

IIS使用eToken 实现网站CA认证登录

信息安全顾问
魏荣巍

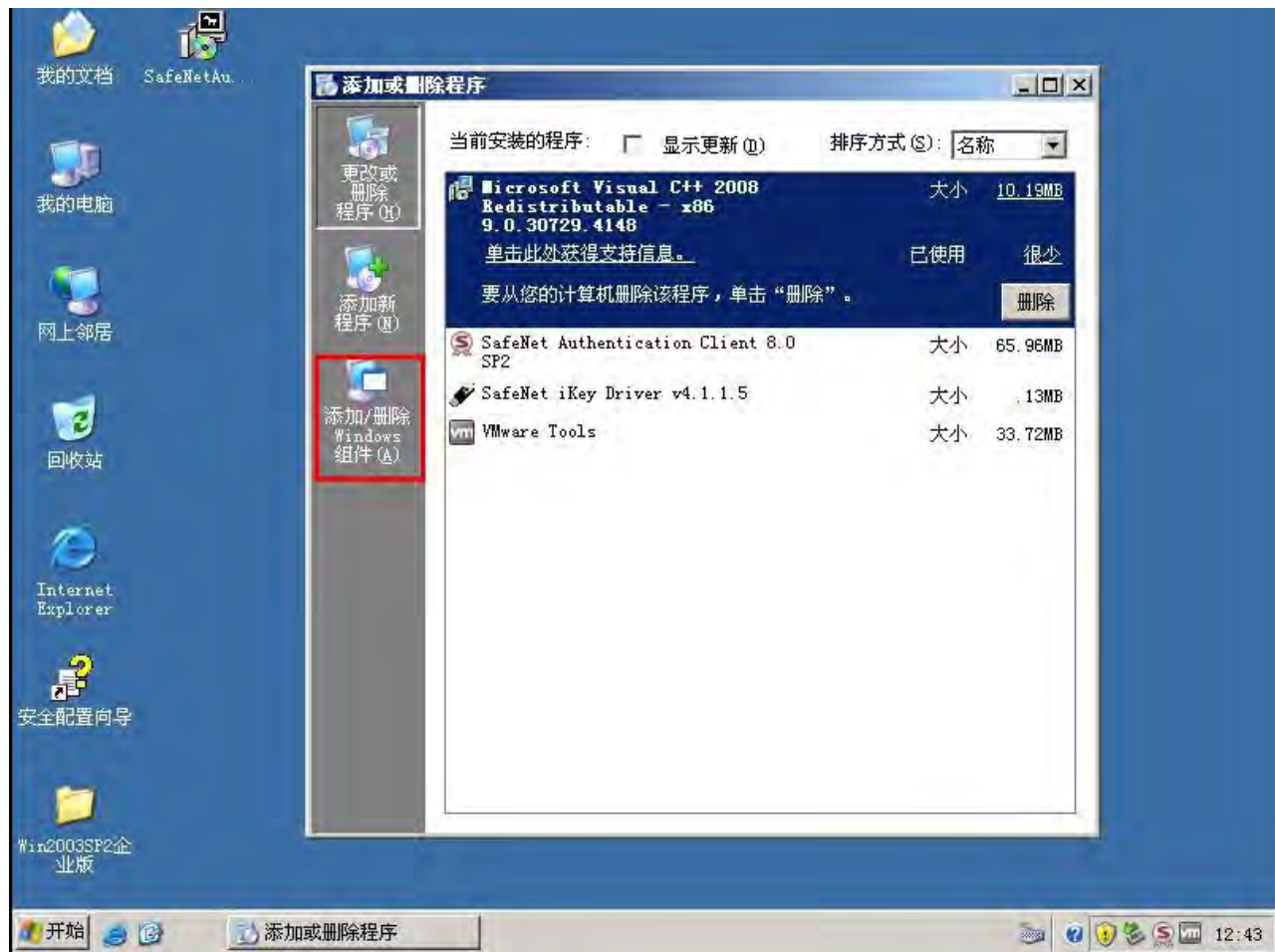


1、相关说明

- 1、本操作是在Windows 2003系统上进行的。
- 2、在操作前，请在电脑上安装eToken驱动软件（SAC），驱动下载地址：
<http://down.wang-cai.com>
- 3、操作过程如下：
 - A、安装IIS和证书服务。（第2——9页）
 - B、为Web站点申请服务器证书。（第10——43页）
 - C、为网站访问用户申请用户证书。

