IIS6.0SSL 证书申请部署指南

沃通电子认证服务有限公司

WoSignCA Limited

目　录

技术支持联系方式

技术支持邮箱：support@wosign.com
技术支持热线电话：0755-26027828 / 0755-26027859
技术支持网页：https://bbs.wosign.com
公司官网地址：https://www.wosign.com

一、生成证书请求文件 CSR

1.1 生成私钥和 CSR 文件

右击需要申请 SSL 证书的网站属性， 再点击“目录安全性”，最下面有一个“安全通信”栏。点击“服务器证书”就开始证书申请向导，如下图 1 所示：

图 1

1.2 创建新证书请求

如下图 2 所示：选择“新建证书”点击“下一步”即可

图 2

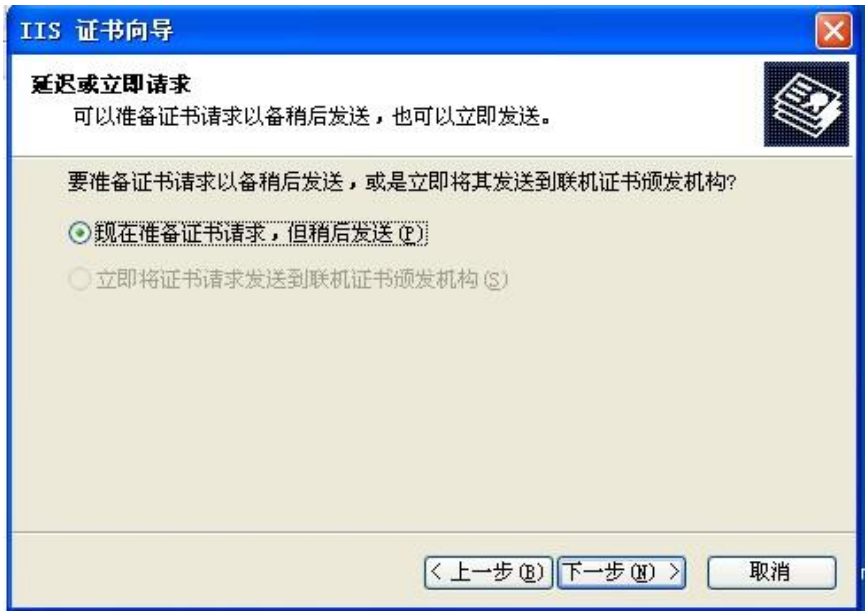

图 3

输入证书的名称和秘钥的长度，选择密钥长度，缺省的 1024 位，推荐选 2048 位，确保有足够的加密强度，点击“下一步”即可，如下图 4 所示。

图 4

输入您单位的合法单位名称，必须和营业执照或组织机构代码证上的名称一致，也可申请英文名称。

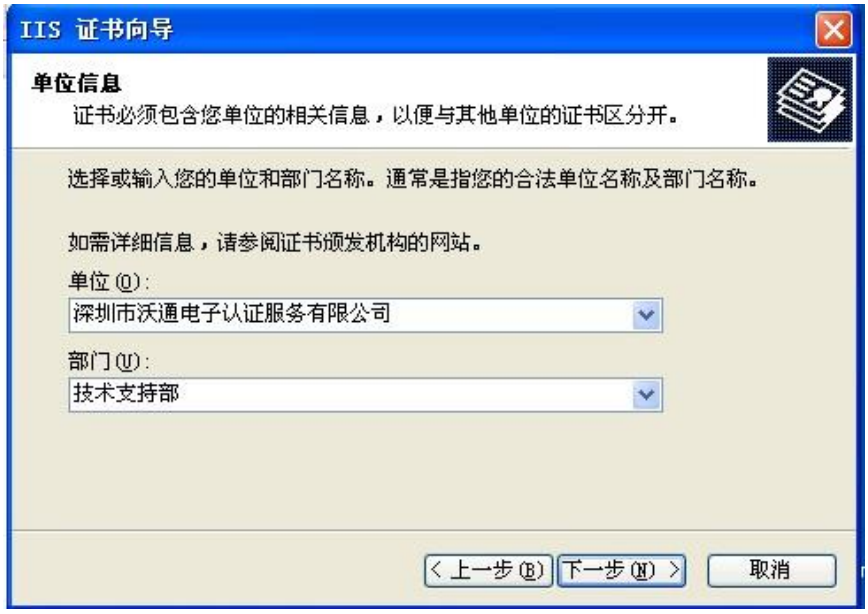

图 5

