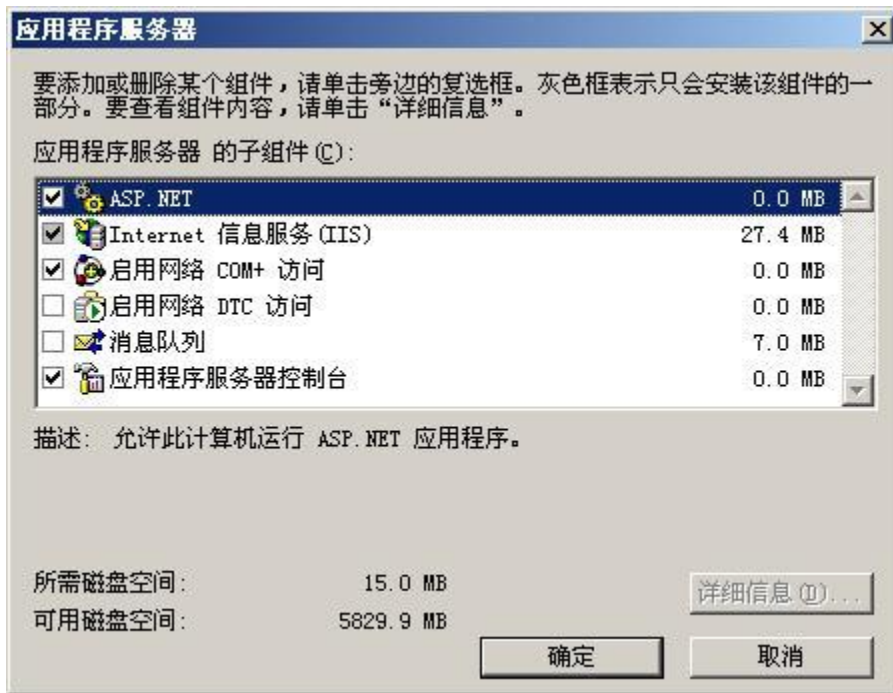


# Windows CA 服务器配置

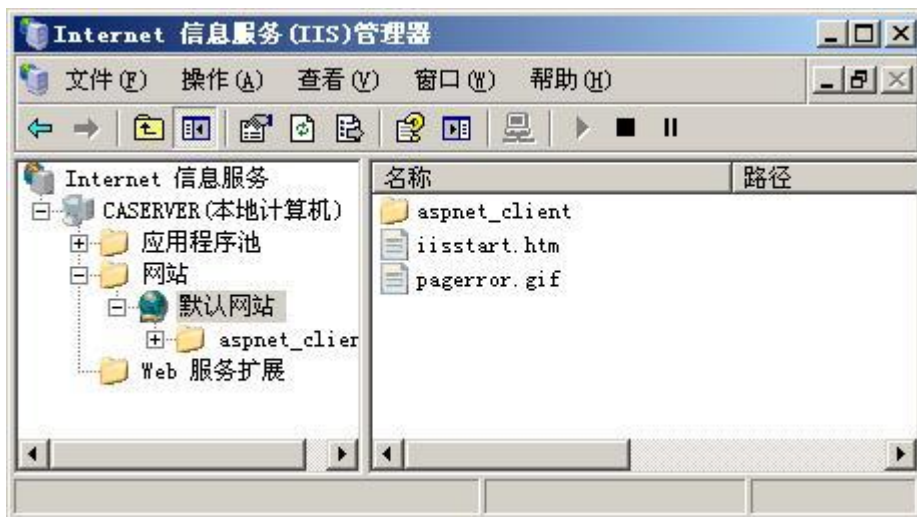
## 1 Microsoft 证书服务安装

安装准备：插入 Windows Server 2003 系统安装光盘

添加 IIS 组件：



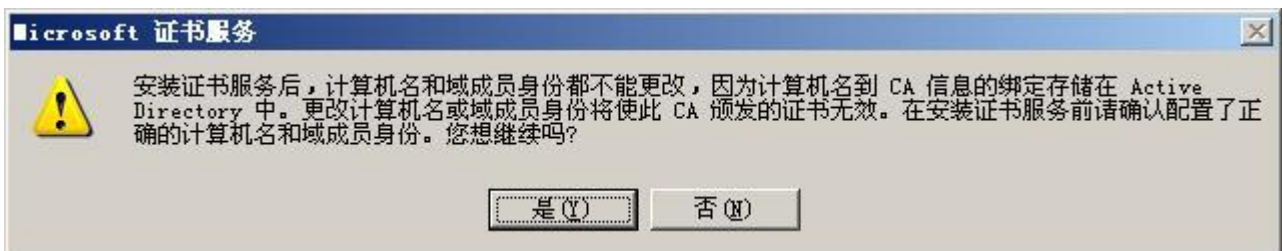
点击‘确定’，安装完毕后，查看 IIS 管理器，如下：



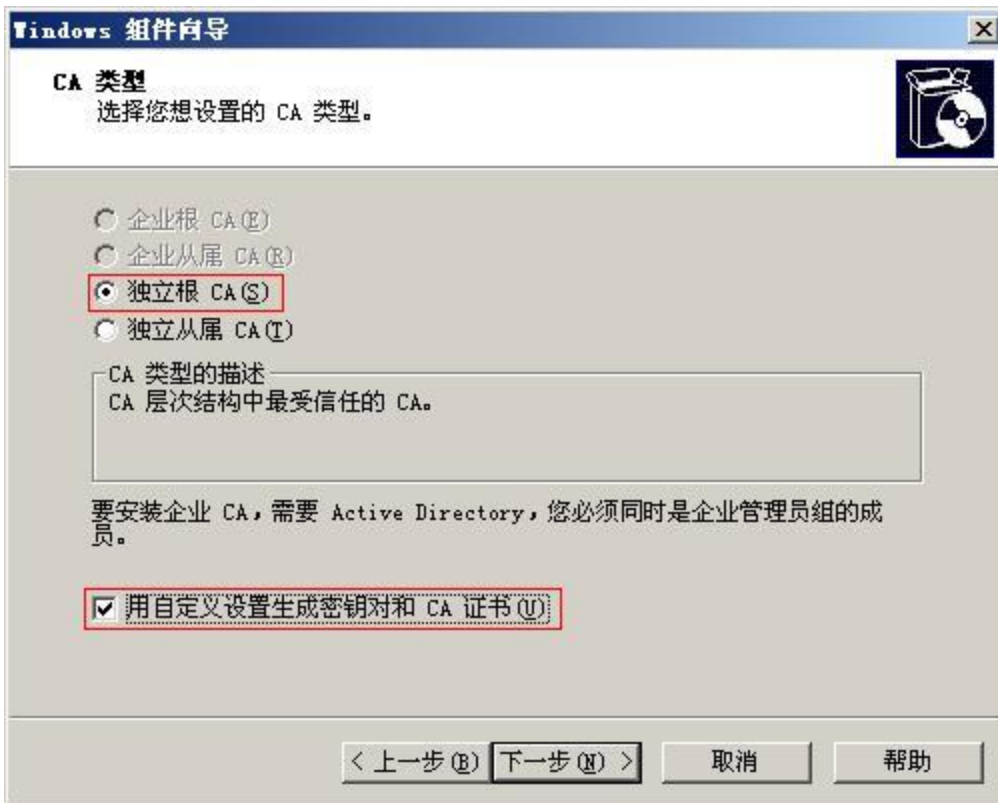
添加‘证书服务’组件：



如果您的机器没有安装活动目录，在勾选以上‘证书服务’时，将弹出如下窗口：



由于我们将要安装的是独立 CA，所以不需要安装活动目录，点击‘是’，窗口跳向如下：



默认情况下，‘用自定义设置生成密钥对和 CA 证书’没有勾选，我们勾选之后点击‘下一步’可以进行密钥算法的选择：



Microsoft 证书服务的默认 CSP 为：Microsoft Strong Cryptographic Provider，默认散列算法：SHA-1，密钥长度：2048——您可以根据需要做相应的选择，这里我们使用默认。点击‘下一步’：



填写 CA 的公用名称（以 AAAAA 为例），其他信息（如邮件、单位、部门等）可在‘可分辨名称后缀’中添加，有效期限默认为 5 年（可根据需要作相应改动，此处默认）。

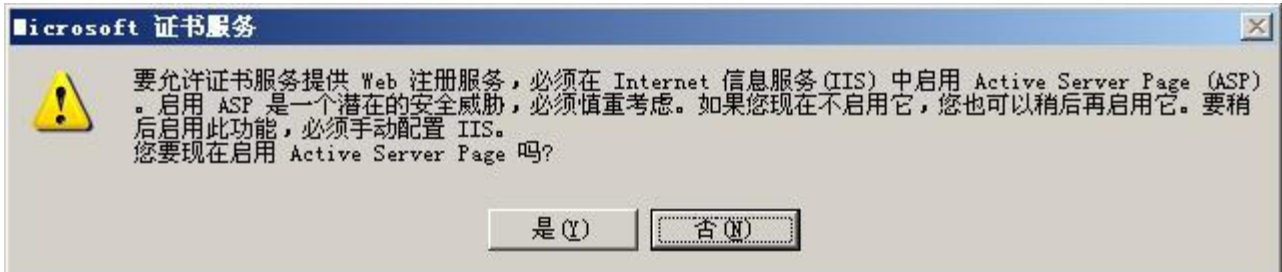
点击‘下一步’：



点击‘下一步’进入组件的安装，安装过程中可能弹出如下窗口：



单击‘是’，继续安装，可能再弹出如下窗口：



由于安装证书服务的时候系统会自动在 IIS 中（这也是为什么必须先安装 IIS 的原因）添加证书申请服务，该服务系统用 ASP 写就，所以必须为 IIS 启用 ASP 功能，点击‘是’继续安装：



‘完成’证书服务的安装。

开始 》 》 》 管理工具 》 》 》 证书颁发机构，打开如下窗口：



我们已经为服务器成功配置完公用名为 AAAAA 的独立根 CA，Web 服务器和客户端可以通过访问该服务器的 IIS 证书申请服务申请相关证书。

此时该服务器（CA）的 IIS 下多出以下几项：



我们可以通过在浏览器中输入以下网址进行数字证书的申请：

<http://hostname/certsrv> 或 <http://hostip/certsrv>

申请界面如下：

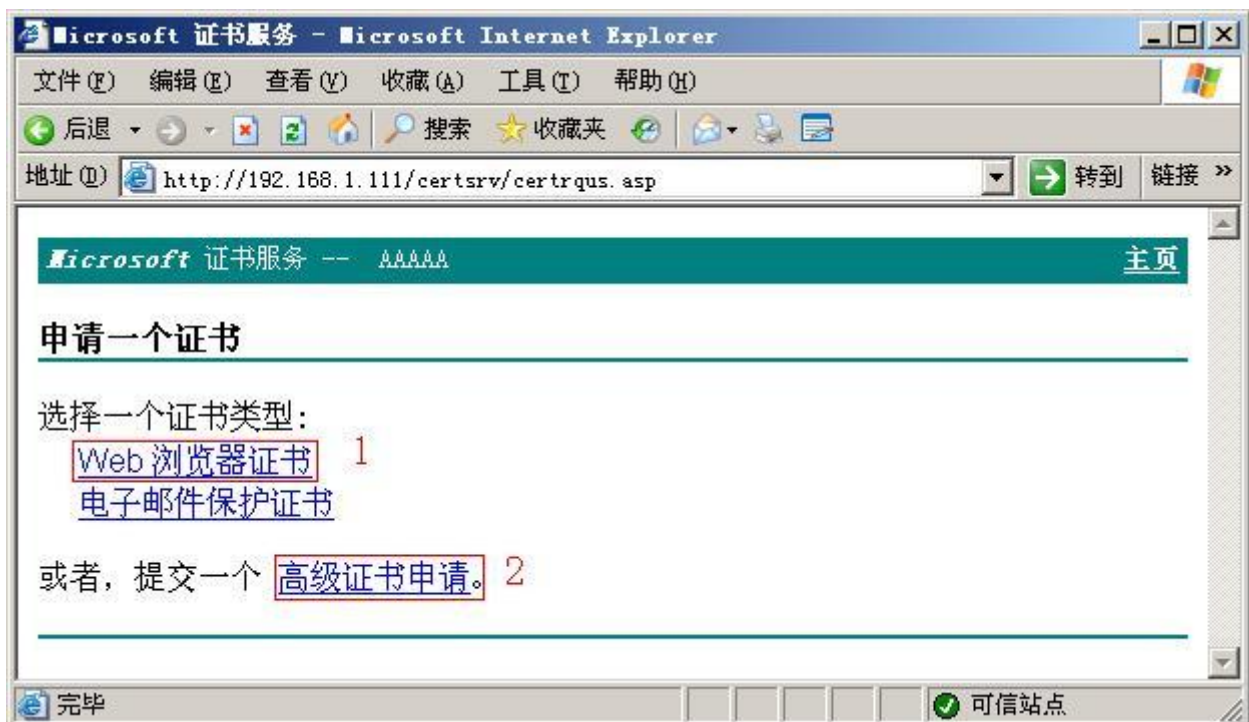


## 2 申请数字证书

在 IE 地址栏中输入证书服务系统的地址, 进入服务主页:



点击‘申请一个证书’进入申请页面:



如果证书用作客户端身份认证，则可点击‘Web 浏览器证书’或‘高级证书申请’，一般用户申请‘Web 浏览器证书’即可，‘高级证书申请’里有更多选项，也就有很多专业术语，高级用户也可点击进入进行申请。

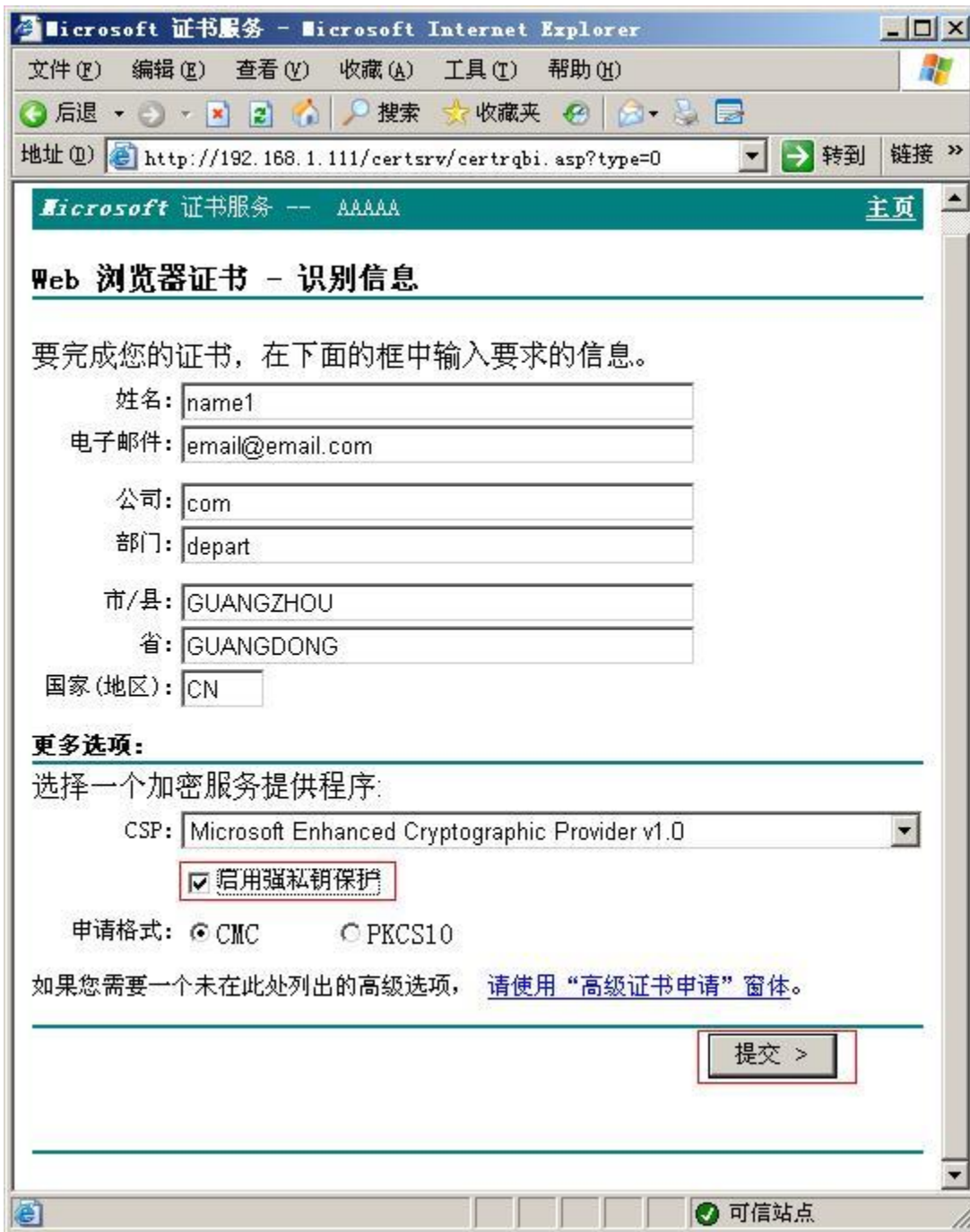
这里我们以点击申请‘Web 浏览器证书’为例：

The screenshot shows a web browser window titled 'Microsoft 证书服务 - Microsoft Internet Explorer'. The address bar shows 'http://192.168.1.111/certsrv/certrqbi.asp?tyj'. The page content includes a header 'Microsoft 证书服务 -- AAAAAA' and a main heading 'Web 浏览器证书 - 识别信息'. Below the heading is a prompt: '要完成您的证书，在下面的框中输入要求的信息。'. The form consists of several input fields: '姓名: name1' (with a red box and '必填项' label), '电子邮件: email@email.com', '公司: com', '部门: depart', '市/县: GUANGZHOU', '省: GUANGDONG', and '国家(地区): CN'. A '更多选项 >>' link is located below the form. At the bottom of the form area is a '提交 >' button. The browser's status bar at the bottom indicates '可信站点' (Trusted Site).

申请‘Web 浏览器证书’，‘姓名’是必填项，其他项目可不填，但由于 CA 服务器的管理员是根据申请人的详细信息决定是否颁发的，所以请尽量多填，并且填写真实信息，因为 CA 管理员会验证申请人的真实信息，然后进行颁发。

需注意的一点是，‘国家（地区）’需用国际代码填写，CN 代表中国。

如果想查看更多选项，请点击‘更多选项’：



在‘更多选项’里，默认的 CSP 为 Microsoft Enhanced Cryptographic Provider v1.0，选择其他 CSP 不会对认证产生影响。

默认情况下‘启用强私钥保护’并没有勾选上，建议将它勾选上，点击提交后就会让申请人设置证书的安全级别，如果不将安全级别设置为高级并用口令进行保护，则只要机器上装有该证书，任何人都可以用它作为认证，所以建议将证书设置为高级安全级别，用口令进行保护。以下将作相应操作，点击‘提交’：



单击‘是’：



单击‘设置安全级别’：



将安全级别设置为‘高’，单击‘下一步’后会弹出口令设置窗口：



输入口令，对证书进行加密，并记住密码，因为在以后调用该证书的时候，浏览器会弹出输入密码的窗口。

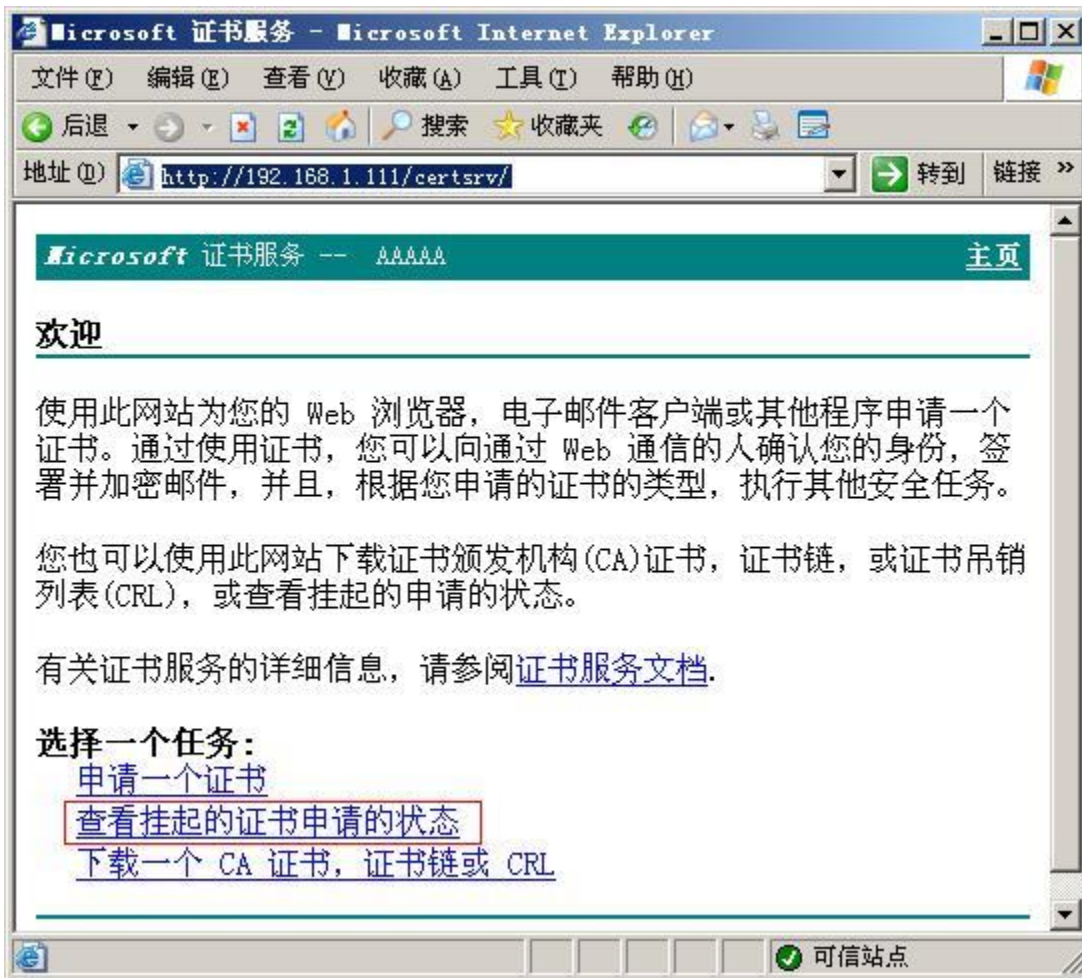
单击‘完成’：



单击‘确定’，浏览器页面跳向如下：



到这一步，申请人已经向 CA 服务器发送证书信息，并等待 CA 管理员对其进行核对，然后决定是否要颁发，如果 CA 管理员核对信息后决定颁发此证书，则申请人在其颁发之后再次访问该系统：