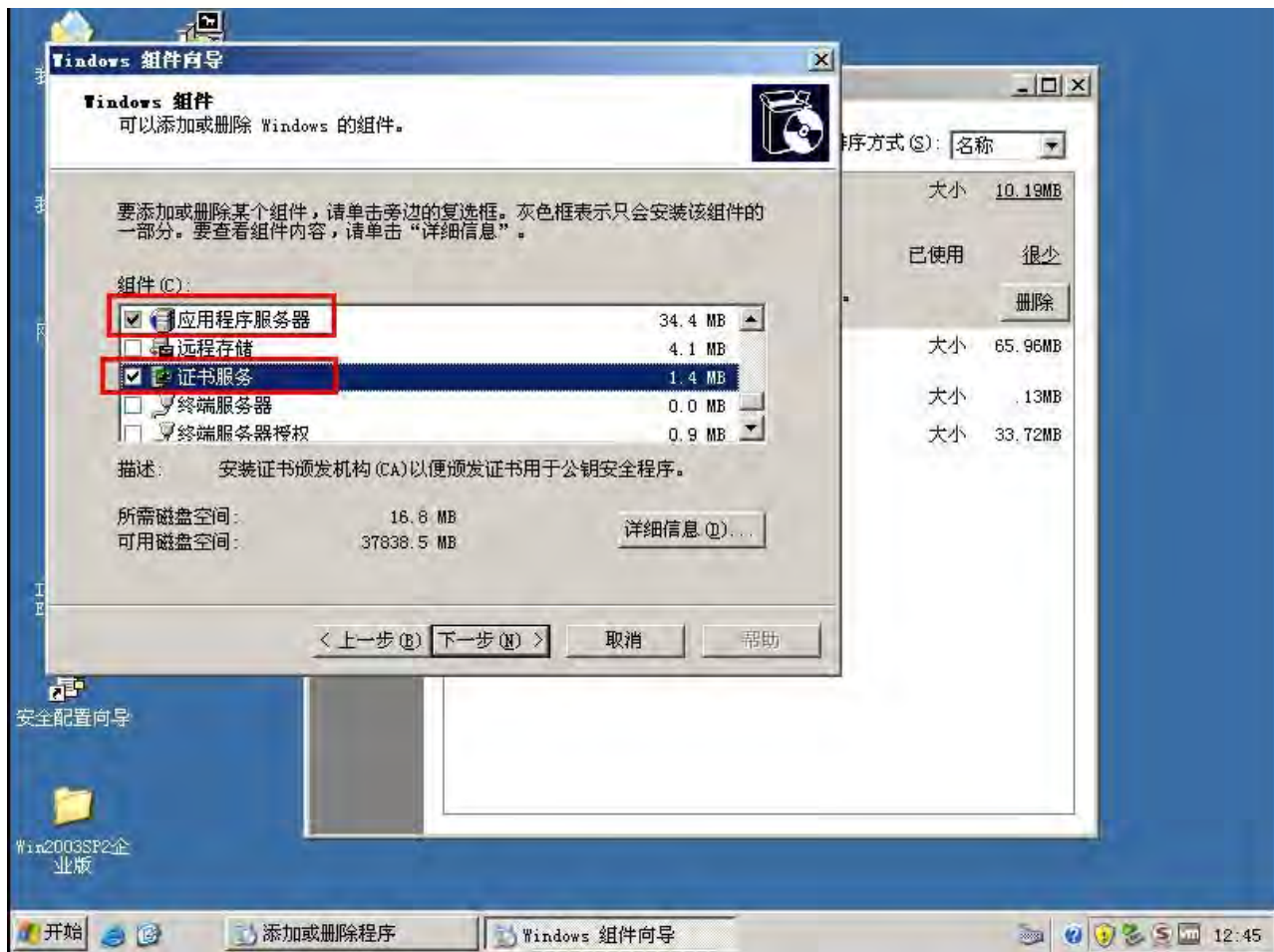


2、打开控制面板——添加删除程序——点击添加/删除Windows组件





3、在列表中选择应用程序服务器、证书服务。





4、双击应用程序服务器，勾选ASP.NET，并确定



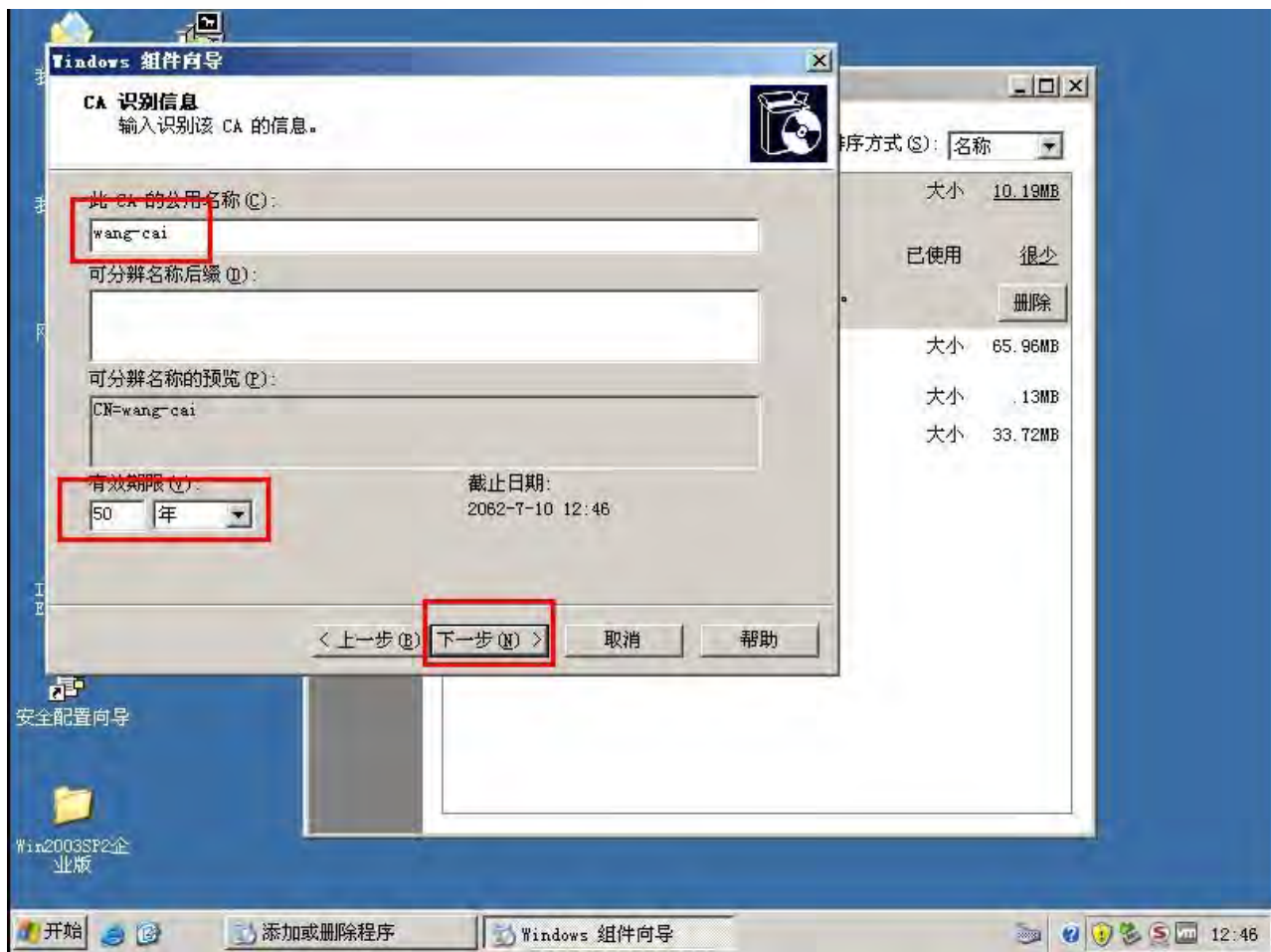


5、在安装证书服务过程中，选择独立根CA



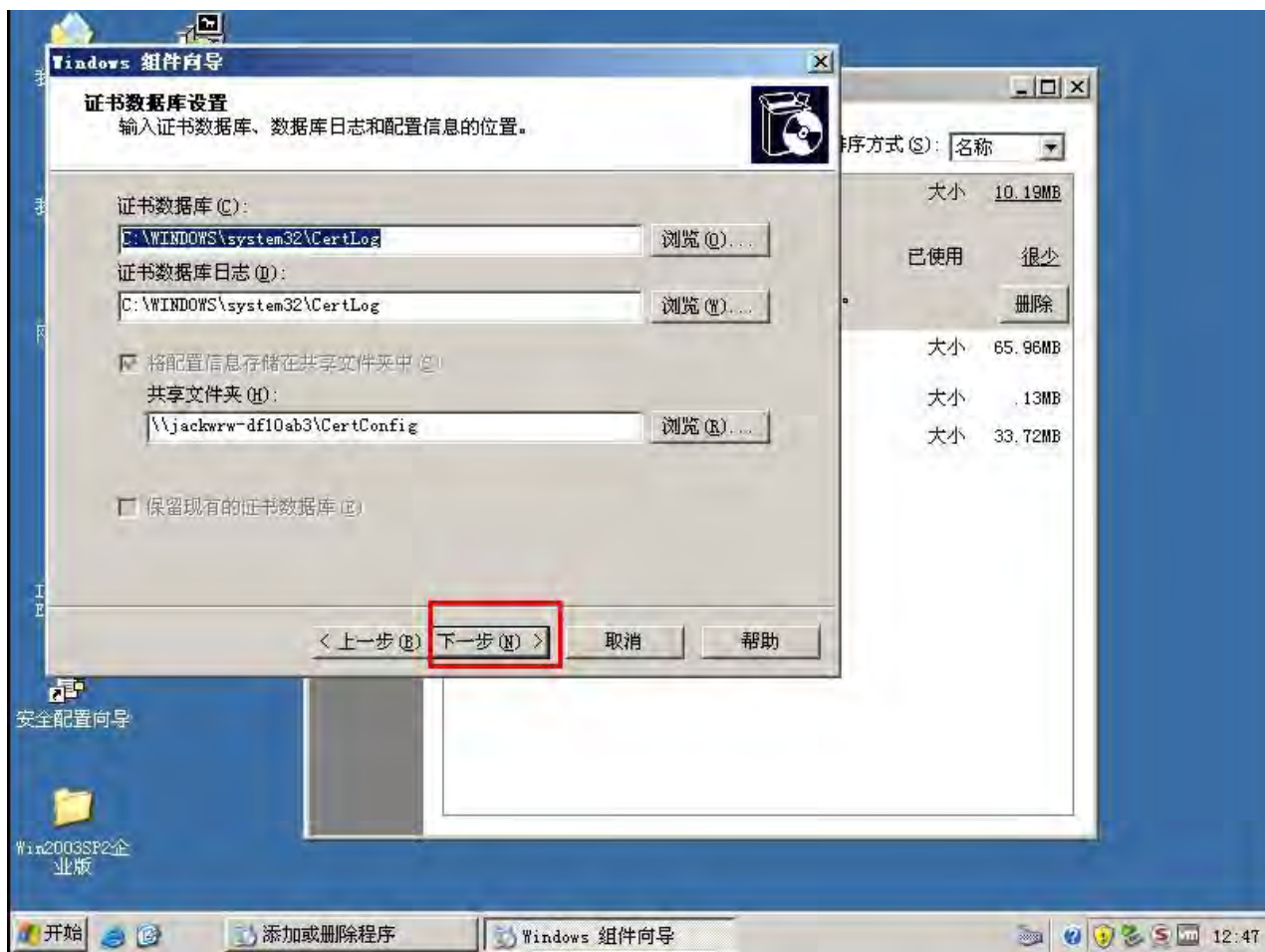


6、设定CA名称、年限



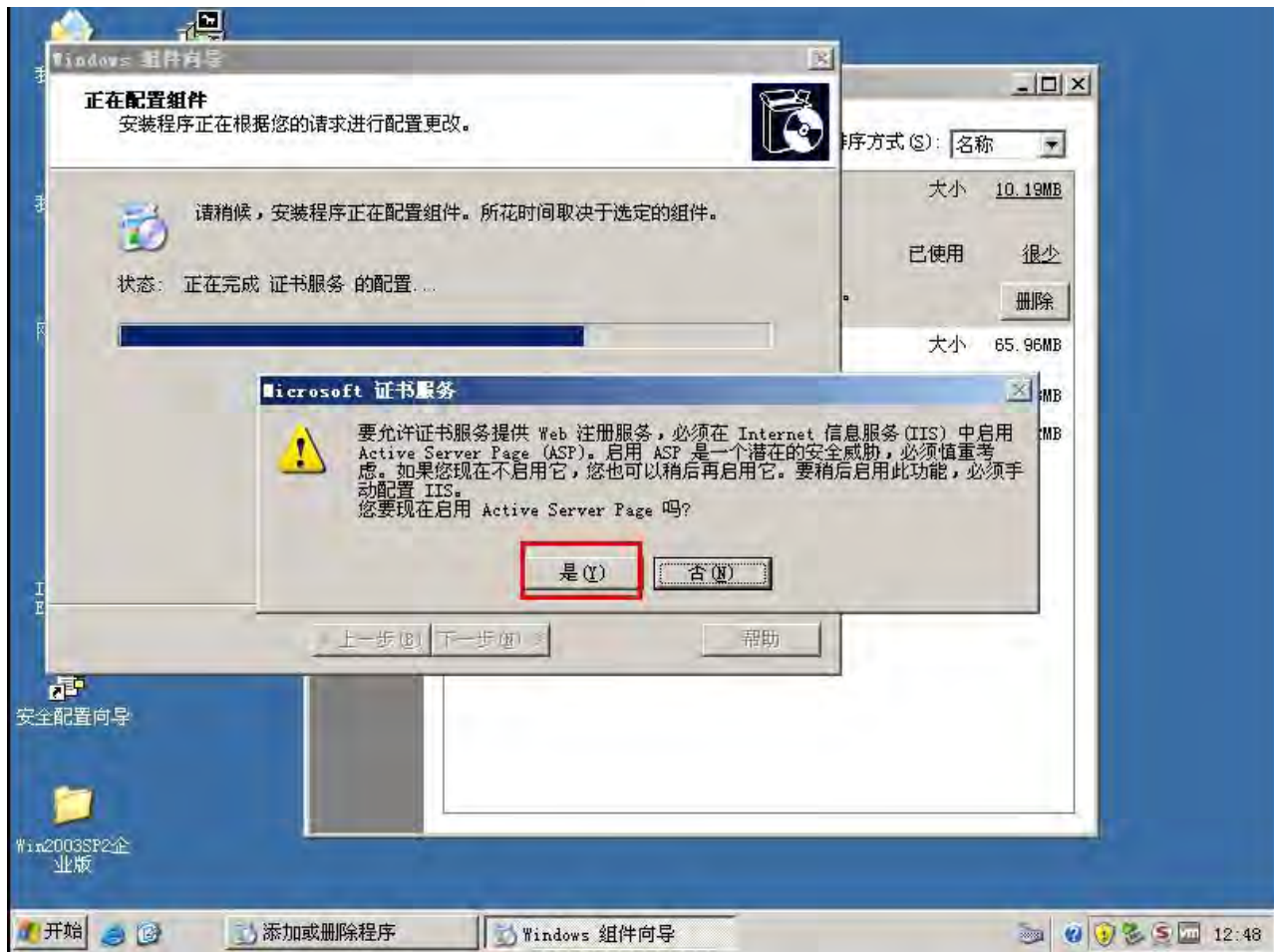


7、设定证书数据库设置（建议使用默认）