输入域名，这个比较重要，证书是需要严格绑定域名的选择国家，缺省为 CN，不用动，输入申请单位所在省或自治区全名和所在市县全名，一定要是国家规定的标准名称，而且不能是缩写。您可以输入省市中文名称，也可以输入省市英文名称。如图 6-7

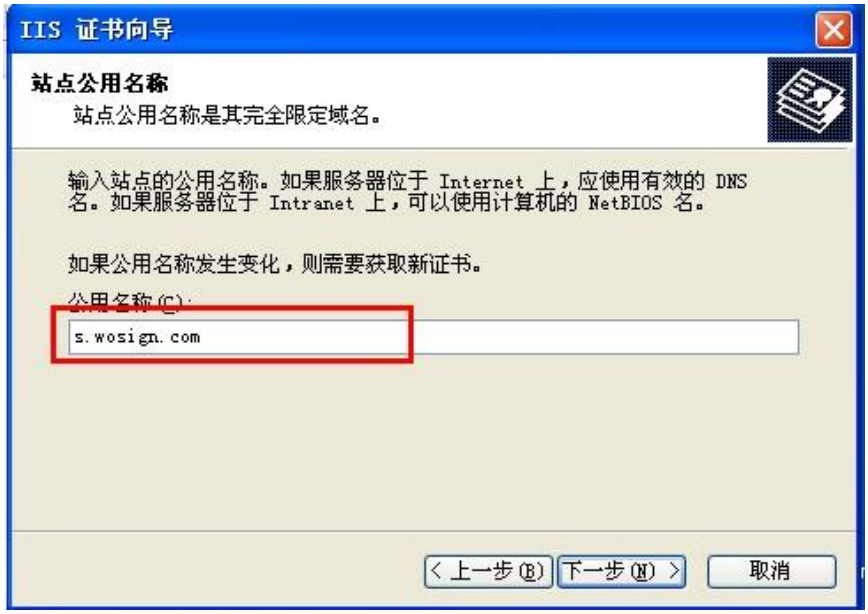

图 6

图 7

1.3 完成生成私钥和 CSR 文件

成功生成 CSR 后，建议您自己测试一下生成的 CSR 文件是否正确，请点击 测试您的 CSR 文件。请把测试成功的 CSR 文件发给 WoSign 即可。**请一定不要再动您的服务器**，等待证书的颁发。如图 8-9


IIS 证书向导
证书请求文件名
以指定的文件名将证书请求保存为文本文件。
输入证书请求的文件名。
文件名(F):
c:\wosign.txt
浏览(R)...
< 上一步(B)
下一步(N) >
取消

图 7


IIS 证书向导
请求文件摘要
已选择生成请求文件。
单击“下一步”按钮生成下列请求。
文件名: c:\wosign.txt
请求包含下列信息:
证书颁发对象 s.wosign.com
友好名称 s.wosign.com
国家(地区) CN
省/自治区 广东
市县 深圳
单位 深圳市沃通电子认证服务有限公司
部门 技术支持部
< 上一步(B)
下一步(N) >
取消

