服务器证书安装配置指南

IIS6.0

Q/ GlobalSign China-QI-XX-YY

GlobalSign 数字证书颁发机构

环玺信息科技（上海）有限公司

2018 年 1 月

目　录

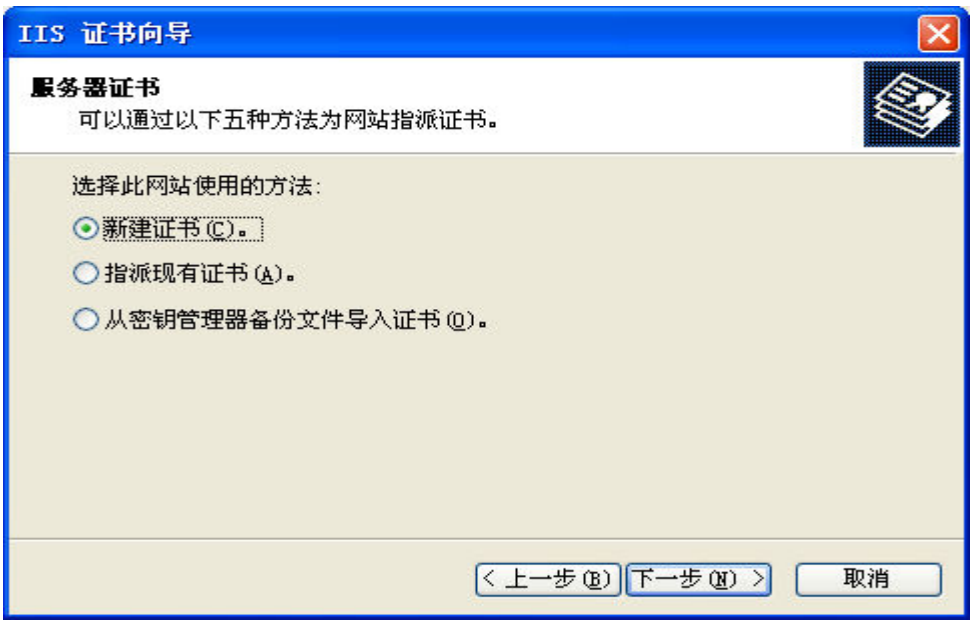
服务器证书安装配置指南（IIS6.0）

1. 生成证书请求

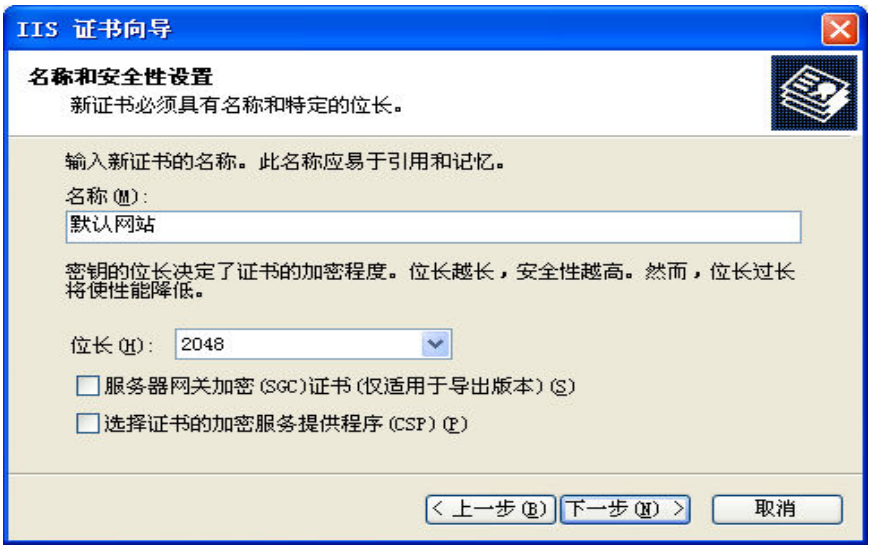
1.1 生成证书请求文件(CSR)

进入 IIS 管理控制台，选择需要配置证书的站点，右键选择“属性”➔“目录安全性”

“服务器证书”➔“新建证书”



