IIS使用eToken 实现网站CA认证登录

信息安全顾问魏荣巍



2:5

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:

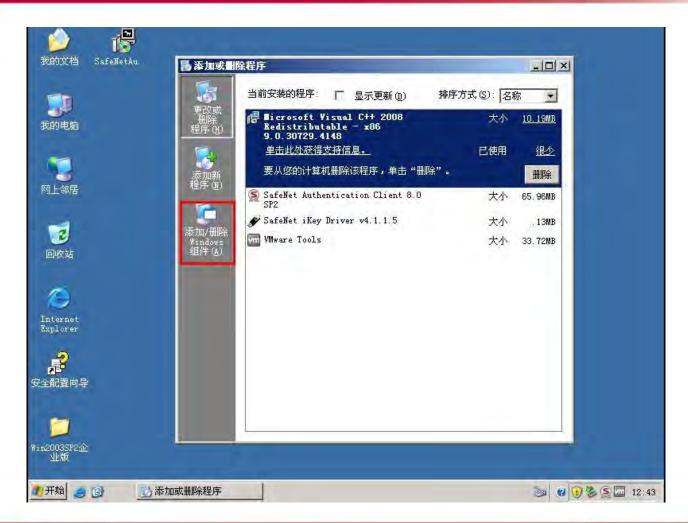
http://down.wang-cai.com

- 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。



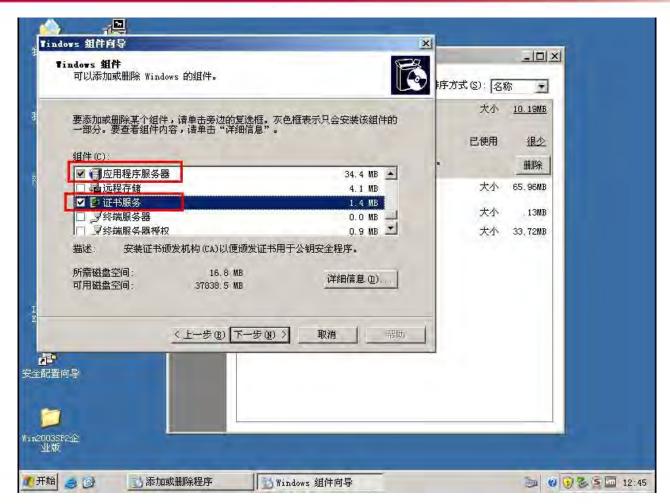


2、打开控制面板——添加删除程序——点击添加/删除Windows组件





3、在列表中选择应用程序服务器、证书服务。



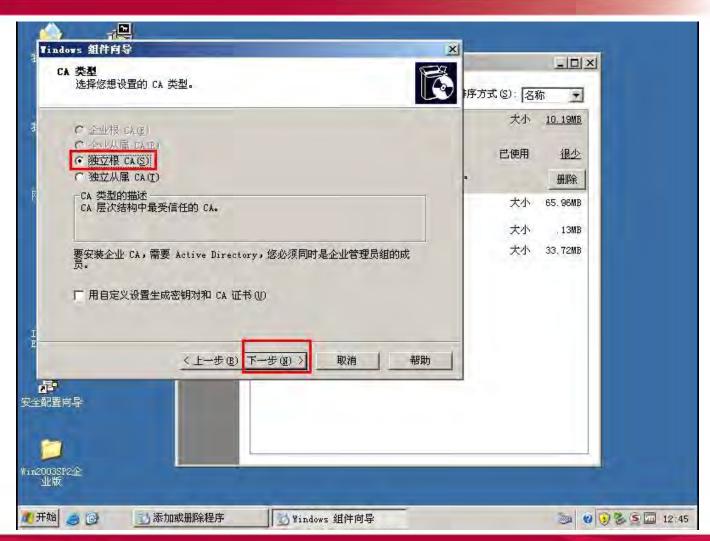


4、双击应用程序服务器,勾选ASP.NET,并确定





5、在安装证书服务过程中,选择独立根CA



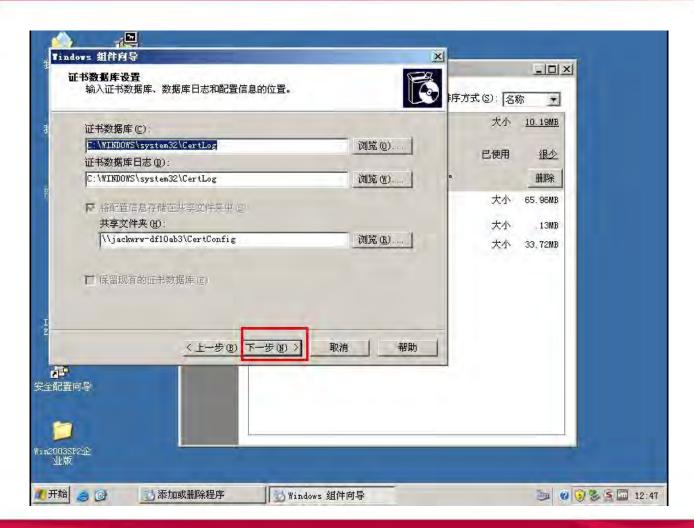


6、设定CA名称、年限

CA 识别信息 輸入识别该 CA 的信息。	3	_ID×
HEID C STOUGH CK HOIGHAS	・	名称 🔻
此 ex 的公用名 称 @):	大小	10.19MB
wangcai	已使用	很少
可分辨名称后缀 (0):	Litter	
	4.1	删除
 可分辨名称的预览 (2):	大小	
CN-wang-cai	大小	100.00
	大小	33,72MB
有效期限立): 截止日期: 50		
〈上一步(8) 下一步(9) 〉 取消 帮助		
 		