图 9

二、提交 CSR 文件

2.1 登录 wosign 站点

登录 https://login.wosign.com/；输入密码和验证码，选择客户端证书登录在线购买系统。

2.2 选择证书类型

点右上边橙色“申请证书”连接，选择您要申请的 SSL 证书，点“立即申请”，

2.3 填写资料

需要填写：证书绑定的域名，申请年限，是否需要发票，并设置证书安装密码。

2.4 验证域名邮箱

进入域名验证，可以选择邮箱验证、DNS 验证或者网站验证方式，进入下一步；

2.5 确认订单信息

用记事本打开生成好的 csr 文件，提交生成的 csr 文件，然后确认订单信息。

2.6 支付订单

可您以在线转账，也可以选择线下转账

2.7 上传证明材料

根据要求上传材料

2.8 等待证书签发

证书申请提交成功。待客服和鉴证审核，您可以联系您的客服专员咨询订单审核情况。

三、导入生成公钥

3.1 导入颁发公钥

右击需要申请 SSL 证书的网站属性， 再点击“目录安全性”，最下面有一个“安全通信”栏。点击“服务器证书 “如图 9

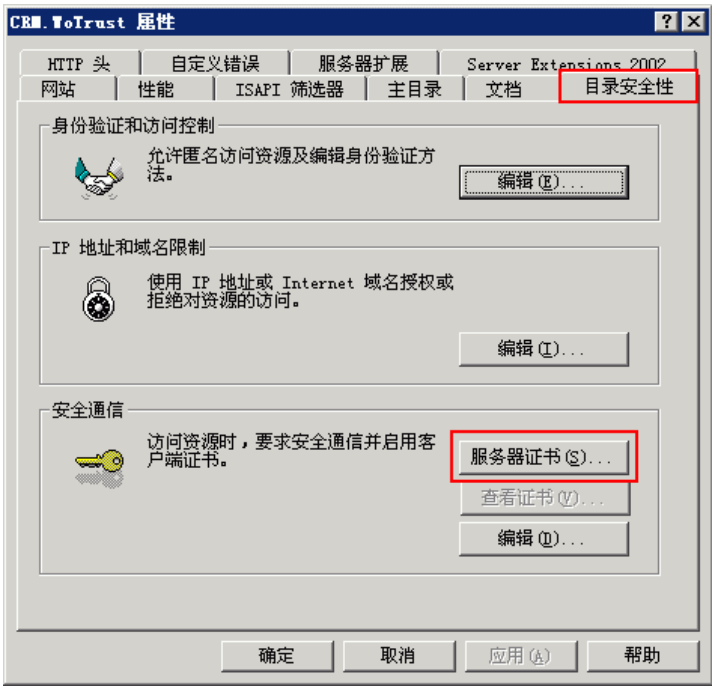

图 9

处理挂起的请求， 如下图 2 所示，选择“处理挂起的请求”，如果您要删除已经生成 CSR 和私钥的请求，则选择“删除挂起的请求”，如果证书已经颁发，则千万不能选“删除请求”，否则证书就不能安装成功！