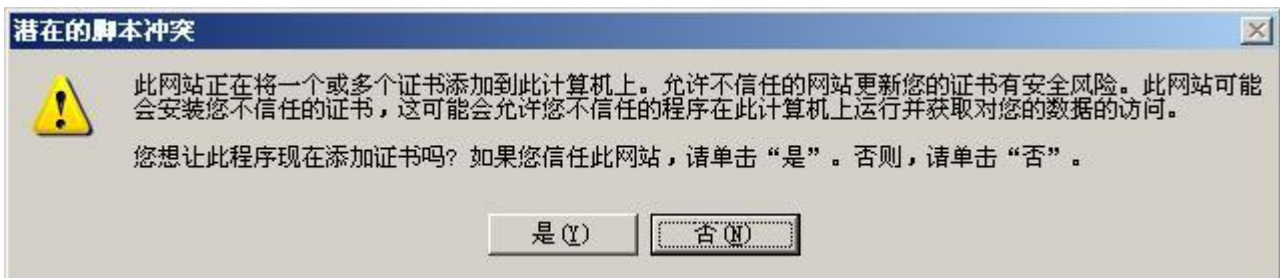
点击‘查看挂起的证书申请状态’：



该页面证明 CA 管理员已经颁发了申请人的证书，点击进入证书安装页面：



点击‘安装此证书’：

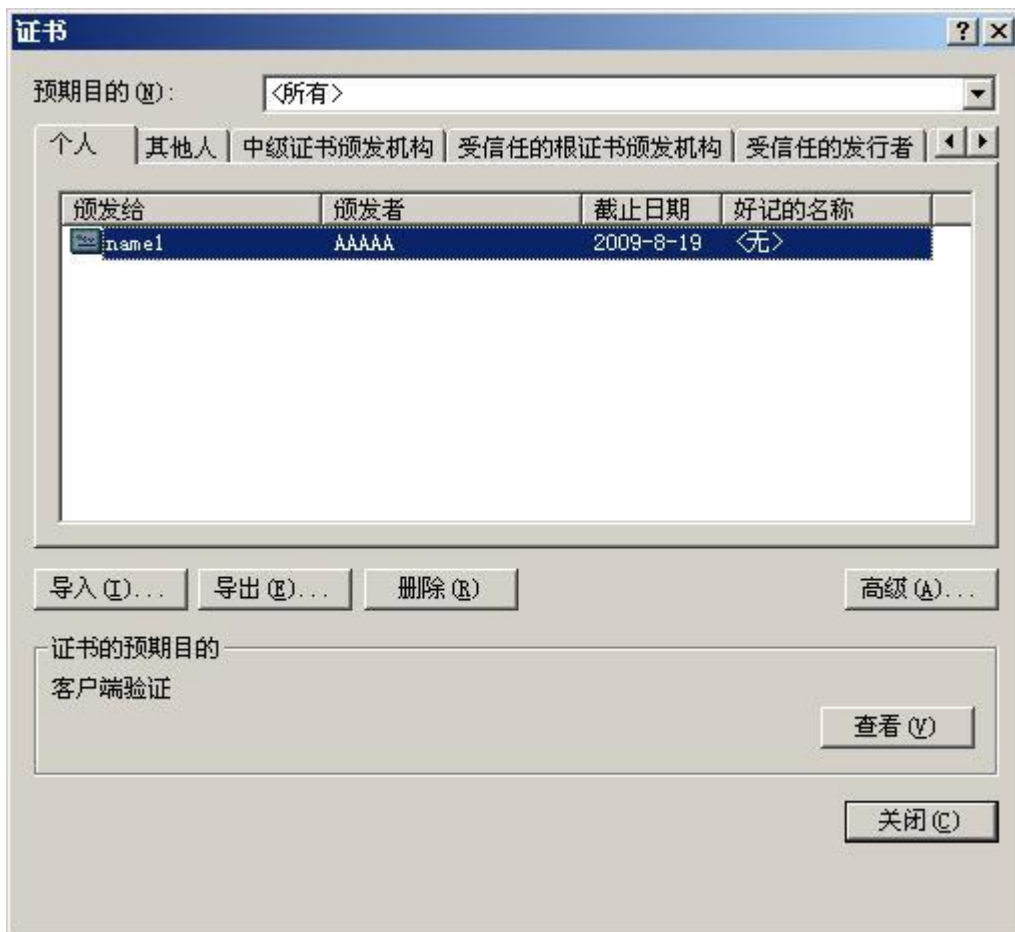


您应该已经信任 CA 机构，所以请单击‘是’：



您已经成功安装数字证书。

如果要找回您刚才安装的数字证书，请单击浏览器上的：工具 >>> Internet 选项 >>> 内容 >>> 证书，弹出如下窗口：



此时您已经发现，在证书个人存储区内已经安装了您刚刚申请并成功安装的证书。  
单击‘查看’：



这就是您的数字证书了。

### 3 CA 证书颁发

开始 》》》 管理工具 》》》 证书颁发机构：



在‘挂起的申请’里已经存在申请挂起等待颁发的证书（如图 ID=2）。

右键点击挂起的证书 》》》 所有任务 》》》 颁发：



刚才的挂起证书已经存入‘颁发的证书’存储区。此时，申请人若在登陆证书申请系统，并查看挂起，就会获取相应的证书。

## 4 Web 服务器配置

### 步骤 1

安装好 IIS，并将其打开（这里用‘默认网站’为例）

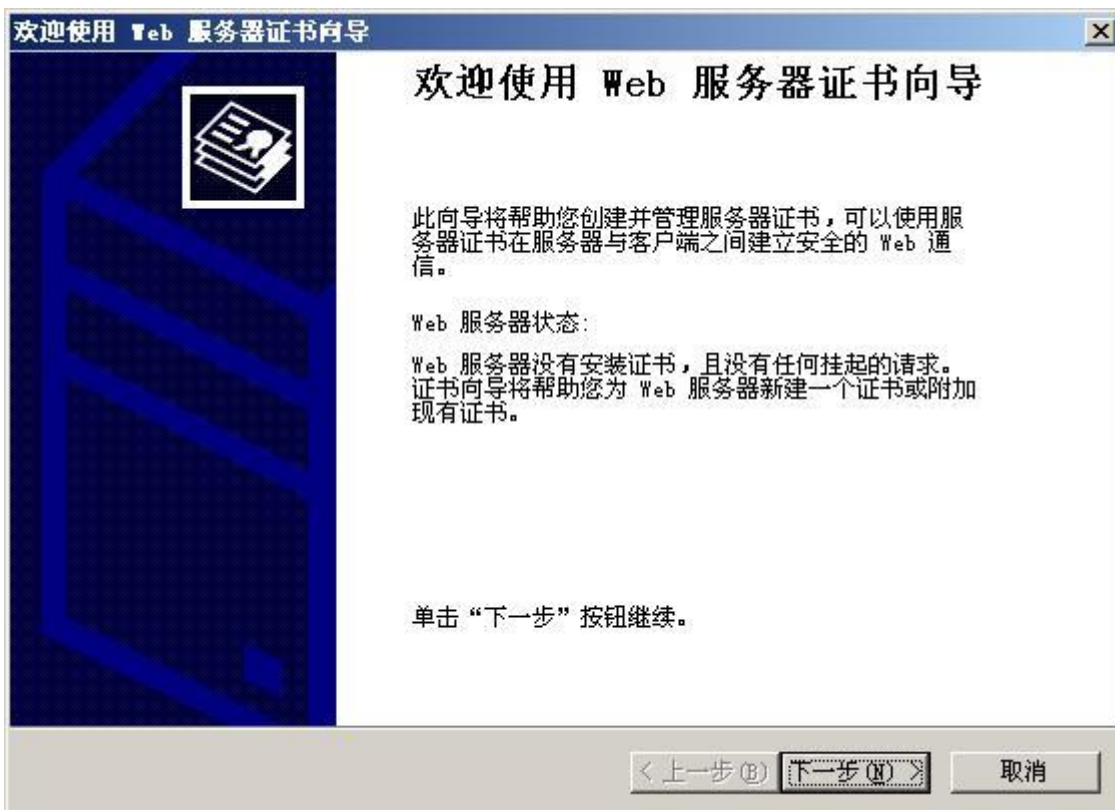
右键点击‘默认网站’》》》 属性：



选择‘目录安全性’选项卡：



图中‘查看证书’为灰色不可用，说明我们还未为‘默认网站’配置数字证书。  
单击‘服务器证书’，弹出如下窗口：



单击‘下一步’：



由于之前并未配置过数字证书，所以应选择‘新建证书’。如果以前配置过数字证书，并且数字证书仍然可用，则选择‘分配现有证书’即可。

单击‘下一步’：



单击‘下一步’：



名称可以根据需要更改，不影响证书的使用。位长默认为 1024，一般已经足够安全，数值越大就越安全，但是数值越大系统的处理速度就会越慢。

直接单击‘下一步’：



单位、部门请填写真实并能够被证实的信息，因为 CA 管理员会根据这些信息进行审核。

单击‘下一步’：



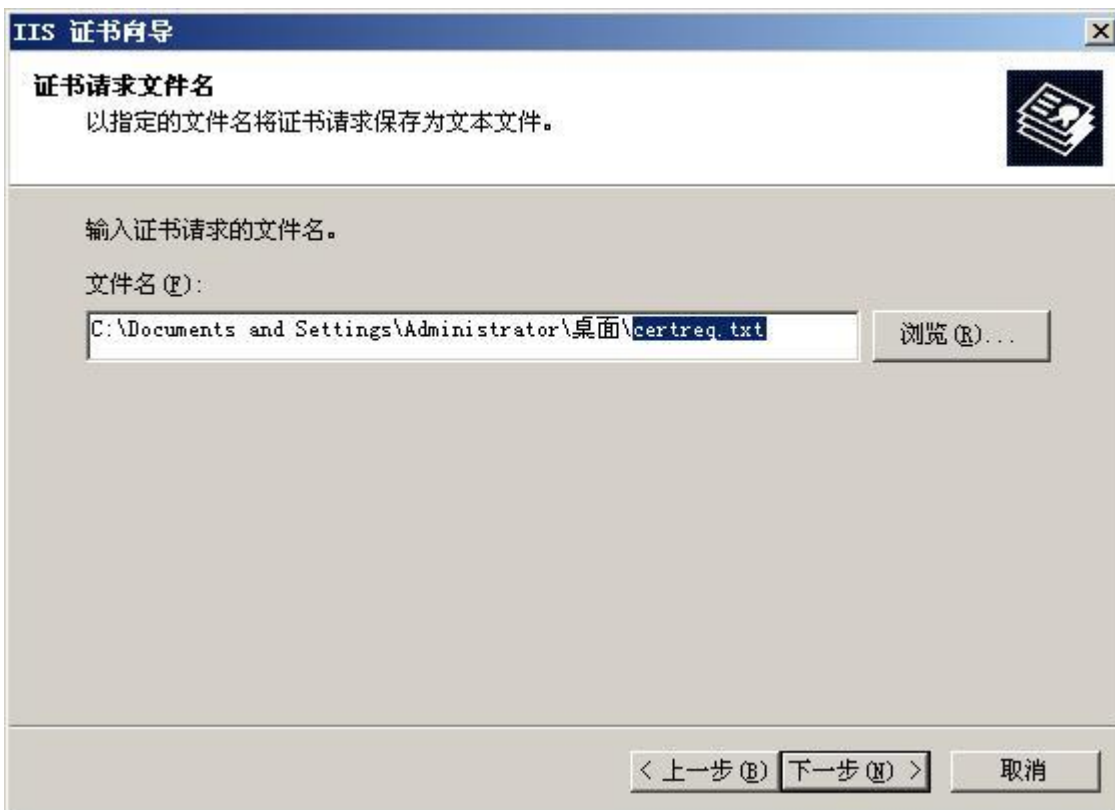
这一步很关键。公用名称不能随便更改，只能是该网站的 DNS，如果尚未申请 DNS 则可以用 IP 地址代替。默认情况下是服务器的计算机名，但这种情况只适合于企业机构（AD 管理），我们要配置的是独立机构，所以公用名只能是 DNS 或 IP 地址。

单击‘下一步’：



这些信息也将是 CA 管理员的审核对象。

单击‘下一步’：



至此，数字证书的信息已经填写完毕，这一步将这些信息以 Base64 编码的形式保存在本地，Web 管理员可以用编码到 CA 证书申请系统进行证书的申请。

单击‘下一步’：



以上就是数字证书的本地信息，CA 管理员将对其进行审核，并决定是否颁发。

单击‘下一步’：



单击‘完成’

接下来就是到 CA 的证书申请系统申请服务器验证证书。

## 步骤 2

打开如下网页：

点击‘申请一个证书’：

点击‘高级证书申请’：



‘使用 base64 编码的 CMC 或 PKCS#10 文件提交一个证书申请，或使用 base64 编码的 PKCS#7 文件续订证书申请’

