



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

1. 生成证书请求.....	1
1.1 生成证书请求文件(CSR).....	1
1.2 提交证书请求.....	4
2. 安装中级 CA 证书.....	4
2.1 获取服务器证书中级 CA 证书.....	4
2.2 配置证书证书链.....	4
3. 安装服务器证书.....	7
3.1 保存服务器证书.....	7
3.2 进入 IIS 控制台.....	7
4. 服务器证书的备份及恢复.....	9
4.1 服务器证书的备份.....	9
4.2 服务器证书的恢复.....	10

服务器证书安装配置指南 (IIS6.0)

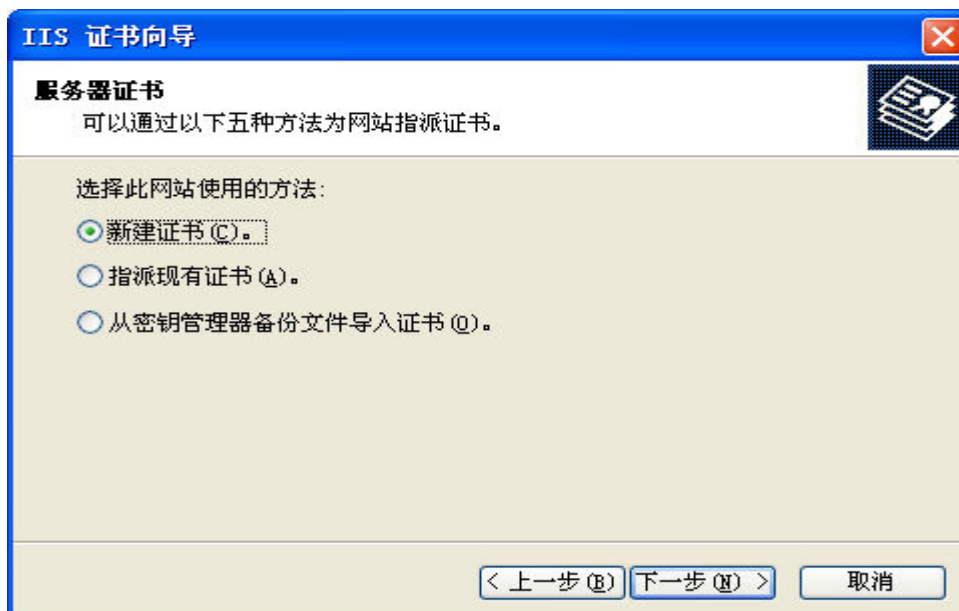
1. 生成证书请求

1.1 生成证书请求文件 (CSR)

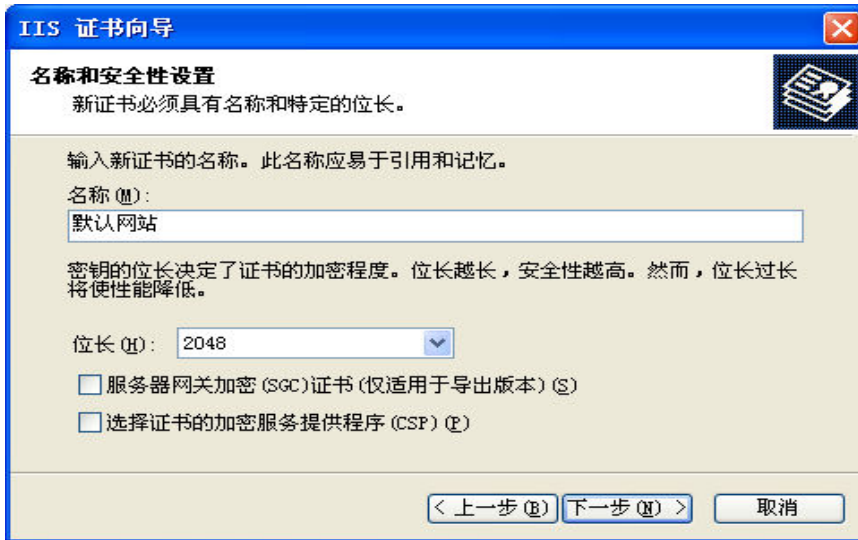
进入 IIS 管理控制台，选择需要配置证书的站点，右键选择“属性” → “目录安全性”