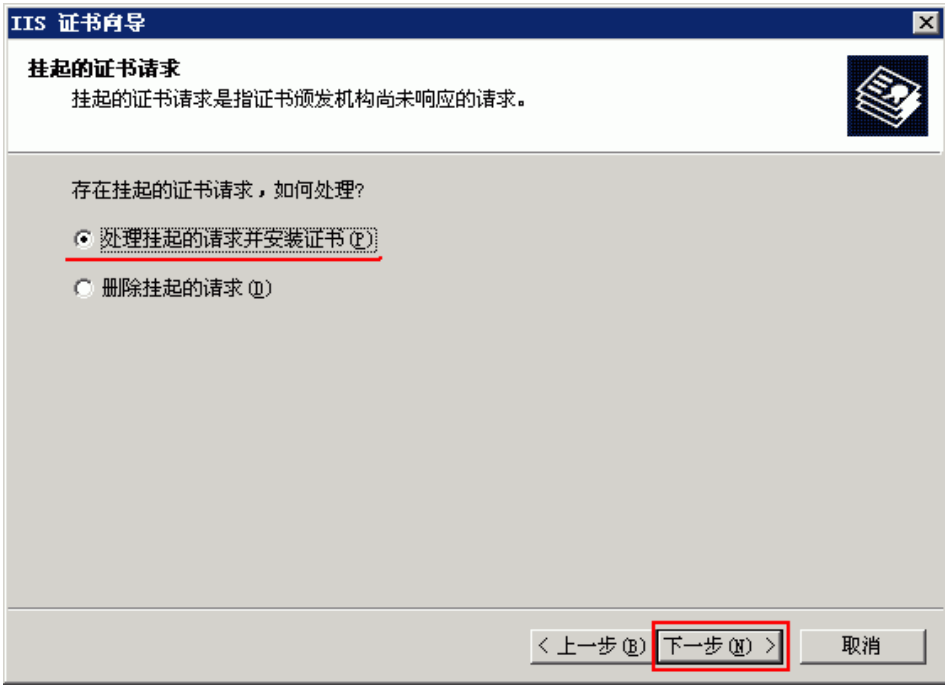

图 10

把您收到的证书文件：www.mydomain.com.zip 解压里面的 for IIS 文件会得到 3 个文件，将 3_user.domian.com.crt 上传到服务器上，并点击“浏览”选择该证书文件。

图 11

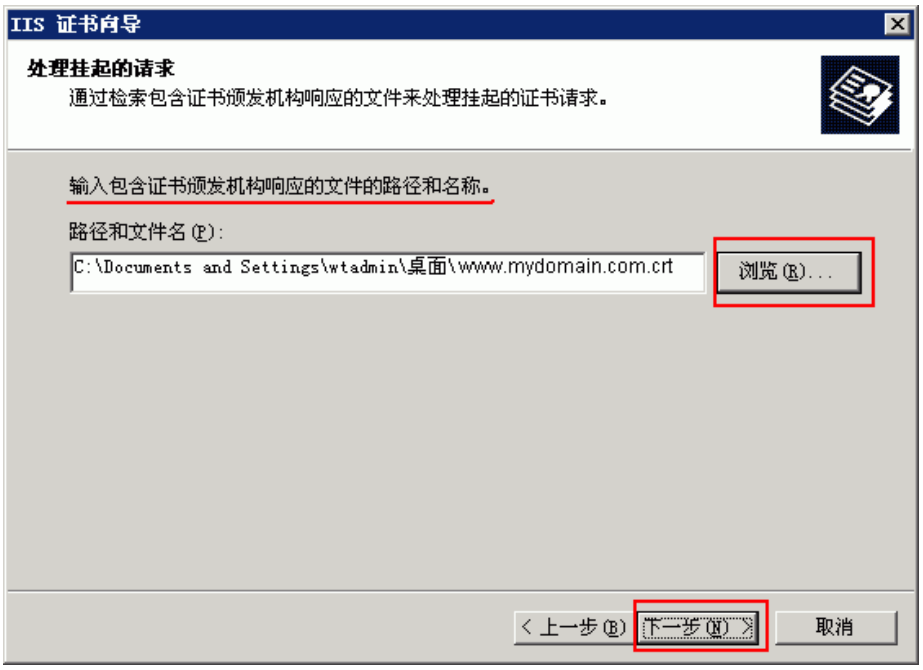

图 12

SSL 缺省端口为 443 端口，请不要修改。如果您使用其他端口如：8443，则访问时必须输入：https://www.domain.com:8443/。同时，请注意：如果您的服务器需要部署多个 SSL，则需要确定一个常用网站使用 443 端口，而其他网站则使用其他端口，并在网页中设置链接到需要设置的端口中。

