**实验 证书管理及SSL配置**

**实验目的**：使用证书服务器CA，配置SSL实现双向/单向认证；

注：相关实验也可用于outlook中配置签名和加密证书来使用安全电子邮件服务。

**实验平台**：

1. Windows平台：编译好的openssl库，使用IIS（添加windows组件IIS服务）、Tomcat（需要下载jdk及Tomcat并配置环境变量等）、Apache及Nginx等；windows server 2003或者2008（添加证书服务器及IIS服务）+ windows IE；

2. linux平台：openssl及Tomcat、Apache及Nginx。

**实验方法**：（1）使用openssl搭建证书服务器，在IIS和浏览器端配置双向/单向SSL

证书服务器部分参见：<http://blog.csdn.net/atco/article/details/7590069>

服务器/浏览器配置部分参见：<https://www.myssl.cn/home/article-0403-20.html>

（2）使用openssl搭建证书服务器，在Tomcat和浏览器端配置双向/单向SSL

<https://wenku.baidu.com/view/d0d6ae4eeff9aef8951e062c.html>

<http://blog.csdn.net/STK_tianwen/article/details/6298648>

（3）使用keytool+tomcat配置双向证书

<http://www.blogjava.net/stevenjohn/archive/2012/08/22/385989.html>

（4）使用windows+apache+openssl

<http://blog.csdn.net/decajes/article/details/41706739>

（4）windows server配置证书服务器，及双向/单向SSL

<http://www.cnblogs.com/zhongweiv/archive/2013/01/07/https.html>

<http://blog.csdn.net/dier4836/article/details/7719532>

也可以参见《实验》后的附录

**实验要求**：

1. windows或者linux平台下，配置证书服务器，完成服务器证书和客户证书申请和生成。

2. 导入证书完成ssl配置，并通过https访问配置好的以**自己名字命名**的站点来验证实验是否成功。

3. 完成上述两个部分，在BB平台提交详细的实验报告word文档，包含完整的实验所用命令及所有配置步骤截图。

在ssl配置加载证书时，chrome仍然提示红色不安全站点的问题：使用F12查看证书时发现：

问题：chrome 提示： Subject Alternative Name Missing

The certificate for this site does not contain a Subject Alternative Name extension containing a domain name or IP address.

可参见如下链接：https://stackoverflow.com/questions/43665243/chrome-invalid-self-signed-ssl-cert-subject-alternative-name-missing，即在生成证书时，使用v3扩展文件，命令如下：  bin\openssl x509 -in server.csr -out server.crt -req -signkey server.key -days 365 -sha256 -extfile v3.ext，v3.ext的写法详见上面链接，或者继续使用上面的问题提示baidu。

如果还不能解决，将结果如实写在实验报告里即可。

**附录**

密码学及应用—PKI技术—证书管理

网络信息安全综合实验平台—密码学及应用—PKI技术---证书管理

#### 实验示例

下面以主机A、B为例，来讲解实验过程，在实验中，主机A担任CA和服务器的角色，主机B担任客户端的角色。

***主机A***

*首先CA要安装证书服务*

*主机A依次选择“开始”|“设置”| “控制面板”|“添加或删除程序”|“添加/删除Windows组件”，选中组件中的“证书服务”，此时出现“Microsoft证书服务”提示信息，单击“是”，然后单击“下一步”。在接下来的安装过程中依次要确定如下信息：*

*CA类型（选择独立根CA），CA的公用名称（userGXCA），证书数据库设置（默认），确定，系统提示要暂停Internet信息服务，单击“是”，系统开始进行组件安装，弹出“所需文件”对话框，指定“文件复制来源”为光盘或者指定系统文件~~D:\ExpNIC\CrypApp\Tools\WindowsCA\i386~~，在启动“证书颁发机构”服务后，主机A便拥有了CA的角色。*

CA通过“开始”|“程序”｜“管理工具”|“证书颁发机构”打开“证书颁发机构”。在“证书颁发机构”的左侧树状结构中右键单击“CA的名称”|“属性”，打开“属性”选项卡，单击“策略模块”|“属性”。在“请求处理”页签中选择“如果可以的话，按照证书模板的设置。否则，将自动颁发证书”。单击“应用”按钮，出现重启证书服务提示信息，单击“确定”直到完成设置，重启证书服务。

***主机B***

客户端通过IE浏览器访问http://~~CA的IP~~/certsrv/（可以是127.0.0.1），选择“申请一个证书”|“高级证书申请”|“创建并向此CA提交一个申请”进入证书申请页面。

在“识别信息”中填入相关信息。

在“需要的证书类型”中选择“客户端身份验证证书”。

在“密钥选项”中选中“标记密钥为可导出”，其它项保持默认设置。

单击“提交”按钮提交信息。

由于CA已经设置“自动颁发证书”策略，所以申请被立刻批准，此时页面显示“证书已颁发”，单击”安装此证书”。出现对话框“潜在的脚本冲突”，单击“是”。页面显示“证书已安装”。