为证书输入名称，并设置服务器证书密钥对位长。服务器证书要求密钥位长 2048。

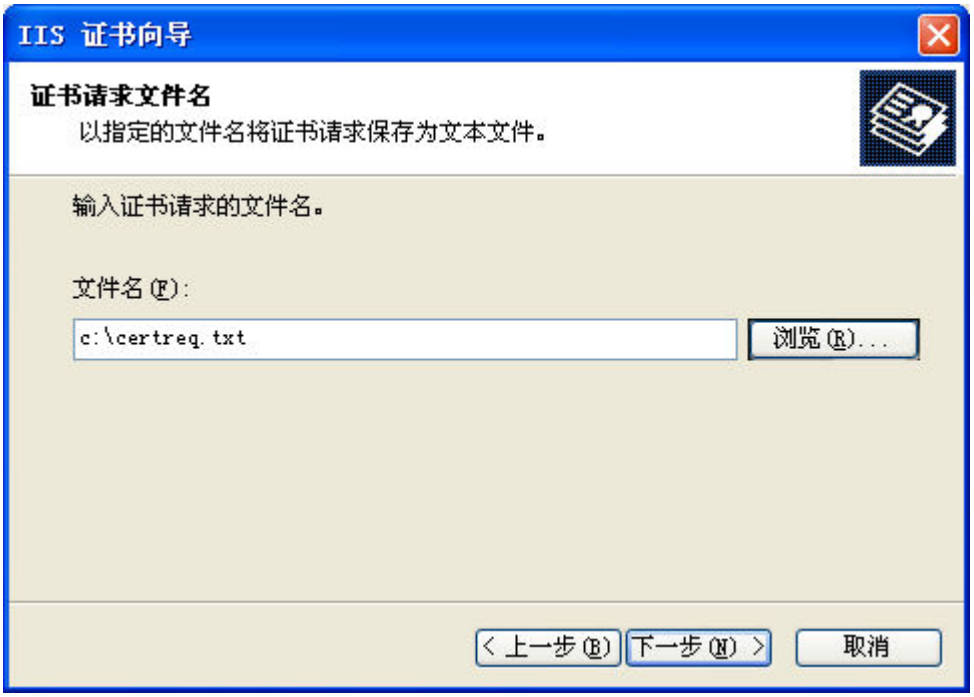


输入公司名称及部门信息。

公用名称栏需要填写完整域名信息

输入公司所在地国家、地区信息

导出证书请求文件



1.2 提交证书请求

将证书请求文件 certreq.txt 提交给我们，等待证书签发。

2. 安装中级 CA 证书

2.1 获取服务器证书中级 CA 证书

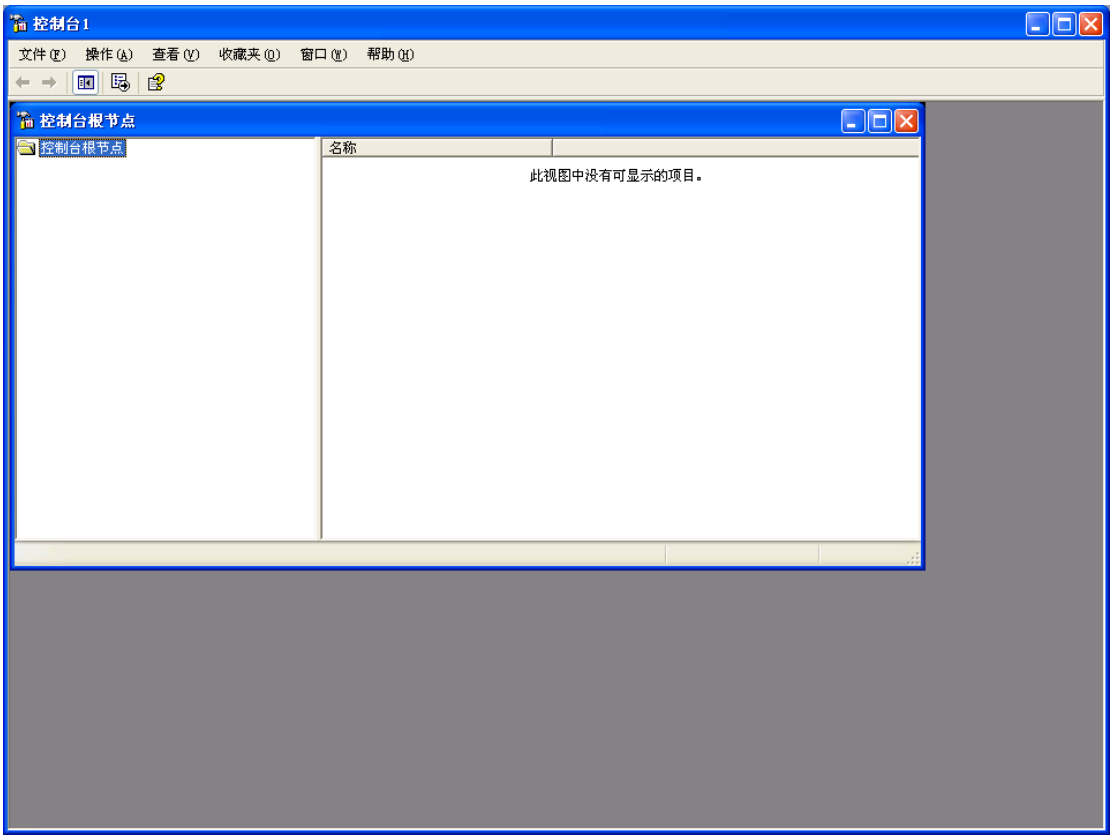