同时请注意：一定要设置防火墙开放 443 端口(TCP)(包括 Windows 2003 Server 自带的防火墙)。

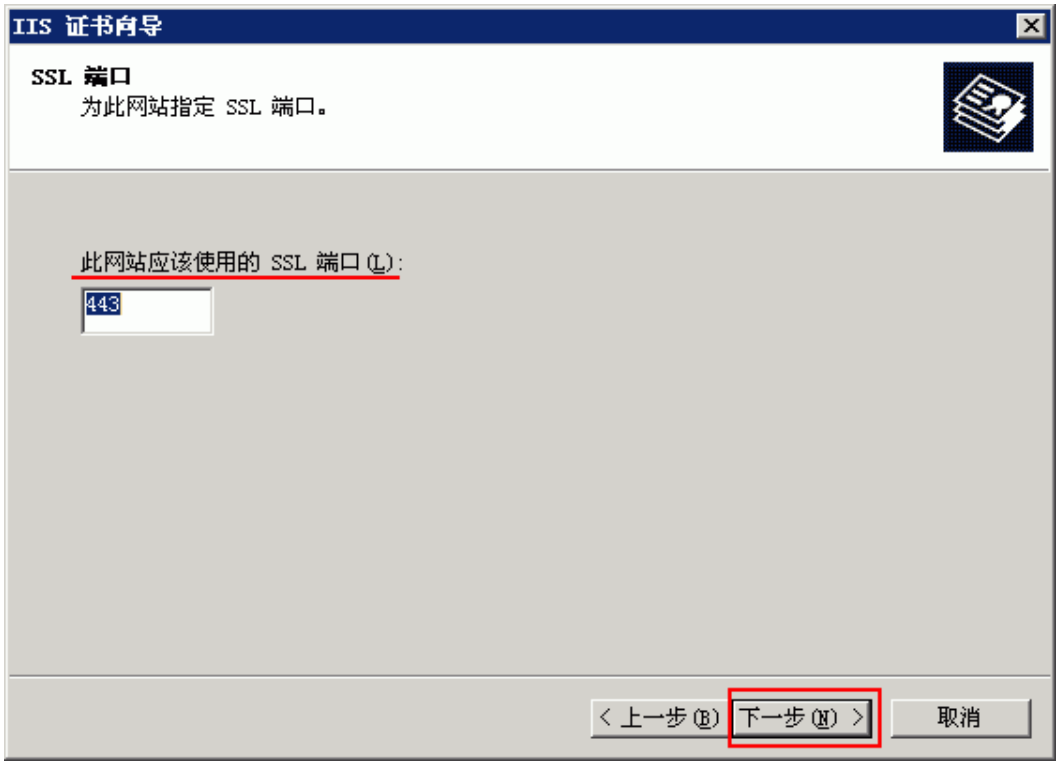

图 13

系统会显示详细的证书信息，直接点击“下一步”即可：

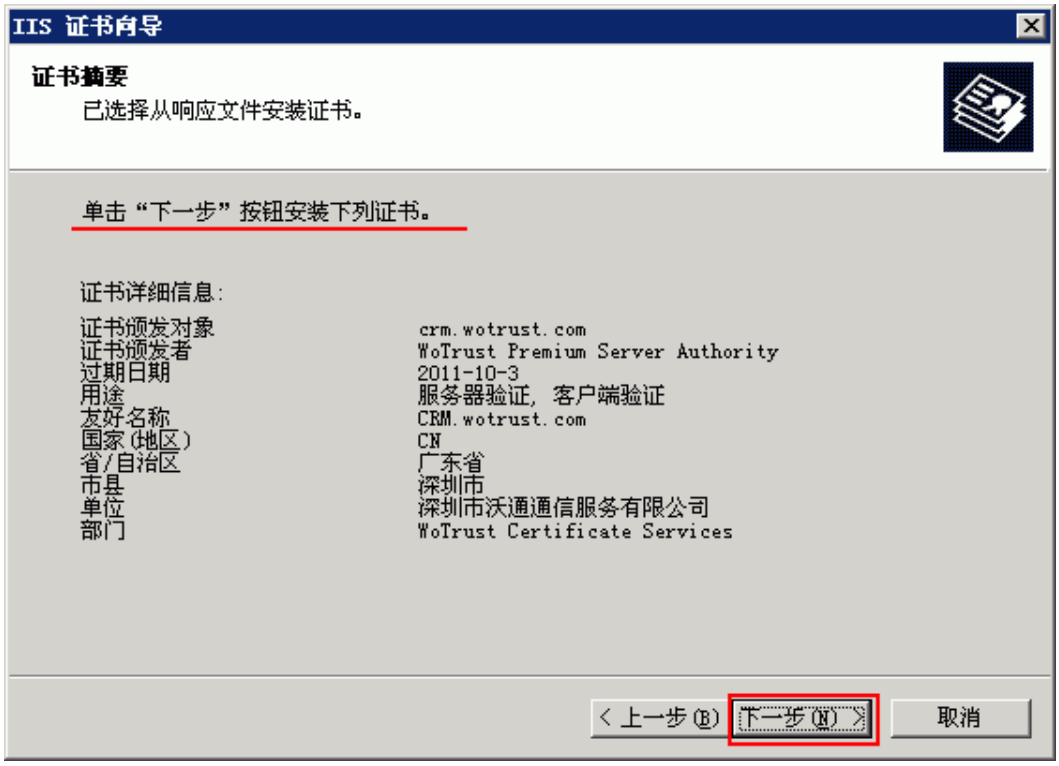

图 14

完成证书装，如图 14 所示

