....            | 31 |
| 图 43 站点公用名称 .....            | 32 |
| 图 44 地理信息 .....              | 32 |
| 图 45 将证书请求存储成文件 .....        | 33 |
| 图 46 请求文件摘要 .....            | 33 |
| 图 47 由IE获取证书 .....           | 34 |
| 图 48 高级证书申请 .....            | 34 |
| 图 49 提供证书请求文件 .....          | 35 |
| 图 50 证书挂起 .....              | 35 |
| 图 51 用IE获取被挂起的证书.....        | 36 |
| 图 52 检查挂起的证书请求 .....         | 36 |
| 图 53 证书下载 .....              | 37 |
| 图 54 完成服务器证书导入 .....         | 37 |
| 图 55 填写SSL Port.....         | 38 |
| 图 56 安装服务器证书后的服务器属性设置窗口..... | 38 |
| 图 57 设置安全通信页面 .....          | 39 |
| 图 58 无法使用http:访问安全站点 .....   | 40 |
| 图 59 安全提示信息 .....            | 40 |
| 图 60 安全Web站点 .....           | 41 |



# 第一章 计算机密码学与 PKI 体系

“世界上有两种密码：一种是防止你的小妹妹偷看你的文件；另一种是防止当局阅读你的文件资料。”

——摘自 Bruce.Schneier 《应用密码学》

本章讲的是后一种情况，包括如下内容：

- 什么是密码学
- 密码学的起源
- 什么是加密算法
- 对称加密算法与非对称加密算法
- 什么是 RSA 算法
- 什么是公开密钥体系(PKI)
- 什么是 SSL
- 配置证书颁发机构
- 配置 SSL 加密站点

## 1.1 什么是密码学

“如果把一封信锁在保险柜中，把保险柜藏在纽约的某个地方，然后告诉你去看这封信，这并不是安全，而是隐藏。相反，如果把一封信锁在保险柜里，然后把保险柜及其设计规范和许多同样的保险柜给你，以便你和世界上最好的开保险柜的专家能够研究锁的装置，而你还是无法打开保险柜去读这封信，这才是安全的概念。”

——摘自 Bruce.Schneier 《应用密码学》

密码学属于信息安全科学的范畴，它的任务就是保护关键信息和敏感数据的安全。

## 1.2 密码学的起源

最早的密码学应用可追溯到公元前 2000 年古埃及人使用的象形文字。这种文字由复杂的图形组成，其含义只被为数不多的人掌握着。而最早将现代密码学概念运用于实际的人是凯撒大帝（尤利西斯·凯撒公元前 100 年——前 44 年）。他不太相信负责他和他手下将领通讯的传令官，因此他发明了一种简单的加密算法把他的信件加密。

第二次世界大战以后，由于与计算机技术的结合，密码学的理论与实际应用得到了飞速的发展，随之产生了很多新的分支理论，如微粒照片、数字图片水印技术和其他很多隐藏被传递和存储的信息的方法。其中，最常见的就是利用计算机将明文和密码变成密文和将密码和密文变成明文。

## 1.3 什么是加密算法

所谓加密算法就是指将信息变成密文的计算方法。有的加密算法就是对信息进行简单的替换或乱序，这种加密算法最明显的缺陷就是算法本身必须保证是保密的。现代加密算法通常都需要密钥来完成对信

息的加密运算，算法本身可以公开，理论上，只要保证密钥的安全就能保证信息的安全。

最早的凯撒密文就是一种简单的字母替换加密算法。算法本身非常简单，也是最容易被破解的算法。其加密方式就是，按照其在英文字母表里的顺序，将字母循环移位。整个算法可归结为下面的公式：

$$F(x) = (x + s) \bmod 26$$

其中  $x$  是原文字母， $s$  是一个常数。例如，如果  $s$  等于 3，则字母 A 就被加密为 D，而字母 Z 就被加密为 C。这种加密方法虽然简单，但是缺点也是显而易见的。比如，明文中字母 C 出现的次数是 5 次的话，则加密后对应的字母出现的次数也是 5 次，也就是说字母出现的频率没有变化。比如 E 是英文中最常用的字母，那么给定一个足够大的密文，该文中出现最多的字母很可能就是 E，如果不是，那可能是 A、I 或 Q。密码学专家只用十几个密码字母就能很快的进行这种统计攻击。

现代加密算法与这种简单的字母替换算法不同的地方在于，加密算法的安全性基于用于加密的密钥而不是算法本身。对于好的加密算法，即使公开其算法设计原理也不会对其安全性产生丝毫的影响。只要用于加密的密钥是安全的，则被加密的信息也就是安全的。

## 1.4 对称加密算法与非对称加密算法

基于密钥的加密算法可以分为两大类：对称加密算法和非对称加密算法(也叫公钥算法)。所谓的对称加密算法就是用加密数据使用的密钥可以计算出用于解密数据的密钥，反之亦然。绝大多数的对称加密算法加密密钥和解密密钥都是相同的。对称加密算法要求通讯双方在建立安全信道之前，约定好所使用的密钥。对于好的对称加密算法，其安全性完全决定于密钥的安全，算法本身是可以公开的，因此一旦密钥泄漏就等于泄漏了被加密的信息。

所谓非对称加密算法是指用于加密的密钥与用于解密的密钥是不同的，而且从加密的密钥无法推导出解密的密钥。这类算法之所以被称为公钥算法是因为用于加密的密钥是可以广泛公开的，任何人都可以得到加密密钥并用来加密信息，但是只有拥有对应解密密钥的人才能将信息解密。在公开密钥算法体系中，用于加密的密钥被称为公钥，而用于解密的密钥则称为私钥。

## 1.5 什么是 RSA 算法

RSA 算法是当今使用最为广泛的非对称加密算法。这个算法是由 Ron. Rivest, Adi.Shamir 和 Leonard.Adleman 三人于 1977 年共同发明的，算法的名称就来自他们三人名字的首字母。

RSA 算法本身是公开的，所有关于这个算法的原理细节都可以从 RSA 公司的网站上找到。RSA 算法的安全性是基于分解一个由两个大素数（素数是只能被 1 和它本身整除的数）相乘所得到的大数在数学上是非常困难的这一事实。

这两个大素数是随机挑选产生的，用于加密和解密的密钥就是由这两个素数计算产生。这两个素数必须是安全的，因为一旦它们被泄漏则等于泄露了私钥的内容。通常，计算出公钥和私钥后这两个素数都会被销毁，但在某些应用中也可能保留用来加速私钥操作的速度。

在使用 RSA 算法进行加密通讯的过程中，发送信息的一方使用接收方的公钥加密信息，接收的一方收到信息后，用自己的私钥解密信息。发送信息的一方也可以用自己的私钥加密信息，接收方用对应的公钥尝试解密信息以此来确定发送信息方的真实身份。

在 RSA 算法协议中，两个大素数称为  $p$  和  $q$ ，它们相乘的结果称为模数  $n$ 。公式描述如下：

$$n = p q$$

选择一个数  $e$ ，小于  $n$ ，且与  $(p-1)(q-1)$  互为质数，也就是说  $e$  和  $(p-1)(q-1)$  只有唯一的最大公约数 1。目前，业界的做法是取  $e = 3$  或者 65537。

然后就是计算  $d$ ，使得  $(ed-1)$  能被  $(p-1)(q-1)$  整除。公式如下：

$$d * e \equiv 1 \pmod{(p-1)(q-1)}$$

通常所说的 RSA 公钥就是  $(n, e)$  二元组，而私钥就是  $(n, d)$  二元组。而最初选择出来的两个大素数  $p$  和  $q$ ，则可根据应用的需要销毁，或保存下来加速 RSA 运算。

如果要使用 RSA 算法加密一段信息  $m$ ，则首先要将  $m$  分割成长度小于  $n$  的长度的多个数据块。也就是说如果  $p$  和  $q$  是 512 位的素数，则  $n$  就为 1024 位的合数，而每段被加密的信息的位数必须小于 1024。加密的过程就是对信息进行一次模运算，公式如下：

$$C = m^e \text{ MOD } n$$

而解密的过程则为：

$$m = C^d \text{ MOD } n$$

签名与校验签名的过程与加密和解密类似。

## 1.6 什么是公开密钥体系

传统的加密系统是基于对称加密理论的，也就是信息采用单密钥加密，其特点是加密密钥与解密密钥可互相推导，信息的发送者和接收者在建立安全通讯信道之前必须商定一个密钥。对称加密算法的安全性依赖于密钥，泄漏密钥意味着任何人都能对信息进行加密和解密。随着对称加密理论的发展，出现了很多对称加密算法。对称加密算法具有速度快，实现简单等特点，能很好地解决数据的保密传输的问题，但是对称加密算法系统的致命弱点在于密钥的安全性，致使对称加密体系解决不了密钥分配和管理的问题。

1976 年，Whitfield . Diffie 和 Martin . Hellman 首次公开提出了公开密钥理论，奠定了 PKI 体系的基础。PKI 即 Public Key Infrastructure 的缩写，也就是所谓“公开密钥体系”，是一种利用现代密码学的公钥密码技术在公开的网络环境中提供数据加密以及数字签名服务的统一的技术框架。常用的公开密钥算法有 RSA，DSA 和 Diffie . Hellman (DH) 算法等。使用公开密钥算法（有时也叫非对称加密算法）的用户同时拥有匹配的公钥和私钥。私钥由用户保存，且不能泄漏，公钥则要广泛公开的发布。私钥无法通过公钥计算获得。公开密钥理论最大的优势是解决了对称加密系统无法很好解决的密钥交换问题。

公开密钥的算法速度比相同强度的对称算法要慢得多，并且由于任何人都能得到用户的公钥，公开密钥算法对选择明文攻击十分脆弱，因此公钥加密/私钥解密不适用于大量的数据加密传输。为了实现数据的加密传输，公开密钥算法需要与对称加密算法结合使用，即公开密钥算法负责密钥交换，而对称加密算法则负责实际的数据加密。下图显示了一种常用的密钥交换方法：

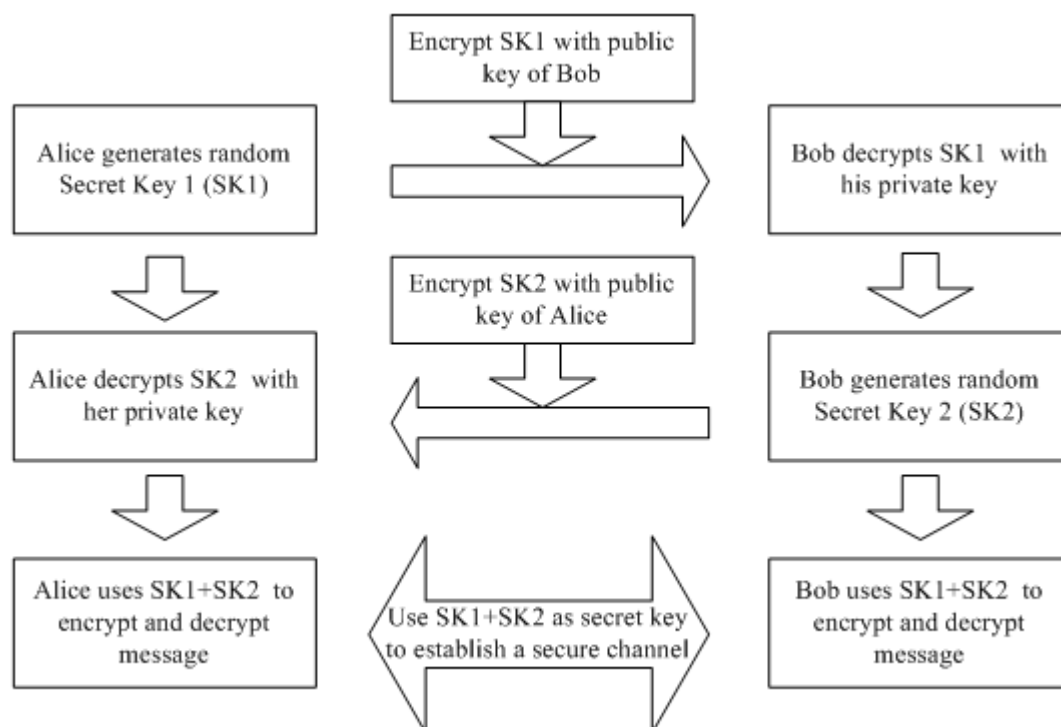


图 1 密钥交换方法

在使用公开密钥算法进行密钥交换的过程中，密钥数据使用公钥加密。在保证用户私钥安全的前提下，攻击者即使截获传输的信息也不能得到用于加密数据的密钥。在整个密钥交换过程中，只要保证用户私钥安全，公钥不被篡改，就能保证通信的安全。

公开密钥体系除了可用于安全密钥交换之外，还可用于鉴别用户身份。下面是一个简单的鉴别用户身份的例子：

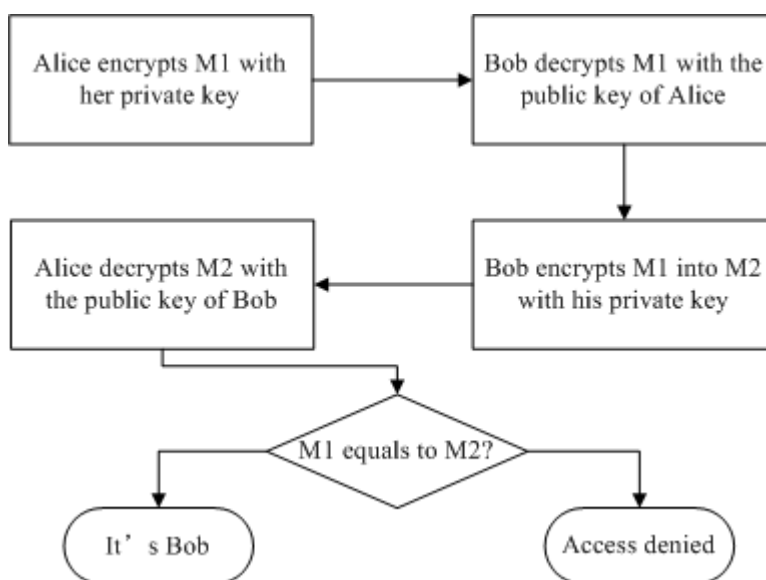


图 2 签名方法

同样原理，公开密钥算法可以进行数据的签名和校验操作，保证数据的一致性和完整性。Alice 将数据和自己对数据的签名一起发送给 Bob，Bob 使用 Alice 的公钥解密得到数据的签名，然后与接收到的数据进行比较，如果一致则证明数据没有被第三者篡改。

因为非对称算法运算速度比较慢，对数据签名一般不采用直接加密数据的方式，而是加密数据的散

列值。数据块的散列值是通过消息摘要算法计算生成。消息摘要算法实际上是一种单向散列函数。数据经过单向散列函数计算得到一个固定长度的值，消息不同得到的散列值也有很大差异。由于是单向函数，用户不可能从散列值推算出原数据，这样就保证了攻击者无法通过散列值伪造数据块。比较消息的散列值与比较消息本身是等价的。常用的消息散列算法有 MD5 和 SHA-1 等。

公钥算法仍然要面临公钥分发，公钥、私钥与用户真实身份绑定的问题。PKI 引入了证书机制解决了这个问题。证书由证书注册中心，也就是常说的 CA 中心统一颁发。

用户获得自己的证书之后，就可以使用证书来表明自己的身份，接收方只要使用 CA 中心的公钥验证用户的证书，如果验证成功，就可以信任该证书的用户身份。证书的颁发和验证充分利用了公开密钥算法的数据签名和验证功能，从原理上杜绝了冒充身份的可能。

## 1.7 什么是 SSL

所谓 SSL 就是安全套接字层，是当今互联网环境中使用最为广泛的密码学应用之一。

Internet 是一个开放的网络环境，开放的网络环境意味着在网络上传输的任何数据都有被截取和监听的可能。当你在一个 WWW 网站提交一些私人信息的时候，这些信息从你的计算机传出，通过 Internet 上的若干节点之后，达到服务器，在这中间的过程中，这些数据是完全暴露的，任何人只要有适当的工具都可以截取这些数据。

正是由于这一安全隐患的存在，Netscape 公司开发了 SSL 来解决这一问题。SSL 是由客户端浏览器创建的一个用来进行信息的安全传输的通讯层。这个安全套接字层位于 TCP/IP 协议簇层和浏览器及 HTTP 等应用层之间的一层，透明的完成信息的加密传输任务。浏览器的 SSL 实现采用了 RSA 公司的公、私钥加密系统和数字证书应用系统。所有当今主流的浏览器都内置了对 SSL 的支持，当用户访问需要 SSL 认证的页面时，浏览器会正确识别和处理相应的请求。SSL 可以有效的防止传输数据被监听和篡改，客户端和服务端可以经过相互验证来建立一条安全的通讯信道。

