**一、生成证书**  
1、确保jdk环境配置成功后，win+r 输入cmd进入命令行窗口  
2、创建密钥：

keytool -genkey -alias server -keyalg RSA -validity 36500 -keystore D:\keys\server.keystore -ext san=ip:192.168.1.111,ip:127.0.0.1,dns:localhost -storepass 123456

行业标准格式 PKCS12写法：

keytool -importkeystore -srckeystore D:\keys\server.keystore -destkeystore

D:\keys\server.keystore -deststoretype pkcs12

[-alias]：指定密钥的别名，该别名是公开的

[-keyalg]： 指定密钥的算法，如：RSA、DSA（如果不指定默认采用DSA）)

[-validity]：指定创建的证书有效期多少天

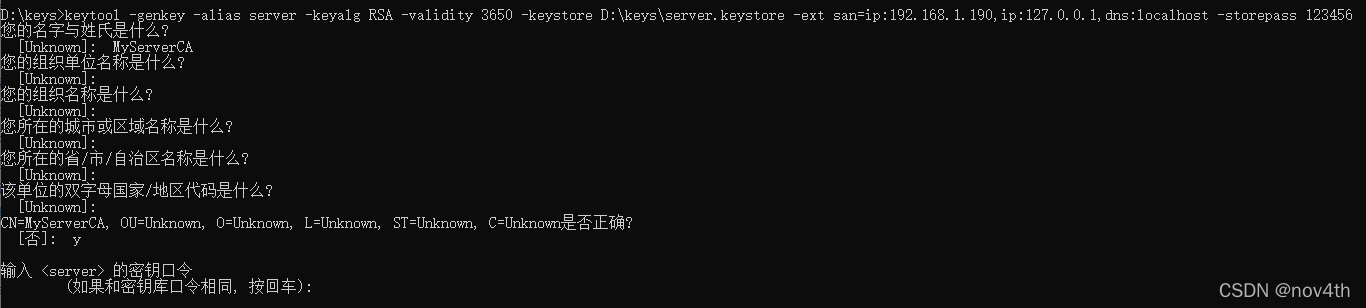
[-keystore]：密钥的存放路径及文件名

[-ext san=ip:] ：安装证书后，通过这个IP进行访问不会提示不安全，多个IP使用[,]分隔

[-ext san=dns:] ：安装证书后，通过这个域名进行访问不会提示不安全，多个域名使用[,]分隔

[-storepass]：密码

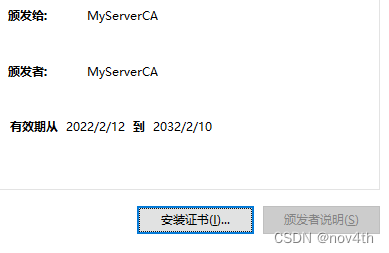
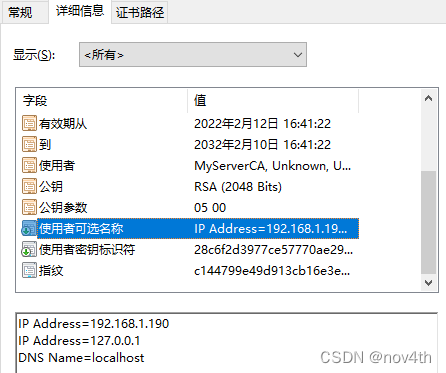
如果指令中包含 [-ext san=ip:] 或 [-ext san=dns:] 那么名字与姓氏填什么就无所谓，不包含的话这个位置需要填写IP或域名，其他内容的可以随便填



3、生成证书，证书创建成功后右键选择安装证书，将证书安装在本地计算机的[受信任的根证书颁发机构]中

keytool -export -alias server -file D:\keys\server.crt -keystore D:\keys\server.keystore -storepass 123456

