广东省数字证书认证中心

GDCA 信鉴易® SSL 服务器证书部署指南

For IIS 6版本

2015/11/20

目录

一、 部署前特别说明

1) 本文档是 GDCA 信鉴易® SSL 服务器证书部署指南(以下简称“本部署指南”),主要描述如何在 IIS 服务器上产生密钥和将 SSL 服务器证书安装到 IIS 服务器
2) 本文档配置基于 Windows server 2003 操作系统
3) 本安装指南的适用范围:IIS6 版本，IIS5 以下版本(含 IIS 5)没有经过严格测试
4) 服务器安装恒信企业 EV SSL 和睿信 OV SSL 证书的操作步骤一致,区别在于:前者在 IE7 以上浏览器访问时,浏览器会显示安全锁标志,地址栏会变成绿色;而后者在浏览器访问时,浏览器显示安全锁标志，但地址栏不变绿色
5) 本部署指南使用 testweb.95105813.cn 作为样例进行安装配置，实际部署过程请用户根据正式的域名进行配置
6) Windows server 2003 不支持 SHA256 算法,需下载微软 HotFix KB968730 补丁 才能正常安装。

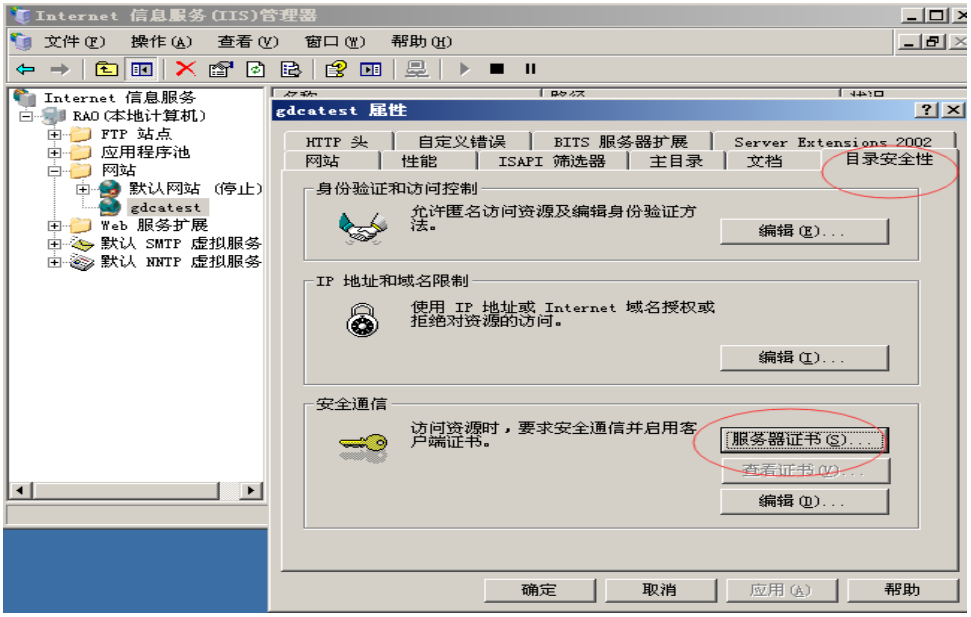
二、 生成证书请求

1. 说明

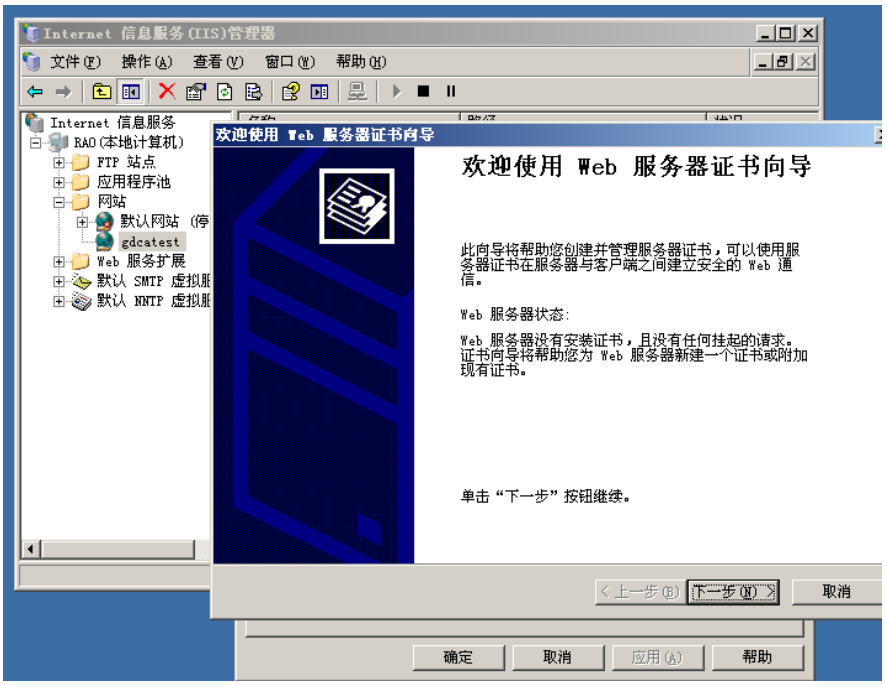
1) 如果您已经拿到证书可跳过此步直接查阅第二步安装证书。
2) 您可以使用您自己的方式生成证书请求文件并不要求必须使用以下方式。

2. 生成证书请求文件

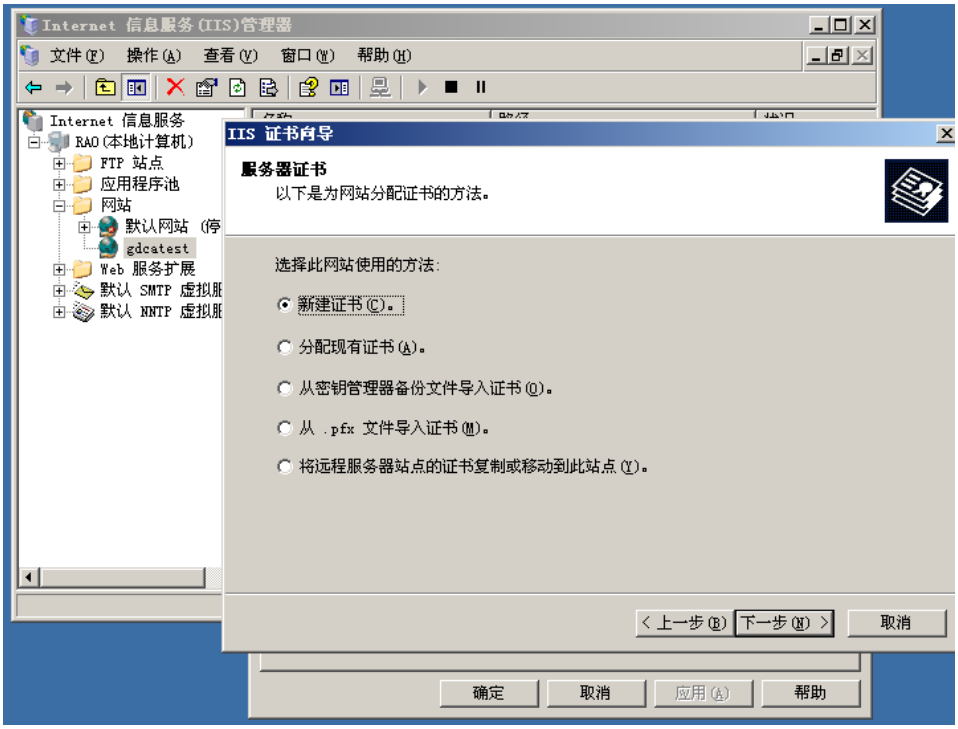
1) 进入 IIS 管理控制台，选择需要配置证书的站点，右键选择“属性”-选择“目录安全性” -“服务器证书”



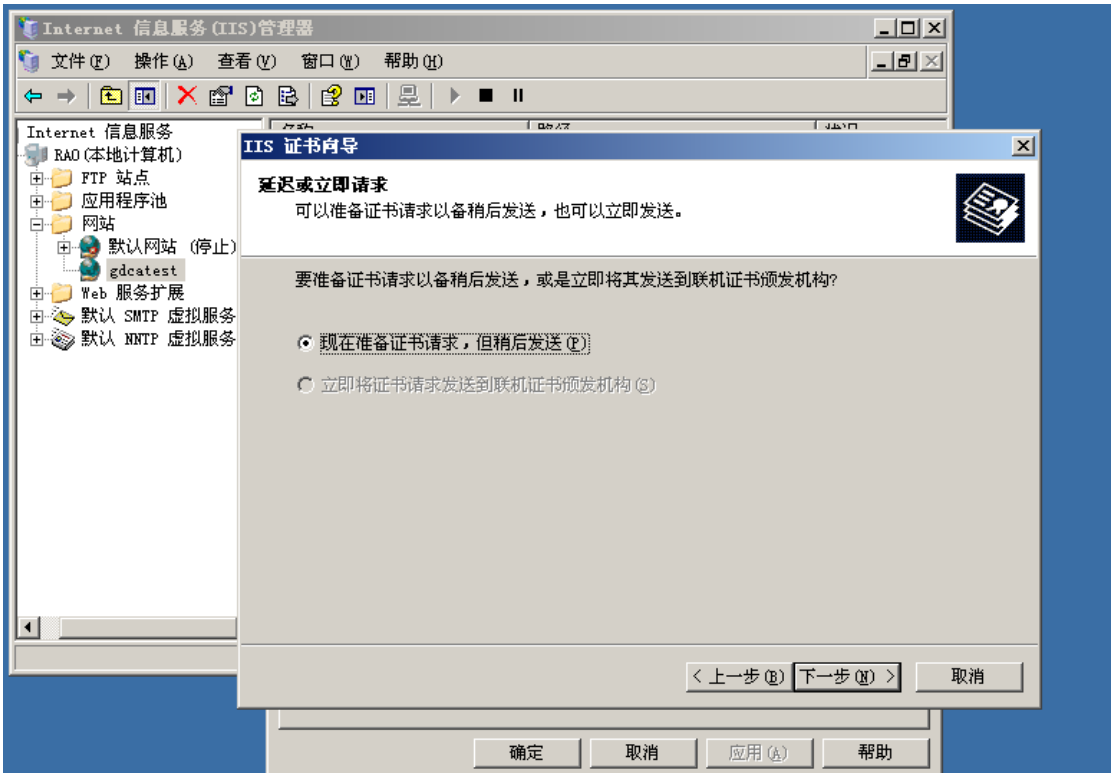
2） 进入服务器证书向导后，点击下一步



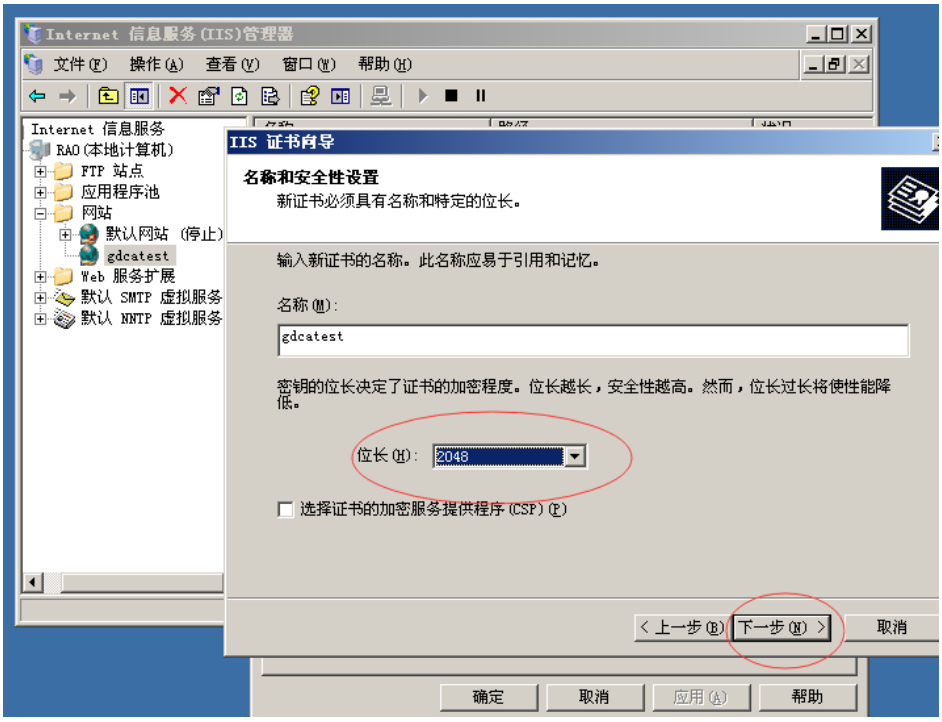
3） 选择“新建证书”，点击下一步



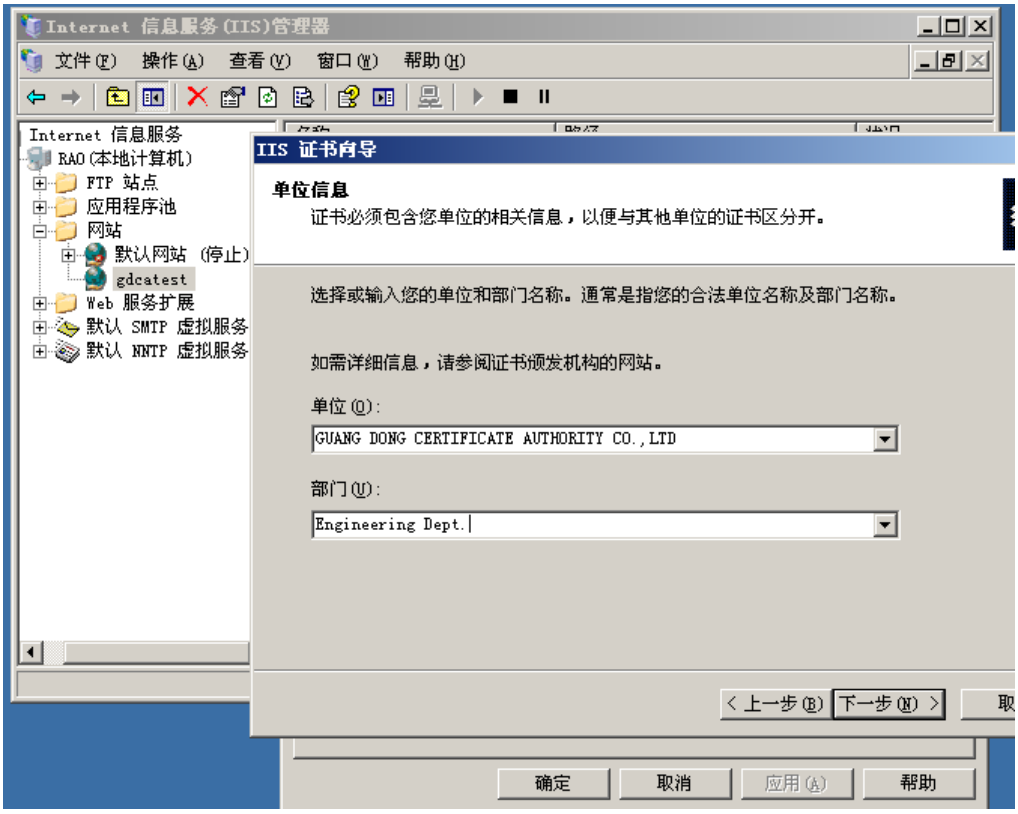
4) 选择“现在准备证书请求”继续进行下一步:



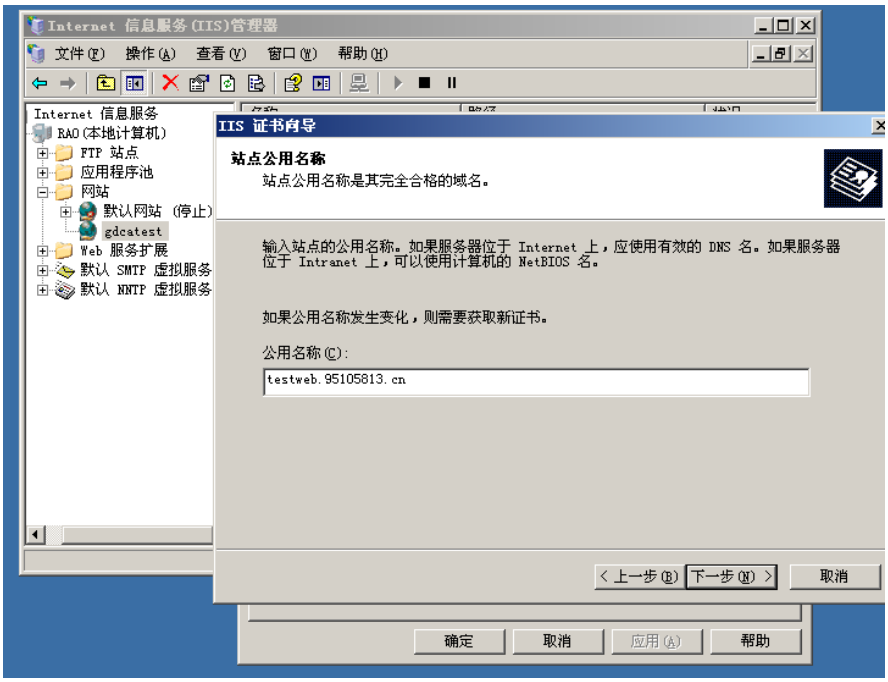
5) 为证书输入名称,并通过位长设置服务器证书密钥长度,支持 2048 位加密长度,点击“下一步”即可,如下图所示:



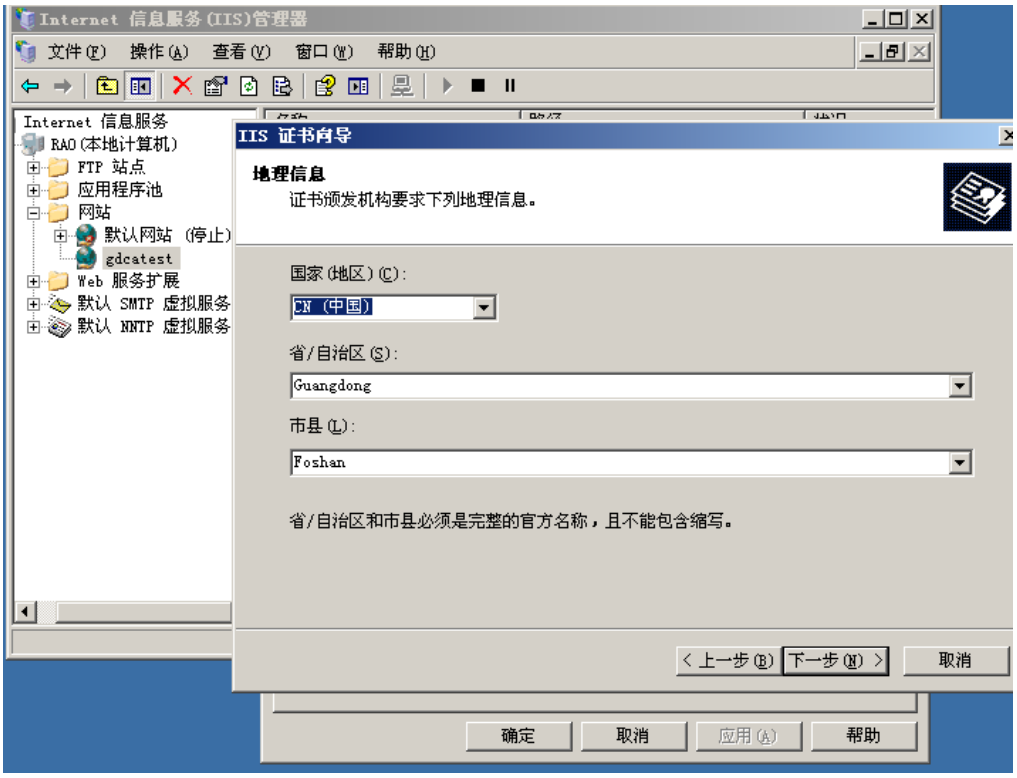
6） 输入公司名称及部门信息(注:请务必填写准确的信息，填写内容可用英文也可用中文)



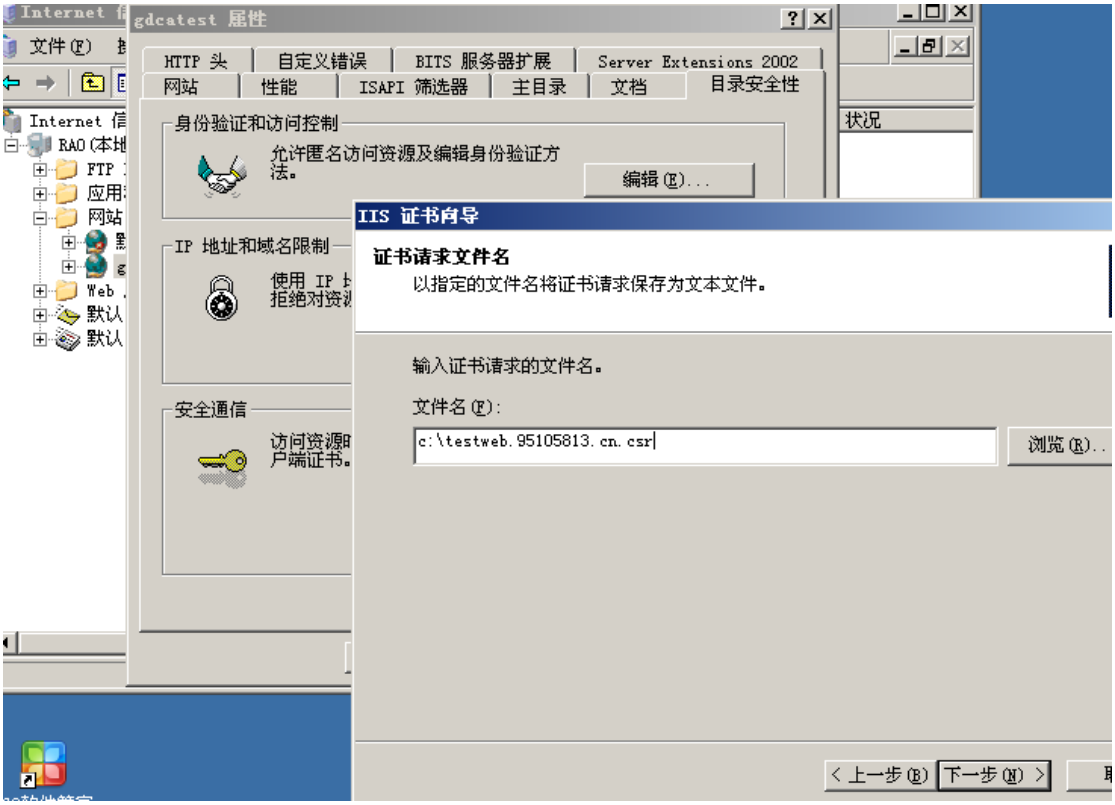
7） 公用名称栏需要填写完整域名信息（注:请务必填写准确的信息）



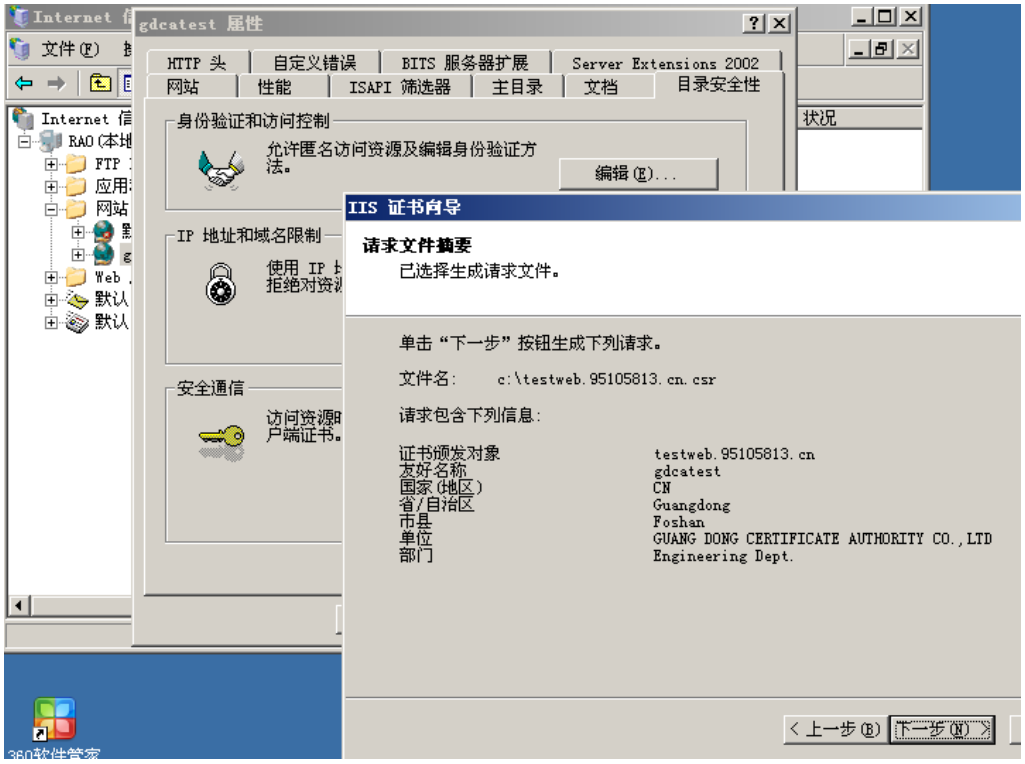
8） 输入公司所在地国家、地区信息(注:请务必填写准确的信息，填写内容可用英文也可用中文）



9） 指定文件名保存，然后点击下一步



10) 确认请求文件摘要，点击下一步，完成生成 P10 文件。



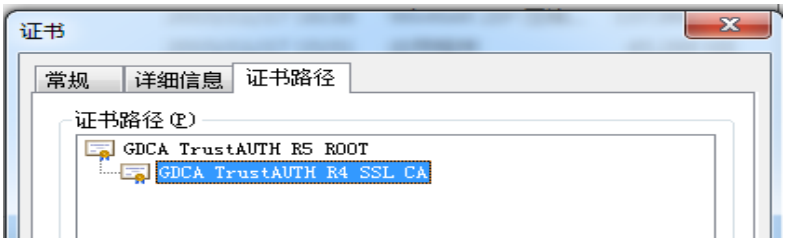
11) 请将生成的 P10 文件另存为.csr 文件后提交给 GDCA 进行审批。

三、 部署证书

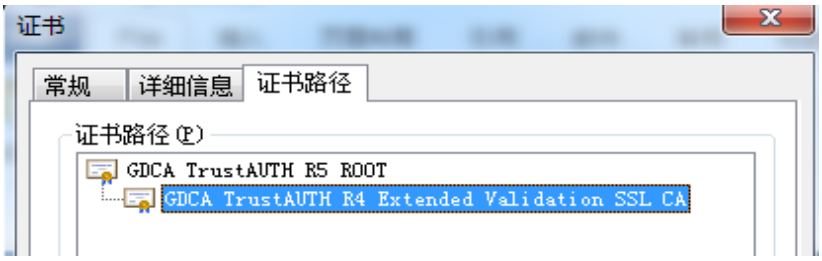
1. 获取服务器证书的根证书和 CA 证书

1) 在您完成申请 GDCA 服务器证书的流程后，GDCA 将会在返回给您的邮件中附上根证书 GDCA_TrustAUTH_R5_ROOT.cer 和相应的 CA 证书。如果您申请的是睿信(OV) SSL 证书（Organization Validation SSL Certificate),CA 证书就是文件就是 GDCA_TrustAUTH_R4_SSL_CA.cer;如果您申请的是恒信企业 EV SSL 证书（Extended Validation SSL Certificate ），CA 证书就是文件就是 GDCA_TrustAUTH_R4_Extended_Validation_SSL_CA.cer,请确认所收到的证书文件是您需要的 CA 证书。

GDCA_TrustAUTH_R4_SSL_CA.cer：



GDCA_TrustAUTH_R4_Extended_Validation_SSL_CA.cer:

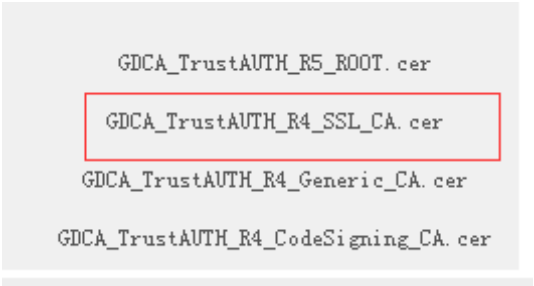


2) 从 GDCA 官网上下载 http://www.gdca.com.cn/channel/001002002

获取第一张证书：根证书 GDCA_TrustAUTH_R5_ROOT.cer 详细如下图所示：

获取第二张证书：

CA 证书如果您申请的证书是睿信(OV) SSL 证书（Organization Validation SSL Certificate），下载：GDCA_TrustAuTH_R4_SSL_CA.cer

