数安时代科技股份有限公司

GDCA 信鉴易® SSL 服务器证书部署指南

For IIS 6版本

修订日期：2017/05/25

目录

地址：广州市东风中路 448 号成悦大厦第 23 楼邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

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 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。
7) 如用户已经正常生成证书请求文件后，请从第三点部署证书开始阅读。

二、 合成 PFX 证书

1. 获取证书

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 OV SSL 证书（Organization Validation SSL Certificate），CA 证书就是文件就是 GDCA_TrustAUTH_R4_OV_SSL_CA.cer；如果您申请的是 EV SSL 证书（Extended Validation SSL Certificate），CA 证书就是文件就是 GDCA_TrustAUTH_R4_EV_SSL_CA.cer,请确认所收到的证书文件是您需要的 CA 证书。（*注意：所发至邮箱的文件是压缩文件，里面有 3 张证书，请确认所收到的证书文件是您需要的 CA 证书文件*）

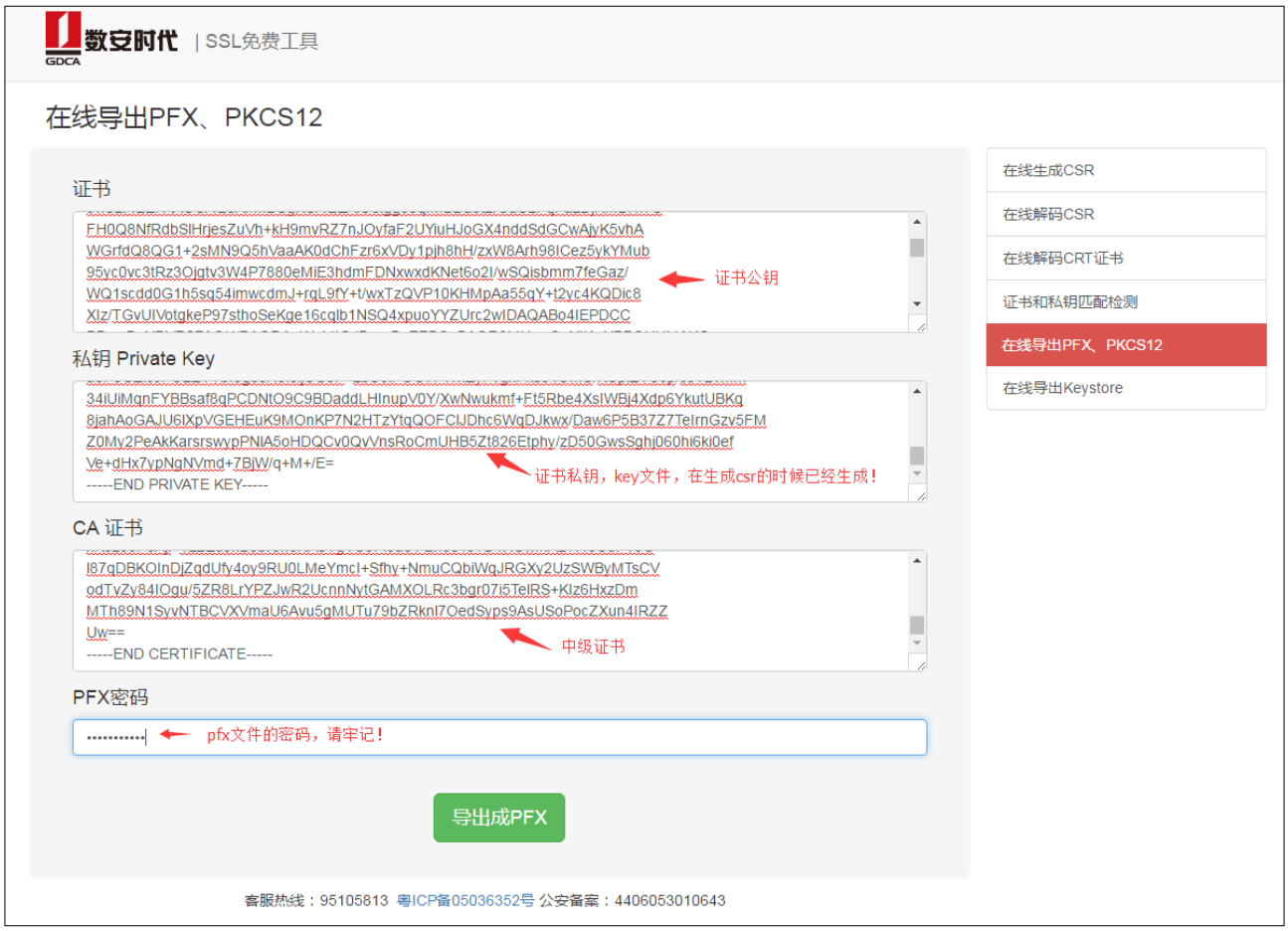
Globalsign 产品获得证书如下图：

2. 私钥证书

请找到之前提交 csr 时会生成一个.key 文件，该文件为证书的私钥，后面配置要用到。

3. 合成证书

1)用浏览器打开以下链接: https://www.trustauth.cn/SSLTool/tool/export_pfx.jsp
2）用文本编辑器 txt 打开上面的证书公钥、私钥、中级证书文件，根据下图所示填入合成证书信息，导出后会下载一个 www.domainame.com.pfx 的文件，保存好这个文件。



地址：广州市东风中路 448 号成悦大厦第 23 楼邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

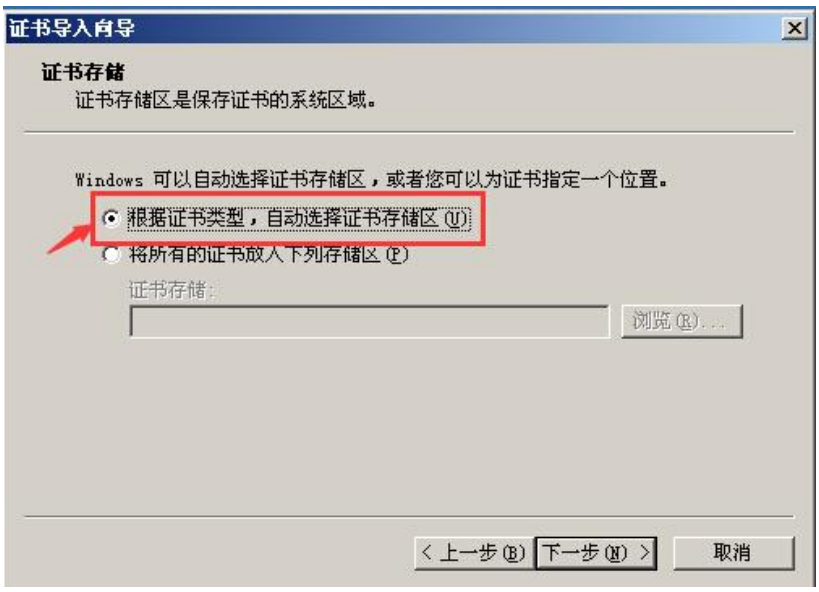
三、 部署证书

1. 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

2. 导入 PFX 证书

1) 在添加的证书管理单元中，选择“证书”- “个人”-“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) 导入上面合成的 www.yourdomain.com.pfx 证书,输入密码，点击“下一步”
4) 选择“**根据证书内容自动选择存储区**”，点击“下一步”