双击生成的server.crt证书

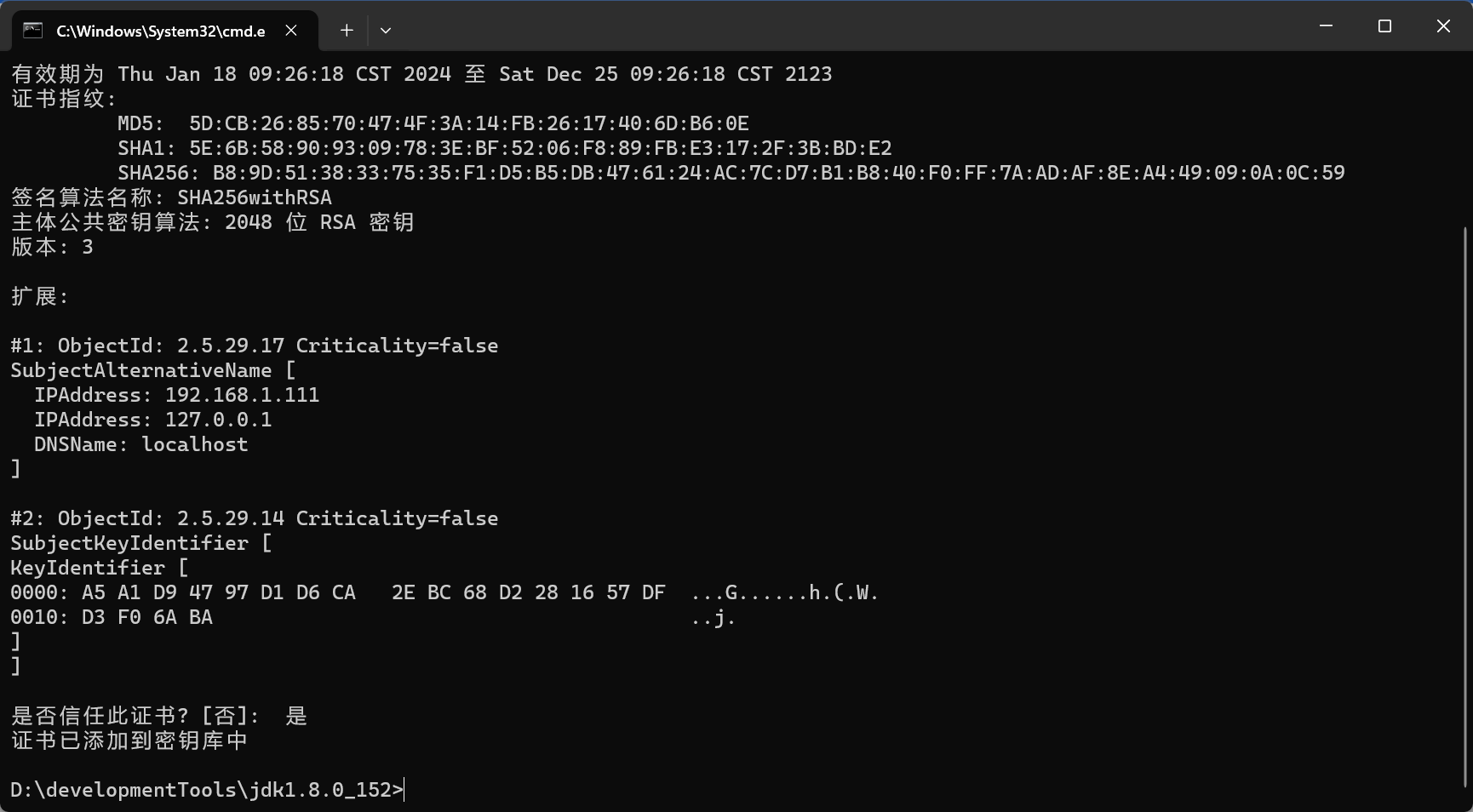
 

**二、导入证书到信任库中**

1、cmd进入jdk的\jre\lib\security目录（C:\Program Files\Java\jdk1.8.0\_221\jre\lib\security）  
2、输入：

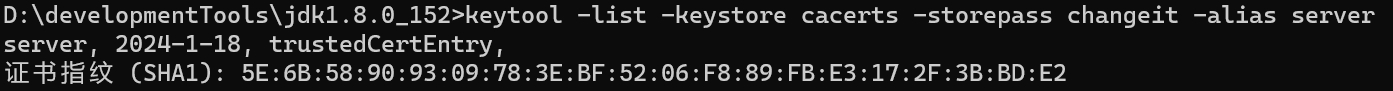
keytool -import -alias server -keystore cacerts -file D:\keys\server.crt -storepass changeit

-file：crt证书存储目录  
-storepass：证书库默认密码：changeit



查找密钥库是否存在指定项：

keytool -list -keystore cacerts -storepass changeit -alias server



删除密钥库指定项：

keytool -delete -keystore cacerts -storepass changeit -alias server

**三、SpringBoot中配置**[**ssl证书**](https://so.csdn.net/so/search?q=ssl%E8%AF%81%E4%B9%A6&spm=1001.2101.3001.7020)

1、将生成出来的密钥文件放在resources目录中  
2、配置application.yml文件

ssl:

key-store: classpath:server.keystore

key-store-password: 123456

key-store-type: JKS

key-alias: server

配置application. properties文件

server.ssl.key-store=classpath:server.keystore

server.ssl.key-store-password=123456

server.ssl.key-store-type=JKS

server.ssl.key-alias=server

3、编译后可能出现文件异常或无法编译到target\class中，建议在pom.xml中添加过滤

<resources>

<resource>

<directory>src/main/resources</directory>

<filtering>true</filtering>

<excludes>

<exclude>\*\*/\*.keystore</exclude>

</excludes>

</resource>

<resource>

<directory>src/main/resources</directory>

<filtering>false</filtering>

<includes>

<include>\*\*/\*.keystore</include>

</includes>

</resource>

</resources>

**解决自签证书不受信任导致报错的问题**

在客户端向服务器发送https请求时，会验证服务端的证书状态，自签证书不受信任就会报以下异常

javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target

解决方法：通过keytools将自签证书导入到java受信证书文件中（见第二步）