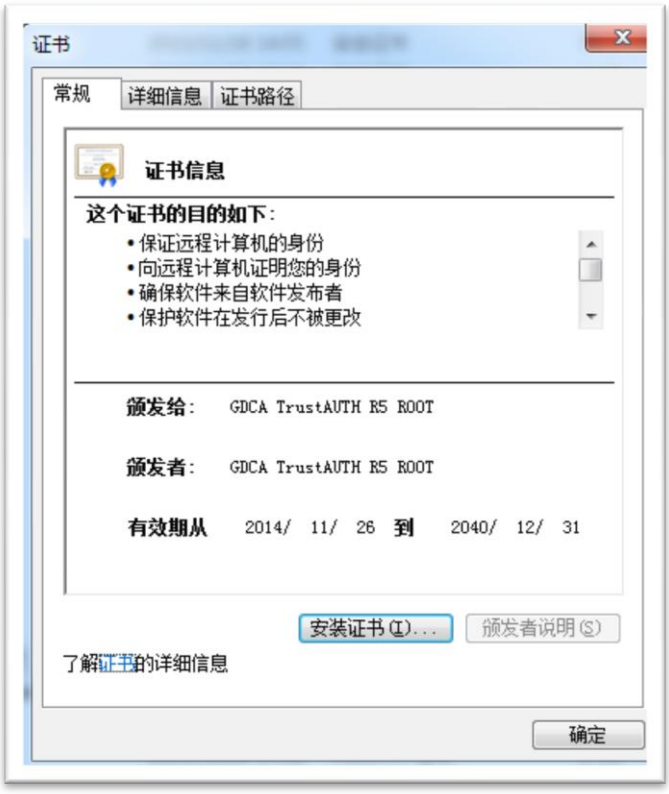


如果您申请的证书是恒信企业 EV SSL 证书（Extended Validation SSL Certificate）则下载：GDCA_TrustAUTH_R4_Extended_Validation_SSL_CA.cer

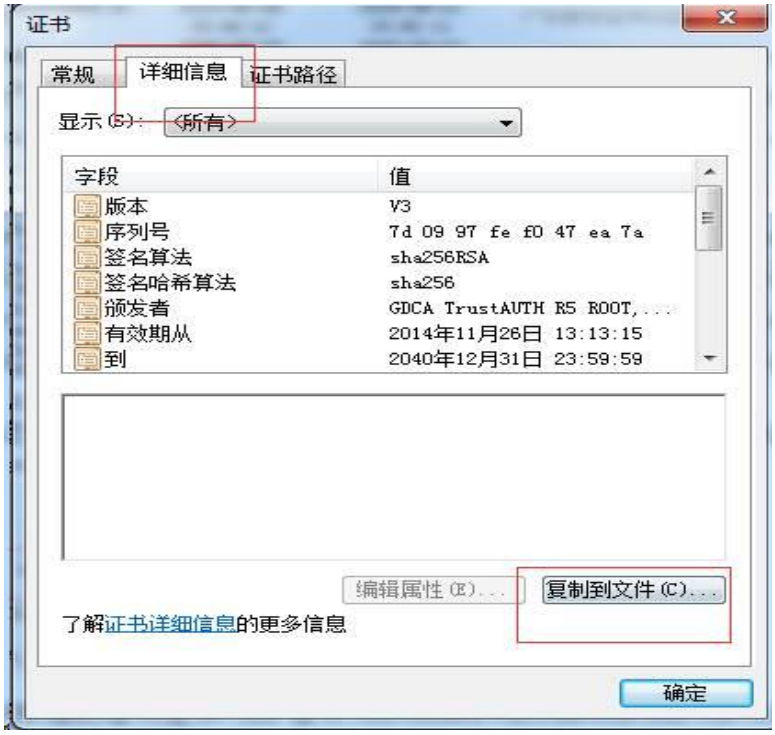
12 项，显示 11 到12.[首页/前一页] 1, 2 [下一页/末页]

CA名称	起始有效时间	截止有效时间	CA证书下载
GDCA TrustAUTH R4 Extended Validation SSL CA	2014-11-26 17:45:25	2030-12-31 00:00:00	GDCA_TrustAUTH_R4_Extended_Validation_SSL_CA.cer

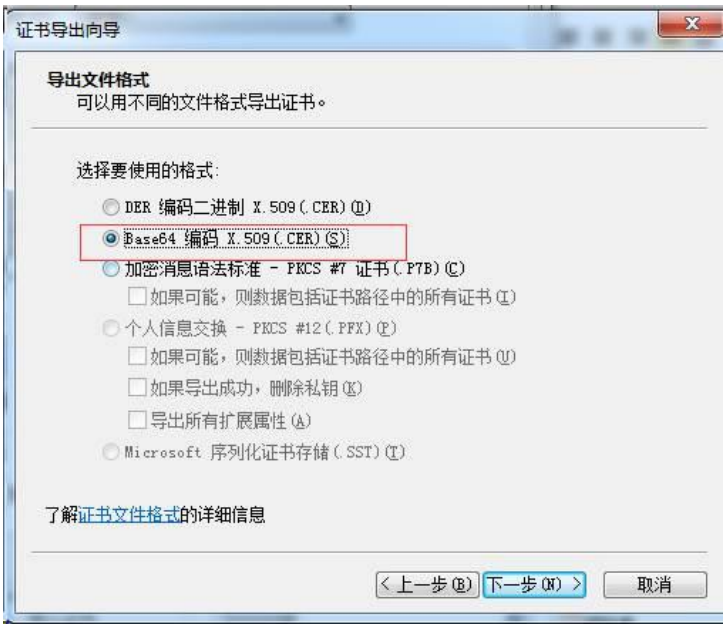
3) 从官网上下载的证书需要先转换为 Base64 编码格式。以根证书为例：打开证书：