“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。



IIS 证书向导

名称和安全性设置
新证书必须具有名称和特定的位长。

输入新证书的名称。此名称应易于引用和记忆。

名称 (N):
默认网站

密钥的位长决定了证书的加密程度。位长越长，安全性越高。然而，位长过长将使性能降低。

位长 (L): 2048

服务器网关加密 (SGC) 证书 (仅适用于导出版本) (S)

选择证书的加密服务提供程序 (CSP) (P)

< 上一步 (P) 下一步 (N) > 取消

输入公司名称及部门信息。



IIS 证书向导

单位信息
证书必须包含您单位的相关信息，以便与其他单位的证书区分开。

选择或输入您的单位和部门名称。通常是指您的合法单位名称及部门名称。

如需详细信息，请参阅证书颁发机构的网站。

单位 (U):
GlobalSign China Co., Ltd.

部门 (D):
IT Dept.

< 上一步 (P) 下一步 (N) > 取消

公用名称栏需要填写完整域名信息

IIS 证书向导

站点公用名称

站点公用名称是其完全合格的域名。

输入站点的公用名称。如果服务器位于 Internet 上，应使用有效的 DNS 名。如果服务器位于 Intranet 上，可以使用计算机的 NetBIOS 名。

如果公用名称发生变化，则需要获取新证书。

公用名称 (C):

cn.globalsign.com

< 上一步 (B) 下一步 (N) > 取消

输入公司所在地国家、地区信息

IIS 证书向导

地理信息

证书颁发机构要求下列地理信息。

国家(地区) (C):

CN (中国)

省/自治区 (S):

Shanghai

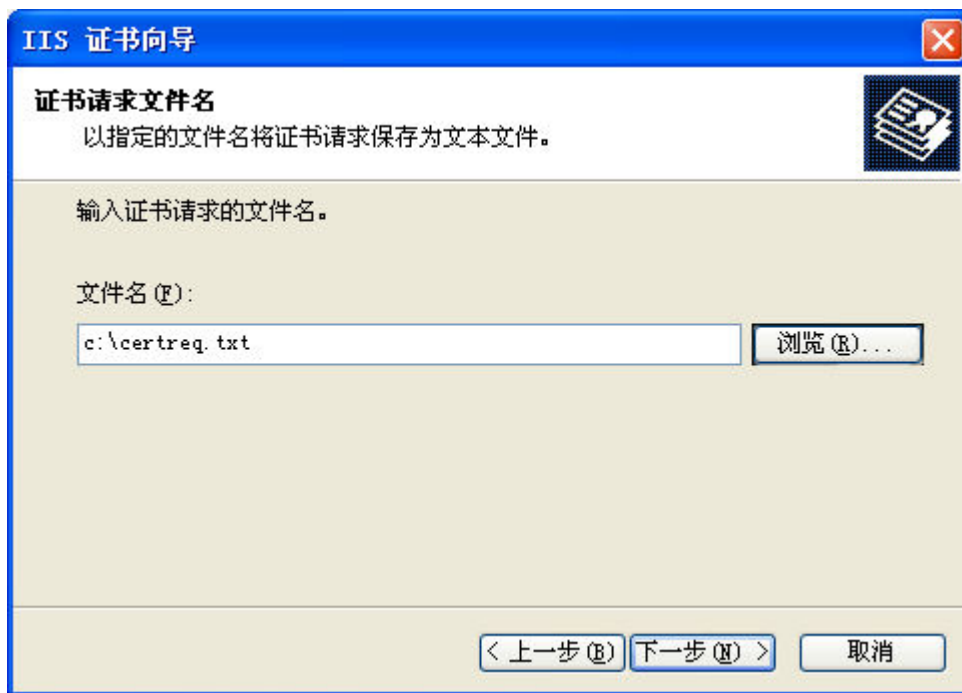
市县 (L):