\$P2企 (

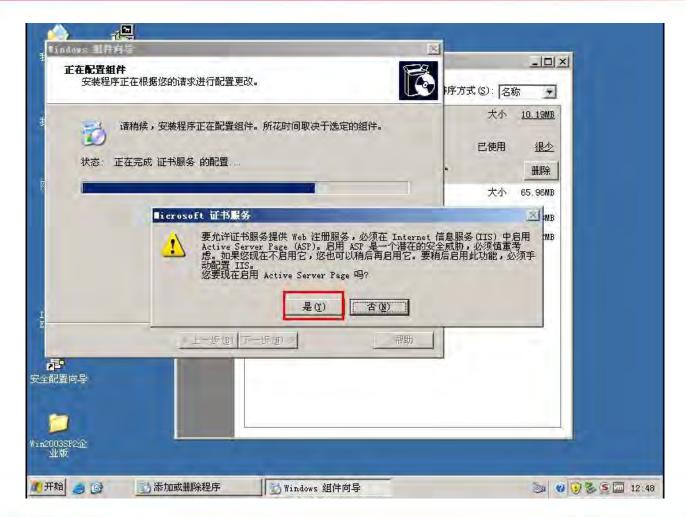


7、设定证书数据库设置(建议使用默认)





8、安装证书服务过程中,启用ASP





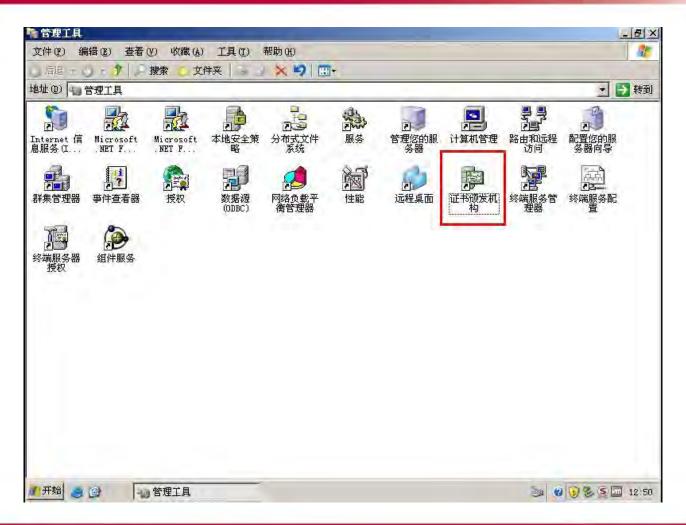


9、完成IIS和证书服务的安装



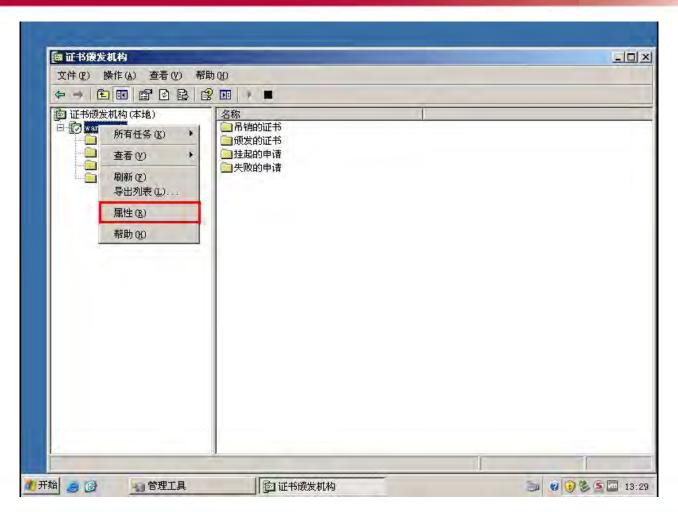


10、在控制面板——管理工具中,打开证书颁发机构



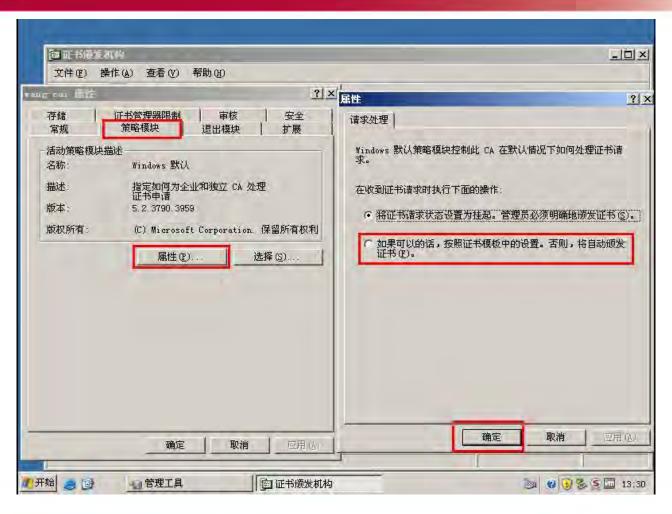


11、在证书机构上点击右键——属性



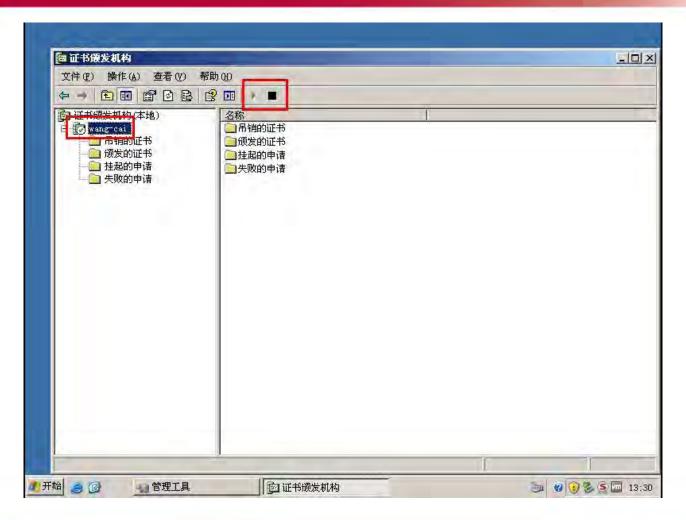


12、选择策略模块——属性,选择自动颁发证书。 (也可以使用手动颁发方式,此处不做单独讲解)





