# 用Tomcat服务器配置https双向认证过程实战

**一、为服务器生成证书**

C:\Windows\system32>keytool -genkey -v -alias tomcat -keyalg RSA -keystore D:\tomcat.keystore -validity 36500  
输入keystore密码：  
再次输入新密码:  
您的名字与姓氏是什么？  
  [Unknown]：  StoneXing  
您的组织单位名称是什么？  
  [Unknown]：  iFLYTEK  
您的组织名称是什么？  
  [Unknown]：  iFLYTEK  
您所在的城市或区域名称是什么？  
  [Unknown]：  合肥市  
您所在的州或省份名称是什么？  
  [Unknown]：  安徽省  
该单位的两字母国家代码是什么  
  [Unknown]：  CN  
CN=StoneXing, OU=iFLYTEK, O=iFLYTEK, L=合肥市, ST=安徽省, C=CN 正确吗？  [否]：  y  
  
正在为以下对象生成 1,024 位 RSA 密钥对和自签名证书 (SHA1withRSA)（有效期为 36,500 天）:  
         CN=StoneXing, OU=iFLYTEK, O=iFLYTEK, L=合肥市, ST=安徽省, C=CN  
输入<tomcat>的主密码  
        （如果和 keystore 密码相同，按回车）：  
[正在存储 D:\tomcat.keystore]  
  
C:\Windows\system32>

“D:\tomcat.keystore”含义是将证书文件的保存路径，证书文件名称是tomcat.keystore(可自定义名称)；  
“-validity 36500”含义是证书有效期，36500表示100年，默认值是90天；

**二、为客户端生成证书**

**1、生成客户端证书**

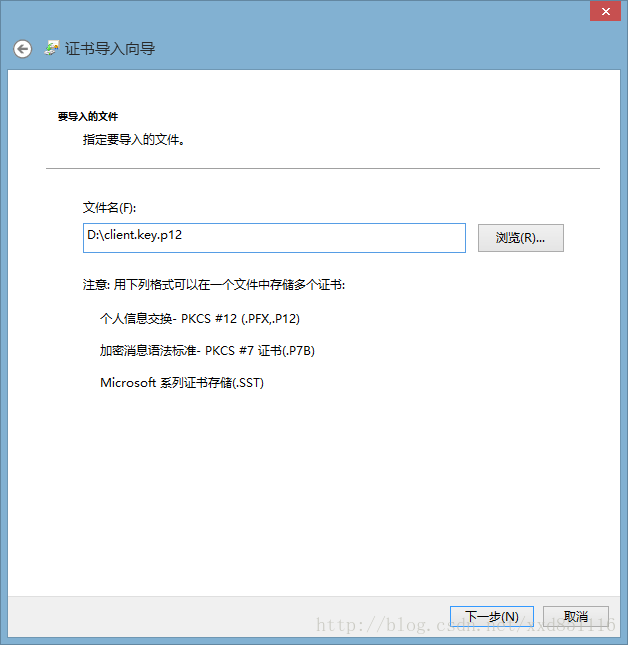
C:\Windows\system32>keytool -genkey -v -alias mykey -keyalg RSA -storetype PKCS12 -keystore D:\client.key.p12  
输入keystore密码：  
再次输入新密码:  
您的名字与姓氏是什么？  
  [Unknown]：  StoneXing  
您的组织单位名称是什么？  
  [Unknown]：  iFLYTEK  
您的组织名称是什么？  
  [Unknown]：  iFLYTEK  
您所在的城市或区域名称是什么？  
  [Unknown]：  合肥  
您所在的州或省份名称是什么？  
  [Unknown]：  安徽省  
该单位的两字母国家代码是什么  
  [Unknown]：  CN  
CN=StoneXing, OU=iFLYTEK, O=iFLYTEK, L=合肥, ST=安徽省, C=CN 正确吗？  [否]：  y  
  
正在为以下对象生成 1,024 位 RSA 密钥对和自签名证书 (SHA1withRSA)（有效期为 90 天）:  
         CN=StoneXing, OU=iFLYTEK, O=iFLYTEK, L=合肥, ST=安徽省, C=CN  
[正在存储 D:\client.key.p12]  
  