在 SSL 应用当中，用户敏感信息的安全是依靠高强度的加密算法来保障的。SSL 使用 RSA 加密算法，数字证书系统和数字签名机制来确保数据的安全性。用户的数据通过由 SSL 建立起来的网络连接进行传输时可以保证其机密性、一致性和完整性。由于 RSA 运算速度的问题，在每次 SSL 会话当中，RSA 运算只在服务器端和客户端各进行一次。在这个过程中，服务器和客户机经过一系列的交互建立起一个安全的通讯信道，这个过程称作 SSL 握手。

SSL 的握手过程可分为如下几个步骤：

1. 客户端向服务器端发送客户端的 SSL 版本号，加密算法设置，随机产生的数据和其他服务器需要用于跟客户端通讯的数据。
2. 服务器向客户端发送服务器的 SSL 版本号，加密算法设置，随机产生的数据和其他客户端需要用于跟服务器通讯的数据。另外，服务器还要发送自己的证书，如果客户端正在请求需要认证的信息，那么服务器同时也要请求获得客户端的证书。
3. 客户端用服务器发送的信息验证服务器的身份。如果验证不成功，用户就将得到一个警告，然后加密通讯连接将无法建立。如果成功，则继续下一步。
4. 用户用握手过程至此产生的所有数据，创建连接所用的 Premaster Secret，用服务器的公钥加密（在第二步中传送的服务器证书中得到），传送给服务器。
5. 如果服务器也请求客户端验证，那么客户端将对另外一份不同于上次用于建立加密连接使用的



数据进行签名。在这种情况下，客户端会把这次产生的加密数据和自己的证书同时传送给服务器用来产生 Premaster Secret。

6. 如果服务器也请求客户端验证，服务器将试图验证客户端身份。如果客户端不能获得认证，连接将被中止。如果被成功认证，服务器用自己的私钥加密 Premaster Secret，然后执行一系列操作产生 Master Secret。

7. 服务器和客户端同时产生 Session Key，之后的所有数据传输都用对称密钥算法来交互数据。

8. 客户端向服务器发送信息说明以后的所有信息都将用 Session Key 加密。至此，他会传送一个单独的信息标识客户端的握手部分已经完成。

9. 服务器也向客户端发送信息说明以后的所有信息都将用 Session Key 加密。至此，他会传送一个单独的信息标识服务器端的握手已经完成。

10. SSL 握手至此成功结束，客户机和服务器开始用 Session Key 加密和解密双方交互的所有数据。

下图是一个常见的 SSL 握手过程：

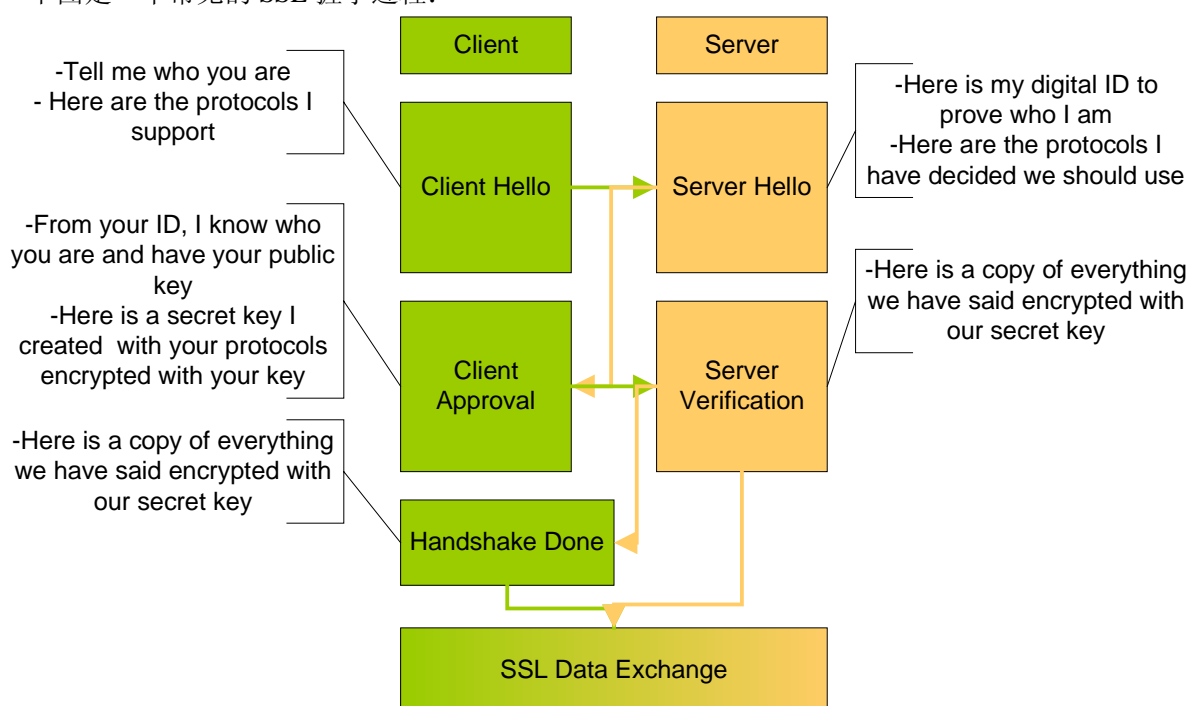


图 3 SSL 握手

在上面使用数字证书进行身份验证的过程中，服务器端的验证与客户端有些差别。客户端使用数字证书验证服务器的过程如下：

1. 从服务器端传送的证书中获得相关信息。
2. 当天的时间是否在证书的合法期限内。
3. 签发证书的机关是否是客户端信任的。
4. 签发证书的公钥是否符合签发者的数字签名。
5. 证书中的服务器域名是否符合服务器自己真正的域名。
6. 服务器被验证成功，客户继续进行握手过程。

服务器端使用数字证书验证客户端的过程如下：

1. 从客户端传送的证书中获得相关信息。
2. 用户的公钥是否符合用户的数字签名。

3. 当天的时间是否在证书的合法期限内。
4. 签发证书的机关是否是服务器信任的。
5. 用户的证书是否被列在服务器的 LDAP 里用户的信息中。
6. 通过验证的用户是否仍然有权限访问请求的服务器资源。

在通过 SSL 应用获得较高的通讯安全性的同时，服务器也需要付出很大的代价。对于一个点击率很高的商业网站来说，如果使用 SSL 保护其站点，会极大的增加服务器的负担。因为服务器需要为每一个请求的用户进行 RSA 运算。解决这一问题的方法就是使用更多的辅助服务器分担客户端访问的处理和使用附加的 RSA 运算加速硬件产品分担服务器 CPU 进行 RSA 运算的负荷。

## 1.8 配置证书颁发机构

证书颁发机构亦即通常所说的 CA 中心，是 PKI 应用的核心。任何 PKI 应用都需要 CA 中心的支持。Windows Server 2003 系统内建了很多对 PKI 应用的支持，通过适当的配置可实现智能卡登录，锁定工作站，VPN 远程登录，SSL 加密站点访问等功能。下面我们将以 Windows Server 2003 自带的证书颁发机构为例，讲解配置证书颁发机构的一般步骤。

### 1.8.1 安装证书颁发机构

Windows Server 2003 的安装程序缺省设置下并不会自动安装证书服务。这是由于安装完证书服务后，Windows Server 2003 计算机就无法再更改计算机名称了。为了提高系统管理灵活性，所以 Windows Server 2003 并未将证书服务安装到用户的 Windows Server 2003 计算机上。所以，当用户要在 Windows Server 2003 计算机上安装证书服务时，用户需要由“添加或删除程序”中的“Windows 组件”，选择安装证书服务。

**注意：如果用户没有安装 IIS，请先安装 IIS。**

若要在 Windows Server 2003 计算机上安装证书颁发机构(CA)，请按照下列的步骤进行操作：

1. 以系统管理员权限的帐号登录 Windows 2003 系统。
2. 请依序打开“开始”菜单→“设置”→“控制面板”选项，以启动 Windows 2003 控制面板。
3. 接着，选择“添加或删除程序”，启动添加或删除程序，如图 4所示：



图 4 添加或删除程序界面

4. 接着，请选择“添加/删除Windows组件”选项，这时候，系统会启动Windows组件向导，让用户选择想安装的Windows Server 2003 操作系统的相关服务或工具的组件，如图 5所示：



图 5 添加或删除 Windows 组件向导

5. 请在 Windows 组件向导的“组件”列表里，选择“证书服务”的选项，以便在 Windows Server 2003 计算机上安装证书服务。当在 Windows Server 2003 计算机上安装了证书服务后，这部 Windows



Server 2003 计算机就会成为证书颁发机构主要的参考计算机，因此，就无法在 Windows Server 2003 计算机上重新为计算机命名了，而且也无法加入其他的域、或者由现存的域中删除。因此，当用户要安装证书服务前，请先确定这部 Windows Server 2003 计算机的稳定性。

6. 当勾选“证书服务”的选项后，请接着按“下一步”按钮。接下来，系统会出现证书授权类型的设置过程。只需要按照需要，选择要安装的证书颁发机构(CA)的类型即可。用户可以选择设置的各种证书颁发机构的类型以及用途，如图 6所示：

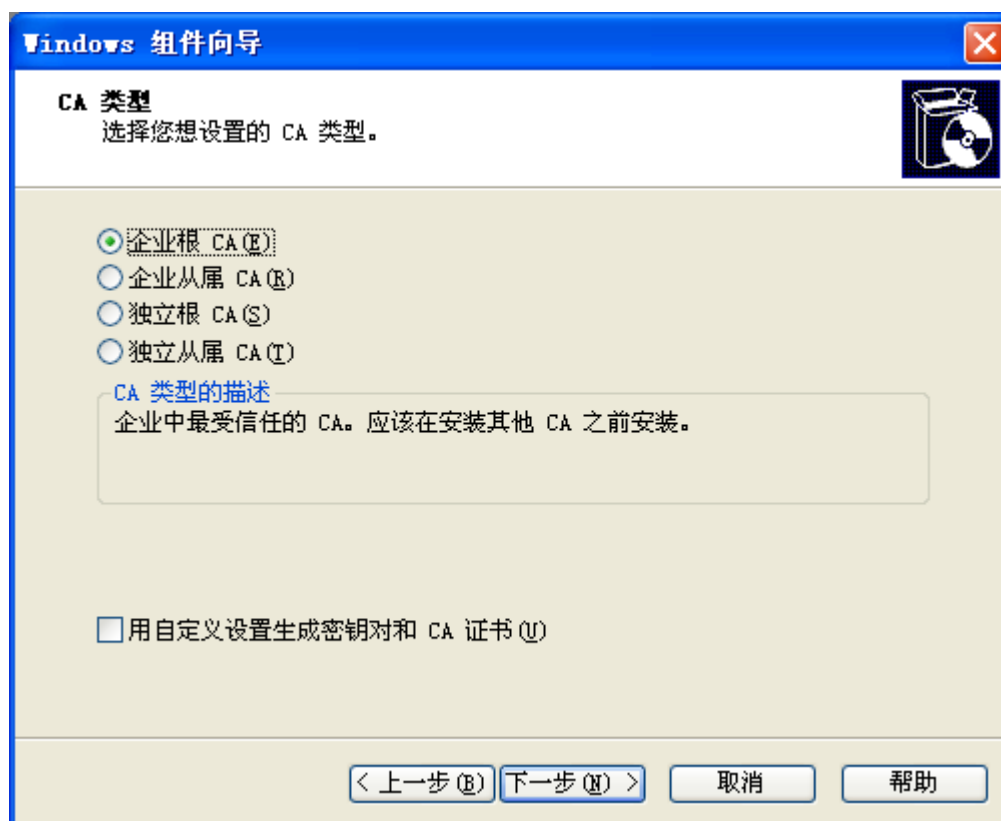


图 6 选择证书颁发机构类型

**企业根 CA(Enterprise Root CA):** 如果所设置的证书颁发机构要将证书发行到企业 Active Directory 域内所有的个体上，用户就必须选择此选项。请注意，此部证书颁发机构将会登记在 Active Directory 域内。如果企业的硬件资源足够时，建议只将企业根 CA(Root CA)使用在发行授权(证书)给企业从属 CA(Subordinate CA)之用，因为这样可以确保较好的安全性。如果企业域内部目前并没有任何的证书颁发机构，也必须选择安装企业根 CA(Root CA)。

**企业从属 CA(Enterprise Subordinate CA):** 如果设置的证书颁发机构要将证书发行到企业 Active Directory 域内的每一个个体上，而且企业域上已经有一台企业根 CA，就可以选择此选项。请注意，此部证书颁发机构将会登记在 Active Directory 域内。

**独立根 CA(Stand-alone root CA):** 如果所安装的这部证书颁发机构将要发行证书给企业域外部的个体使用时，就必须选择这种证书颁发机构方式。选择了这种方式的证书颁发机构，将会成为一个证书颁发机构层次架构的独立根证书颁发机构。

**独立从属 CA (Stand-alone subordinate CA):** 如果要将此部证书颁发机构设置为一个已经设置好的证书层次架构里的一员，就应该选择此选项。证书层次架构组织可以是用户之前所安装的独立证书系统，也可以是存在于企业外部的一个商用性证书颁发机构。

在图 6 中显示选择了企业根证书颁发机构。

在 Windows Server 2003 操作系统的证书服务器上已经采用了默认的加密系统，提供证书的安全机制。若要设置证书颁发机构一些高级设置值(例如证书颁发机构所使用的加密服务提供者(CSP)、数字签名或信息完整性检查所使用的散列算法、证书所使用的密钥长度、所使用的密钥类型等)，可以勾选下方的“用户自定义设置生成密钥对和CA证书”复选框。若勾选了此选项的话，当按下“下一步”按钮时，接下来会出现“公钥/私钥对”的设置窗口，如图 7 所示：



图 7 公钥/私钥对高级设置

此对话框可以让您更改系统默认的加密功能，如使用哪一种加密服务提供者（CSP）、使用哪一种散列算法等等。在上面的对话框里的每一种加密功能的选项（例如加密服务提供者、散列算法等），是根据目前您这部 Windows Server 2003 计算机上所有的软硬件的支持能力所提供的选项出现在上图的设置窗口里。

用户可以在“密钥长度”的选择框里调整数据加密时所使用的密钥长度。一般来说，密钥长度越长，加密出的密文越安全，但是所需要的加密/解密时间越久。如果选择“默认”的密钥长度，系统会根据所选择的加密服务来自动设置所需要的密钥长度。我们建议用户在许可的范围内，尽量选择较长的密钥长度，但是如果密钥长度较长所需要计算加密/解密的时间可能会较长，而且可能有些硬件会无法支持较长的密钥长度（因为有些硬件设计空间或其他因素，限制密钥长度的使用）。如果要使用目前存在系统内的一些密钥建立证书颁发机构，请选择下方的“使用现有密钥”框以及“导入”按钮来设置此证书颁发机构所使用的密钥。

完成上述的设置后，请按“下一步”按钮，继续证书颁发机构的安装设置。

**7.** 接下来，向导会出现“CA识别信息”的设置窗口。用户必须在此窗口里设置此证书颁发机构的标识信息，如图 8 所示：



Windows 组件向导

**CA 识别信息**  
输入识别该 CA 的信息。

此 CA 的公用名称(C):  
TestCA

可分辨名称后缀(D):  
DC= TestCA

可分辨名称的预览(P):  
CN= TestCA, DC= TestCA

有效期限(Y):  
5 年

截止日期:  
2009-4-12 15:27

< 上一步(B) 下一步(N) > 取消 帮助

图 8 证书颁发机构标识信息

在这里请用户要特别注意，在“CA 名称”的字段上，用户务必为此证书颁发机构命名一个名称，因为稍后将会使用此名称来标识建立在证书服务器上的证书颁发机构对象。

如果用户建立的是企业型的证书颁发机构，此名称将会使用来标识建立在 Active Directory 域内的证书颁发机构对象，如果用户建立的是独立证书颁发机构，此名称将会使用在标识此证书颁发机构上。在这里，还需要请读者注意另外一点，如果所设置的是根证书颁发机构(Root CA)，那证书颁发机构的“有效期限”需要比较长的时间，至少都需要比从属证书颁发机构的有效时间长。如果设置的是根证书颁发机构，请将“有效期限”设置在一个合理的时间范围内。当然用户必须考虑到安全以及系统管理的负担，在这两个相对的考虑上获取一个平衡点。当根证书颁发机构过期时，系统管理人员就必须重新刷新一次所有的信任关系。

