NETCA IIS CNG使用手册

# 1、简介

NETCA IIS CNG是广东省电子商务认证有限公司（简称：NETCA）实现的一个专用于IIS服务器的CNG提供者，用于提供实现IIS的TLS协议中的私钥操作。NETCA IIS CNG的名称为NETCA CNG Provider For IIS。其支持TLS中的RSA解密、RSA签名和ECDSA签名等算法。

NETCA IIS CNG可以在IIS 7以上的版本使用。

本文主要介绍如何在IIS中配置使用NETCA IIS CNG。

# 2、NETCA IIS CNG的使用说明

## 2.1 概述

要配置IIS使用NETCA IIS CNG主要有有以下步骤：

1. 申请NETCA的证书，其私钥可以通过NETCA中间件来访问
2. 在IIS中配置证书
3. 配置相关的TLS选项

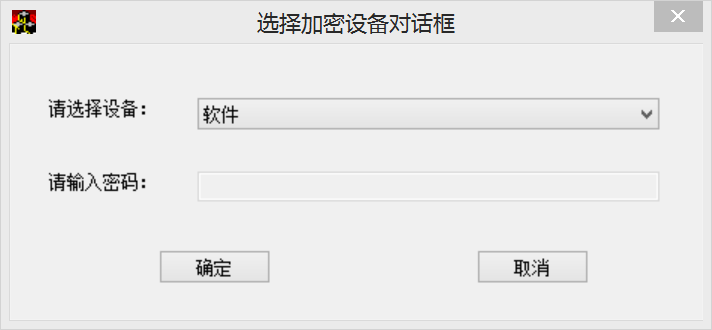
本文以IIS 7为例进行介绍。

## 2.2 申请证书

要配置IIS使用TLS协议首先需要申请服务器证书。要使用NETCA IIS CNG则证书是要求通过NETCA中间件访问私钥的，而不是使用微软自带的CSP/CNG来访问私钥的。下面以得安加密机申请RSA证书为例进行说明，具体步骤如下：

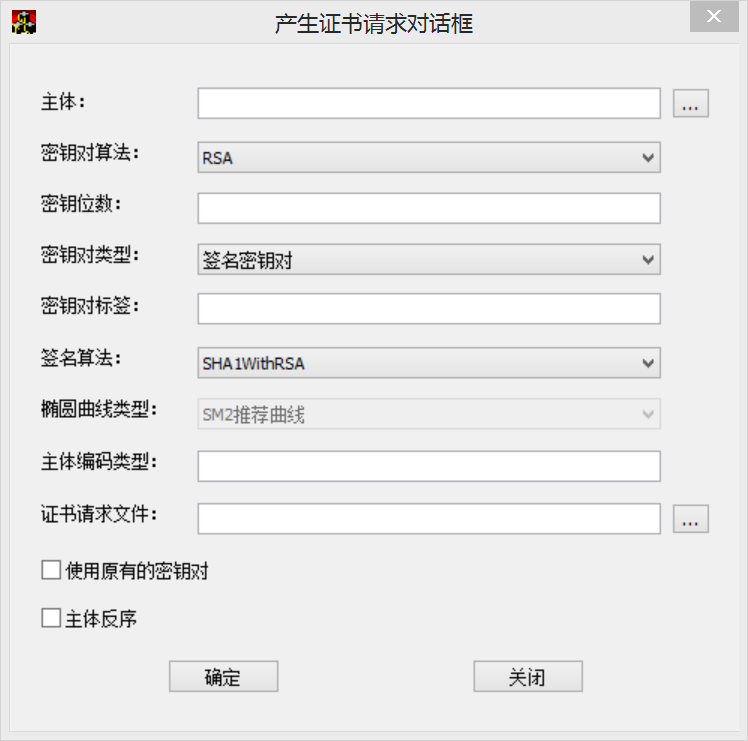
1. 安装NETCA中间件，可以使用安装包，也可以手工安装。手工安装参见《NETCA PKI API Cookbook》相关说明
2. 安装得安加密机的设备DLL，并进行相关配置。参见《NETCA PKI API Cookbook》相关说明。至此，应该能够通过NETCA中间件来访问得安加密机了。
3. 使用CryptoTestTool产生证书请求。