为保障服务器证书在 IE7 以下客户端的兼容性，服务器证书需要安装两张中级 CA 证书。

从邮件中获取中级 CA 证书：

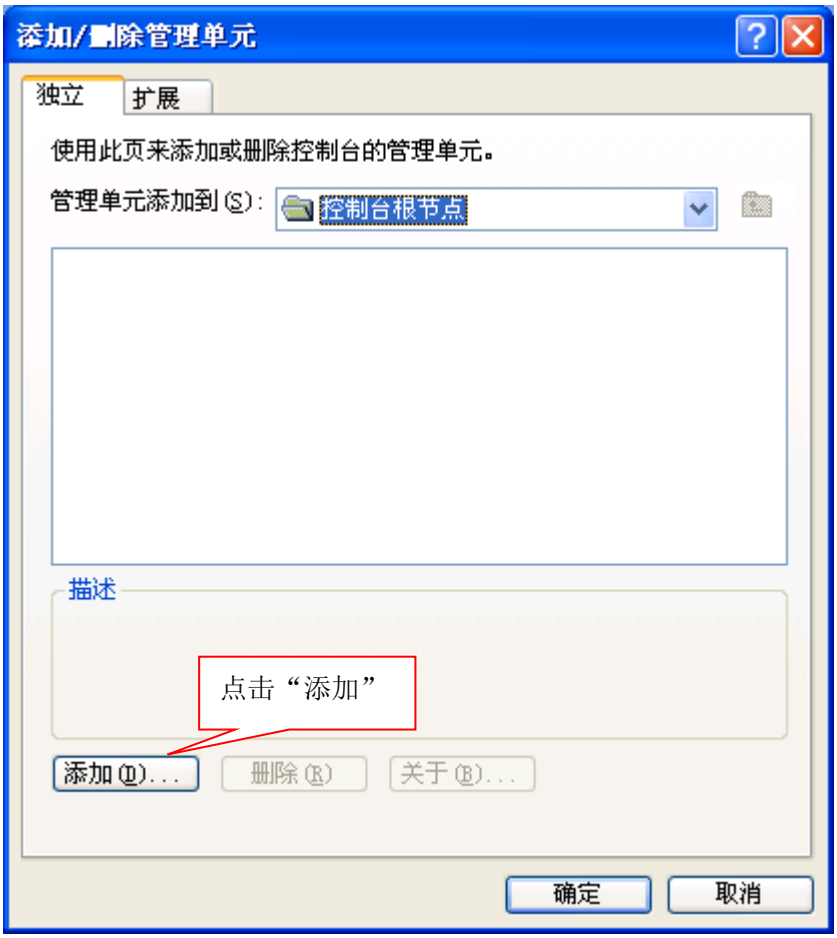
将证书签发邮件中的从 BEGIN 到 END 结束的两张中级 CA 证书内容（包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”）分别粘贴到记事本等文本编辑器中，并修改文件扩展名，保存为 intermediate1.cer 和 intermediate2.cer 文件。