当完成上述的设置后，请按“下一步”按钮，继续证书颁发机构设置的下一个步骤。

**8.** 接下来，向导会出现“证书数据库设置”窗口，如图 9所示，此窗口主要的目的是要指定证书数据库的储存位置、证书服务器设置信息的储存位置、储存证书撤销列表的位置以及证书数据库记录文件的位置。



图 9 证书数据库设置

如果所设置的证书颁发机构类型为企业型的证书颁发机构，则企业型的证书颁发机构会将它的一些设置信息以及属性信息存储在域里（域控制器上）。

若不是在域控制计算机上设置证书服务器的话，请选择“共享文件夹”选项，并输入一个位于本地上的共享文件夹路径，用来指定证书颁发机构设置信息的存储位置（用户可以指定在共享文件夹里，这样即使未参与域的客户机器，也能够获取证书撤销列表的相关信息）。

当完成上述的设置后，请按“下一步”按钮，继续证书颁发机构设置的下一个步骤。

**9.** 如果安装的是一个从属证书颁发机构，用户将会看到“CA证书申请的设置窗口（如果您安装的不是从属证书颁发机构，请跳到第 10 个步骤继续证书颁发机构的设置过程）。之前，我们曾经提到过，从属证书颁发机构会直接向根证书颁发机构获取证书信息，在这里，就是要设置此从属证书颁发机构要向哪一台 Windows Server 2003 计算机上的根证书颁发机构获取证书颁发机构的证书信息。用户可以选择采用网络直接传输的方式，或者以文件的形式，来获取证书颁发机构的证书信息。若采用网络直接传输的方式，用户只要指定根证书颁发机构的计算机名称、以及证书颁发机构的名称即可。若采用文件形式来获取根证书颁发机构的证书信息，必须指定存储证书信息的文件位置，如图 10 所示：

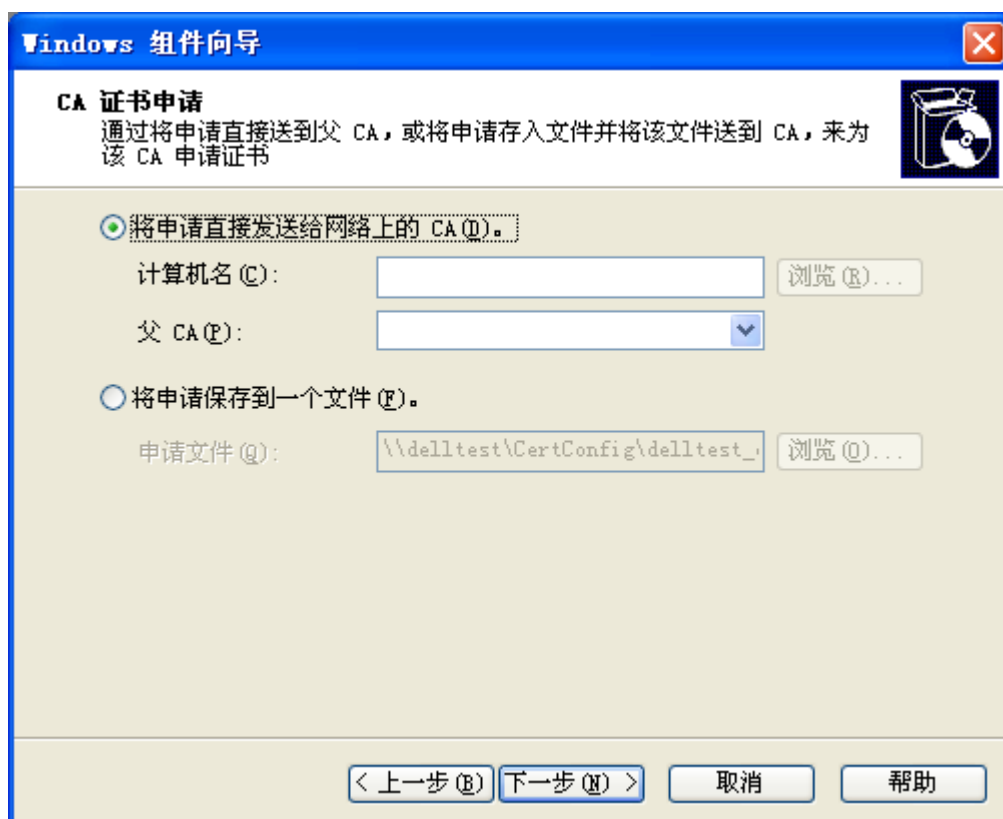


图 10 选择获取证书授权的主要证书颁发机构

用户可以选择“将申请直接发送给网络上的 CA”选项，并按下“浏览”按钮，选择一台可以获取证书授权的根证书颁发机构计算机以及证书颁发机构。如果必须由特定的商用证书颁发机构获取授权证书信息，或者需要获取授权的证书颁发机构无法由网络上获取授权信息时，用户可以选择“将申请保存到一个文件”的选项，并将此文件带到指定的主要证书颁发机构上处理，获取发行证书的授权。

当完成上述的设置后，请按“下一步”按钮，继续下一个证书颁发机构的设置过程。

**10.** 因为Microsoft的证书服务也直接支持其他IIS服务器的运行，因此，如果这时候您的Microsoft Internet 信息服务器IIS(Microsoft Internet Information Server)还在运行阶段，系统会出现提示信息，要求您先停止IIS的运行，以便顺利安装证书服务器，如图 11所示：

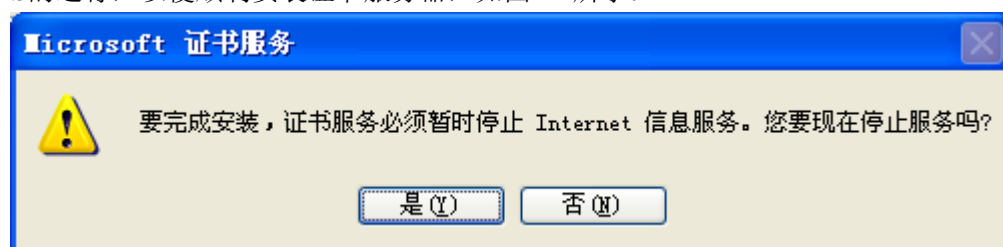


图 11 要求停止 IIS 的执行对话框

**11.** 当点击“是”按钮后，接下来系统便开始安装证书服务器相关的组件以及程序，如图 12所示：



图 12 证书服务器组件安装

**12.** 请注意一下%SystemRoot%\system32\CerSrv\CertEnroll 文件夹是共享的。因为证书服务的客户端计算机需要获取此目录下的信息，以便核对撤销的相关信息。如果此磁盘文件夹没有处于共享状态，可能证书服务客户端计算机无法正常运行。

**13.** 这时候证书服务器已经成功地安装在Windows Server 2003 计算机上了。已经可以由“开始”菜单→“所有程序”→“管理工具”→“证书颁发机构”选项，启动证书颁发机构系统管理工具来管理证书服务器了，如图 13所示：

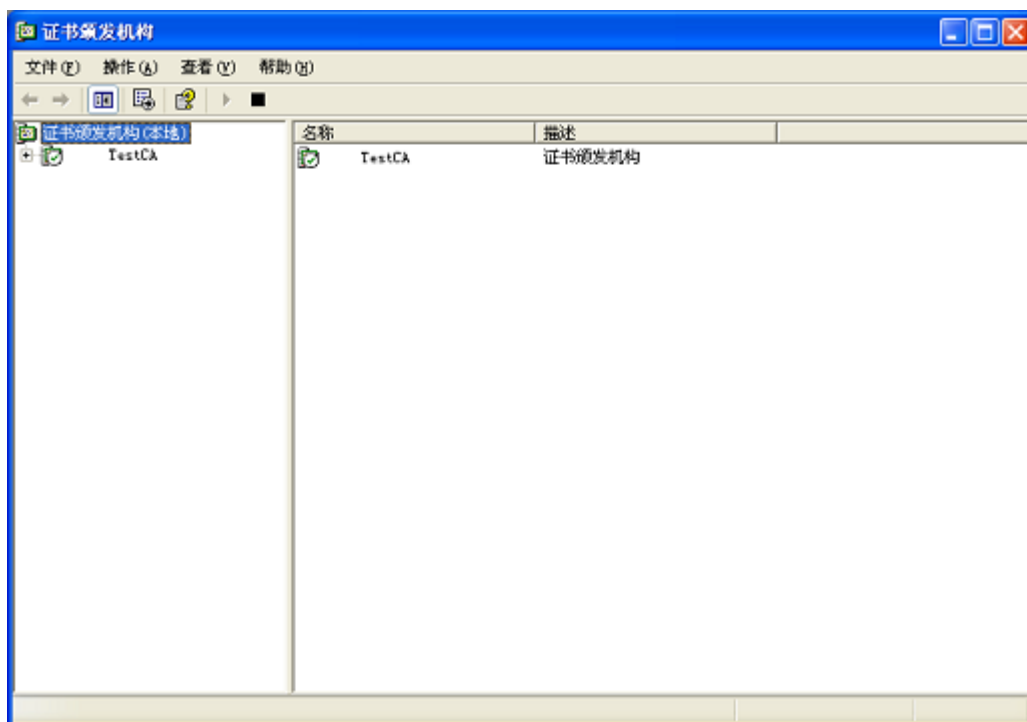


图 13 证书授权系统管理工具

## 1.8.2 安装根证书

若要开始向该证书颁发机构申请证书，必须先安装该证书颁发机构的标识证书，这时候，当向该证书颁发机构要求其他证书信息时，该证书颁发机构就会先检查您有无该根证书颁发机构所发行的许可证书，若有，就会提供给您发行证书的服务。

所以，若企业内部已经具有证书服务器，用户必须先向企业内部的根证书颁发机构获取属于用户帐号的根证书，当获取了根证书后，系统才会启动由该证书颁发机构所发行出来的所有证书（启动这些证书的有效性）。下面我们以简单的操作步骤来说明如何从证书颁发机构获取信息，来安装根证书。

首先，在企业内部域上安装证书服务器。关于证书服务器的安装方式，请参考上一小节的说明。

**1.** 启动Internet Explorer，并连接上企业内部的证书服务器。（例如<http://企业提供根证书颁发机构的Windows Server 2003 计算机的DNS名称/certsrv>，例如假设在delltest这部Windows Server 2003 计算机上安装根证书颁发机构时，用户就可以用 <http://delltest/certsrv> 网址）。接下来，就可以直接进入到证书颁发机构的证书发行网页，如图 14所示：





图 14 证书授权网页

2. 因为现在需要先获取此部证书颁发机构的根证书，因此，请选择“下载一个 CA 证书，证书链或 CRL”的选项。

3. 系统会呈现此证书颁发机构的安装证书或下载证书的选项网页，如图 15所示：

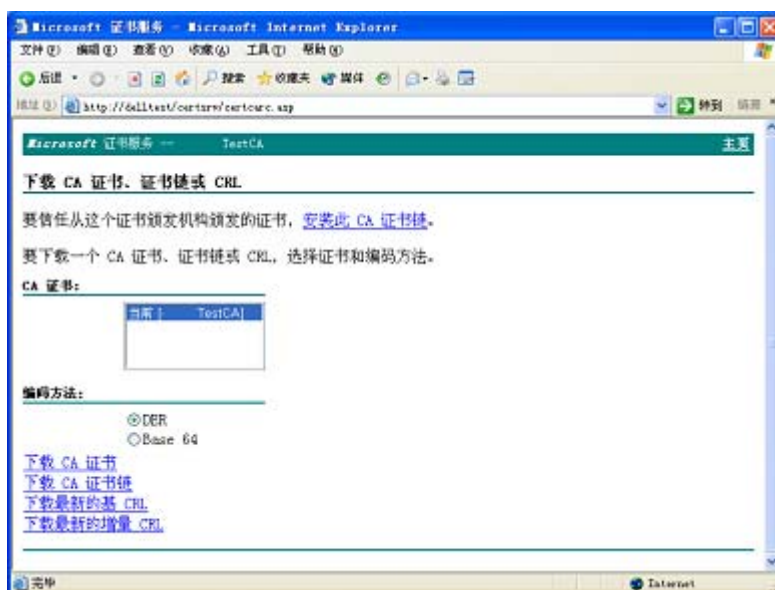


图 15 证书颁发机构的证书下载安装窗口

用户可以直接选择“安装此CA证书链”的链接，当按下此链接后，系统会自动将该证书颁发机构的证书链(证书信任关系)安装到您的Windows Server 2003 计算机上，这时候，用户的计算机就可以使用该证书颁发机构所发行的证书来完成身份验证或其他安全性的处理，如图 16所示：



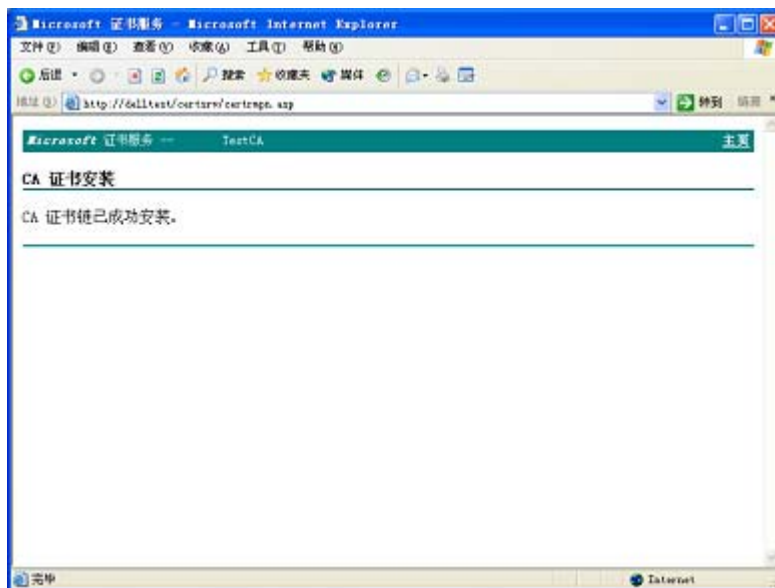


图 16 自动安装 CA 证书链

除了选择上述的“安装此 CA 证书链”的链接方法以外，用户还可以选择下方的“下载 CA 证书”的链接，以手动的方式直接获取证书颁发机构所发出的证书信息。可以采用 DER 编码的方式、或者以 Base 64 编码的方式，让证书颁发机构以这两种数据编码的方式将该证书颁发机构的证书信息打包成证书导出文件的形式，用户直接通过 Internet Explorer 下载该证书颁发机构的代表证书或者相关的数据（包含下载证书路径（也就是证书授权信任的关系）、以及证书吊销列表）。