Shanghai

省/自治区和市县必须是完整的官方名称，且不能包含缩写。

< 上一步 (B) 下一步 (N) > 取消

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

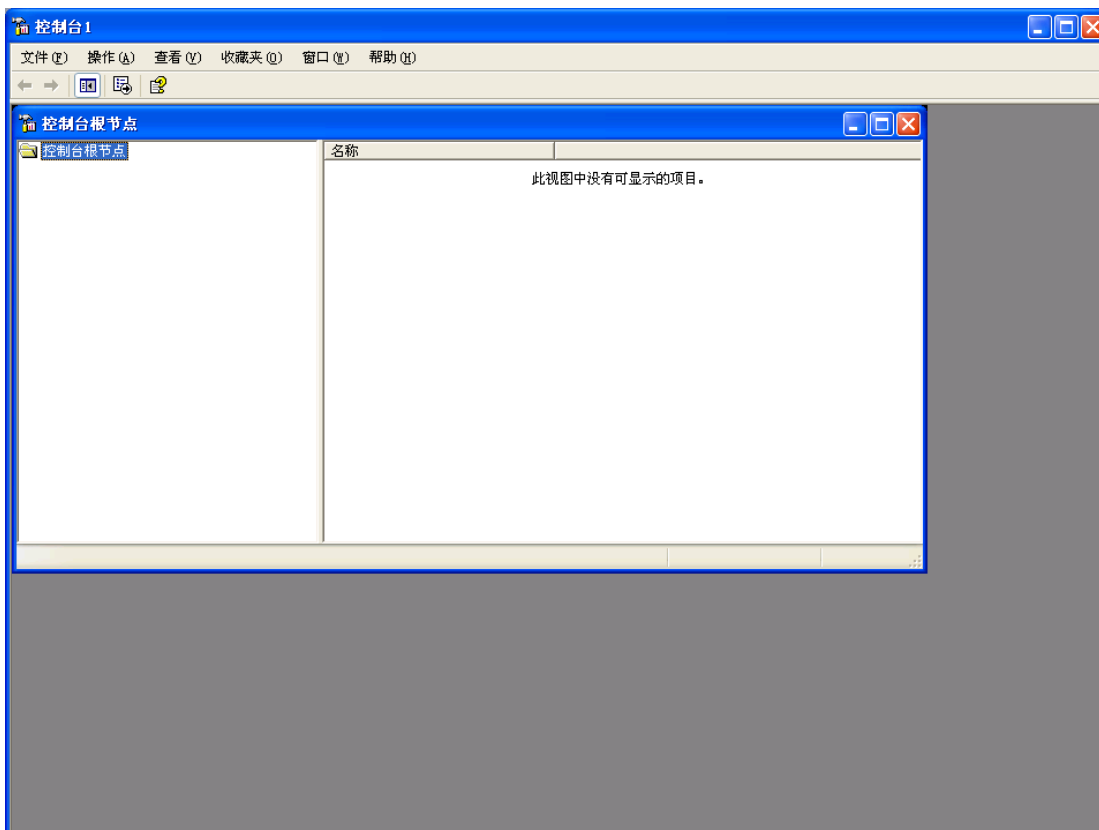
2.1 获取服务器证书中级 CA 证书

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：

