环境说明

为了测试基于 Tomcat WEB 服务的 SSL 双向认证，本文档采用了最新的 Tomcat 6.0 WEB 服务。以下是本文档的具体试验环境：

WEB 服务器：Windows 2003 Enterprise Server English Edition +Tomcat6.0+JDK1.4

客户端：Windows XP Professional English Version + Service Pack 3

Tomcat 各种版本的配置方式大体相同，如有问题，请咨询 SHECA：

密钥和证书的获取

本文采用标准的 Java keytool 方式，并基于标准的 Java keystore 方式为 WEB 服务器提供 Private key、Identity Cert 和 Trusted Cert 存储。

（注：本文档在命令行模式下执行的命令运行路径均需要定位于 keytool.exe 所在的路径，请遵照执行，以免差错）

产生密钥对：

在 windows 操作系统上打开“命令提示符”窗口，用“cd”命令定位到 keytool.exe 所在的文件夹。在命令行模式下运行以下命令产生密钥对，产生的密钥对文件将会以 jks 进行保存。

随即在命令行模式下运行以下命令以产生密钥既 jks 文件。

例：

.\keytool -genkey -keyalg rsa -keysize 2048 -alias test -keypass 123456 -keystore server.jks -storepass 123456

其中各参数的解释如下：

- keysize 为密钥长度，一般为 2048 位
- alias 为密钥库的别名，请自行设置，本例中设置为 test
- keypass 和 storepass 为密钥和密钥库库的密码，请自行设置，本例中设置为 123456
- keystore 为密钥库文件的名称，请自行设置，本例中设置为 server.jks

此时系统会提示您输入信息，请确保以下内容和您提交到 SHECA 的资料一致：

Common Name（服务器域名或者 IP）

Organization name （组织名或公司名）

Organization unit name （组织单位名或部门名）

City or location name（城市或区域名）

State or province name （省份或者州名）

Country name （国家名的两位编码，中国为“CN”）

产生证书请求：

再运行以下命令产生证书请求，证书请求文件以 csr 格式进行保存，例：

.\keytool -certreq -alias test -keystore server.jks -file server.csr -storepass 123456

其中各参数的解释如下：

- alias 为密钥库的别名，此处必须填为您之前设置的别名
- keystore 为密钥库的名称，此处必须填为您之前生成的 jks 的名称
- file 为生成的证书请求文件的名称，请自行设置，此处以 server.csr 为例
- storepass 为密钥库的密码，此处必须填为您之前设置的密码

产生证书请求文件“server.csr”；

申请万维信安全站点证书：

将“server.csr”文件提交给 SHECA 负责您的万维信安全站点证书的相关人员，SHECA 将会根据您的证书请求文件和提交的资料进行万维信安全站点证书的签发；

部署万维信安全站点证书：

1. 证书处理

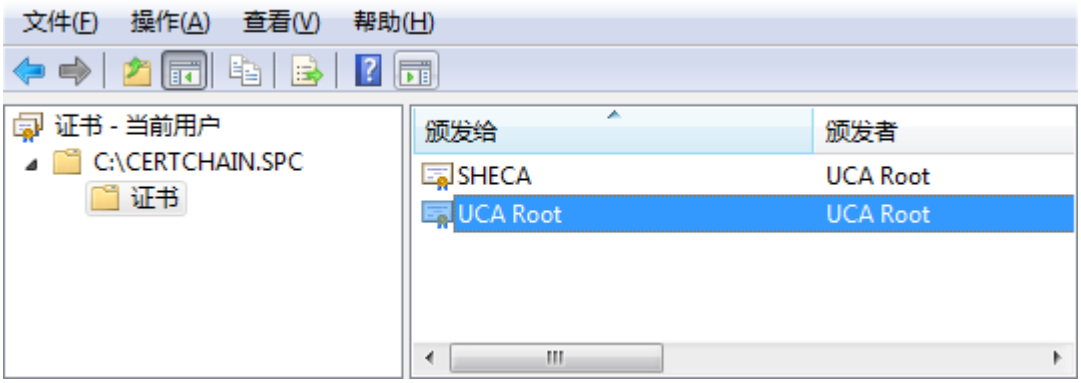
SHECA 处理完毕之后，将提供给您万维信安全站点证书，可能包括以下内容：

- UserCert.der 为二进制编码的万维信安全站点证书文件。
- UserCert.cer 为 Base64 编码的万维信安全站点证书文件。
- CertChani.spc 文件为 SHECA 证书链文件。
  - 如果您申请的是 UCA Globle Root 签发的万维信安全站点证书，那么该证书链中包含的根证书为 UCA Globle Root，中级证书为其颁发的 SHECA。
  - 如果您申请的是 UCA Root 签发的万维信安全站点证书，那么该证书链中包含的根证书为 UCA Root，中级证书为其颁发的 SHECA。