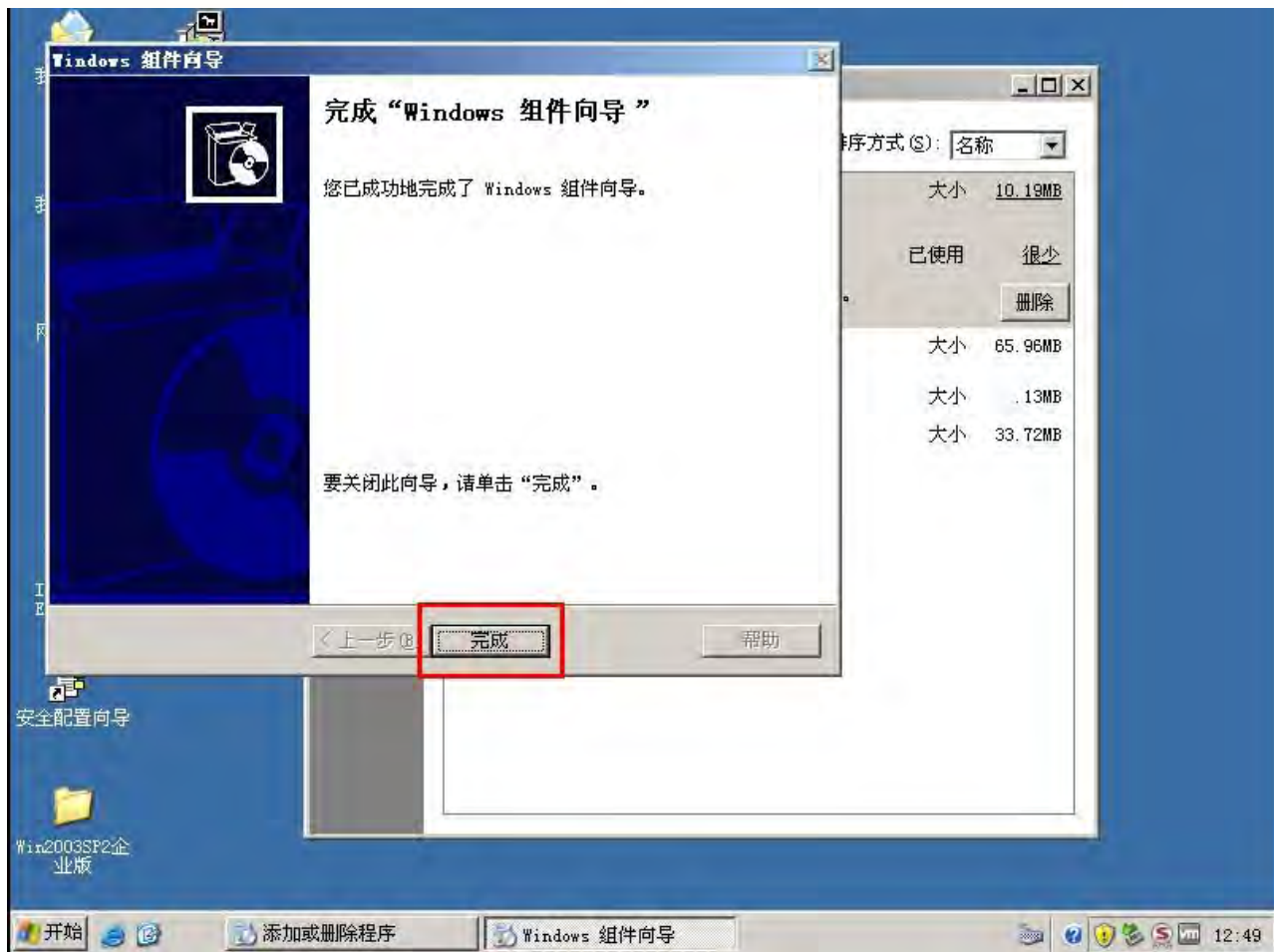


8、安装证书服务过程中，启用ASP



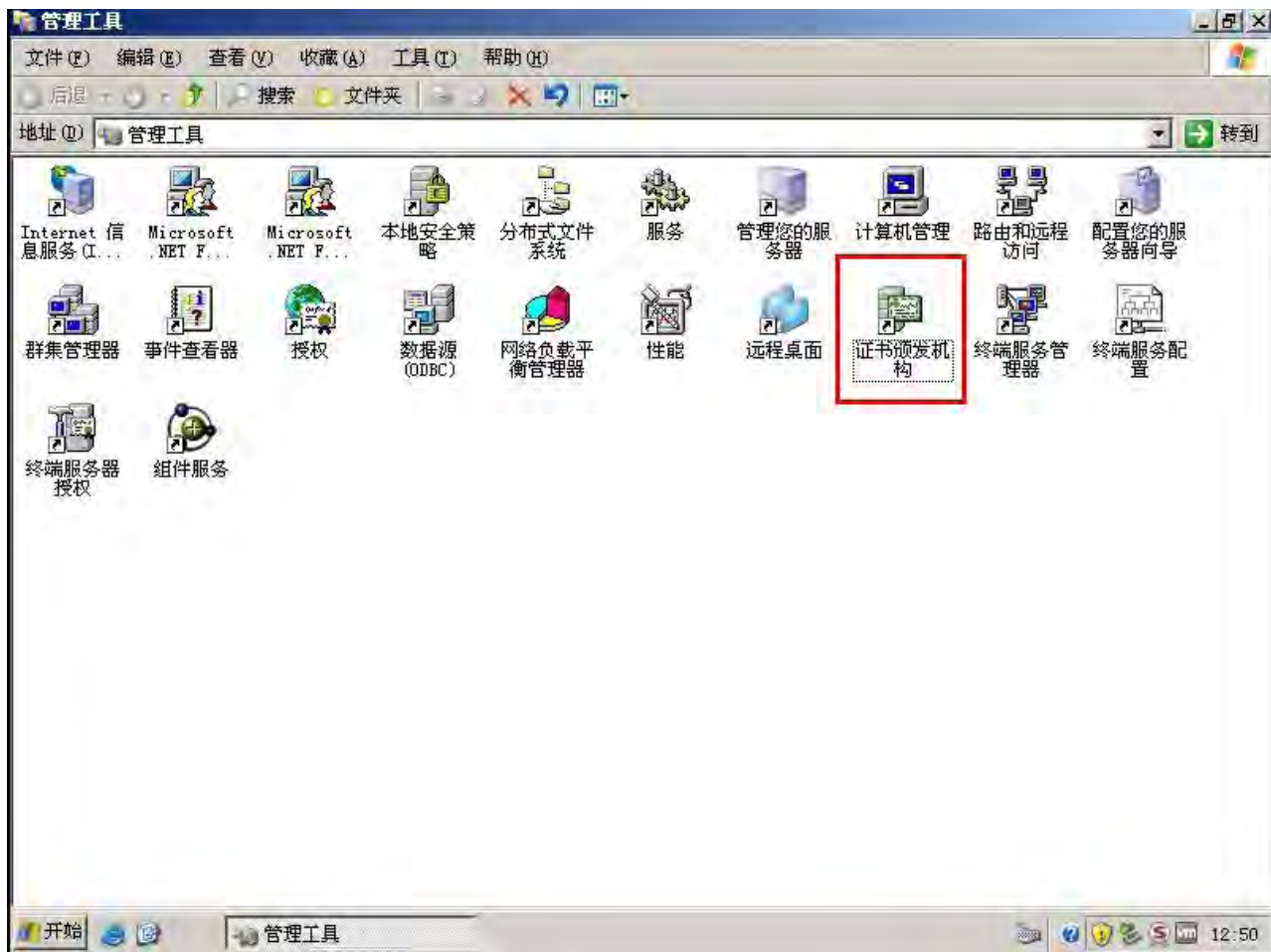


9、完成IIS和证书服务的安装



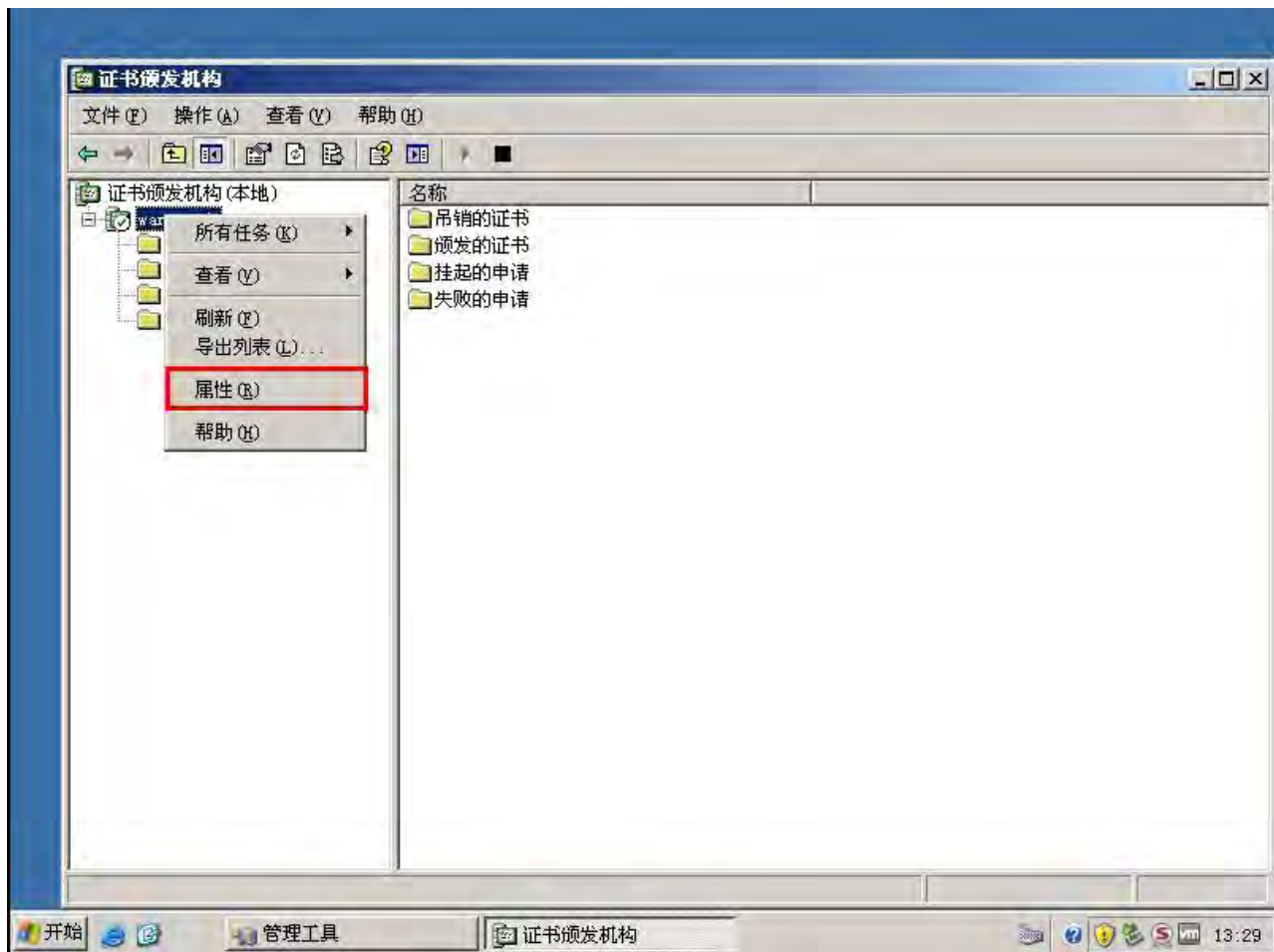


10、在控制面板——管理工具中，打开证书颁发机构



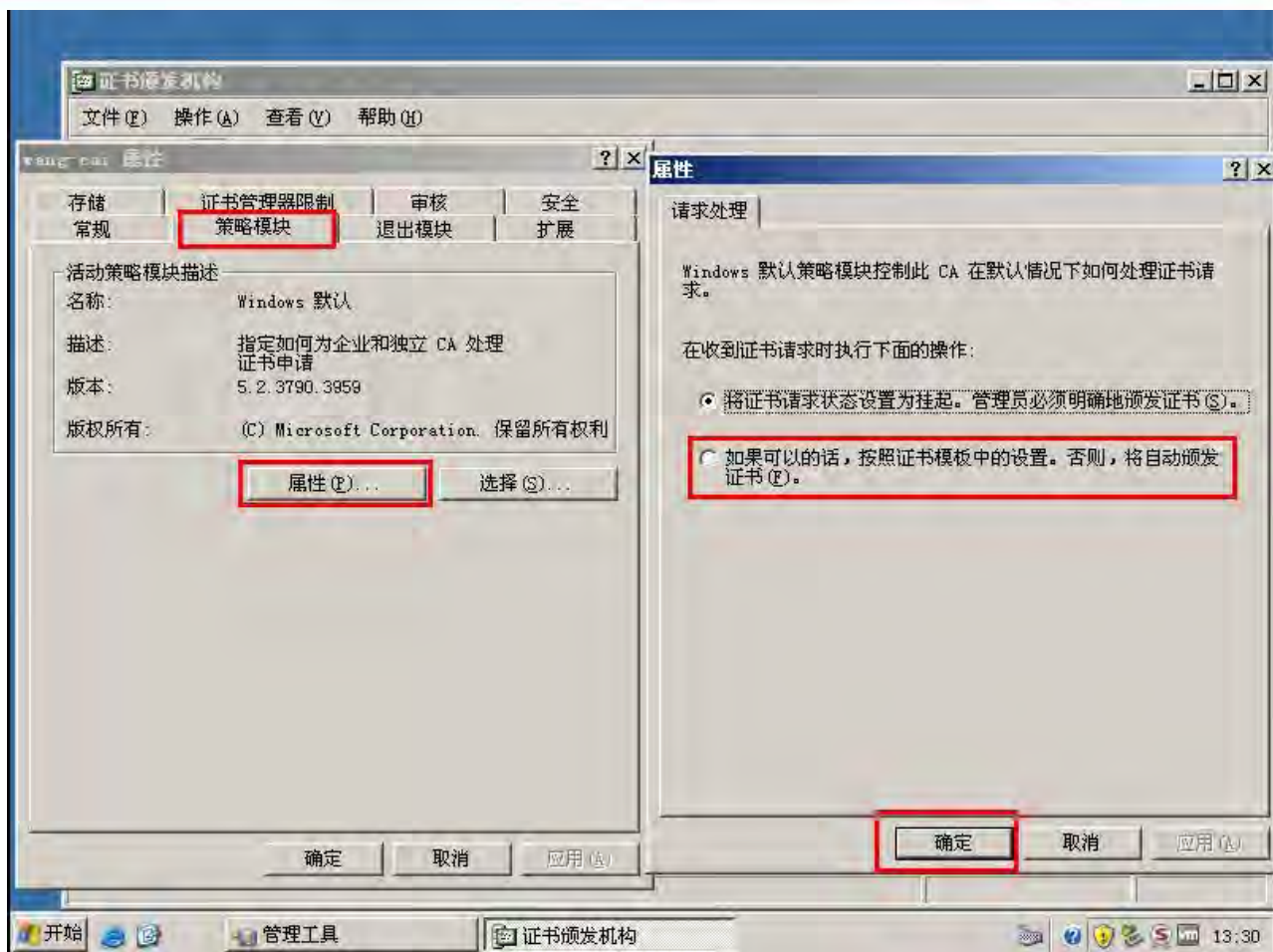


11、在证书机构上点击右键——属性



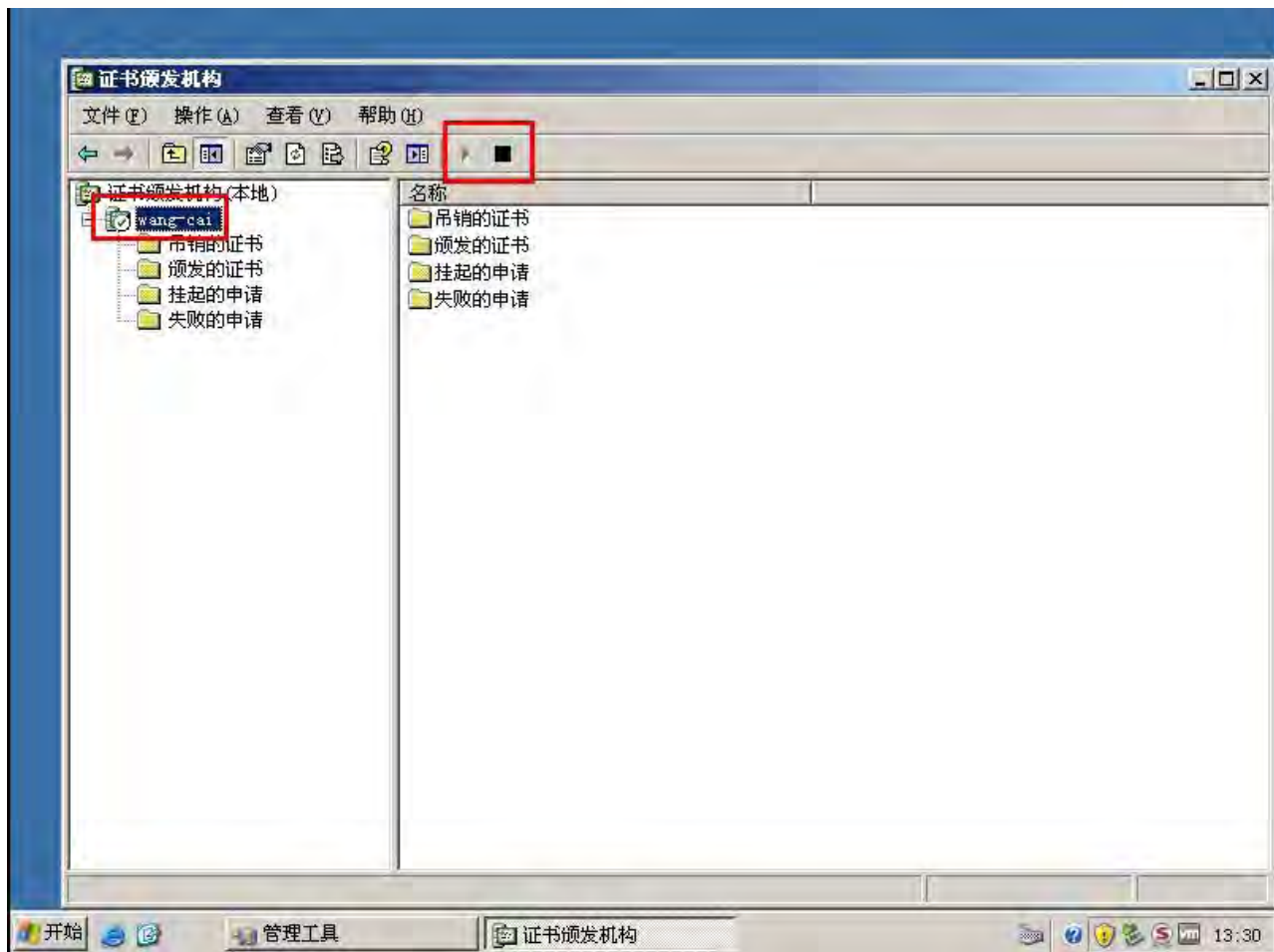


12、选择策略模块——属性，选择自动颁发证书。 (也可以使用手动颁发方式，此处不做单独讲解)





