SIEMENS

常问问题 05 月/2014 年

用 HTTS 访问 SCALANCE X

Scalance X

http://support.automation.siemens.com/CN/view/zh/93843162

目录

1 HTTPS 简介

超文本传输安全协议（缩写：HTTPS，英语：Hypertext Transfer Protocol Secure）是超文本传输协议和 SSL/TLS 的组合，用以提供加密通讯及对网络服务器身份的鉴定。HTTPS 连接经常被用于万维网上的交易支付和企业信息系统中敏感信息的传输。

HTTPS 的主要思想是在不安全的网络上创建一安全信道，并可在使用适当的加密包和服务器证书可被验证且可被信任时，对窃听和中间人攻击提供合理的保护。

HTTPS 的信任继承基于预先安装在浏览器中的证书颁发机构（如 VeriSign、Microsoft 等）（意即“我信任证书颁发机构告诉我应该信任的”）。因此，一个到某网站的 HTTPS 连接可被信任，当且仅当：

1. 用户相信他们的浏览器正确实现了 HTTPS 且安装了正确的证书颁发机构；
2. 用户相信证书颁发机构仅信任合法的网站；
3. 被访问的网站提供了一个有效的证书，意即，它是由一个被信任的证书颁发机构签发的（大部分浏览器会对无效的证书发出警告）；
4. 该证书正确地验证了被访问的网站（如，访问 https://example 时收到了给“Example Inc.”而不是其它组织的证书）；
5. 或者互联网上相关的节点是值得信任的，或者用户相信本协议的加密层（TLS 或 SSL）不能被窃听者破坏。

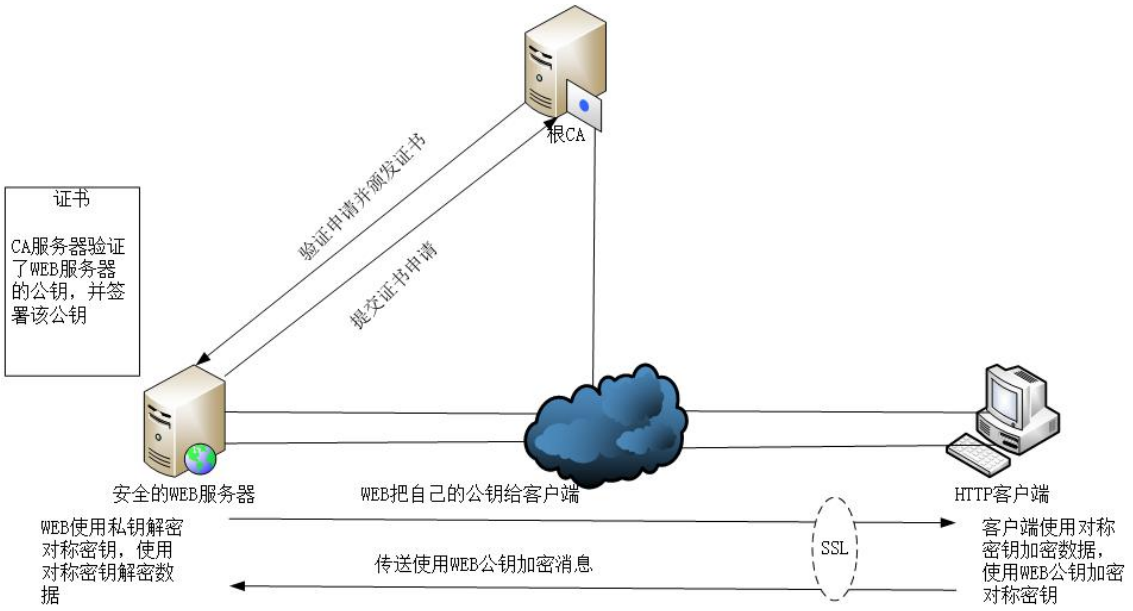

图 1-1 HTTPS 建立连接的认证过

图 1-1 是 HTTPS 建立连接的认证过程。认证分为以下步骤：

- 支持 HTTPS 的 WEB 服务器向 CA 申请数字证书。
- CA 核实 WEB 服务器的信息后颁发证书。
- HTTPS 客户端信任该根 CA。
- 安全的 WEB 服务器将 CA 颁发的含有自己公钥的数字证书传递给 HTTPS 客户端。
- HTTPS 客户端使用对称密钥加密数据，使用 WEB 公钥加密对称密钥。
- HTTPS 客户端将加密后的对称密钥传递给 WEB 服务器。
- WEB 服务器使用自己的私钥解密加密的对称密钥。
- WEB 服务器得到对称密钥，HTTPS 客户端和 WEB 服务器具有相同的对称密钥。
- HTTPS 客户端和 WEB 服务器使用对称密钥加密数据通信。

2 将 WINDOWS SERVER 2008 配置为 CA

用 HTTPS 访问 SCALANCE X 交换机，SCALANCE X 交换机相当于 WEB SERVER。如果使用 HTTPS 访问交换机，交换机首先要向 CA 申请数字证书。CA 一般是政府或商业机构，提供有付费服务。CA 的一般层级结构如下图。

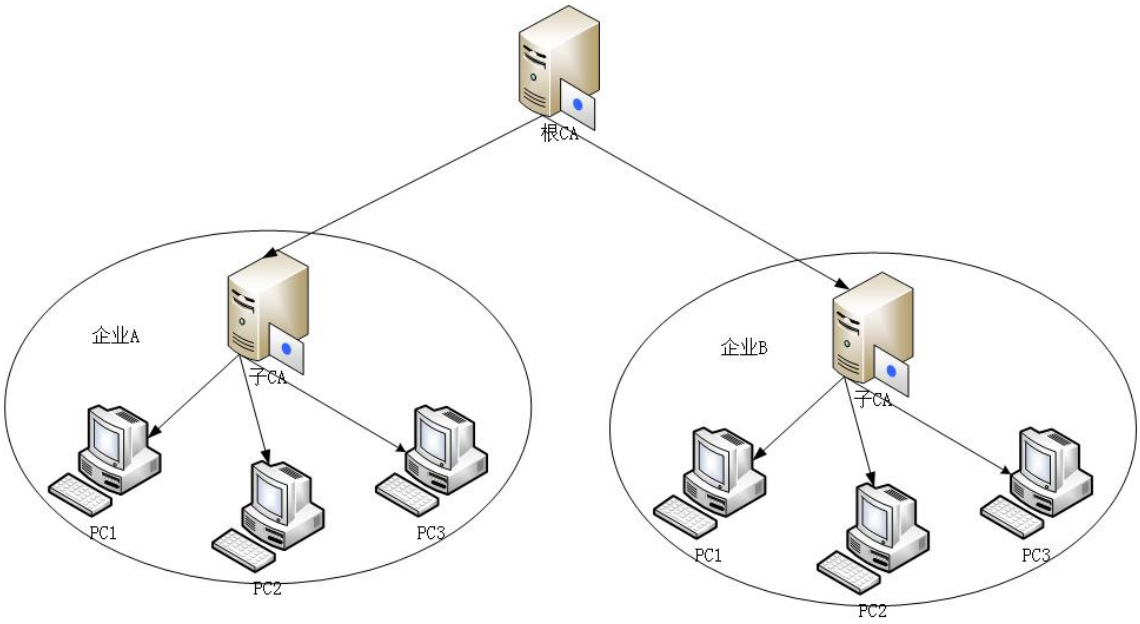

图 2-1 CA 层级结构

如上图，CA 是分层树形结构。最顶层的是根 CA，根 CA 还有分支机构子 CA。根 CA 负责认证子 CA。各个子 CA 还可以继续分支。客户可以向任何一个子 CA 申请数字证书。如果 HTTPS 客户端要访问该 WEB 服务器，HTTPS 客户端需要信任该子 CA 所属的根 CA。

如果在企业内部搭建 CA 体系结构，可以使用 WINDOWS SERVER 2008 作为根 CA 或子 CA。如果企业外部的客户需要访问，则最好向公共的 CA 申请数字证书，这是由于企业外部的客户通常只信任公共的 CA。以下介绍使用 WINDOWS SERVER 2008 建立 CA 服务器的过程。

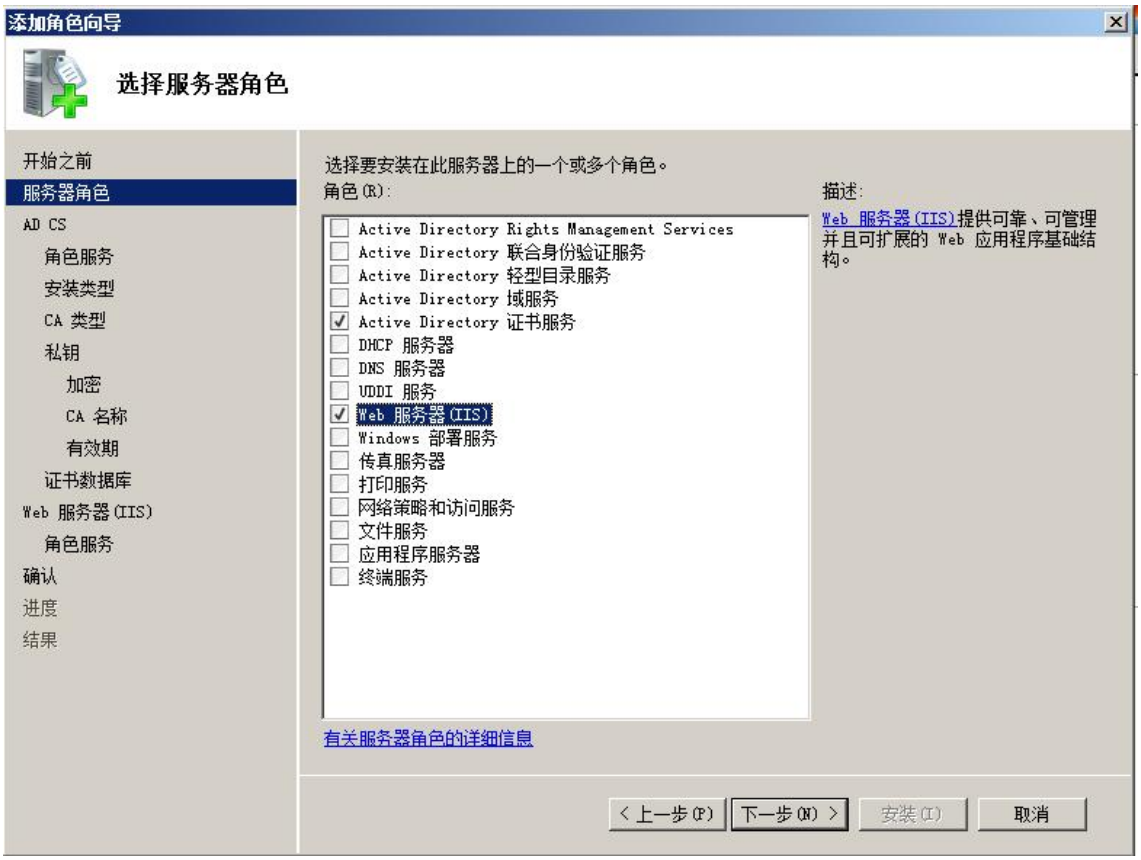

图 2-2 添加角色

在开始菜单中点击服务器管理器。打开服务器管理器的界面后，选中左侧的角色，在右侧选择添加新角色。出现图 2-2 的界面。选中“ Active Directory”证书服务及“ Web 服务器（IIS)”。安装这两个服务。