4. 选择编码形式后，直接按下“下载CA证书”的链接，这时候系统就会以用户所选择的证书编码形式，将该CA的代表证书下载到用户所使用的计算机上，如图 17所示：

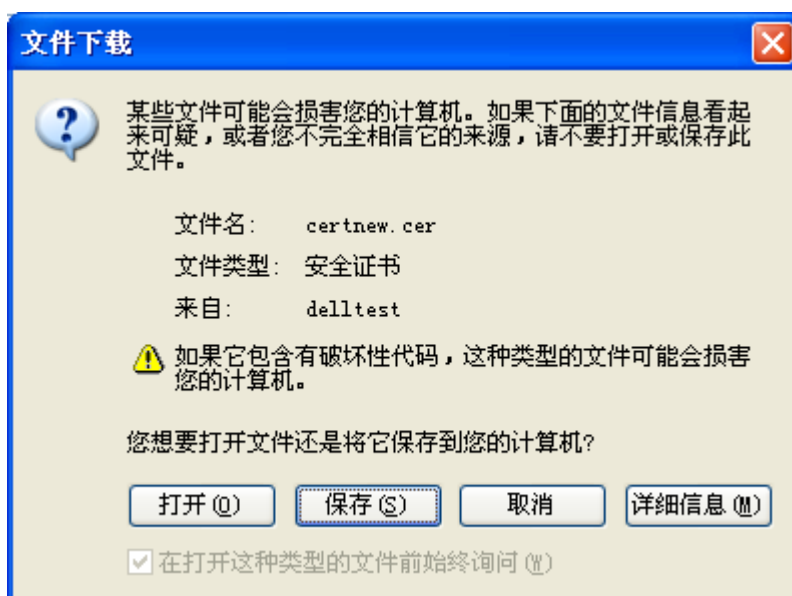


图 17 下载 CA 证书

5. 若要查看此证书，可以选择“打开”按钮。这时候，系统便会立即打开这个certnew.cer（也就是该证书颁发机构发行给用户的证书导出文件），如图 18所示：

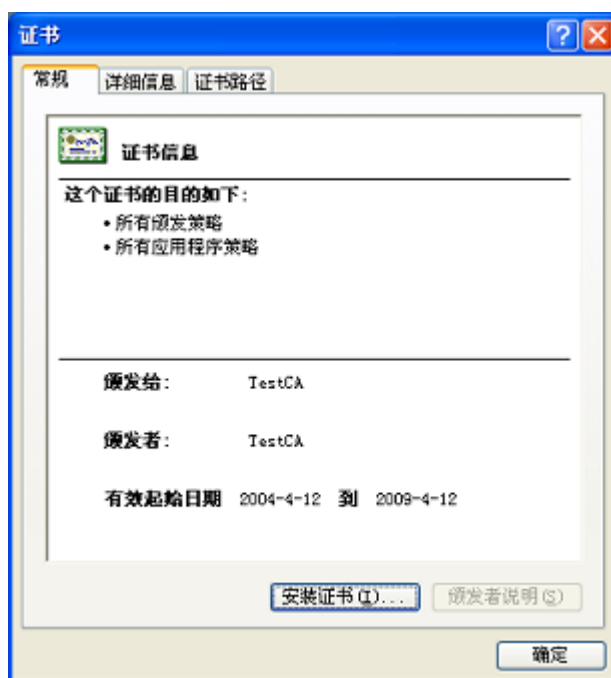


图 18 证书信息对话框

6. 用户可以查看此证书的相关信息，若确定无误后，可以按下“常规”页面下方的“安装证书”按钮，以便将此证书安装到用户的作业环境上。当按下“安装证书”按钮后，系统会启动证书导入向导。因为当使用 Internet Explorer 从证书颁发机构下载该 CA 的代表证书时，该 CA 是以用户所选择的证书导出的文件格式(DER 编码或者 Base 64 编码)来打包此证书信息的，因此，必须通过 Windows 操作系统的证书导入向导，才能将该证书信息顺利安装到您的系统环境上。

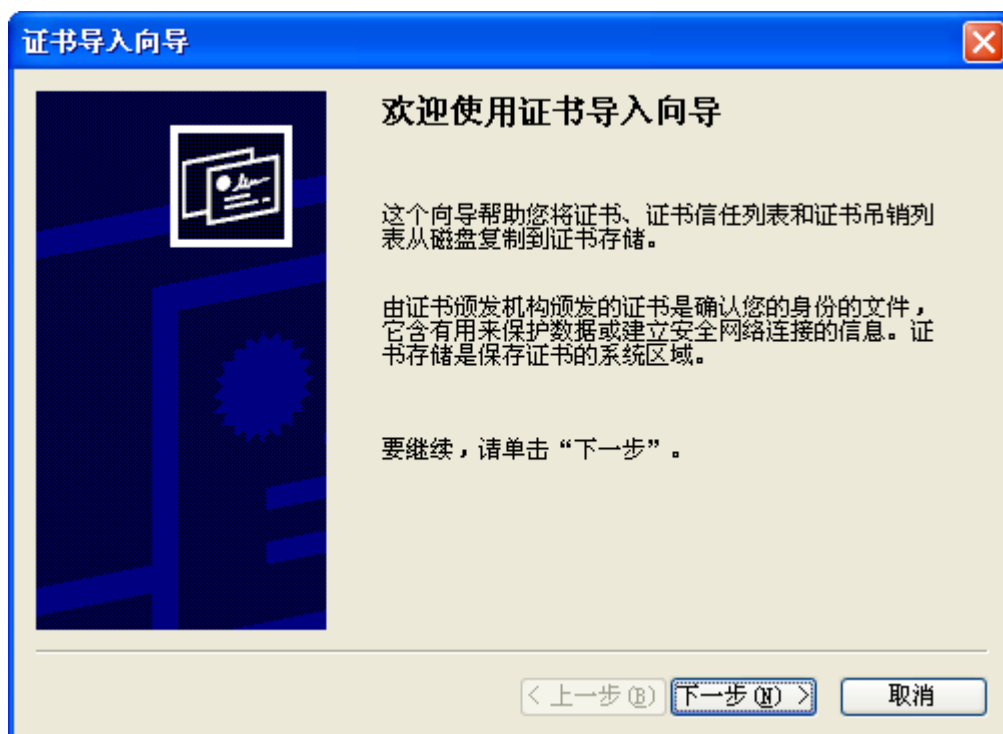


图 19 证书导入向导

用户只需要按照证书导入向导的提示步骤，依序进行操作，即可将证书顺利安装到用户计算机的运

行环境上。

以上是下载 CA 代表证书的操作方式。也可以采用同样的方法来下载 CA 证书链导出文件或者该 CA 的基证书吊销列表和增量证书吊销列表的导出文件。若要下载 CA 证书链，只需要按下“下载 CA 证书链”的链接即可。

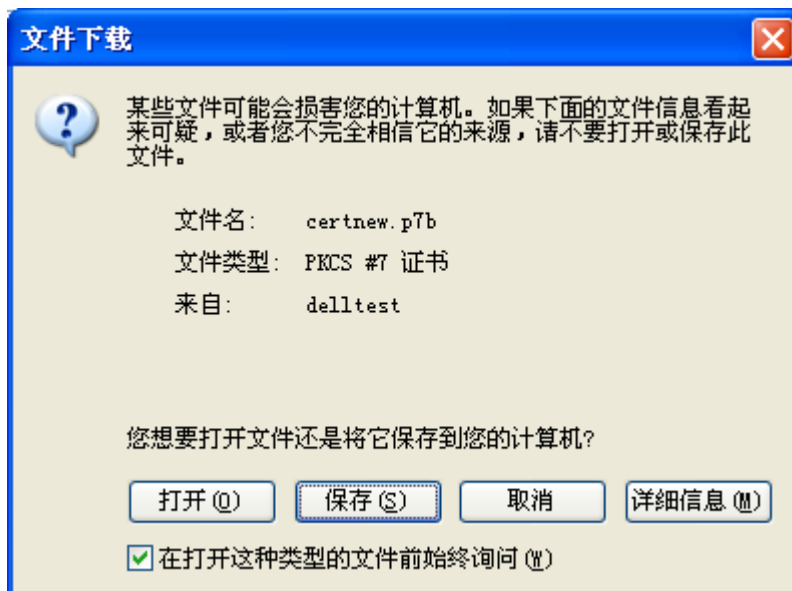


图 20 下载 CA 证书链

当按下“下载CA证书链”的链接后，系统会接着出现如图 20的文件下载窗口。用户可以选择将此文件先存储在您的磁盘驱动器内，如图 21所示：

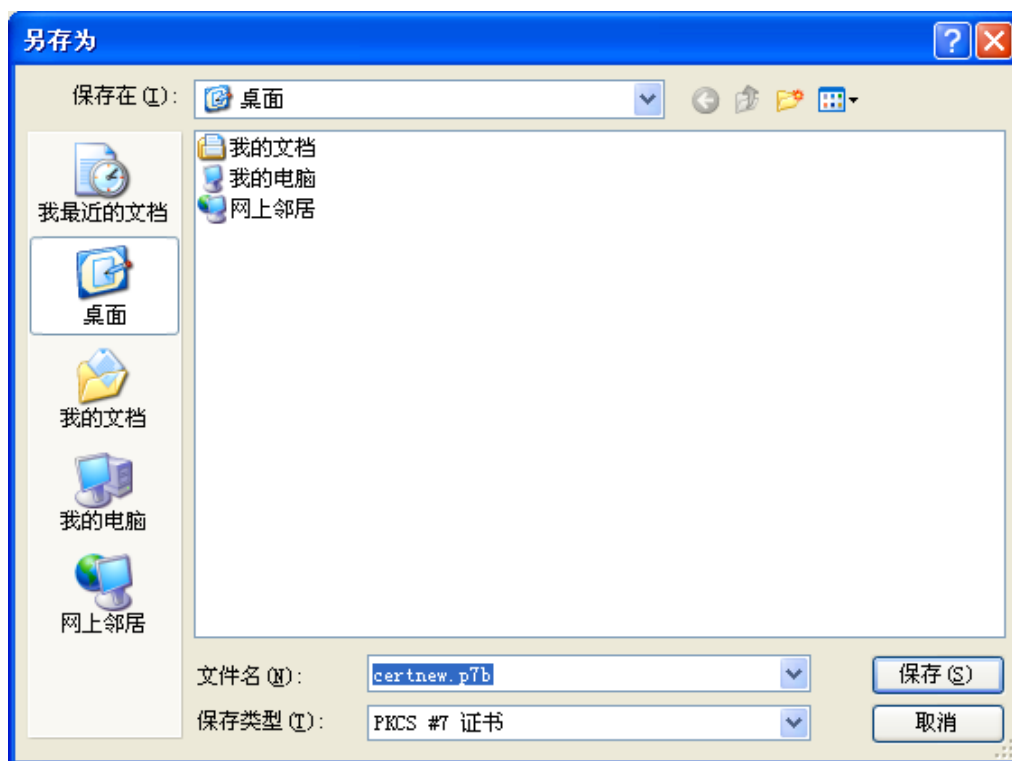


图 21 存储 CA 证书路径文件

当下载完成后，可以以手动的方式启动证书导入向导，将CA证书链的相关信息导入到您的系统里。

也可以采用同样的方式来下载该证书颁发机构的最新基证书吊销列表或增量证书吊销列表，用户只需要按下“下载最新的基CRL”或“下载最新的增量CRL”链接，即可打开文件下载列表，如图 22所示：

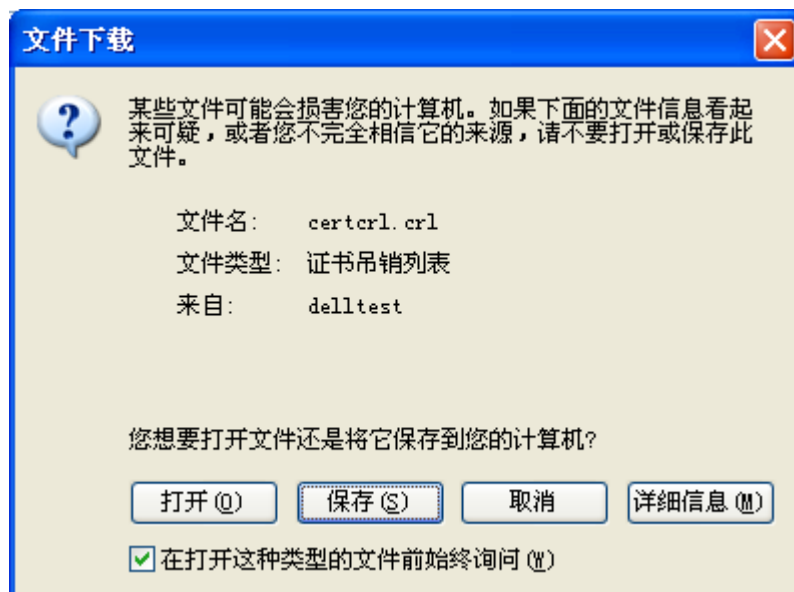


图 22 下载证书吊销列表

同样的，若要使用此证书吊销列表的话，可以在下载的文件上按下鼠标右键，并选择“安装 CRL”的选项。这时候，系统会启动证书导入向导，用户只需要按照向导的提示操作步骤，依序进行设置即可。

### 1.8.3 显示可用的 CSP 名称

证书颁发机构中会提供一些基本的证书模板，但是这些模板的信息不能修改，并且不能在申请证书的页面上显示使用计算机上可用的 CSP 名称。如果想显示所有可用的 CSP，你需要从证书模板库中添加完成 CSP 设置的证书模板。

证书模板库中原有证书模板的 CSP 信息是不能修改的，要修改 CSP 的设置必须复制一个模板，然后再进行修改。现在就介绍如何设置证书模板以显示可用的 CSP：

1. 由“开始”菜单→“程序”→“管理工具”→“证书颁发机构”选项，启动证书颁发机构系统管理工具。展开要操作的CA，在左侧列表中选择“证书模板”项。如图 23所示：

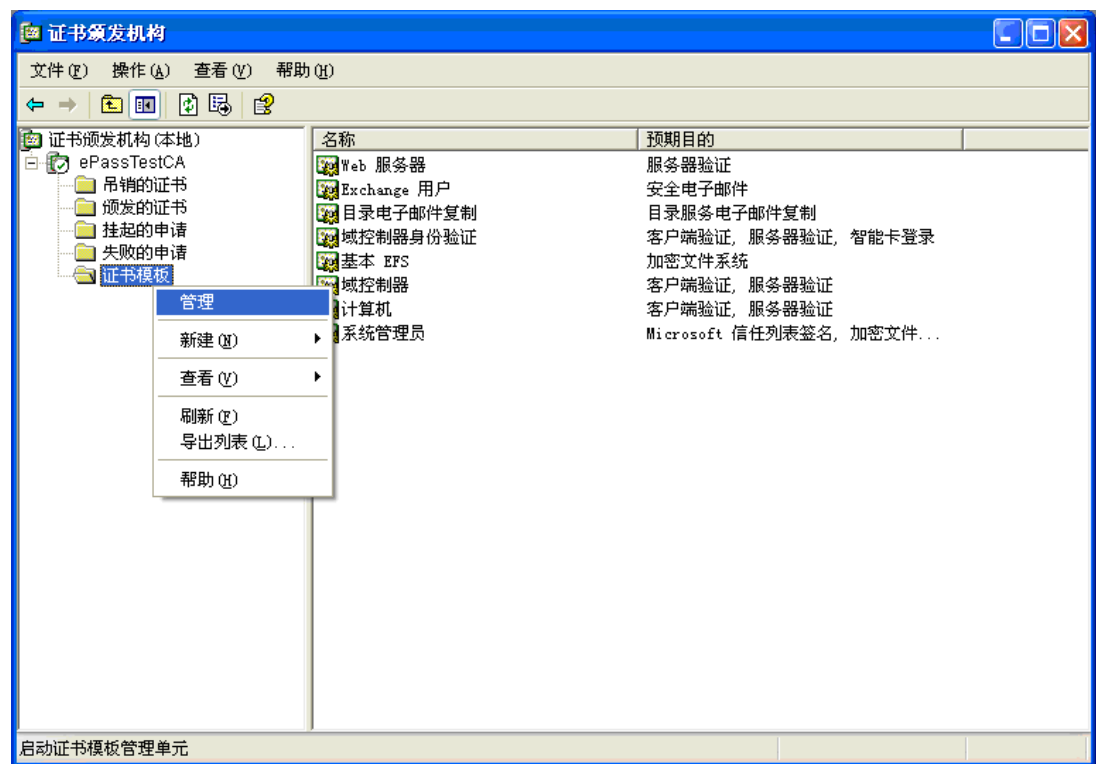


图 23 启动证书模板管理单元

2. 单击鼠标右键，在弹出的列表中单击“管理”项，即可打开证书模板窗口。如图 24所示：

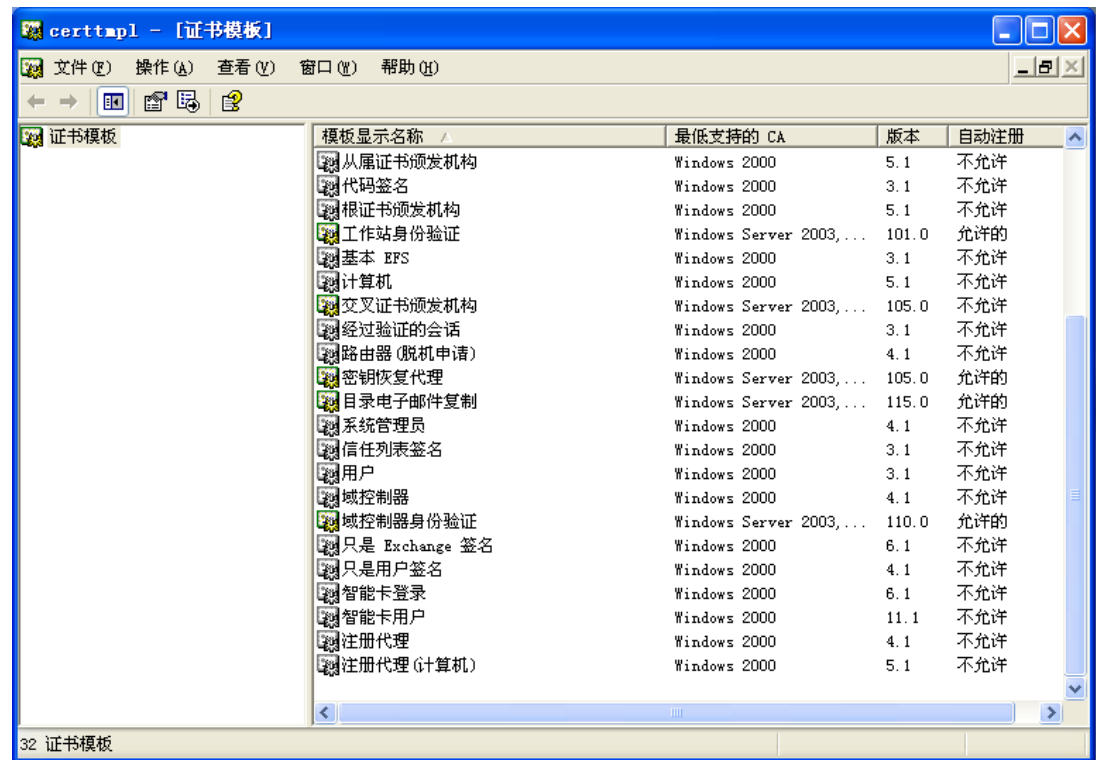


图 24 证书模板界面

3. 证书模板窗体的右侧显示了所有的模板类型，你可以根据自己的需求选择相应的证书模板类型。选中证书类型后，单击鼠标右键，在弹出的列表中选择“复制模板”。如图 25所示：