首先连接加密机，点击菜单，“开始”->”连接…”，弹出“选择加密设备对话框”，如下图所示。



在“请选择设备：”右边的下拉框，选择得安ECC加密机。然后，在“请输入密码：”右边的密码输入框，输入加密机的密码，点击“确定”按钮完成连接加密机的操作。

接着产生证书请求，点击菜单，“操作”->”产生证书请求…”，弹出“产生证书请求对话框”，入下图所示：



首先，要勾选”使用原有的密钥对“，在主体项中输入类似C=CN,CN=www.test.com的名称。密钥对类型选择“加密密钥对”。密钥对标签输入RSA\_n，其中n为密钥对号，比如，第3对RSA密钥对，输入RSA\_3，要确保密钥对存在，否则产生证书请求会失败。可以通过“操作”->“设备信息”来看到当前加密机的所有密钥对信息。签名算法根据不同CA的要求来选择，通常优先选择SHA256WithRSA，但是有些CA仅仅支持SHA1WithRSA，这时只能选择SHA1WithRSA。总之，如果有疑问，请咨询CA。证书请求文件填入保存产生的证书请求文件名。点击“确定”按钮，成功后，证书请求保存到填入的证书请求文件中。

1. 提交3产生的证书请求给CA，CA签出服务器证书。如何通过申请证书，请咨询CA。
2. 获得CA签发的证书。

## 2.3安装证书

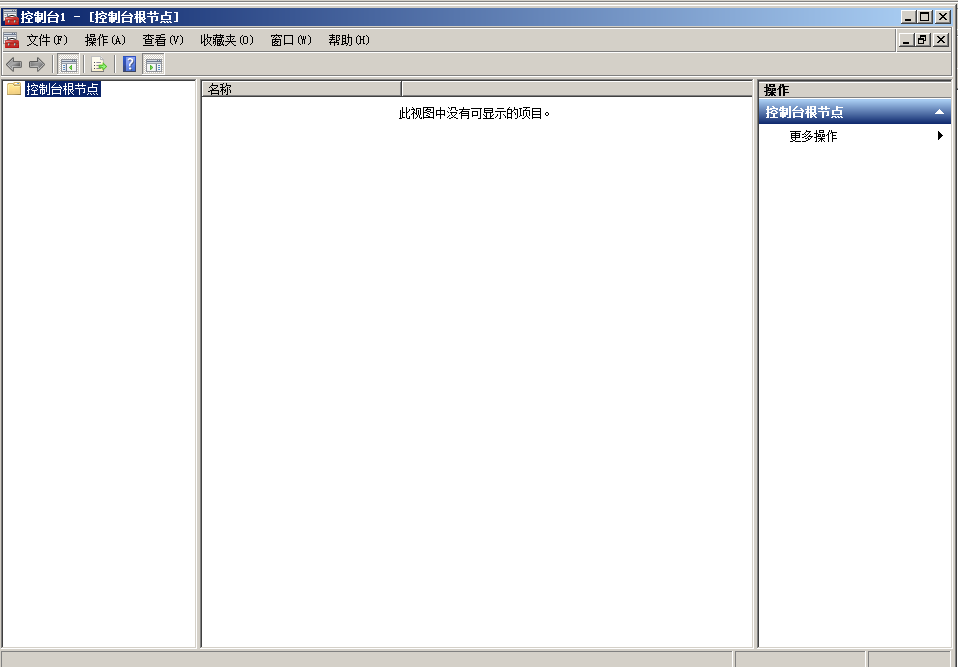
安装证书主要包括：根证书的安装、中级CA证书的安装和服务器证书的安装。

### 2.3.1 根证书的安装

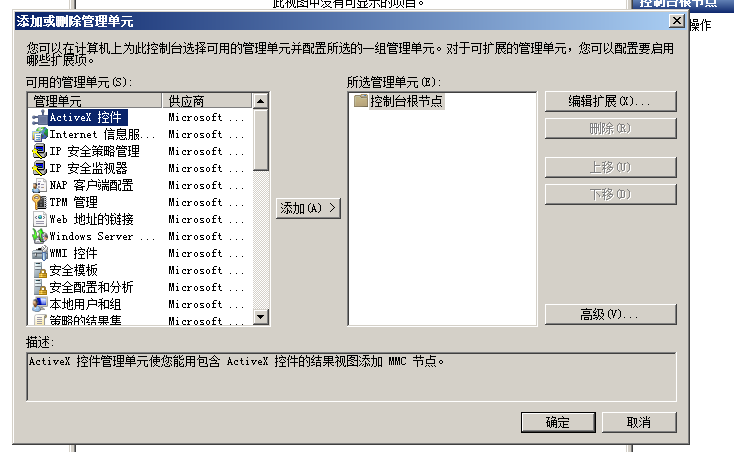
根证书的安装的步骤如下：

以管理员权限得到一个命令行窗口，在Windows2008上，”开始“->”运行”，输入cmd，点击确定

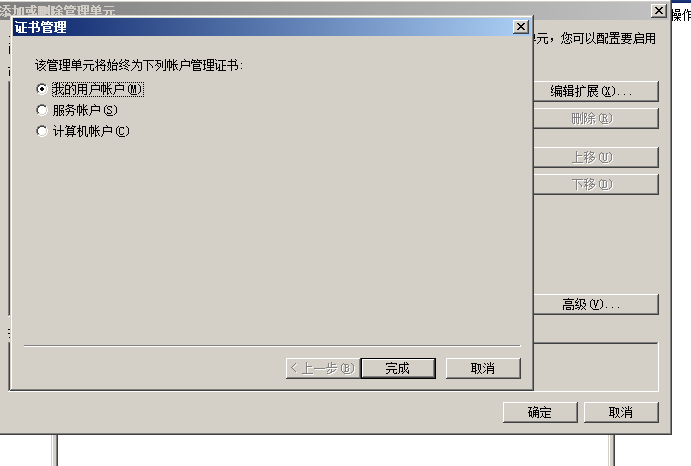
打开本机证书库导入根证书和中级CA证书，在命令行窗口上输入mmc



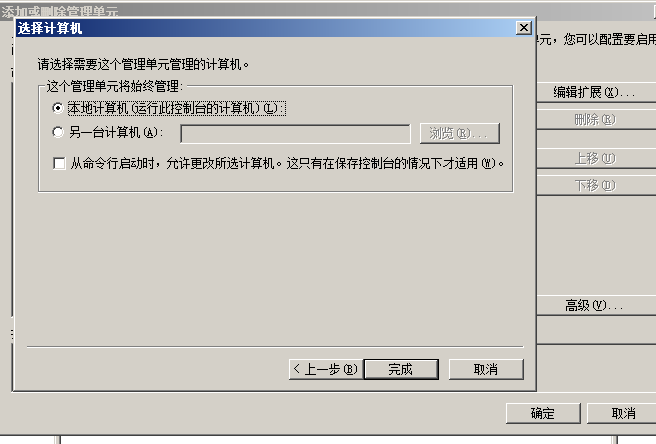
点击“文件”->”添加管理单元”,出现“添加或者删除管理单元”对话框，如下图所示