图 2-3 安装证书服务

图 2-4 安装证书服务

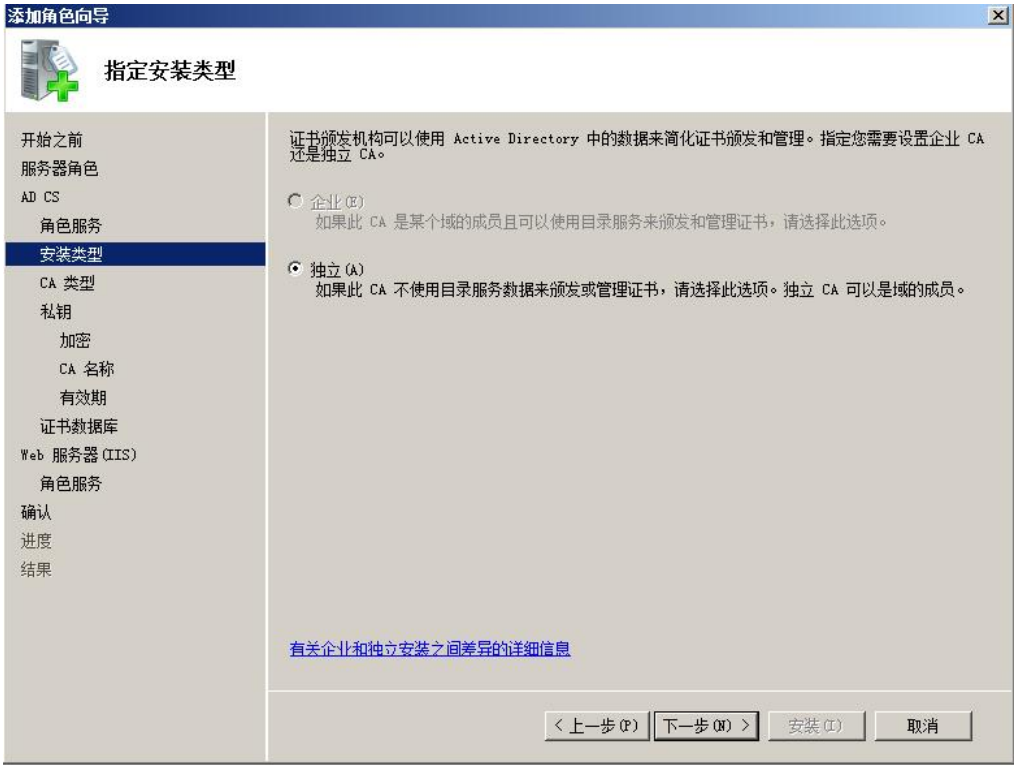

图 2-5 安装证书服务

图 2-6 安装证书服务

在图 2-6 中，由于只配置了一个 CA，所以选择为根 CA。

图 2-7 安装证书服务 生成密钥

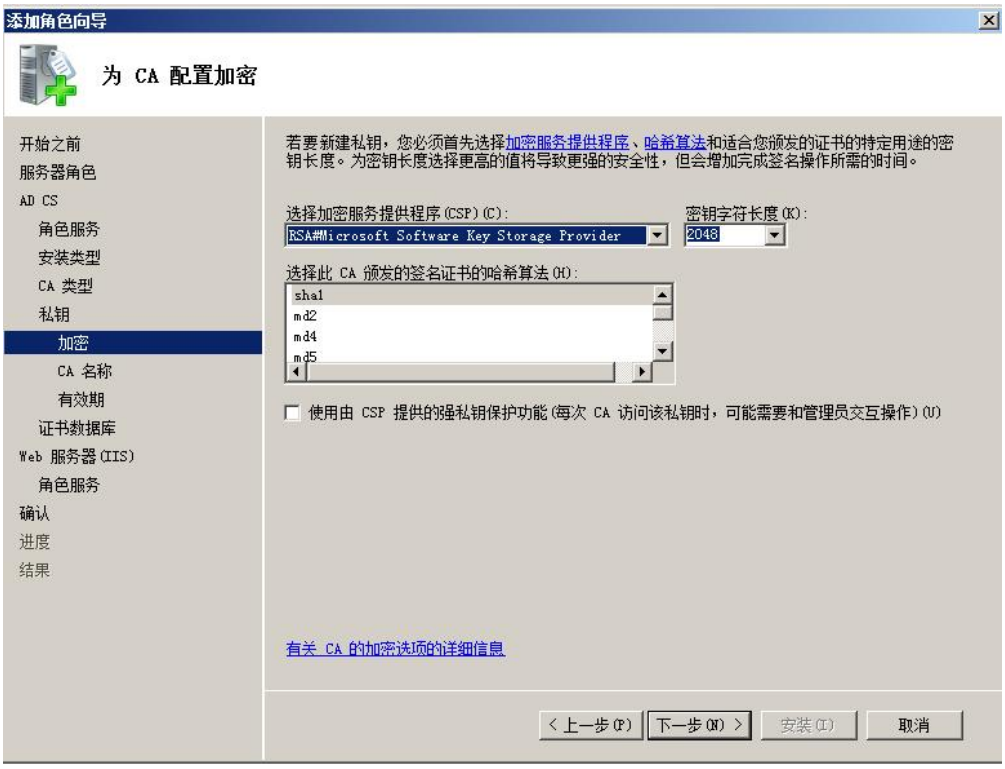

图 2-8 安装证书服务 选择密钥长度和哈希算法

密钥越长，越不容易被破解，选择 2048。签名证书的哈希算法选择更安全的“ sha1"。

图 2-9 配置 CA 的名称

图 2-10 选择 CA 的有效期

图 2-11 选择证书保存的位置

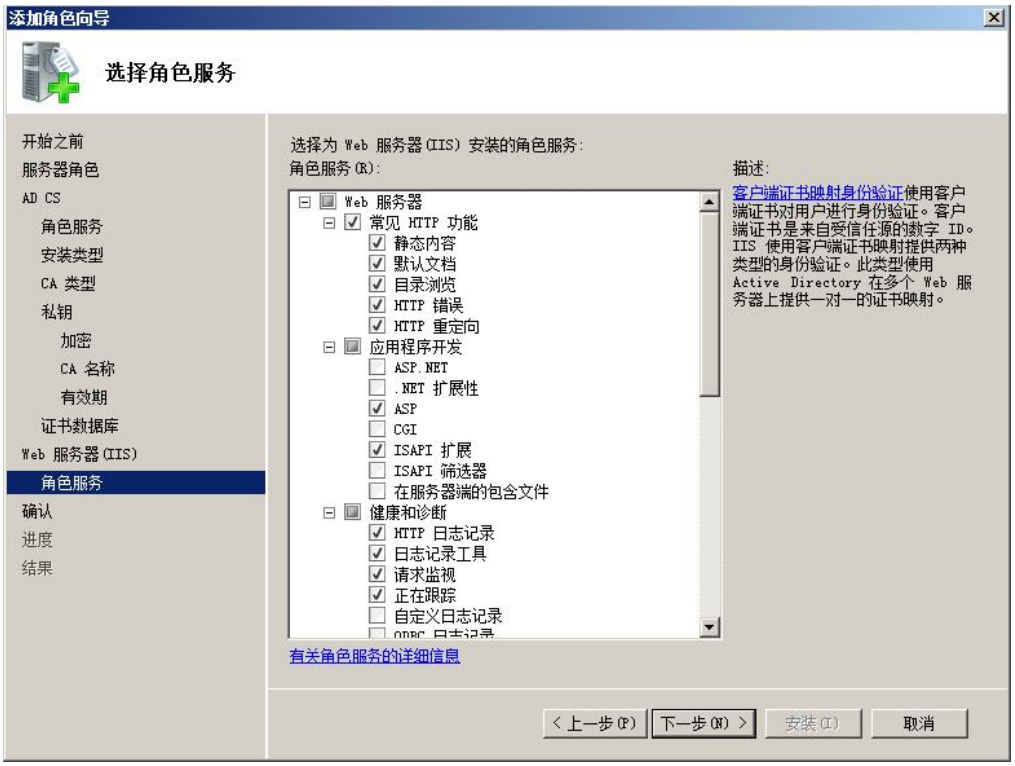

图 2-12 安装 IIS 服务

图 2-13 确认安装

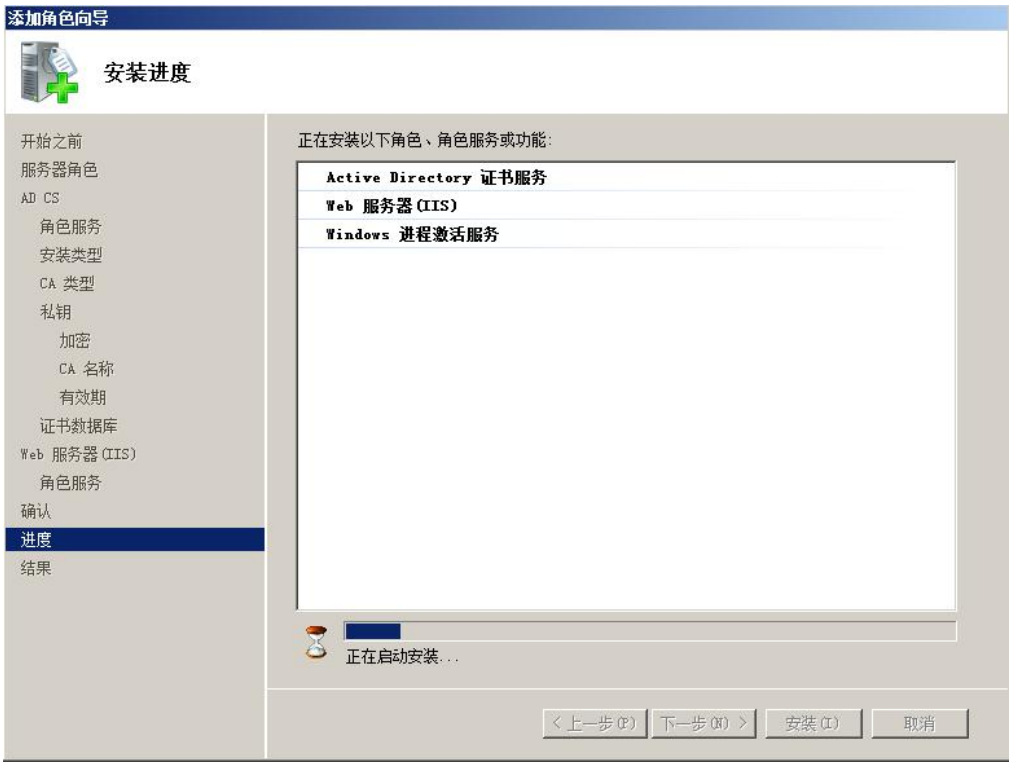

图 2-14 开始安装证书服务和 IIS 服务

图 2-15 成功安装证书服务和 IIS 服务

图 2-16 服务管理器

成功安装后，在服务管理器中应该与图 2-16 显示的相同。

3 配置证书服务和 IIS 服务

角色服务安装完成后，在开始菜单中打开“管理工具”。选中其中的“ Certification Authority”打开。如下图的界面。其中证书颁发机构“ WIN-TEST-ROOTCA”就是刚才建立的根 CA。下面的各个目录中分别是：吊销的证书，颁发的证书，挂起的申请，失败的申请。

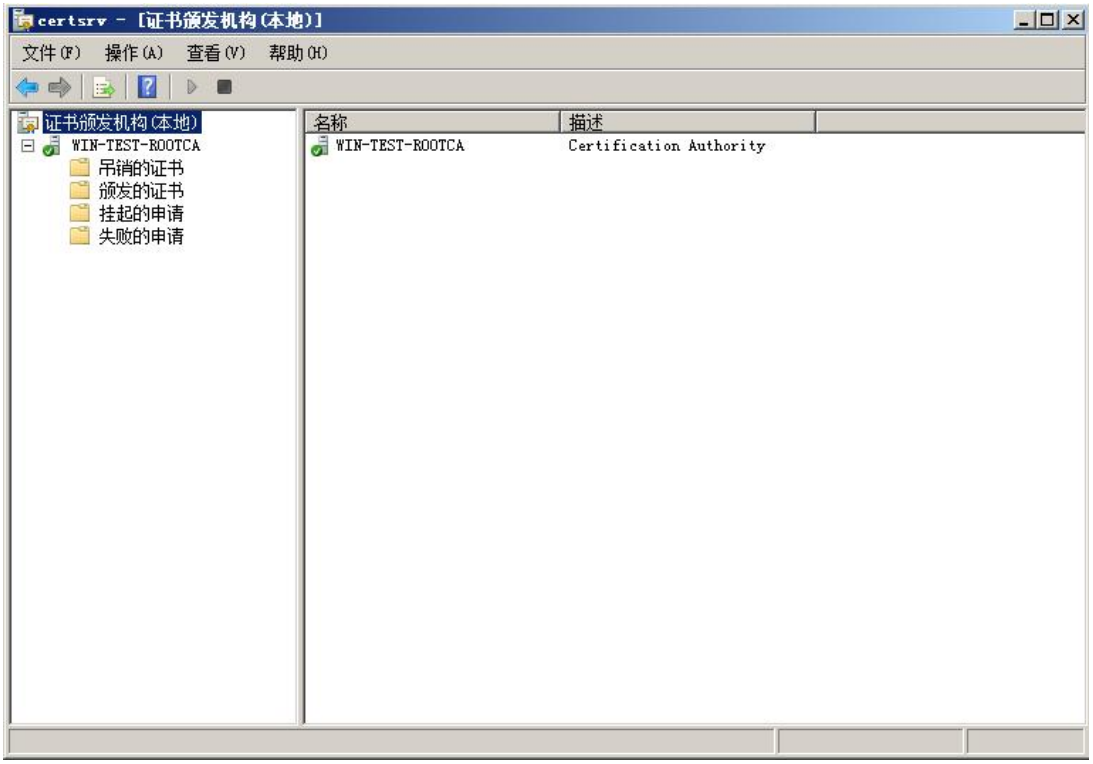

图 3-1 证书颁发机构

由于向 CA 申请数字证书需要使用 HTTPS 的方式，所以首先要给 CA 服务器的 WEB Server 申请一个数字证书。该数字证书是基于根证书颁发机构“ WIN-TEST-ROOTCA”申请的。也就是说，其它计算机只要信任该根证书颁发机构，就能信任 CA WEB Server 的数字证书。

首先给 Web 服务器申请一个数字证书。申请方式如以下步骤。

图 3-2 IIS 管理器

在开始菜单中打开“管理工具”，打开 IIS 管理器。左侧选中最顶层目录，双击“服务器证书”的图标打开。如图 3-2 所示。点击右侧的创建证书申请，为 IIS WEB 服务器申请一个数字证书。

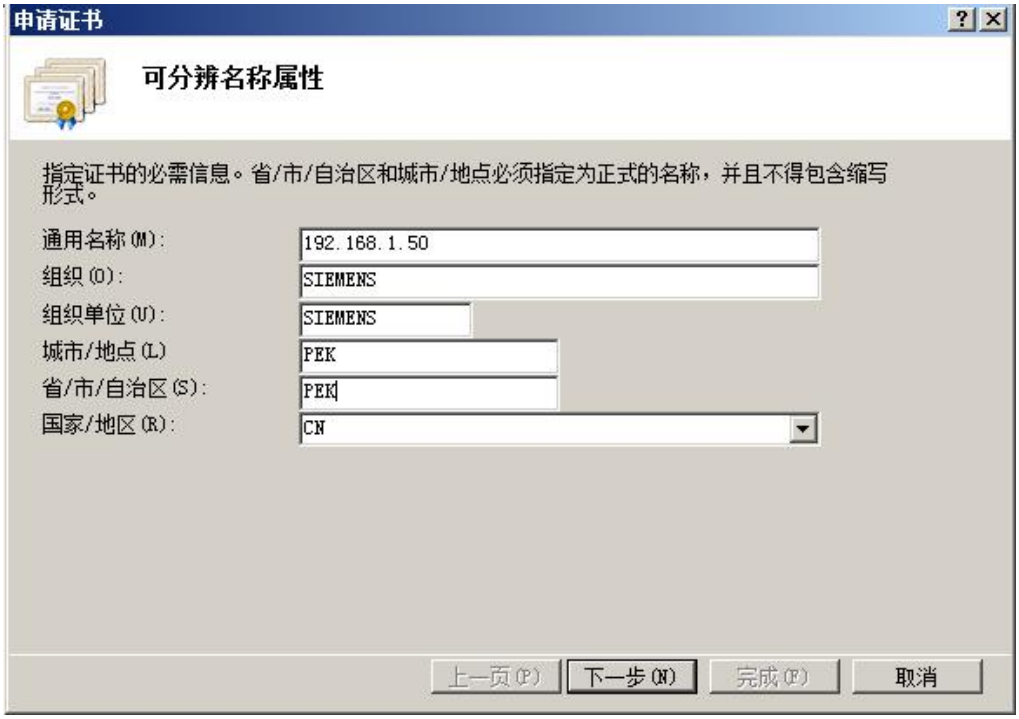

图 3-3 申请证书

申请数字证书需要提供一系列机构信息。通用名称指申请数字证书的 WEB 服务器的域名。由于这里没有使用 DNS 解析域名，在此处填写 WEB 服务器的 IP 地址。以下部分是组织结构的详细信息。CA 需要核实这些信息无误后才给申请证书的机构颁发。