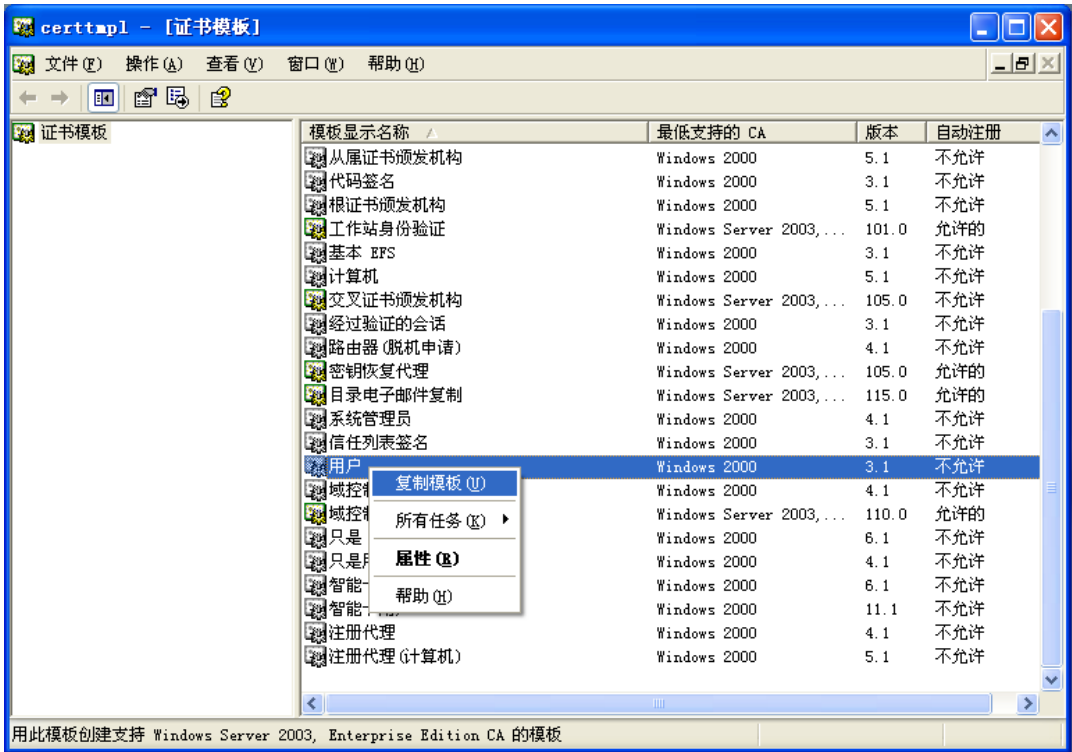


图 25 复制模板

4. 在“新模板的属性”窗口中，选择“常规”选项卡，设置“模板显示名称”、“有效期”以及“续订期”，也可以默认为缺省。但是复制完成后，新模板的“模板显示名称”将不能修改。如图 26所示：

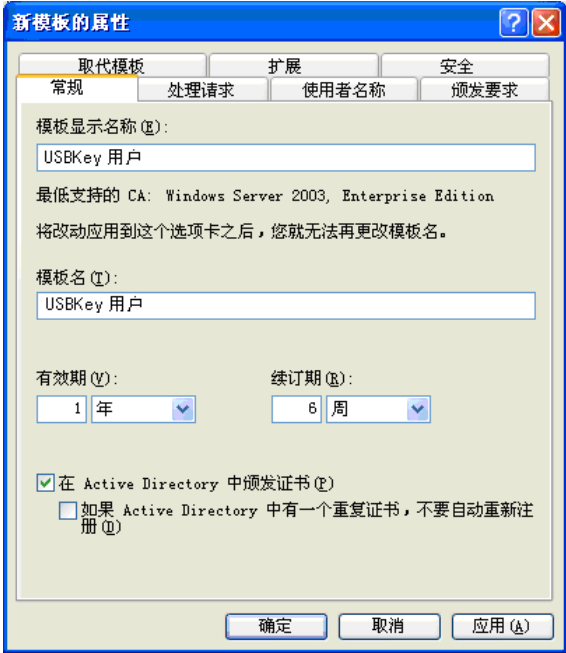


图 26 设置模板常规信息

5. 要显示所有可用的CSP名称，需要进入“处理请求”选项界面对CSP进行修改。在界面中点击“CSP(C)...”按钮，如图 27所示：

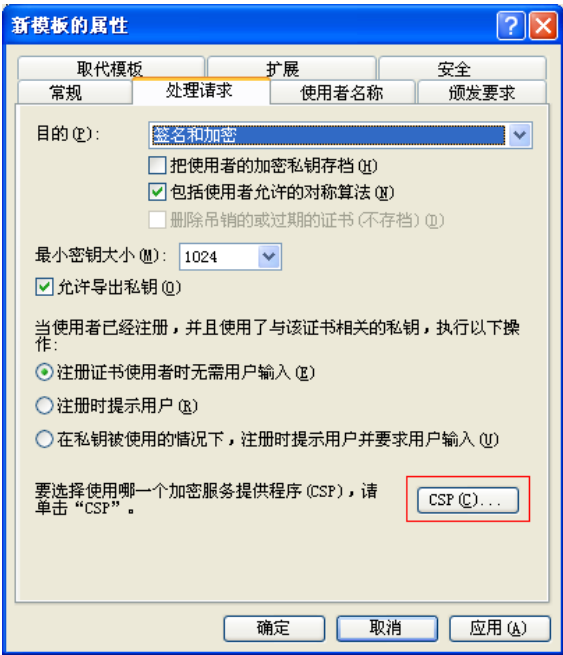


图 27 设置处理请求

6. 因为要显示使用者计算机上所有可用的CSP，所以在弹出的“CSP选择”对话框中请选择第一项“请求可以使用证书使用者计算机上任何可用的CSP”，然后点击“确定”按钮。如图 28所示：

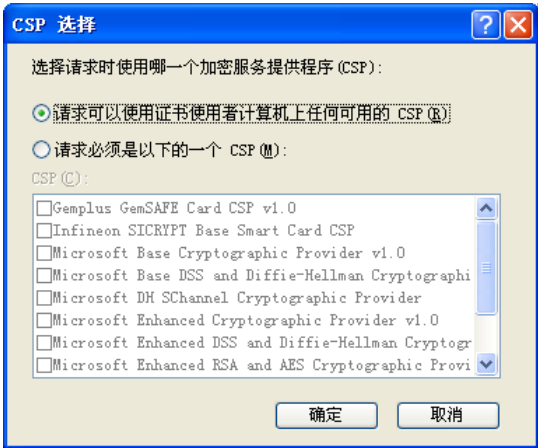


图 28 选择 CSP

7. 返回模板属性界面后，单击“确定”按钮完成模板的复制操作，可以对新复制的模板进行查看和编辑。如图 29所示：

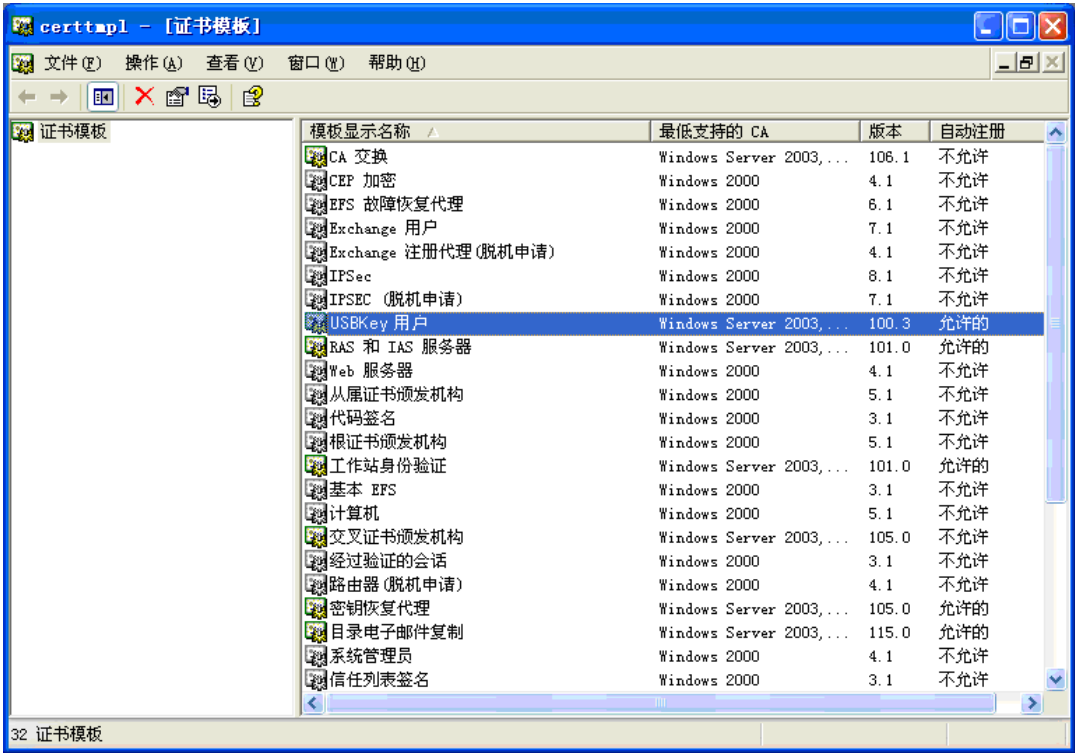


图 29 模板复制完成

8. 根据要求设置完成证书模板后，需要把生成的模板添加到“证书颁发机构”中，以实现所修改的设置。返回“证书颁发机构”，选择“证书模板”，然后单击鼠标右键，在弹出的对话框中选择“新建”→“要颁发的证书模板”。如图 30所示：

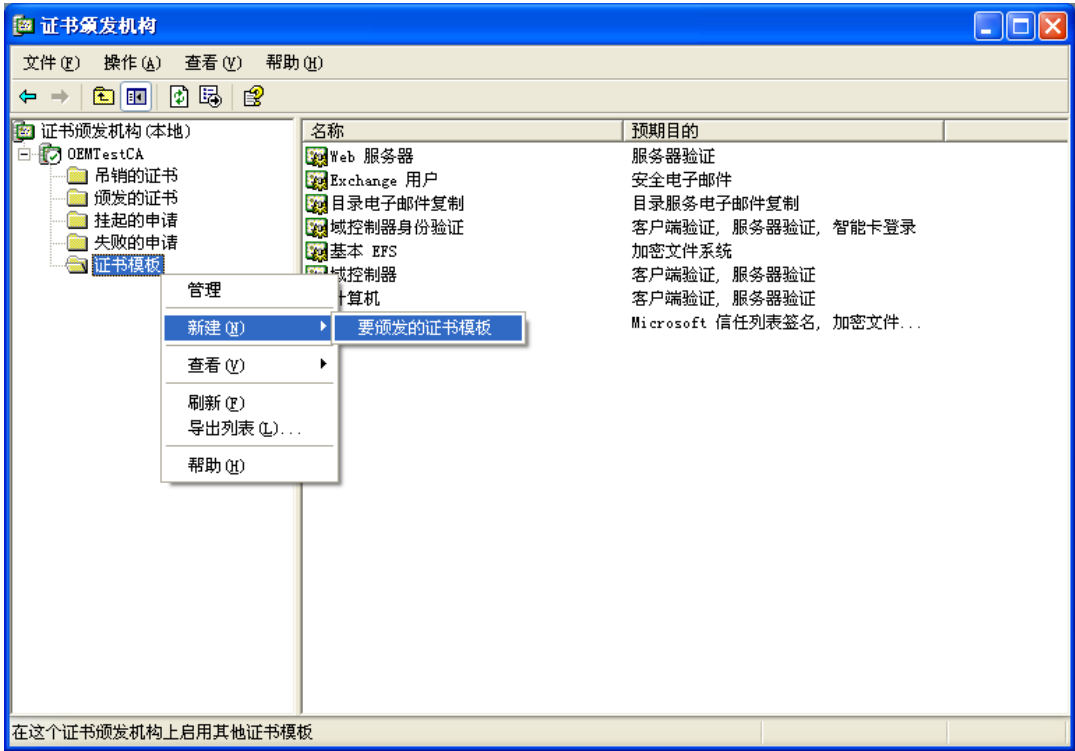


图 30 添加证书模板到证书颁发机构中

9. 此时会弹出“启用证书模板”对话框，会列出所有可供使用的证书模板，如图 31所示：



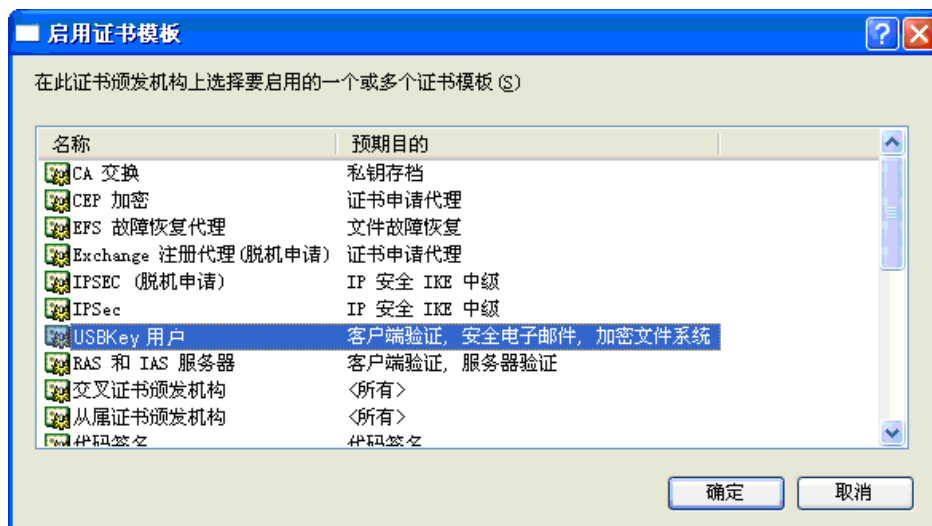


图 31 选择证书模板

**10.** 在列出的证书模板列表中选择刚复制的证书模板，点击“确定”按钮，即可把所选择的证书模板添加到证书颁发机构的证书模板列表中。

添加完成后，打开Internet Explorer浏览器，连接证书服务器（这里以上面刚刚搭建的CA为例）申请证书，如图 32所示：

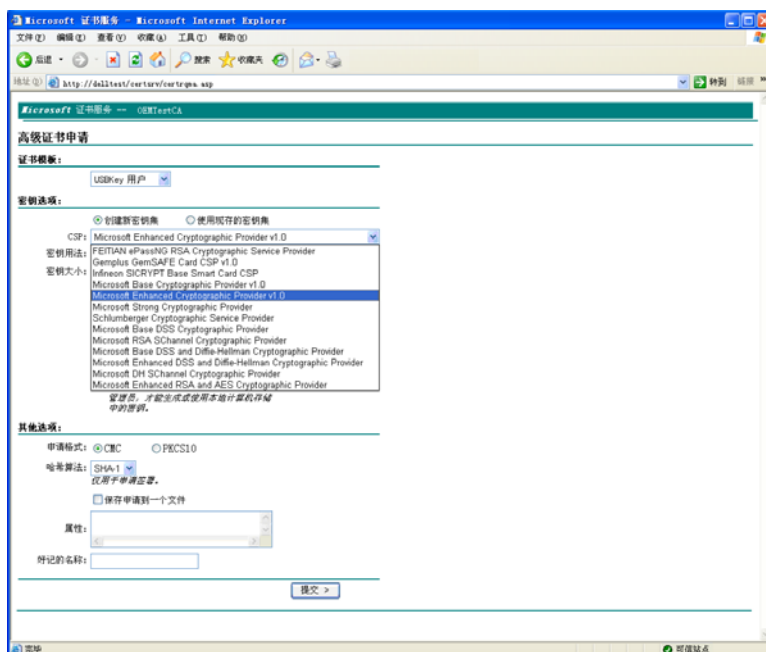


图 32 显示所有可用的 CSP

选择添加的证书模板时，CSP 的下拉列表中即可显示出所有可用的 CSP。

## 1.9 配置 SSL 加密站点

IIS是Microsoft Internet信息服务的简称(Microsoft Internet Information Service)。IIS为Windows Server 2003 操作系统的一个服务之一，IIS主要提供了WWW、FTP、Gopher、以及其他国际互联网上的重要服务的主要服务器的功能。一般来说，在安装Windows Server 2003 操作系统时，Windows Server 2003

