# HTTPS证书的使用

HTTPS是以安全为目标的 HTTP 通道，在HTTP的基础上通过传输加密和[身份认证](https://baike.baidu.com/item/%E8%BA%AB%E4%BB%BD%E8%AE%A4%E8%AF%81/5294713)保证了传输过程的安全性 。HTTPS 在HTTP 的基础下加入[SSL](https://baike.baidu.com/item/SSL/320778) 层，HTTPS 的安全基础是 SSL，因此加密就需要 SSL证书。

SSL证书是用于在Web服务器与浏览器以及客户端之间建立加密链接的加密技术，通过配置和应用SSL证书来启用HTTPS协议，来保证互联网数据传输的安全。

## 1 Keytool工具

通过JDK自带工具keytool就可以生成证书，运行keytool时需要以管理员权限的方式运行。下面是keytool命令的所有参数：

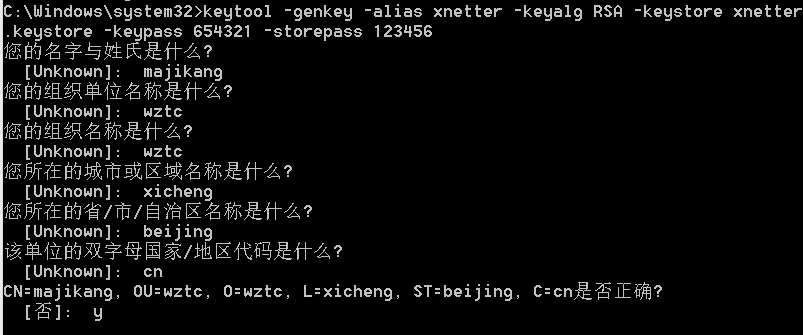


## 2 证书的生成

通过keytool生成的证书包括公钥和私钥，由认证端使用。默认的生成路径为命令行的当前路径，如下面命令的当前路径为C:\Windows\System32 或C:\Windows\SysWOW64。

**执行命令，生成证书:**

keytool -genkey -alias xnetter -keyalg RSA -keystore xnetter.keystore -keypass 654321 -storepass 123456

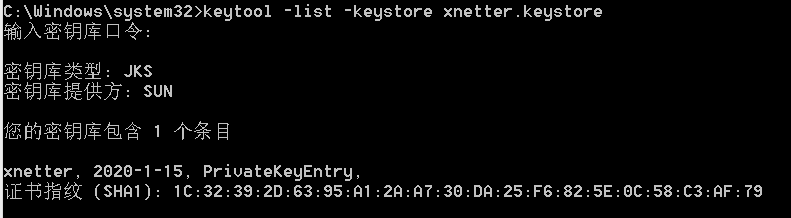


**生成证书时，也可以通过简便命令：**

keytool -genkey -alias xnetter -keyalg RSA -keystore xnetter.keystore -keypass 654321 -storepass 123456 –dname “CN=majikang, OU=wztc, O=wztc, L=xicheng, ST=beijing, C=cn”

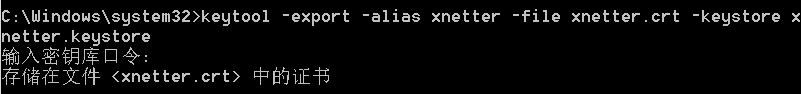
## 3 证书的查看

执行命令keytool -list -keystore xnetter.keystore，就可以查看证书。但是需要输入生成证书时的storepass，在这里是输入123456。



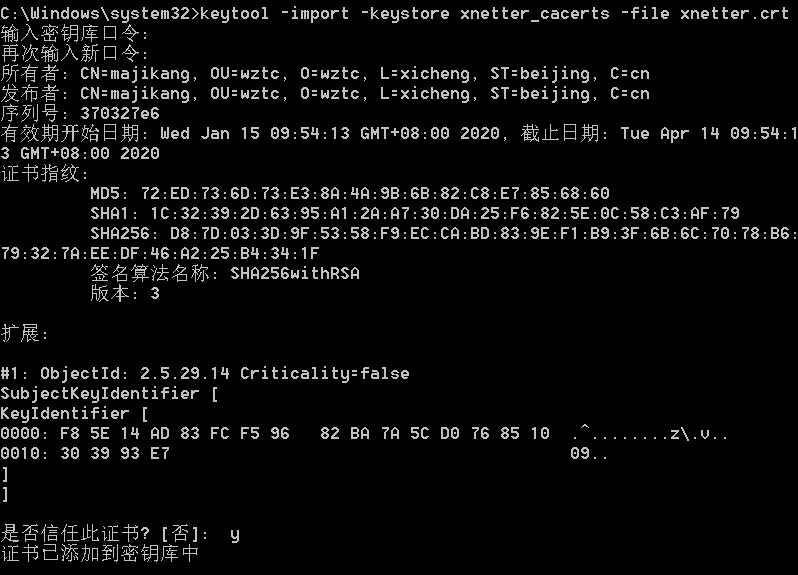
## 4 导出到证书文件

将名为xnetter.keystore的证书库中别名为xnetter的证书条目导出到证书文件xnetter.crt中。**导出命令**： keytool -export -alias xnetter -file xnetter.crt -keystore xnetter.keystore。得到的xnetter.crt是可信任的证书实体，只包含公钥。



## 5 导入证书文件

将证书文件xnetter.crt导入到名为xnetter\_cacerts的证书库中。**导入命令**：keytool -import -keystore xnetter\_cacerts -file xnetter.crt。输入密钥库口令时，使用的是123456。导入后，如果想查看证书的内容，可以用keytool -printcert –file xnetter.crt来查看。



## 6 浏览器导入证书

这里以Chrome为例。点击弹出菜单的”安全”按钮。然后按照下面步骤，就可以导入xnetter.crt证书了。

