**在Java中使用openssl制作的双向认证**

一 创建根证书  
1 生成根证书私钥  
openssl genrsa -des3 -out root.key 1024  
  
密码为:handwin1      #使用root.key 时，需要输入密码  
  
2 生成根证书签名请求文件  
openssl req -new -out root-req.csr -key root.key -keyform PEM  
  
3 自签根证书  
openssl x509 -req -in root-req.csr -out root-cert.cer -signkey root.key -CAcreateserial -days 7300  
  
4 导出p12格式证书  
openssl pkcs12 -export -clcerts -in root-cert.cer -inkey root.key -out root.p12  
  
  
  
二 创建服务端证书  
1.生成服务端key  
openssl genrsa -des3 -out server-key.key 1024  
  
2.生成服务端请求文件  
  
openssl req -new -out server-req.csr -key server-key.key

备注： Common Name (eg, your name or your server's hostname) []:172.16.20.144  （或域名）  
  
3.生成服务端证书（root证书，rootkey，客户端key，客户端请求文件这4个生成客户端证书）  
openssl x509 -req -in server-req.csr -out server-cert.cer -signkey server-key.key -CA root-cert.cer -CAkey root.key -CAcreateserial -days 7300  
  
4.生成服务端p12格式根证书  
openssl pkcs12 -export -clcerts -in server-cert.cer -inkey server-key.key -out server.p12  
  
  
三 创建客户端证书  
1.生成客户端key  
openssl genrsa -des3 -out client-key.key 1024  
  
  
2.生成客户端请求文件  
  
openssl req -new -out client-req.csr -key client-key.key  
  
3.生成客户端证书（root证书，rootkey，客户端key，客户端请求文件这4个生成客户端证书）  
openssl x509 -req -in client-req.csr -out client-cert.cer -signkey client-key.key -CA root-cert.cer -CAkey root.key -CAcreateserial -days 7300  
  
4.生成客户端p12格式根证书

openssl pkcs12 -export -clcerts -in client-cert.cer -inkey client-key.key -out client.p12

四：Java项目使用

4.1   服务端使用

trustStore使用root.p12，keyStroe使用server.p12

同时设置：

        sslEngine.setUseClientMode(false);  
        sslEngine.setNeedClientAuth(true);//启动对客户端证书的校验

4.2 客户端使用

trustStore使用root.p12,keyStore使用client.p12  
        sslEngine.setUseClientMode(true);

说明: 根证书作为CA,用来验证对方发送的签名是否正确。如果不对签名进行验证，则不需要根证书放到trustStore中.