操作系统的安装程序默认不会将IIS的相关组件安装到计算机上。不过也可以在安装Windows Server 2003操作系统时，将IIS的组件安装的过程加上。假设目前还未安装IIS组件，用户可以由“配置服务器向导”进行安装，如图 33所示：

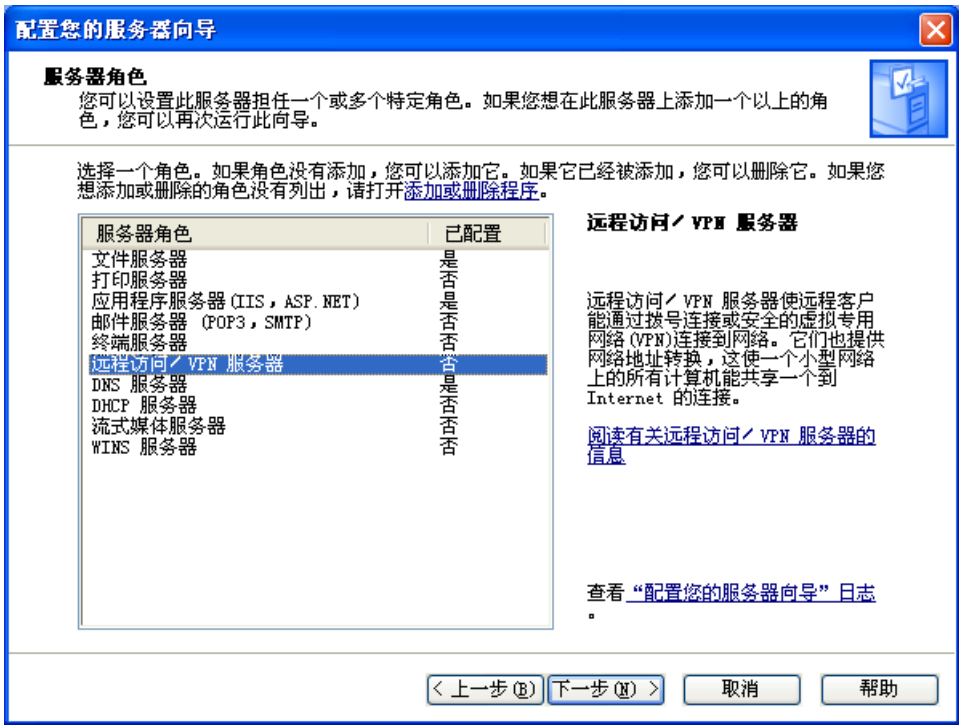


图 33 安装 IIS

假设用户已经在Windows Server 2003 计算机上安装了IIS，而且目前IIS已经开始启动运行了。用户可以由“控制面板”→“管理工具”→“Internet服务管理器”选项来启动IIS服务管理工具，如图 34所示：



图 34 IIS 管理界面

因为Windows Server 2003 上默认是asp服务是没有启动的，如图 35所示：

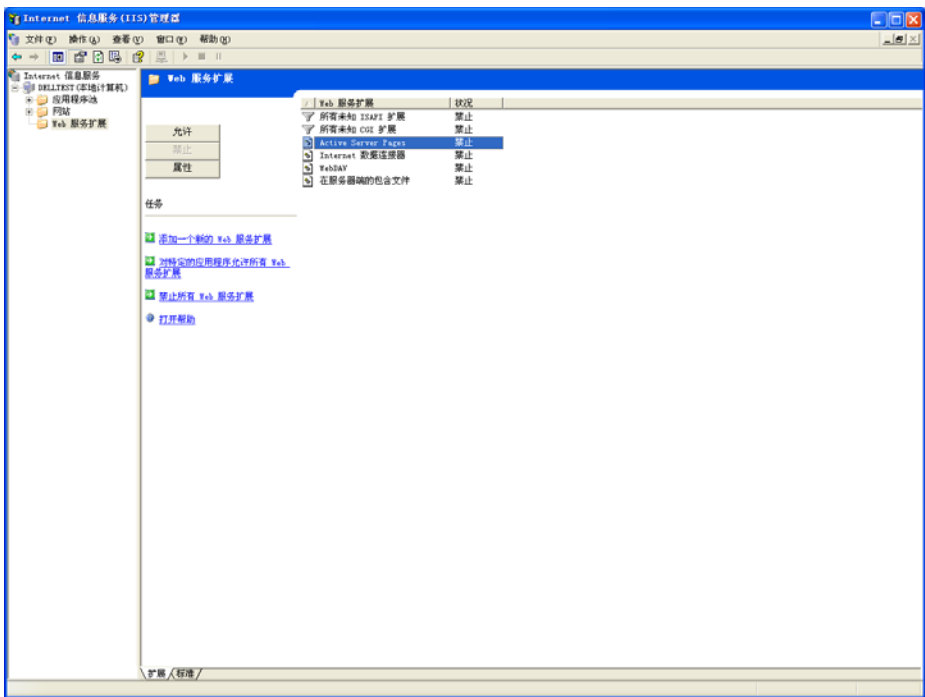


图 35 ASP 禁止界面

选择Active Server Page后选择启动按钮来启动asp支持，启动后的界面如图 36所示：

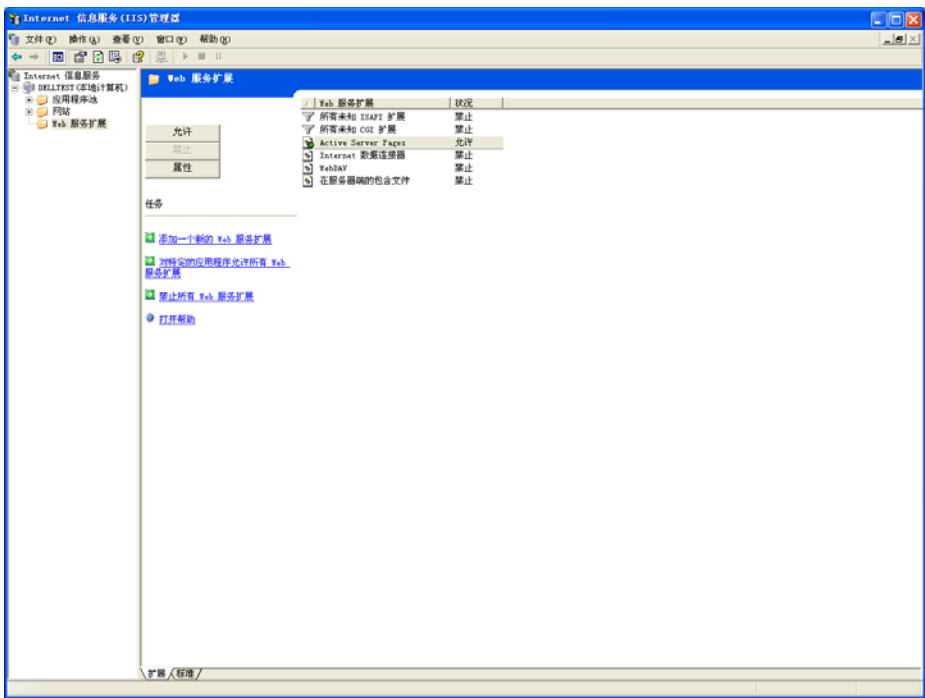


图 36 ASP 启动界面

我们的目的是要设置 IIS 系统，让用户 IIS 系统内的 Web 站点能够具有使用 SSL 安全性协议的能力及通过 Internet Explorer 来申请证书。要设置 Web Server 的 SSL 使用能力，必须打开 IIS 的主要目录安全对话框。要打开主要的 IIS 目录安全对话框，请按照下面的过程进行操作：

1. 以系统管理员权限的帐户登录 Windows Server 2003 计算机。
2. 依序打开“控制面板”→“管理工具”→“Internet 服务管理器”选项，来启动 IIS 服务管理工具。

3. 展开Internet信息服务（IIS）管理器，并在网站下的默认网站上点右键选择“属性”选项，系统会打开“网站属性”设置窗口，接着，请选择“目录安全性”页面，如图 37所示：

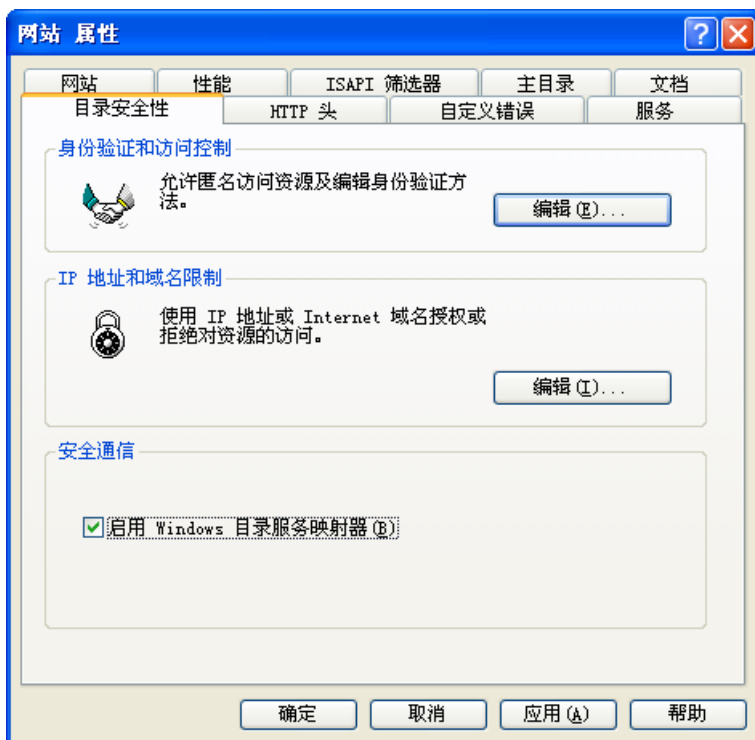


图 37 目录安全性设置

4. 接着，请勾选“安全通信”部分的“启用 Windows 目录服务映射器”的复选框选项。

如果在这里勾选“启用 Windows 目录服务映射器”的选项，那么 IIS 将会要求 Active Directory 域控制器来负责处理证书与帐号的映射关系。请注意，只有在 IIS 主要属性里才可以设置此选项。

如果使用 Windows 2003 Active Directory 域控制器的映射方式，用户就可以使用由在企业内部的证书颁发机构所发给的登录证书来连接上企业的 Web 站点。因为根据默认的状态，Windows Server 2003 会自动完成一对一的证书与用户帐户的映射关系，所以用户目前就可以采用此映射关系来连接 Web 网站。

我们将来看看如何设置一个单一的 Web 站点的安全功能。若用户不希望使用到 Windows 2003 Active Directory 域的映射功能（也就是用户在前一个操作步骤里没有勾选“启用 Windows 目录服务映射器”的复选框选项），直接跳到这一小节来操作即可。

在 IIS 里，可以同时设置管理多个 Internet 信息服务器（包括多部的 WWW Server、多部的 FTP Server、或是其他的国际互联网上的信息服务器），前面所说明的部分是针对整个 IIS 的安全性控管的设置（称为主要 IIS 目录安全设置），接下来，我们便要说明如何针对 IIS 内部的一个站点做安全性的设置与管理。

5. 接着，请再回到控制台，请在您想设置的Internet服务节点上（例如默认的Web站点），按下鼠标右键，并选择“属性”选项，系统会打开该Internet信息服务的属性设置窗口，请选择“目录安全性”的页面，如图 38所示：



图 38 目录安全性页面

当要开始启用 IIS 功能时，必须先获取 Web 服务器证书，以提供基础的证书身份验证服务。

6. 请读者注意“安全通信”的部分，若用户还未获取并安装 Web 服务器证书，这时候“查看证书”按钮为不可用的状态。用户必须先安装服务器证书，才能继续设置安全通信的属性。要安装服务器使用的证书，请按“服务器证书”按钮。当按下“服务器证书”按钮后，接着会出现 Web 服务器证书向导，指导用户进行服务器证书的安装过程，如图 39 所示：

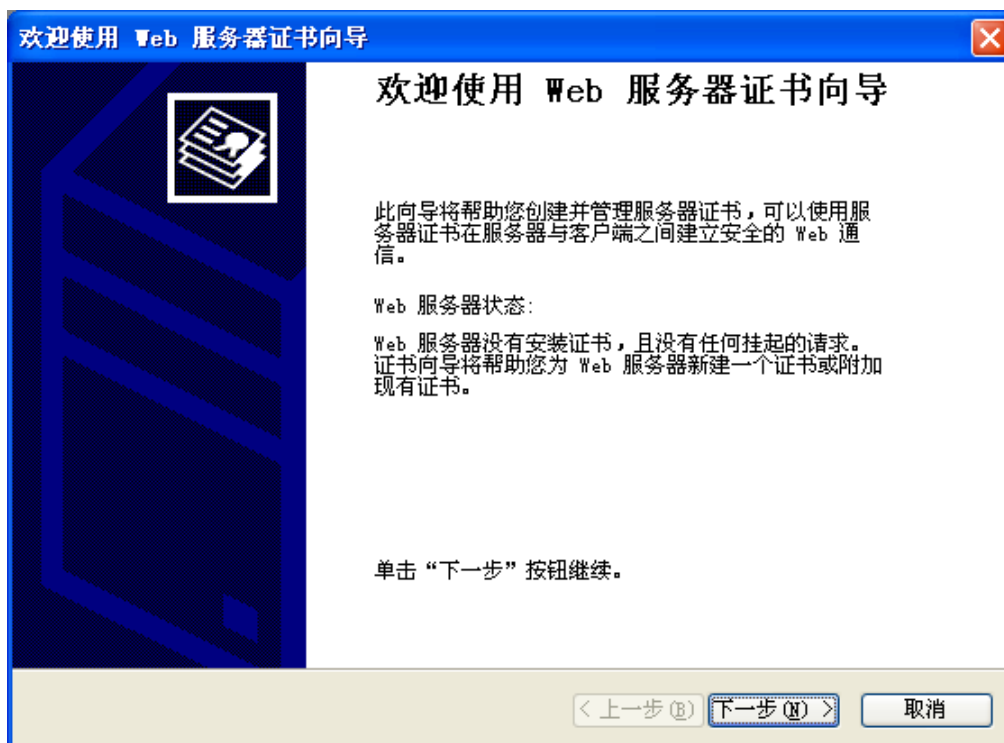


图 39 Web 服务器证书向导

7. 继续按“下一步”按钮，进行下一个步骤的服务器证书安装设置过程。接下来，系统会要求用户选择指定服务器证书的来源方式，如果尚未安装过服务器证书，这时候用户必须选择“新建证书”选项。若之前已获取过Web服务器证书，而且想要重新利用这些已有的证书，请选择“分配现有的证书”、“从密钥管理器备份文件导入证书”、“从.pfx文件中导入证书”、或者“将远程服务器站点的证书复制或移动到此站点”选项，将原有的Web服务器证书安装到IIS系统上，如图 40所示：