13、点击按钮,重新启动证书服务











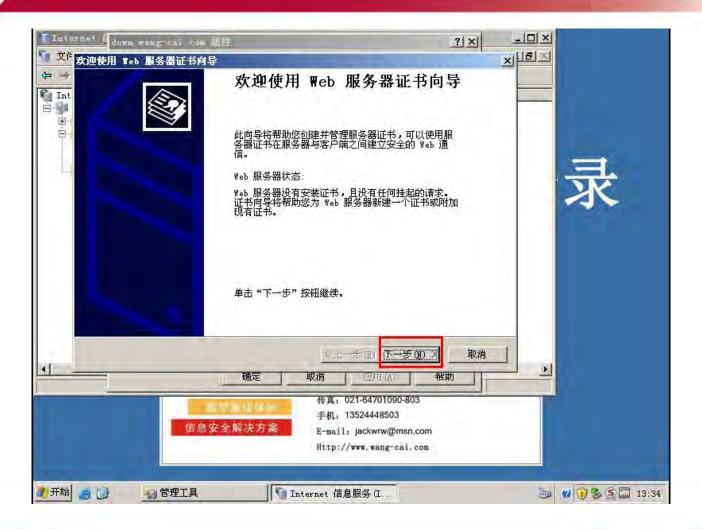
15、选择目标站点,右键——属性





16、在目录安全性中,选择服务器证书

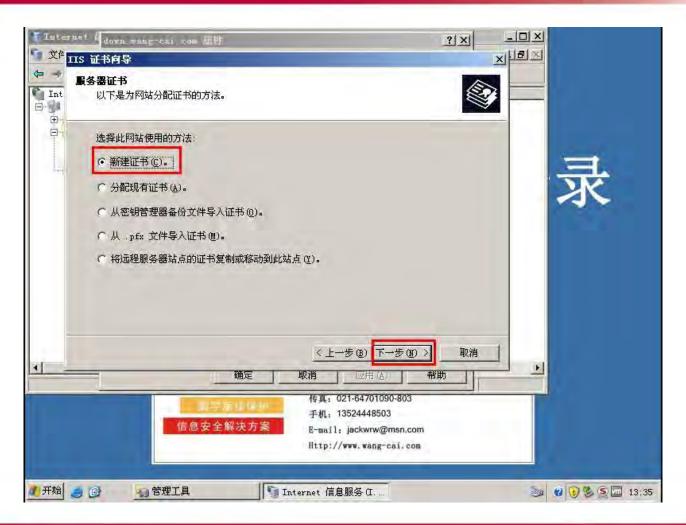






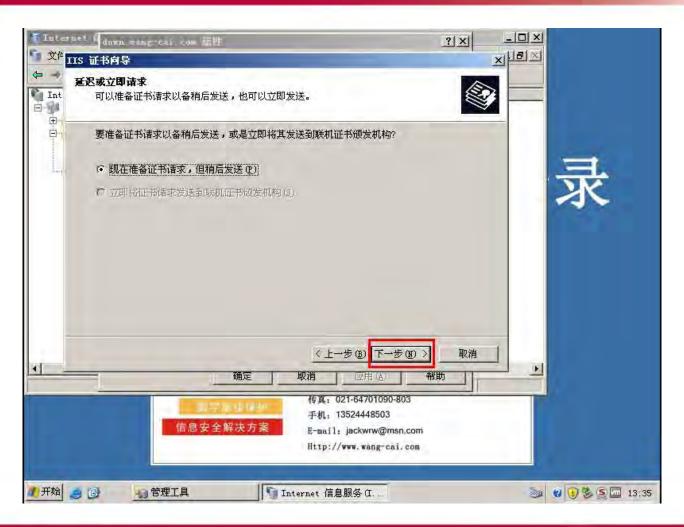


18、选择新建证书,点击下一步



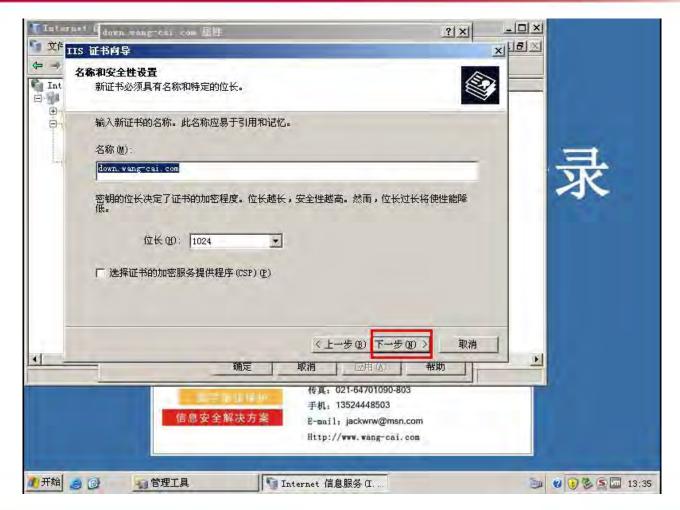








20、点击下一步

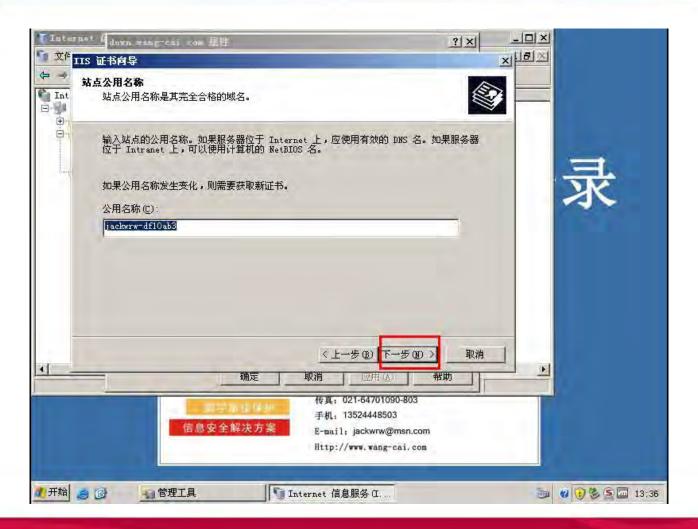




21、设定单位名称和部门,点击下一步

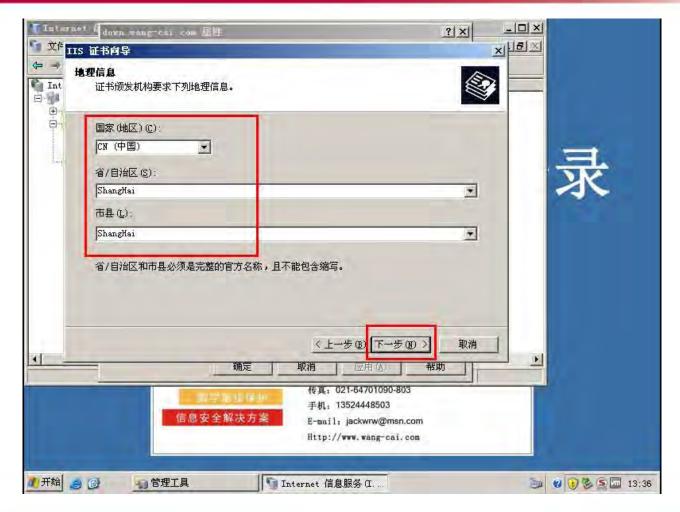








23、设定地理信息,点击下一步





24、保存证书请求文件(建议默认),点击下一步







