

---

# IIS7.0 SSL 证书申请部署指南



沃通电子认证服务有限公司

WoSign CA Limited

## 目 录

一、 生成证书请求文件 CSR .....	3
1.1 生成私钥和 CSR 文件 .....	3
1.2 完成生成私钥和 CSR 文件 .....	5
二、 提交 CSR 文件.....	6
2.1 登录 wosign 站点 .....	6
2.2 选择证书类型 .....	6
2.3 填写资料 .....	6
2.4 验证域名 .....	6
2.5 确认订单信息 .....	6
2.6 支付订单 .....	6
2.7 上传证明材料 .....	6
2.8 等待证书签发 .....	6
三、 证书导入 .....	7
3.1 导入颁发公钥证书 .....	7
3.2 安装中级根证书 .....	8
3.3 配置服务器证书 .....	8
3.4 测试安装是否成功 .....	9
四、 证书的备份 .....	10
五、 证书的恢复 .....	11

## 技术支持联系方式

技术支持邮箱：[support@wosign.com](mailto: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

进入 IIS 控制台，并选择服务器的“服务器证书设置”选项。



图 1

进入站点后，选择“创建证书请求”来生成 csr 请求文件，如下图 2 所示：



图 2

填写证书的详细信息，也可申请英文证书。如下图 3 所示：



图 3

选择密钥长度，缺省的 1024 位，请选 2048 位，确保有足够的加密强度，加密服务选择默认的，点击“下一步”即可，如下图 4 所示。

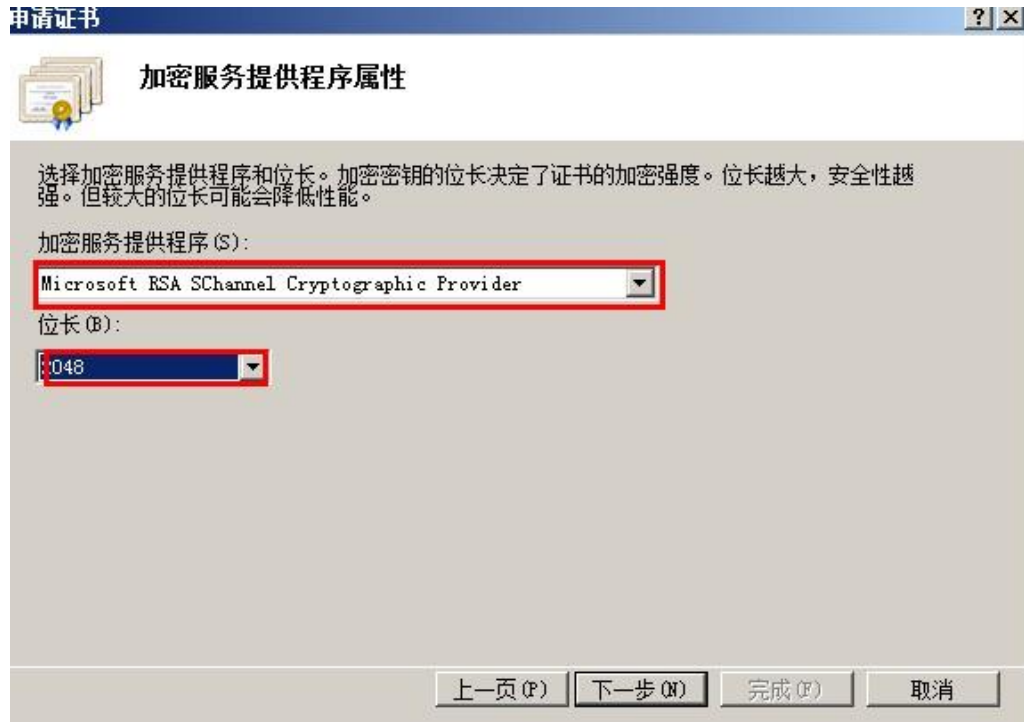


图 4

## 1.2 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 [这里](#) 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 5



图 5

## 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

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、 证书导入

#### 3.1 导入颁发公钥证书

成功申请证书后，您会收到一个压缩证书文件：www.mydomain.com.zip，解压里面的for IIS 文件会得到 3 个文件。

for Apache.zip	2014/8/22 9:47	360压缩
for IIS.zip ← 解压此文件	2014/8/22 9:47	360压缩
for Nginx.zip	2014/8/22 9:47	360压缩
for Other Server.zip	2014/8/22 9:47	360压缩

cross.crt ← 交叉根	2016/12/7 9:41	安全证书
issuer.crt ← 中级根	2016/12/7 9:41	安全证书
test.wosign.com.crt ← 公钥	2016/12/7 9:41	安全证书