图 40 选择指定服务器证书的来源方式

以下的步骤假设用户选择“新建证书”选项来进行说明。

8. 当您设置好上一个设置步骤后，请继续按“下一步”按钮进行下一个步骤的服务器证书安装设置过程。系统会要求您选择证书请求的时机，您可以按照您的需要来选择是否要先准备好证书请求，稍后再将此证书请求发送到证书颁发机构上，以获取适当的证书信息；或者立即将证书请求传递到您在稍后指定的证书颁发机构上，立即向证书颁发机构请求获取证书信息。

在这个步骤里，可以选择在线上直接连接证书颁发机构，直接获取证书信息（“立即发送一个请求到一个在线证书颁发机构”选项）；或是将证书请求储存成文件（选择“现在准备请求，但稍后发送”选项）再将此证书请求的文件发送到证书颁发机构上，以获取需要的证书。

9. 假设用户目前需要由企业外部商用性质的证书颁发机构获取所需要的证书，那么用户可能需要使用文件方式的证书请求方式，产生请求证书的文件（一般是提供给该部商用证书颁发机构处理身份验证过程使用的信息），并由该部商用证书颁发机构确认核对后，再发行用户证书，这时候，用户就可以获取需要的证书。一般来说，联机获取的证书颁发机构通常是本地的证书颁发机构，以及企业内部（域内）的证书颁发机构。

若证书服务器（证书颁发机构）目前处理证书的数量不是很多，或者需要立即操作 IIS 系统的 SSL 安全通信协议的设置时，用户可以选择“立即发送请求到一个在线证书颁发机构”选项，以便立即将稍后所设置的证书请求信息传递到适当的证书颁发机构上，以便获取适当的证书信息。在这里，我们选择“现在准备请求，但稍后发送”。

当设置好这一个设置步骤后，请继续按“下一步”按钮，进行下一个步骤的服务器证书安装设置过程。

10. 接下来，系统会出现“名称和安全性设置”的设置窗口。这时候系统会要求用户设置此证书的

名称以及此证书安全设置项目。此时需要为请求获取的服务器证书定义一个易于标识的证书名称，并设置此证书要使用的密钥长度。根据应用的需要，设置适当的密钥长度。并注意，若密钥长度设置太短，可能导致安全性的降低；若密钥长度设置太长，可能导致系统运算处理时间过长，导致系统效率不佳或者软硬件系统无法配合等现象。一般来说大约 1024~2048 Bits 会是比较好的选择，如图 41 所示：

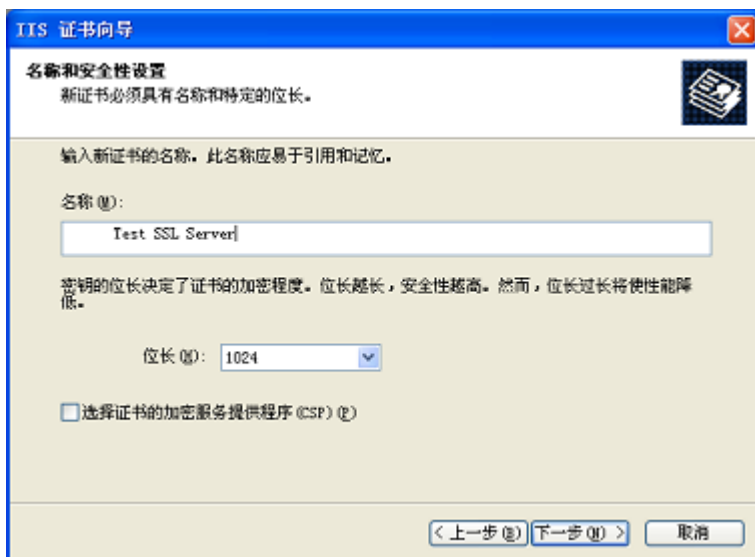


图 41 命名及安全设置

当完成此设置步骤后，按“下一步”按钮，进行下一个步骤的服务器证书安装设置过程。

**11.** 接下来，用户需要输入企业组织的一些相关信息，以便让系统将企业以及目前所处的单位等相关信息记录在想获取的证书信息内，如图 42 所示。输入完毕后，按“下一步”按钮继续下一个步骤的服务器证书安装设置过程。



图 42 组织信息设置

**12.** 命名安装服务器证书的国际互联网服务器的标识公用名称。输入提供此 Web 服务器的 Windows Server 2003 计算机的完整资格名称(也就是 DNS 名称)。若服务器是在企业内部运行的网络(Intranet)，用户可以输入提供此 Web 服务器的 Windows Server 2003 计算机的 NetBIOS 名称，如图 43 所示。当设置好这一个设置步骤后，继续按“下一步”按钮，进行下一个步骤的服务器证书安装设置过程。



