# 1、证书处理

### -genkeypair 生成密钥

### -keyalg 指定密钥算法，这时指定RSA,

### -keysize 指定密钥长度，默认是1024位,这里指定2048，长一点，我让你破解不了（哈哈…）,

### -siglag 指定数字签名算法，这里指定为SHA1withRSA算法

### -validity 指定证书有效期，这里指定36500天，也就是100年，我想我的应用用不到那么长时间

### -alias 指定别名，这里是cas.server.com

### -keystore 指定密钥库存储位置，这里存在d盘

### -dname 指定用户信息，不用一个一个回答它的问题了；注意：CN=域名，我们采用passport.sso.com

## 1、命令如下

## keytool -genkeypair -keyalg RSA -keysize 2048 -sigalg SHA1withRSA -validity 36500 -alias passport.sso.com -keystore /Users/healerjean/Desktop/tomcat.keystore -dname "CN=passport.sso.com,OU=kawhi,O=carl,L=GuangZhou,ST=GuangDong,C=CN"

## 2、输入上述命令，下面密码我们输入123456,然后一直回车，就在mac桌面盘生成了tomcat.keystore文件；



# 2、证书生成

## 1、在cmd下输入如下命令，，密码为上面输入的123456：

### keytool -exportcert -alias passport.sso.com -keystore /Users/healerjean/Desktop/tomcat.keystore -file /Users/healerjean/Desktop/tomcat.cer -rfc

## 2、证书生成在：桌面

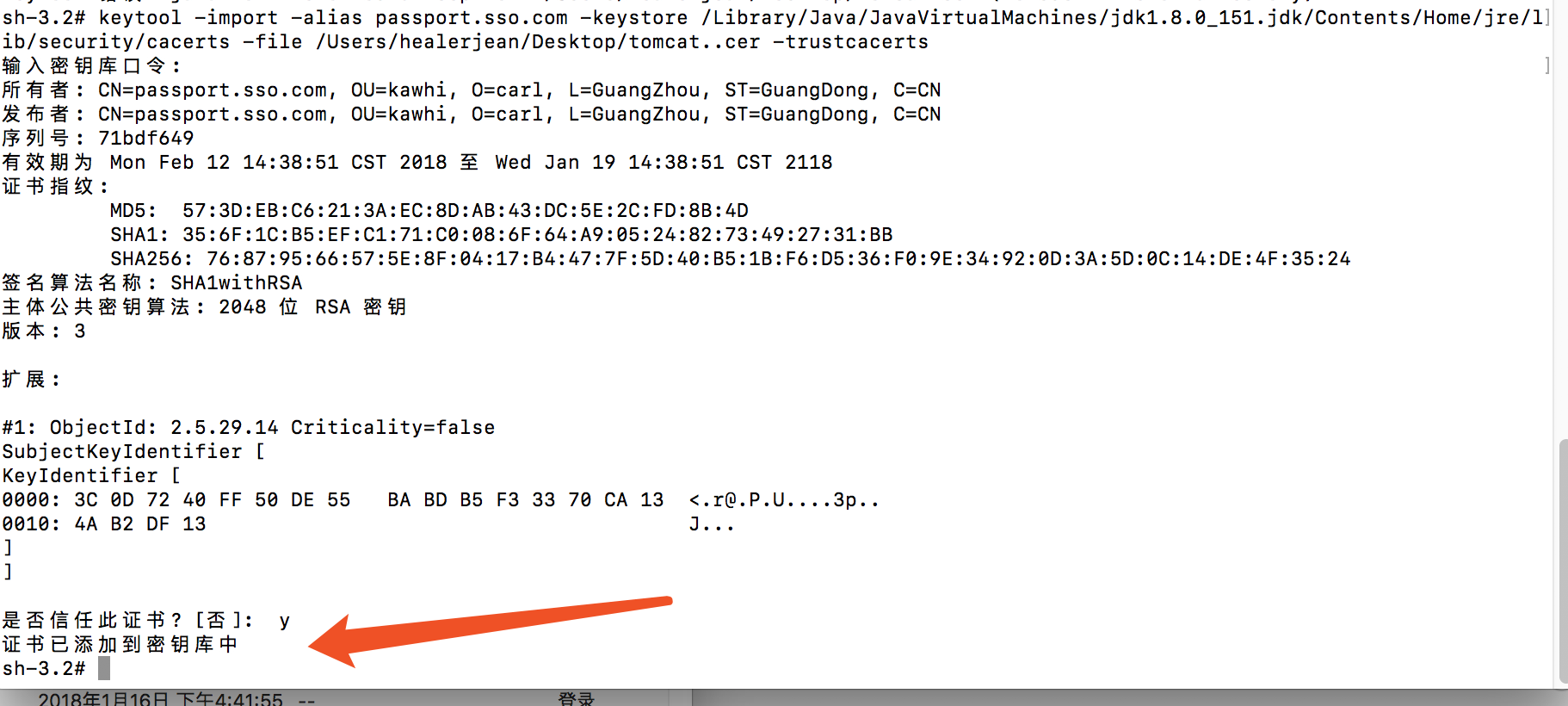


# 3、导入cacerts证书库

## 输入密码为 changeit并同意导入

### keytool -import -alias passport.sso.com -keystore /Library/Java/JavaVirtualMachines/jdk1.8.0\_151.jdk/Contents/Home/jre/lib/security/cacerts -file /Users/healerjean/Desktop/tomcat.cer -trustcacerts

家里的mac的jdk为jdk1.8.0\_131.jdk



keytool -list -keystore "/Library/Java/JavaVirtualMachines/jdk1.8.0\_151.jdk/Contents/Home/jre/lib/security/cacerts " | find/i server

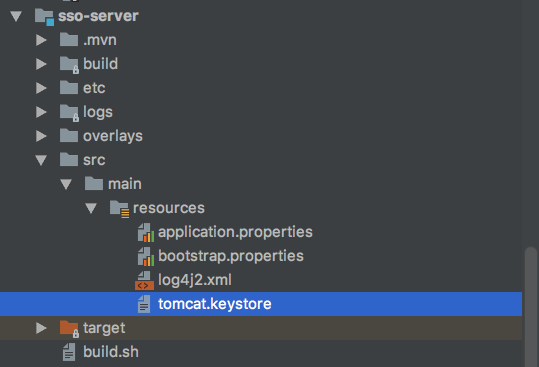
# 4、项目设置

## 1、证书有了，我们必须让项目识别证书，并且把ssl开关打开，再sso-config 中的ss0-dev-properties 打开，同时添加证书配置

server.ssl.enabled=true

server.ssl.key-store=classpath:tomcat.keystore  
server.ssl.key-store-password=123456  
server.ssl.keyAlias=passport.sso.com  
#SSL配置

## 2、密钥引用，把tomcat.keystore拷贝到sso-server\src\main\resources下



## 3、host文件中添加url 安全链接

# cas 单点登录

127.0.0.1 passport.sso.com

~

~

~

## 4、重新启动sso-config 和sso-server,浏览器访问，