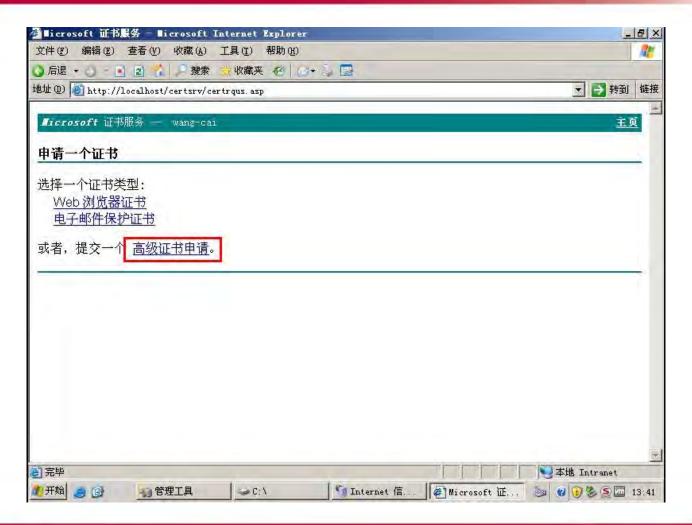


26、打开IE,访问http://localhost/certsrv点击申请一个证书



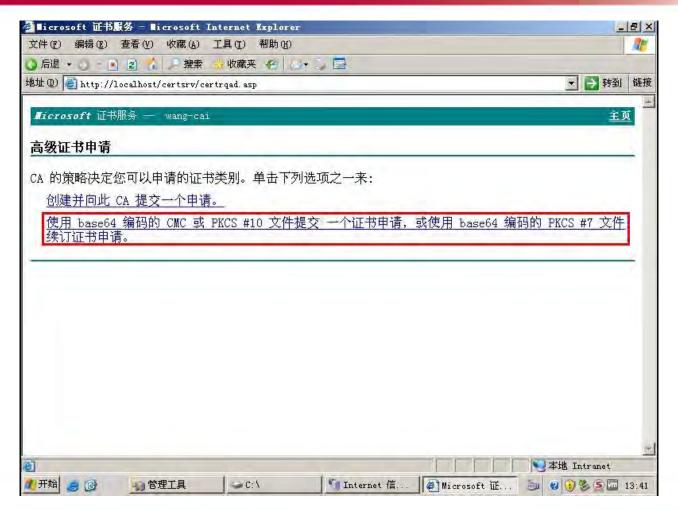


27、选择高级证书申请



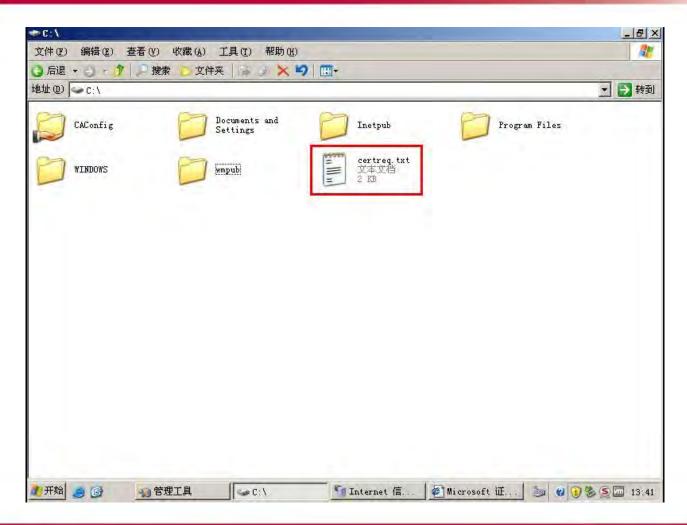


28、选择续订证书申请



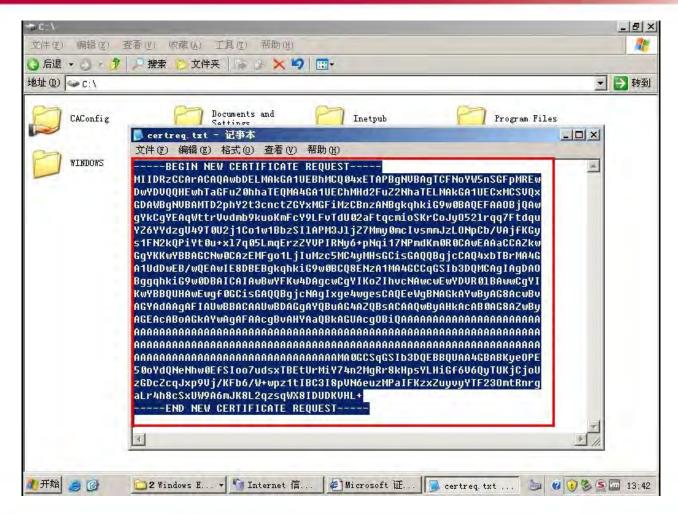


29、打开第24步骤中保存的TXT文件,



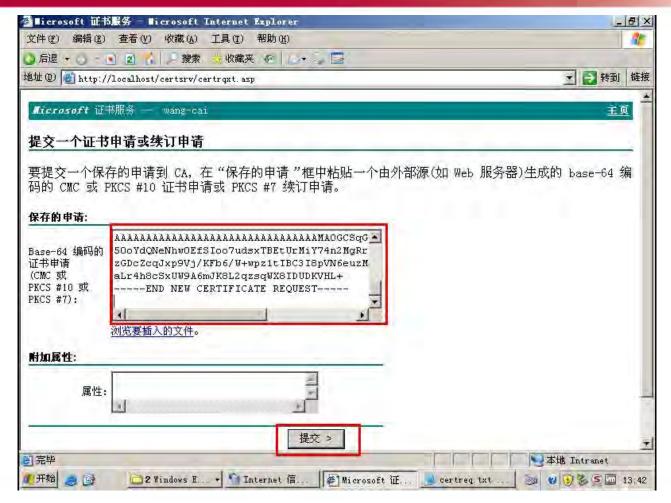


30、全选TXT里的文字,并复制





31、将文字粘贴到IE中,点提交





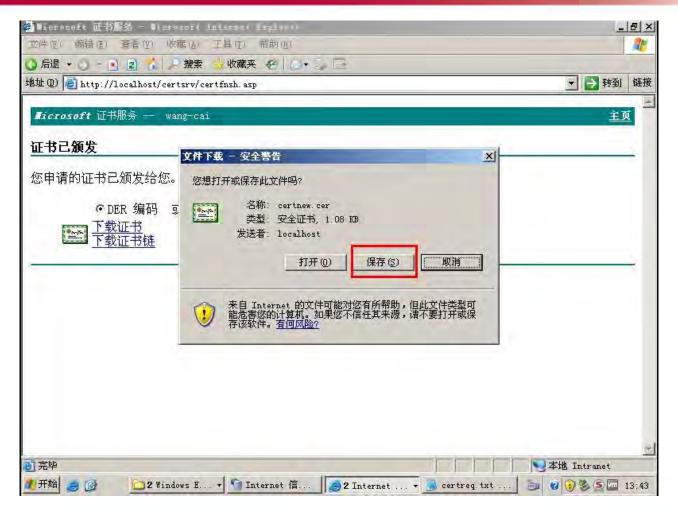


32、点击下载证书



