1）服务器证书

--生成jcbk.jks

keytool -genkey -alias jcbk -validity 36500 -keyalg RSA -keysize 1024 -keypass 123456 -storepass 123456 -dname "cn=localhost, ou=00, o=00, l=00, st=01, c=CN" -keystore jcbk.jks

2）导出服务器证书

keytool -keystore D:/jcbk.jks -export -alias jcbk -file D:/jcbk.cer

3）客户端证书生成

生成客户端证书：

keytool -genkey -alias jcbk\_client -validity 7 -keyalg RSA -keysize 1024 -keypass 123456 –storetype PKCS12 -storepass 123456 -dname "cn= 姓名 账号, ou=00, o=00, l=00, st=01, c=CN" -keystore jcbk\_client.p12

4）导出客户端证书

keytool -export -alias dc\_client -keystore D:/jcbk\_client.p12 -storetype PKCS12 -keypass 123456 -file D:/jcbk\_client.cer

5）将客户端证书导入服务器端可信任库

keytool -import -v -file D:/jcbk\_client.cer -keystore D:/jcbk.jks -storepass 123456

6）将客户端证书导入浏览器

将jcbk\_client.cer客户端证书添加到个人证书