C:\Windows\system32>

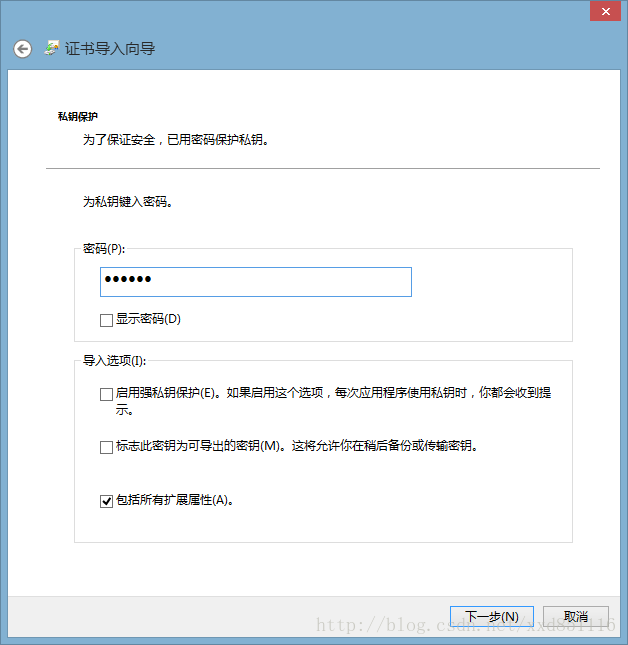
生成的两个文件：

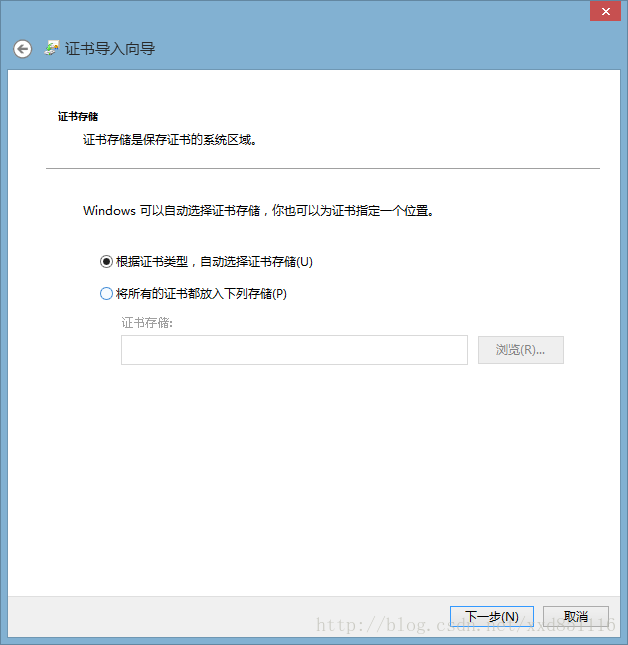
http://img.blog.csdn.net/20140123124107281?watermark/2/text/aHR0cDovL2Jsb2cuY3Nkbi5uZXQveHhkODUxMTE2/font/5a6L5L2T/fontsize/400/fill/I0JBQkFCMA==/dissolve/70/gravity/SouthEast

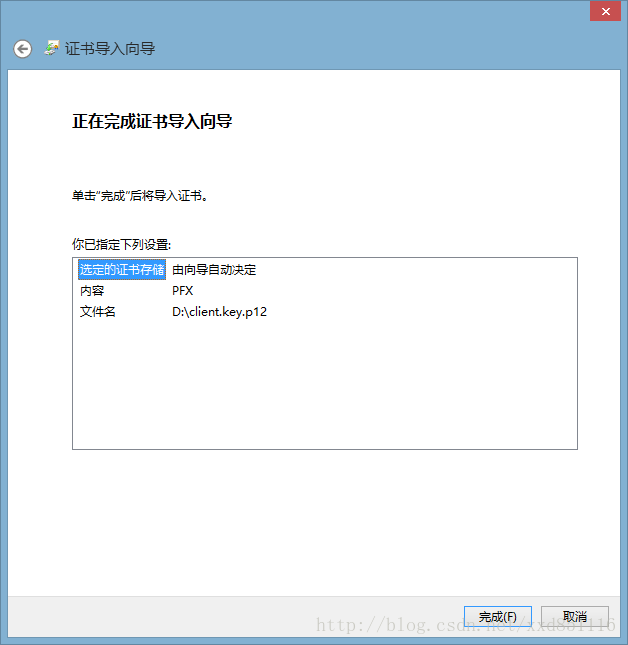
**2、安装客户端证书**  
双击客户端证书“client.key.p12”完成导入证书过程如下：