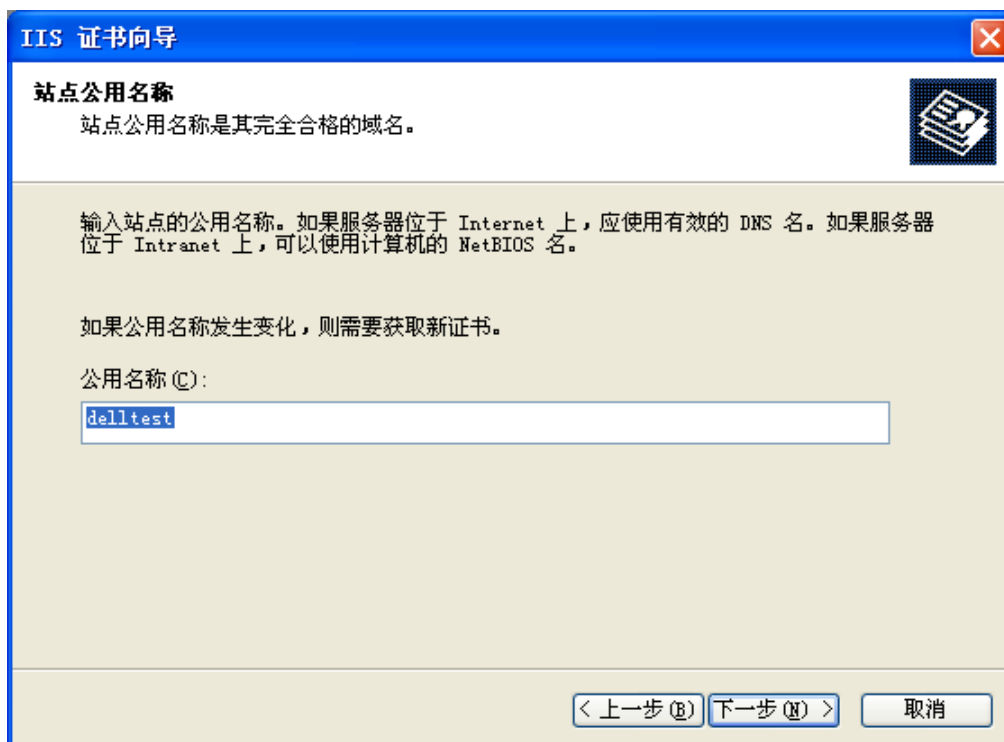


图 43 站点公用名称

**13.** 填入目前此Web服务器所在的地理位置信息，以便提供证书信息更详细的更丰富的数据，如图 44所示。当完成这一个设置步骤后，继续按“下一步”按钮，进行下一步骤的服务器证书安装设置过程。



图 44 地理信息

**14.** 屏幕上出现“证书请求文件名”的设置窗口，用户可以在这里设置证书请求文件的文件名，并为其选择安装路径，如图 45所示：



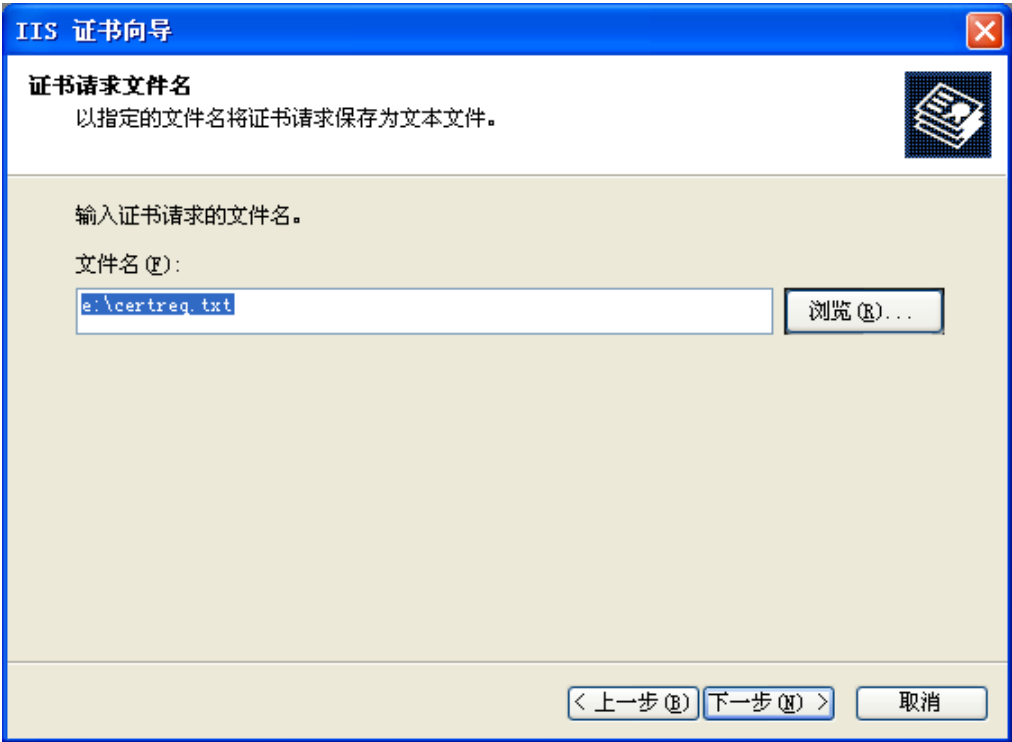


图 45 将证书请求存储成文件

**15.**当设置完成后，系统会显示刚刚所设置的证书申请信息，用户可以检查是否有错误，若无错误，可以继续按“下一步”按钮，进行下一个步骤的服务器证书安装设置过程，如图 46所示：



图 46 请求文件摘要

**16.**按“完成”按钮，这时计算机已经把证书请求文件存储下来了。现在，就可以去证书颁发机构去获取证书了。

**17.**打开Internet Explorer浏览器，连接证书服务器（这里以上面刚刚搭建的CA为例），进入证书颁发网页，选择“申请一个证书”选项，如图 47所示：



图 47 由 IE 获取证书

**18.** 接下来，进入选择证书申请类型页面，在这里我们选择“高级证书申请”选项，如图 48所示。这里要选择文件形式的证书获取方式，即利用刚刚得到的证书请求文件来申请证书。

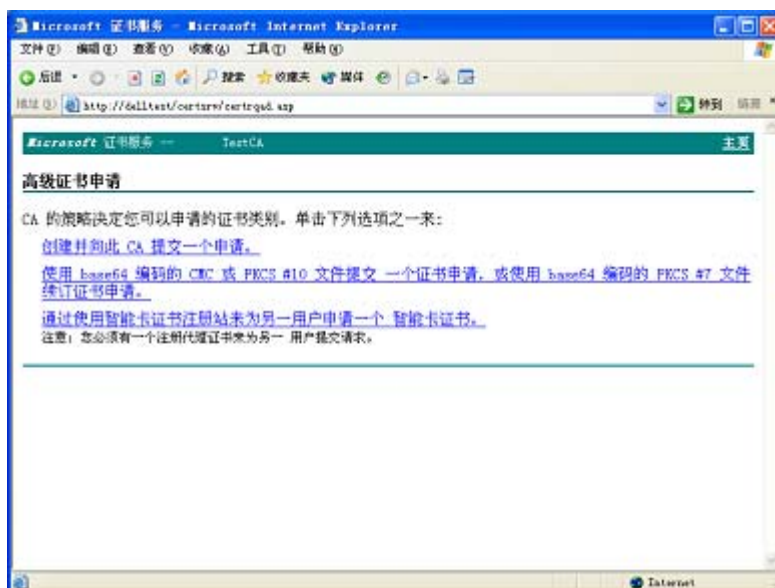


图 48 高级证书申请

**19.** 进入如图 49所示的界面，用户需要将存储起来的证书请求文件的内容拷贝到“保存的申请”一栏中。然后按“提交”按钮。

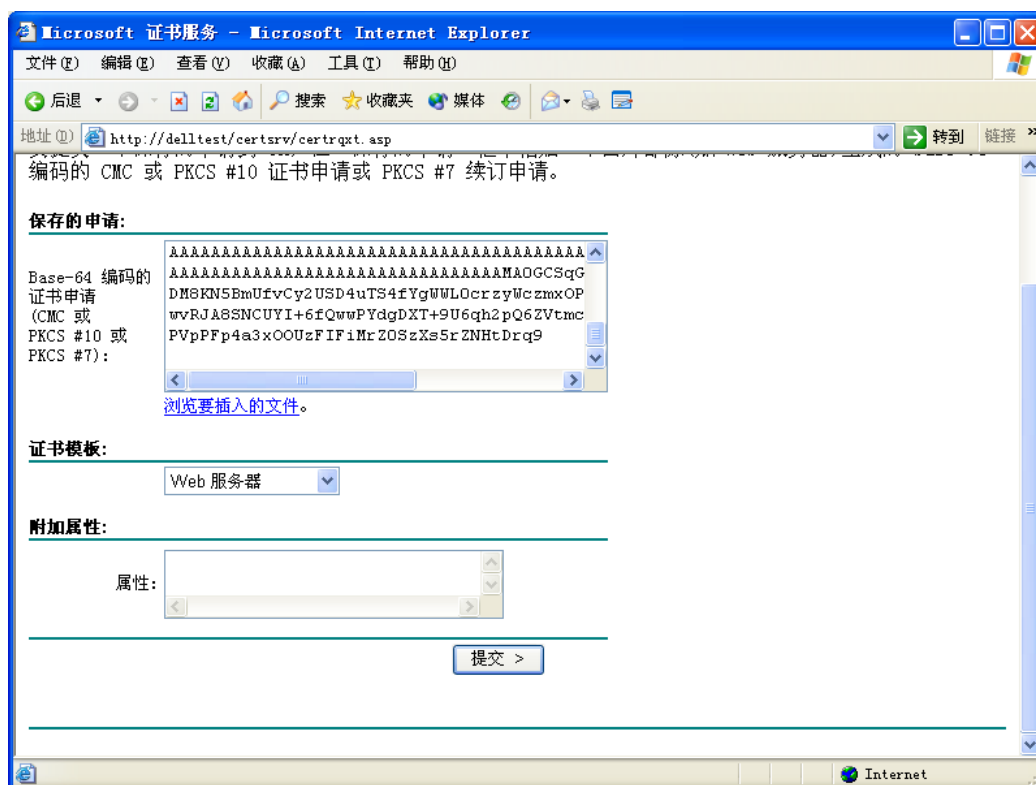


图 49 提供证书请求文件

**20.** 提交完证书请求文件后，会进入如图 50 所示的页面。虽然在前面安装证书颁发机构时选择的是企业根类型的证书颁发机构，但设置了不在线发放，所以这里可以看到请求的证书被挂起，要等待颁发机构确认身份并发行证书后才能去领取。



图 50 证书挂起

**21.** 等待证书颁发机构确认身份并通知用户去领取证书后，用户就可以再次进入颁发机构去领取证书了。打开颁发证书页面，选择“查看挂起的证书申请的状态”选项，如图 51 所示：



图 51 用 IE 获取被挂起的证书

22. 选中与申请日期一致的证书申请请求，去领取证书，如图 52所示：



图 52 检查挂起的证书请求

23. 这时能看到用户所申请的证书已经发行了，如图 53所示。单击“下载证书”开始证书下载过程。

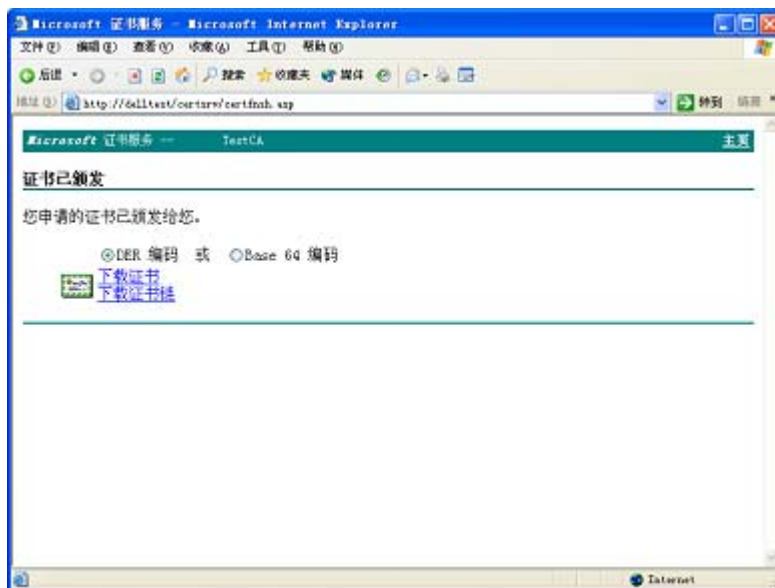


图 53 证书下载

24. 完成了证书下载，用户还必须启动证书安装向导来把证书安装在服务器上。有关如何打开证书安装向导请参照第 6、7 步骤。完成证书导入如图 54所示：

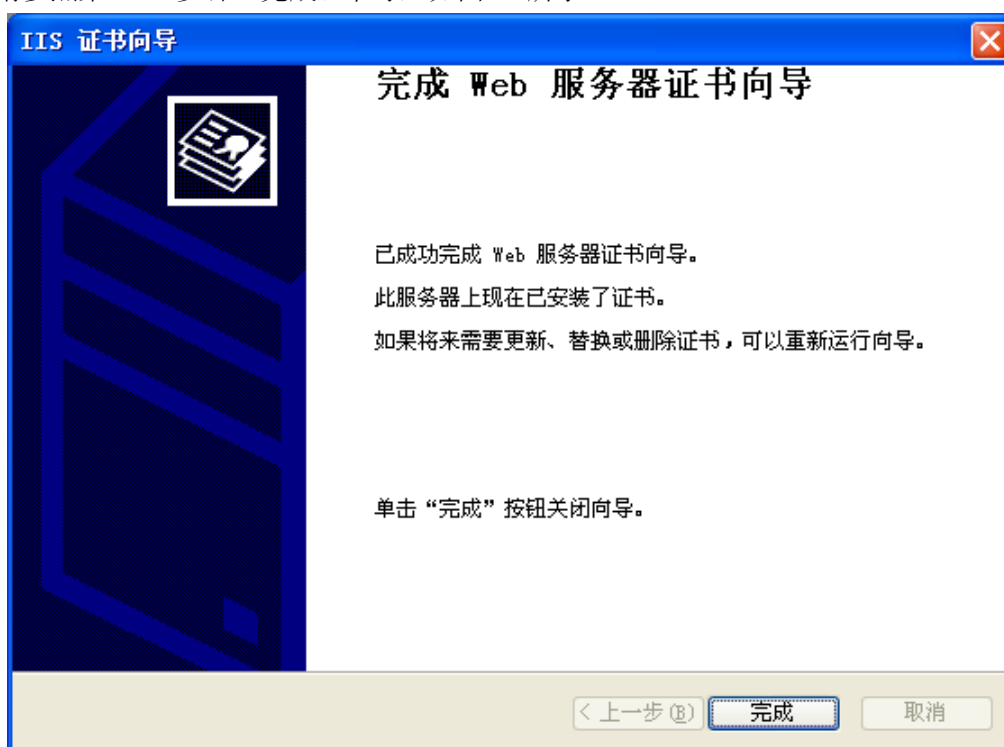


图 54 完成服务器证书导入

如果采用直接链接上证书颁发机构的方式来获取证书，那么这时候向导会向用户所指定的证书颁发机构发出一个获取证书的请求信息，当该证书颁发机构身份验证通过时，就会发给用户一个证书，此证书会自动安装在用户 Web 服务器上。

在安装了服务器的证书后，接下来，用户就可以回到原来所打开的Internet服务器站点（Web站点）的属性设置窗口上，这时SSL Port变为可填写状态。这里用户要为该Web站点填写一个安全通道端口（SSL Port），推荐填写默认值 443，如图 55所示：

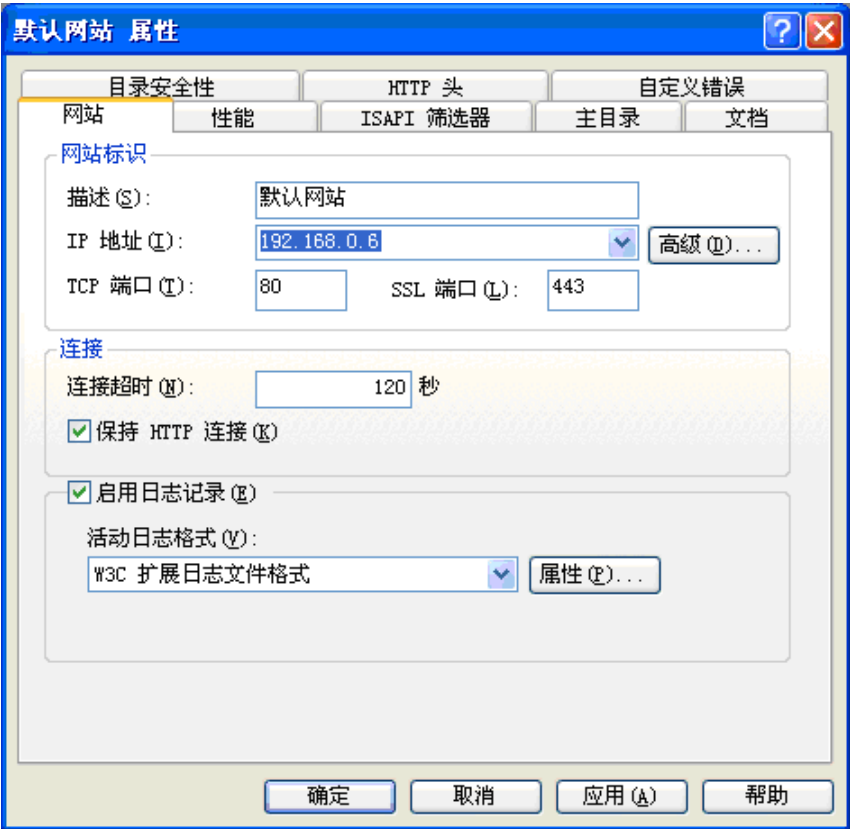


图 55 填写 SSL Port

现在展开“目录安全性”页面，用户可以看到在“安全通信”部分里的“查看证书”按钮已经呈现启用状态了，表示这时候就可以开始设置该国际互联网服务器的安全性协议使用设置了，如图 56所示：



图 56 安装服务器证书后的服务器属性设置窗口

接下来，用户就可以开始进行此 Web 服务器使用 SSL 安全性协议的设置处理了。要设置此 Web 服务器使用的安全性协议功能的操作时，按照下列的过程进行设置：

1. 回到该Internet信息服务器的属性设置窗口，并选择“目录安全性”页面，如图 56所示的画面。
2. 这时候，按下在“安全通信”部分里的“编辑”按钮，来进行该Web服务器的安全设置。当按下“编辑”按钮后，会出现安全通信编辑窗口，如图 57所示：
3. 因为我们的目的是要完成设置安全Web站点，因此，勾选位于窗口上方的“要求安全通道(SSL)”的复选框。在客户证书中选择“要求客户端证书”选项，如图 57所示。以下是关于这些选项的说明。

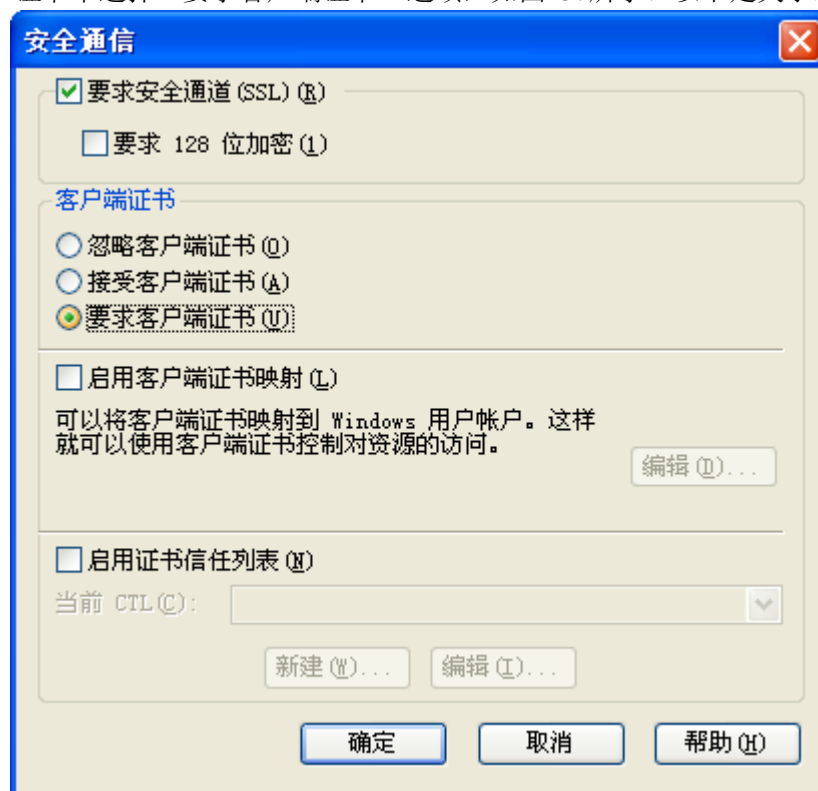


图 57 设置安全通信页面

- 要求安全通道（SSL）：一般来说，若没有启动此选项的话，Web 服务器默认都会以 HTTP 的通讯协议来提供 WWW 服务。但若启动了此选项后，IIS 系统就会强迫 WWW 客户端浏览器使用 SSL 的通讯协议（采用 SSL 安全协议）来使用 WWW 的服务。也就是当启用此选项后，系统就会关闭使用 http:的连接，仅能使用 https:连接来接上 Web 服务器（当服务器证书已经安装在您的国际互联网服务器上时，用户服务器就允许接受 https:协议方式的联机了，若将该国际互联网服务器上的服务器证书删除，那么就无法使用 https 的方式进行联机）。

换句话说，若勾选了这个选项，便是强迫终端用户一定要使用 SSL 的安全协议与服务器建立连接，以确保安全。

- 要求客户端证书：用户必须提供一个证书才能够获得访问权限，这种方式具有较高的安全性。

当设置完成后，单击“确定”按钮。这时，已经完成了安全Web站点的设置工作，并已经启用了安全通道，如果再通过http:连接来连接该Web站点，会出现如图 58所示的情况：



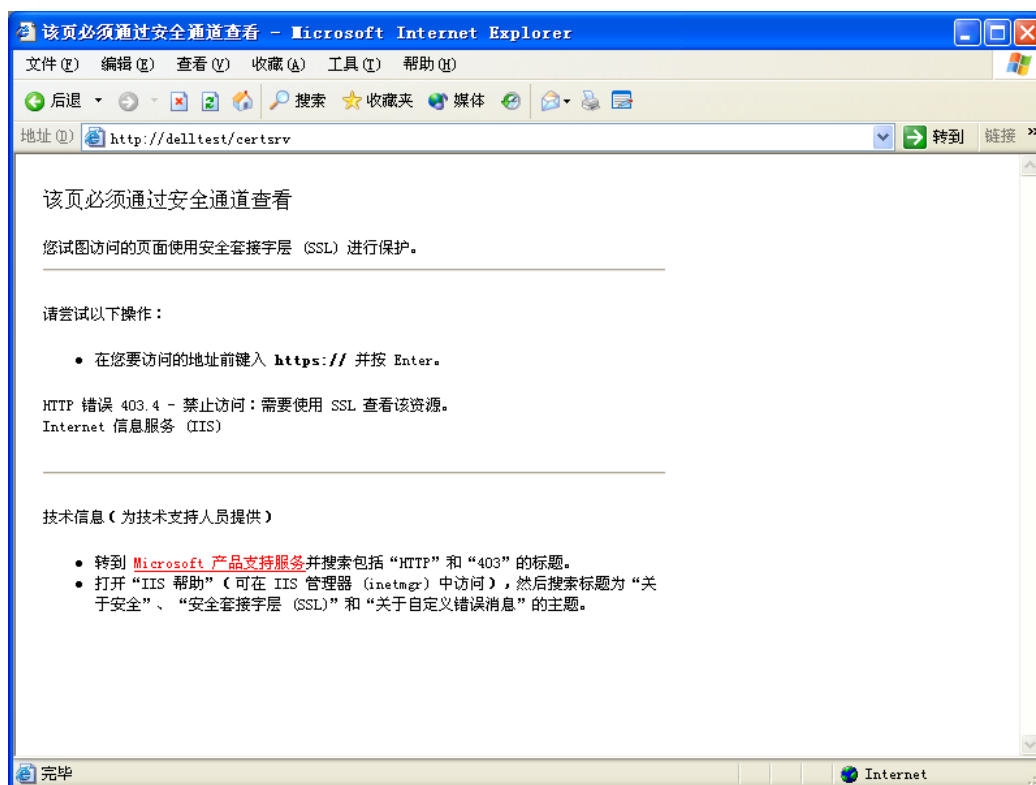


图 58 无法使用 http:访问安全站点

系统提示必须通过https:连接来连接上要访问的站点。用户再通过https:连接来连接上刚刚设置的安全Web站点。会看到系统有如图 59所示的安全提示。

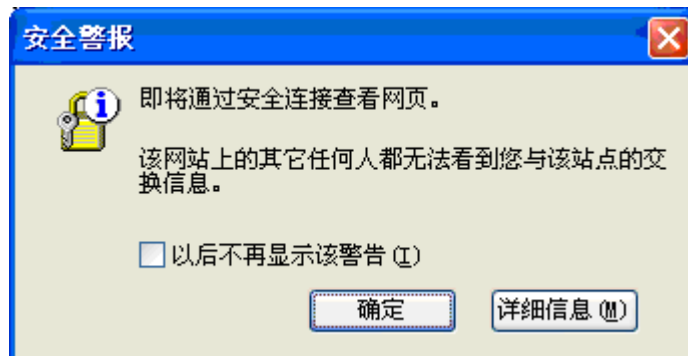


图 59 安全提示信息

单击“确定”按钮后，会有客户认证提示，要求选择用户要使用的证书，如果用户还没有申请客户证书，则证书列表为空，请先申请一个用户证书（参见ET199 的CAPI应用）。选择正确的证书后按“确定”按钮，即可访问安全Web站点，如图 60所示：

**注：此安全 Web 站点为示例站点。**



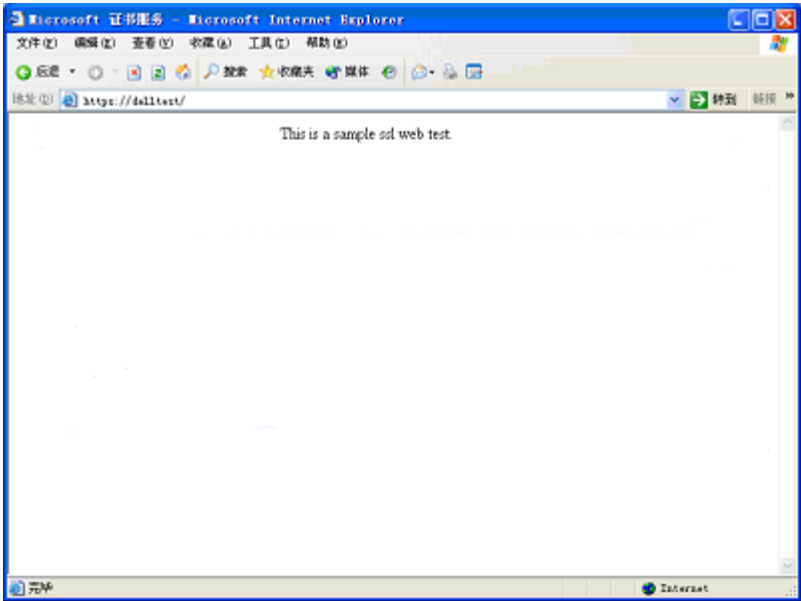


图 60 安全 Web 站点

## 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<br>(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。                          |