2.2 配置 EV 证书证书链

点击开始菜单，在“运行”中输入“mmc”，打开控制台窗口。

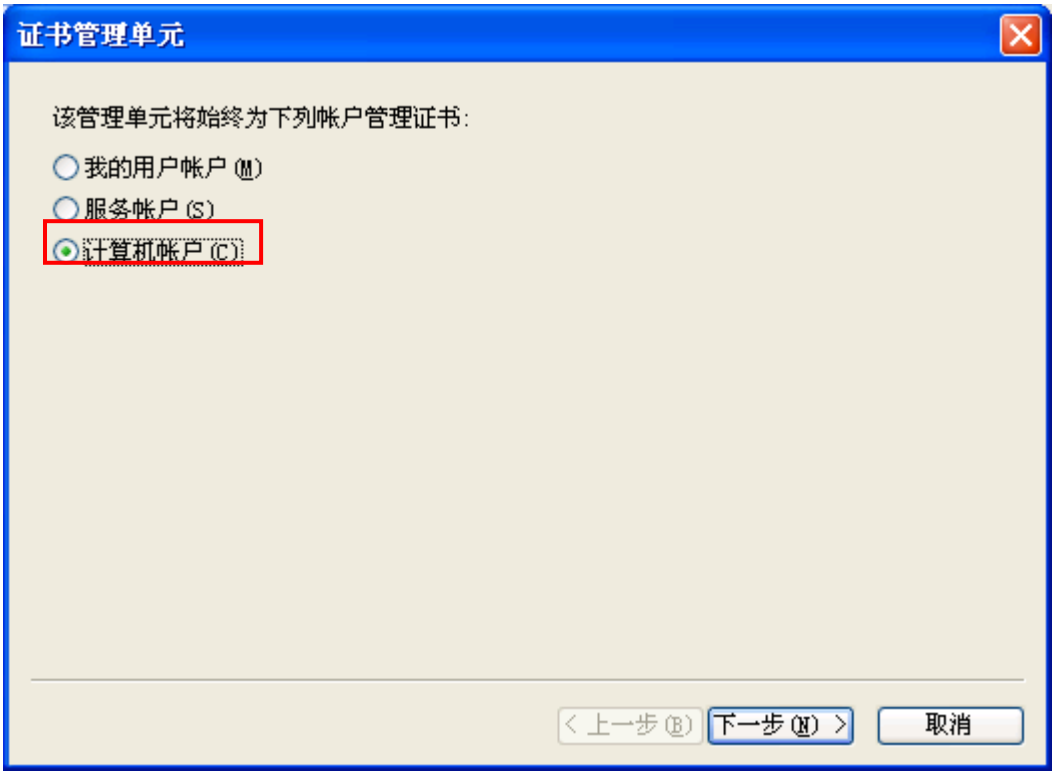


点击“文件➔添加删除管理单元”