我们的用于申请的 base64 编码保存在一个名为 certreq.txt 的请求文件中。

将其打开

全选编码，并将其复制，粘贴到：

点击‘提交’：

我们已经向 CA 服务器发送证书请求信息，等待 CA 管理员对信息进行审核并颁发证书。

我们假设 CA 管理员审核证书信息后执行了颁发。

我们再次打开 CA 的证书申请系统：

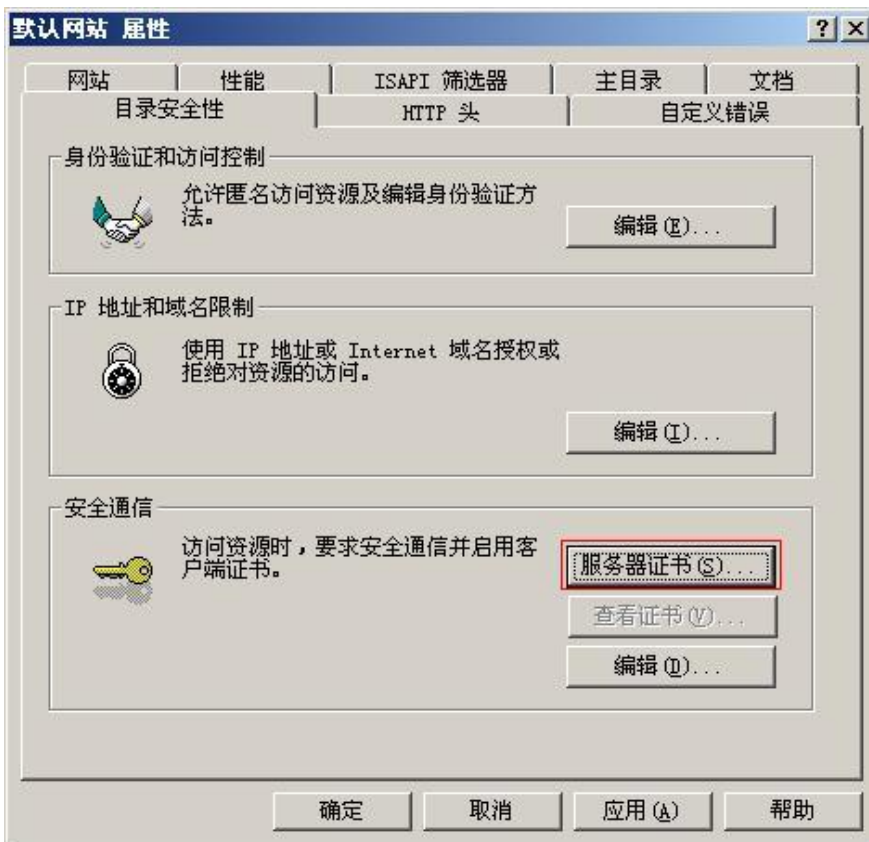
点击‘查看挂起的证书申请的状态’：



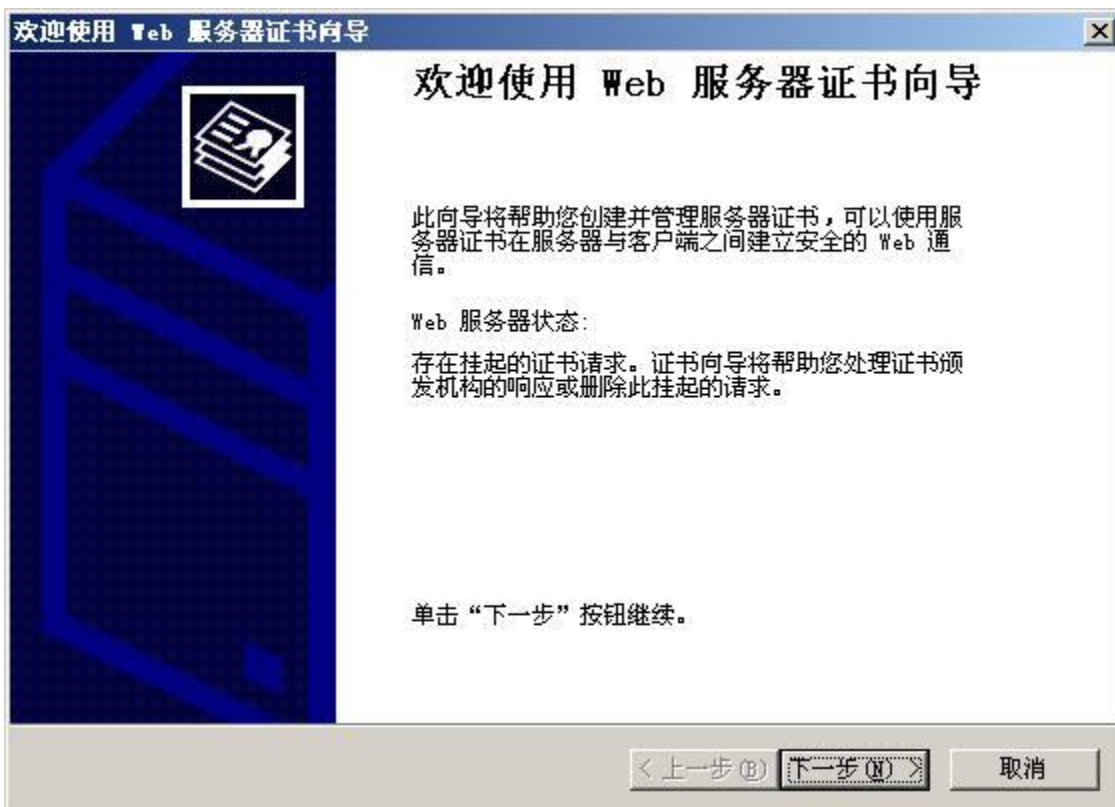
点击‘下载证书’

我们等一下要用到的就是该保存到本地的 .cer 文件。（如果有需要也可以将‘证书链’也下载，证书链里包含 CA 服务器的数字证书）

我们再返回默认网站 >>> 属性 >>> 目录安全性：



单击‘服务器证书’进行数字证书的安装：





选择好刚才保存的 .cer 证书文件



SSL 的默认端口是 443。我们也可以设置能其他端口，但是设置成其他端口号时，用户访问的时候必须在 URL 中指定端口号。

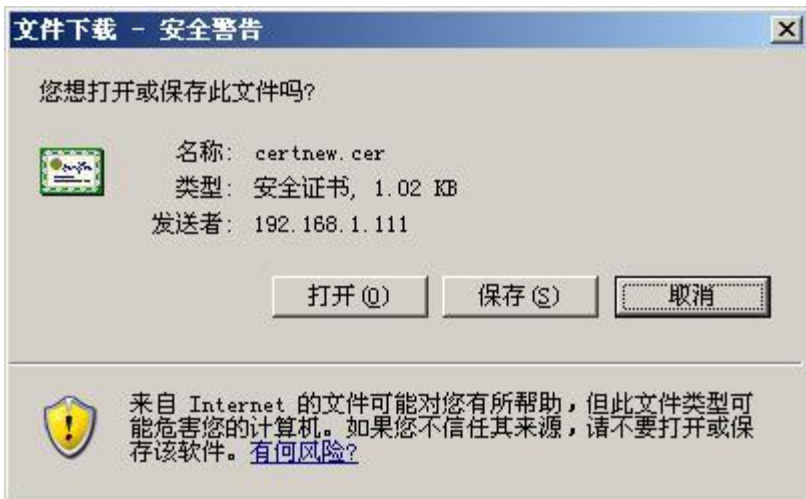


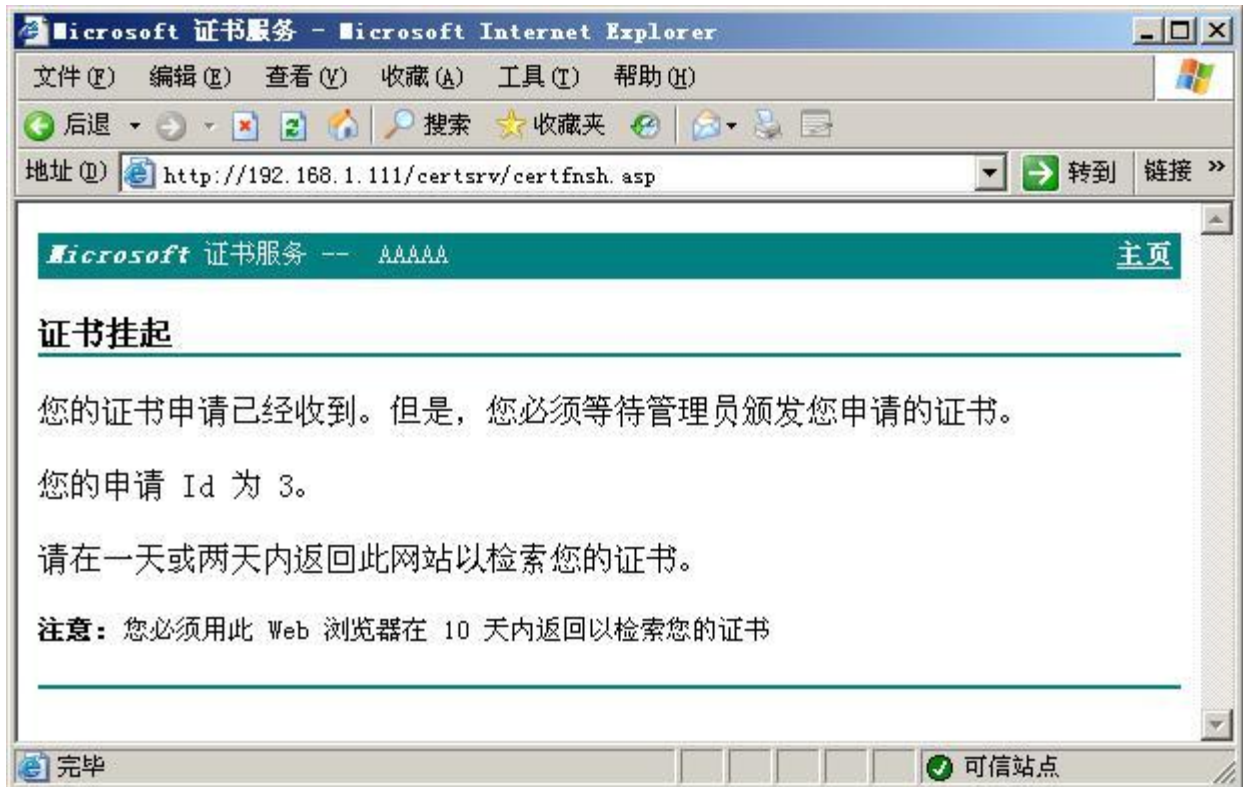
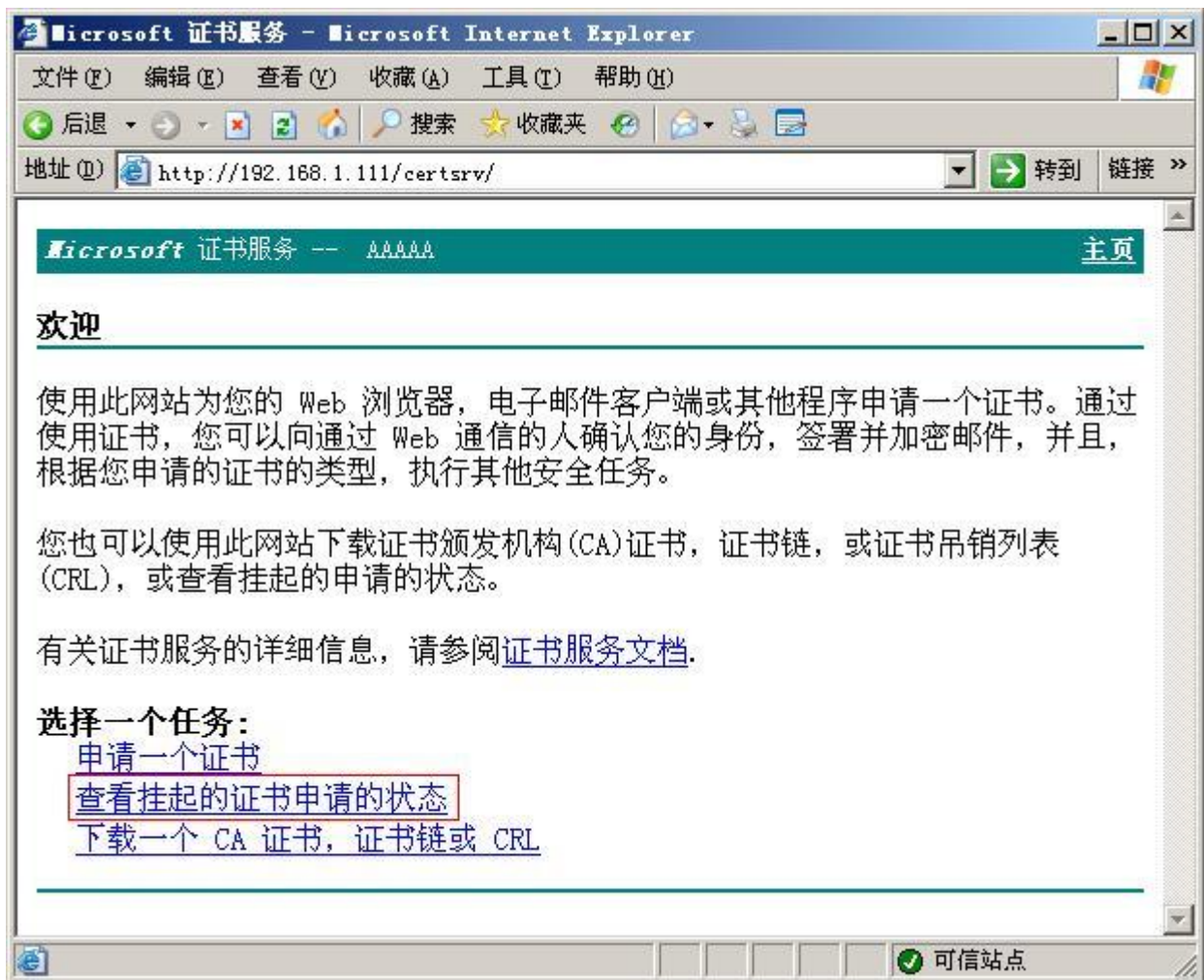
证书安装成功，以上就是数字证书的所有信息