***主机A***

下面来演示，CA的备份和还原

当CA备份时， CA右键单击“CA的名称”|“所有任务”|“备份CA”，出现“证书颁发机构备份向导”，单击“下一步”。

在“选择要备份的项目”中选中两个选项。

“备份到这个位置中”选择一个新建的空目录，单击“下一步”。

输入密码并确认密码，单击“下一步”，“完成”。

在“颁发的证书”目录中，选择证书，右键单击此证书选择“所有任务”|“吊销证书”。弹出对话框要求指定“理由码”，选择任意“理由码”，单击确定。此时证书已经转移到“吊销的证书”目录中，右键单击，证书选择“所有任务”|“解除吊销证书”，此时出现提示信息“取消吊销命令失败…”，单击“确定”。

需要还原时，右键单击“CA的名称”|“所有任务”|“还原CA”，出现“证书颁发机构还原向导”提示要立即关闭证书服务，单击“确定”。出现“证书颁发机构还原向导”，单击“下一步”。

“选择要还原的项目”中选中两个选项。“从这个位置还原”选择CA备份的目录，单击“下一步”。

输入密码，单击“下一步”，“完成”。

“证书颁发机构还原向导”提示要启动证书服务，单击“是”启动证书服务。

此时检查刚才被吊销的证书，已经从“吊销的证书”目录中还原到“颁发的证书”目录中。

***主机A***

主机A申请服务器证书。

点击“开始”|“程序”｜“管理工具”打开“Internet信息服务（IIS）管理器”，选中“Internet信息服务”|“计算机名（本地计算机）”|“网站”|“默认网站”，右键单击“默认网站”，单击”属性”。

选择“目录安全性”页签，单击“安全通信”中的“服务器证书”，此时出现“Web服务器证书向导”，单击“下一步”。

在“选择此网站使用的方法”中，选择“新建证书”，单击“下一步”。

选择“现在准备证书请求，但稍后发送”，单击“下一步”。

填写有关证书申请的相关信息，单击“下一步”。

在“证书请求文件名”中，指定证书请求文件的文件名和存储的位置（默认c:\certreq.txt）。单击“下一步”，直到“完成”。

然后通过Web服务向CA申请证书，在IE中输入<http://CA的IP/certsrv/>

进入主页之后，单击“申请一个证书”|“高级证书申请”|“使用base64编码...提交一个申请”进入“提交一个证书申请或续订申请”页面。

打开证书请求文件certreq.txt，将其内容全部复制粘贴到提交证书申请页面的“保存的申请”文本框中，然后单击“提交”，由于CA已经设置“自动颁发证书”策略，所以申请被立刻批准，点击下载证书，将证书保存到本地，点击下载证书链接，保存到本地，

在“默认网站”｜“属性”的“目录安全性”页签中单击“服务器证书”按钮，出现“Web服务器证书向导”，单击“下一步”。

选择“处理挂起的请求并安装证书”，单击“下一步”。

在“路径和文件名”中选择存储到本地计算机的证书文件，单击“下一步”。

在“SSL端口”文本框中填入“443”，单击“下一步”直到“完成”。

回到桌面，右键单击certnew.p7b证书文件，在弹出菜单中选择“安装证书”，进入“证书导入向导”页面，单击“下一步”按钮，在“证书存储”中选择“将所有的证书放入下列存储”，浏览选择“受信任的根证书颁发机构”｜“本地计算机”，单击“下一步”按钮，直到完成。

在“默认网站”｜“属性”的“目录安全性”页签中单击编辑按钮，选择要求安全通道和要求客户端证书。单击确定按钮，

***主机B***

客户端访问服务器，在IE中输入 https://服务器IP。出现“安全警报”对话框提示“即将通过安全连接查看网页”，单击“确定”，弹出“安全警报”对话框询问“是否继续？”，单击“是”。出现“选择数字证书”对话框，选择相应的数字证书，单击“确定”就可以访问服务器的Web服务了。

***主机A***

CA在“颁发的证书”中找到客户端使用的Web浏览器证书。右键单击此证书，选择“所有任务”|“吊销证书”，选择任意“理由码”，单击“确定”，此时证书即转移到“吊销的证书”目录中。在左侧树状结构中右键单击“吊销的证书”|“所有任务”|“发布”，出现对话框“发布CRL”，单击“确定”。在左侧树状结构中右键单击“吊销的证书”|“属性”弹出“吊销的证书的属性”对话框，单击“查看CRL”页签,单击“吊销列表”按钮，可以查看刚发布的CRL。

***主机B***

客户端重新访问服务器的证书服务，此时发现不能访问服务器，页面显示“该页要求有效的SSL客户证书”。说明此时客户端证书已经不被信任。

至此本实验结束。