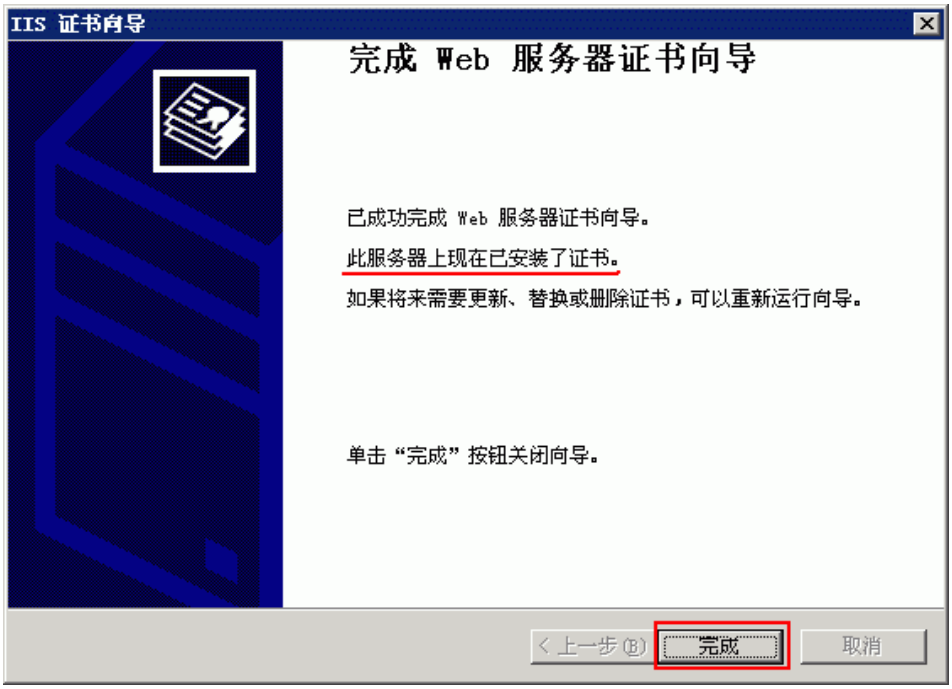

图 15

3.2 安装中级根证书

通过以上步骤已经安装成功，将文件中的另外两个 cross.crt、issue.crt 证书导入到中级证书颁发机构，开始 →运行 → MMC，启动控制台程序→ 选择菜单“文件” → “添加/删除管理单元” → “添加” → “可用的独立管理单元列表”中选择“证书” → 选择“**计算机帐户**”，选择“中级证书颁发机构”，“证书”，右键“导入”。