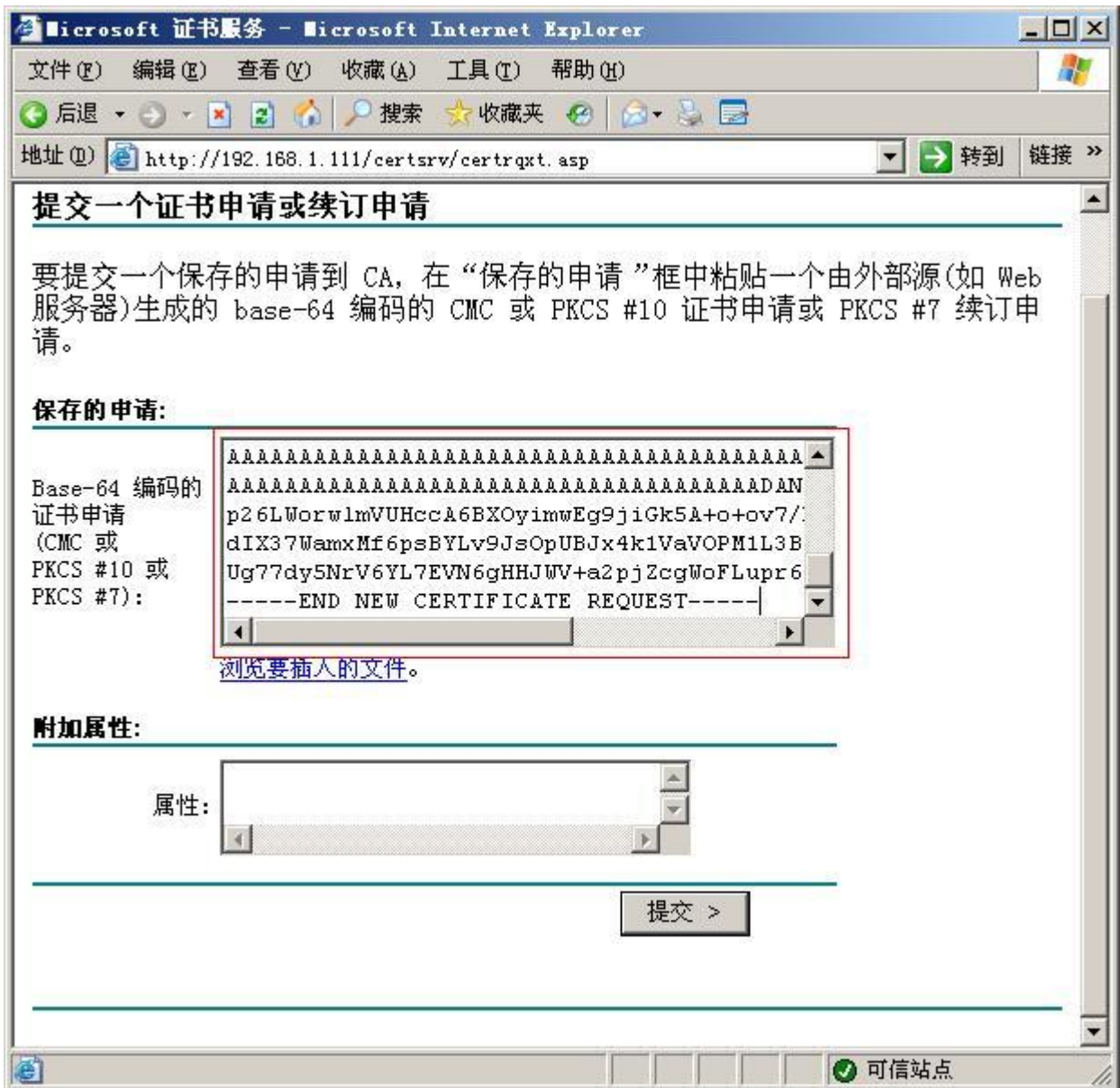


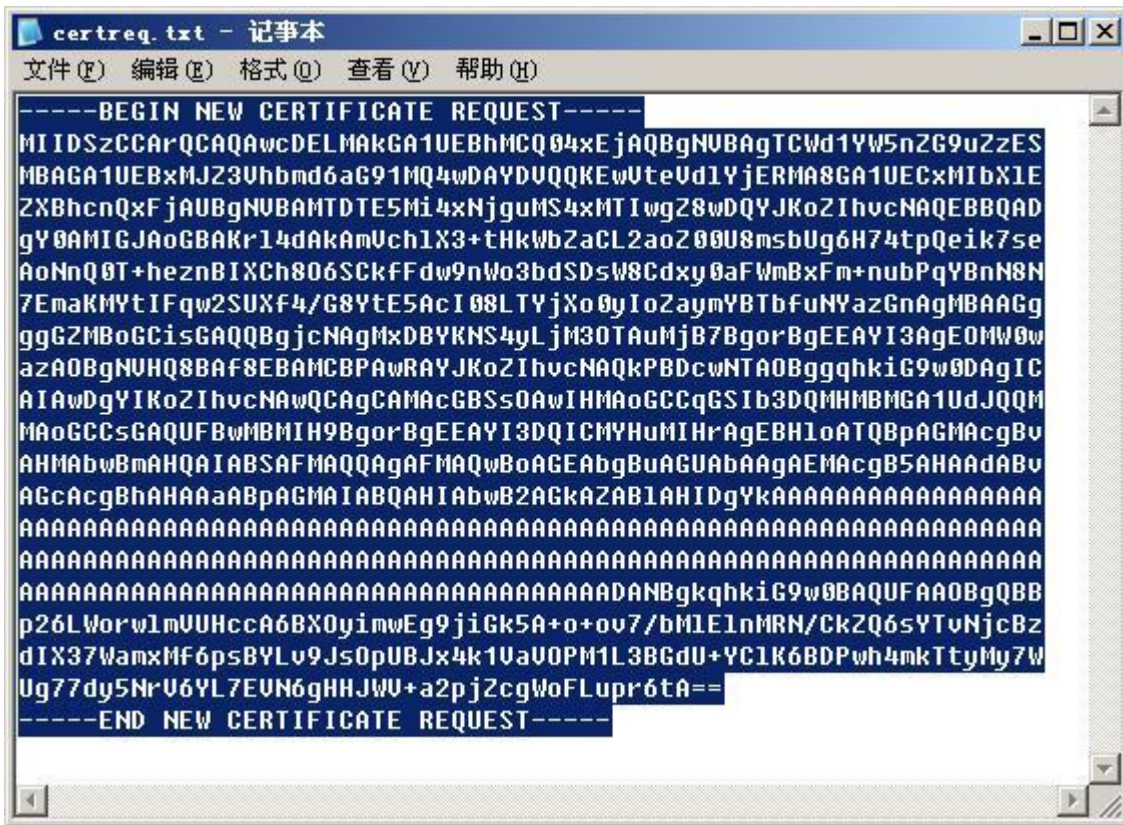
单击‘完成’

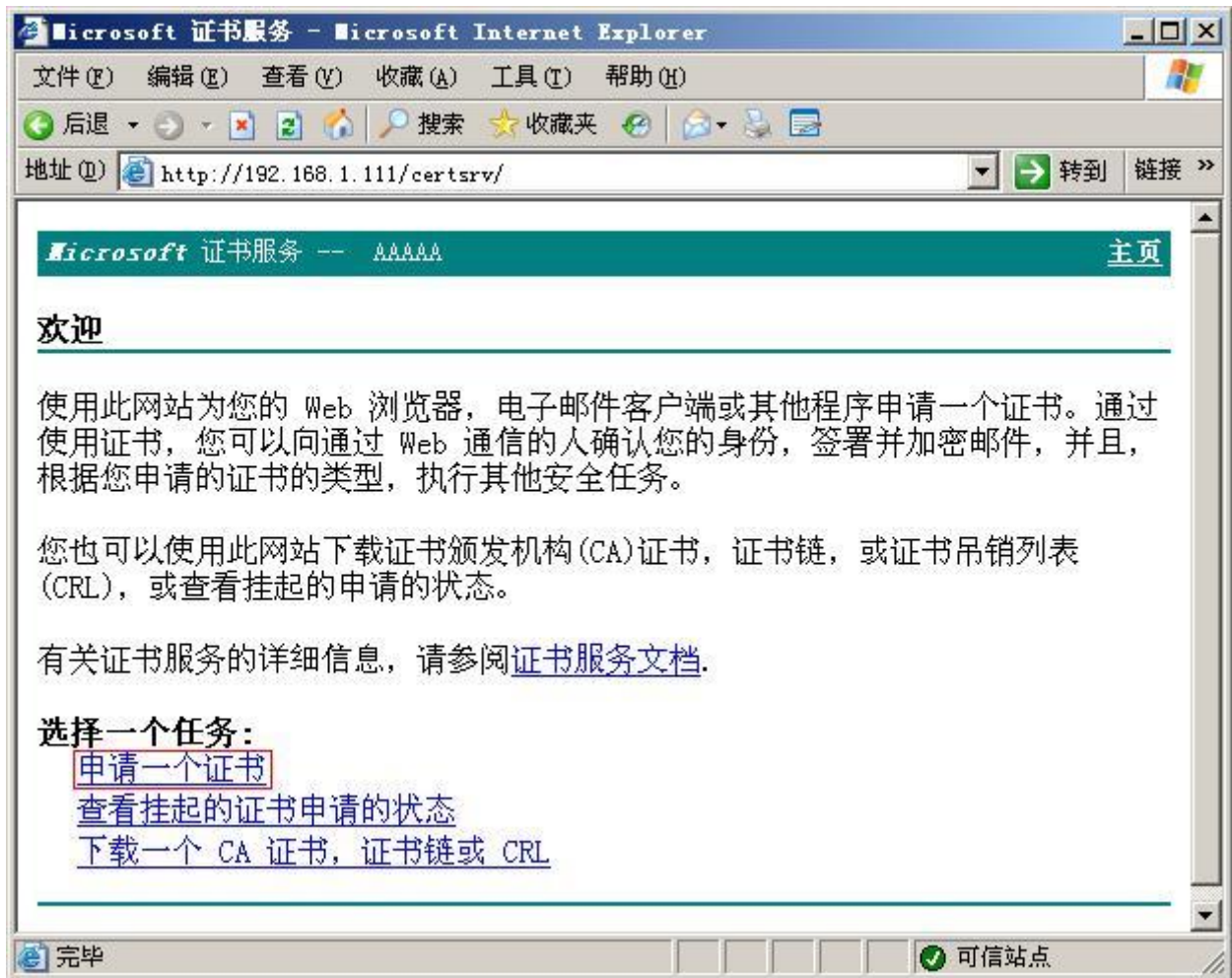
(待续)