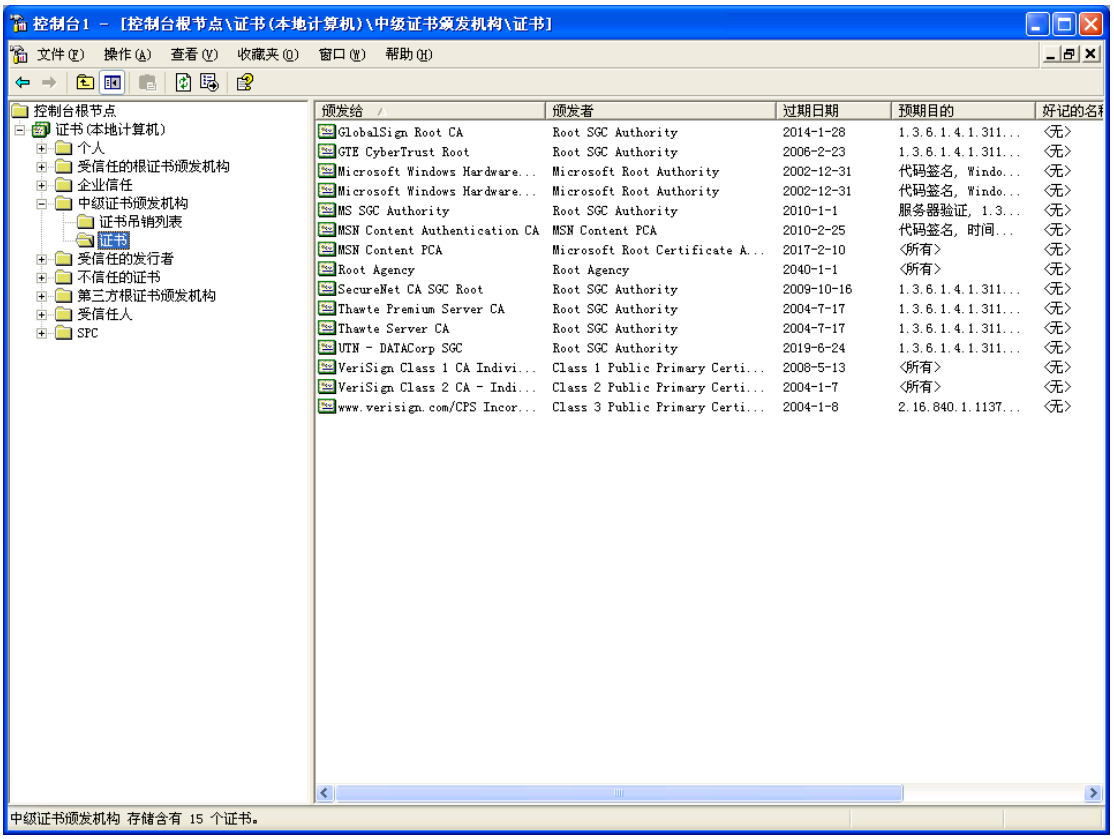


选择“证书”，然后点击“添加”：

选择“计算机帐户”➔“本地计算机”



在添加的证书管理单元中，选择“证书”➔“中级证书颁发机构”➔“证书”