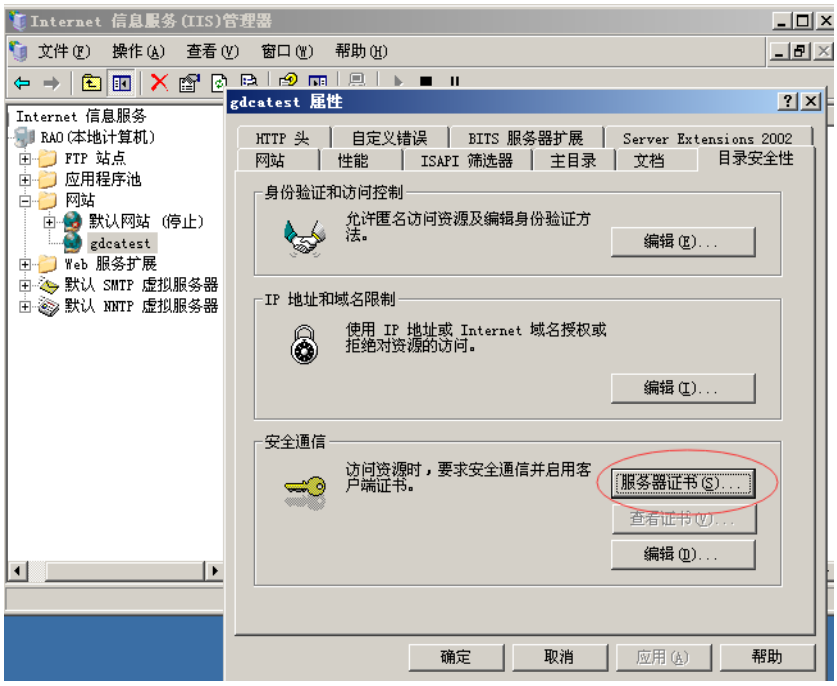


5) 点击“完成“导入 CA 证书完成
6) 证书导入成功

地址：广州市东风中路 448 号成悦大厦第 23 楼邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

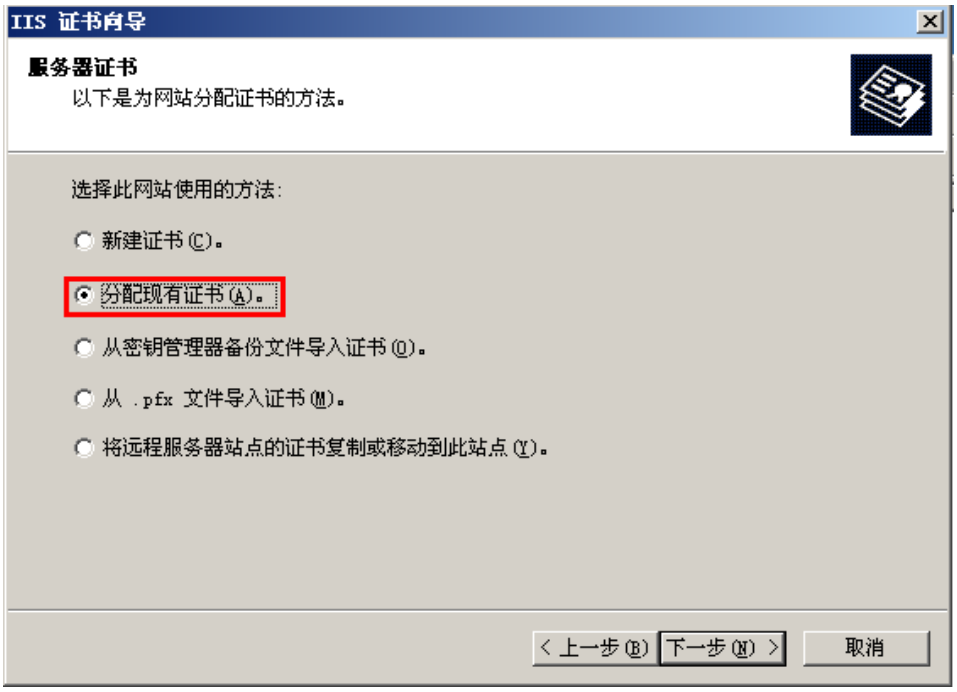
3. 分配服务器证书

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

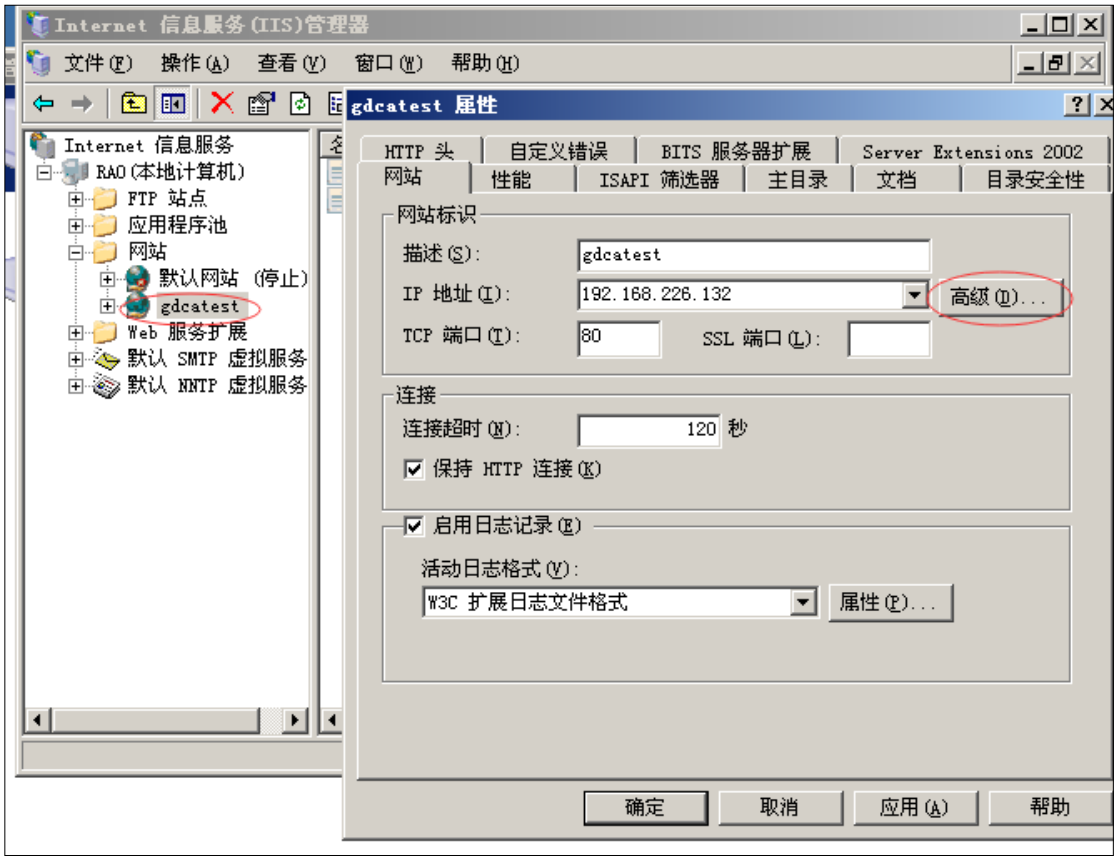


地址：广州市东风中路 448 号成悦大厦第 23 楼邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