13、点击按钮，重新启动证书服务



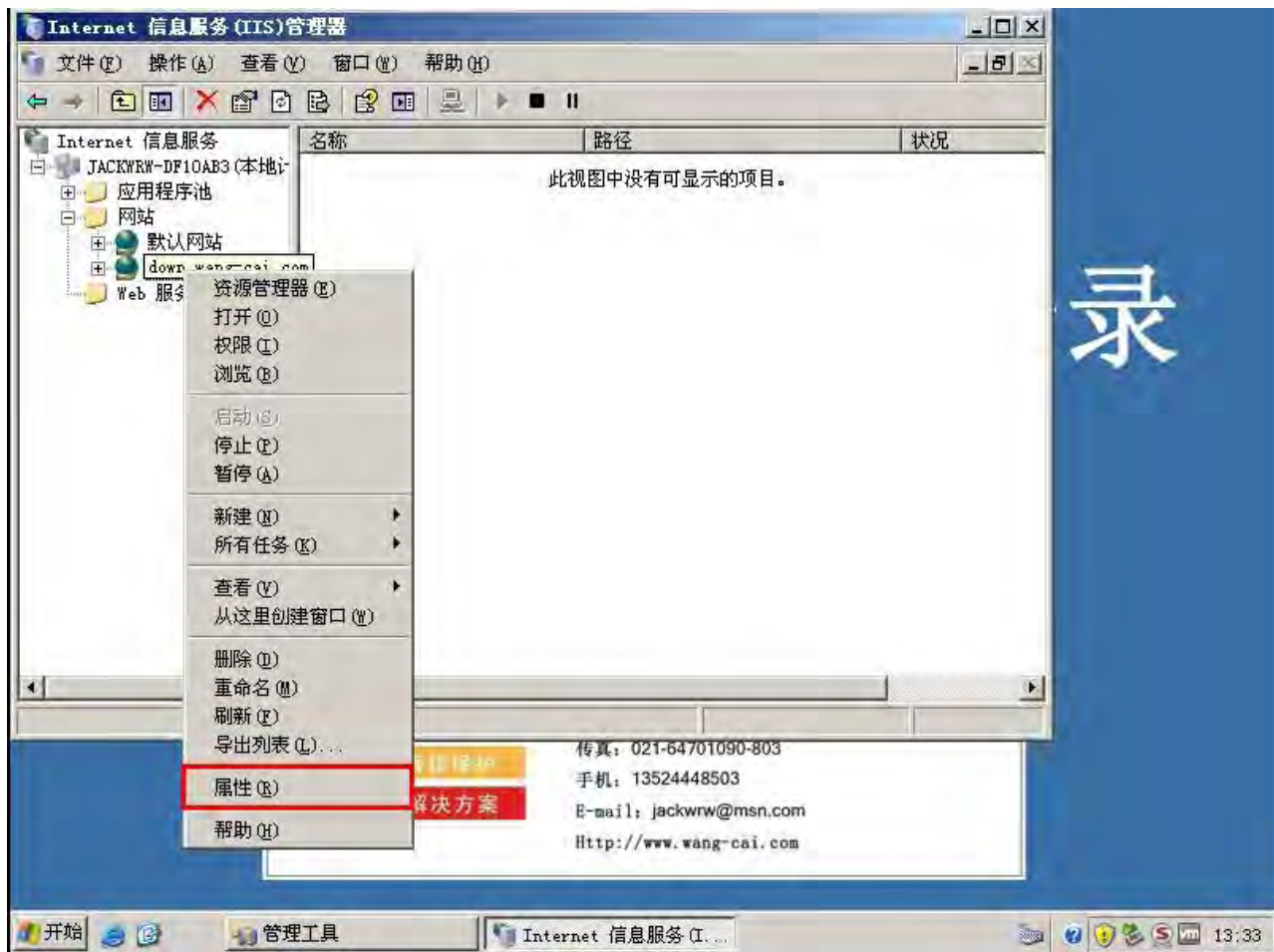


14、打开IIS



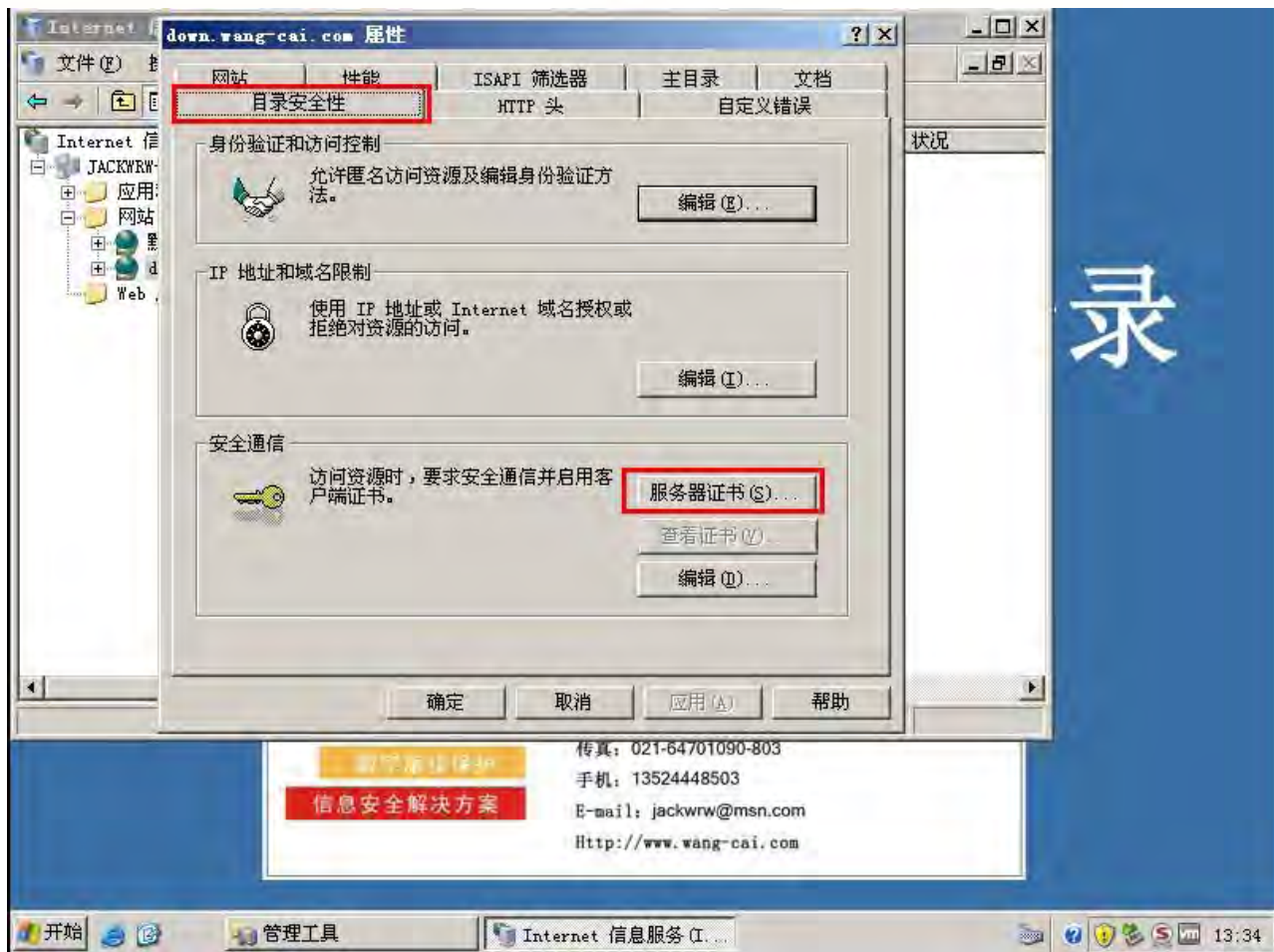


15、选择目标站点，右键——属性



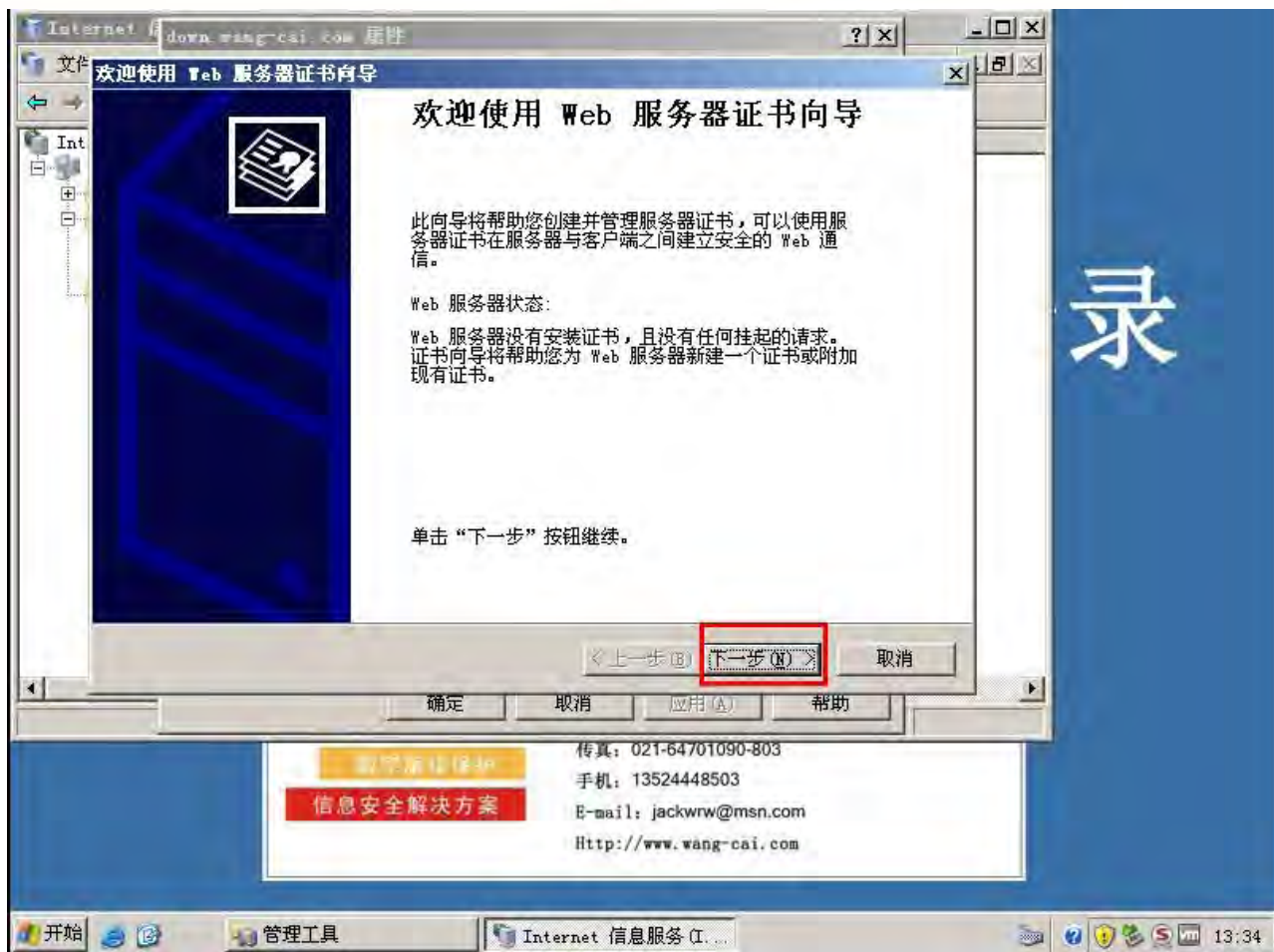


16、在目录安全性中，选择服务器证书



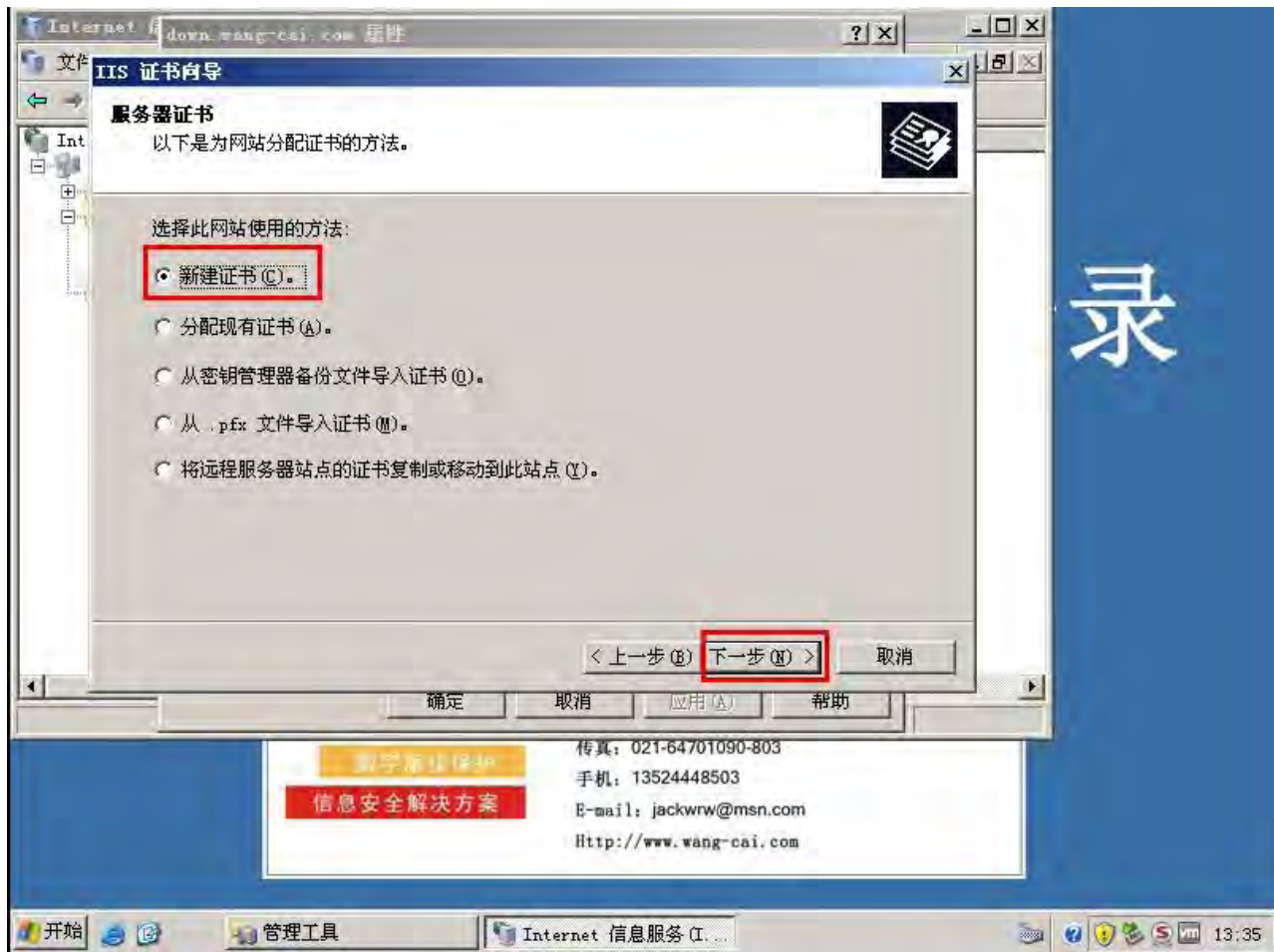


17、点击下一步



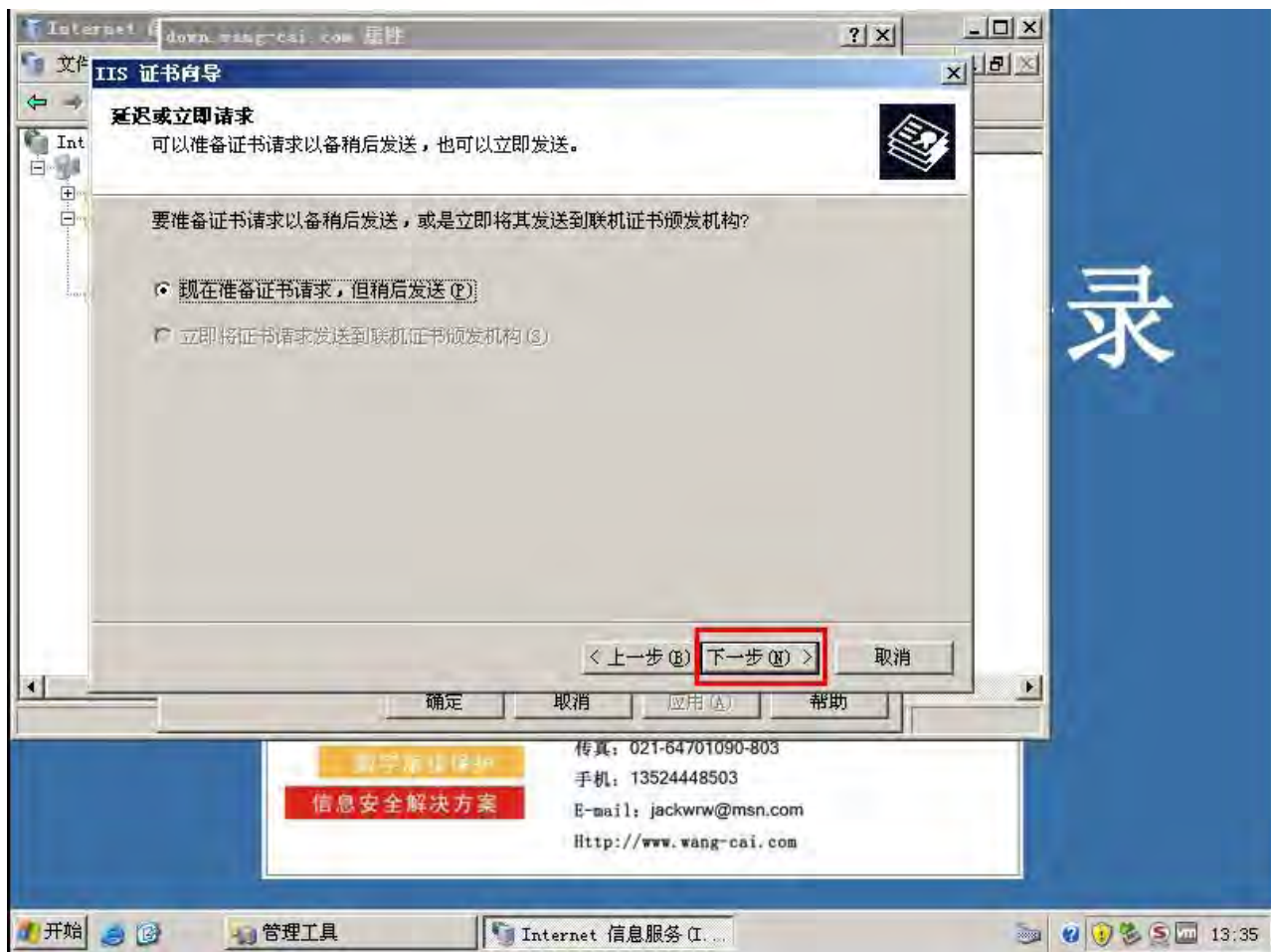


18、选择新建证书，点击下一步





19、点击下一步



录

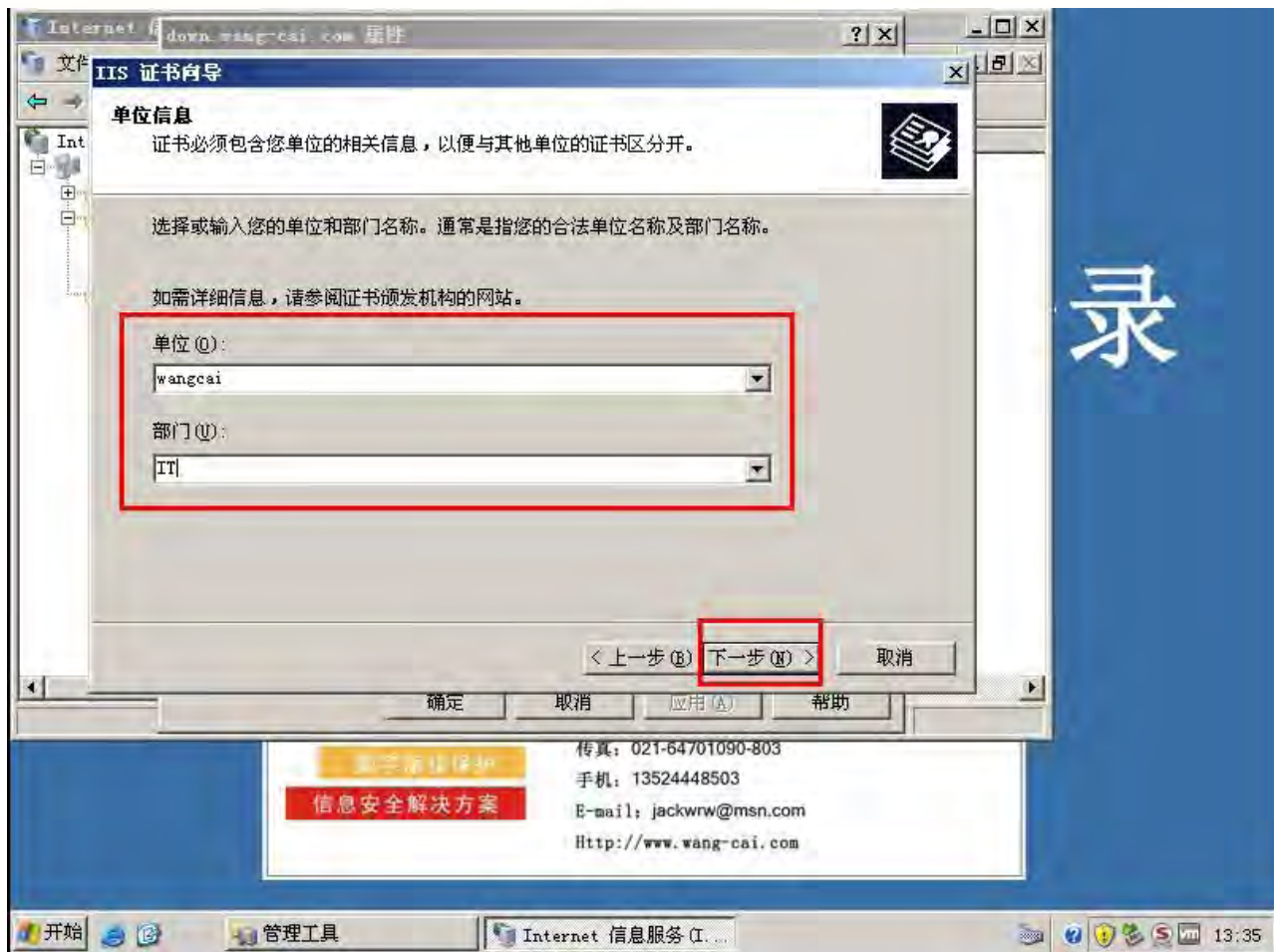


20、点击下一步





21、设定单位名称和部门，点击下一步





22、点击下一步





23、设定地理信息，点击下一步



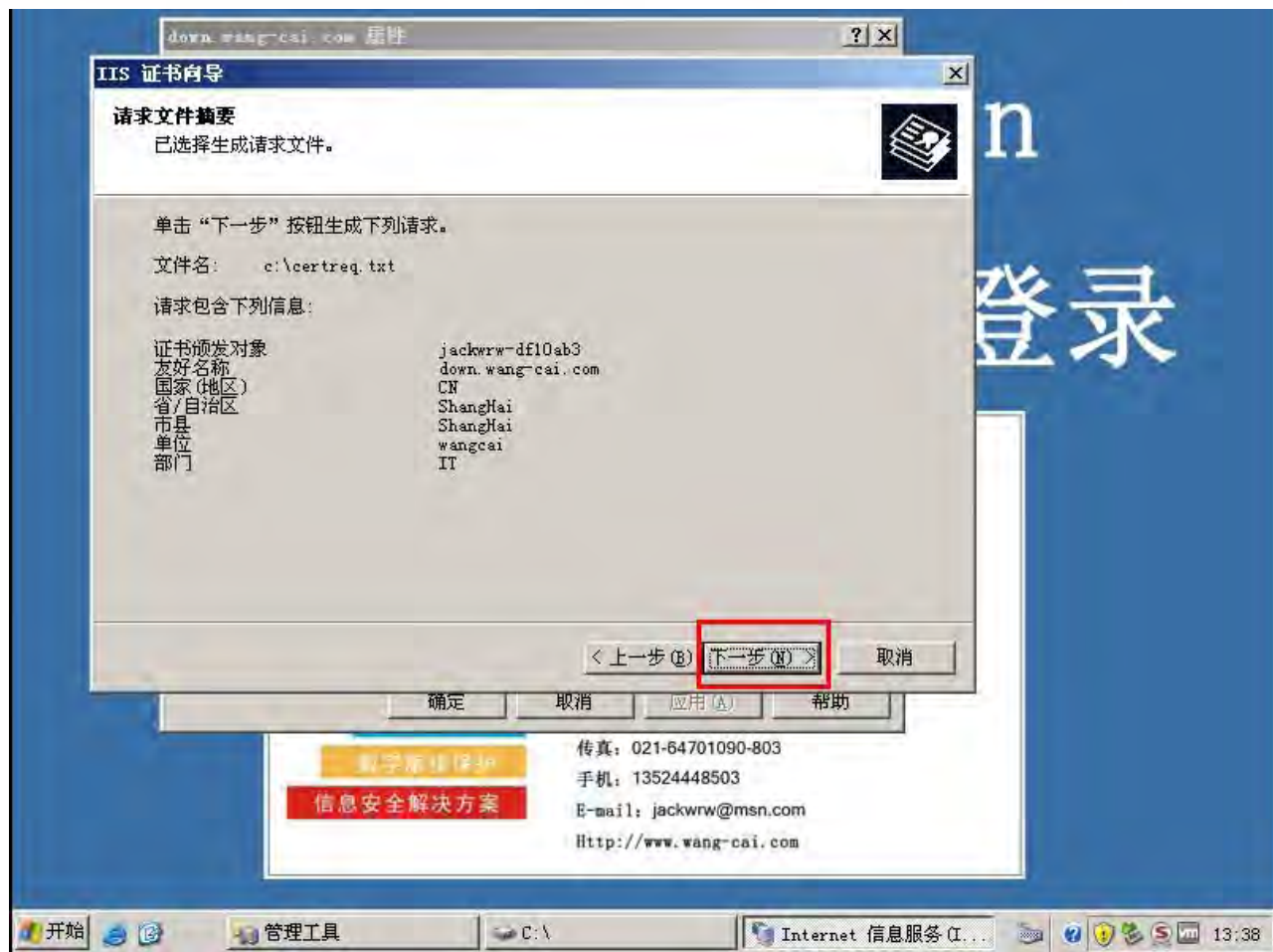


24、保存证书请求文件（建议默认），点击下一步





25、点击下一步