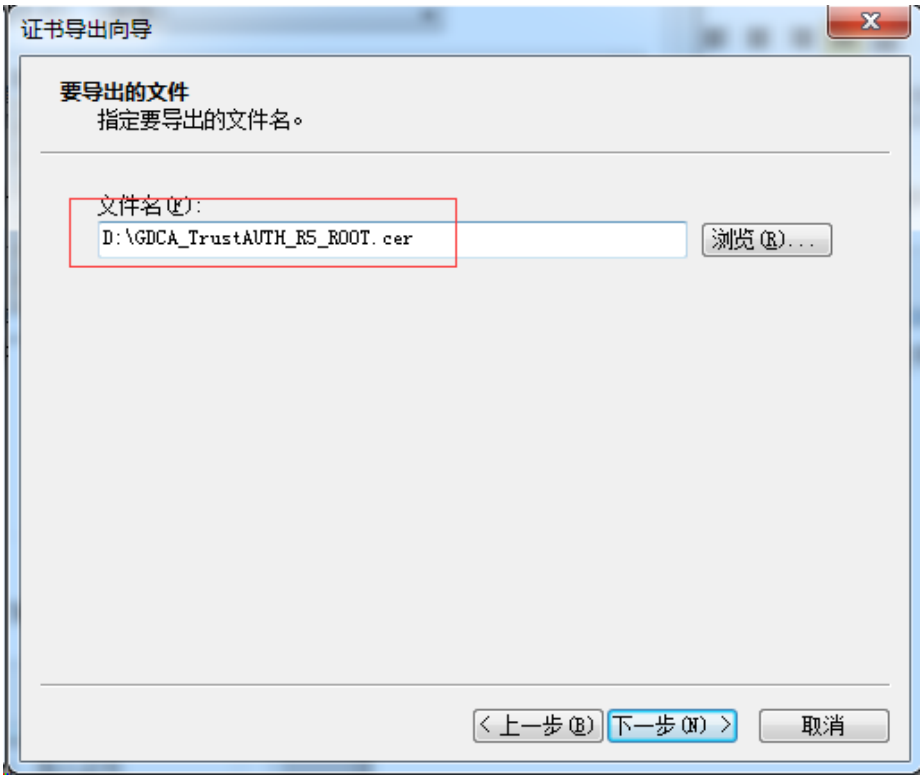
详细信息-复制到文件



在证书导出向导里，将证书编码改成 Base64 编码格式



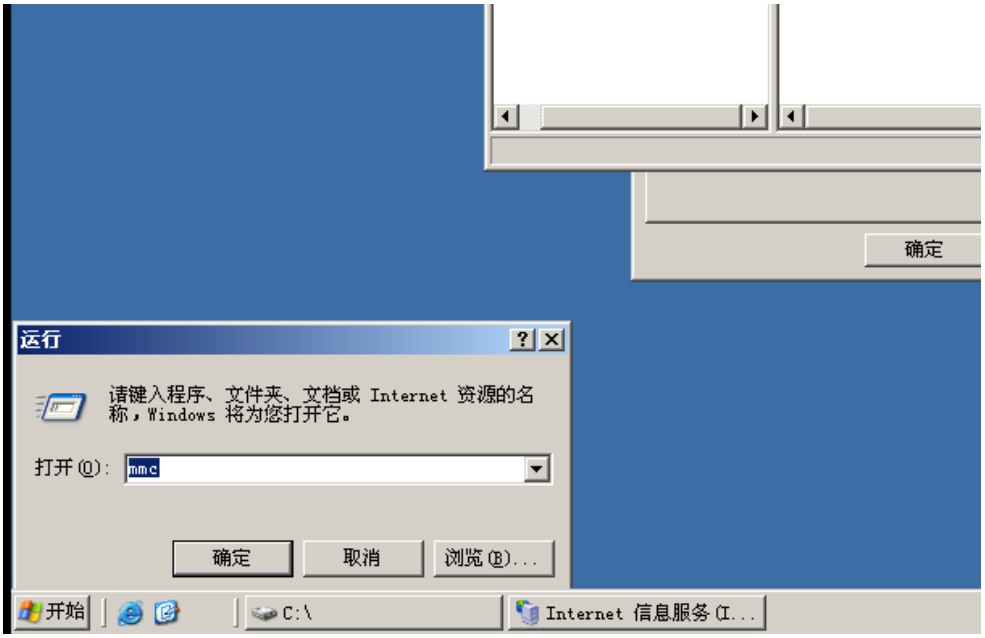
导出到指定目录里



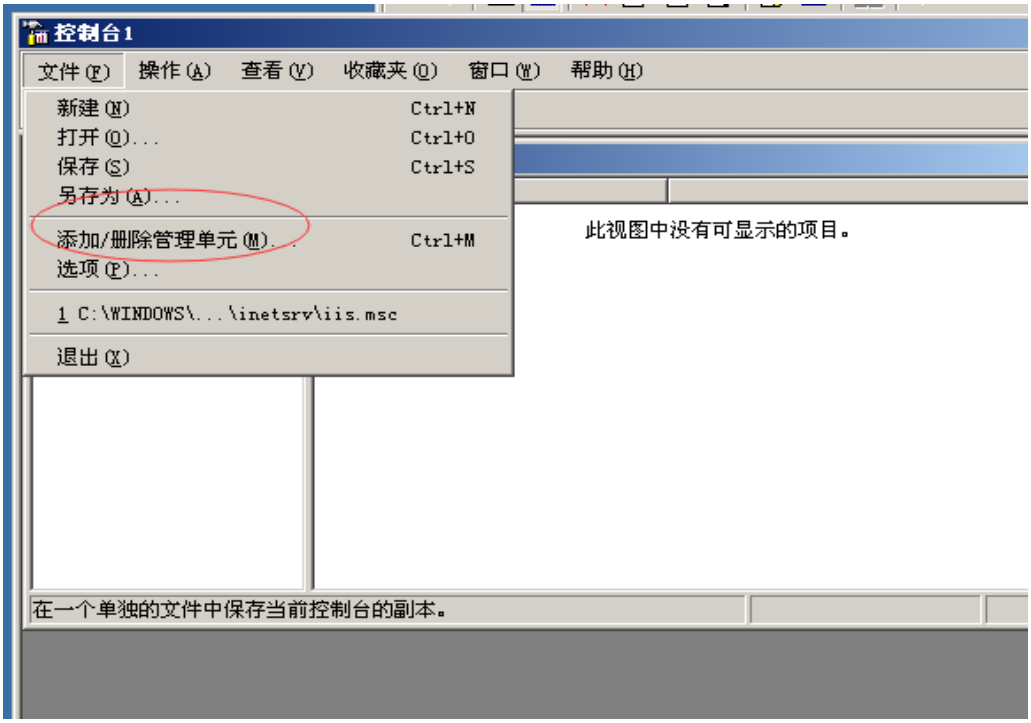
以同样方式将 CA 证书也转换成 Base64 编码格式即可

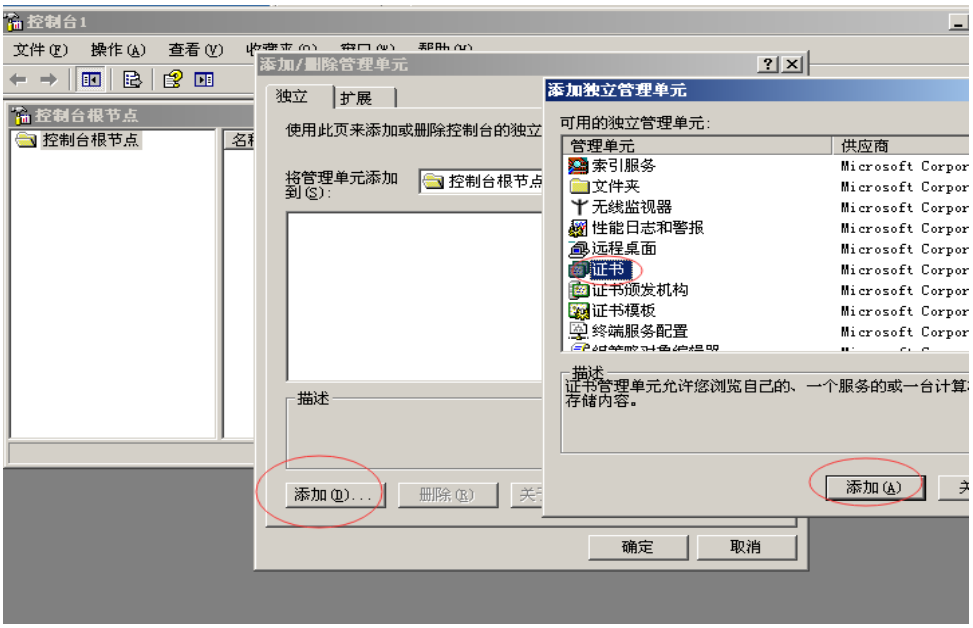
2. 创建控制台

1） 点击开始菜单，在“运行”中输入“mmc”，打开控制台窗口。

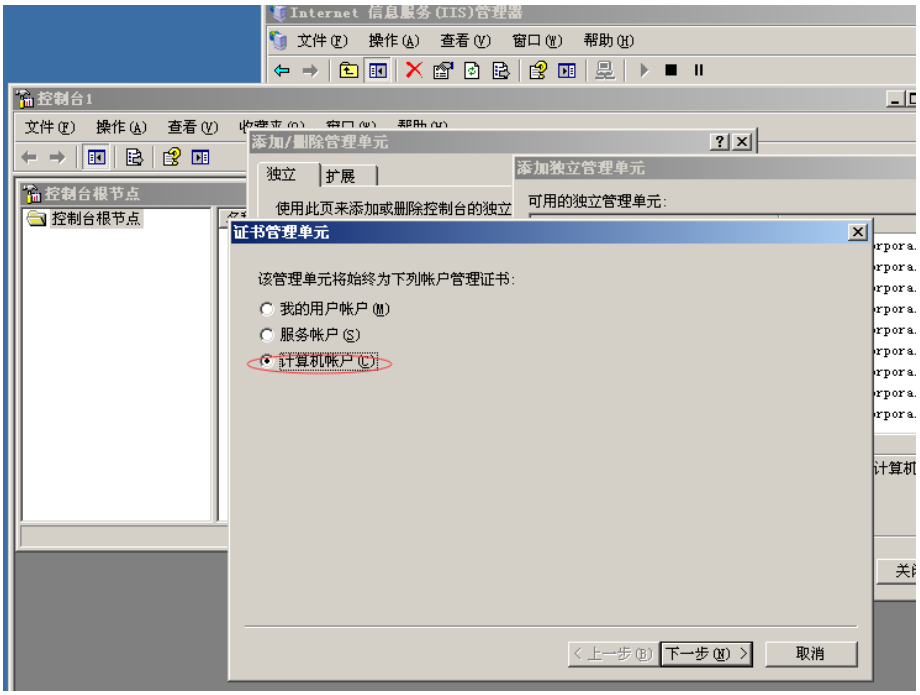


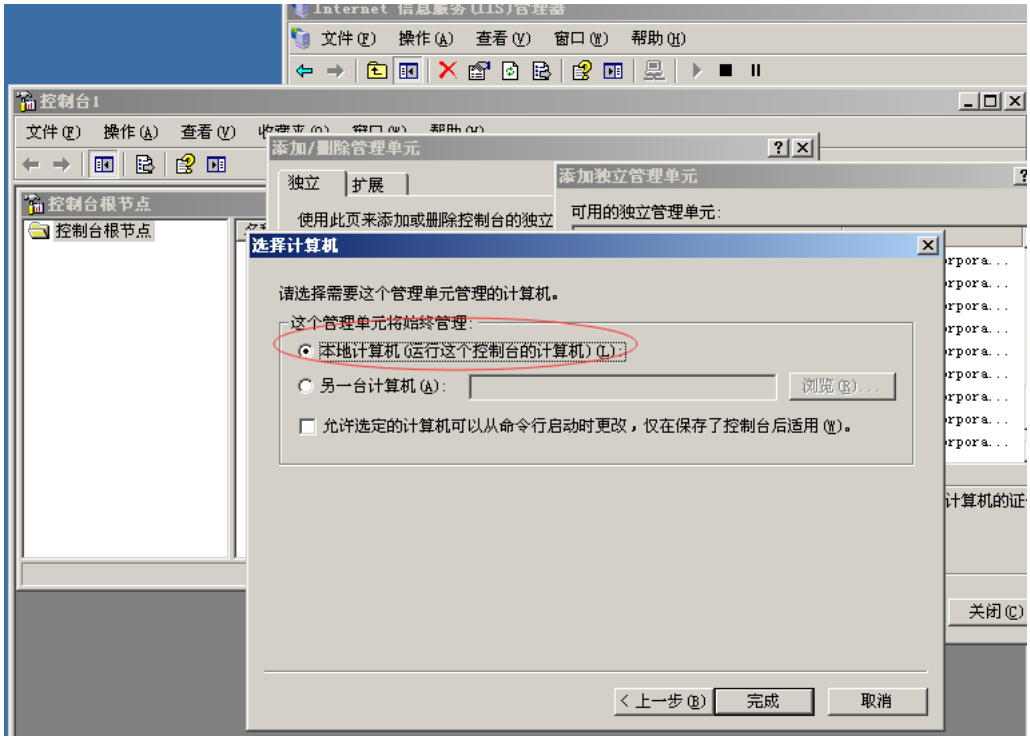
2) 点击-文件-添加删除管理单元-选择“证书”，然后点击“添加”：





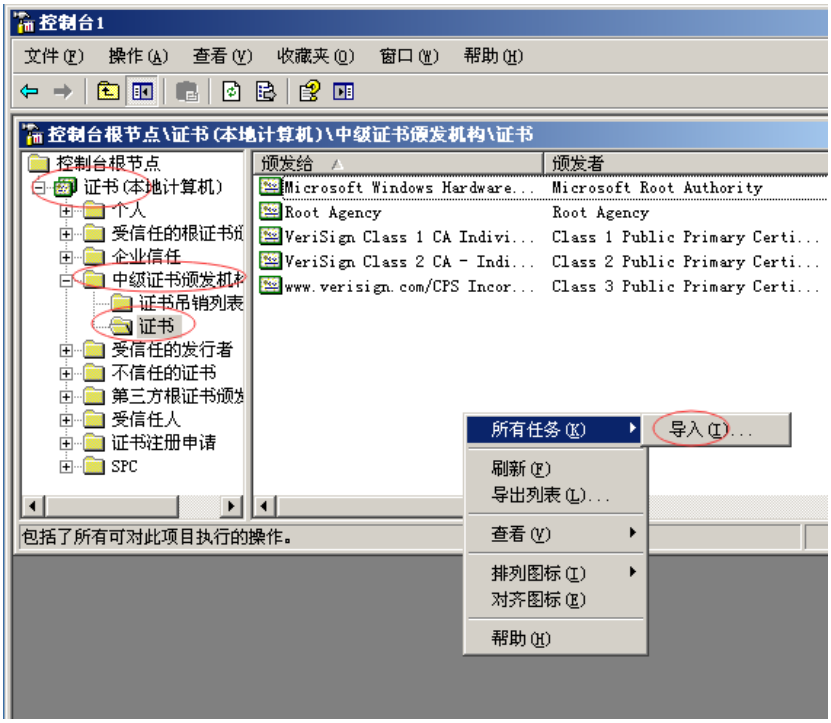
3） 选择“计算机帐户”-“本地计算机”，点击完成





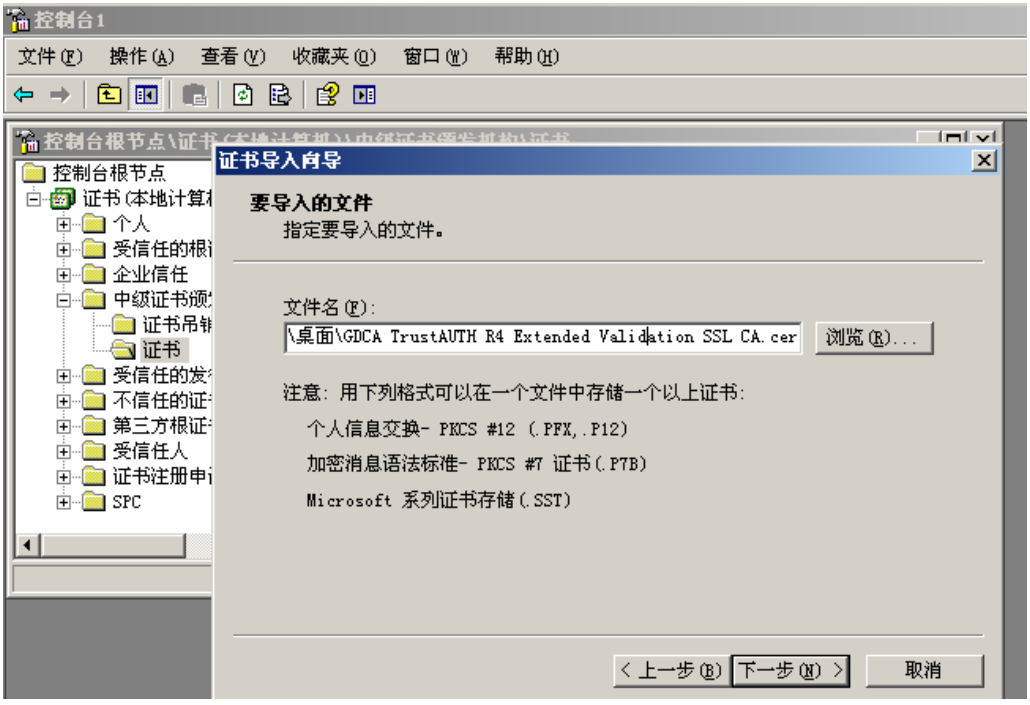
3. 导入 CA 证书

1) 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”，右键空白处点“所有任务”选择“导入”

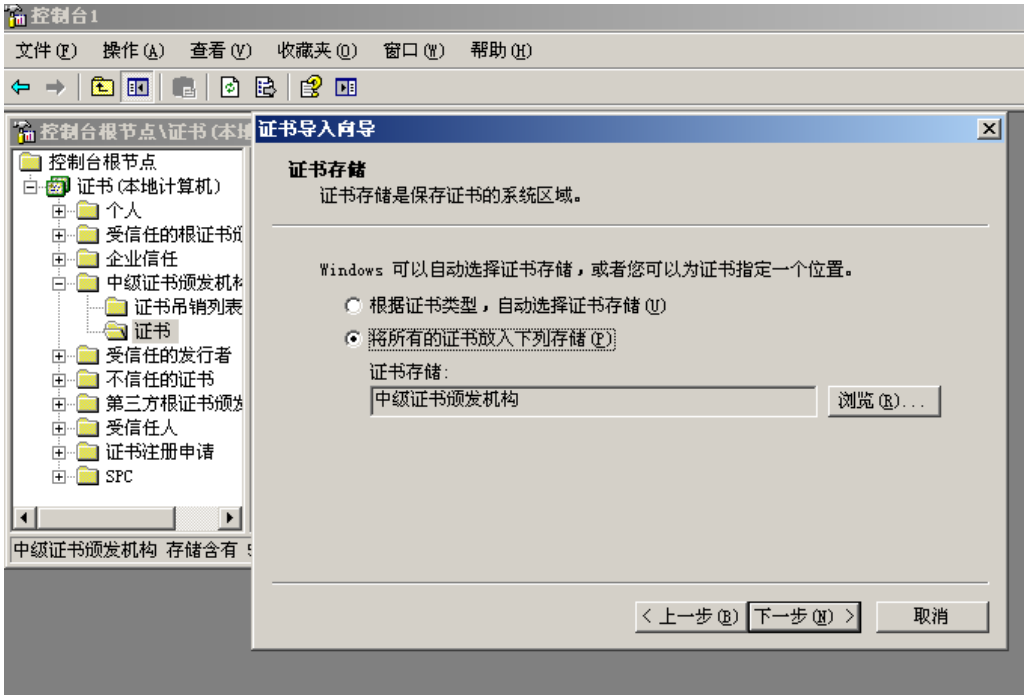


2） 进入证书导入向导，点击下一步

3） 通过证书向导导入 CA 证书 GDCA TrustAUTH R4 Extended Validation SSL CA.cer 证书，点击“下一步”

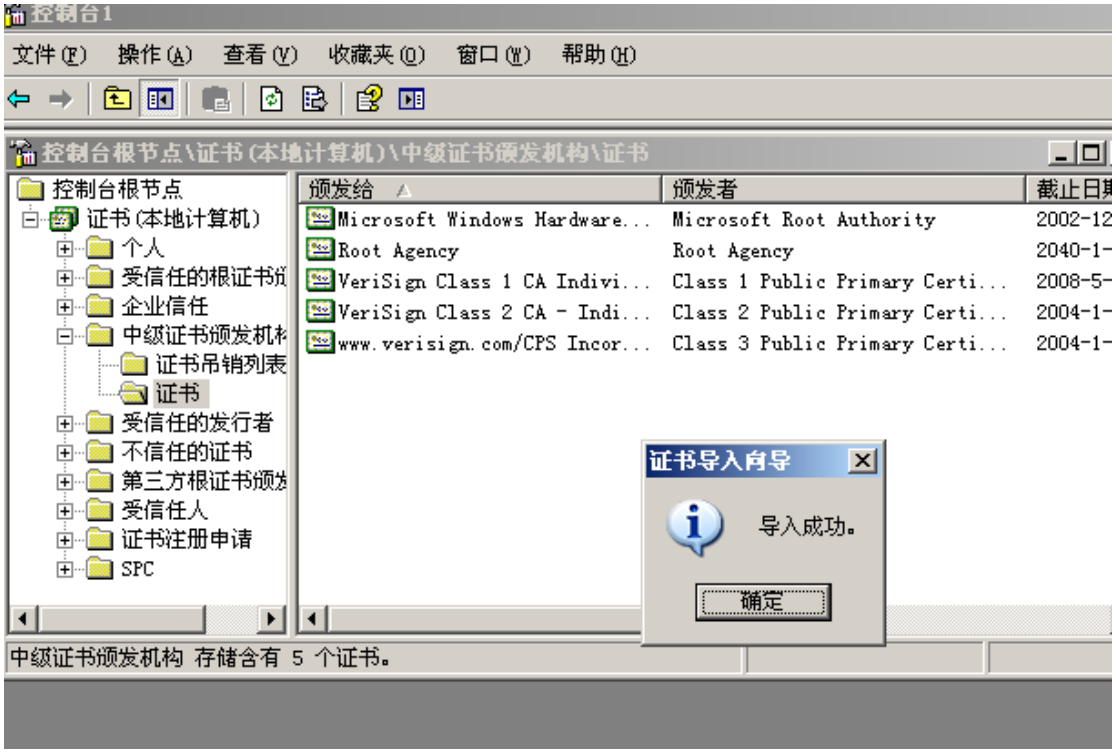


4） 选择“将所有的证书放入下列存储”，点击“下一步”