图 6

点击下图页面中的“完成证书申请”。



图 7

选中 3\_user.domain.com.crt 证书文件，并为证书设置好记名称，并完成证书的导入。

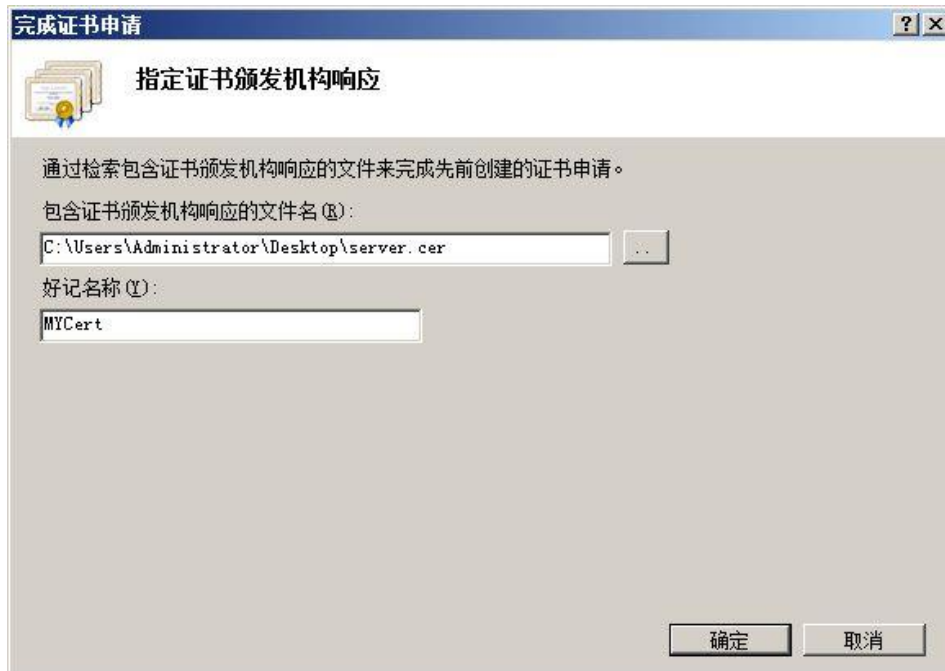


图 8

### 3.2 安装中级根证书

将文件中的另外两个证书 cross.crt、issue.crt 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 配置服务器证书

选中需要配置证书的站点, 并选择右侧“编辑站点”下的“绑定”



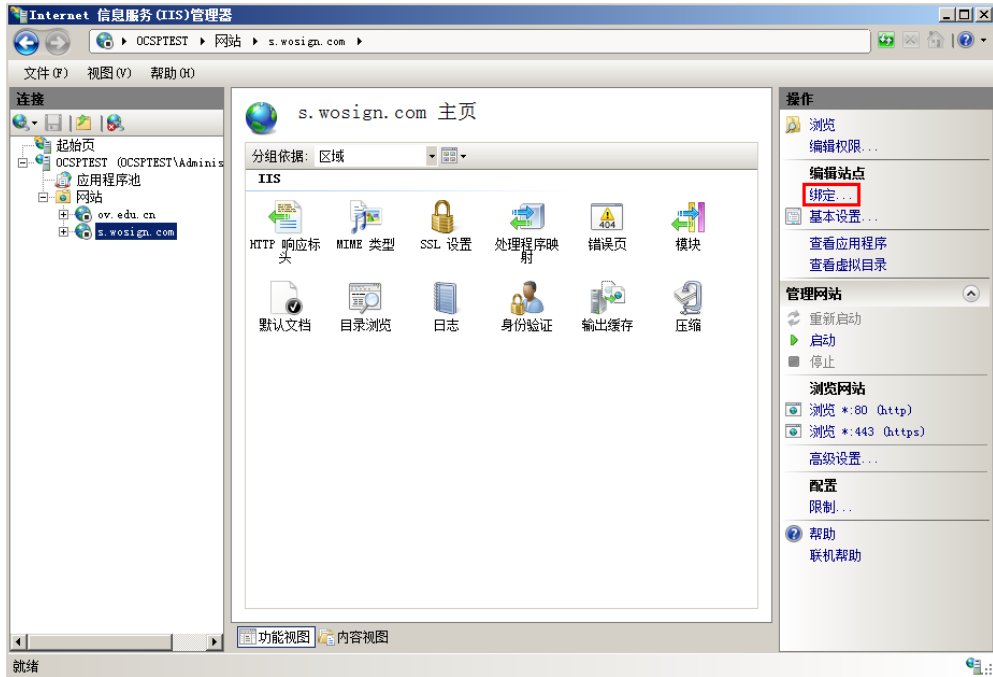
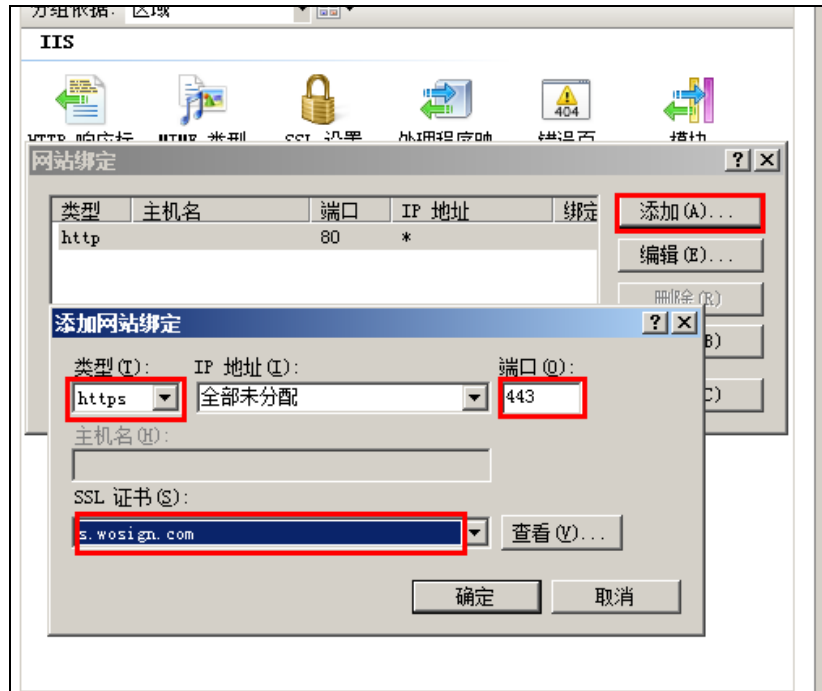