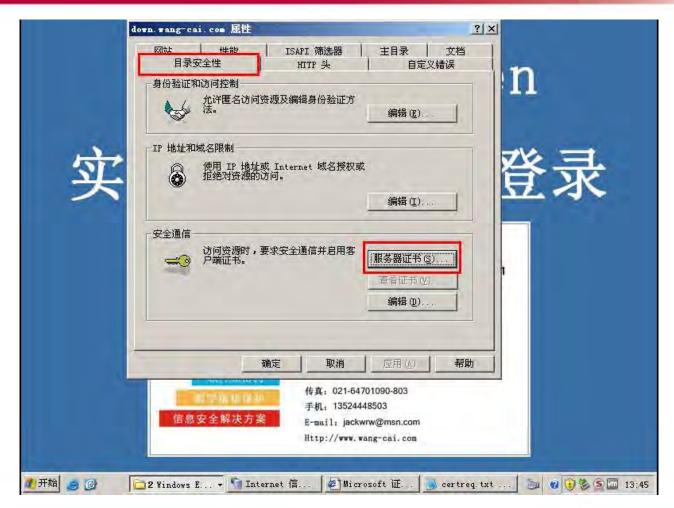


33、保存证书

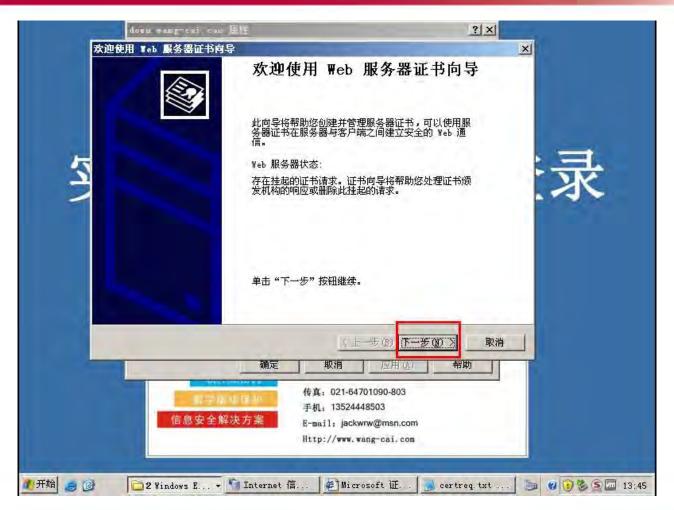




34、在站点属性中,再次点击服务器证书







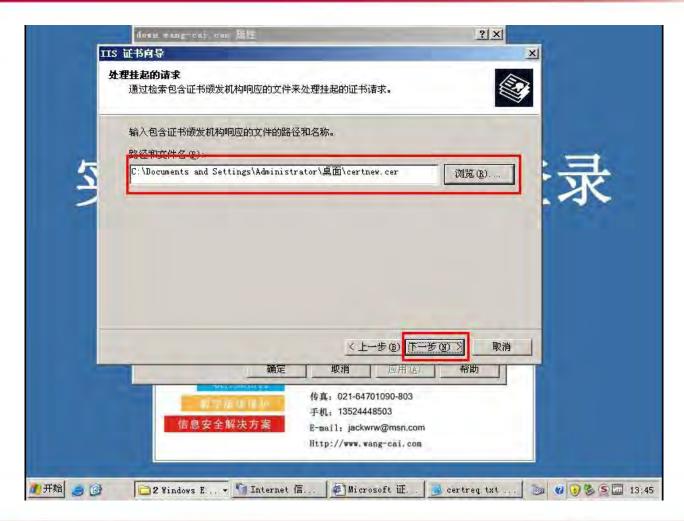


36、选择处理挂起的请求并安装证书,点击下一步





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

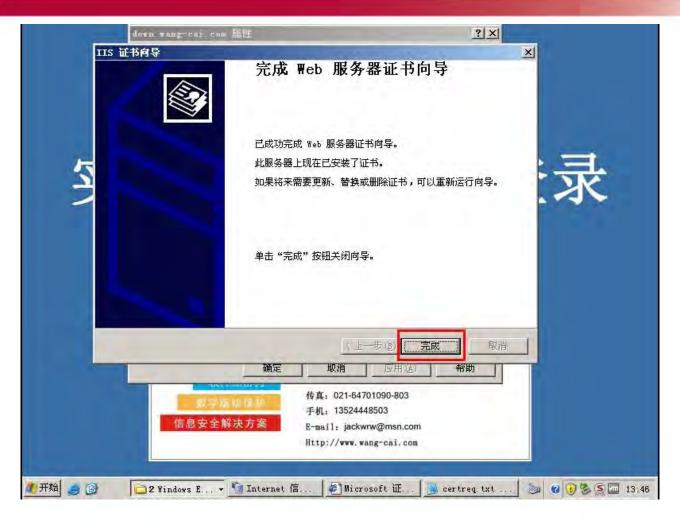






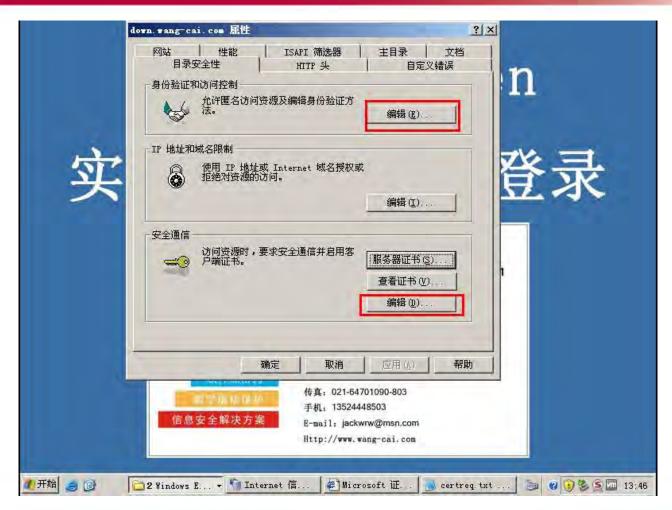






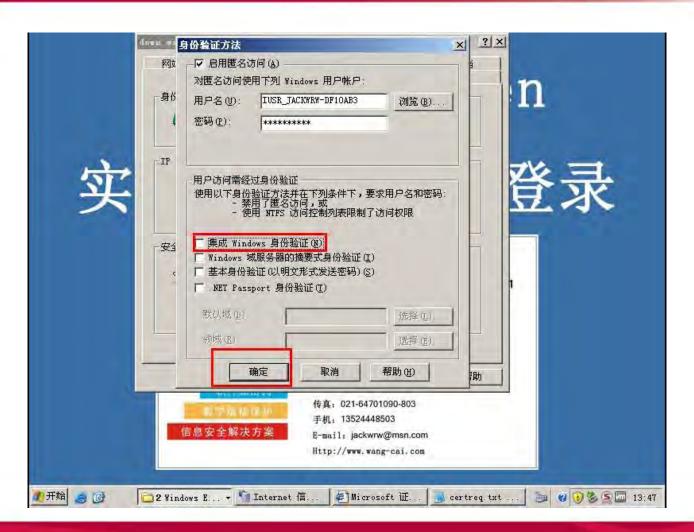


41、分别编辑身份验证和安全通信



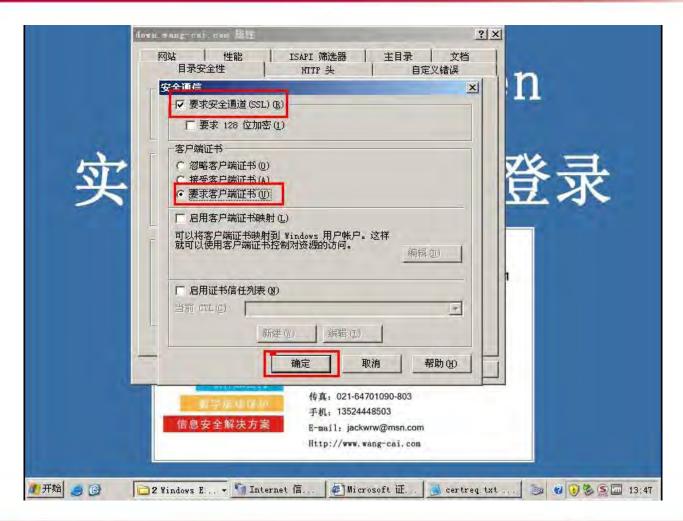