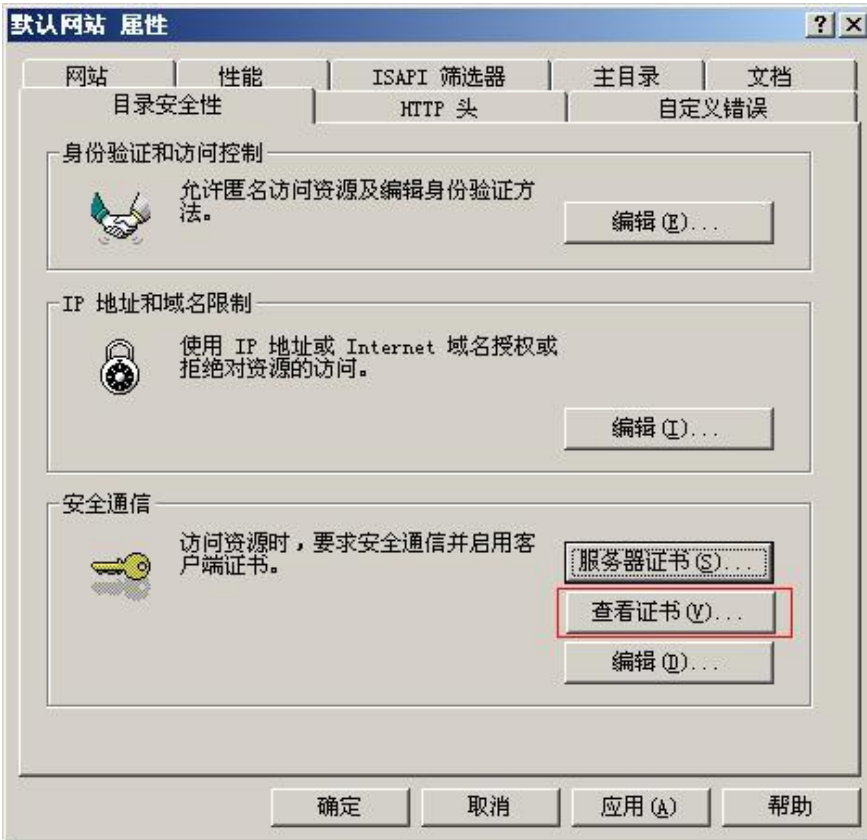




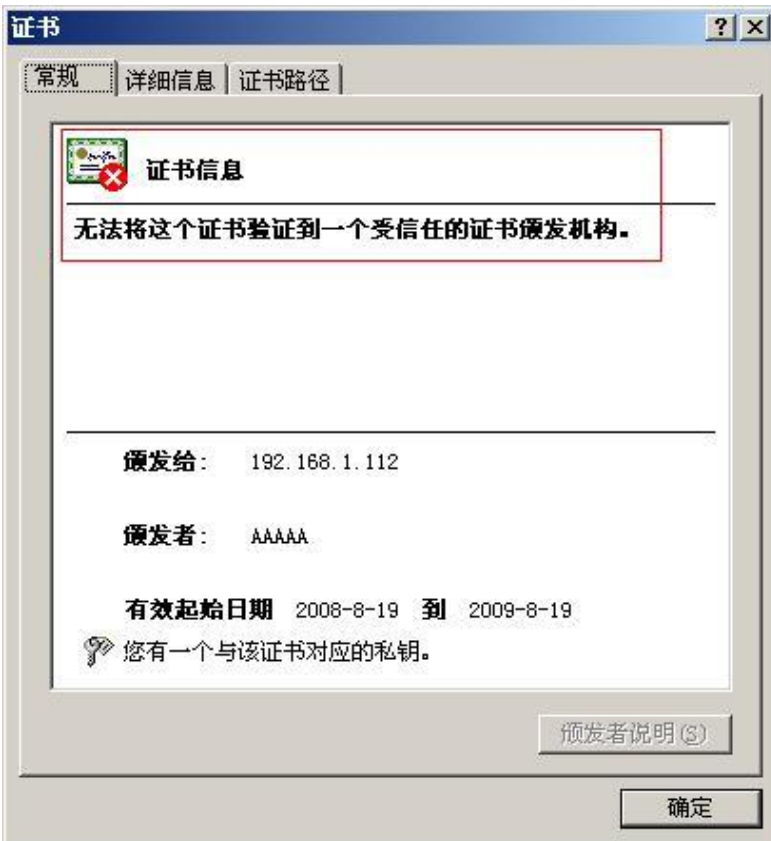




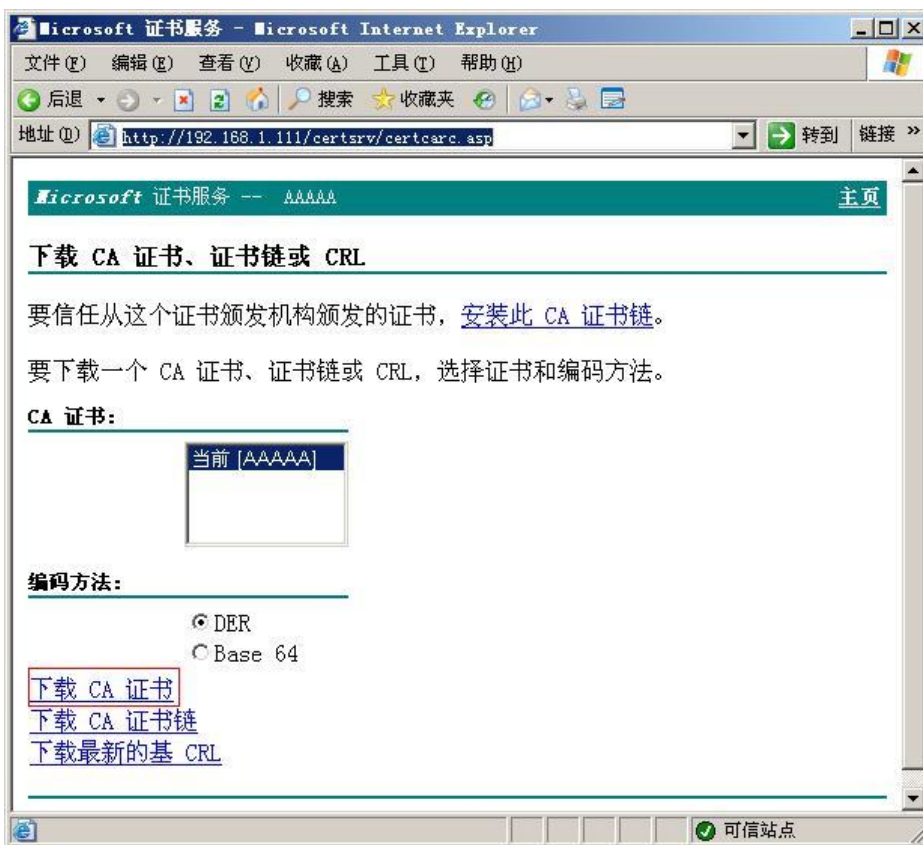
### 步骤 3



我们已经可以‘查看证书’了。



这就是我们安装完成的证书。如图中所示，Web 服务器还不信任我们自己配置的证书颁发机构。没关系，先到 CA 证书申请系统中下载 CA 根证书



直接键入以上地址栏中的 URL 即可打开网页，‘下载 CA 证书’

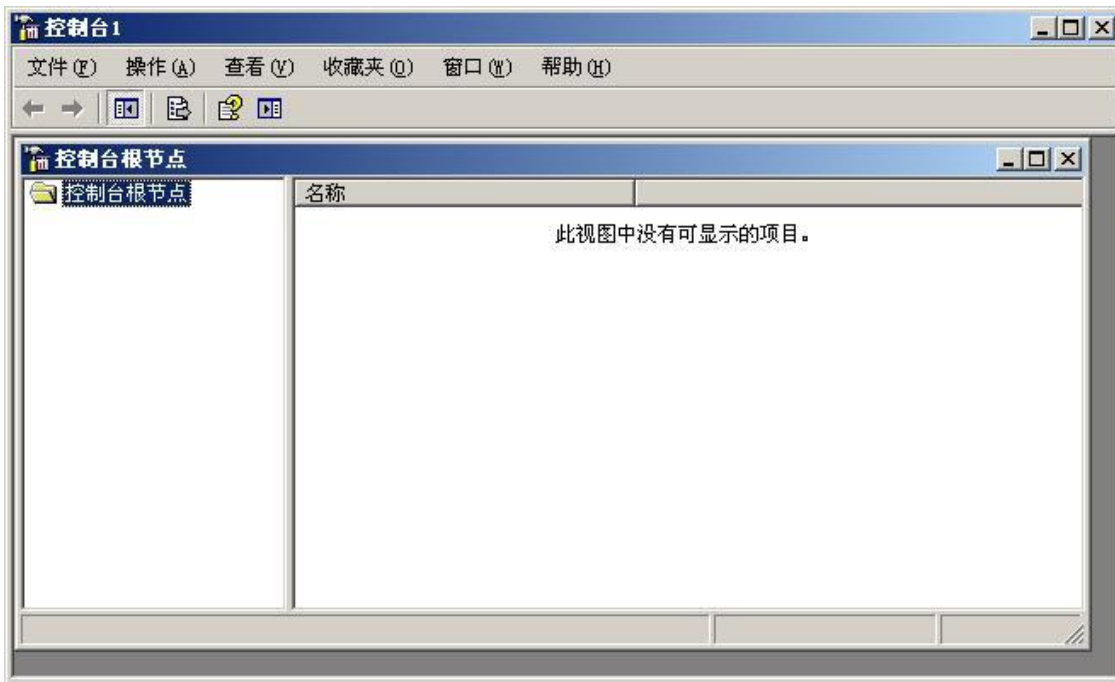
如果之前在下载证书的时候同时下载了‘证书链’则可以不执行此步操作，因为证书链里包含有 CA 证书。