空白处右键点“所有任务”➔“导入”，将服务器的两张中级 CA 证书 intermediate1.cer 和 intermediate2.cer 分别导入。

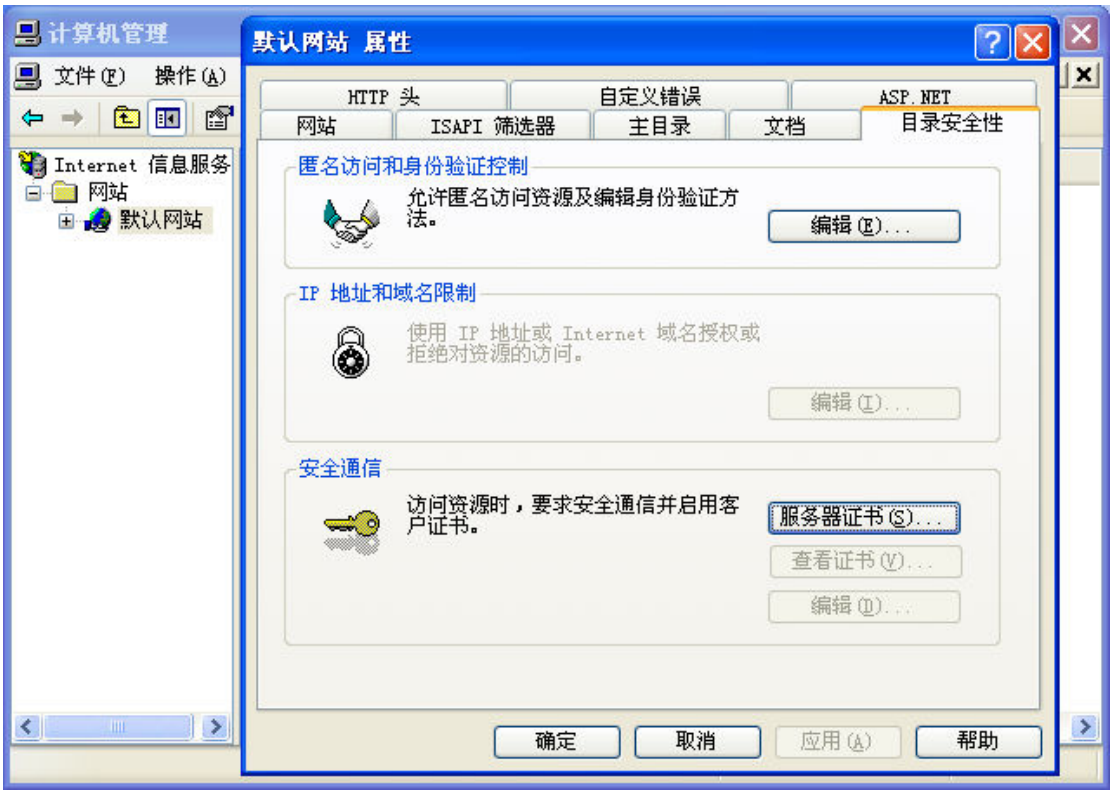
3. 安装服务器证书

3.1 保存服务器证书

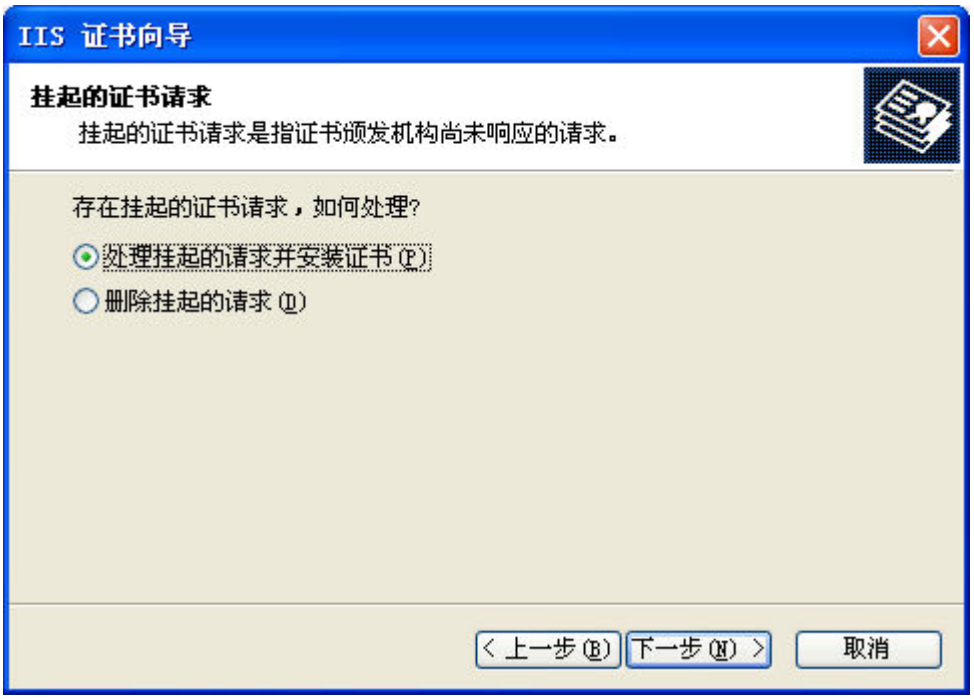
将证书签发邮件中的从 BEGIN 到 END 结束的服务器证书内容（包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”）粘贴到记事本等文本编辑器中，并修改文件扩展名，保存为 server.cer 文件。