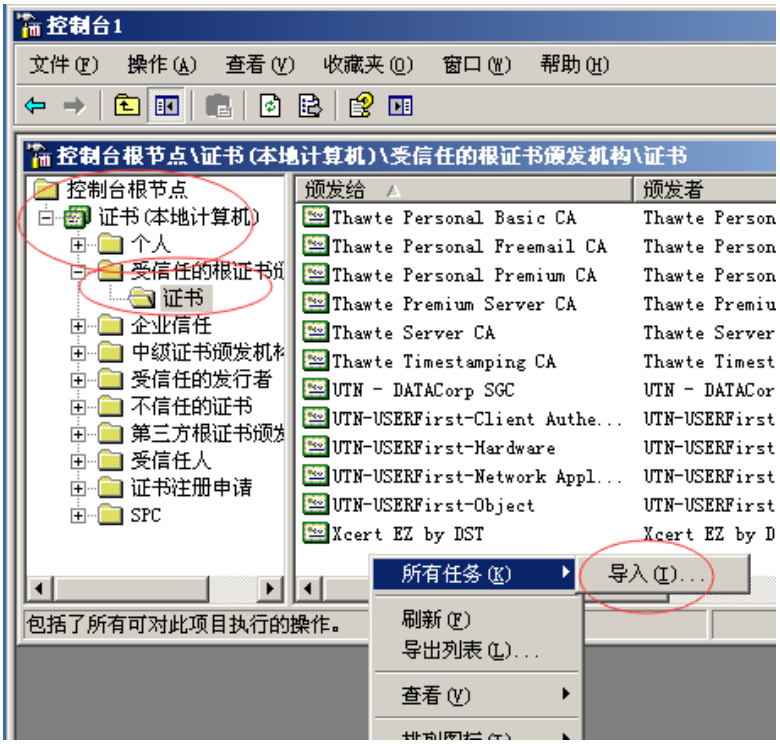
5） 点击“完成“导入 CA 证书完成

6） CA 证书导入成功



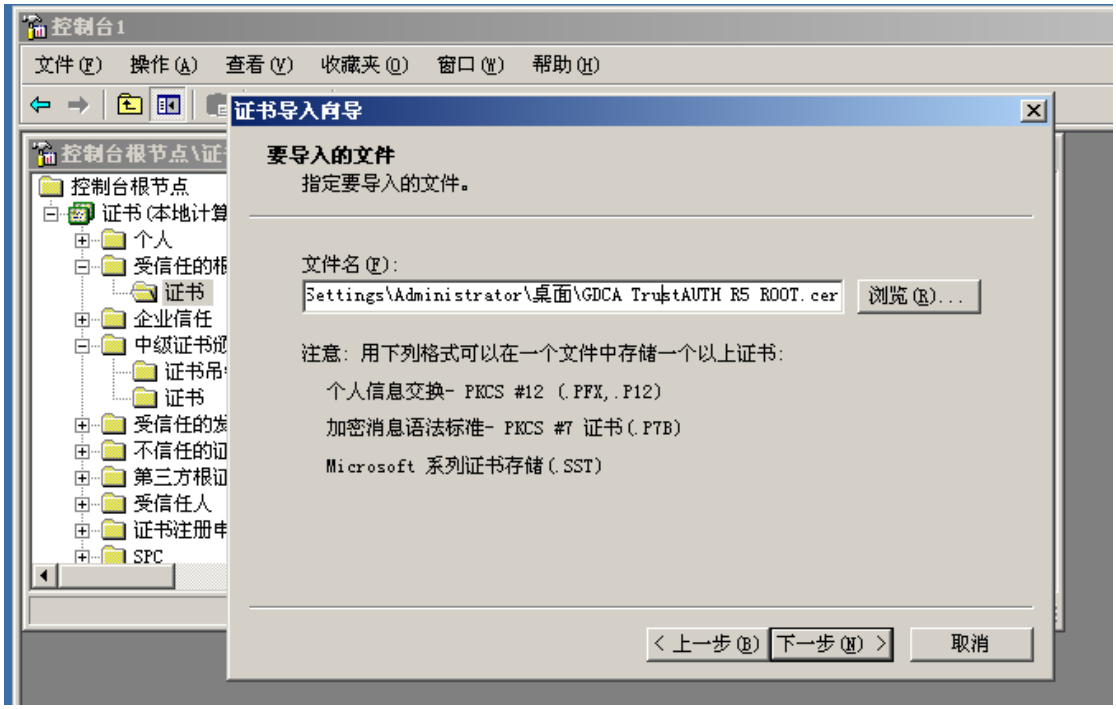
4. 导入根证书

1） 点击“证书”，选择“受信任的根证书”-“证书”在空白处点击右键，选择“所有任务”-“导入”

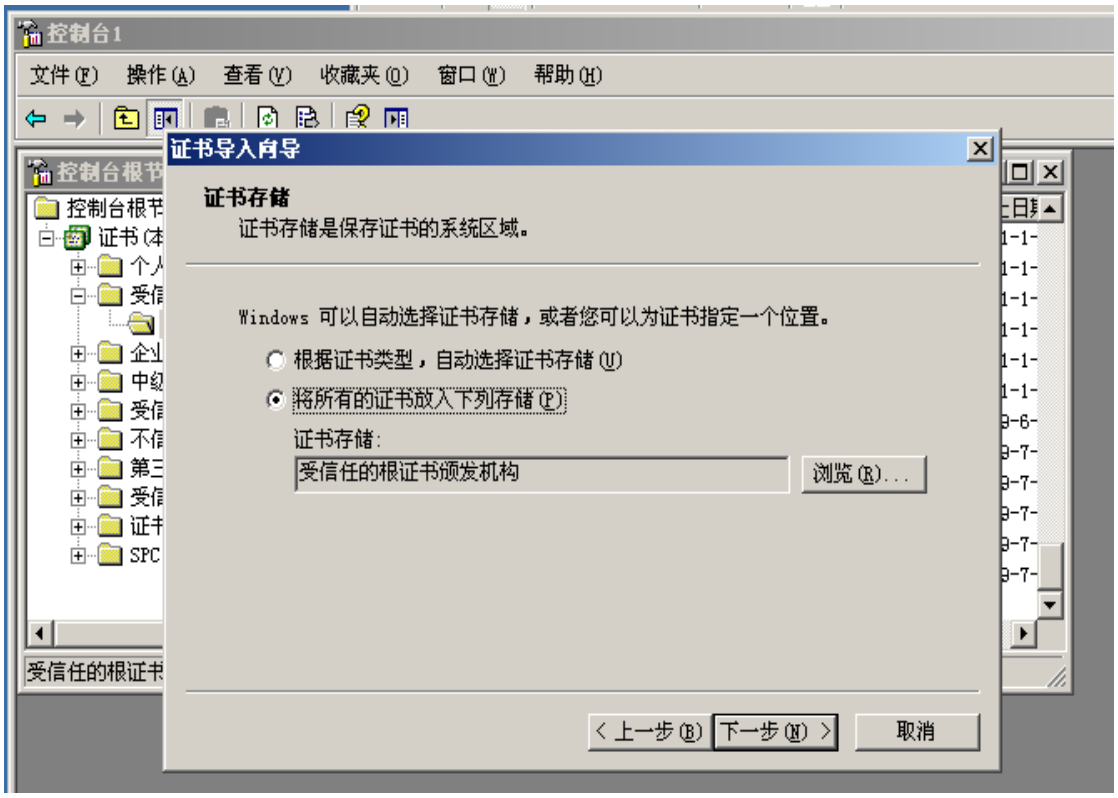


2) 进入证书导入向导，点击下一步

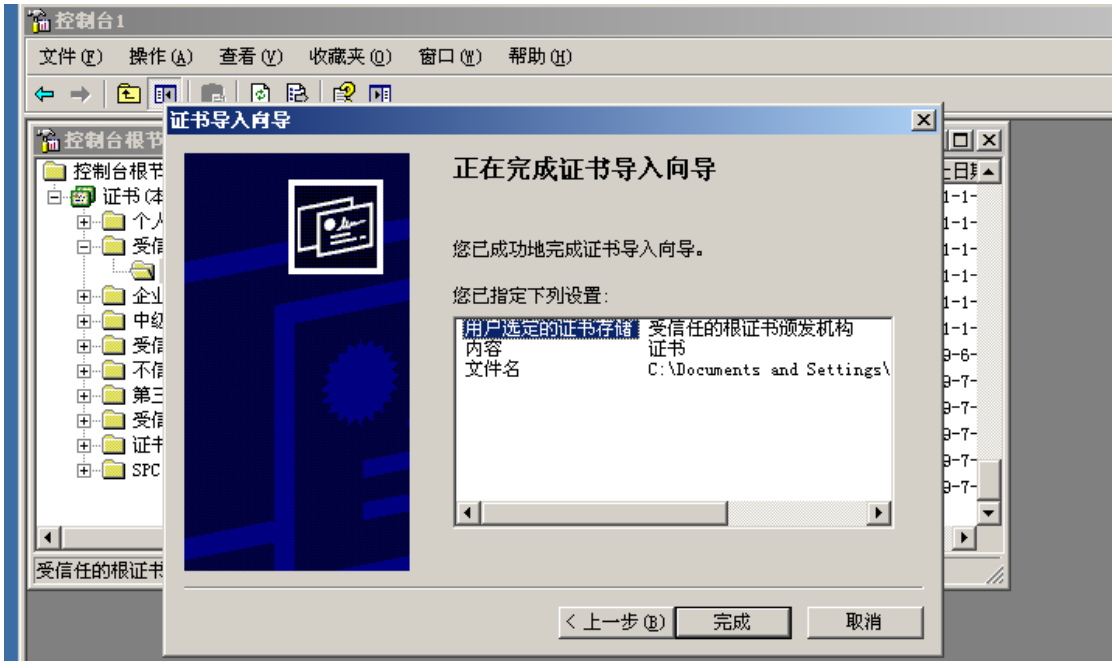
3) 通过证书向导导入根证书 GDCA TrustAUTH R5 ROOT.cer 证书,点击“下一步”



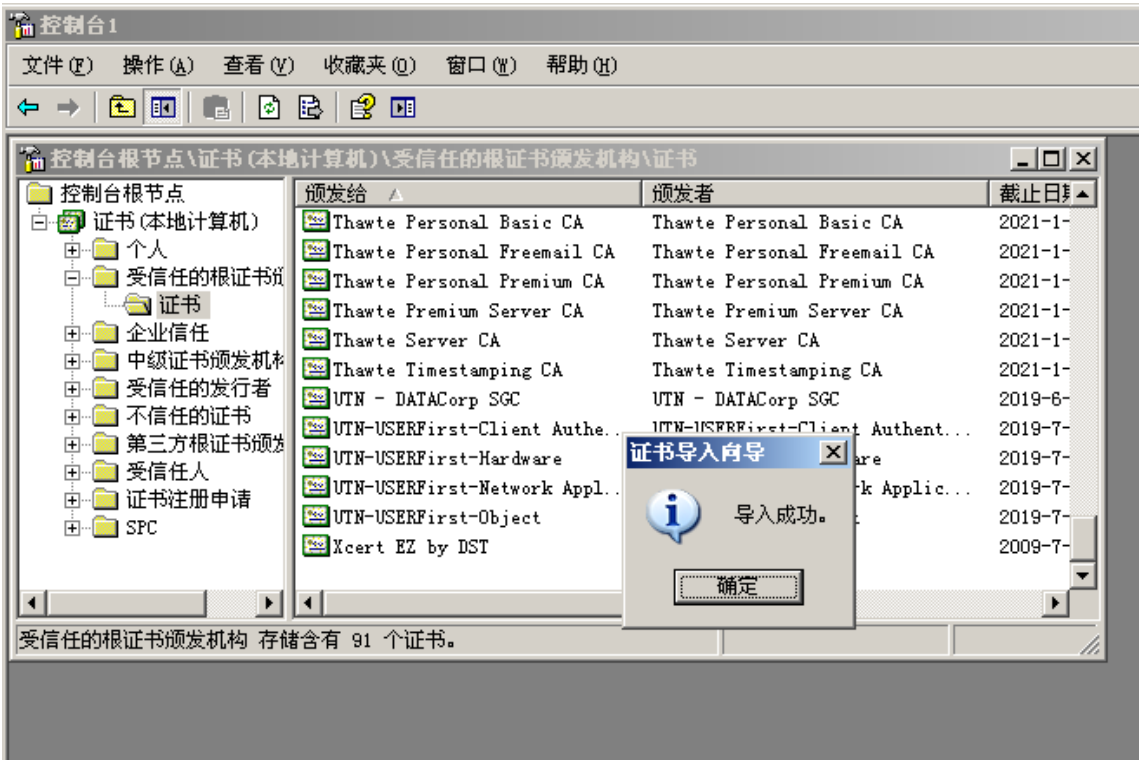
4) 选择“将所有的证书放入下列存储”-“受信任的根证书颁发机构”，点击“下一步”