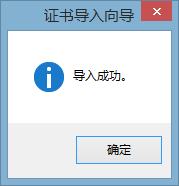


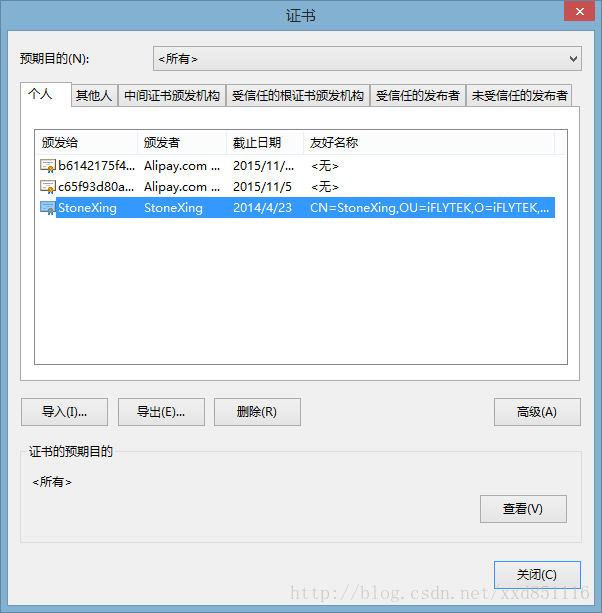












**三、让服务器信任客户端证书**

**1、将客户端证书导出为CER文件**  
由于是双向SSL认证，服务器必须要信任客户端证书，因此，必须把客户端证书添加为服务器的信任认证。因不能直接将PKCS12格式的证书库导入服务器证书库，将客户端证书导出为一个单独的CER文件  
keytool -export -alias mykey -keystore D:\client.key.p12 -storetype PKCS12 -storepass password -rfc -file D:\client.key.cer  
注：password为客户端证书的密码

C:\Windows\system32>keytool -export -alias mykey -keystore D:\client.key.p12 -storetype PKCS12 -storepass 888888 -rfc -file D:\client.key.cer  
保存在文件中的认证 <D:\client.key.cer>  
  
C:\Windows\system32>

**2、将CER文件导入到服务器的证书库**  
添加为一个信任证书使用命令如下：

C:\Windows\system32>keytool -import -v -file D:\client.key.cer -keystore D:\tomcat.keystore  
输入keystore密码：  
所有者:CN=StoneXing, OU=iFLYTEK, O=iFLYTEK, L=合肥, ST=安徽省, C=CN  
签发人:CN=StoneXing, OU=iFLYTEK, O=iFLYTEK, L=合肥, ST=安徽省, C=CN  
序列号:52e07723  
有效期: Thu Jan 23 09:57:55 CST 2014 至Wed Apr 23 09:57:55 CST 2014  
证书指纹:  
         MD5:15:29:58:68:8D:63:E1:00:8E:E6:EC:5E:AD:23:79:38  
         SHA1:B7:EF:B9:67:BD:56:95:82:3D:D8:14:0D:20:69:F0:C8:60:98:31:9A  
         签名算法名称:SHA1withRSA  
         版本: 3  
信任这个认证？ [否]：  y  
认证已添加至keystore中  
[正在存储 D:\tomcat.keystore]  
  
C:\Windows\system32>

**3、检查安装结果**  
通过list命令查看服务器的证书库，可以看到两个证书，一个是服务器证书，一个是受信任的客户端证书：  
keytool -list -keystore D:\tomcat.keystore (tomcat为你设置服务器端的证书名)。

C:\Windows\system32>keytool -list -keystore D:\tomcat.keystore  
输入keystore密码：  
  
Keystore 类型： JKS  
Keystore 提供者： SUN  
  
您的 keystore 包含 2 输入  
  
tomcat, 2014-1-23, PrivateKeyEntry,  
认证指纹 (MD5)： 4B:71:06:02:7C:35:F8:BF:B1:24:E2:68:8F:65:75:15  
mykey, 2014-1-23, trustedCertEntry,  
认证指纹 (MD5)： 15:29:58:68:8D:63:E1:00:8E:E6:EC:5E:AD:23:79:38  
  