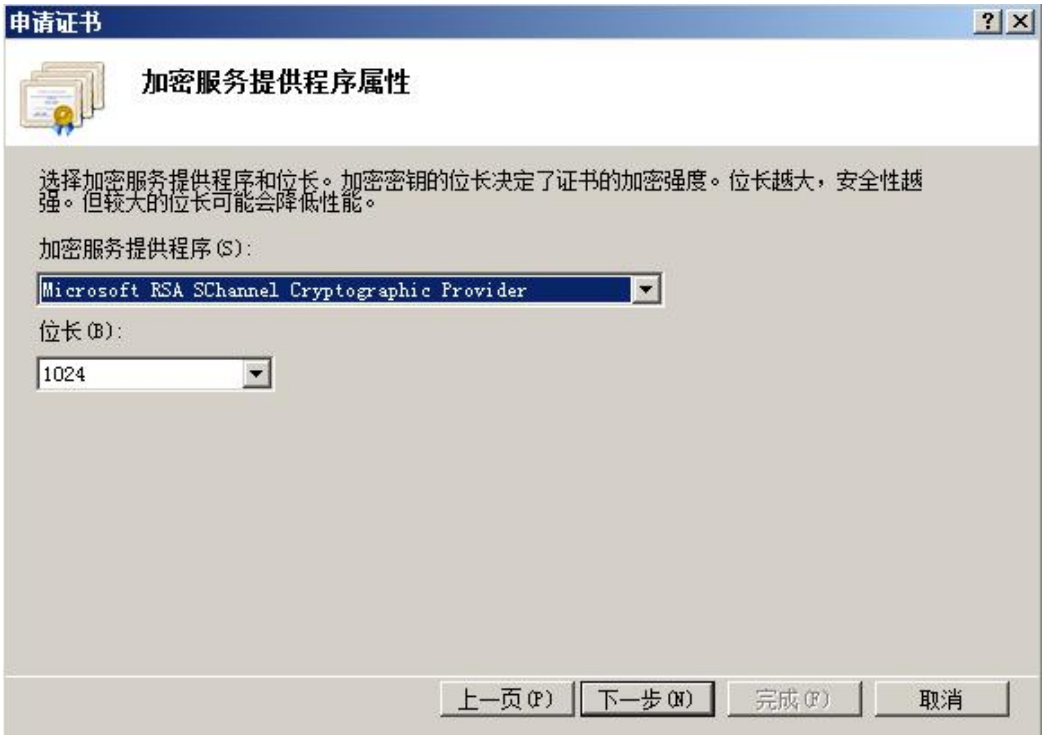

图 3-4 选择加密服务程序

选择加密服务程序，这里选用默认设置。证书加密的位长越长越安全，但会增加计算的负荷，降低性能。

图 3-5 选择证书申请文件导出的文件名

这里将证书导出到“C”盘的根目录下，文件名为“CAWEB”。

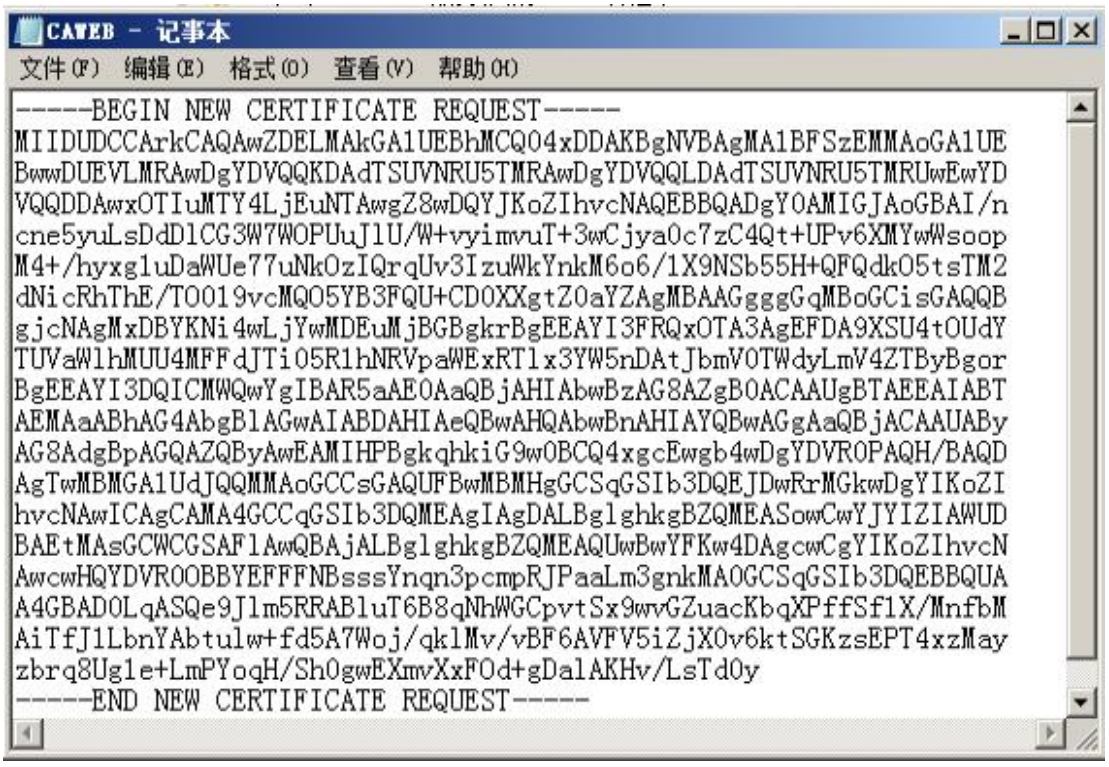

图 3-6 生成的证书申请文件

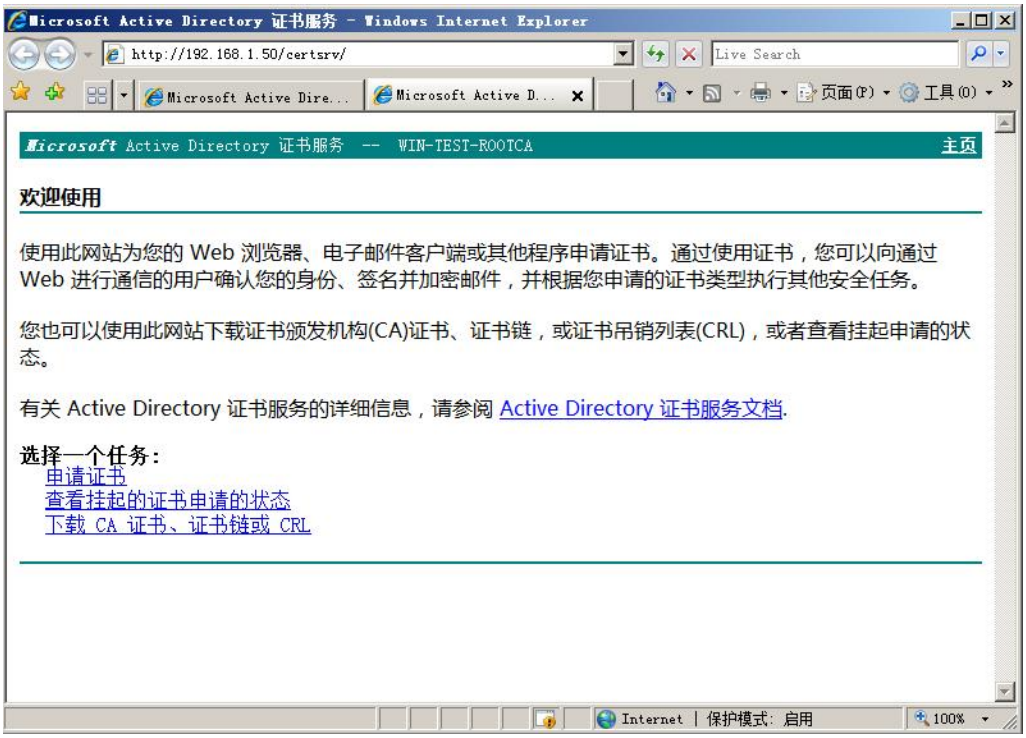

图 3-7 申请 WEB 服务器数字证书

如图 2-6 所示。在 IE 浏览器中输入“ http://192.168.1.50/certsrv/”。其中“ 192.168.1.50”是服务器的 IP 地址。在打开的界面中选择申请证书。

图 3-8 申请 WEB 服务器数字证书

在图 3-8 中可以选择申请的证书类型，这里选择高级证书申请。

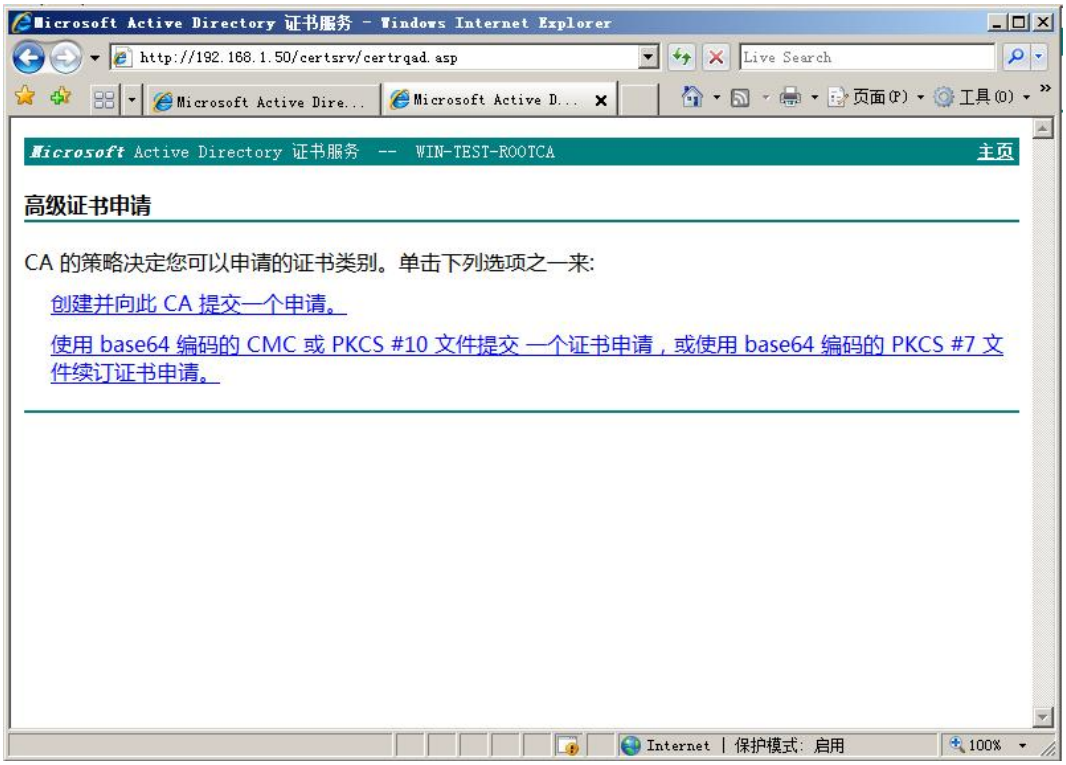

图 3-9 申请 WEB 服务器数字证书

在图 3-9 中选择使用 base64 编码提交证书申请。

图 3-10 申请 WEB 服务器数字证书

在图 3-10 的页面中，将刚才申请得到的数字证书申请文件“ CAWEB”用写字板打开后，拷贝粘贴到该页面中，并点击提交按钮。

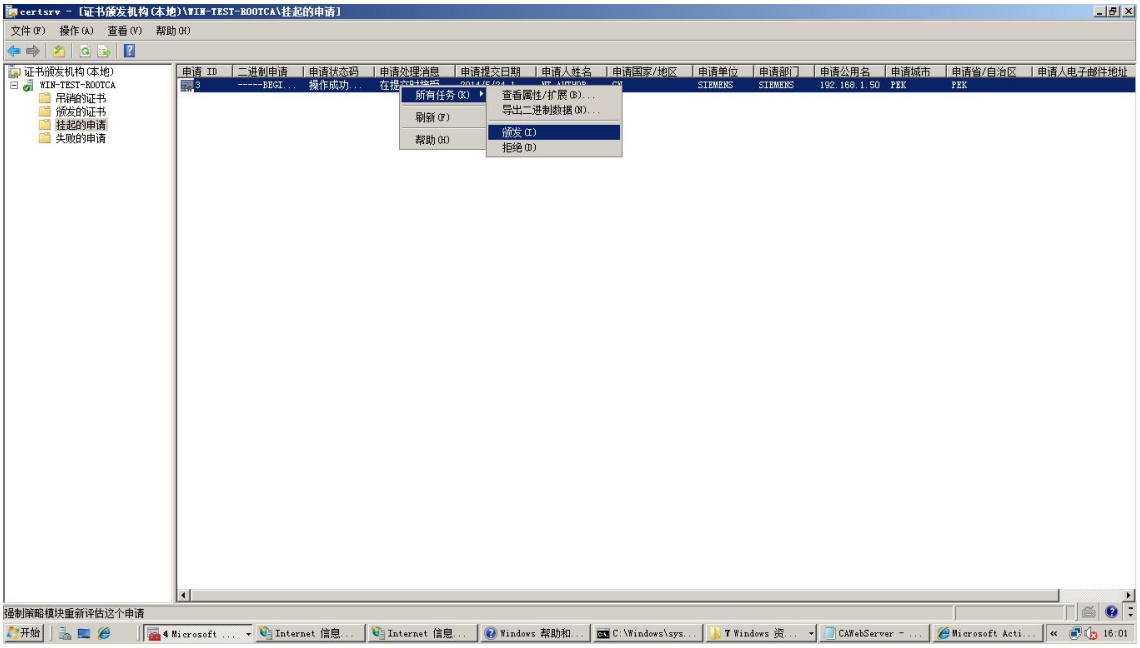

图 3-11 颁发 WEB 服务器数字证书

在开始菜单中打开“管理工具”。选中其中的“ Certification Authority”打开。在挂起的申请目录中可以看到刚才提交的证书申请，如图 3-11 所示。在右键菜单中选择“颁发”。