5） 点击“完成“导入根证书完成

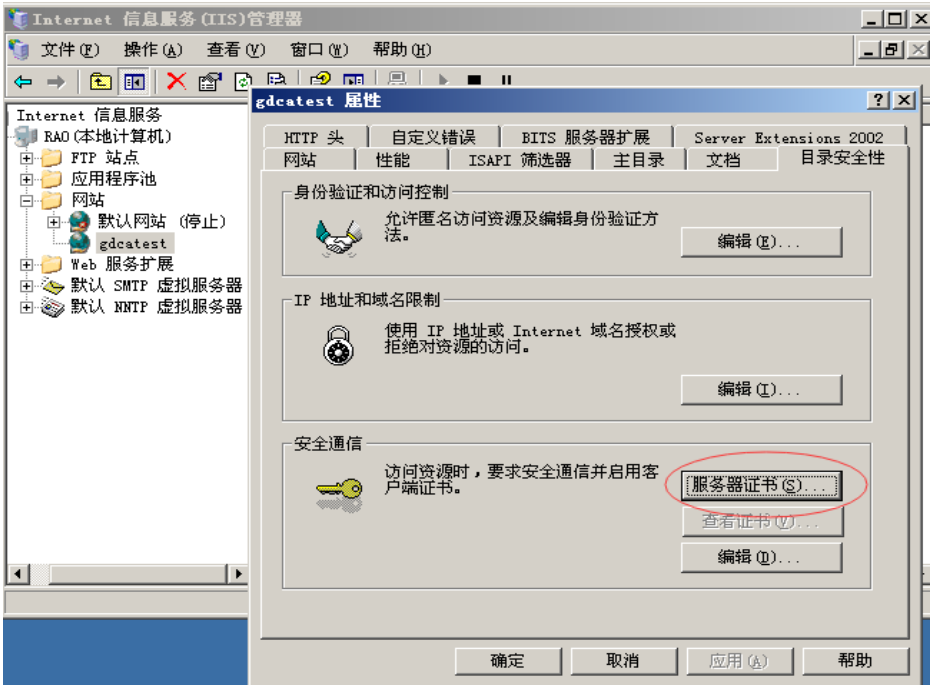


6） 根证书导入成功

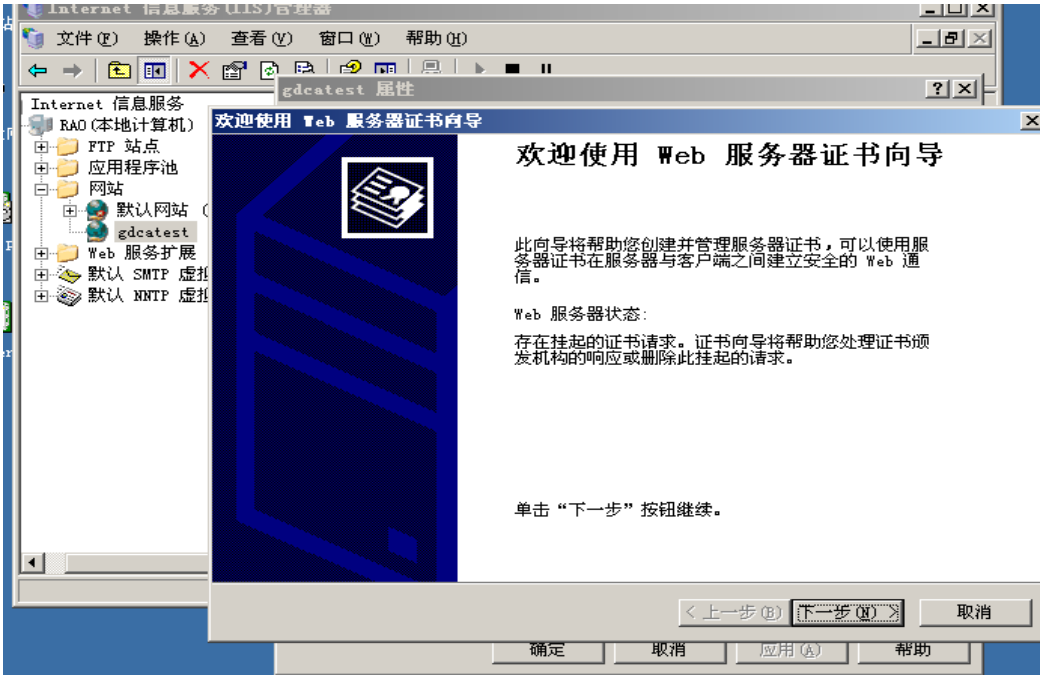


5. 导入服务器证书

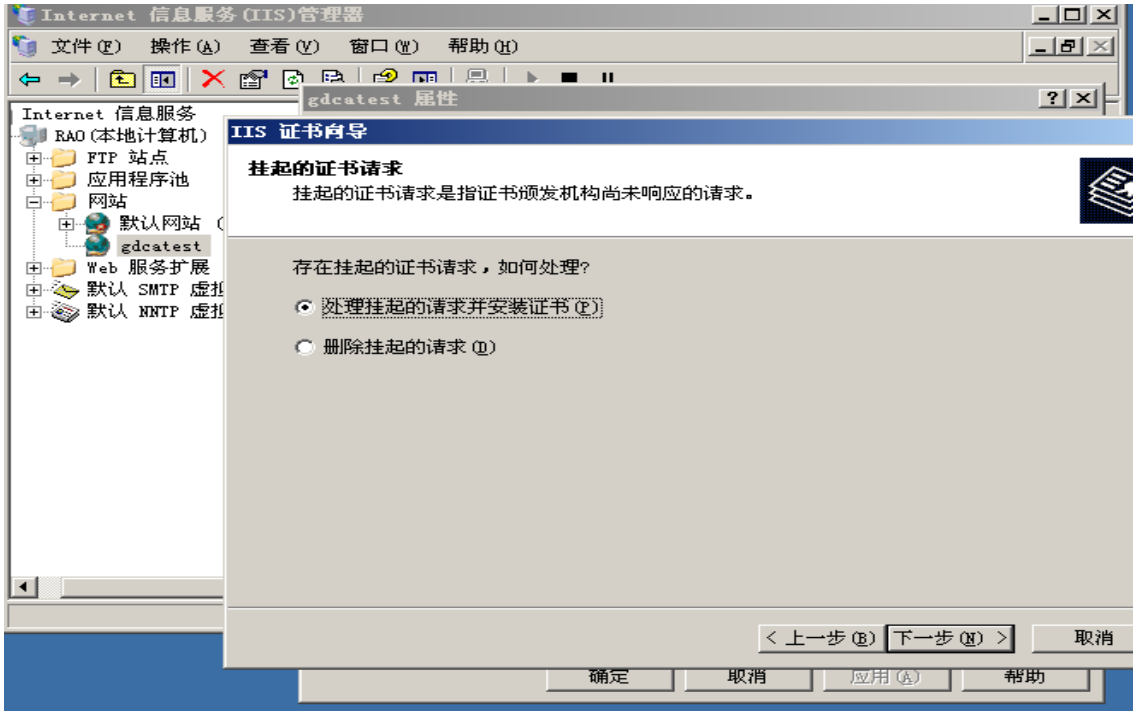
1) 进入 IIS 控制台，并选中需要配置服务器证书的站点，“属性”-“目录安全性”-“服务器证书”



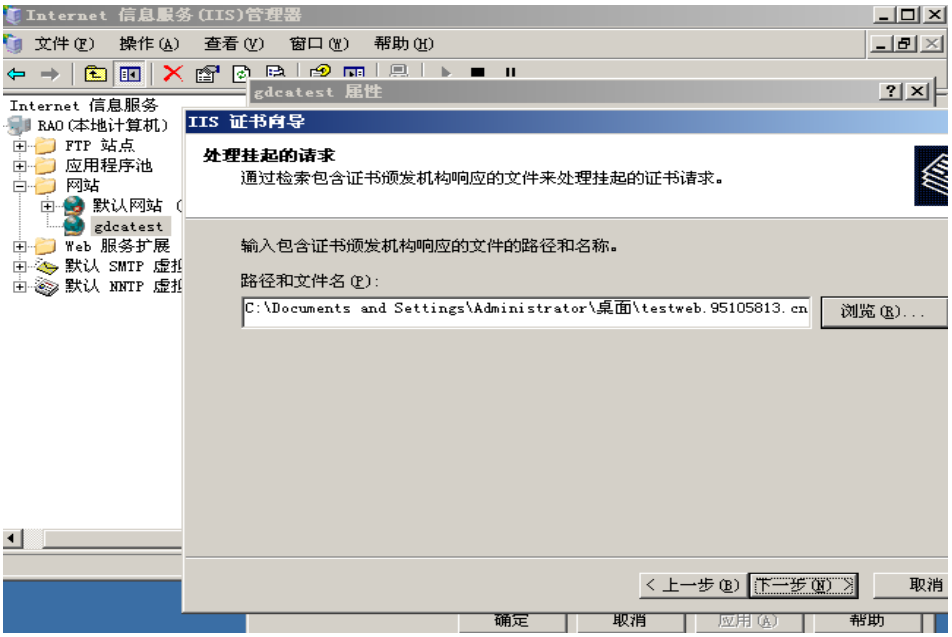
2） 进入配置服务器证书向导，点击下一步



3） 选择“服务器证书”-“处理挂起的请求并安装证书”，点击下一步

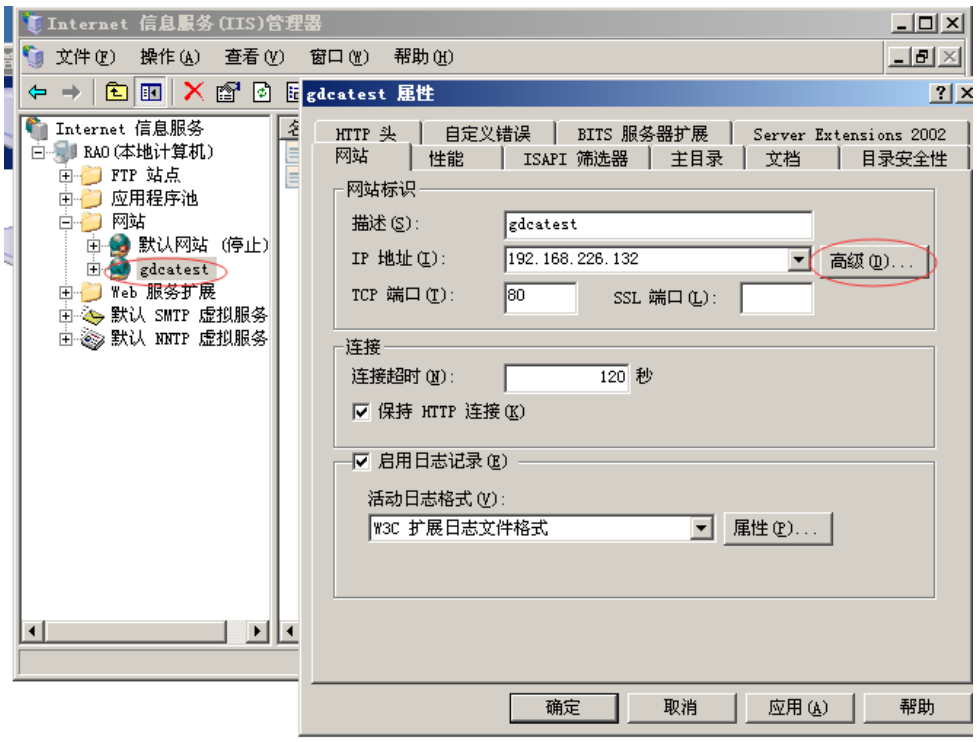


4） 选中您的服务器证书文件，点击下一步，完成

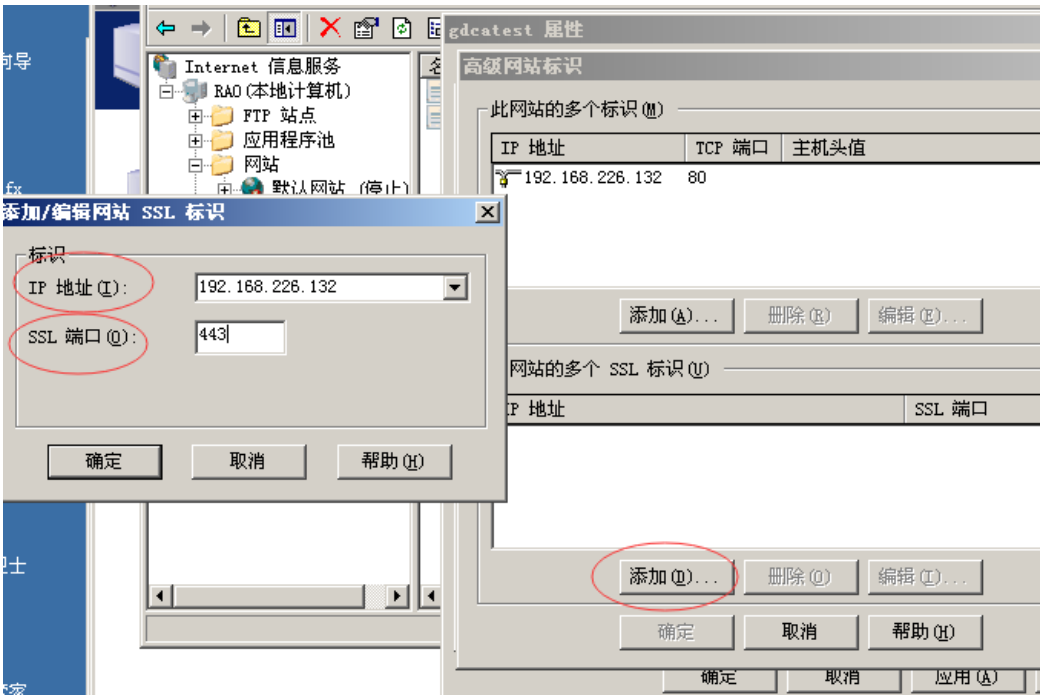


6. 部署服务器证书

1) 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”-选择“网站”-“高级”