C:\Windows\system32>

**四、让客户端信任服务器证书**

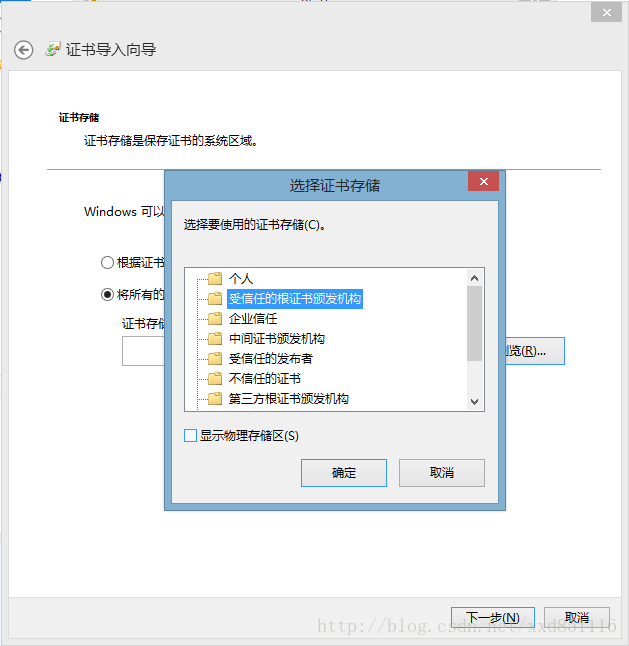
**1、把服务器证书导出为CER文件**  
由于是双向SSL认证，客户端也要验证服务器证书，因此，必须把服务器证书添加到浏览的“受信任的根证书颁发机构”。由于不能直接将keystore格式的证书库导入，必须先把服务器证书导出为一个单独的CER文件，使用如下命令：  
keytool -keystore D:\home\tomcat.keystore -export -alias tomcat -file D:\home\tomcat.cer (tomcat为你设置服务器端的证书名)。

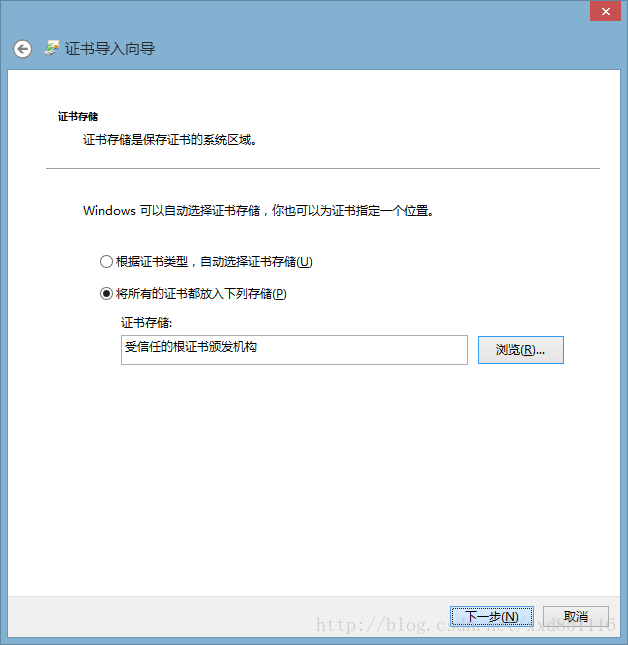
C:\Windows\system32>keytool -keystore D:\tomcat.keystore -export -alias tomcat -file D:\tomcat.cer  
输入keystore密码：  
保存在文件中的认证 <D:\tomcat.cer>  
  
C:\Windows\system32>

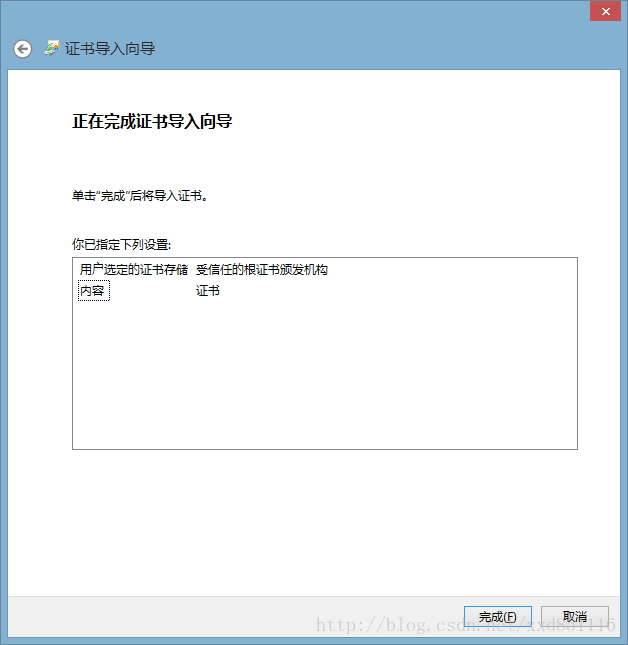
**2、在客户端安装服务器证书**  
双击“tomcat.cer”，按照提示安装证书，将证书填入到“受信任的根证书颁发机构”。