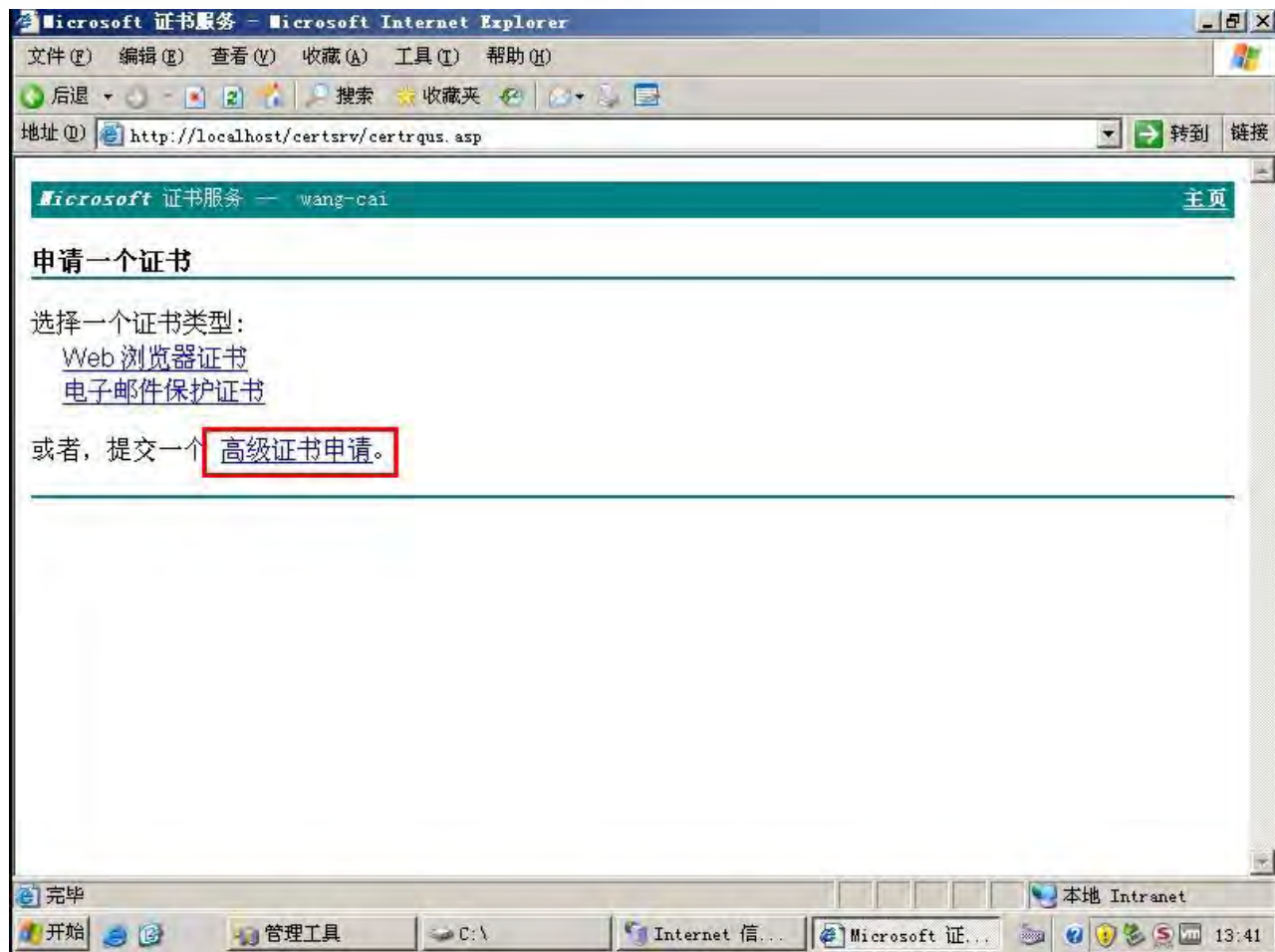


26、打开IE，访问<http://localhost/certsrv> 点击申请一个证书



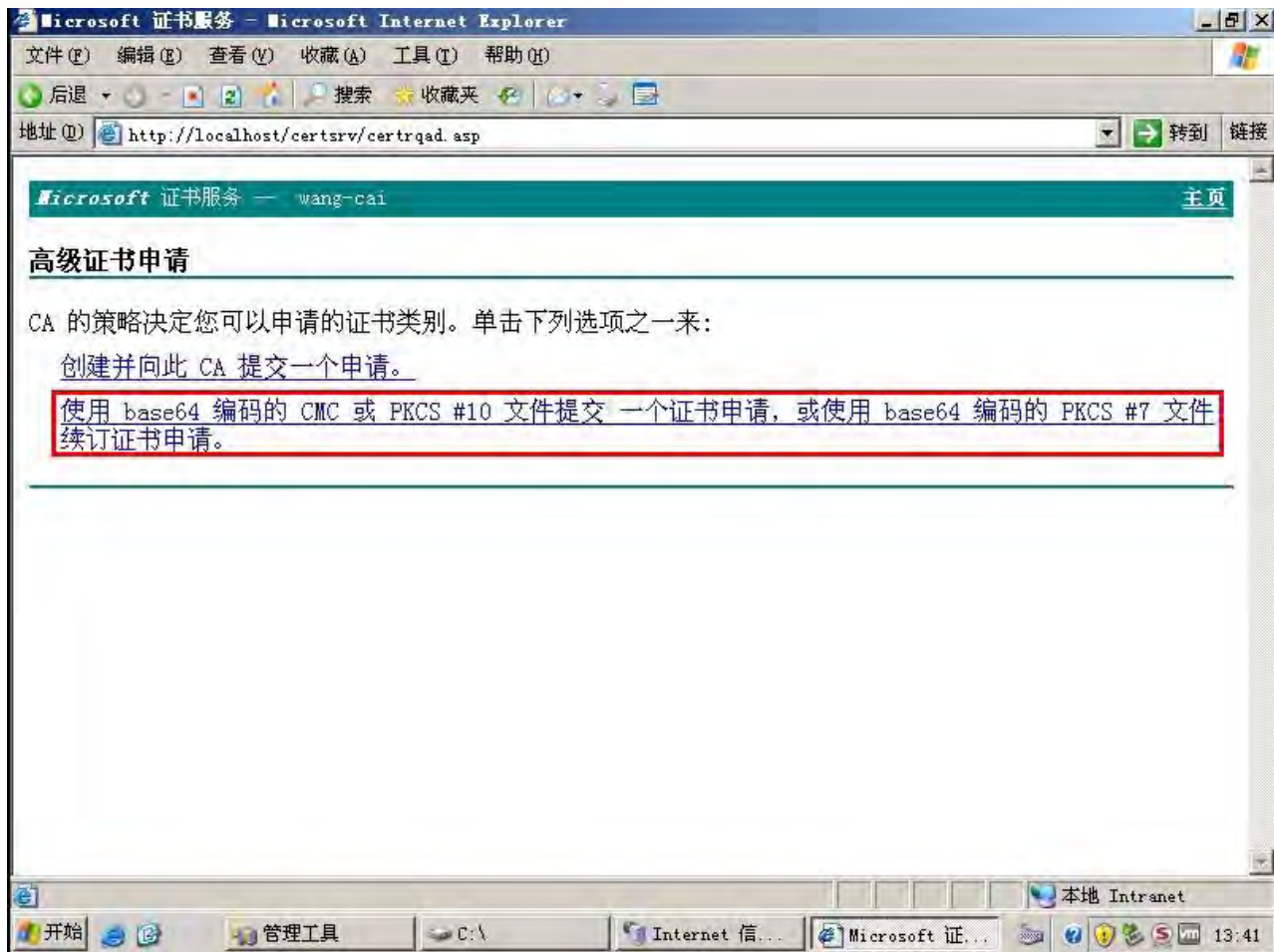


27、选择高级证书申请



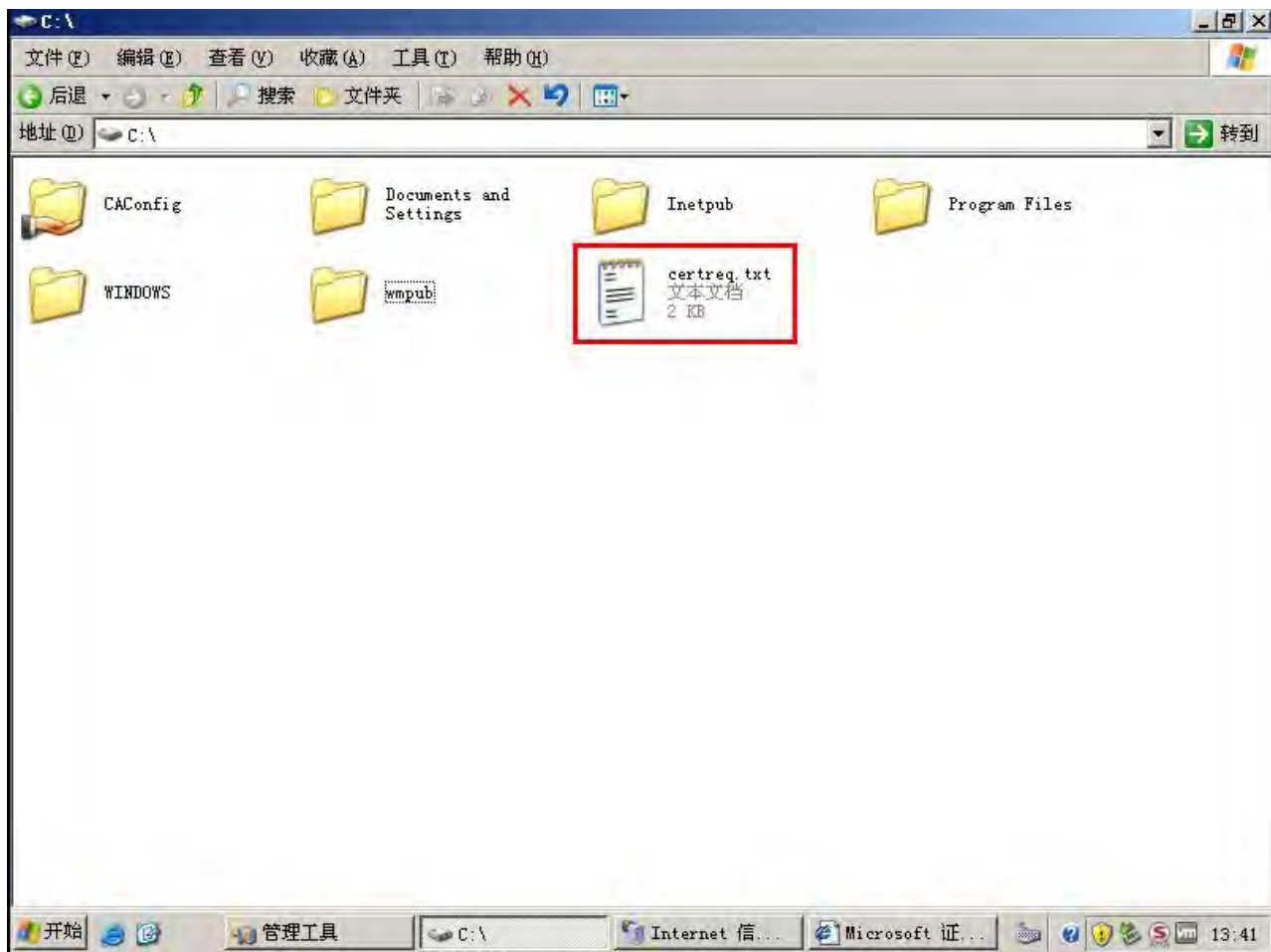


28、选择续订证书申请



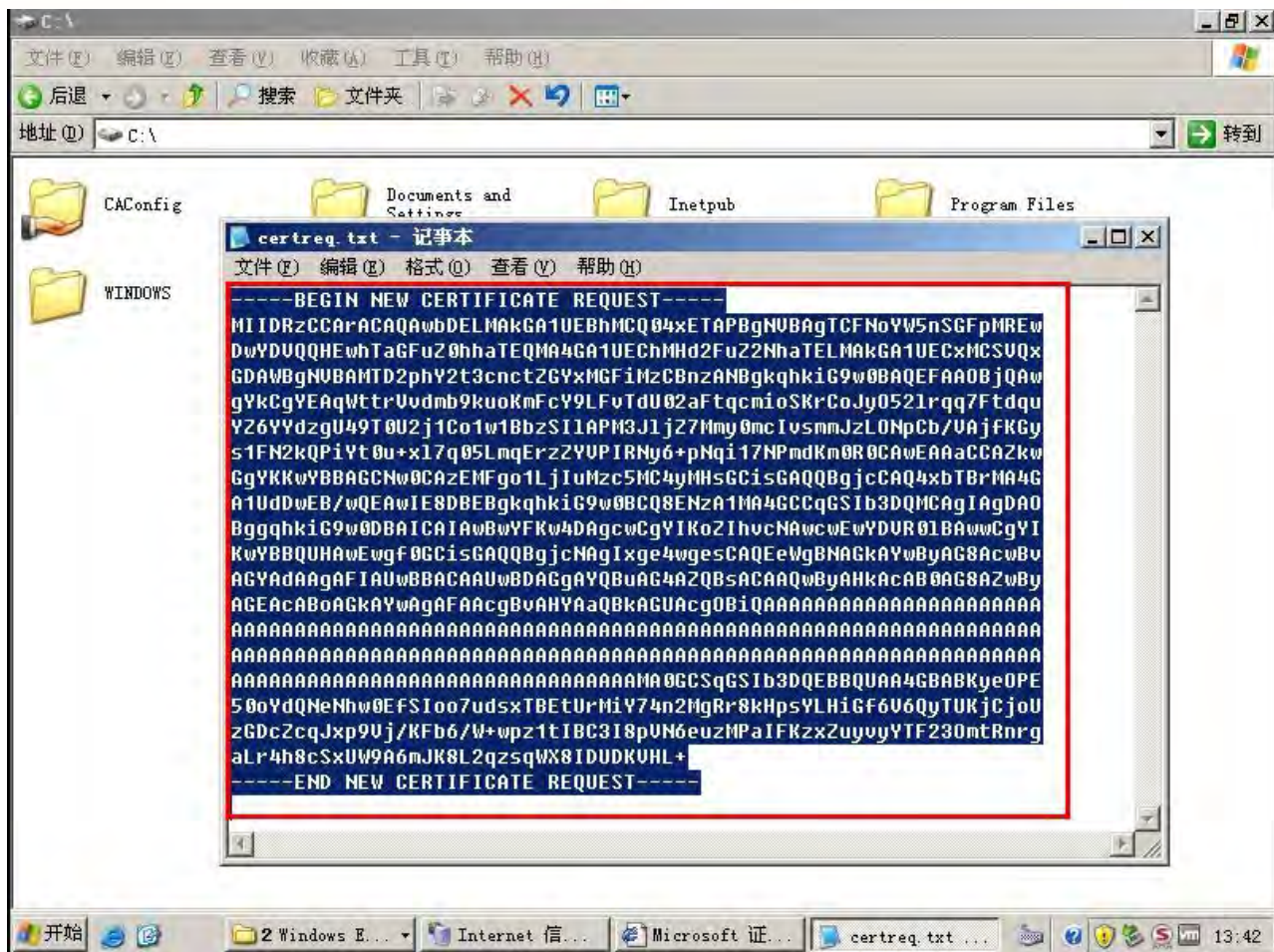


29、打开第24步骤中保存的TXT文件，



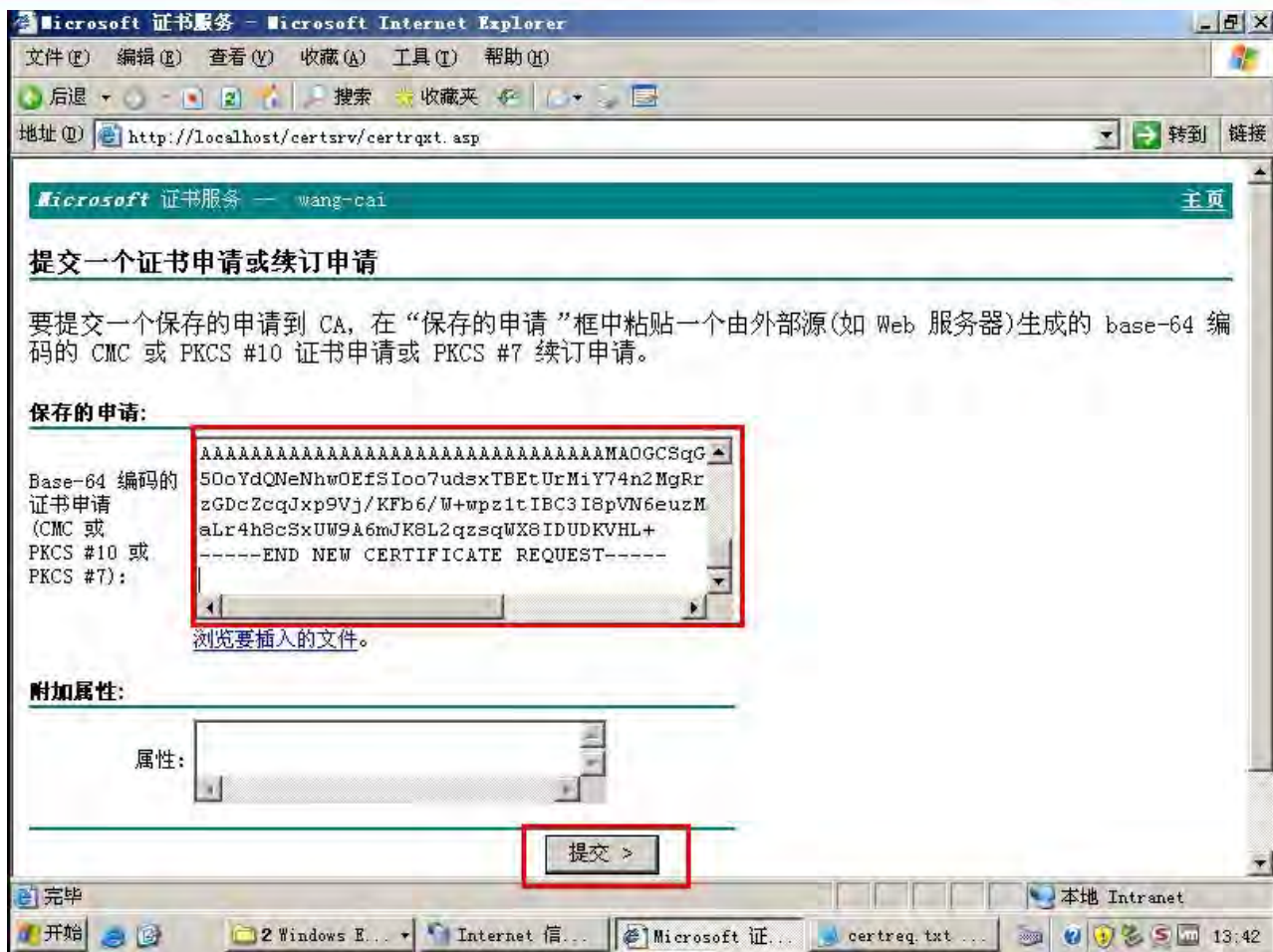


30、全选TXT里的文字，并复制





31、将文字粘贴到IE中，点提交



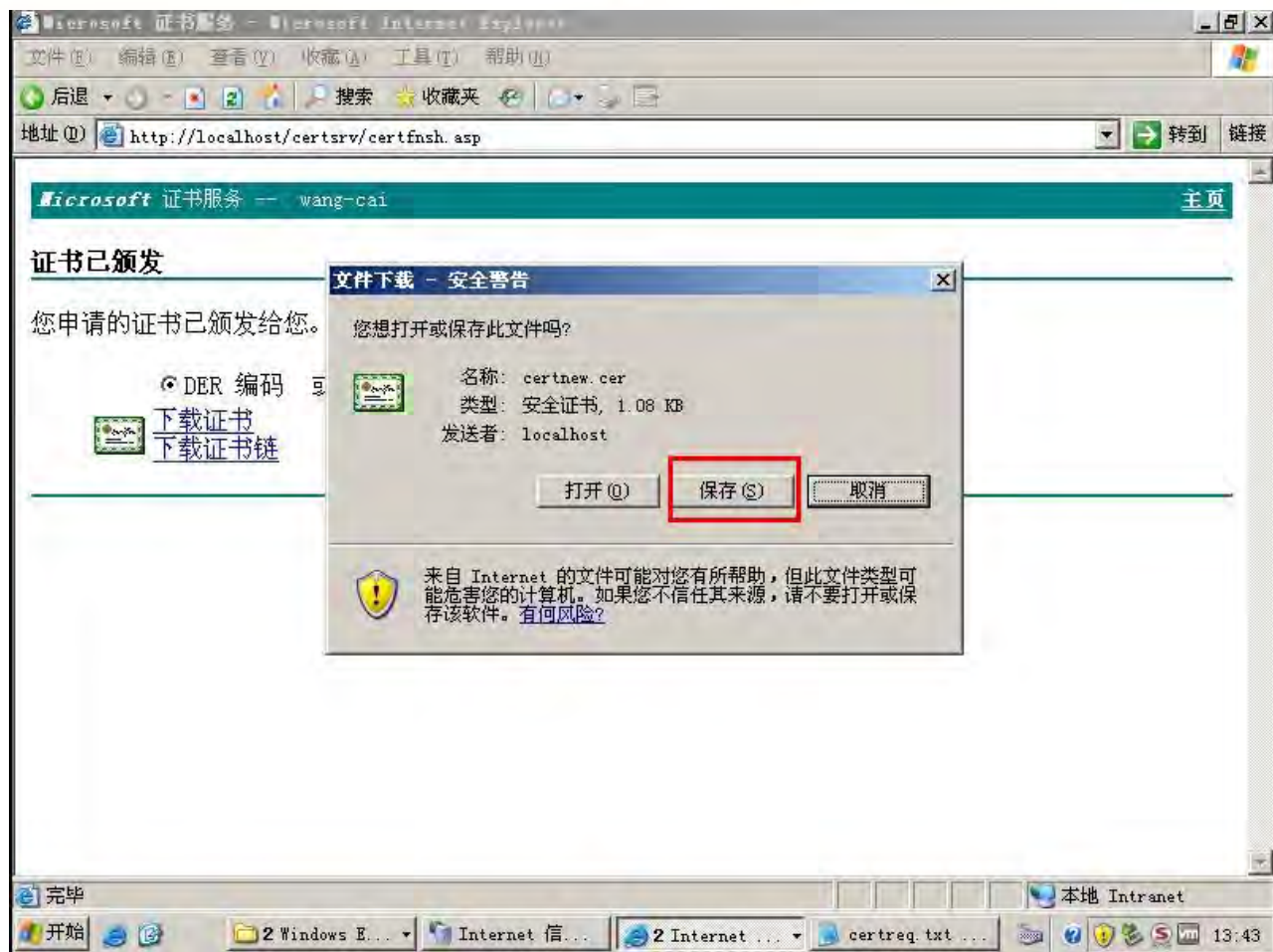


32、点击下载证书



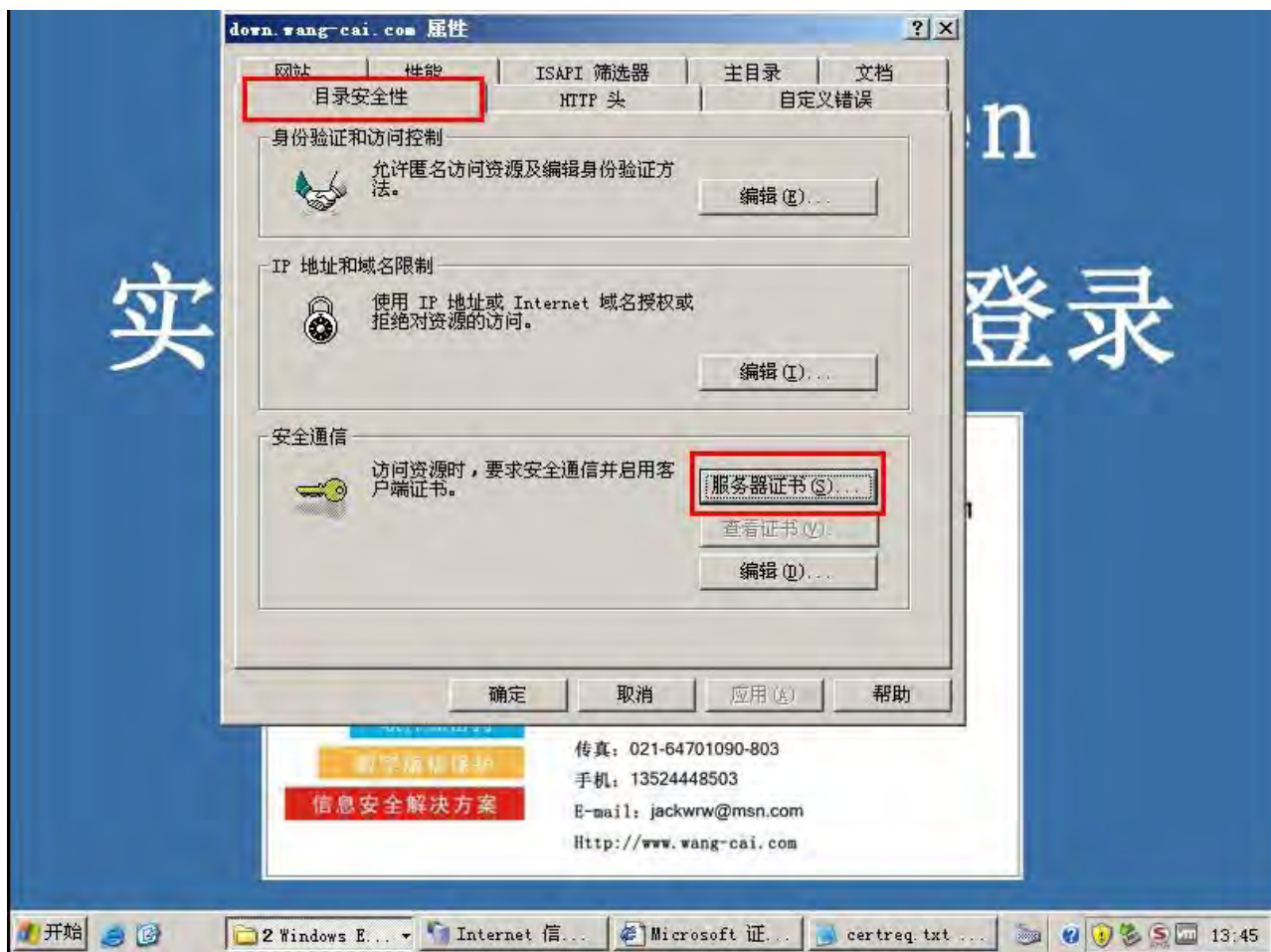


33、保存证书



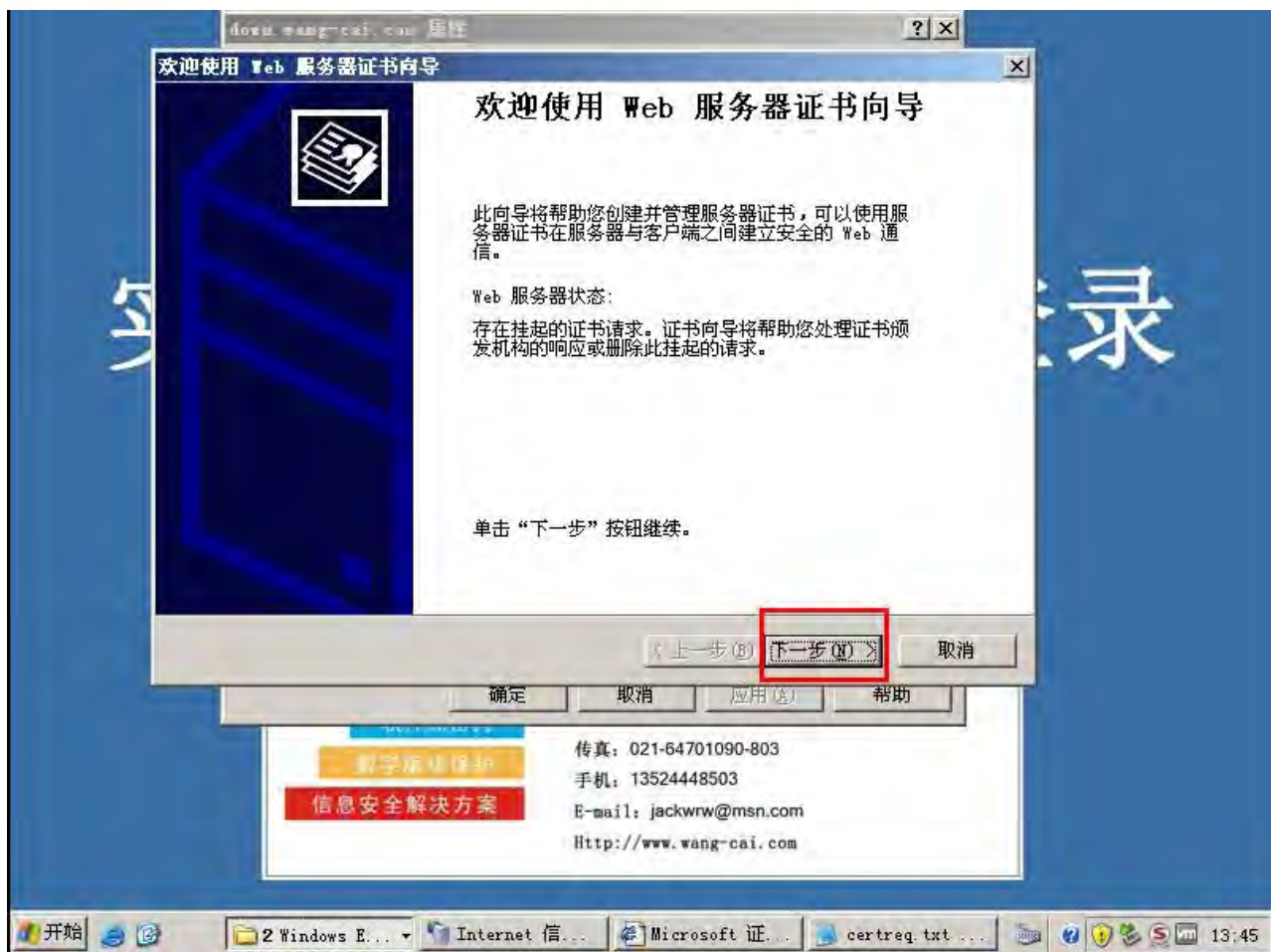


34、在站点属性中，再次点击服务器证书



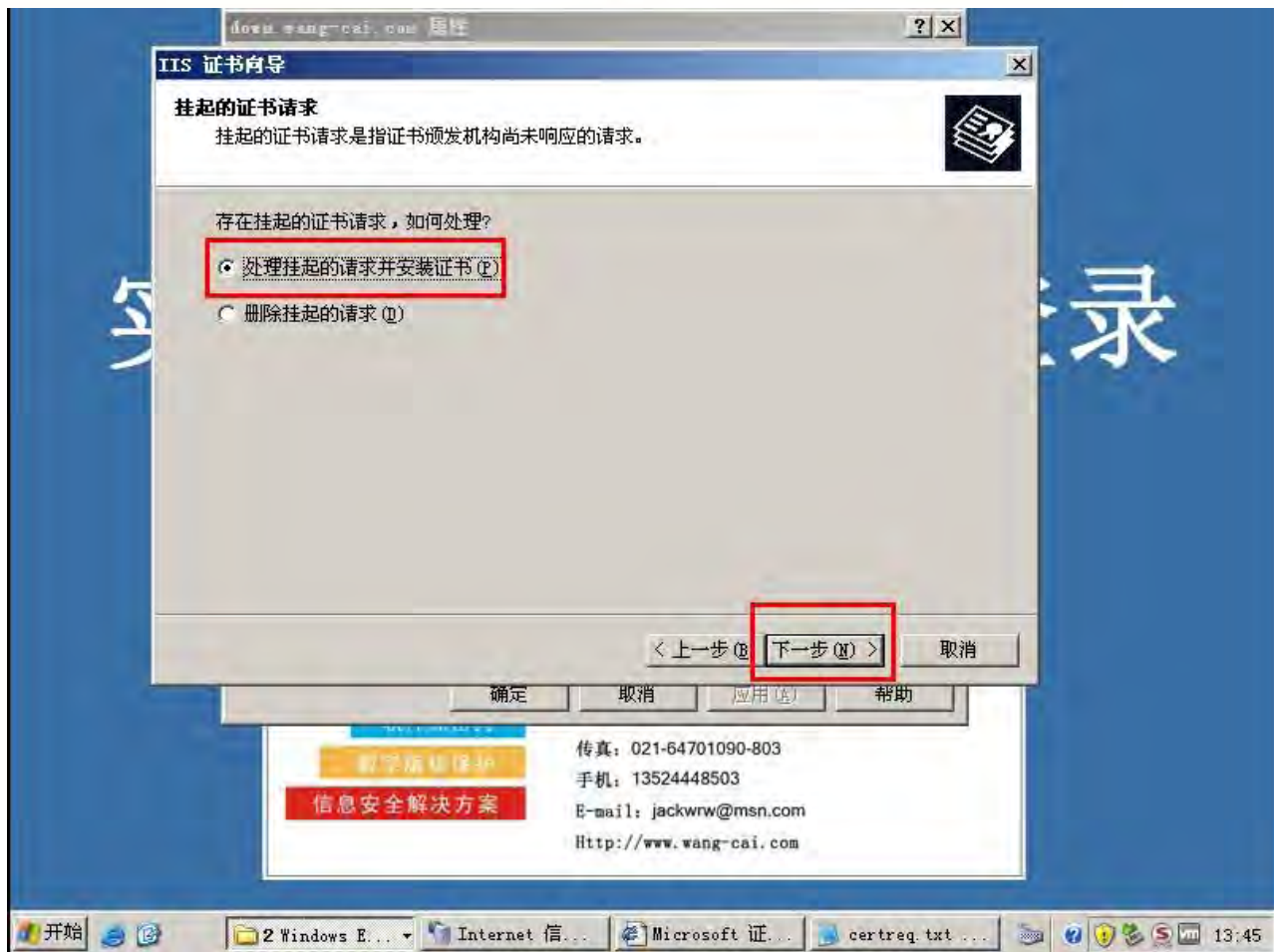