本例中以 UCA Root 为例：

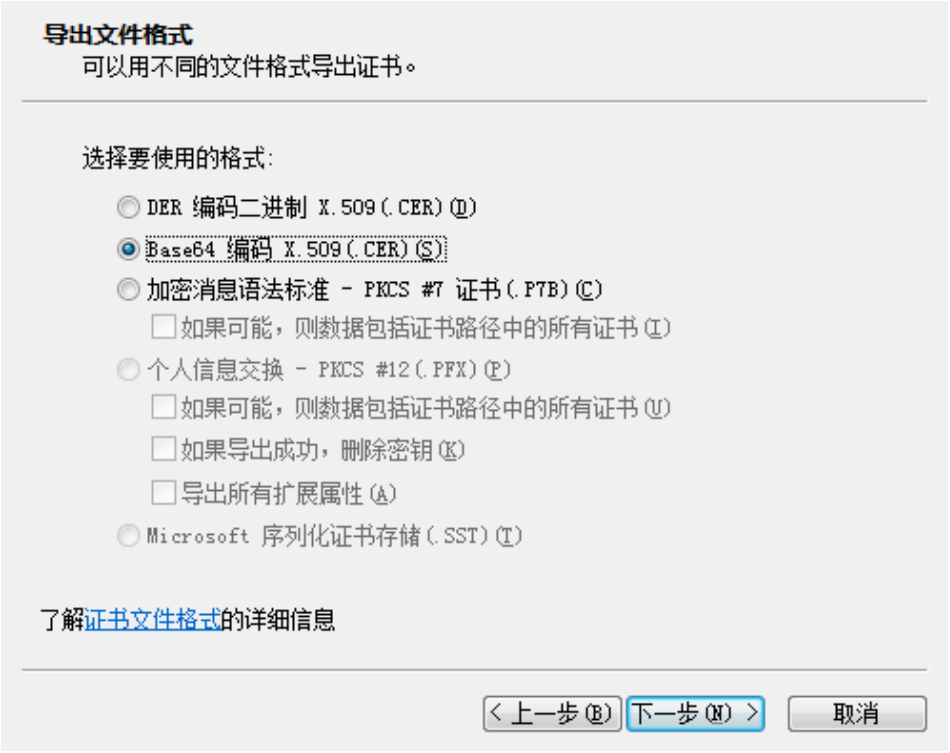
2. 导入根证书：

将 CertChain.SPC 文件打开，选中 UCA Root 这张证书右键选择“打开”



在详细信息的标签栏中选择“复制到文件”

选择 Base64 编码导出证书



将此证书保存为文件 root.cer，并放置于 keytool.exe 同一目录下，运行以下命令导入根证书：

.\keytool -import -trustcacerts -alias root -file root.cer -storepass 123456 -keystore server.jks

3. 导入中级证书

按照步骤一，同样的将 CertChain.SPC 文件当中的 SHECA 证书导出为 sheca.cer，并放置于 keytool.exe 目录下，运行以下命令以导入中级证书：

.\keytool -import -trustcacerts -alias sheca -file sheca.cer -storepass 123456 -keystore server.jks

4. 导入万维信安全站点证书：

将得到的服务器证书 UserCert.der 放入 keytool.exe 所在的文件夹中,并继续在命令行模式中执行以下命令导入服务器证书到 testkeystore.jks 中.

.\keytool -import -trustcacerts -alias test -keystore server.jks -file UserCert.der -storepass 123456

注：此时请特别注意该处的 alias 别名应和生成 JKS 的别名保持一致

成功后会提示认证回复已安装在 keystore 中

5. 证书查看：

使用以下命令查看证书是否正确导入：

.\keytool -list -v -keystore server.jks -storepass 123456