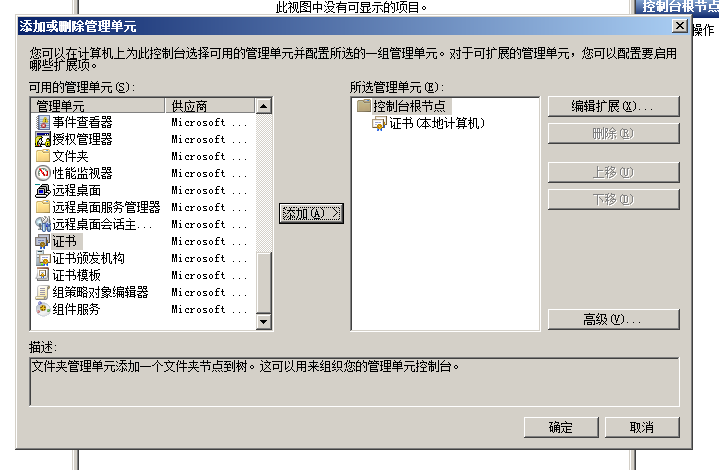
4、在左边选择“证书”，点击中间的“添加”按钮，出现“证书管理”对话框，如下图所示。



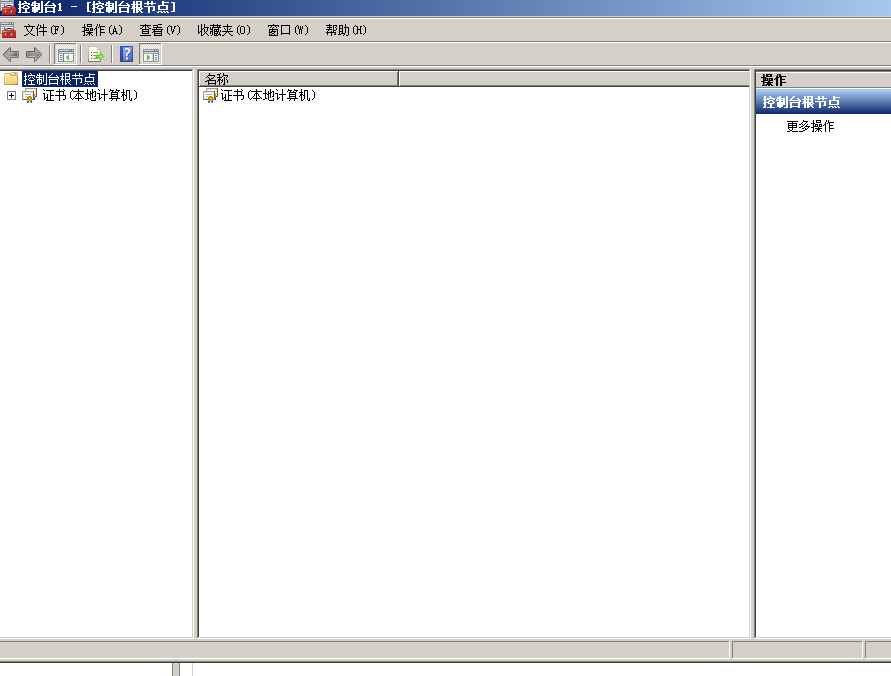
5、选择“计算机账户”，点击“下一步”按钮。如图所示



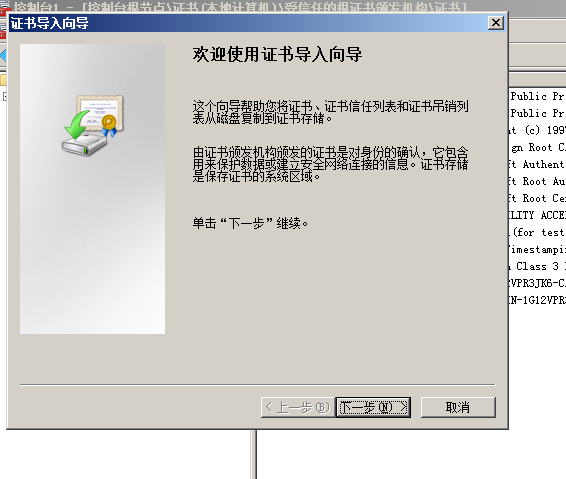
选择“本地计算机”，点击“完成”按钮，关闭“选择计算机”对话框。这时，“添加或者删除管理单元”对话框右边就出现了“证书（本地计算机）”这个管理单元，如图所示