接下来我们要安装 CA 的数字证书，安装完成后 Web 服务器才会信任该 CA 机构。

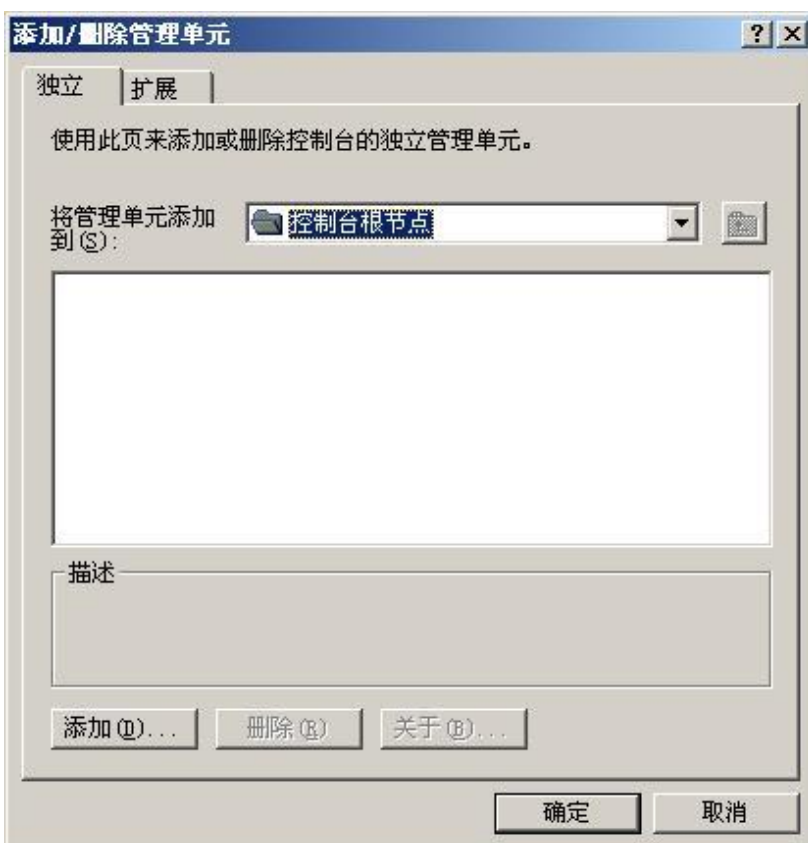
开始 》》》 运行：



运行打开 mmc，单击‘确定’，打开如下窗口。



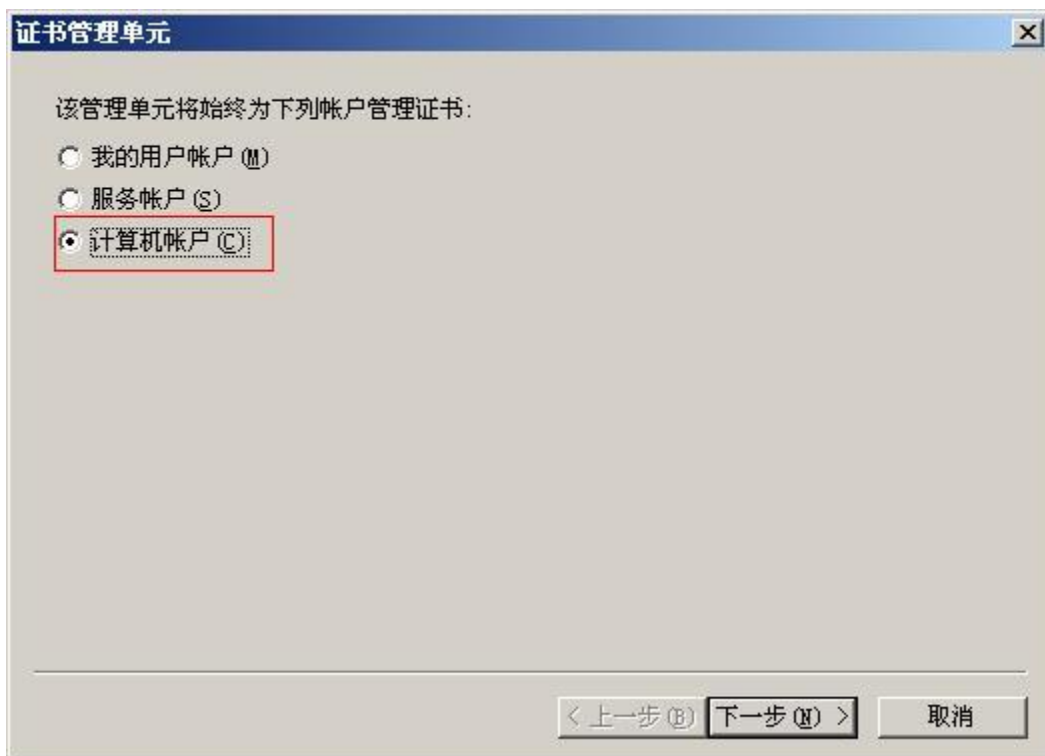
此时在控制台管理单元里什么都没有，没关系，文件 》 》 》 添加/删除管理单元



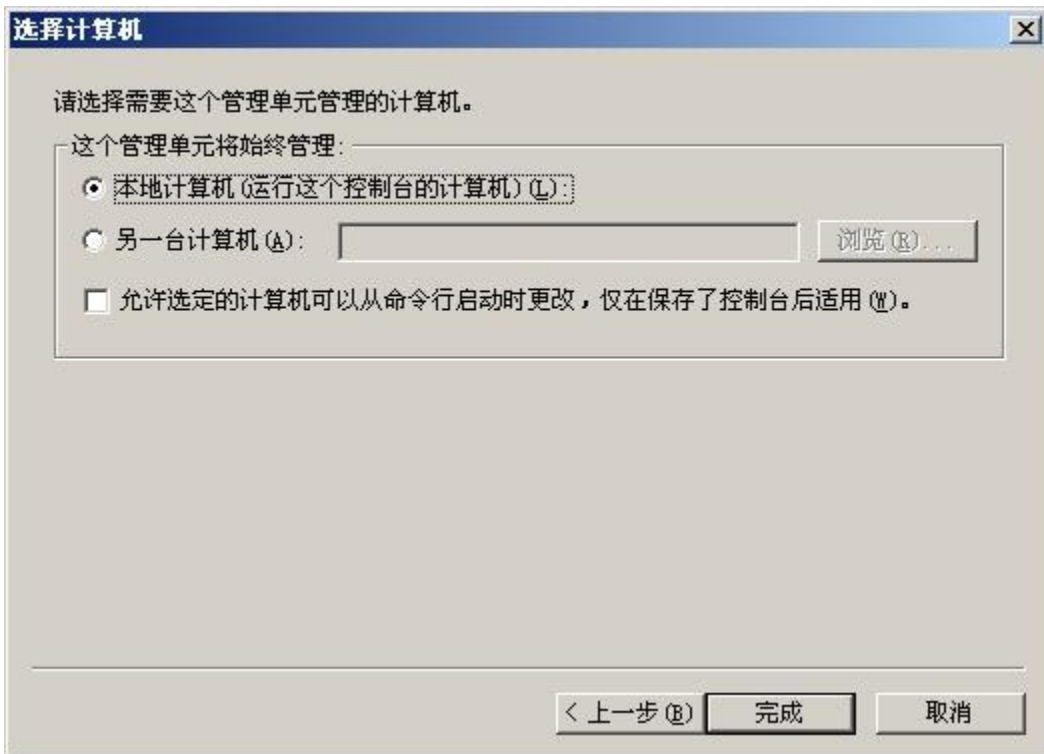
单击‘添加’



找到‘证书’的管理单元，单击‘添加’



选择‘计算机帐户’，单击‘下一步’



单击‘完成’



当然我们还可以添加其他管理单元，但是我们现在还用不到，所以单击‘关闭’

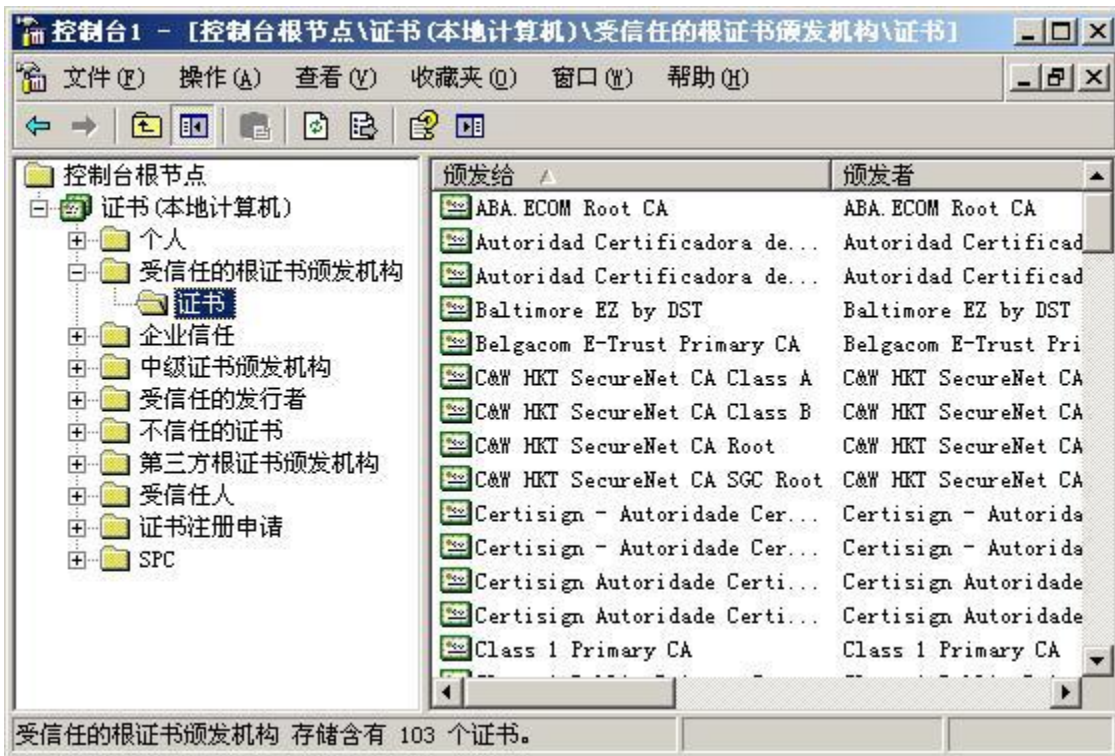


单击‘确定’



我们已经将‘证书（本地计算机）’添加到控制台。

将其展开，展开‘受信任的根证书颁发机构’