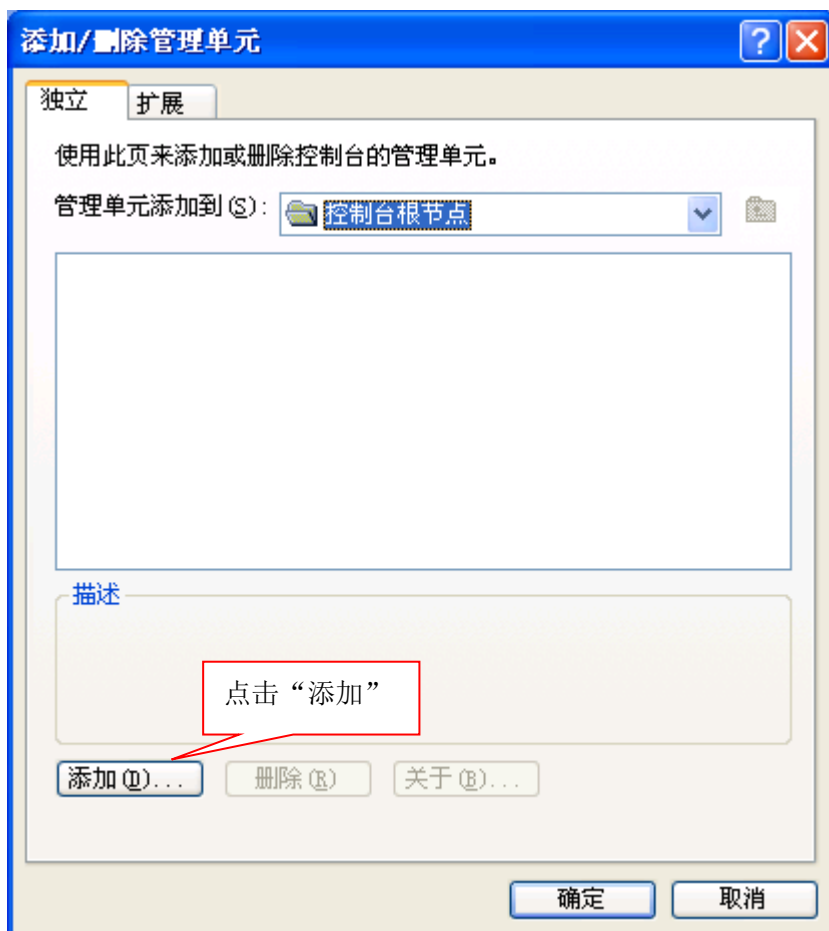
将证书签发邮件中的从 BEGIN 到 END 结束的两张中级 CA 证书内容（包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”）分别粘贴到记事本等文本编辑器中，并修改文件扩展名，保存为 intermediat1.cer 和 intermediate2.cer 文件。