35、点击下一步





36、选择处理挂起的请求并安装证书，点击下一步





37、选择第33步骤中保存的证书，点击下一步





38、设定CA认证的SSL端口（默认443），点击下一步



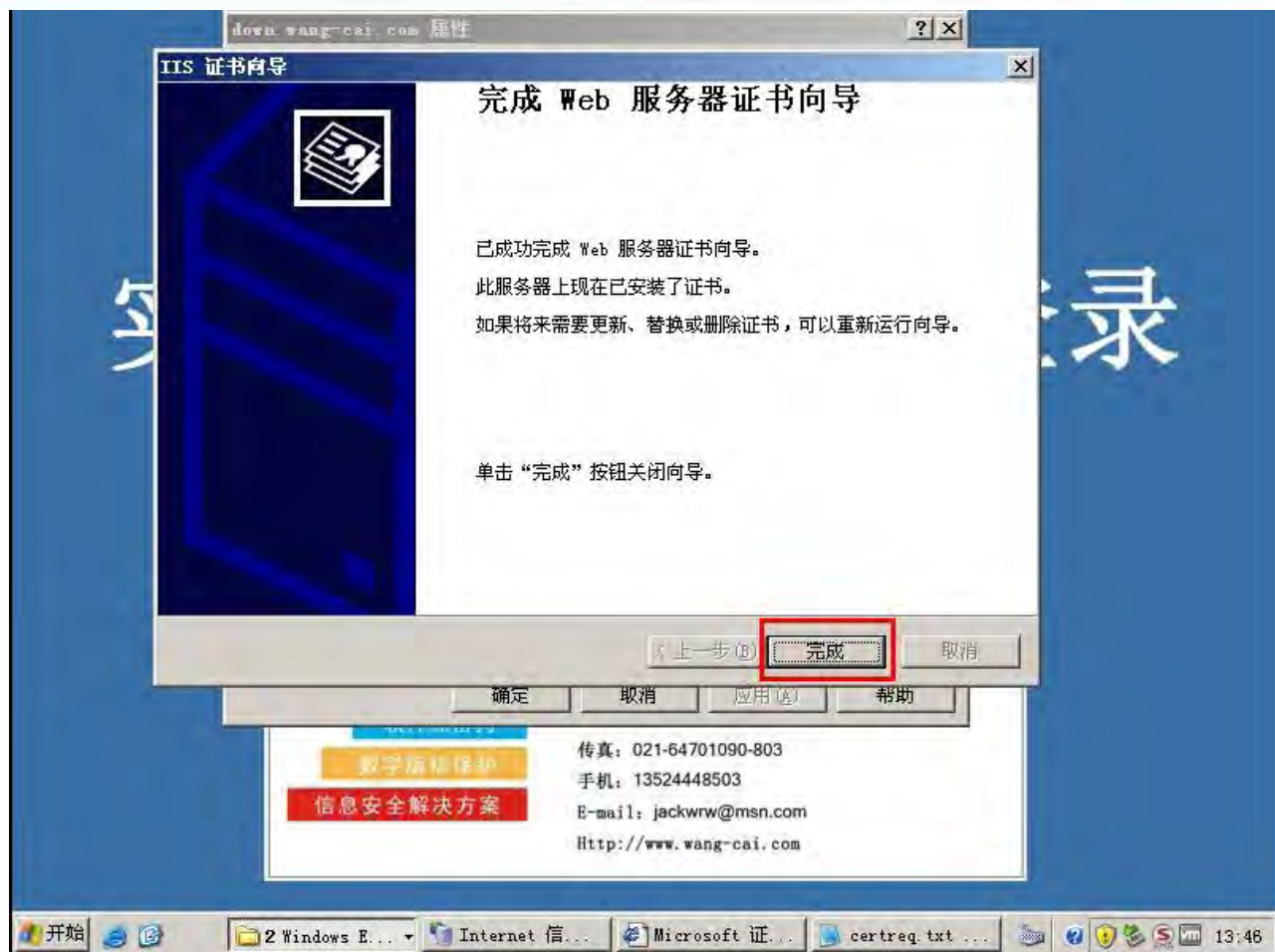


39、点击下一步



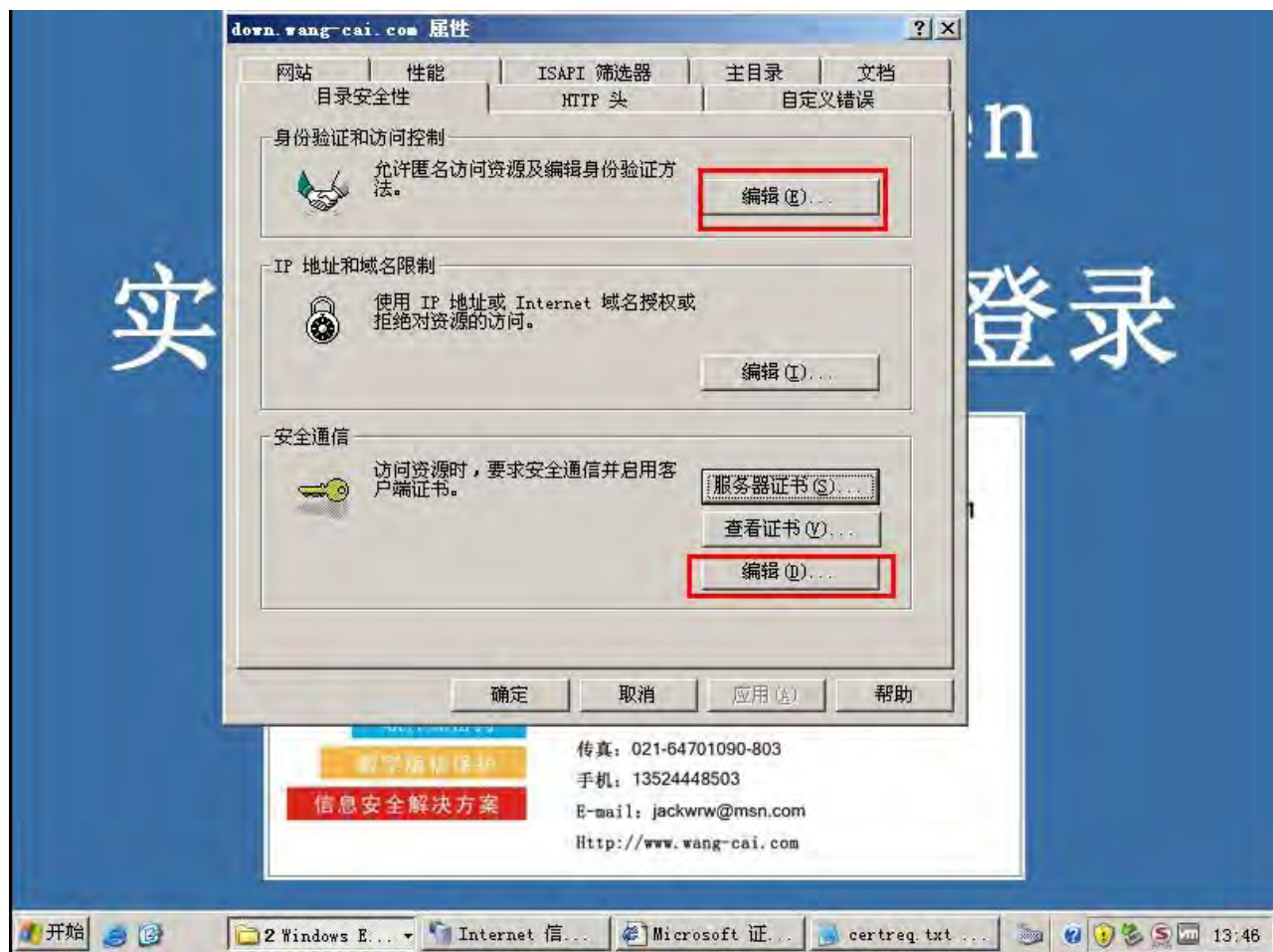


40、点击完成



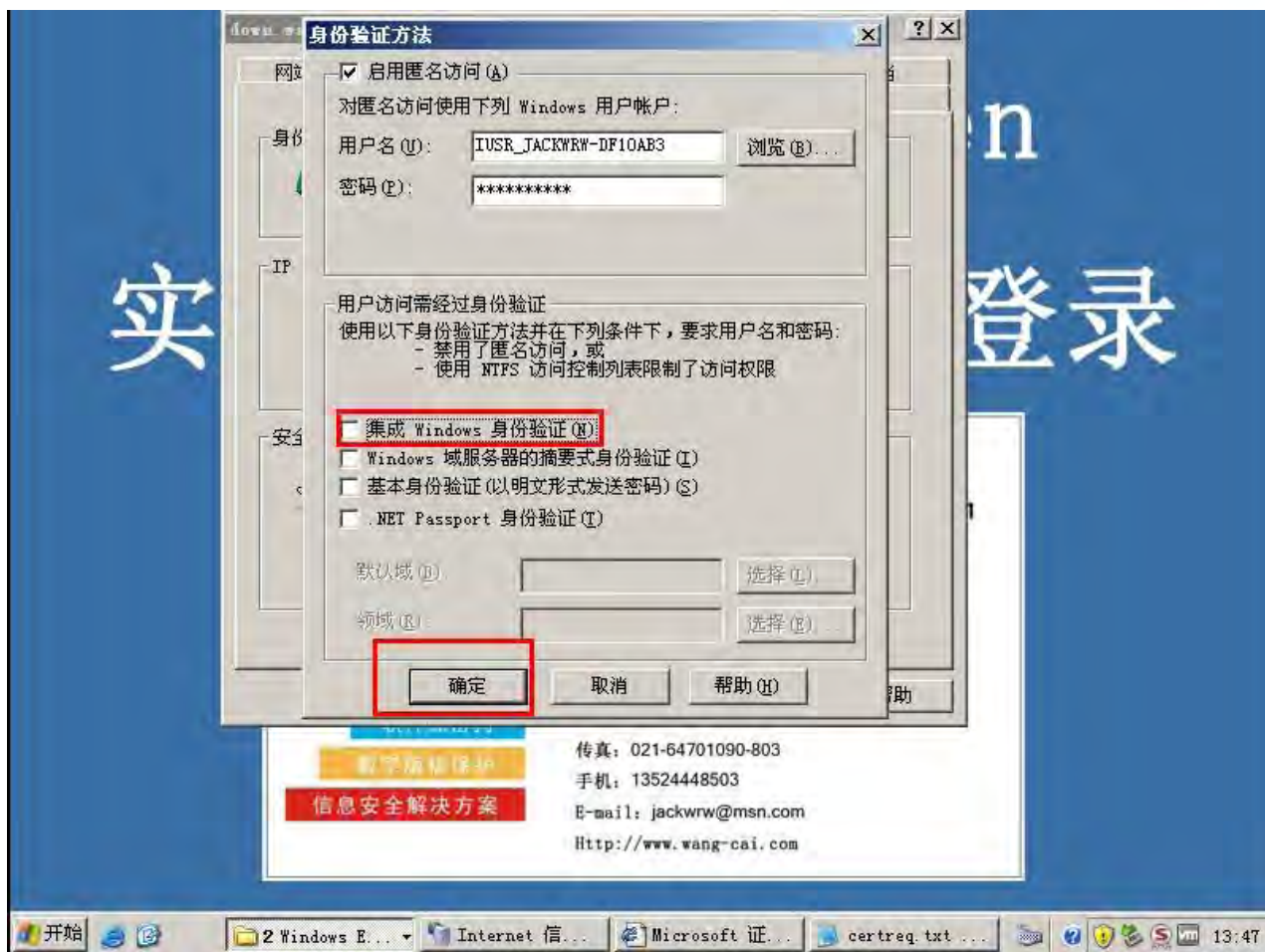


41、分别编辑身份验证和安全通信



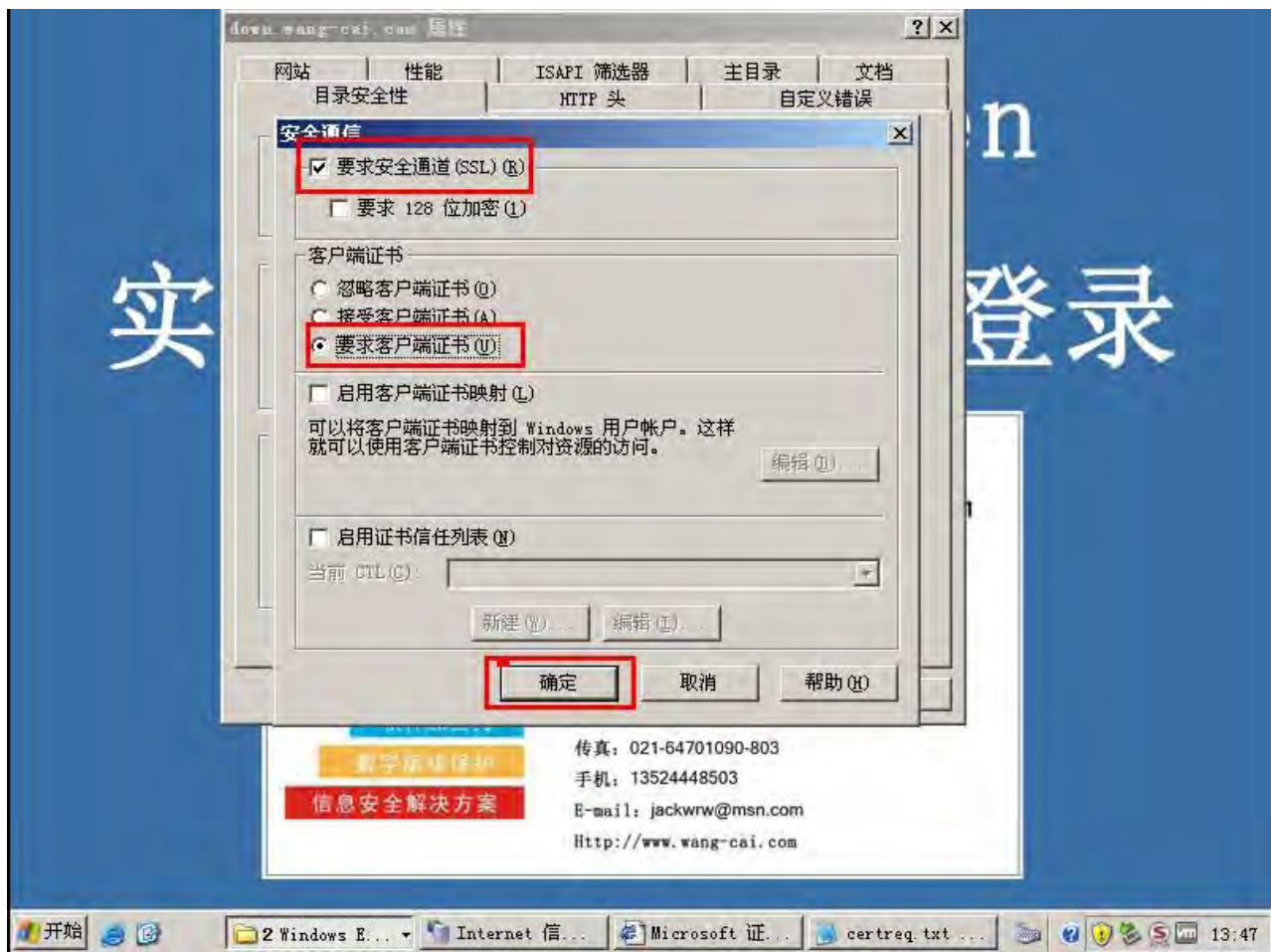


42、编辑身份验证：去掉集成windows身份验证前的勾选，点击确定



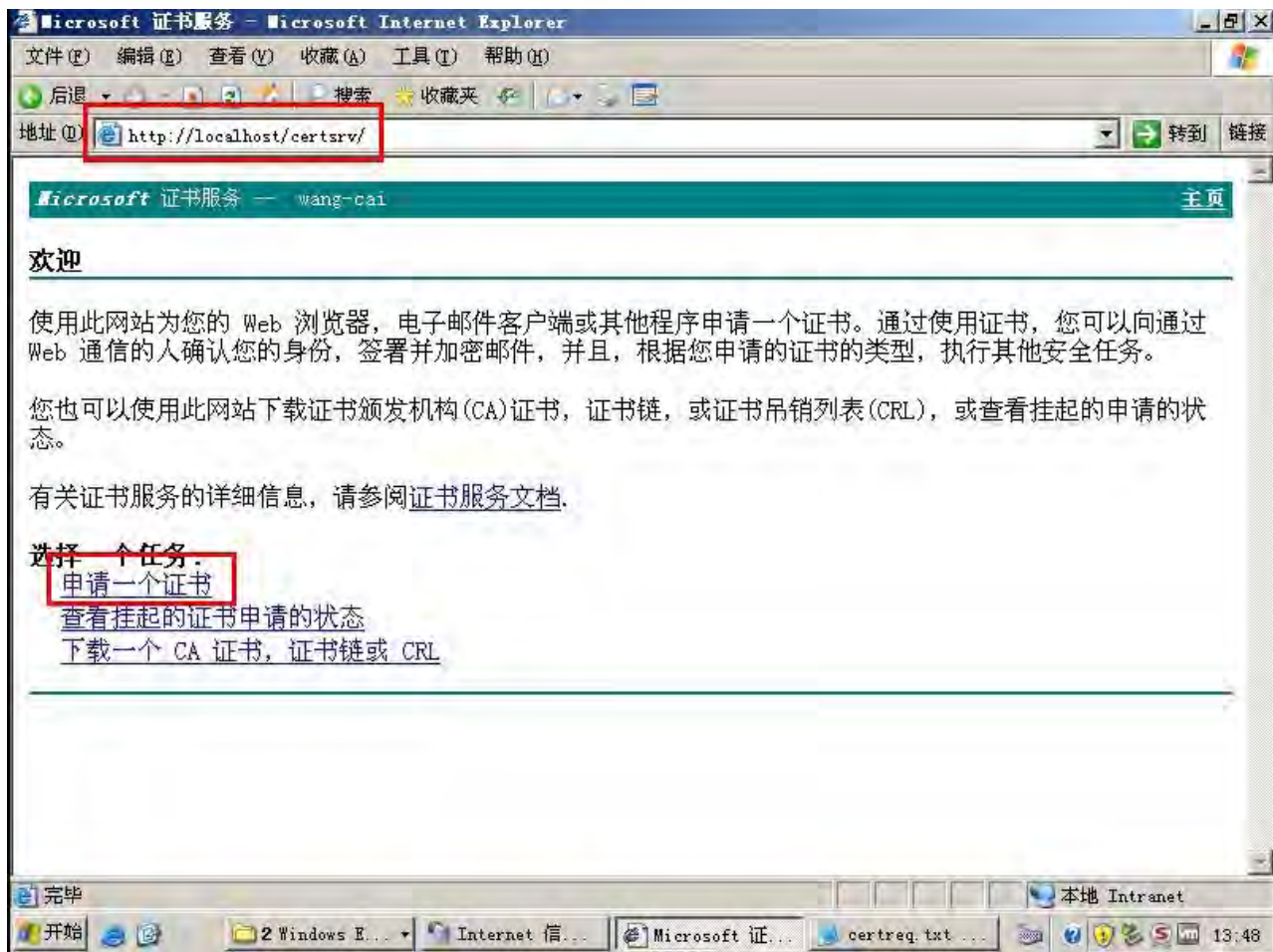


43、编辑安全通信：勾选要求安全通道和要求客户端证书



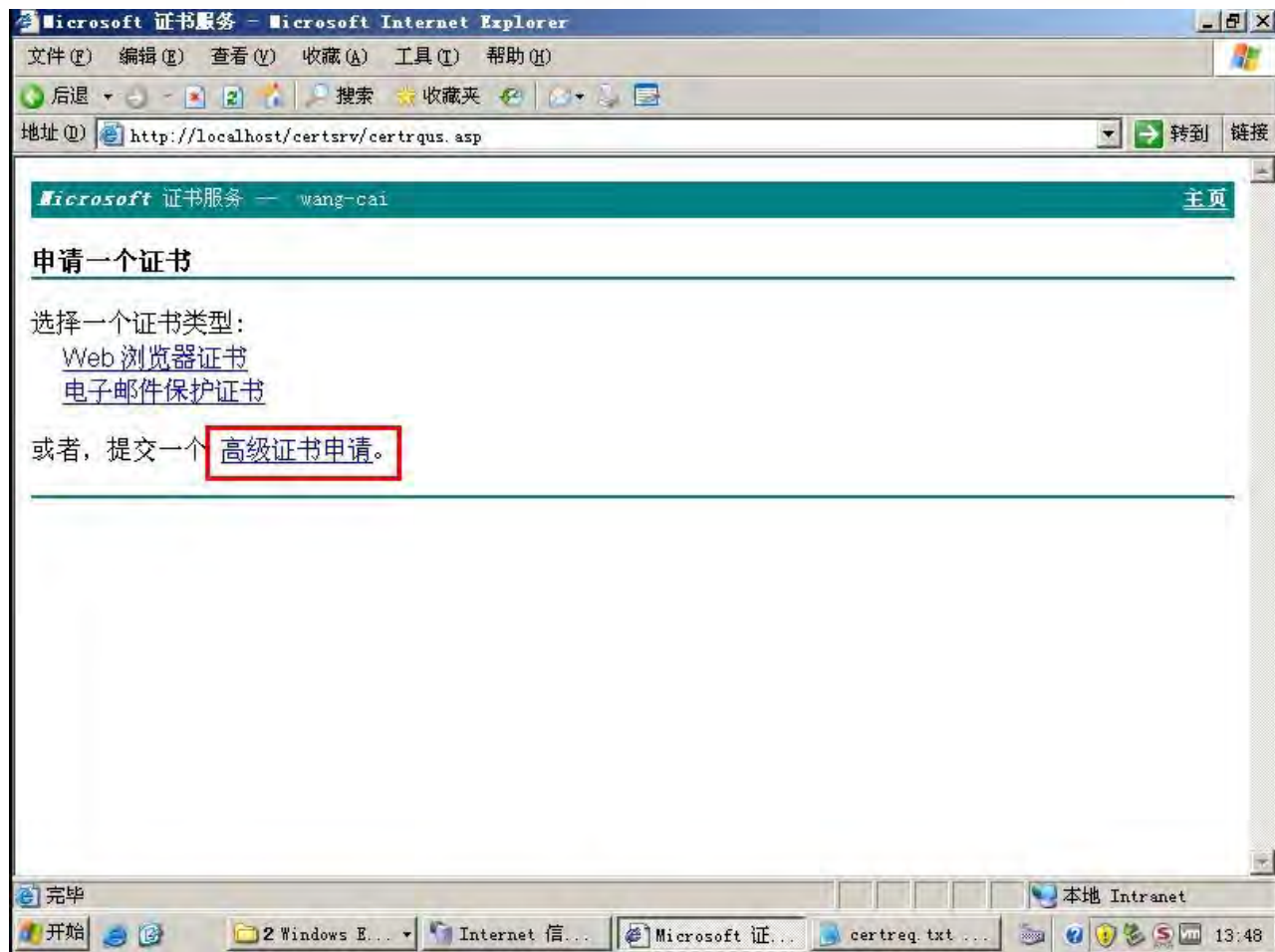


44、打开IE，访问<http://localhost/certsrv/> 选择申请一个证书