此时我们自己配置根证书颁发机构还不被计算机信任，所以我们必须导入证书颁发机构的数字证书。

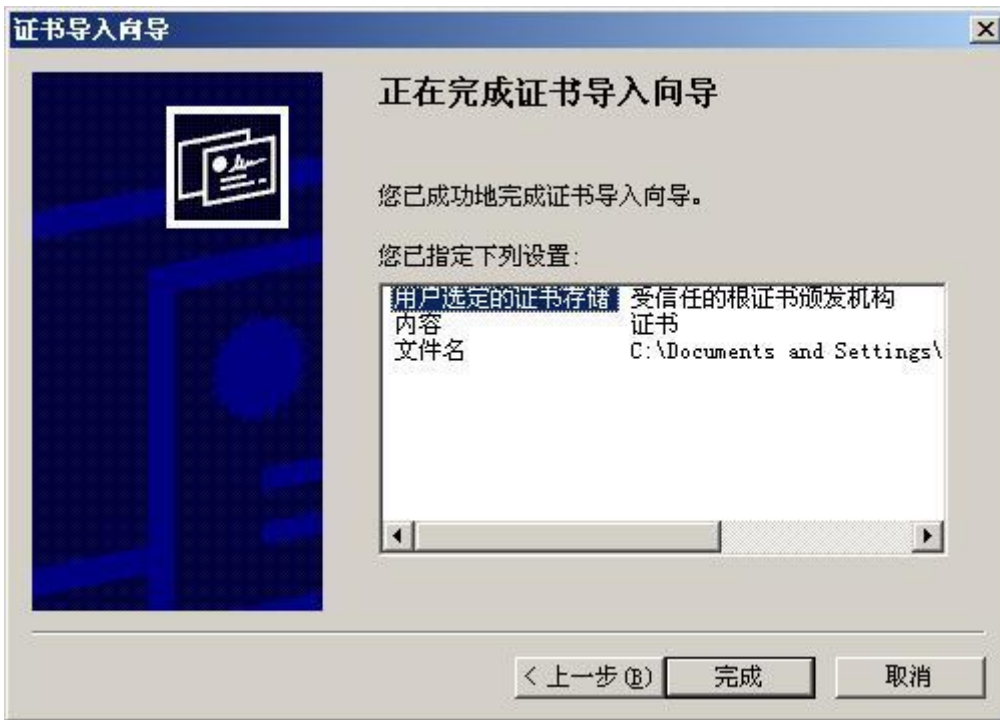
右键‘证书’导入证书





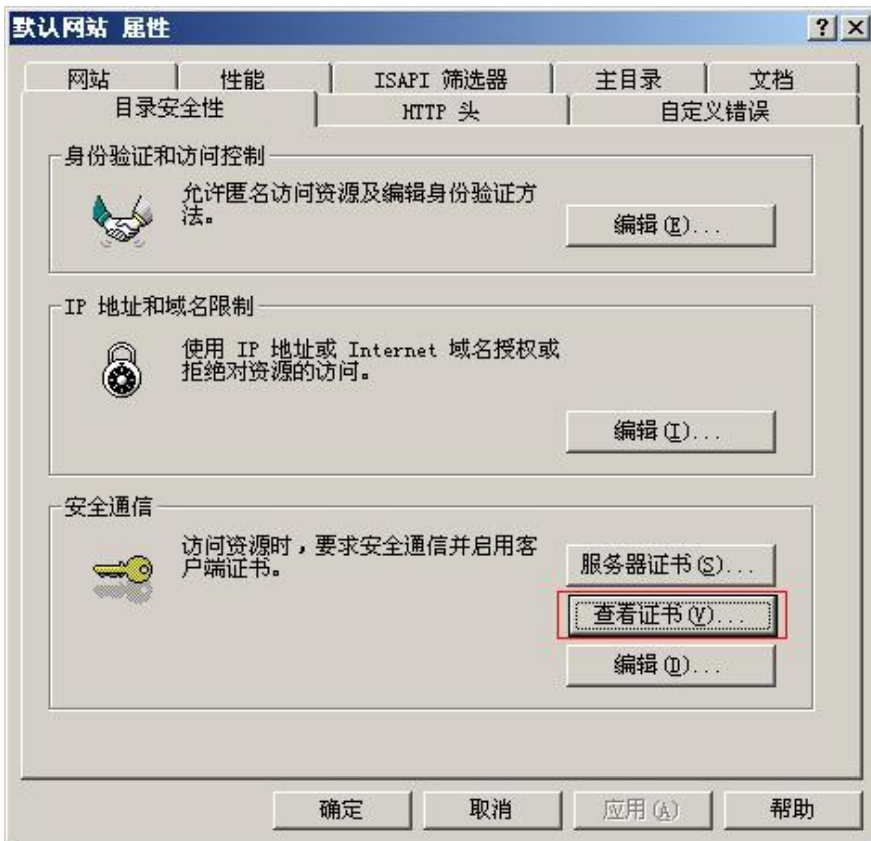
选择我们已经保存的 CA 证书，单击‘下一步’：





此时我们发现，CA 证书已经添加到相应区域。

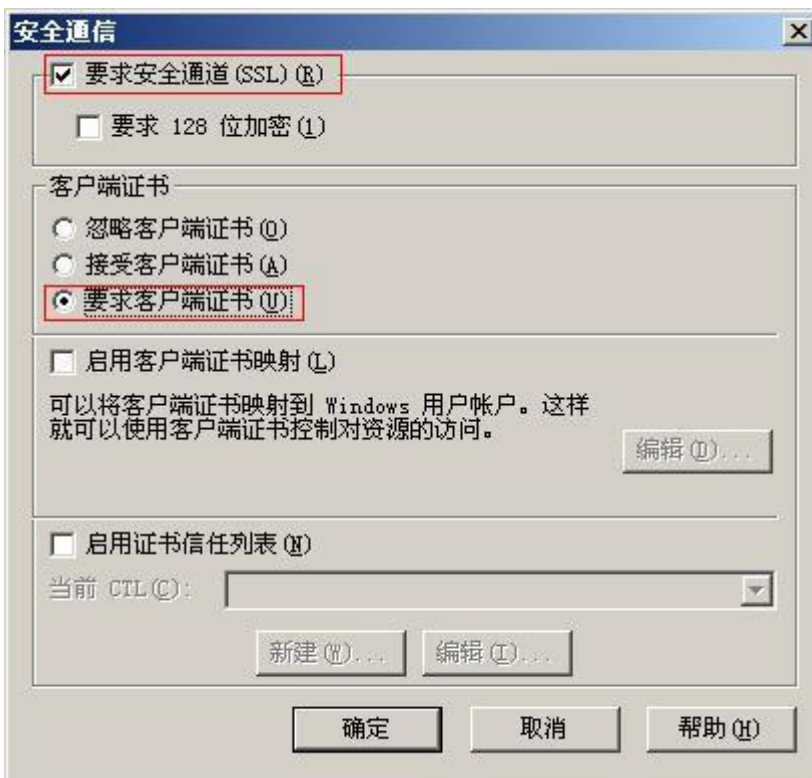
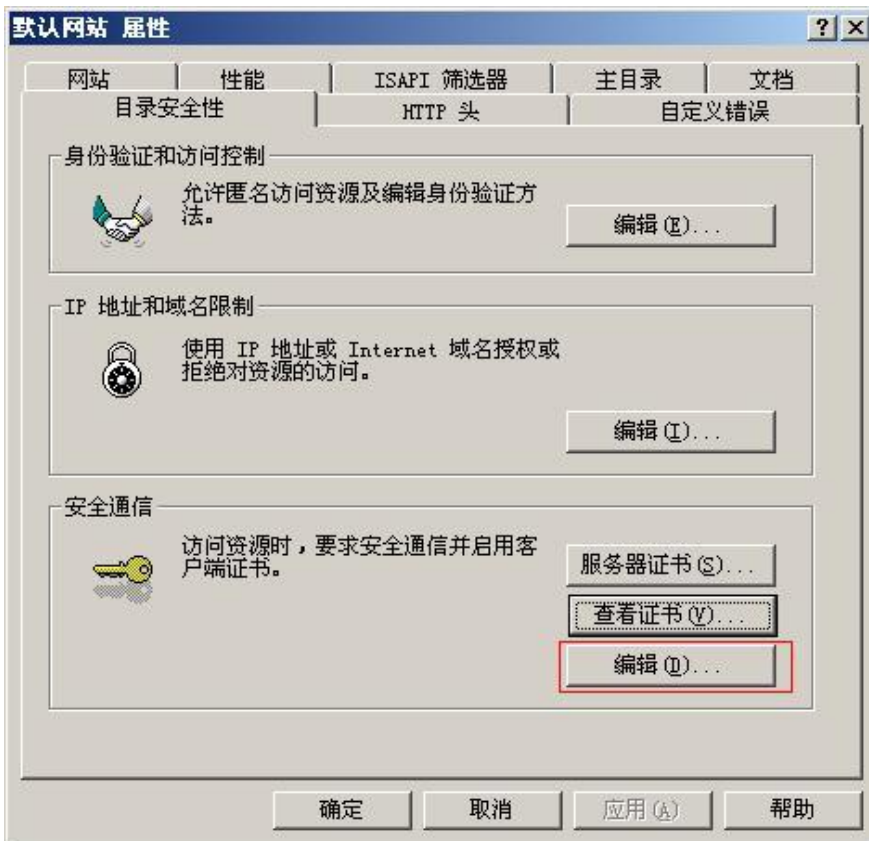
我们再返回默认网站 >>> 属性 >>> 目录安全性



服务器已经信任 CA 机构了

接下来可以建立 SSL 通道请求

点击‘编辑’



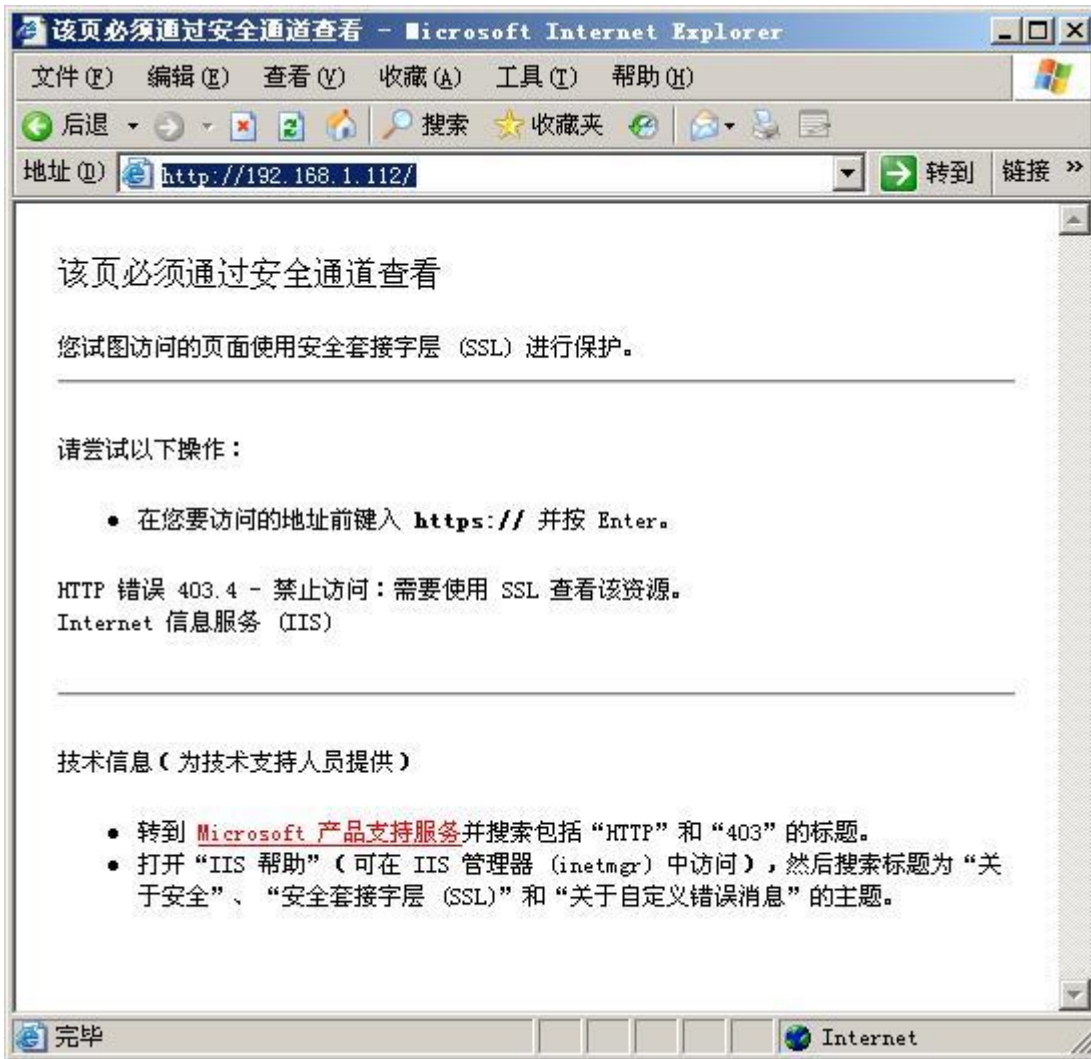
选择‘要求安全通道’，选择‘要求客户端证书’（也可选择其他选项，视具体情况而定）。

‘确定’

Web 服务器配置完毕。

## 5 客户端访问 Web 服务

在客户端浏览器中输入 Web 地址，打开网页

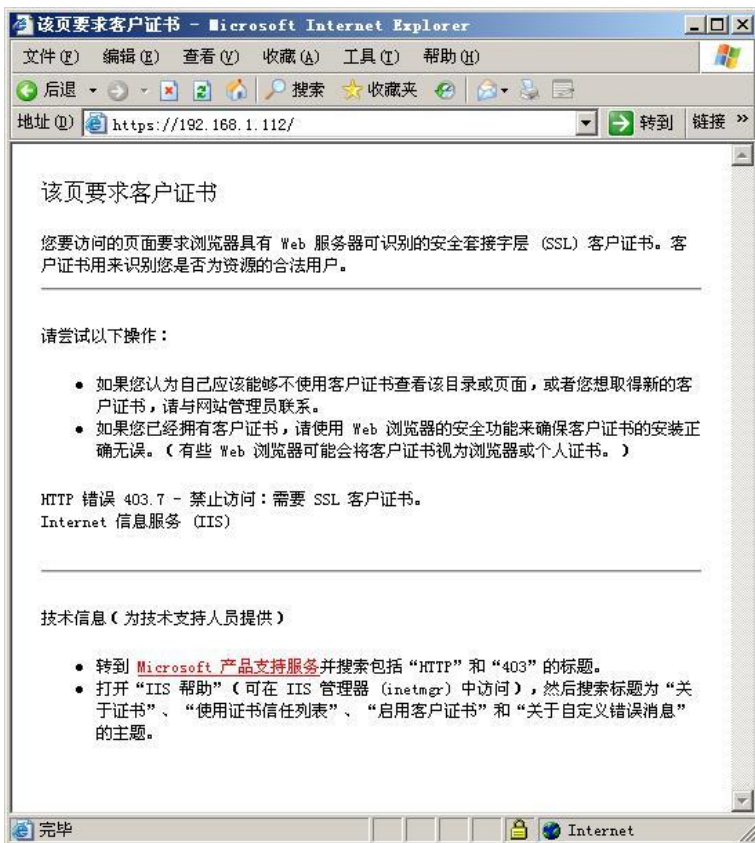


由于 Web 已经配置成要求 SSL 通道,所以客户访问的时候不能再用 http 协议,而应该用 https 协议

修改成 https 协议后再次打开网页,弹出证书选择的窗口(我们默认客户端已经安装 CA 证书,如果客户端尚未安装 CA 证书,则在弹出此窗口之前会弹出一个警告窗口,单击确定后就会弹出证书选择窗口)



客户端尚未安装数字证书，所以并没有数字证书提供选择，单击确定后进入错误页面



客户端到 CA 申请数字证书并安装完成后，再次访问 Web



这一次就会有个人身份验证证书提供选择，选择好，并点击确定



由于申请证书的时候将证书的安全级别设置为‘高’，并设置了口令，所以每次需要用到该证书的时候都必须输入口令。用户可以在申请证书的时候将安全级别设低，但是将安全级别设置为‘高’的好处是如果你到一台公共机上使用证书，并且在临走之前忘记删除已安装的证书，别人没有你的口令仍旧是无法使用的。

单击‘确定’