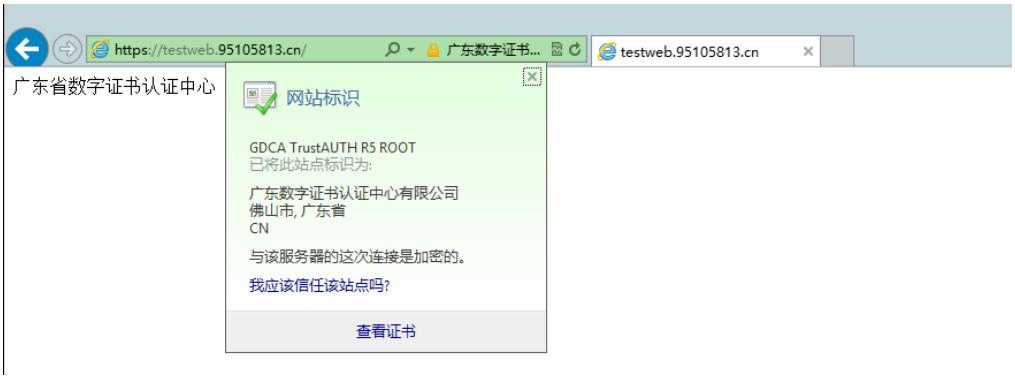


2) 配置默认的 https 访问端口 443，重启 IIS 并使用 https 方式访问测试站点证书安装



7. 访问测试

服务器若部署了 SSL 证书，浏览器访问时将出现安全锁标志；若部署了 EV SSL 证书，浏览器除了显示安全锁标志，地址栏会变成绿色，如下图：



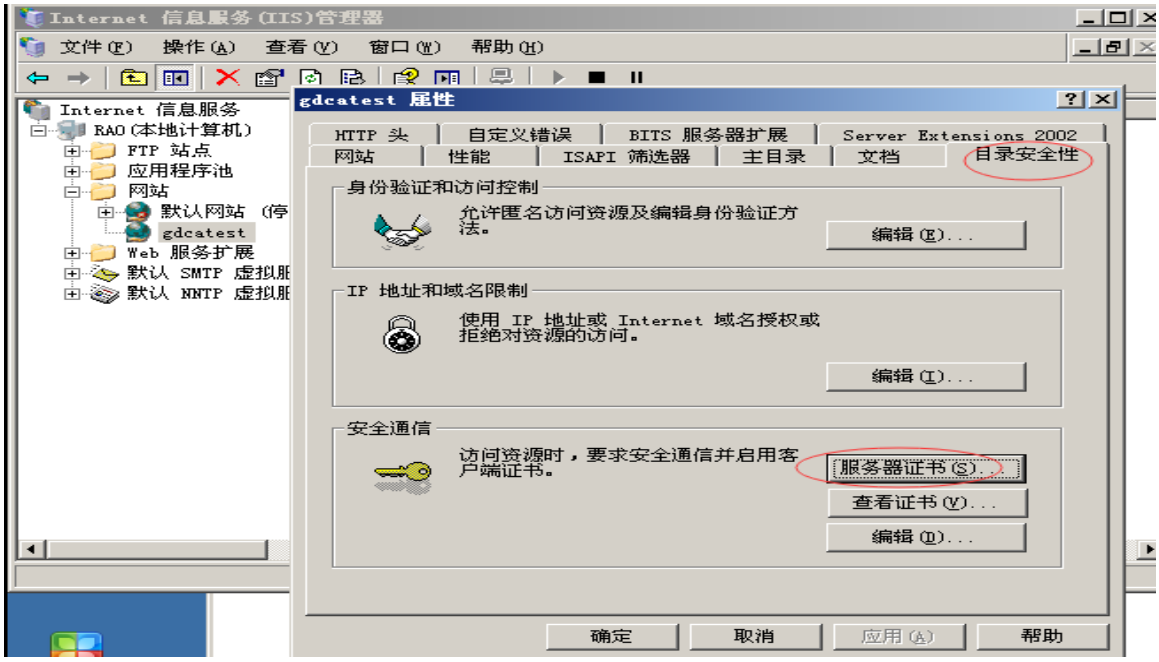
四、 服务器证书的备份与恢复

1. 说明

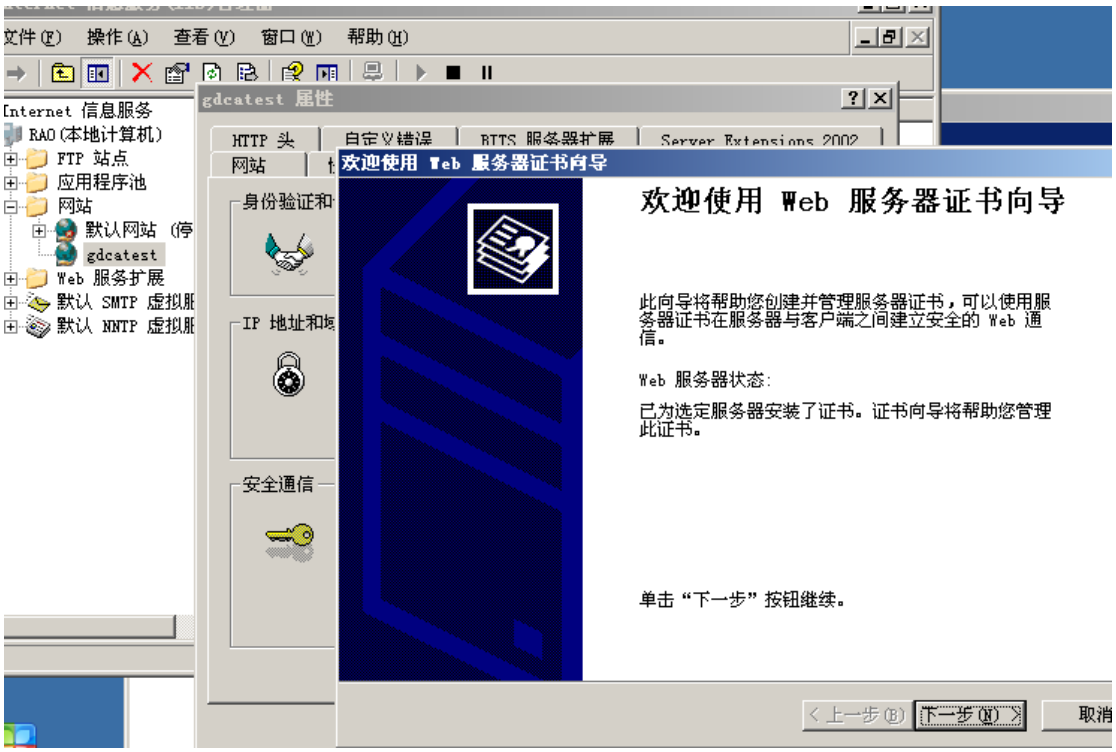
在您成功的安装和配置了服务器证书之后，请务必依据下面的操作流程，备份好您的服务器证书，以防证书丢失给您带来不便。

2. 服务器证书的备份

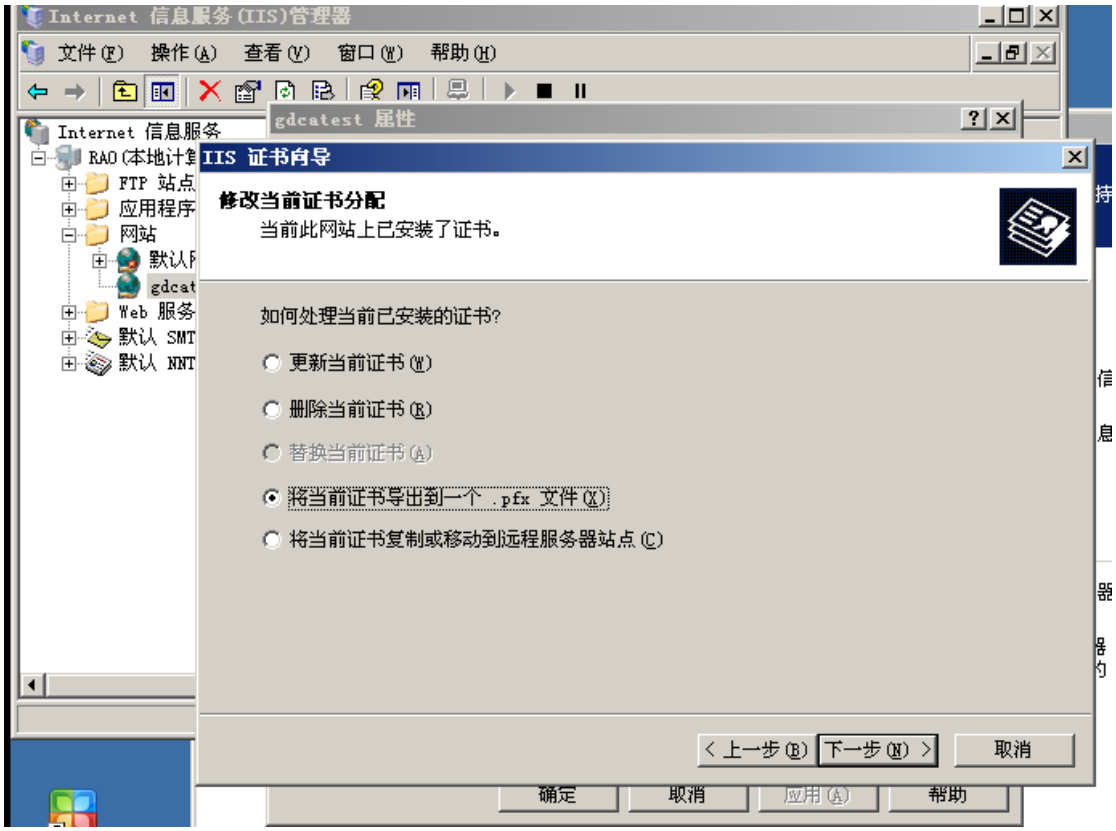
1) 进入 IIS 控制台，选择安装有服务器证书的站点，右键选择“属性”-“目录安全性”-“服务器证书”