4) 在列表里面选中您的服务器证书文件,点击下一步,完成

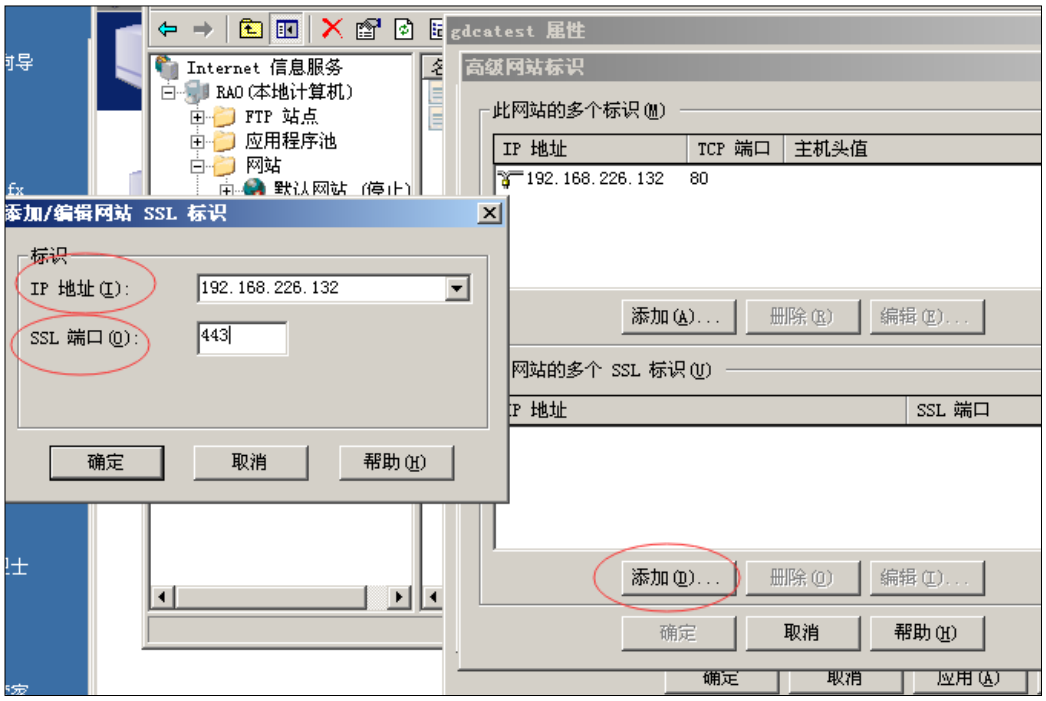
4. 部署服务器证书

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

地址：广州市东风中路 448 号成悦大厦第 23 楼邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813



5. 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，IE 浏览器除了显示安全锁标志，地址栏会变成绿色，（*如果访问不通，请查看防火墙是否拦截 443 端口*）如下图：