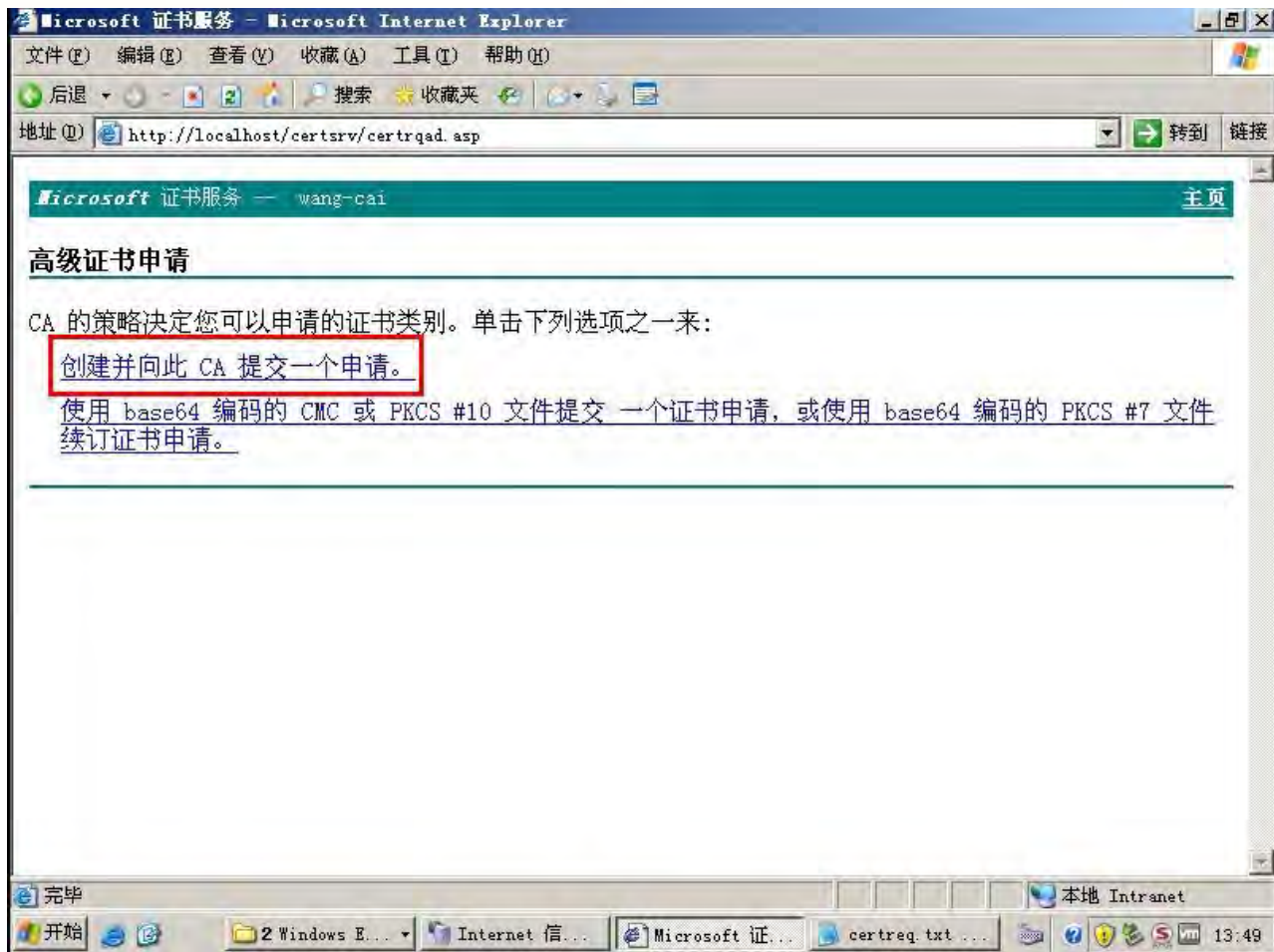


45、选择高级证书申请





46、选择创建并向此CA提交一个申请





47、填写个人信息，**CSP选择eToken**，点击提交

Microsoft 证书服务 - Microsoft Internet Explorer

文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)

后退 前进 停止 刷新 搜索 收藏夹 历史记录 地址栏

地址(1) http://localhost/certsrv/certrqma.asp 转到 链接

高级证书申请

识别信息:

姓名:	jackwrw
电子邮件:	jackwrw@msn.com
公司:	wangcai
部门:	IT
市/县:	ShangHai
省:	ShangHai
国家(地区):	CN

需要的证书类型:

客户端身份验证证书

密钥选项:

☒ 创建新密钥集 ☐ 使用现存的密钥集

CSP: eToken Base Cryptographic Provider

密钥用法: ☐ 交换 ☐ 签署 ☒ 两者

密钥大小: 1024 最小值: 1024 最大值: 2048 (一般密钥大小: 1024 2048)