2.2 配置 EV 证书证书链

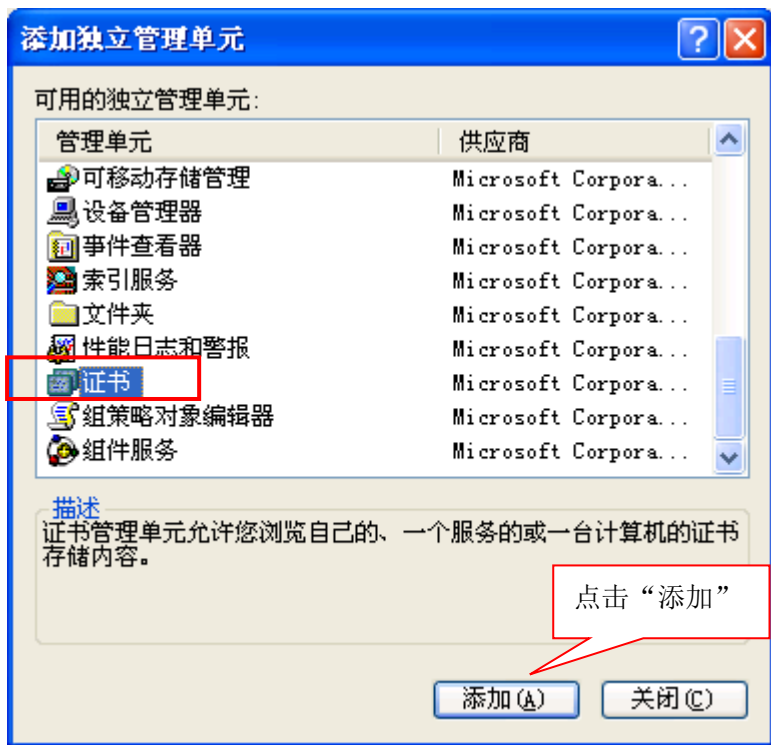
点击开始菜单，在“运行”中输入“mmc”，打开控制台窗口。



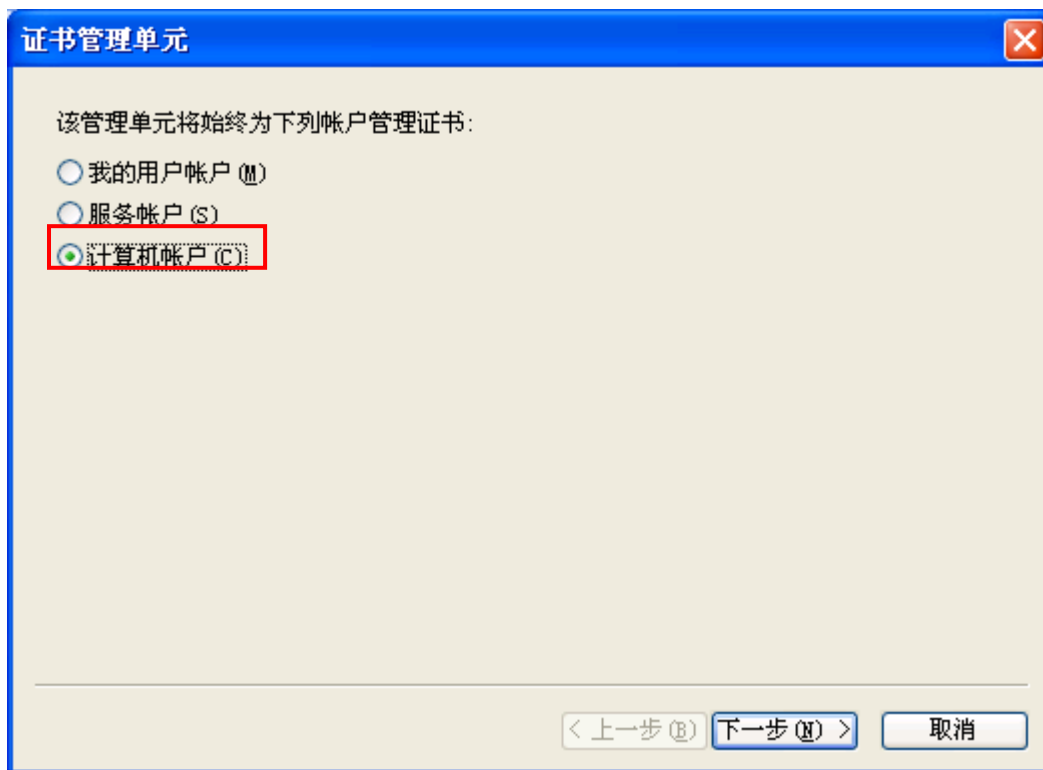
点击“文件→添加删除管理单元”