3.3 测试安装是否成功

重启 IIS6.0 服务，在浏览器地址栏输入：https://www.yourdomain.com (申请证书的域名)测试您的 SSL 证书是否安装成功，如果成功，则浏览器下方会显示一个安全锁标志。请注意：如果您的网页中有不安全的元素，则会提供“是否显示不安全的内容”，赶紧修改网页，删除不安全的内容(Flash、CSS、Java Script 和图片等)。

备注：安装完 ssl 证书后部分服务器可能会有以下错误，请按照链接修复

a. 加密协议和安全套件：https://bbs.wosign.com/thread-1284-1-1.html

b. 部署 https 页面后出现排版错误，或者提示网页有不安全的因素，可参考以下链接：

https://bbs.wosign.com/thread-1667-1-1.html

四、证书的备份

开始 -〉运行 -〉MMC，启动控制台程序 -> 选择菜单“文件 -〉添加/删除管理单元”->“添加”->“可用的独立管理单元”列表中选择“证书”-> 选择“**计算机帐户**”。 选择“个人”-“证书”，右键单击证书，选择“所有任务-〉导出”，如图 16 所示，

图 17

导出步骤中有一步请选择“是 导出私钥”

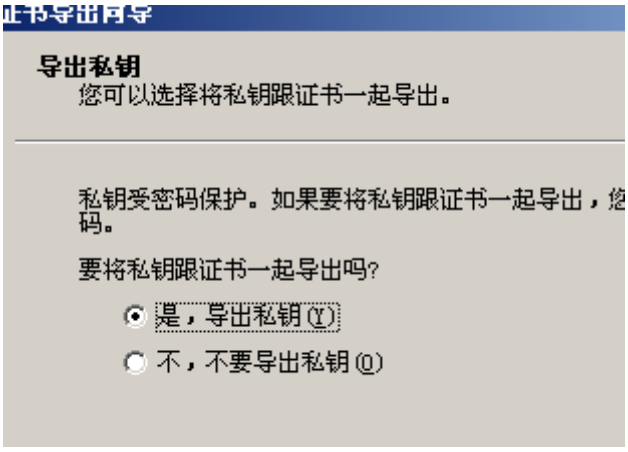

图 18

导出步骤周请选择图 18 选项，“包括证书路径中的所有证书”

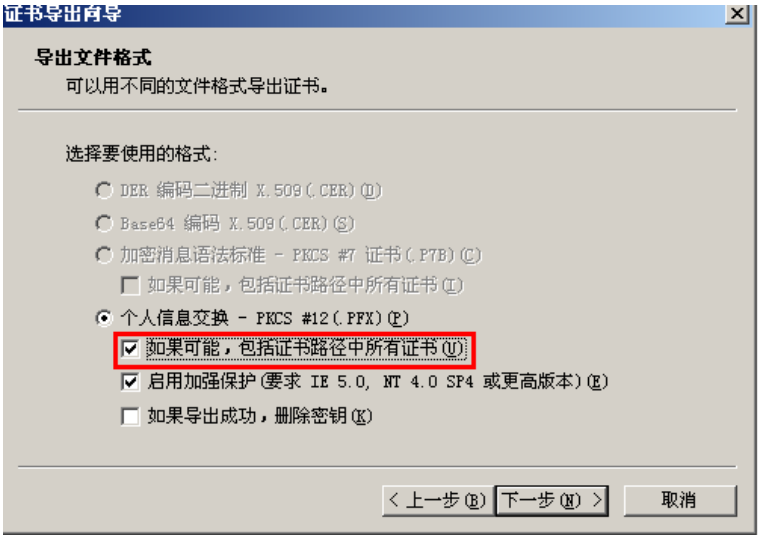

图 19

输入导出的密钥文件文件名、存储路径:，并为导出的 pfx 格式证书备份文件设置保护密码，请妥善保管 pfx 文件，以防丢失。

五、证书的恢复

请参考《IIS6.0SSL 证书部署指南》操作。