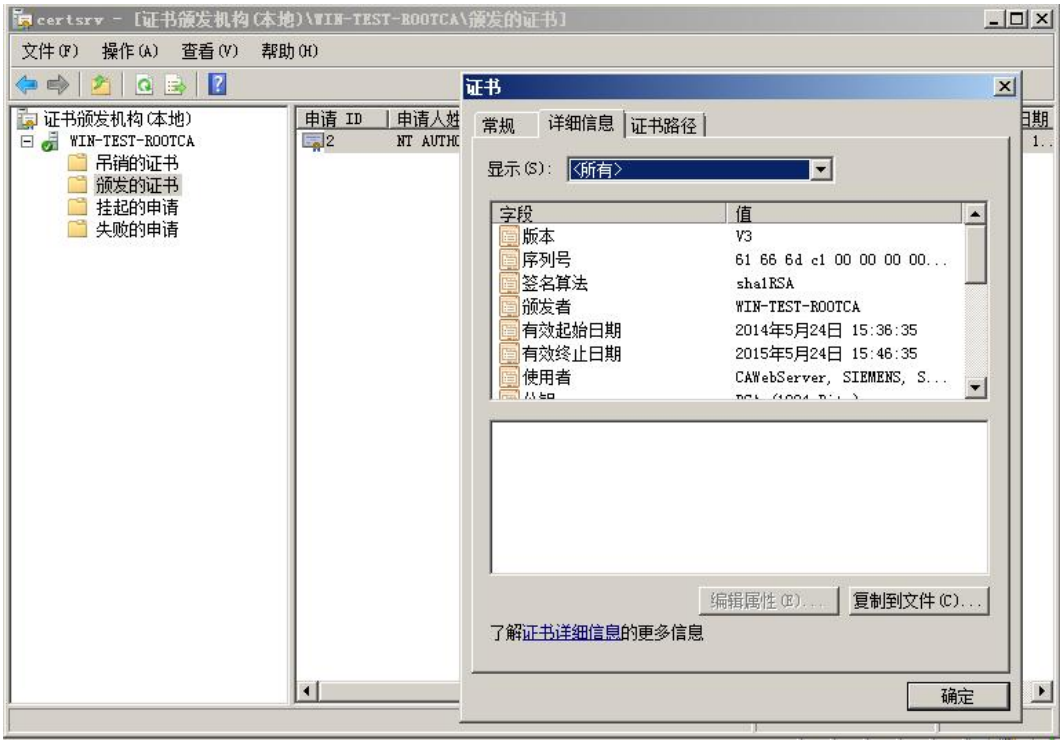

图 3-12 导出证书

证书颁发成功后，在颁发的证书目录中可以找到。双击打开，如图 3-12。选择复制到文件。

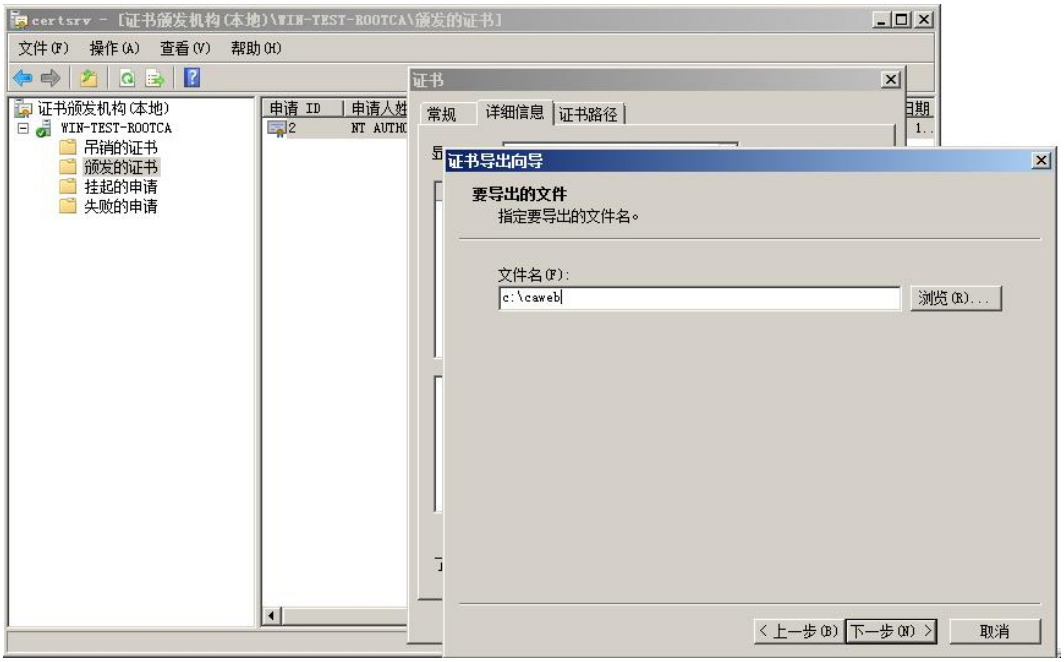

图 3-13 导出证书

如图 3-13，选择证书导出的目录和文件名。

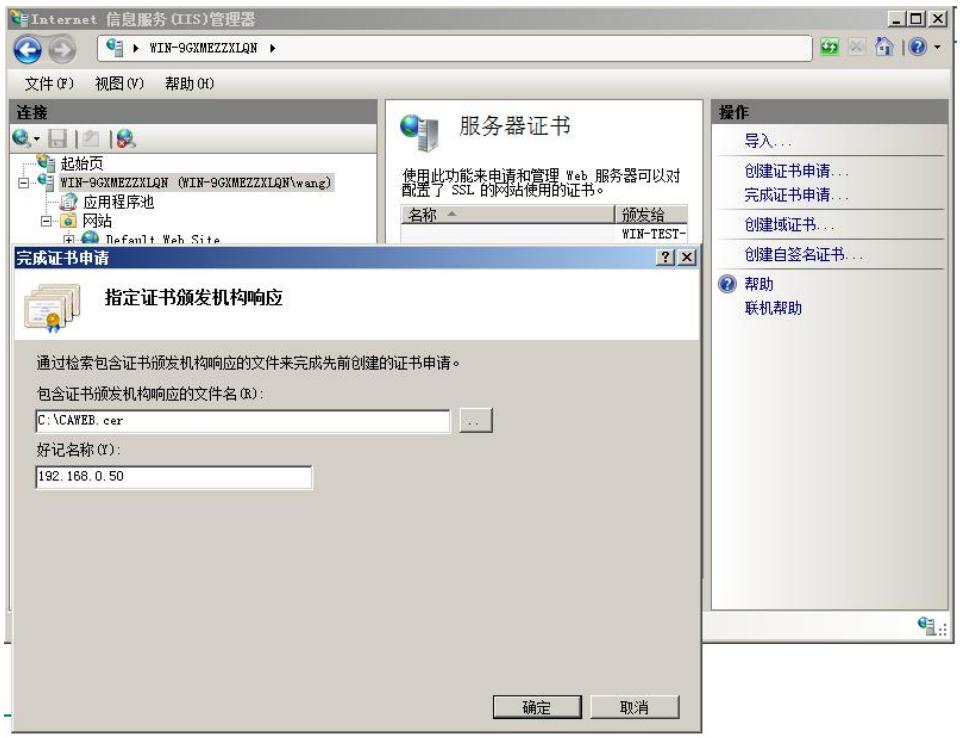

图 3-14 导入证书

打开 IIS 管理器，在左侧选择根目录，然后双击“服务器证书”打开。在右侧选择“完成证书申请”。选择刚才生成的证书，并起一个好记的名字。点击确认将证书导入。

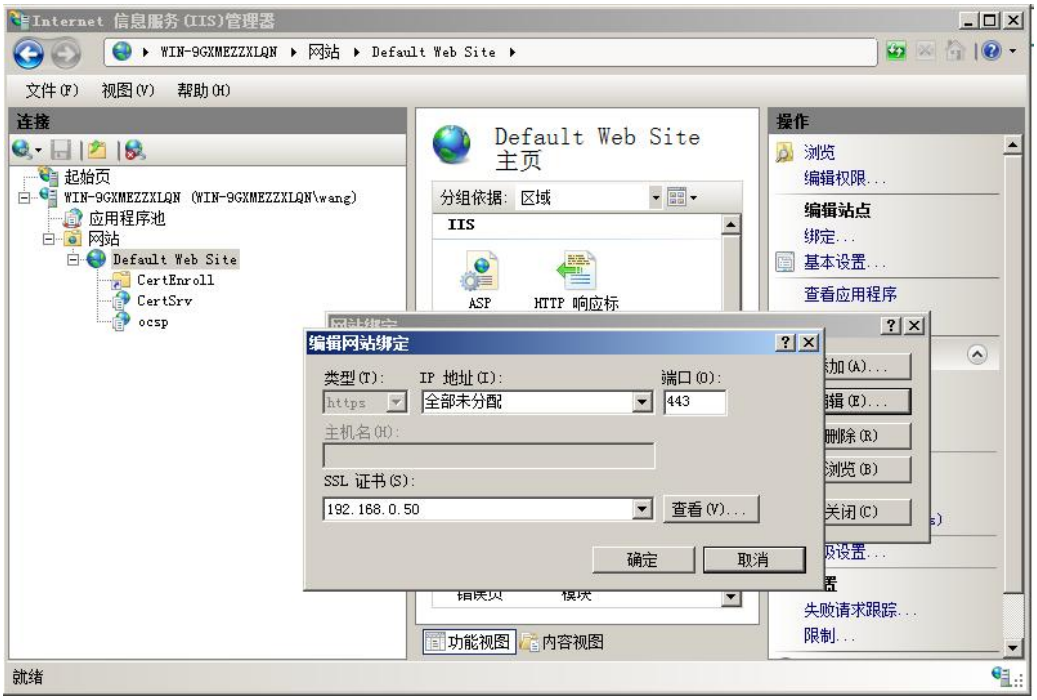

图 3-15 编辑网站绑定

在左侧目录中选择“ Default Web Sit"，然后再右侧点击“绑定”。在“网站绑定”对话框点击“添加”按钮，添加一个类型“ https"的绑定。IP 地址选择“全部未分配”，SSL 证书选择刚才生成的证书。

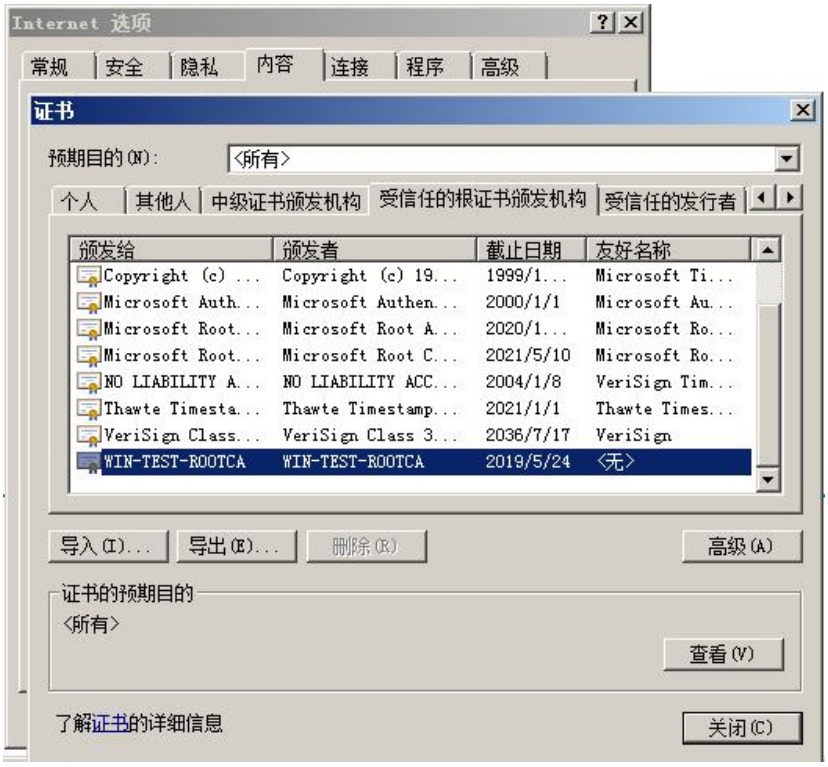

图 3-16 根证书颁发机构

在 IE 浏览器中选择工具菜单——内容页面，点击“证书”按钮打开如图 3-16 的界面。确认刚才创建的根证书颁发机构“ WIN-TEST-ROTCA”在受信任的根证书颁发机构中。

图 3-17 导出根证书颁发机构

如果要通过其它计算机申请数字证书。由于其它计算机中没有根证书颁发机构“WIN-TEST-ROTCA”用 HTTPS 访问时会报证书错误。所以首先要导入该根证书颁发机构。在服务器中的 IE 浏览器证书对话框中，如图 3-17，双击根证书颁发机构“WIN-TEST-ROTCA”，打开证书对话框，点击“复制到文件”，导出证书。然后再将导出的根证书颁发机构导入其它计算机。