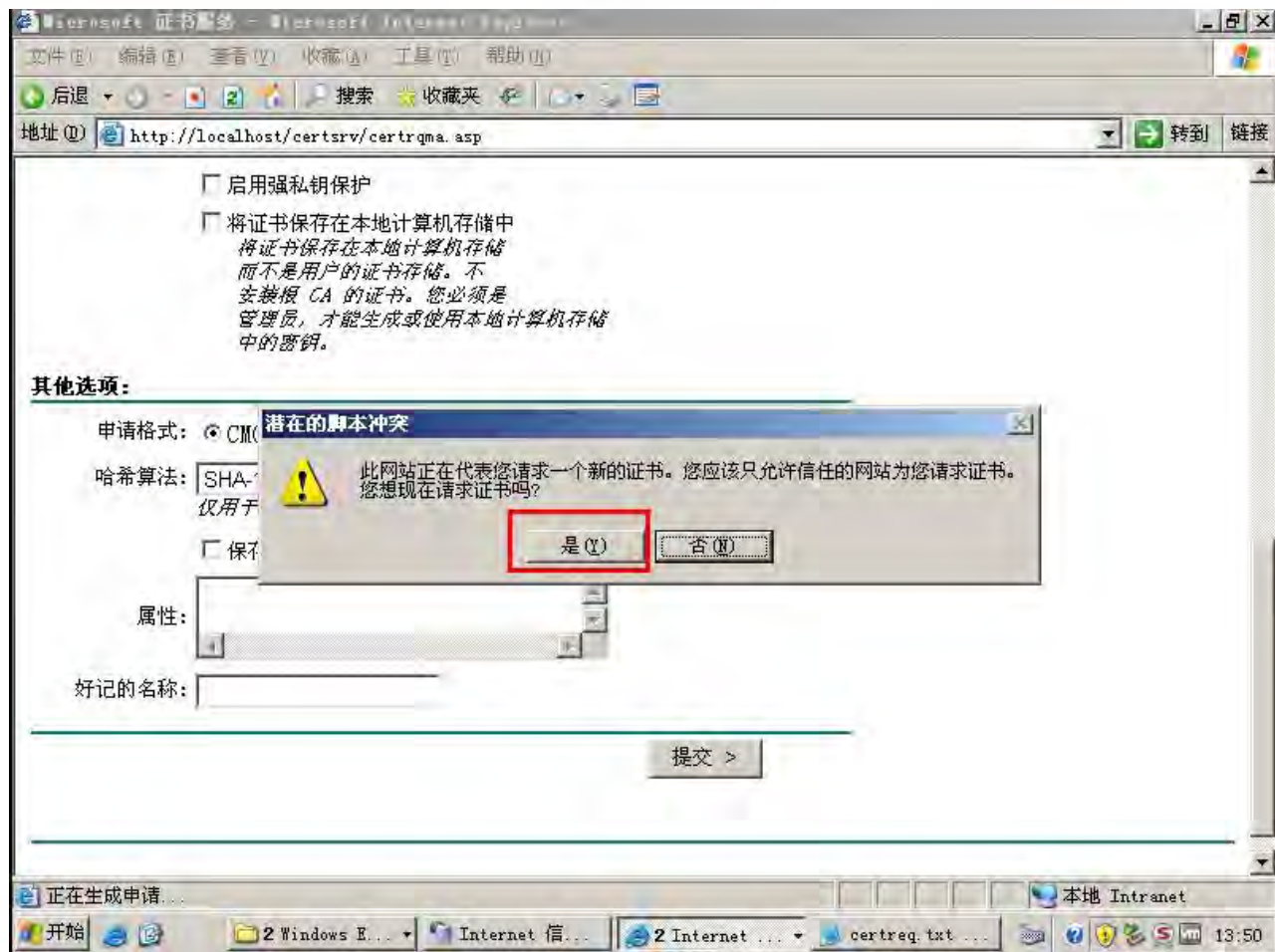
☒ 自动密钥管理 ☐ 用白名单的密钥管理策略

完毕

开始 2 Windows E... Internet 信... Microsoft 证... certreq.txt ... 本地 Intranet 13:49

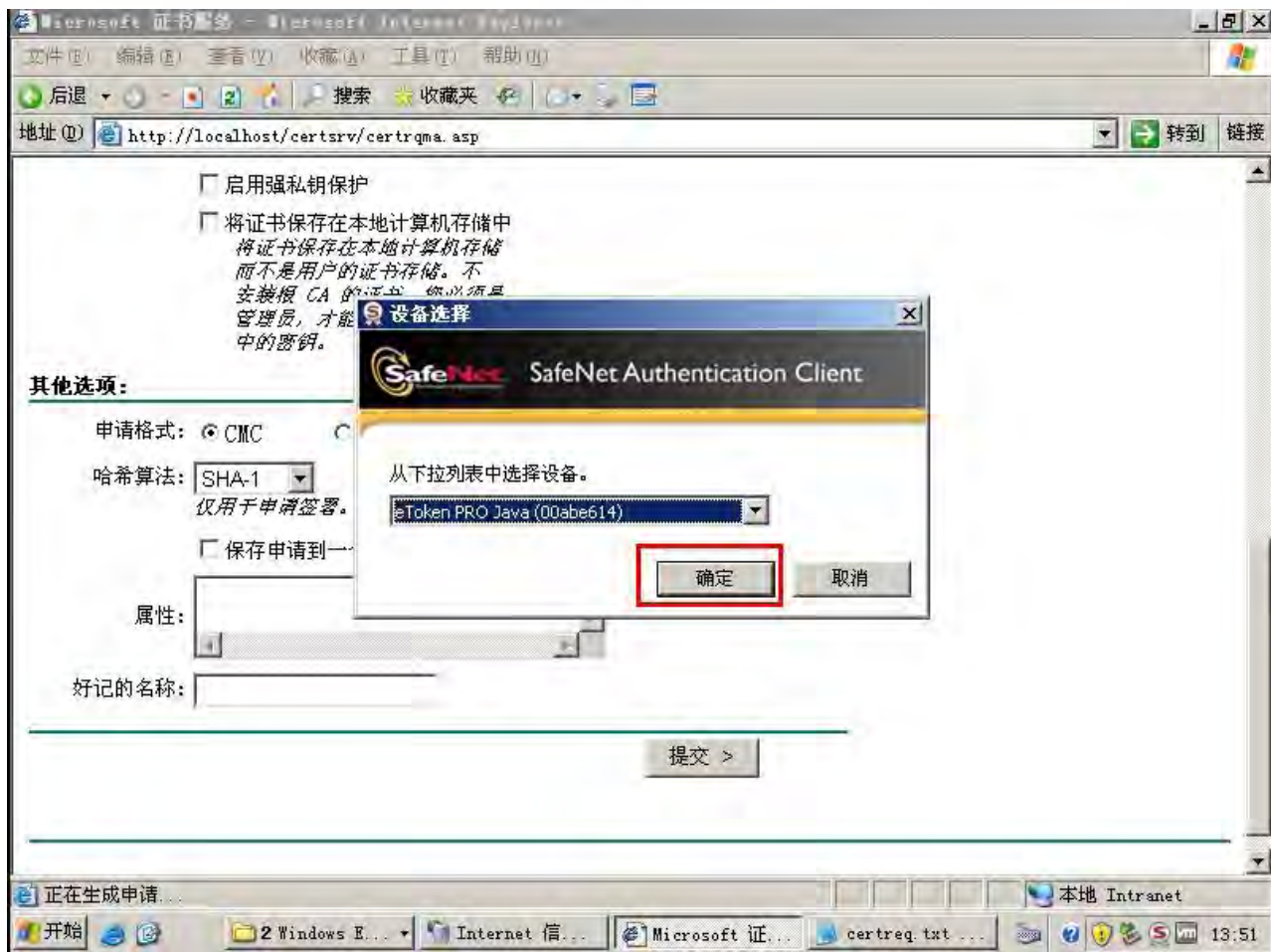


48、点击“是(Y)”





49、插入eToken硬件，并在页面中选择硬件



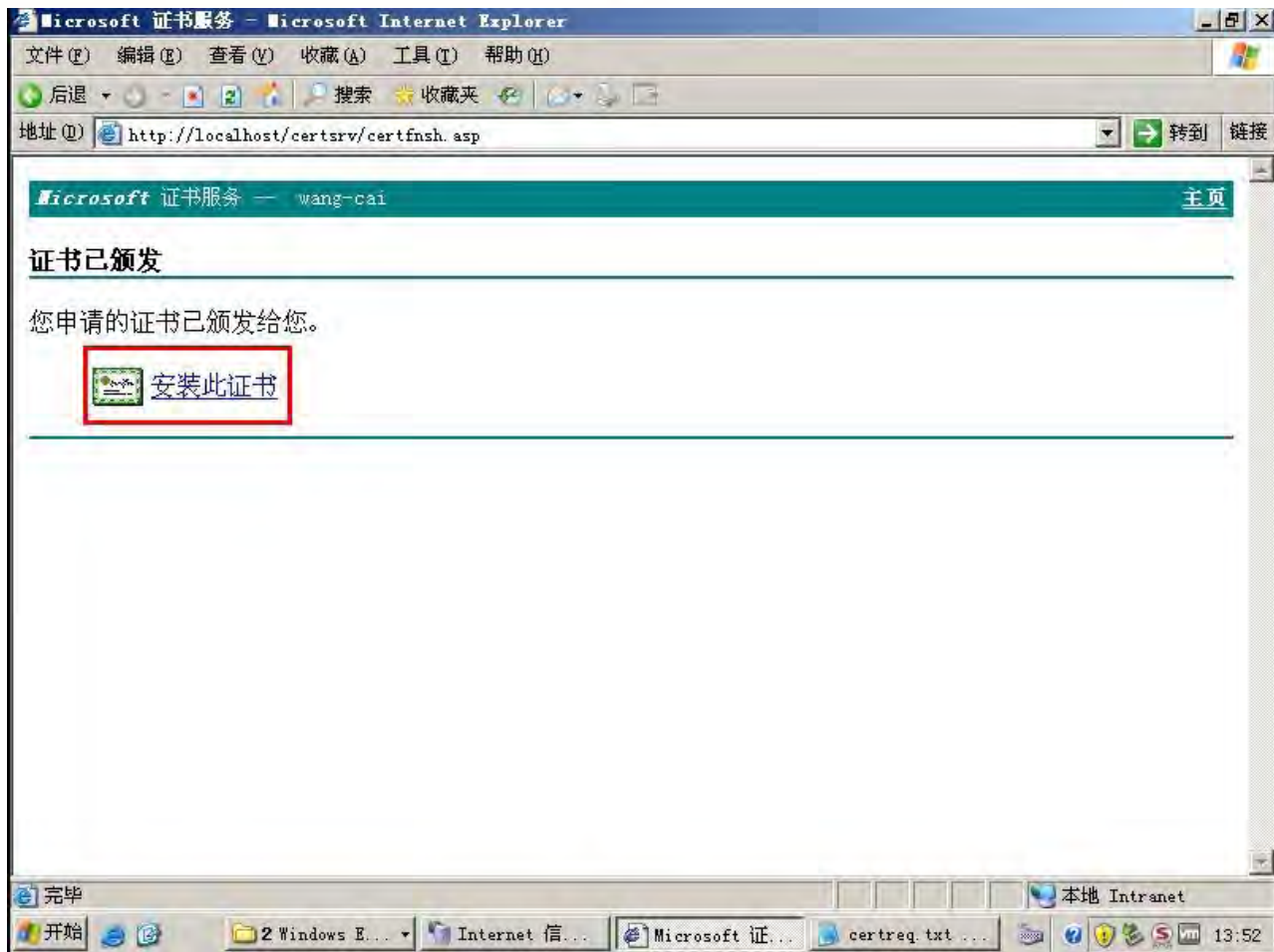


50、输入硬件密码，默认密码：1234567890，后面需要更改密码，请保证密码一定的安全级别，可参考：1qaz@WSX（更改密码不单独介绍）



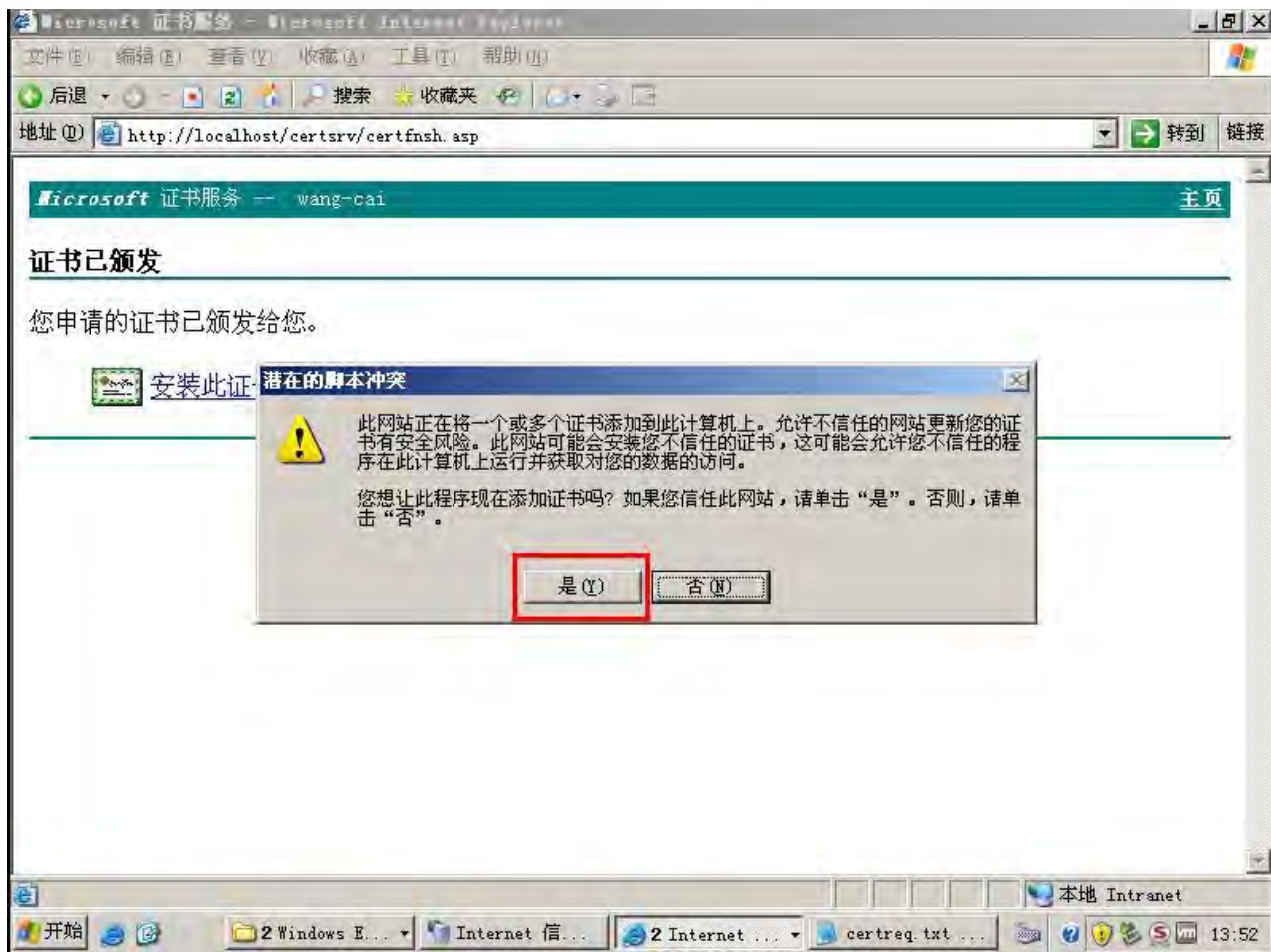


51、选择安装此证书



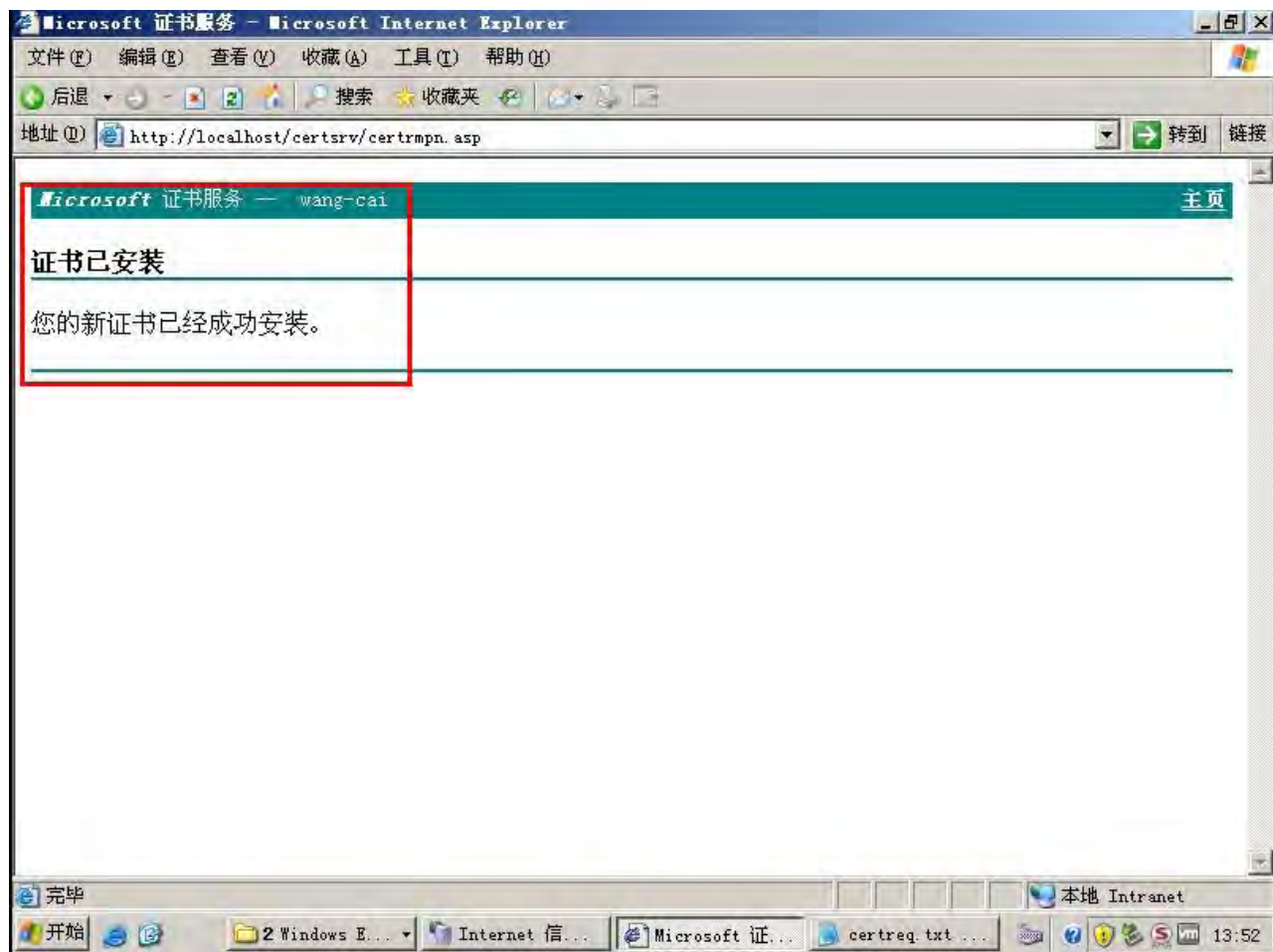


52、选择“是(Y)”开是安装证书





53、完成用户证书的申请和安装。





54、进行测试

- 到此为止，我们已经完成了站点的所有配置，以及为一个用户颁发CA证书。下面可以进行测试，检验是否存在问题。请注意：
- A、访问网址需要使用HTTPS，如<https://ca.wang-cai.com>
- B、网站代码中，关于页面跳转时，不可使用http://



谢谢！



软件加密狗

数字版权保护

信息安全解决方案

魏荣巍 信息安全顾问

QQ: 58424918

MSN: jackwrw@msn.com

上海旺财信息技术有限公司

地址: 上海市桂林路396号, 3号楼, 611室

电话: 021-54640133-805

传真: 021-64701090-803

手机: 13524448503

E-mail: jackwrw@msn.com

Http://www.wang-cai.com