3.2 进入 IIS 控制台

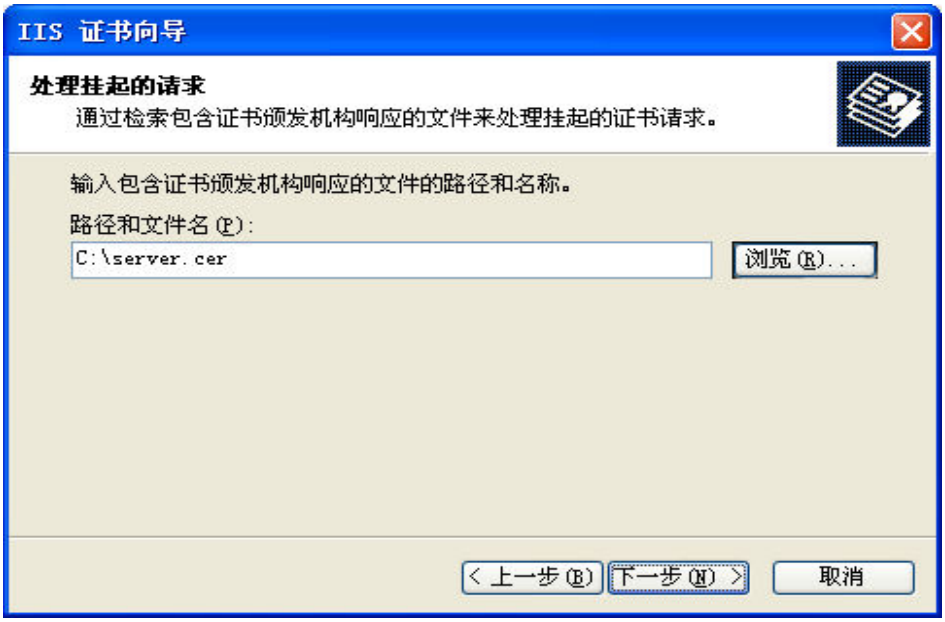
进入 IIS 控制台，并选中需要配置服务器证书的站点，“属性”➔“目录安全性”



选择“服务器证书”➔“处理挂起的请求并安装证书”



选中您的服务器证书文件



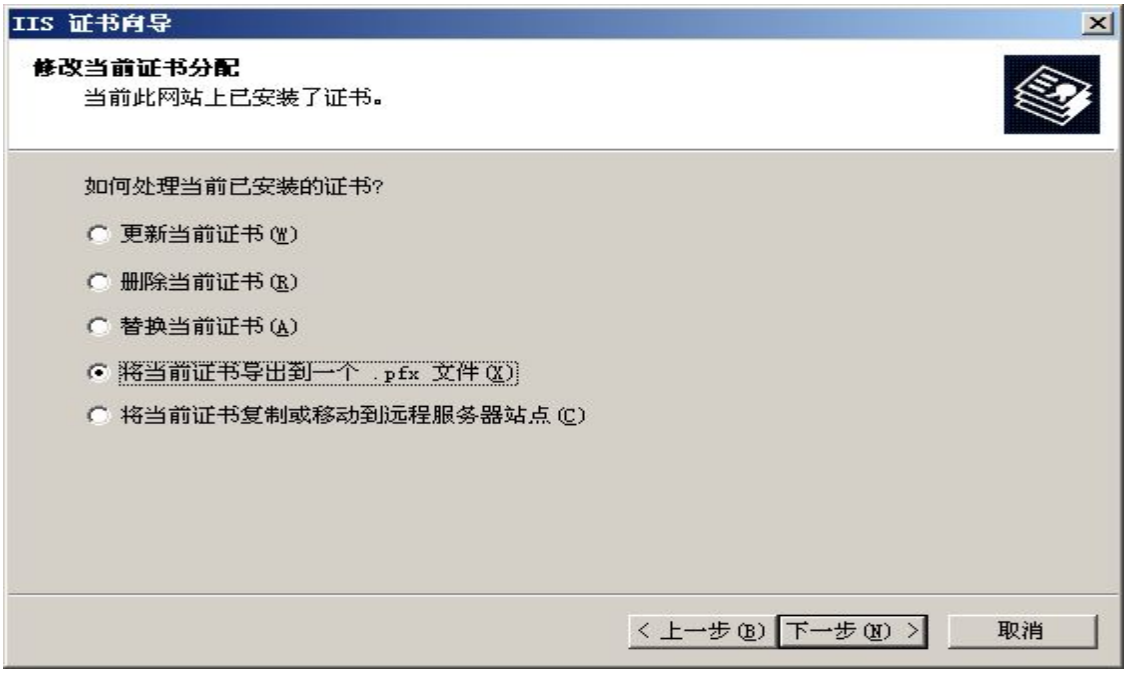
配置默认的 https 访问端口 443，重启 IIS 并使用 https 方式访问测试站点证书安装。