4 给 SCALANCE X 申请数字证书

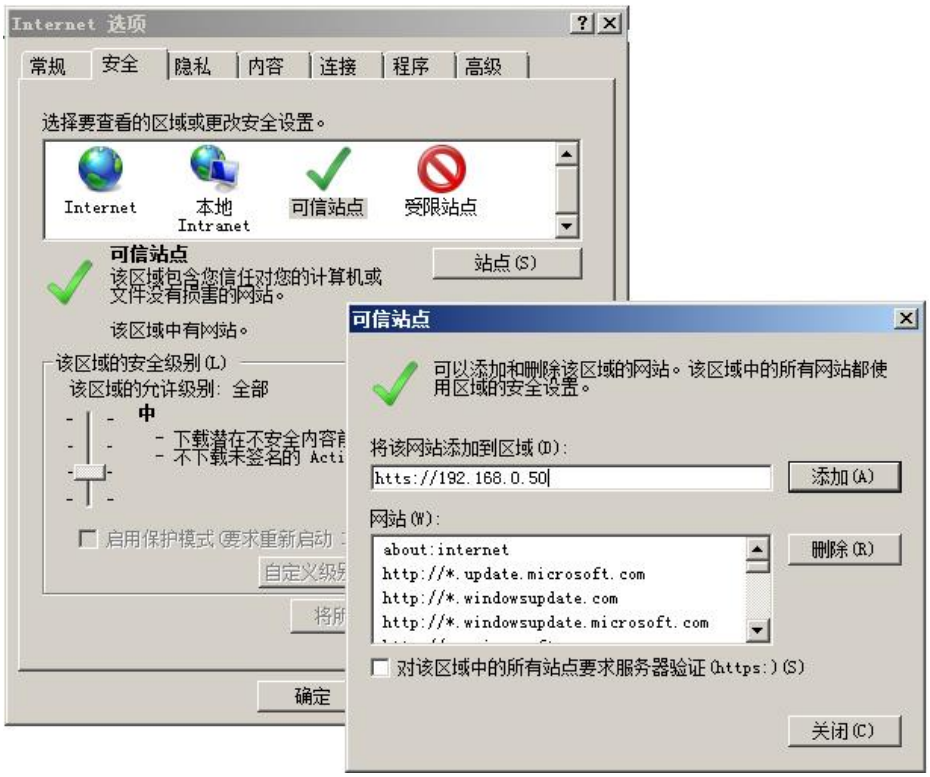

图 4-1 浏览器设置

在使用 HTTPS 给 SCALANCE X 申请数字证书前，需要对浏览器做一些设置。在“工具”菜单中，选择“Internet 选项”，打开“安全”页面。选择“可信站点”，然后将“https://192.168.0.50”添加到可信任站点中。

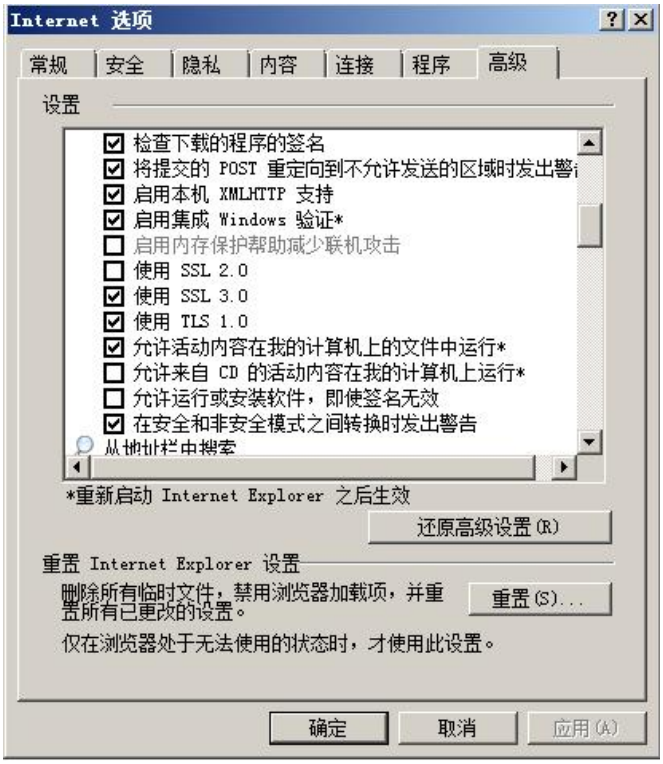

图 4-2 浏览器设置

在“高级”选项页中，勾选“允许活动内容在我的计算机上的文件中运行”。

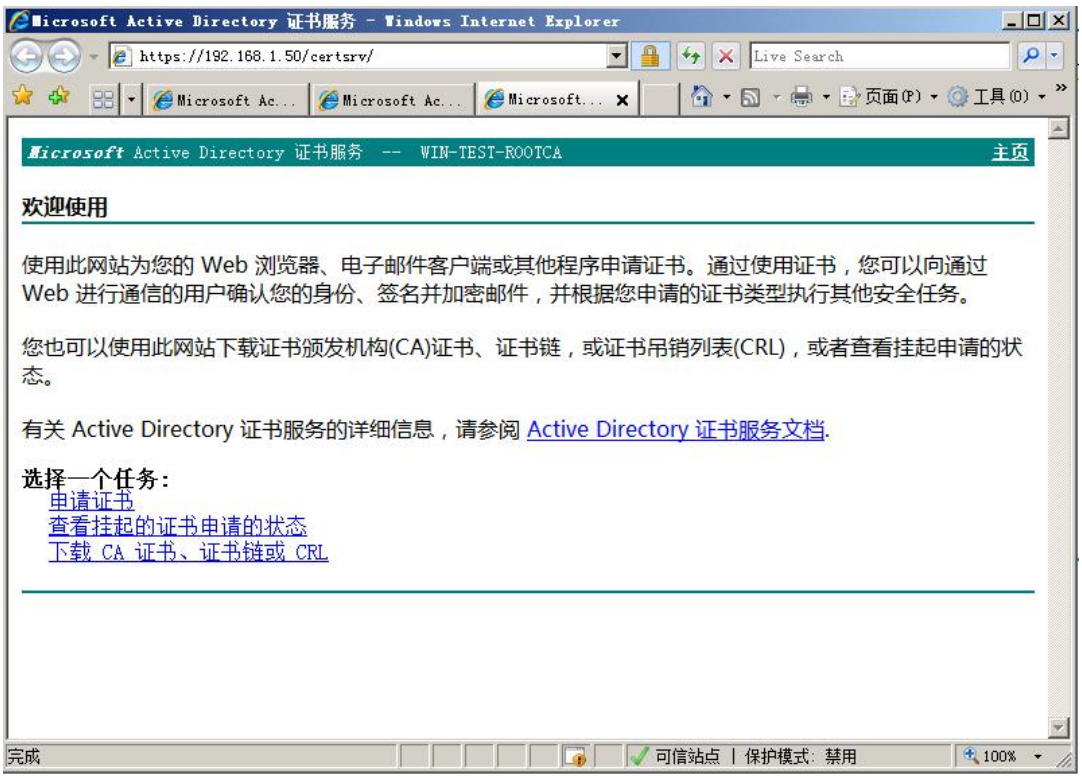

图 4-3 给 SCALANCE X 申请证书

在地址栏中输入“ https://192.168.1.50/certsrv/”，进入证书申请页面。

图 4-4 给 SCALANCE X 申请证书

在图 4-4 的页面中，选择高级证书申请。

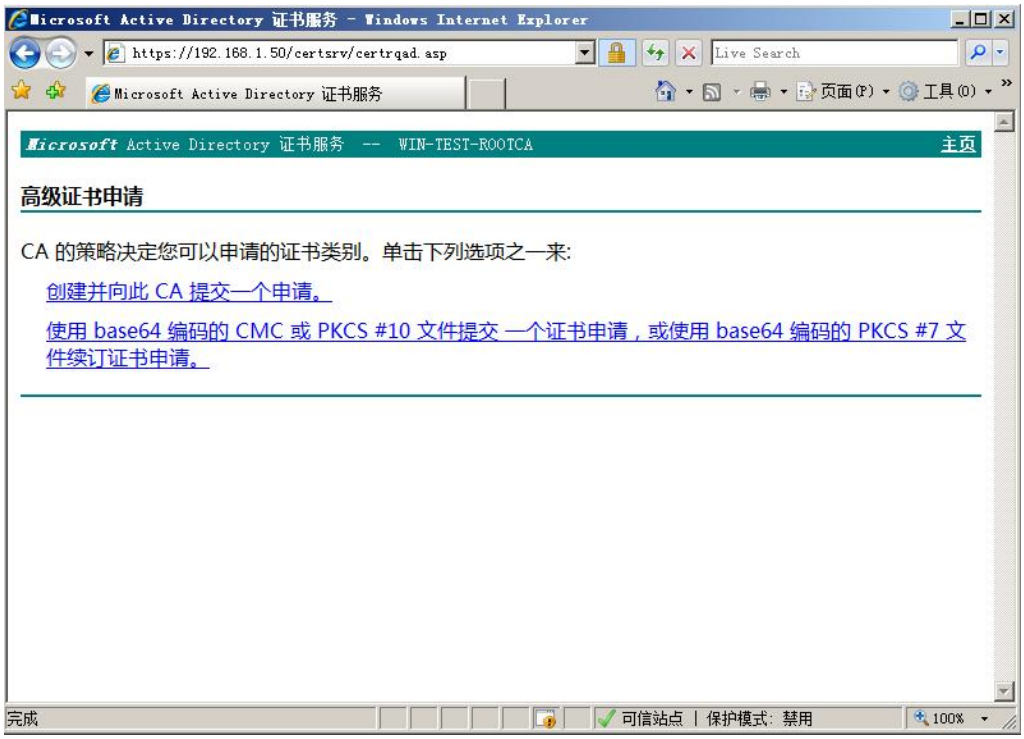

图 4-5 给 SCALANCE X 申请证书

在以上页面中选择“创建并向此 CA 提交一个申请”。

图 4-6 给 SCALANCE X 申请证书

在图 4-6 的页面中，填写申请数字证书必须的信息。姓名栏需要填写申请证书的交换机的 WEB 服务器域名，由于这里交换机没有使用域名，需要填写交换机的实际 IP 地址。必须勾选“标记密钥为可导出”选项。这样申请的数字证书私钥才能导出。