四、 服务器证书的备份与恢复

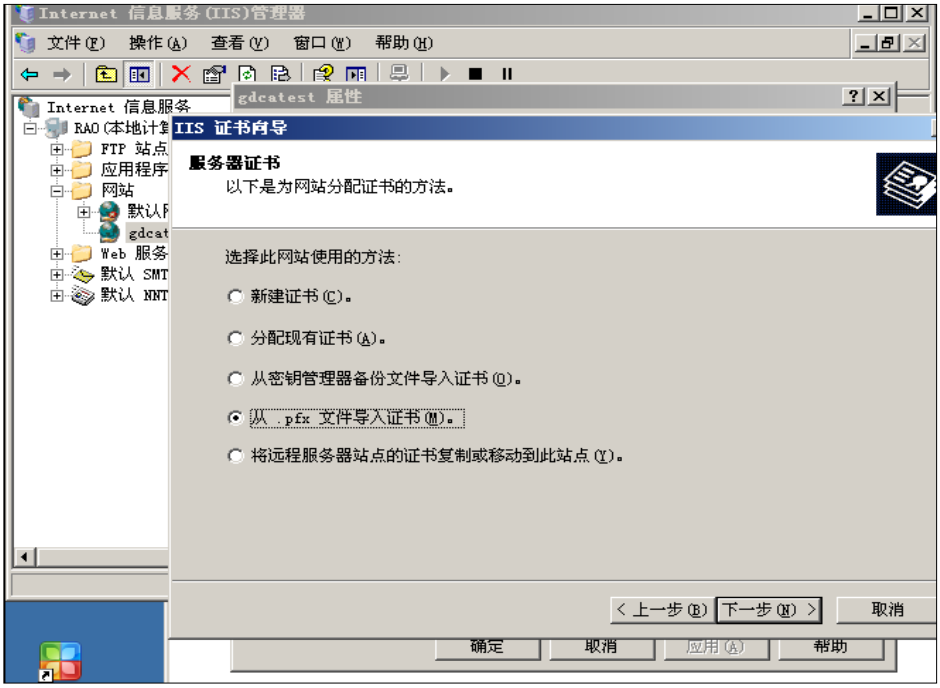
1. 证书的备份

请保存好上面合成的 www.domainame.com.pfx 的文件，并且牢记设置的密码！

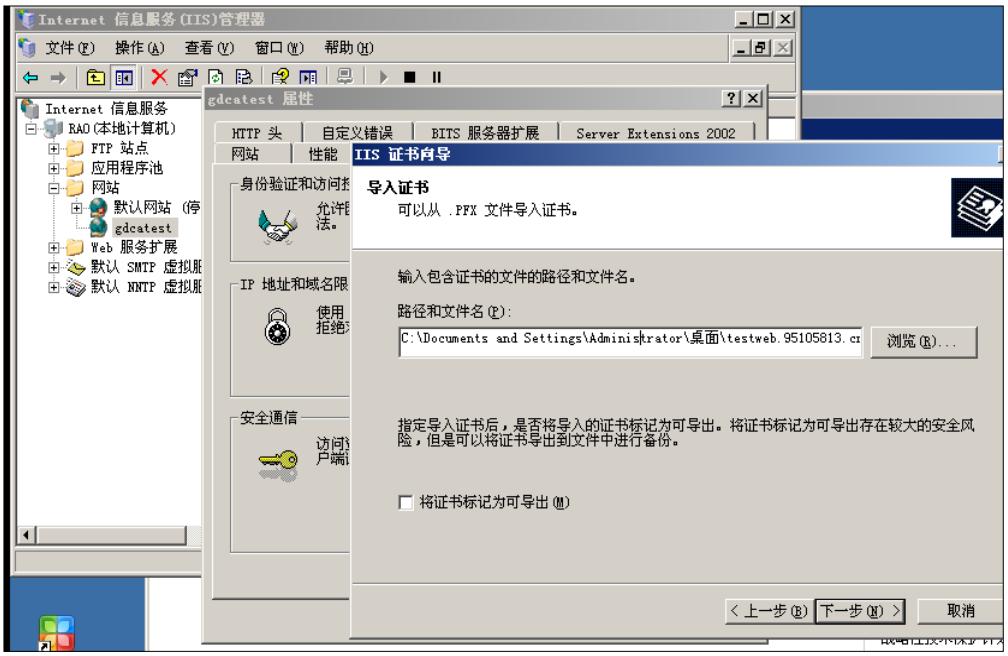
2. 证书的恢复

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

地址：广州市东风中路 448 号成悦大厦第 23 楼邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