图 10

### 设置主要参数

选择“绑定” -> “添加” -> “类型选择 https” -> “端口 443” -> “ssl 证书【导入的证书名称】” -> “确定”，SSL 缺省端口为 443 端口，IP 地址根据站点实际情况选择。（请不要随便修改。如果您使用其他端口如：8443，则访问时必须输入：<https://www.domain.com:8443>）。如图



### 3.4 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 11 所示，



图 11

导出步骤中有一步请选择“是 导出私钥”

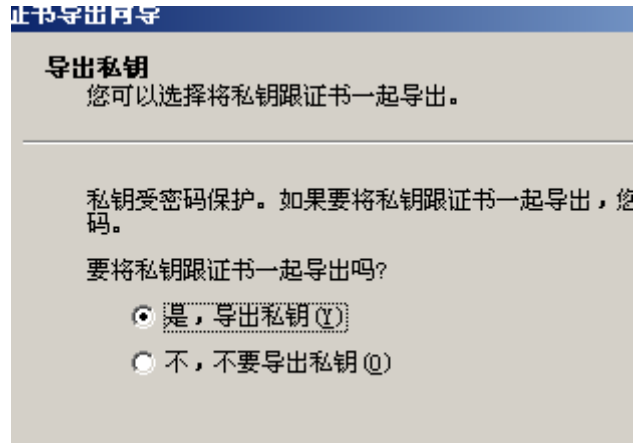


图 12

导出步骤周请选择图 13 选项，“包括证书路径中的所有证书”

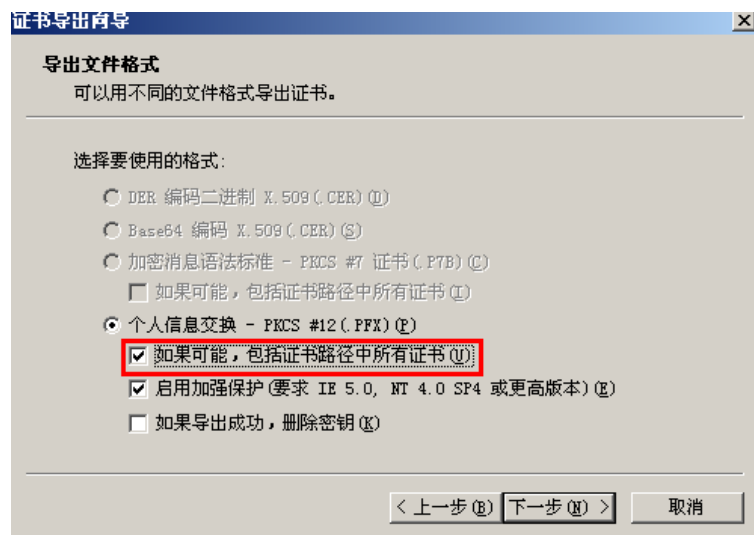


图 13

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《IIS7.0SSL 证书部署指南》操作。