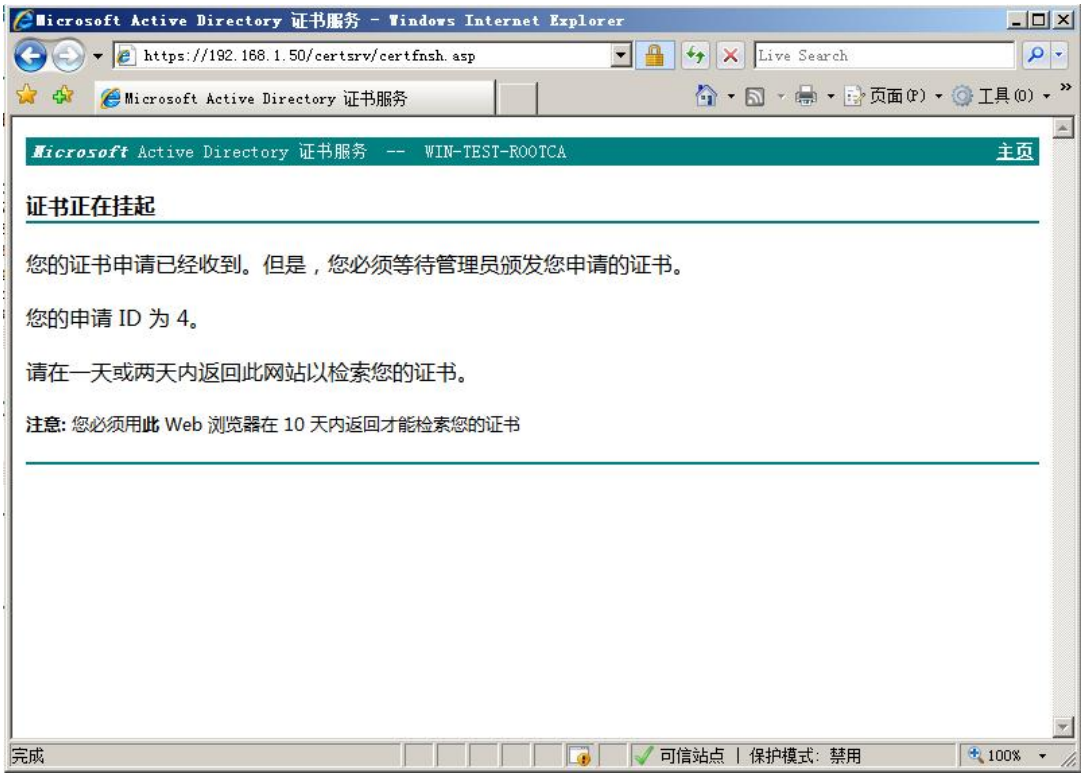

图 4-7 给 SCALANCE X 申请证书

提交数字证书申请成功后，如图 4-7 所示的页面。

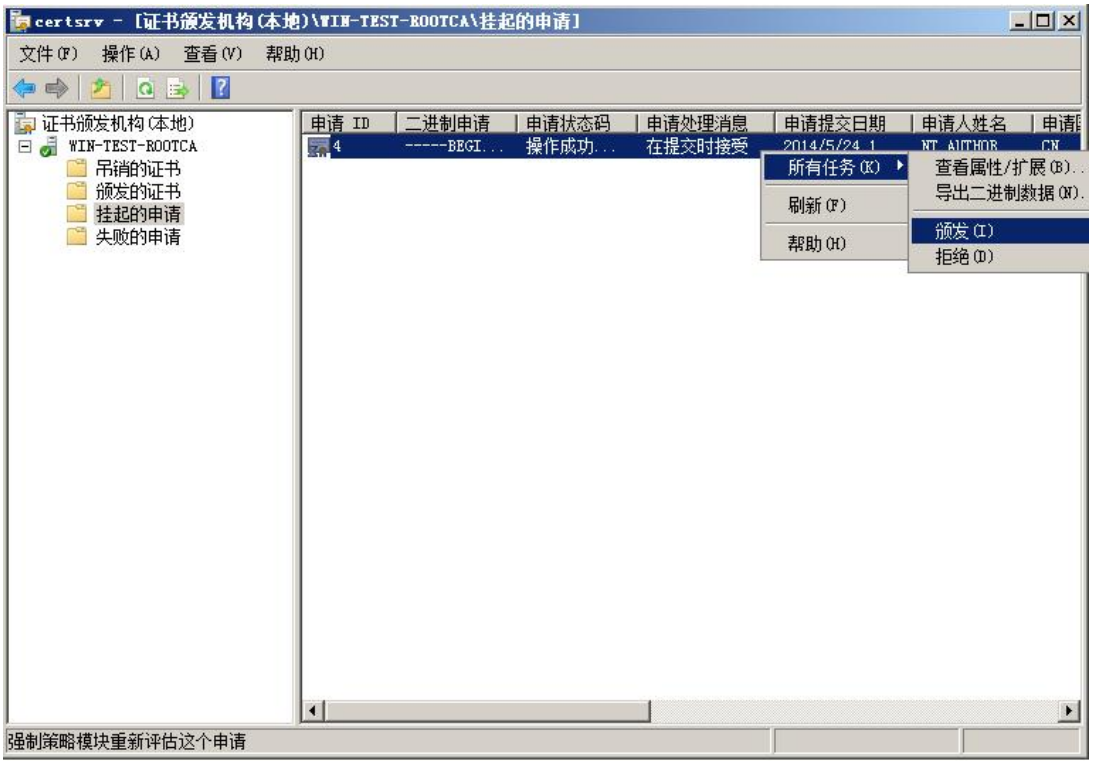

图 4-8 颁发证书

在“证书颁发机构”，挂起的申请目录中，找到该证书，并在右键菜单选择“颁发”。

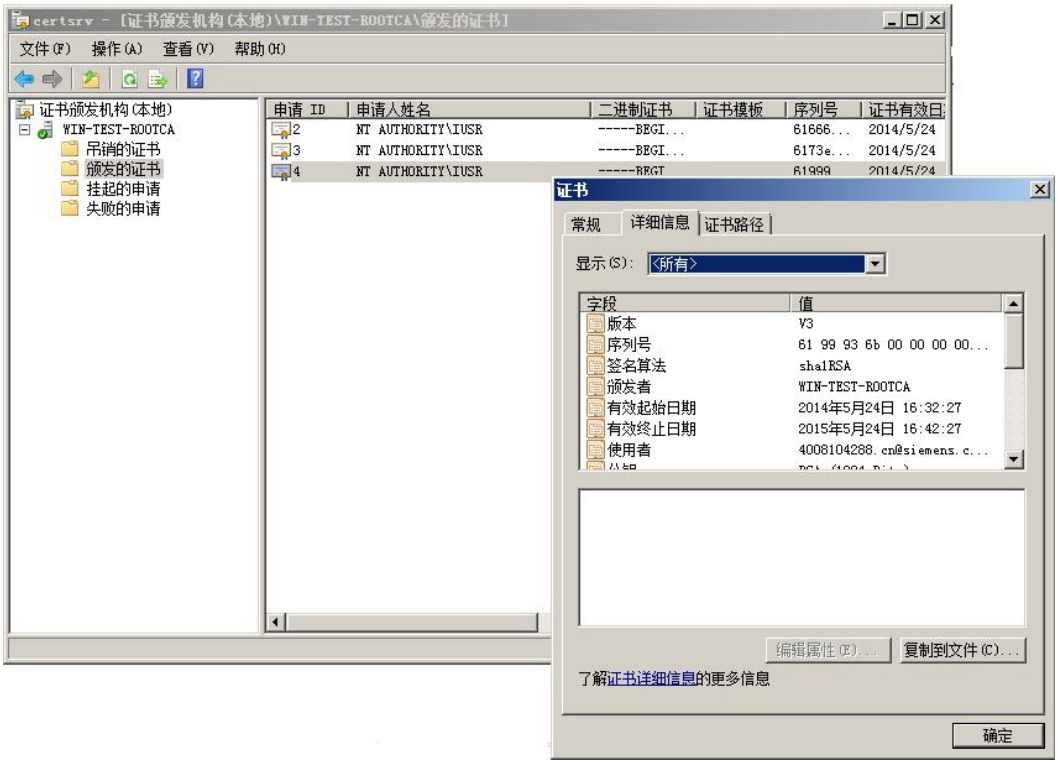

图 4-9 导出证书

双击颁发的证书，并点击“复制到文件”，将证书导出。

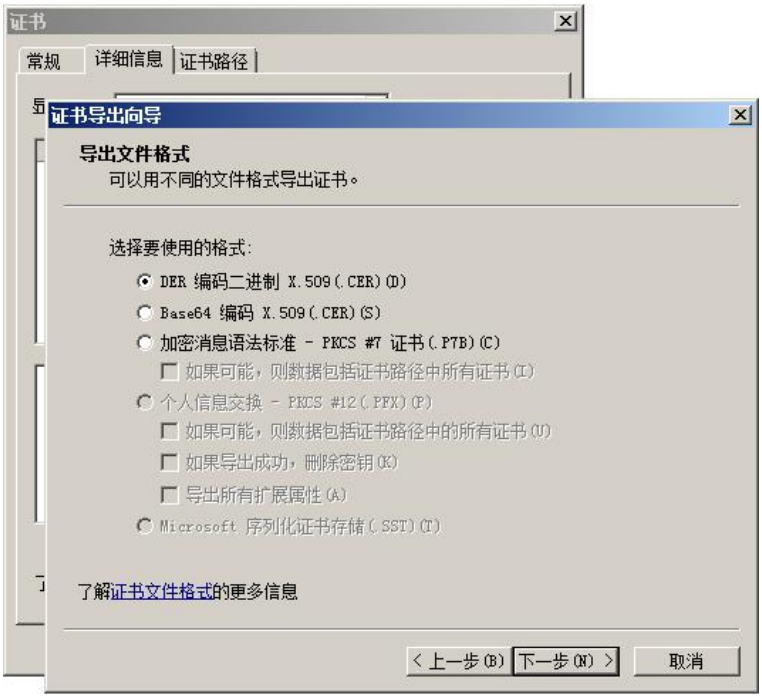

图 4-10 导出证书

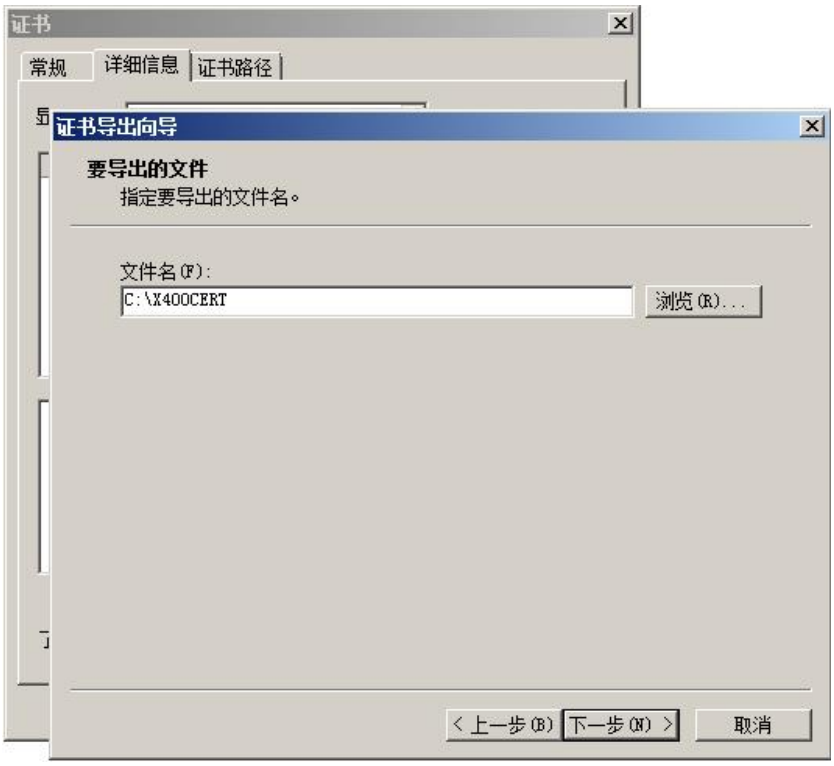

图 4-11 导出证书

图 4-12 导出证书

找到“X400CERT”文件，双击安装证书。然后在 IE 浏览器中找到安装的证书，如上图。然后再点击“导出”按钮。

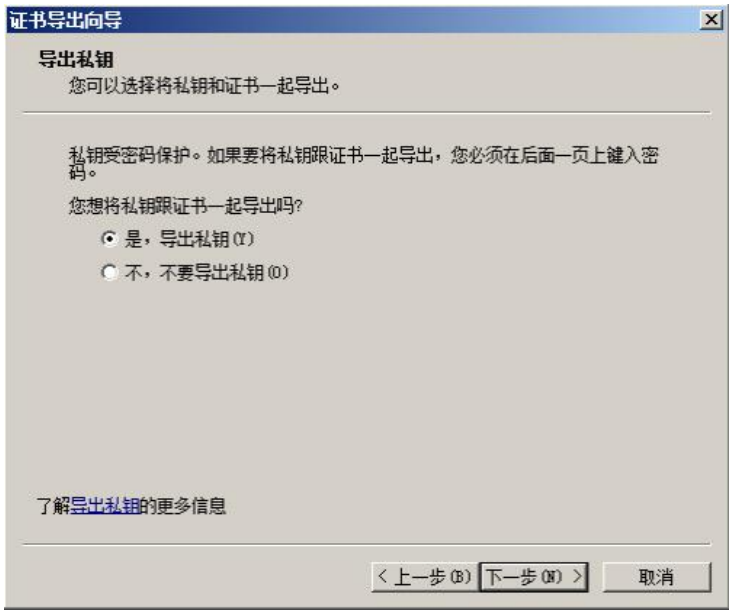

图 4-13 导出证书

在导出对话框中，如图 4-13 所示，选择“是，导出私钥”。

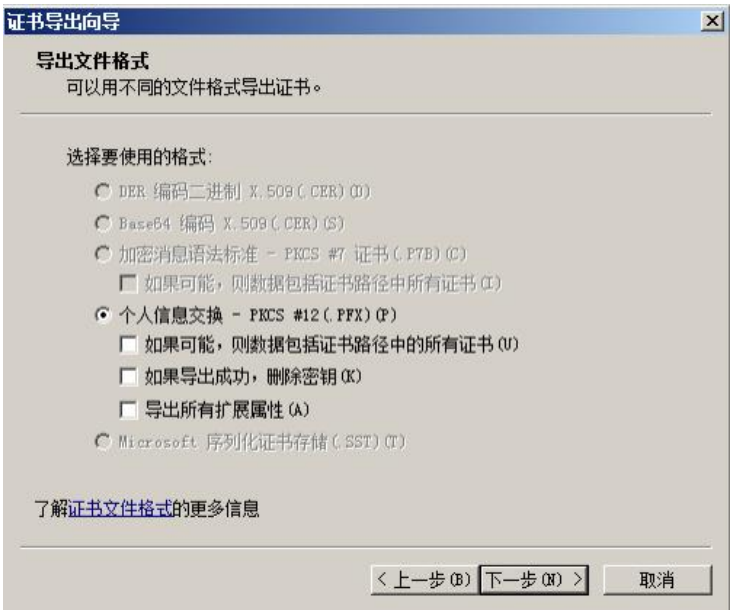

图 4-14 导出证书

图 4-15 导出证书

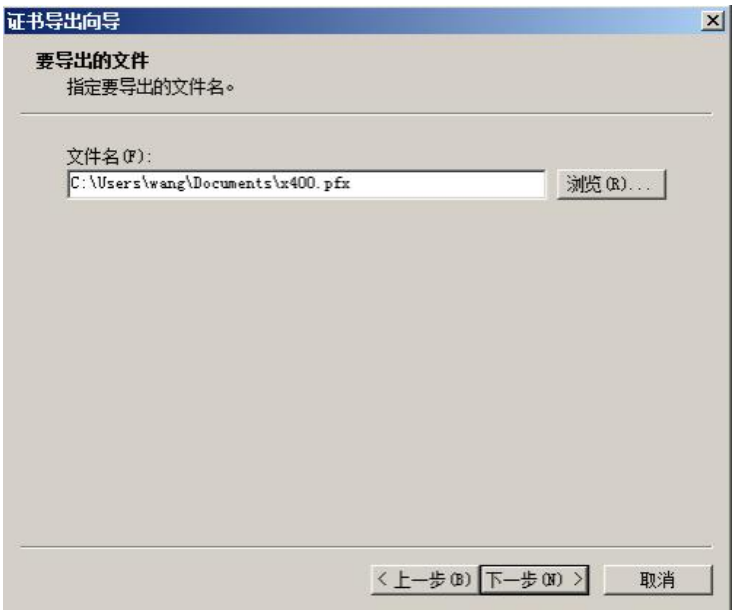

图 4-16 导出证书

证书的私钥需要密码保护，在图 4-15 的对话框中，输入用于保护私钥的密码

得到的证书是 PFX 格式，SCALANCE X400 需要 PEM 格式的证书。可以使用 OPENSSL 转换。OpenSSL 是免费软件，从以下链接下载：http://www.openssl.org/

可以从以下链接下载 WINDOWS 版本的 OpenSSL

http://www.openssl.org/related/binaries.html

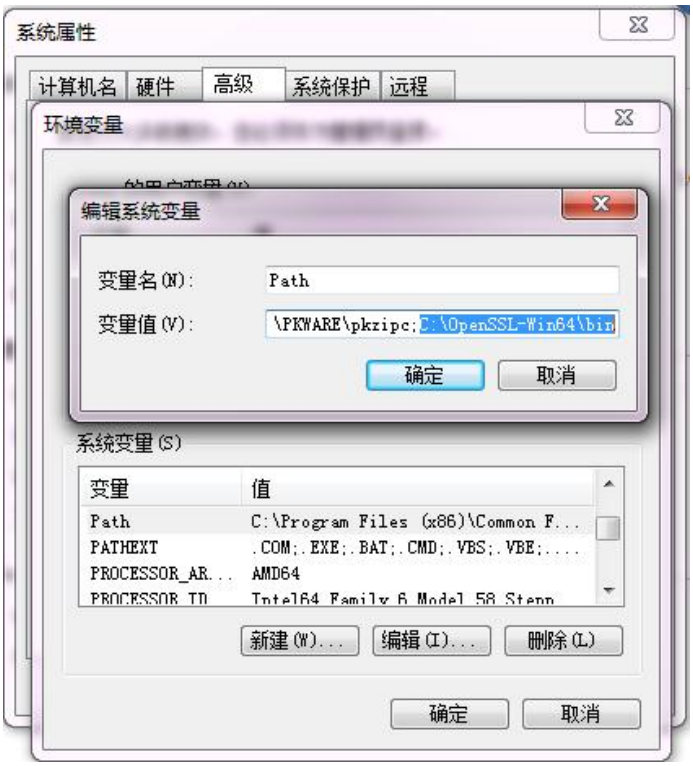

图 4-17 计算机环境变量设置

安装完 OPEN SSL 后，需要设置环境变量。右键选择“计算机——属性——高级系统设置——环境变量”。在环境变量“ Path”字符串中添加 OpenSSL 的安装路径，如图 4-17。