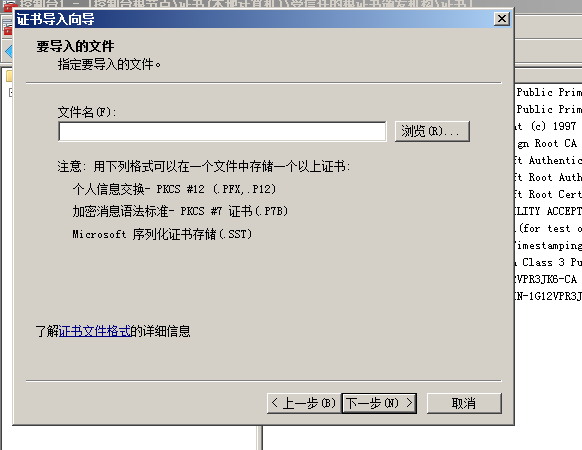
点击“确定”按钮。出现下图



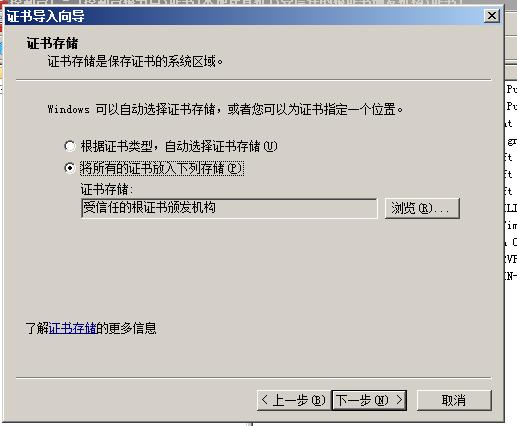
展开“证书（本地计算机）”，在“受信任的根证书颁发机构”那里导入根证书。选定“受信任的根证书颁发机构”下的“证书”，点击鼠标右键，在菜单中选择“所有任务”->“导入”，出现下面的证书导入向导。



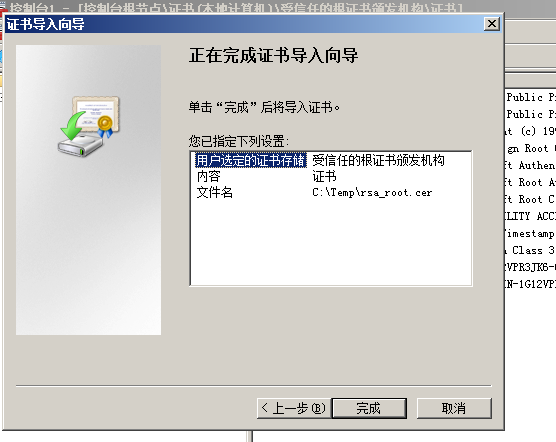
点击“下一步”按钮



点击“浏览”按钮选中根证书，然后点击“下一步”按钮。



点击“下一步”