4. 服务器证书的备份及恢复

在您成功的安装和配置了服务器证书之后，请务必依据下面的操作流程，备份好您的服务器证书，以防证书丢失给您带来不便。操作流程如下：

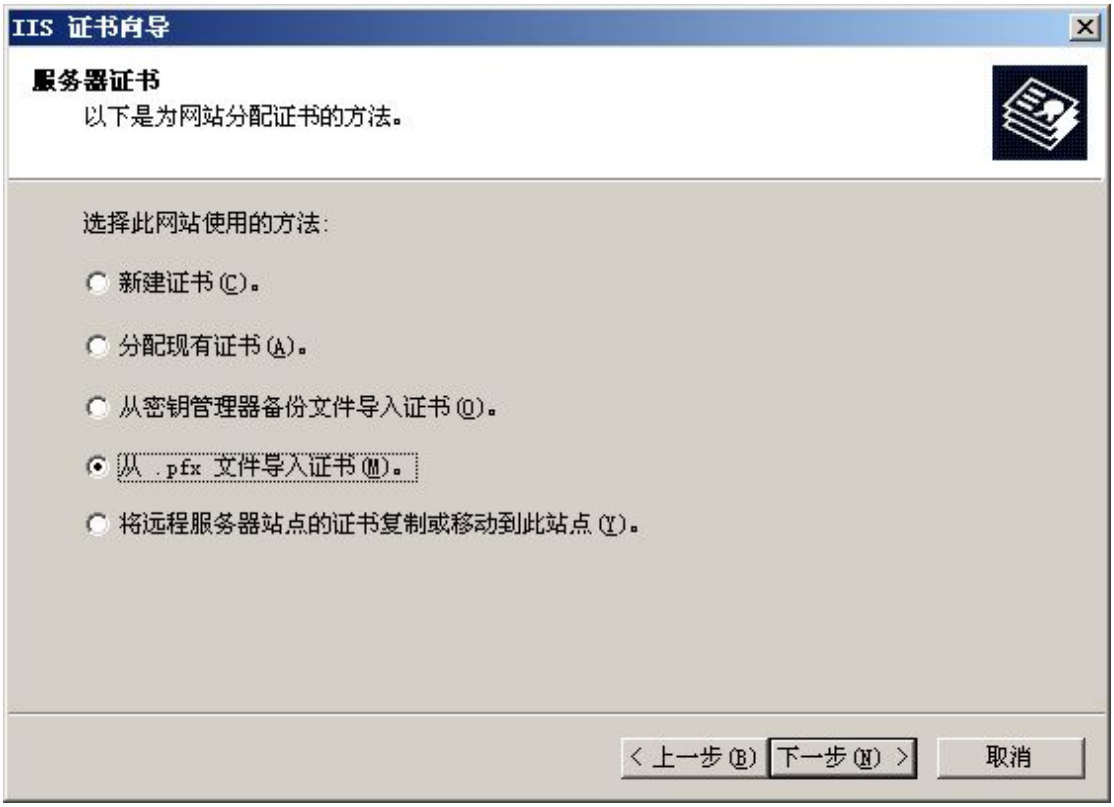
4.1 服务器证书的备份

进入 IIS 控制台，选择安装有服务器证书的站点，右键选择“属性”➔“目录安全性”➔“服务器证书”➔“将当前站点证书导出到一个.pfx 文件”



4.2 服务器证书的恢复

进入 IIS 控制台，选择安装有服务器证书的站点，右键选择“属性”➔“目录安全性”➔“服务器证书”➔“从.pfx 文件导入证书”



配置 https 默认访问端口 443，重新安装中级 CA 证书文件，重启 IIS 完成证书的恢复。