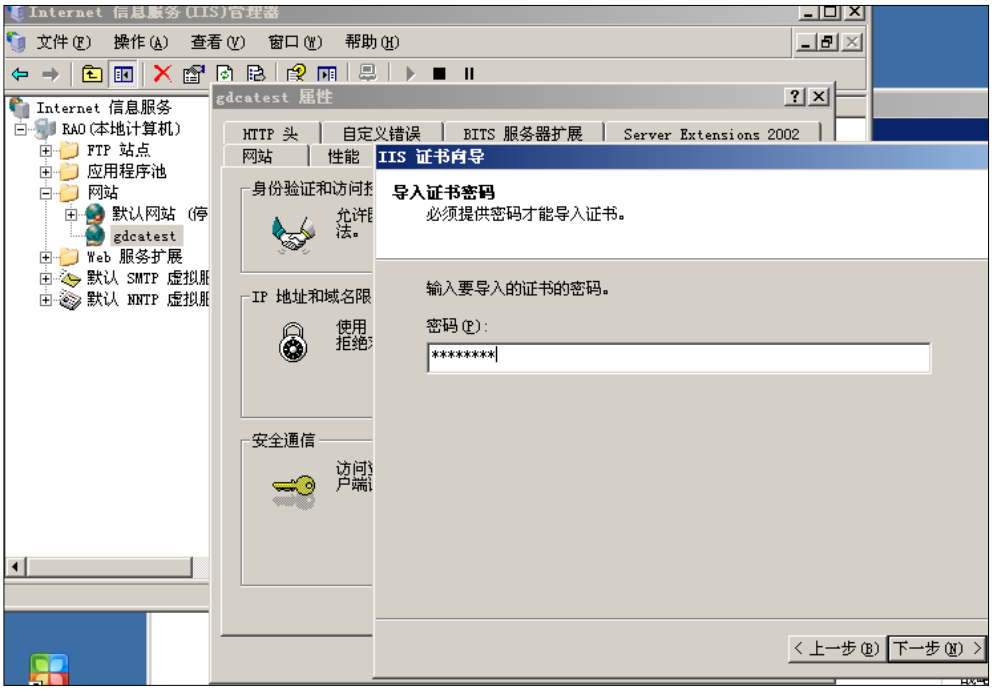


2） 选择您的服务器证书备份文件，点击下一步如果选中“将证书标记为可导出”则您稍后可以将私钥从该服务器导出。不选中此选项时，私钥将无法从服务器中导出。建议您将证书备份文件保存好，不勾选此选项，这将更有利于服务器证书密钥的安全。

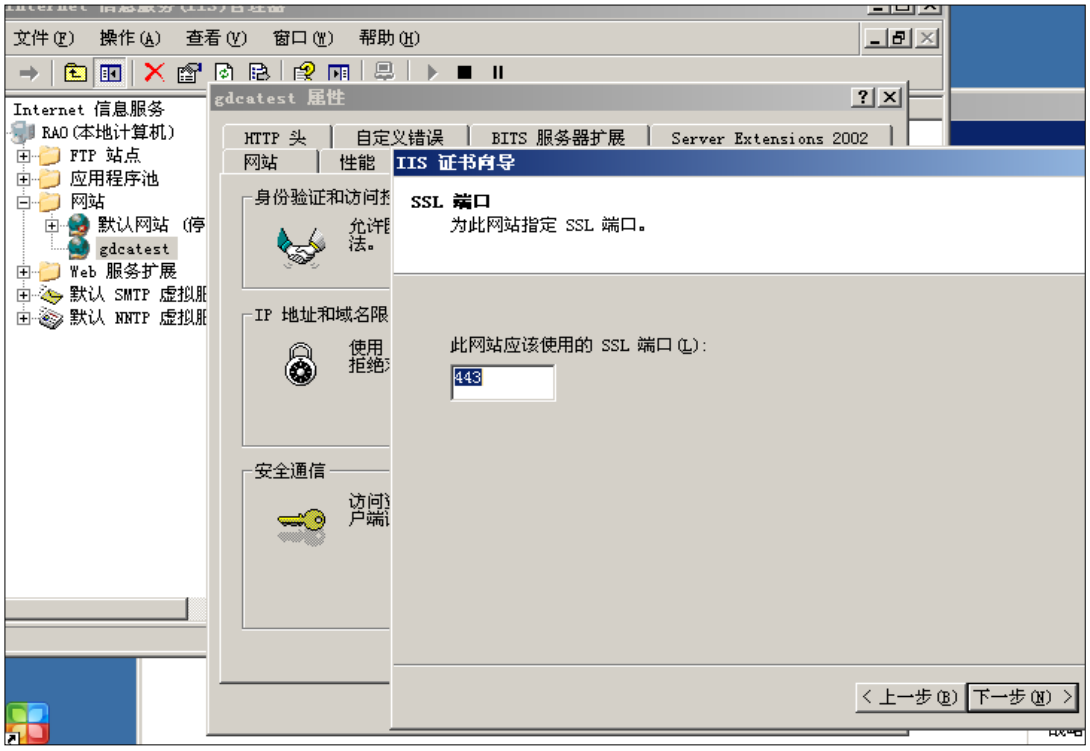


3） 输入备份文件保护密码

地址：广州市东风中路 448 号成悦大厦第 23 楼邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813



4) 指定 SSL 端口，默认为 443



5) 确认导入证书摘要，点击下一步，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）

地址：广州市东风中路 448 号成悦大厦第 23 楼邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813

办理遗失补办业务，重新签发服务器证书。

地址：广州市东风中路 448 号成悦大厦第 23 楼邮编：510030 网址：www.gdca.com.cn
电话：8620—83487228 传真：8620—83486610 客户服务（热线）： 95105813