42、编辑身份验证:去掉集成windows身份验证前的勾选,点击确定





43、编辑安全通信: 勾选要求安全通道和要求客户端证书



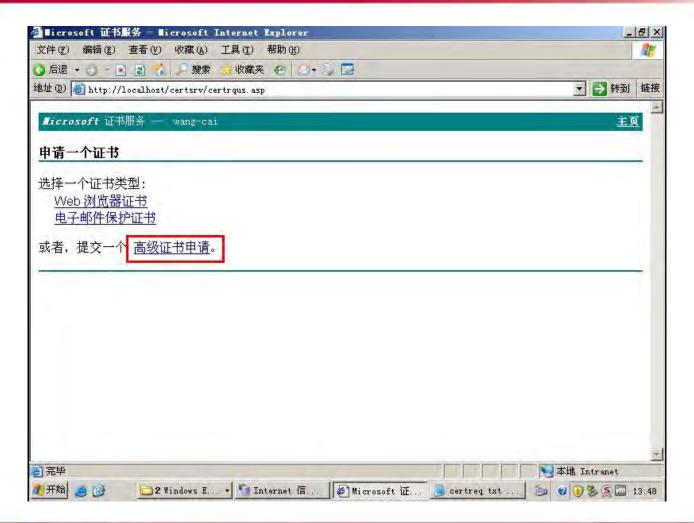


44、打开IE,访问<u>http://localhost/certsrv</u> 选择申请一个证书



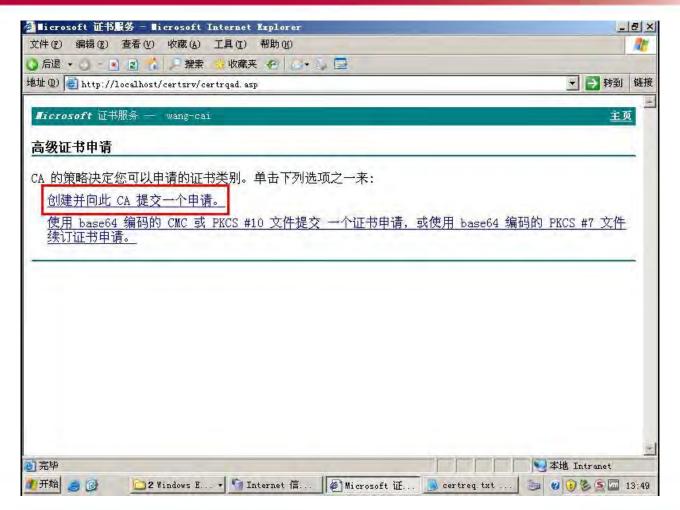


45、选择高级证书申请





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

■icrosoft 证書	形服务 - Wicrosoft Internet Explorer	_ 5 ×
文件(图) 编辑(图)) 查看·(Y) 收藏·(A) 工具·(T) 帮助·(H)	1
③ 后退 ▼ () - [■ ② 🏌 🖟 搜索 🖐 收藏夹 🚱 🕒	
地址 (D) 🐻 http://	//localhost/certsrv/certrqma.asp	▼ ▶ 转到 链接
高级证书申请		
识别信 <mark>息:</mark>		19
姓名:	: jackwrw	
电子邮件:	ijackwrw@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	
CSP:	eToken Base Cryptographic Provider	
密钥用法:	· ○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○	
密钥大小:	1 024 最小值:1024 (一般密钥大小: 1024 2048)	
	6. 台升家和家里友称	
完毕		■ 本地 Intranet
一开始 🥭 📵	[2 Windows E → M Internet 信 Microsoft 证 d certreq. txt	🧓 🕡 🐧 🕏 🔚 13:49