点击“完成”按钮。

### 2.3.2 中级CA证书的安装

如果有中级CA证书，则需要安装中级CA证书,其方法和根证书的安装类似，只是这次是在“中间CA颁发机构”导入，而不是在“受信任的根证书颁发机构”导入。

### 2.3.3 服务器证书的安装

服务器的安装的具体步骤如下：

1. 如果没有安装IIS的CNG，则需要先安装IIS的CNG。

把NetcaIISCNGProvider.dll拷贝到C：\windows\System32目录下。然后注册它

在命令行窗口输入

cd C：\windows\System32

regsvr32 NetcaIISCNGProvider.dll

1. 安装服务器证书到个人证书库。

在命令行窗口输入

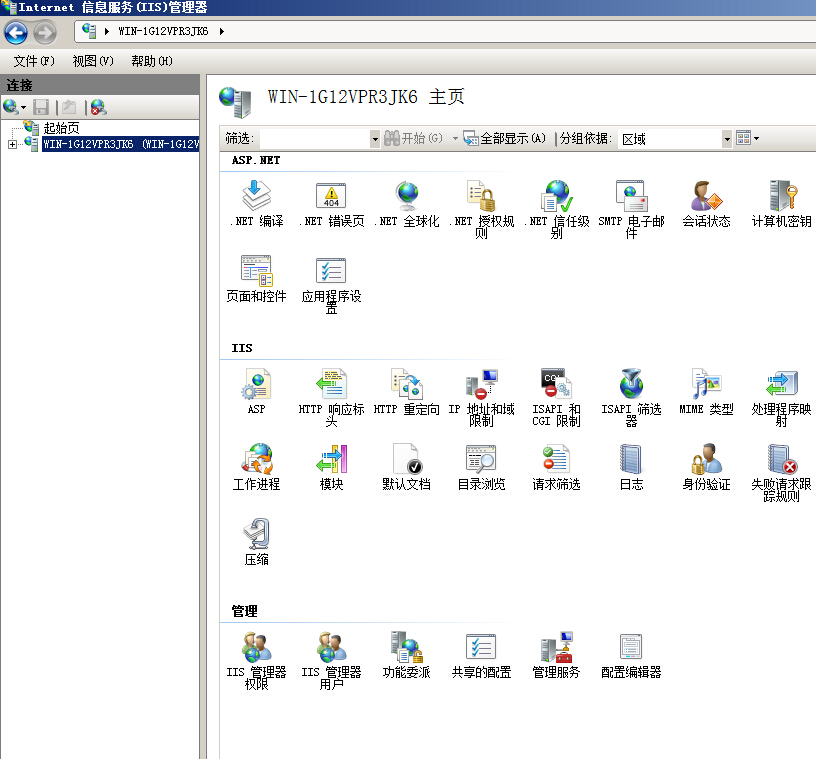
RegIISCert.exe 服务器证书文件名 密码

成功后，会提示你运行certutil

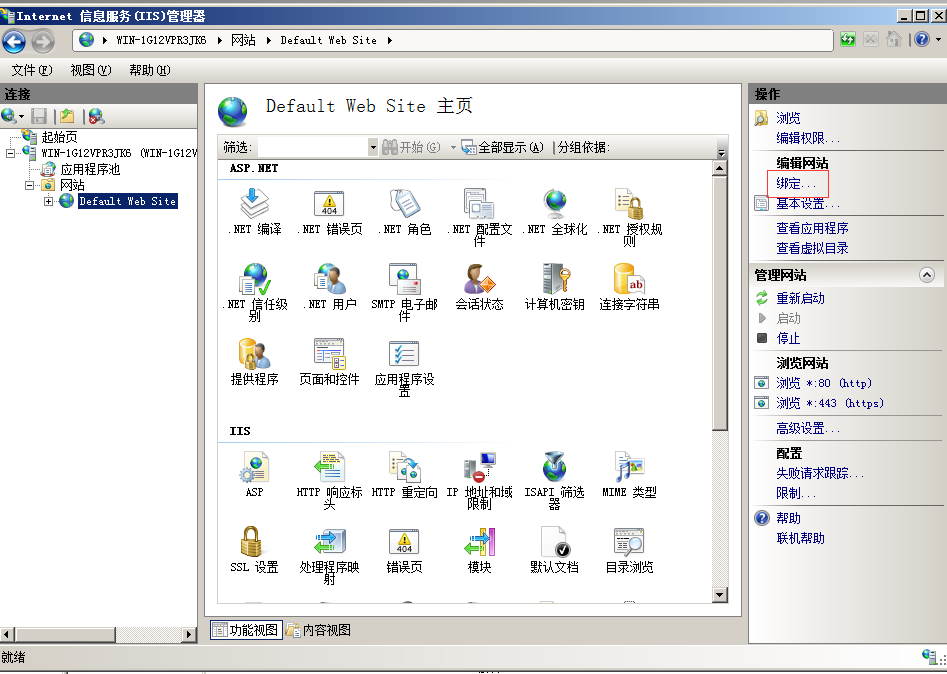
在命令行窗口运行提示的certutil命令

1. 配置IIS服务器证书。

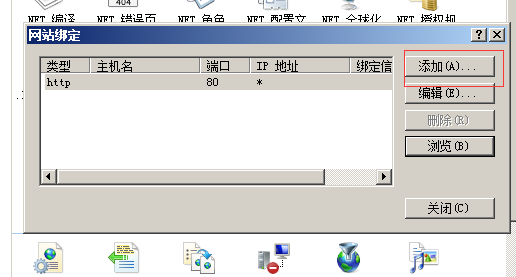
点击windows的“开始”->”管理工具”->”Internet 信息服务（IIS）管理器”，出现