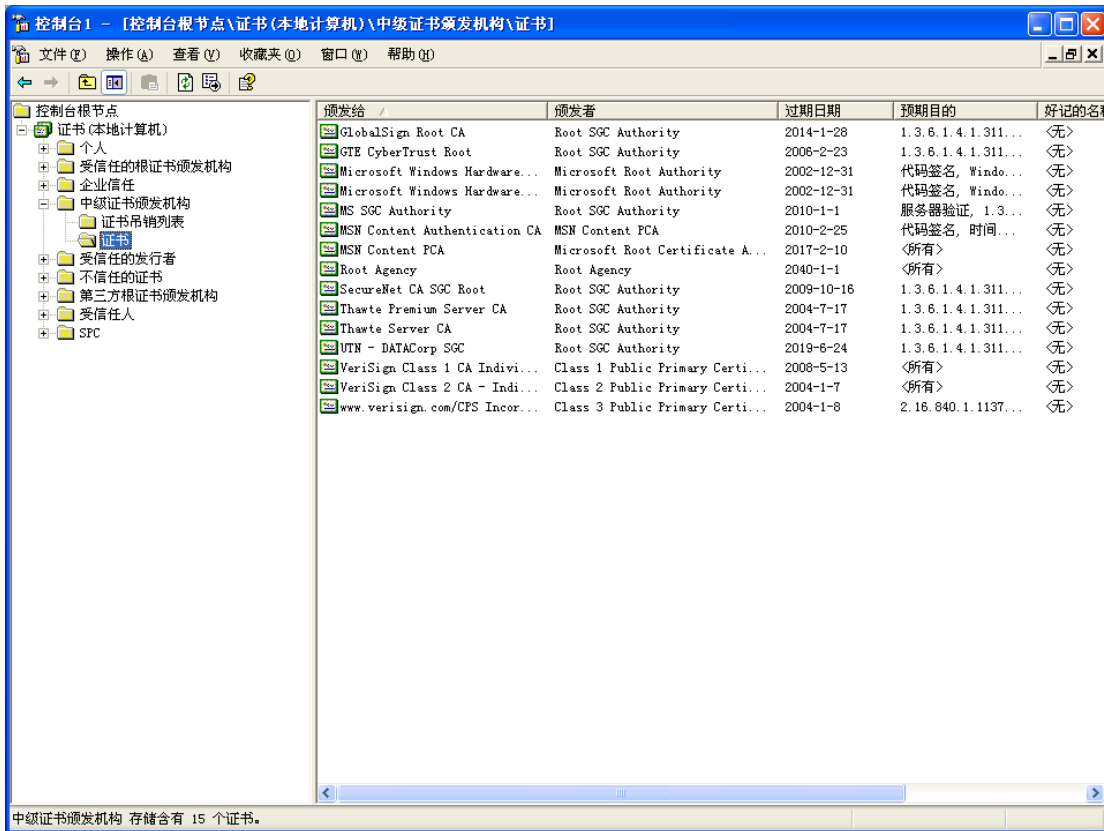
选择“证书”，然后点击“添加”：



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 intermediatel 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

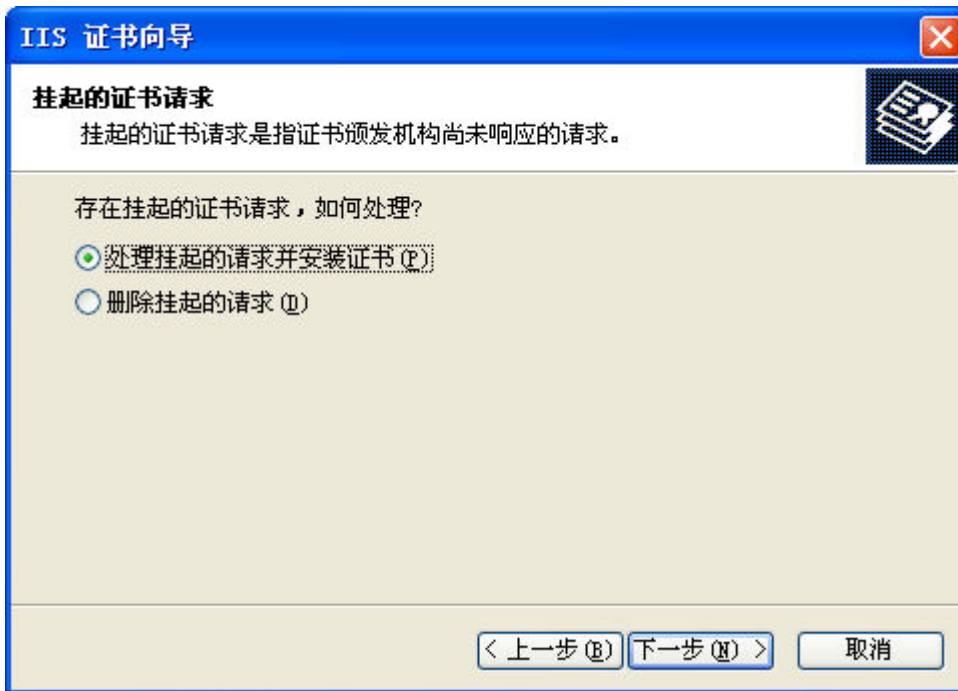
将证书签发邮件中的从 BEGIN 到 END 结束的服务器证书内容（包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”）粘贴到记事本等文本编辑器中，并修改文件扩展名，保存为 server.cer 文件。