□ 上	□ All 中 □ □ Plane All Note of the property o	1
bù ⑫ ► http://localhost/certsrv/certrqma.asp □ 启用强私钥保护 □ 将证书保存在本地计算机存储中 将证书保存在本地计算机存储 耐不是用户的证书存储。不 安装假 CA 的证书。您必须是 管理员,才能生成或使用本始计算机存储 中的密钥。 其他选项: □ 申请格式: ⓒ CM (潜在的脚本冲突 □ 哈希算法: SHA- 仅用于 □ 保不 是 ⑫ 查 ⑫ 查 ⑫ 查 ⑫ 查 ⑫ 查 ⑫ 是 ⑫ 查 ⑫ 查 ⑫ 查 ⑫	■ http://localhost/certsrv/certrqma.asp □ 启用强私钥保护 □ 将证书保存在本地计算机存储中 将证书保存在本地计算机存储 而不是用户的证书存储。不 安装根 CA 的证书。您必须是 管理员,才能生成或使用本地计算机存储 中的密钥。	
□ 启用强私钥保护 □ 将证书保存在本地计算机存储中 将证书保存在本地计算机存储	一 启用强私钥保护 一 将证书保存在本地计算机存储中 将证书保存在本地计算机存储 而不是用户的证书存储。不 安装根 CA 的证书。您必须是 管理员,才能生成或使用本地计算机存储 中的密钥。	The second secon
将证书保存在本地计算机存储	□ 将证书保存在本地计算机存储中 将证书保存在本始计算机存储 而不是用户的证书存储。不 安装根 CA 的证书。您必须是 管理员,才能生成或使用本始计算机存储 中的密钥。	转到 链
将证书保存在本始计算机存储 而不是用户的证书存储。不 安装银 CA 的证书。您必须是 管理员,才能生成或使用本始计算机存储 中的密钥。 申请格式: ◆ CM(将证书保存在本地计算机存储 而不是用户的证书存储。不 安装根 CA 的证书。您必须是 管理员,才能生成或使用本地计算机存储 中的密钥。	
申请格式: © CMC 潜在的身本冲突 哈希算法: SHA-		
属性:	申请格式: © CMC 潜在的原本冲突 哈希算法: SHA- 《次用子 《您想现在请求证书吗?	
好记的名称:		
A SECOND CONTRACTOR OF THE CON	好记的名称:	
提交>	提交>	



49、插入eToken硬件,并在页面中选择硬件

」后退 ▼	▼ ▶ 转到 链接
□ 启用强私钥保护 □ 将证书保存在本地计算机存储中将证书保存在本地计算机存储 而不是用户的证书存储。不安装很 CA 的证书 你必须是管理员,才能中的密钥。 其他选项: □ SafeNet Authentication Client	¥7.5U NC.1
申请格式:	
提交 >	■ 本地 Intranet

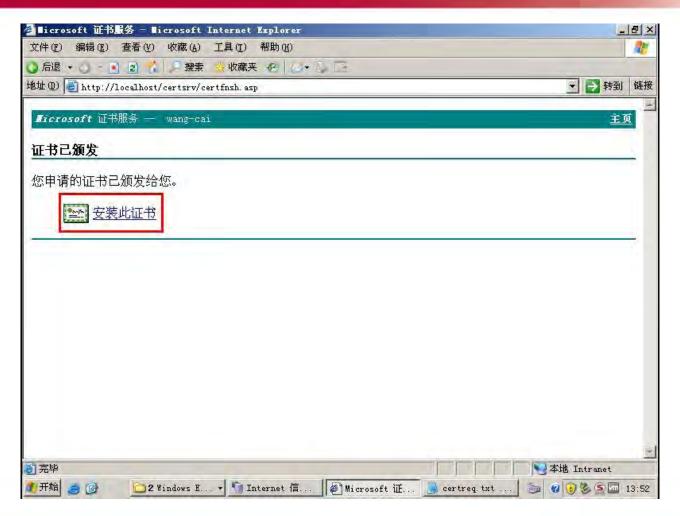


50、输入硬件密码,默认密码: 1234567890,后面需要更改密码,请保证密码一定的安全级别,可参考: 1qaz@WSX(更改密码不单独介绍)

	.host/certsrv/certrqma.asj)	▼ → 转到
	用强私钥保护 F证书保存在本地计算机存	储中	
	貝设备登录		×
	SafeMet SafeN	let Authentication Client	
他选项:			
申请格式: ⊙ С	输入设备 密码。		
哈希算法: SHA	设备名称:	eToken PRO Java	
仅用	设备 密码:	******	
口作		当前语言: CH	
属性:			
周1生:		确定	取消
好记的名称:			
12 - 12 - 12 - 12 - 12 - 12 - 12 - 12 -			
		提交 >	

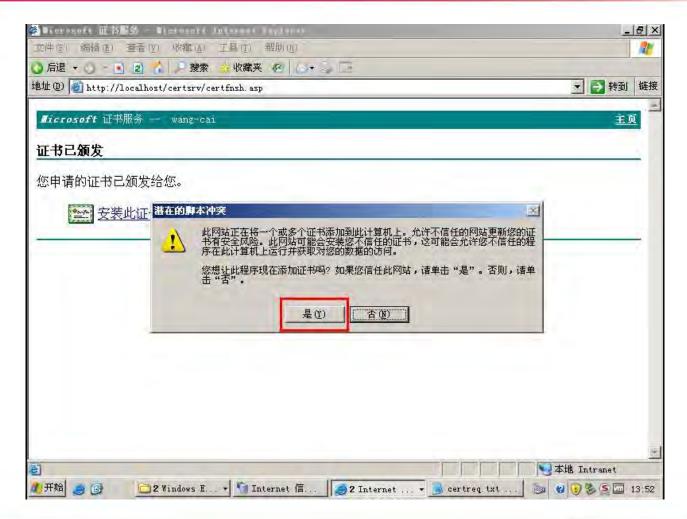


51、选择安装此证书





52、选择"是(Y)"开是安装证书





53、完成用户证书的申请和安装。

Bicrosoft 证书服务 - Bicrosoft Internet Explorer	_16
工件(P) 编辑(E) 查看(Y) 收藏(A) 工具(T) 帮助(H)	A
)后退 ▼ ○ ▼ ② 👔 🔭 / / / / / / / / / / / / / / / / / /	=1 ==
址① @ http://localhost/certsrv/certrmpn.asp	▼ → 转到 報
Microsoft 证书服务 — wang-cai	主页
正书已安装	
您的新证书已经成功安装。	
完毕	■本地 Intranet



- 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!