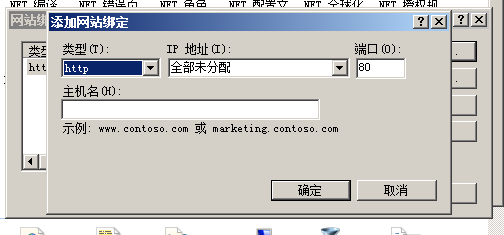
展开左边，选择“Default Web Site”



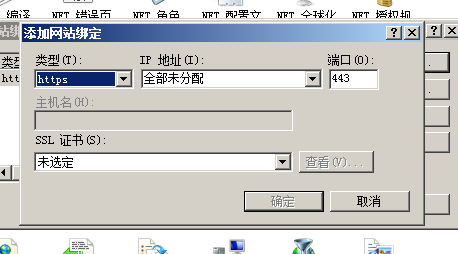
点击右边的“绑定…”



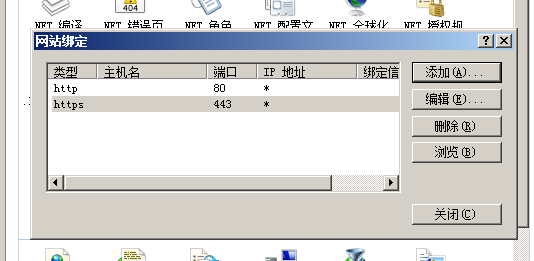
点击“添加”按钮



类型选择“https”



SSL证书选择，刚才注册的服务证书，点击“确定”按钮



点击“关闭”按钮，完成SSL服务器证书的配置

## 2.4配置相关的TLS选项

### 2.4.1 配置SSL/TLS版本

SSL 2.0和SSL 3.0已经不安全需要禁用。有些协议可能默认并不开启，需要启用。

禁用SSL 2.0：

在注册表HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\ Server项下设置两个DWORD值：DisabledByDefault和Enabled。DisabledByDefault为1，Enabled为0。如果注册表没有该项则创建，没有改值也要新建（下同）。

禁用SSL 3.0：

在注册表HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\ Server项下设置两个DWORD值：DisabledByDefault和Enabled。DisabledByDefault为1，Enabled为0。

启用TLS 1.0：

在注册表HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\ Server项下设置两个DWORD值：DisabledByDefault和Enabled。DisabledByDefault为0，Enabled为1。如果需要禁用则DisabledByDefault为1，Enabled为0。

启用TLS 1.1：

在注册表HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\ Server项下设置两个DWORD值：DisabledByDefault和Enabled。DisabledByDefault为0，Enabled为1。如果需要禁用则DisabledByDefault为1，Enabled为0。

启用TLS 1.2：

在注册表HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\ Server项下设置两个DWORD值：DisabledByDefault和Enabled。DisabledByDefault为0，Enabled为1。如果需要禁用则DisabledByDefault为1，Enabled为0。

以上注册表项修改后，重启计算机后生效。

### 2.4.2 配置算法套件

算法套件可以参考：<https://msdn.microsoft.com/en-us/library/aa374757(VS.85).aspx>

配置算法套件需要谨慎，除非你知道了解各种算法套件的含义以及客户端支持的情况，否则可能会导致某些客户端访问不了你的网站。具体方法如下：修改HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Cryptography\Configuration\SSL\00010002项的Functions字符串值。算法套件直接以逗号隔开。有优先顺序的，越前面越优先。

以上注册表项修改后，重启计算机后生效。