执行以下命令进行转换

pkcs12 -in X400CERT.pfx -out X400CERT.pem -nodes

转换的结果存放在 X400CERT 中。

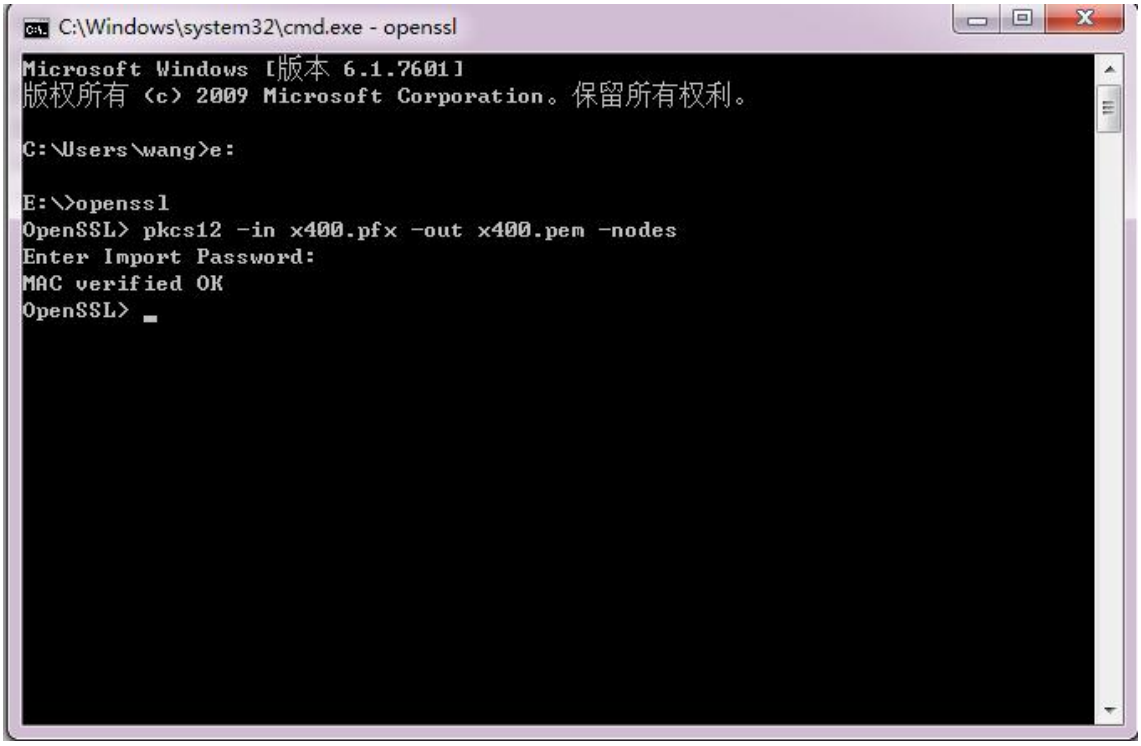

图 4-18 OpenSSL 指令

```
Bag Attributes
    localKeyID: 01 00 00 00
    friendlyName: le-8b599217-1c2e-419d-9e9b-37865cc9df0f
    Microsoft CSP Name: Microsoft Enhanced RSA and AES Cryptographic Provider
Key Attributes
    X509v3 Key Usage: 10
-----BEGIN PRIVATE KEY-----
MIICdgIBADANBgkqhkiG9w0BAQEFAASCAmAwggJcAgEAAoGBAMItTbm1m2Obe22K
vWSwrLn60vFAFxtxKsStTzevYX+7OXROHYhp2uYGMv2N2NwCHD1s2kgEIMC6qCmV
jD/cx8ML+ZAdMCHCJF/p7Khxs2a5ZrNmtCveQOf7YTaHaNbyD8Ve8YkK8cu6IQqw
sC3s6g4gVZ0iWI8GXnjLnhqZjrahAgMBAAECgYEAIK+btV9KYf+u39CPN5l3Fx4A
wIb196rUODPCiy9qADi7E6x29HB3RI8DGsmvb9Aa+ni0tH5fkwT2ByQ+UBHwXkmw
mE277ArwCEXQkk7WPTpjxTscZvtHdvg9MOZ+TDIrrUCJmQQzrKV4QtlpHbzosIn9
cOTzNUXsKZFVatF50nUCQQDrECiaEUmaP3v9jUSUQqM1d7/YxWZXOLJ1/gPugdDL
rQPnf4PJPLe4K6xuOwzuANtOD8blR885uwbLnJTYMPODAkEA214u5M+IUHiTxmT3
i6tNC4++bPjiOJxnXwAIz1ERRVEcWKieO3Q/3XYsanOsdyy8Kmr9snvmrr+MHL7h
5W5yiwJAIFhW3exnDlyR+S/JMgWBY8gYIAGFtZbNp8LOU7F1Q7GJCf/X6Ib8WNFZ
pt5PtyhTBQjSu5YIA8+ifb4MFTuYdQJAGKwoJA3/a+WT4U171hanLLS3GzSG5Q0a
ROIOu5qHkb9Eq+gTG+bARB1Fc5ec/y5l33N3IzryQBdFH/qMF6zrbwJAZMdi22wp
TyYEe8nua8fw1hrp59Kz6cinTdRhSRfH+gLAnSZ82AqP1PuAcU4ZfzKCt5t+rPtn
eHdcXgwfd6+Y2Q==
-----END PRIVATE KEY-----
Bag Attributes
    localKeyID: 01 00 00 00
    friendlyName: X400CERT
```

subject=/C=CN/ST=PEK/L=PEK/O=SIEMENS/OU=CS/CN=192.168.1.19/emailAddress=40081
04288.cn@siemens.com
issuer=/CN=WIN-TEST-ROOTCA
-----BEGIN CERTIFICATE-----
MIIERzCCAy+gAwIBAgIKYZ9AygAAAAAABTANBgkqhkiG9w0BAQUFADAaMRgwFgYD
VQQDEw9XSU4tVEVTVC1ST09UQ0EwHhcNMTQwNTI0MDgzODM5WhcNMTUwNTI0MDg0
ODM5WjCBiTELMAkGA1UEBhMCQ04xDDAKBgNVBAgTA1BFSzEMMAoGA1UEBxMDUEVL
MRAwDgYDVQQKEwdTSUVNRU5TMQswCQYDVQQLEwJDUzEVMBMGA1UEAxMMMTkyLjE2
OC4xLjE5MSgwJgYJKoZIhvcNAQkBFhk0MDA4MTA0Mjg4LmNuQHNpZW1lbnMuY29t
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDJbU25tZtjm3ttir1ksKy5+tLx
QBcbcSrErU83r2F/uzl0dB2ladrmBjL9jdjcAhw9bNplBCDAuqgplYw/3MfDC/mQ
HTAhwiRf6eyocbNmuWazZrQr3kDn+2E2h2jW8g/FXvGJCvHLuiEKsLAt7OoOlFWd
IliPBl54y54amY62oQIDAQABo4IBoTCCAZ0wDgYDVR0PAQH/BAQDAgTwMBMGA1Ud
JQQMMAoGCCsGAQUFBwMBMB0GA1UdDgQWBBRJt96+BR3TlFD5swe0zSTG3Fi8njAf
BgNVHSMEGDAWgBRtPWwnYMNGLBDpY8EFVoeRP6mMPTB9BgNVHR8EdjB0MHKgcKBu
hjVodHRwOi8vd2luLTIneG1lenp4bHFuL0NlcnRFbnJvbGwvV0lOLVRFU1QtUk9P
VENBLmNybIY1ZmlsZTovL1dJTi05R1hNRVpaWExRTi9DZXJ0RW5yb2xsL1dJTi1U
RVNULVJPT1RDQS5jcmwwgbYGCCsGAQUFBwEBBIGpMIGmMFEGCCsGAQUFBzAChkVo
dHRwOi8vd2luLTIneG1lenp4bHFuL0NlcnRFbnJvbGwvV0lOLTIHWE1FWlpYTFFO
X1dJTi1URVNULVJPT1RDQS5jcnQwUQYIKwYBBQUHMAKGRWZpbGU6Ly9XSU4tOUdY
TUVaWlhMUU4vQ2VydEVucm9sbC9XSU4tOUdYTUVaWlhMUU5fV0lOLVRFU1QtUk9P
VENBLmNydDANBgkqhkiG9w0BAQUFAAOCAQEApDgP/vUV4XKdKtSumgxvqAir+9Um
2qfa5RmemWROsalzMkk3dv1qV9NL3iFreRpAEyuhFOu10XGj5fwQrBmgxbbtdnok
UBbR+1hTwD6pgcHG7P6bxXXPKgBaEsZ8aQU1Q5KYOmscjpBD248/e7QjkAAvNWXR
Wh248qYfj6EmMznxYwcKRQya0OTeHPo7eOhXL9xtKFfllTigpz+Vy29ZbDHfbQ4i
DgQVeMwCBnI7CAqnP1xUIjMfja06z3L6hq59xgnZl1sf2h4P+UkoeMLmI5lqF7vm
H6npkiAF+OHojaBzY4ZZnuzkWhlJamRMAnK8hsD/wM+/KzKVgpEWnkP8qg==
-----END CERTIFICATE-----

如上所示是生成的 PEM 文件。上半部分红色部分是私钥，下半部分是证书。由于 Scalance X400 需要分别导入私钥和证书。这里将红色和绿色部分分别拷贝到不同的“ txt ”记事本文件中。保存完毕后，再将记事本文件的扩展名“ txt ”更改为扩展名“ pem ”。将私钥部分保存为 x400key.pem，将证书部分保存为 x400cert.pem，分别导入交换机中，如下图。

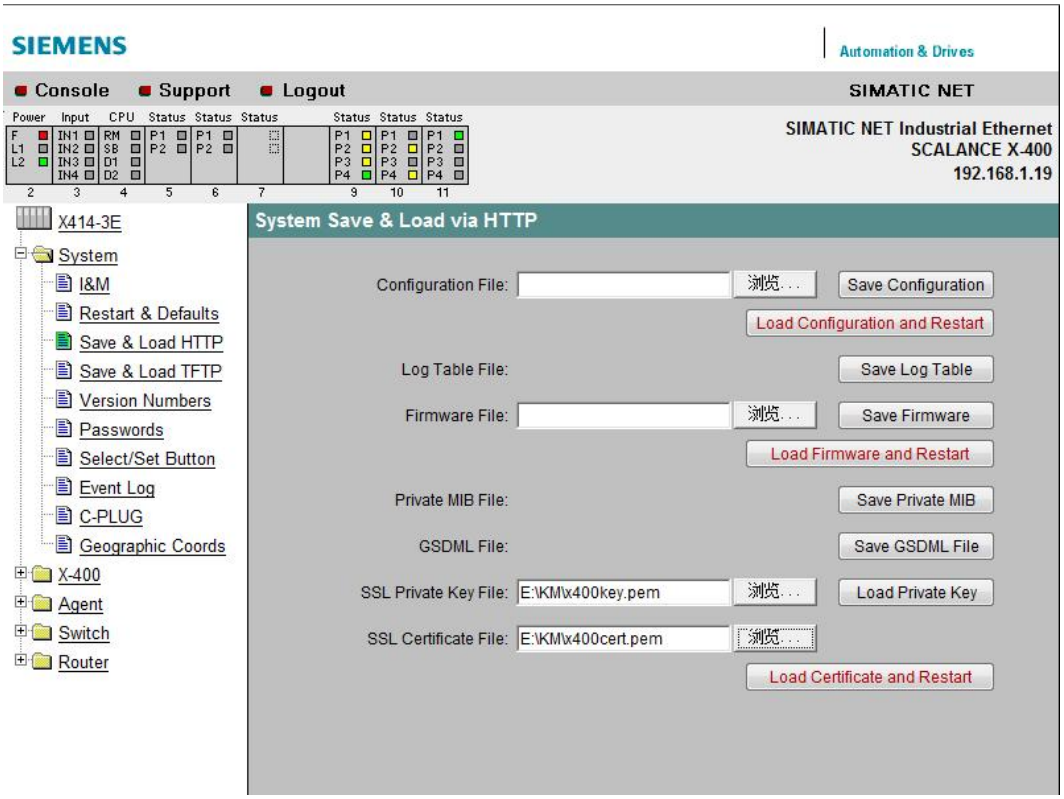

图 4-19 导入证书和私钥

如图 4-19 所示，进入 SCALANCE X414-3E 的管理界面，“System”菜单下选择“Save&Load HTTP”。在“SSL Private Key File”中导入刚才生成的密钥，在“SSL Certificate File”中导入证书部分。先点击“Load Private Key”导入密钥，然后点击“Load Certificate and Restart”导入证书。注意：导入证书后交换机会自动重启。