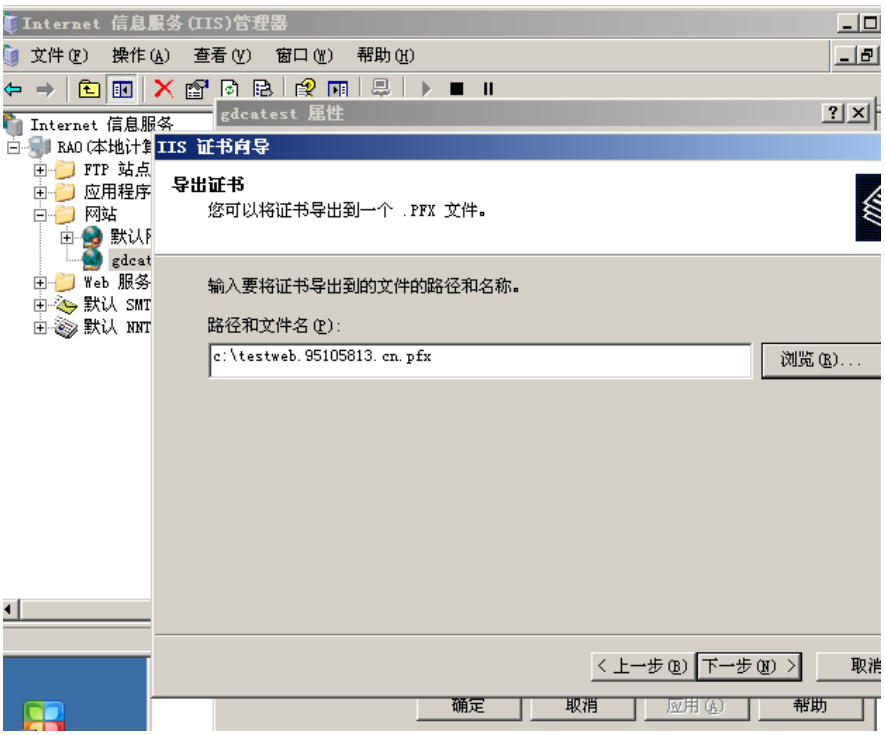
2) 进入服务器证书向导，点击下一步



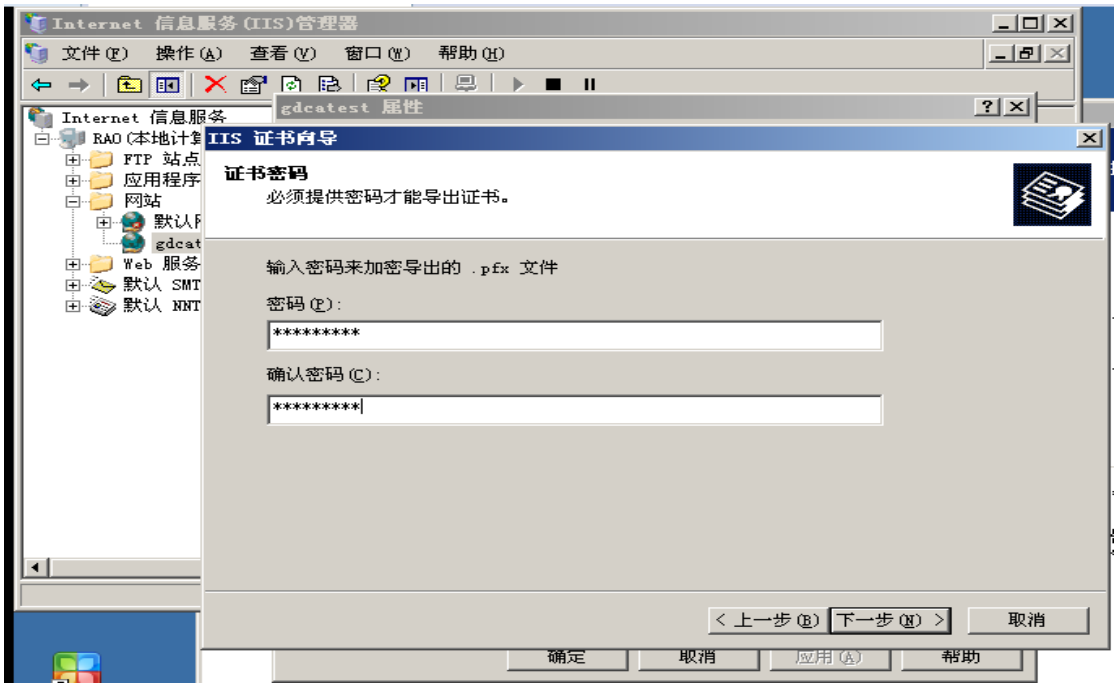
3） 将证书导出到一个.pfx 文件，点击下一步



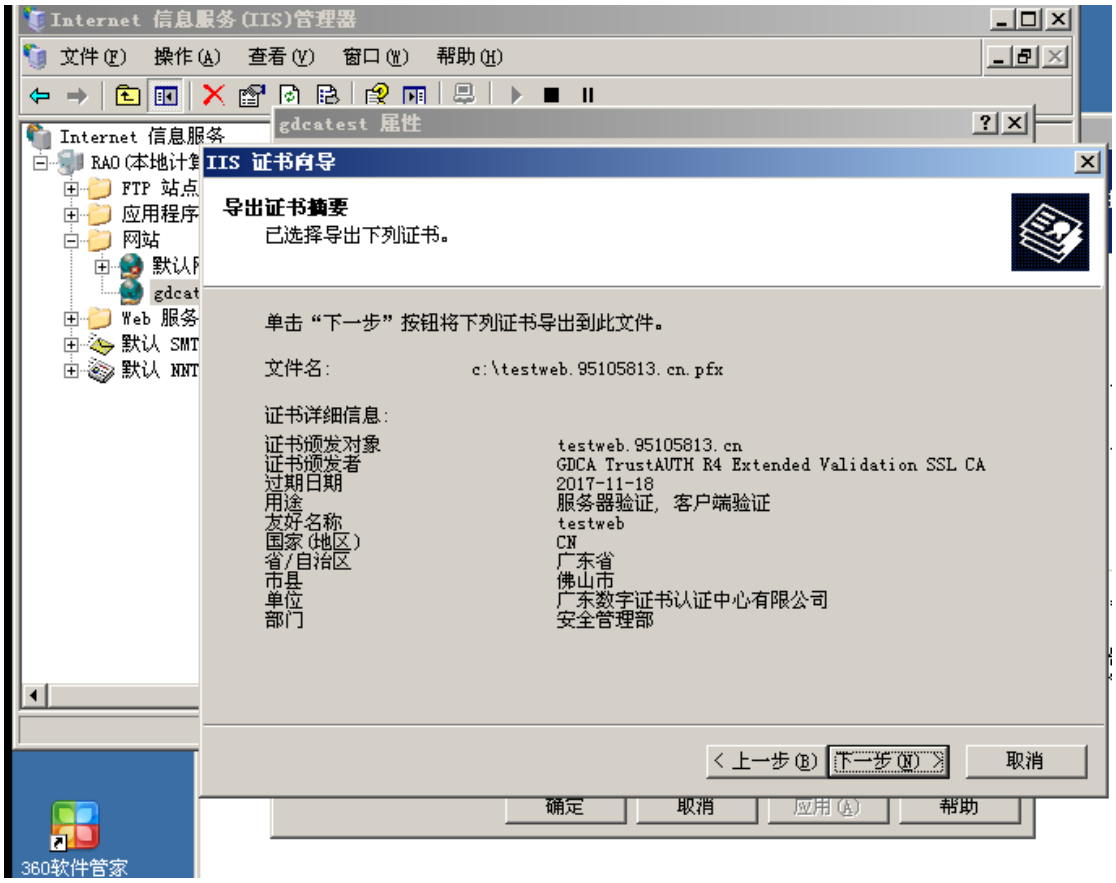
4） 设置文件导出路径



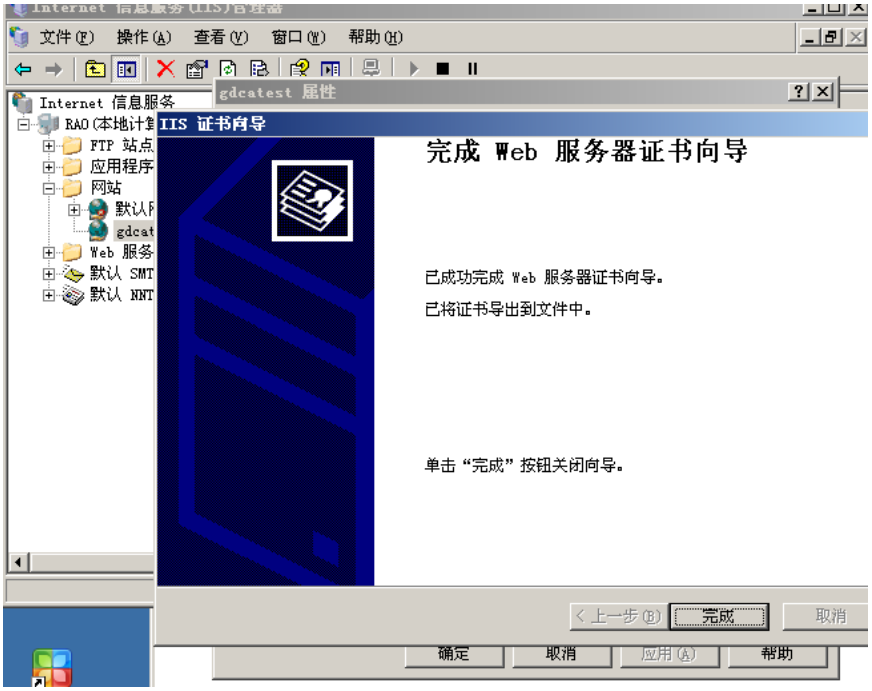
5） 为导出的证书备份文件设置一个保护密码



6） 确认导出证书摘要，点击下一步

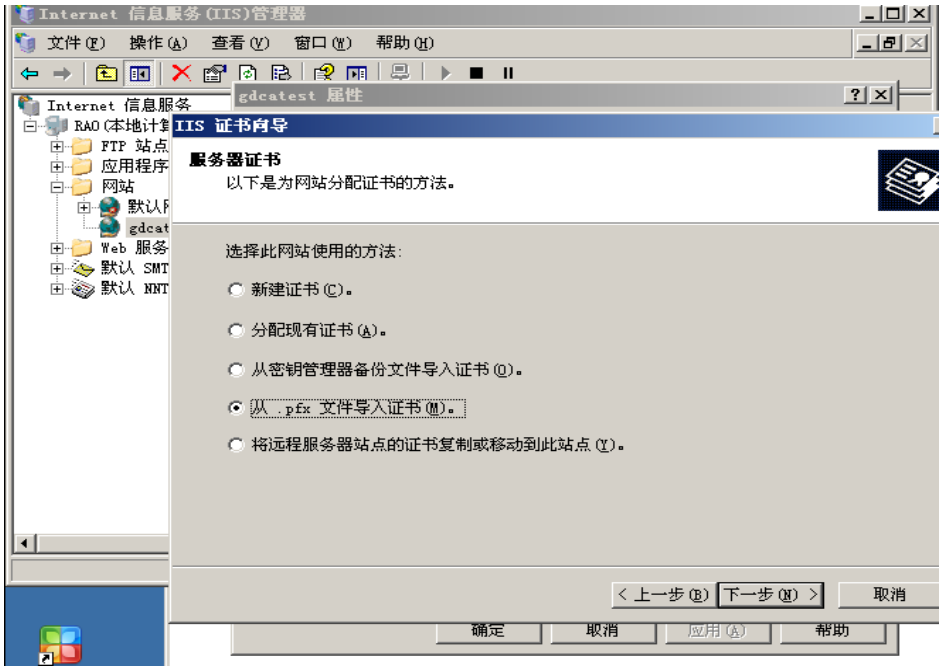


7） 完成证书导出，成功备份服务器证书

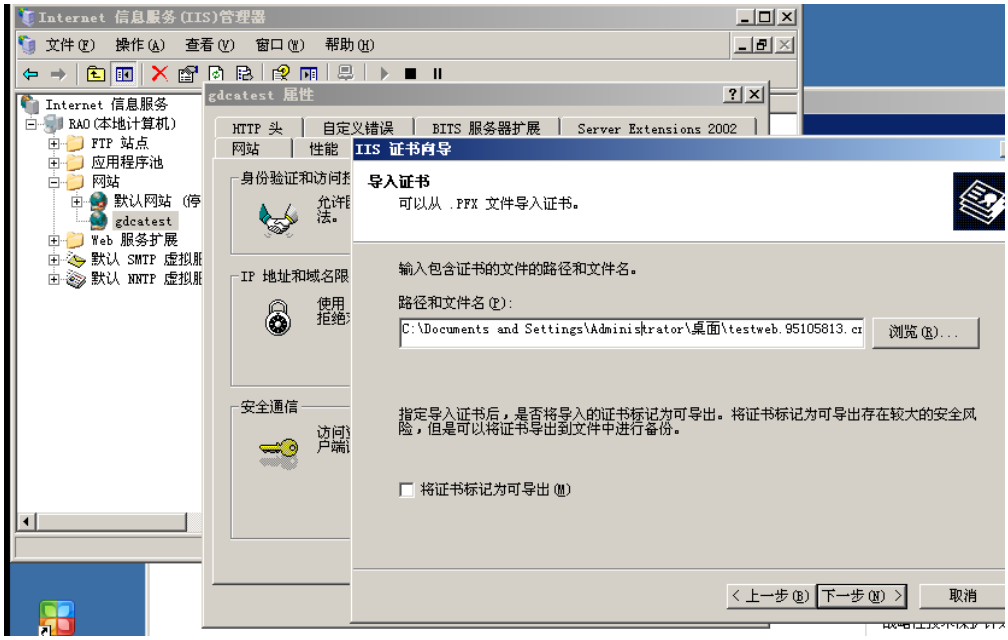


3. 服务器证书的恢复

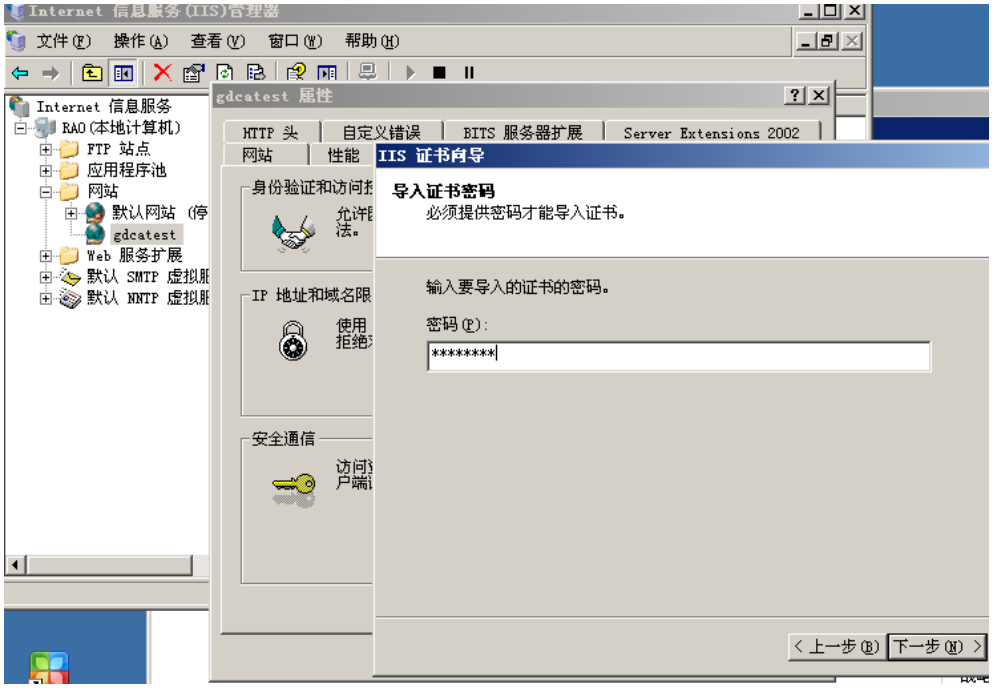
1） 进入 IIS 控制台，选择安装有服务器证书的站点，右键选择“属性”è“目录安全性”-“服务器证书”-从.pfx 文件导入证书



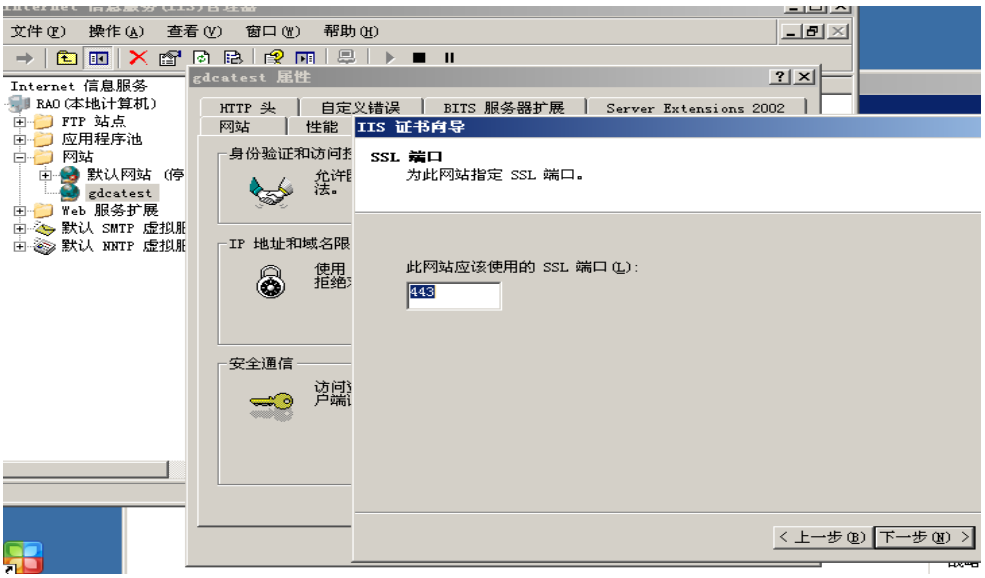
2） 选择您的服务器证书备份文件，点击下一步。



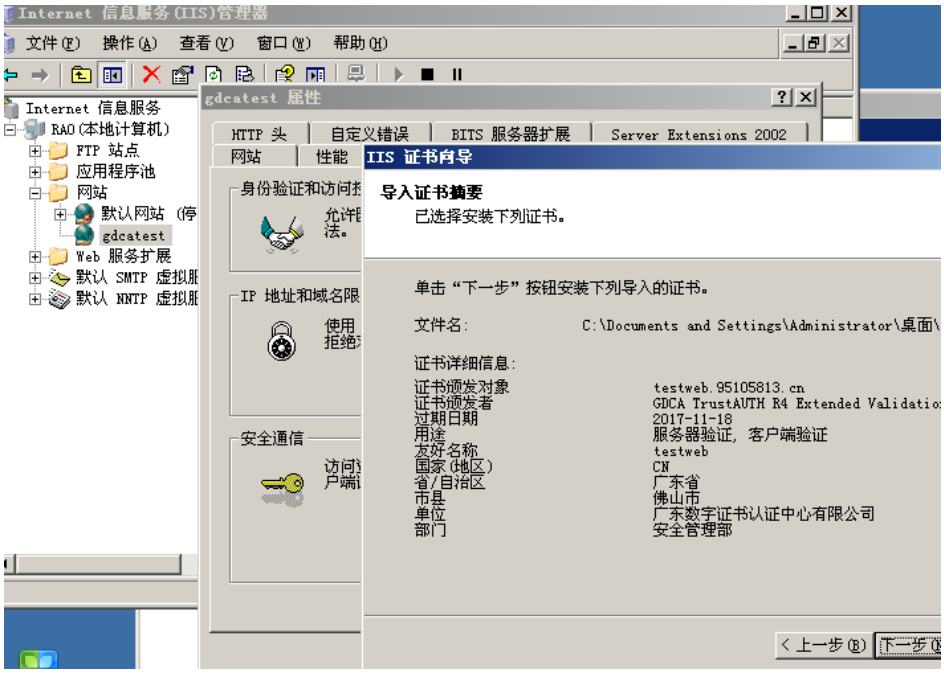
3） 输入备份文件保护密码



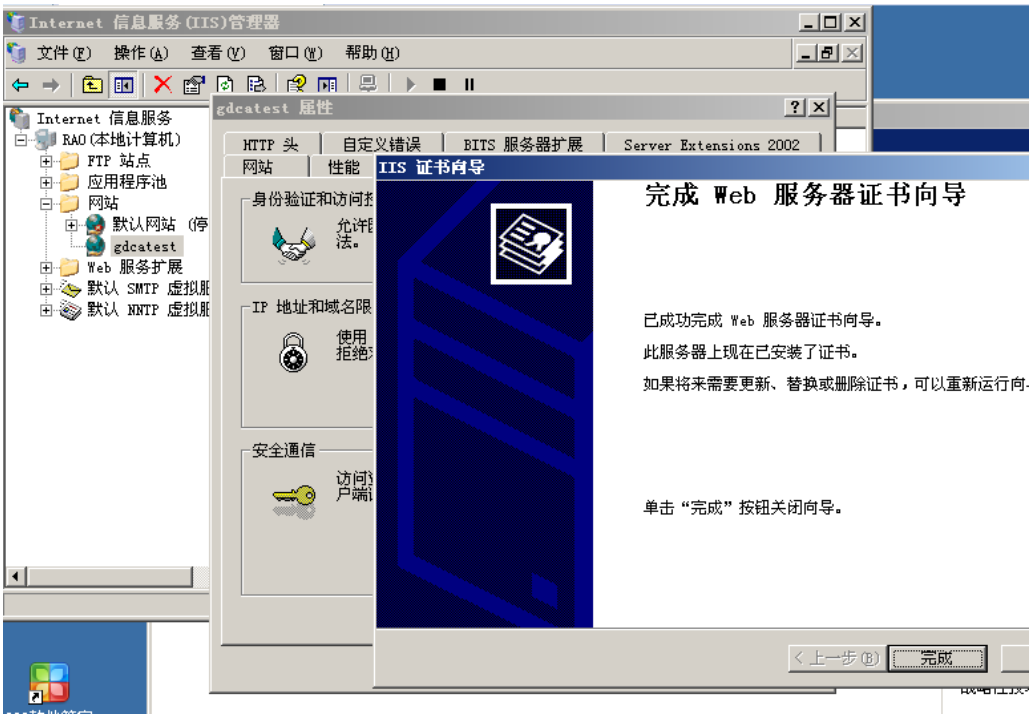
4) 指定 SSL 端口，默认为 443



5) 确认导入证书摘要，点击下一步：



6） 完成服务器证书导入



五、 证书遗失处理

若您的证书文件损坏或者丢失且没有证书的备份文件，请联系 GDCA（客服热线 95105813）办理遗失补办业务，重新签发服务器证书。