3.2 进入 IIS 控制台

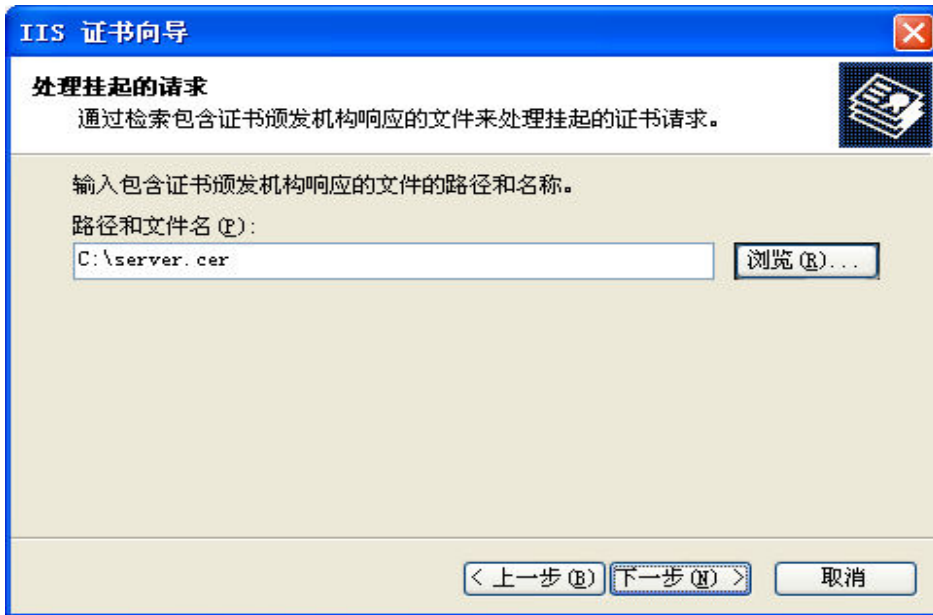
进入 IIS 控制台，并选中需要配置服务器证书的站点，“属性” → “目录安全性”



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



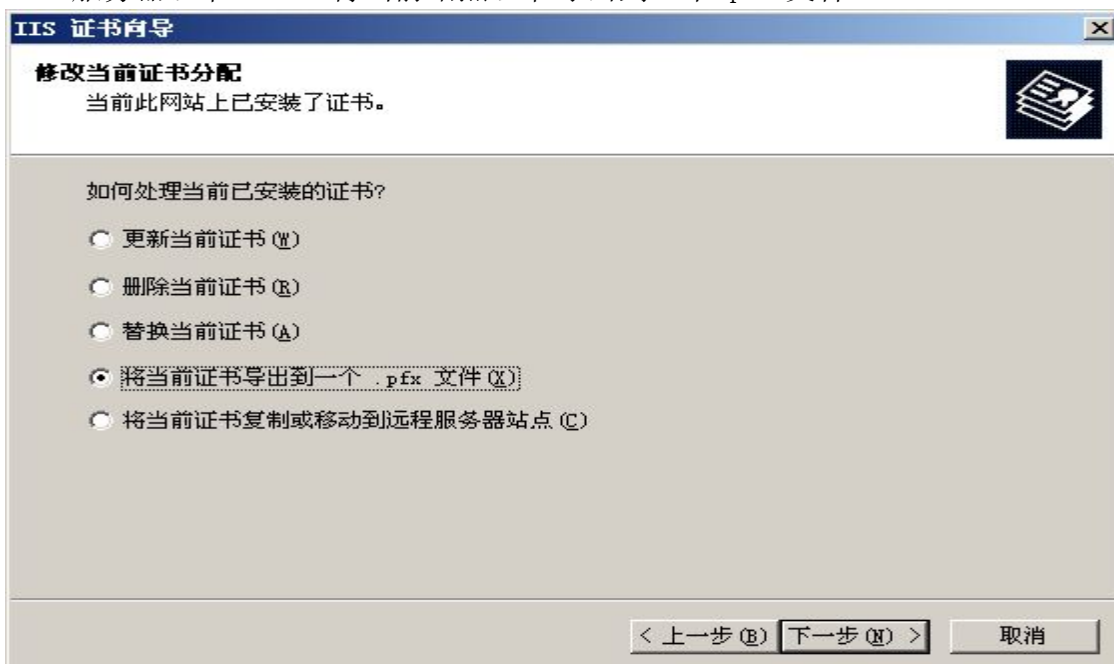
配置默认的 https 访问端口 443，重启 IIS 并使用 https 方式访问测试站点证书安装。

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。