以上操作完成后，在 IE 浏览器输入 https://192.168.1.19 通过 IE 浏览器的方式试图进入会出现如下图界面。

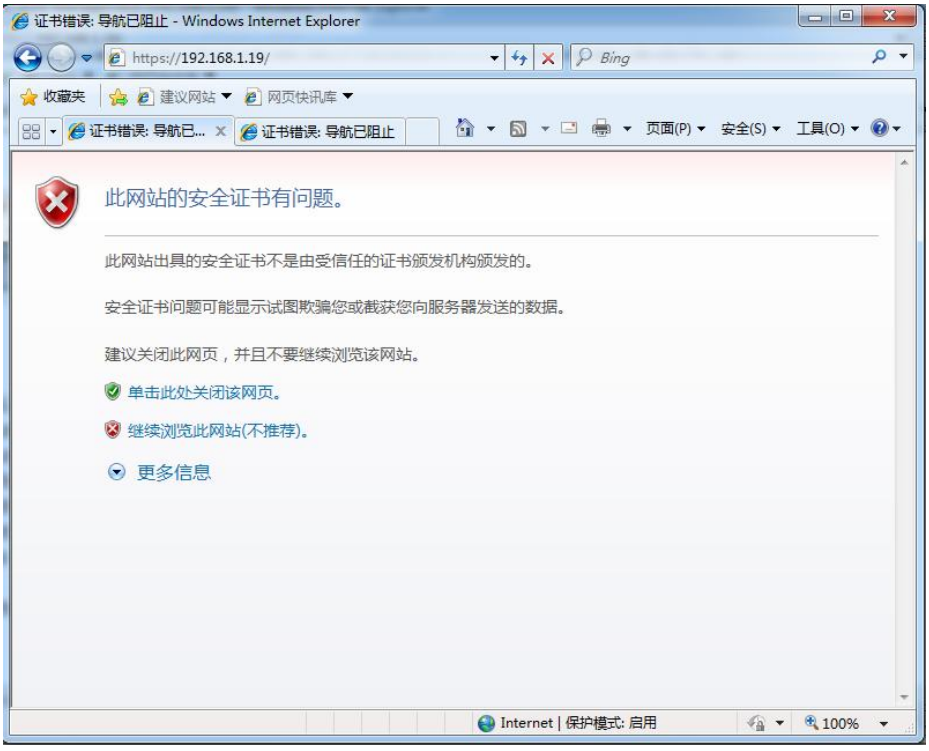

图 4-20 交换机 HTTPS 登录界面

点击“继续浏览此网站”，会提示证书错误。

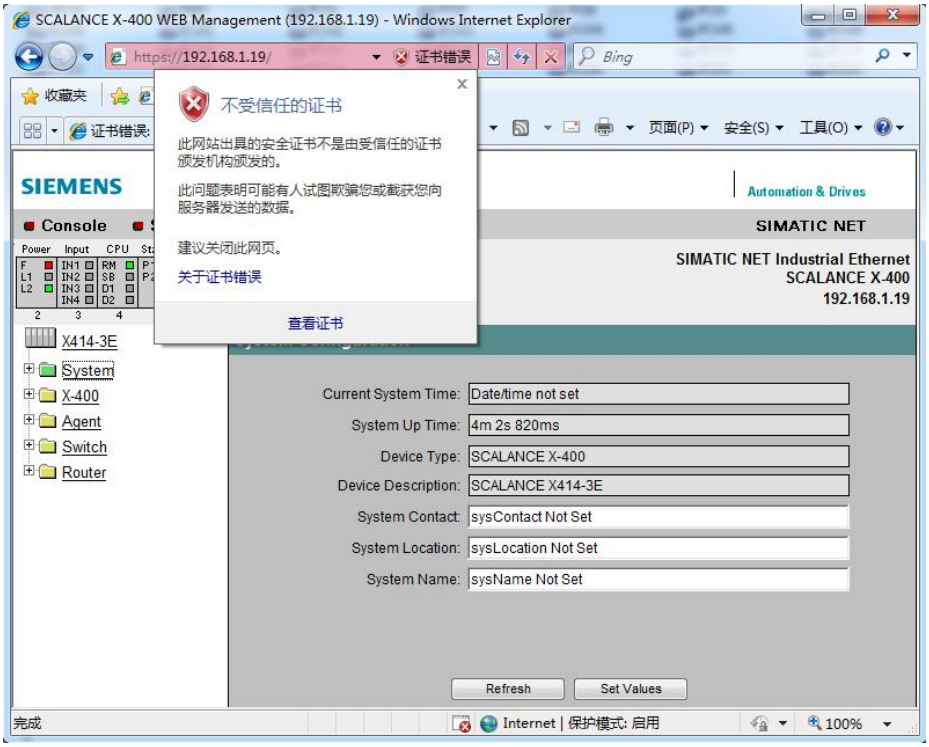

图 4-21 证书错误页面

点击查看证书，可以看到该证书是颁发给“ WIN-TEST-ROOTCA”，由于我们的 PC 没有信任该 CA，所以报证书错误。

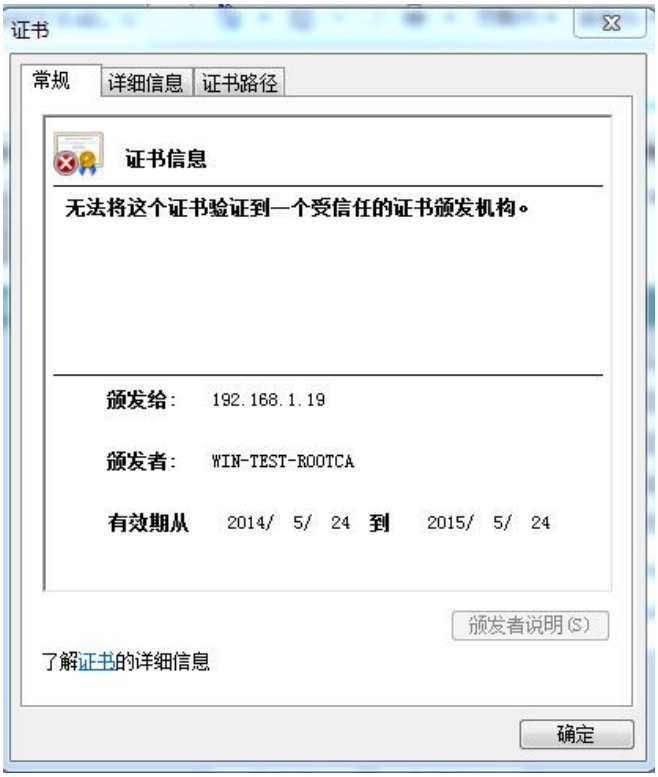

图 4-22 证书错误

现在将图 3-17 中导出的证书导入到访问交换机的 PC 中来，如下图。将证书导入到信任的根证书颁发机构中来。

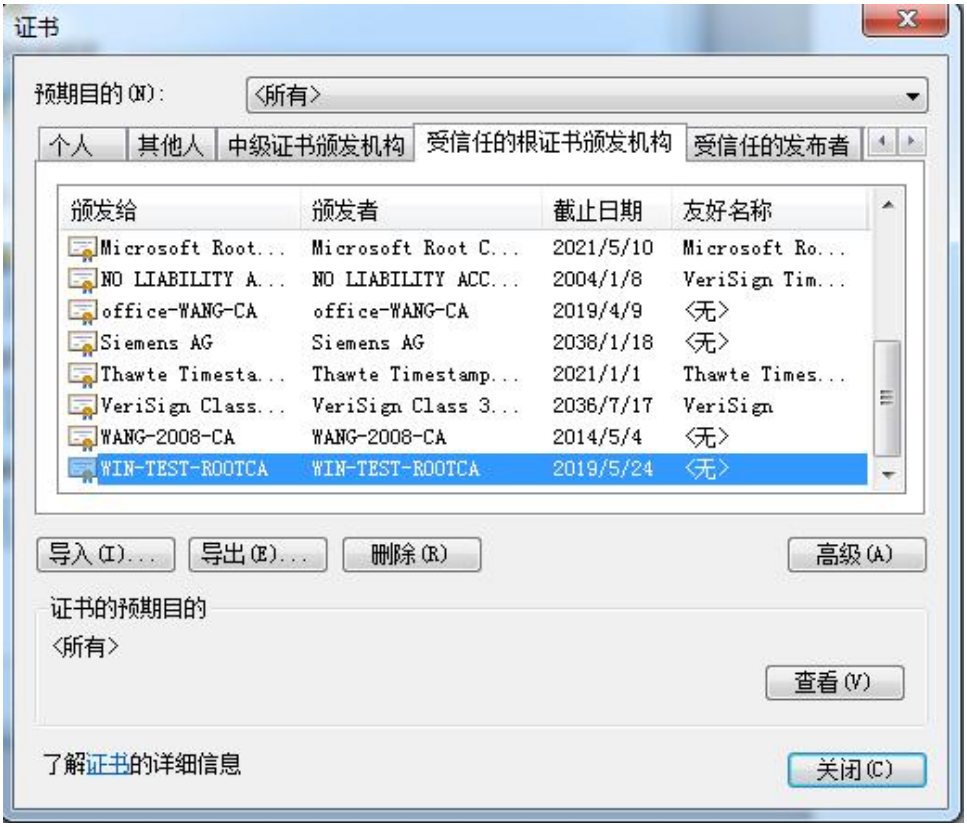

图 4-23 信任的根证书颁发机构

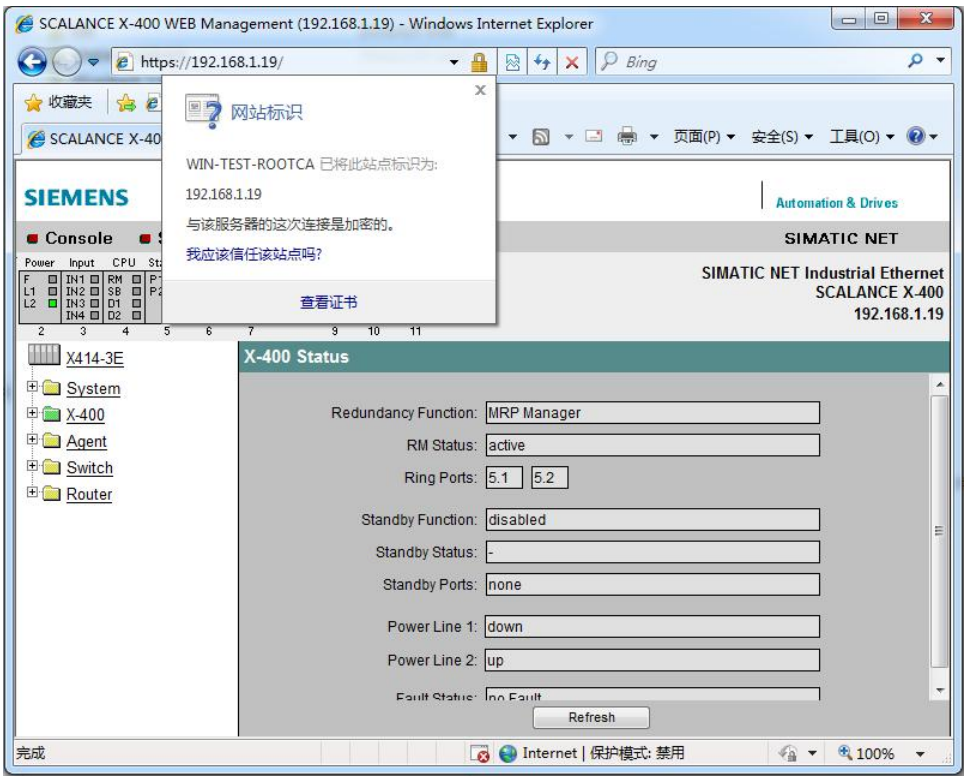

图 4-24 用 HTTPS 打开交换机管理页面

证书安装成功后，重新打开 IE 浏览器，输入交换机的 IP 地址，可以看到如图 4-24 的界面。网页不再报错，点击小锁图标，可以看到该站点信任的根证书名称，并提示通信是加密的。

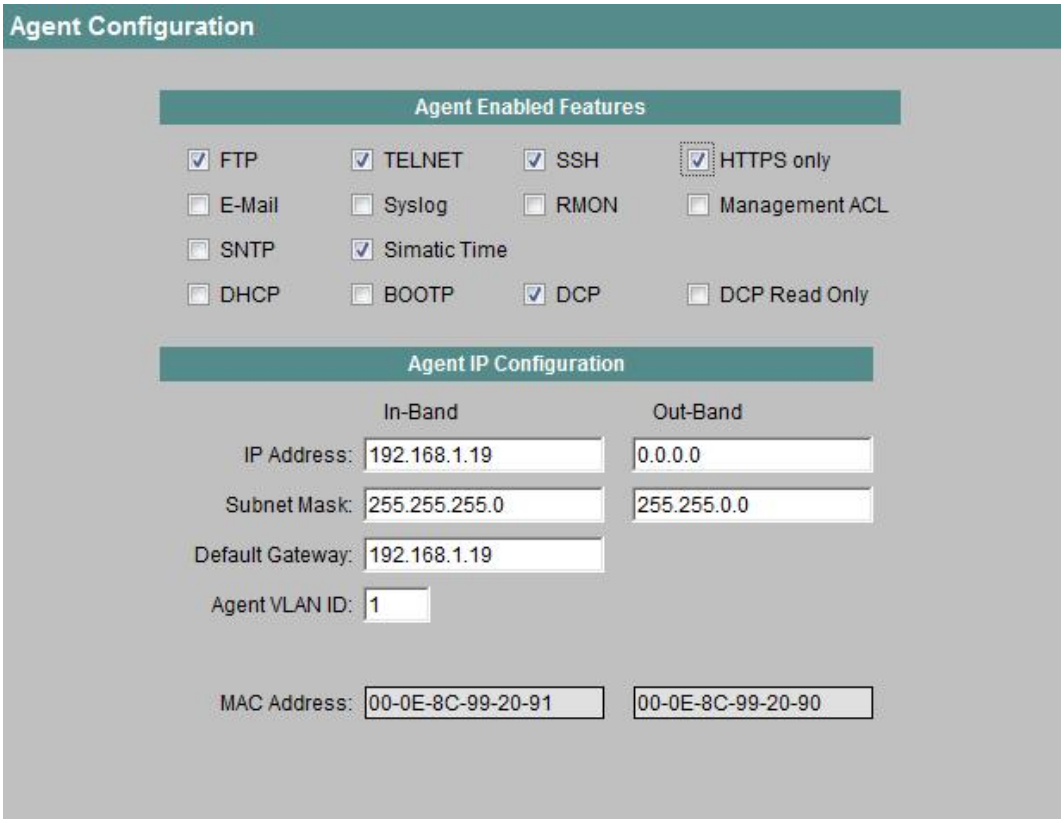

图 4-25 SCALANCE X Agent 设置

为了提高安全性，可以限定交换机只允许 HTTPS 方式访问。如上图所示，在 SCALANCE X414-3E 交换机管理页面左侧目录树选择“ Agent”。然后勾选“ HTTPS only ”选项。