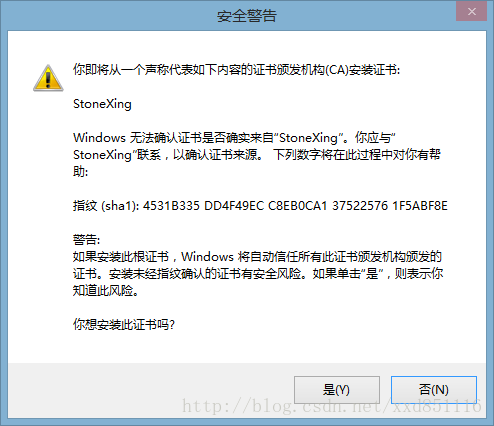


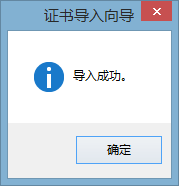


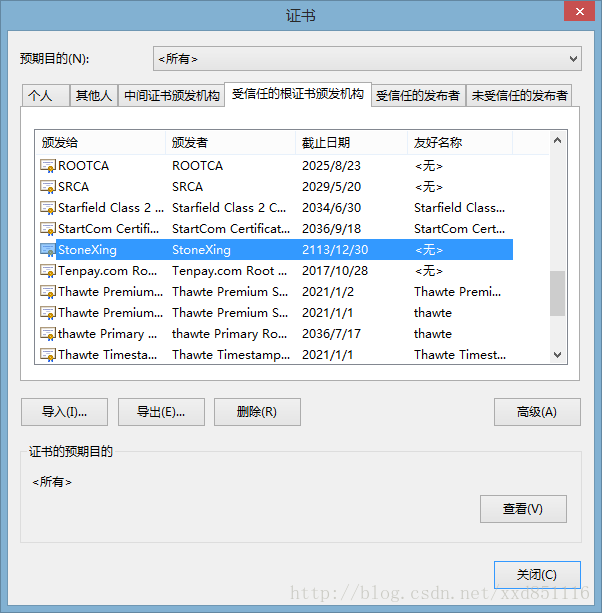










**3、检查安装结果**  
IE -> Internet选项 -> 内容 -> 证书  


**五、配置Tomcat服务器**

**[html]** [view plaincopy](http://blog.csdn.net/xxd851116/article/details/18701731)[在CODE上查看代码片](https://code.csdn.net/snippets/167917)

1. <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
2. maxThreads="150" scheme="https" secure="true"
3. clientAuth="false" sslProtocol="TLS"
4. keystoreFile="D:\\tomcat.keystore" keystorePass="888888"
5. truststoreFile="D:\\tomcat.keystore" truststorePass="888888" />

注意服务端证书名保持一致  
属性说明：  
clientAuth:设置是否双向验证，默认为false，设置为true代表双向验证  
keystoreFile:服务器证书文件路径  
keystorePass:服务器证书密码  
truststoreFile:用来验证客户端证书的根证书，此例中就是服务器证书  
truststorePass:根证书密码

**六、测试**

https://localhost:8443/





**服务器的证书与网址不相符问题需要理解浏览器做了什么：**

1、浏览器将自己支持的一套加密规则发送给网站。  
2、网站从中选出一组加密算法与HASH算法，并将自己的身份信息以证书的形式发回给浏览器。证书里面包含了网站地址，加密公钥，以及证书的颁发机构等信息。  
3、获得网站证书之后浏览器要做以下工作：  
      a)  验证证书的合法性（颁发证书的机构是否合法，证书中包含的网站地址是否与正在访问的地址一致等），如果证书受信任，则浏览器栏里面会显示一个小锁头，否则会给出证书不受信的提示。  
      b)  如果证书受信任，或者是用户接受了不受信的证书，浏览器会生成一串随机数的密码，并用证书中提供的公钥加密。  
      c)  使用约定好的HASH计算握手消息，并使用生成的随机数对消息进行加密，最后将之前生成的所有信息发送给网站。