# CA证书操作手册

## 生成证书

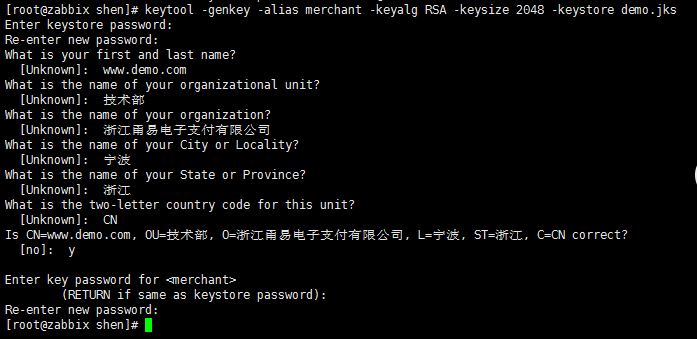
首先保证系统（linux或windows均可）中已安装高于1.4的jdk版本，利用Java的keytool工具输入下列命令来生成证书：

命令第一步：

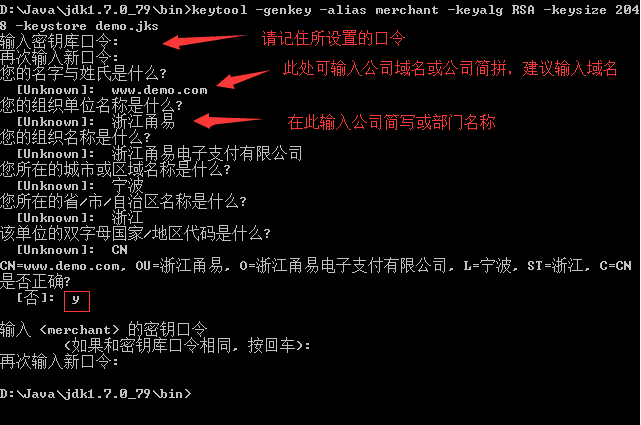
keytool -genkey -alias merchant -keyalg RSA -keysize 2048 -keystore demo.jks（证书名可自定义）

注：window系统需切换至jdk的bin目录

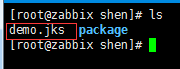
Linux：



Windows：



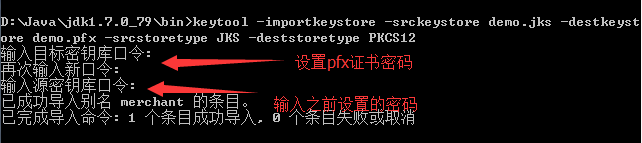
此时将在当前路径下生成创建成功的jks文件



然后输入下列命令将其转换成pfx证书文件：

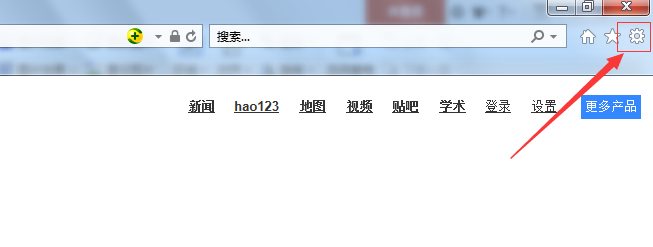
命令第二步：

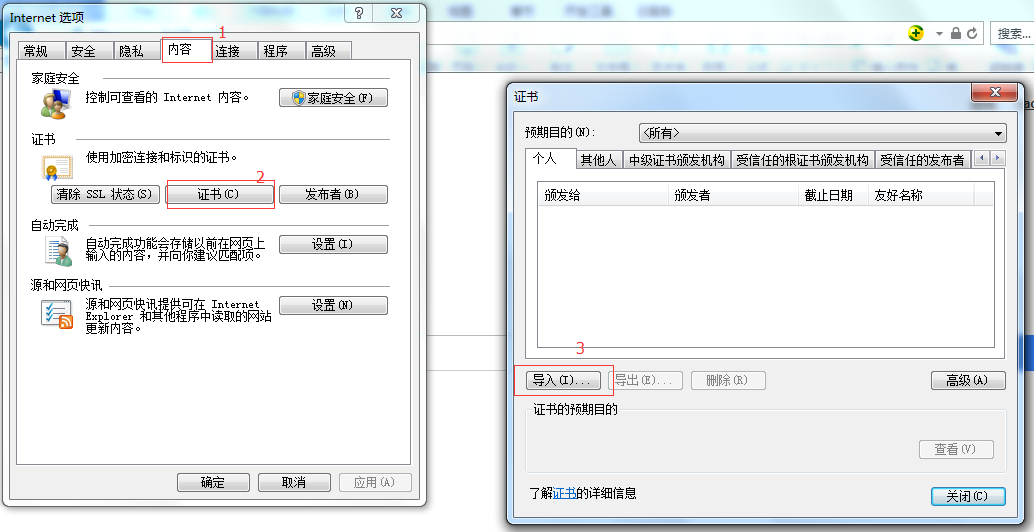
keytool -importkeystore -srckeystore demo.jks -destkeystore demo.pfx -srcstoretype JKS -deststoretype PKCS12(pfx证书名可自定义)



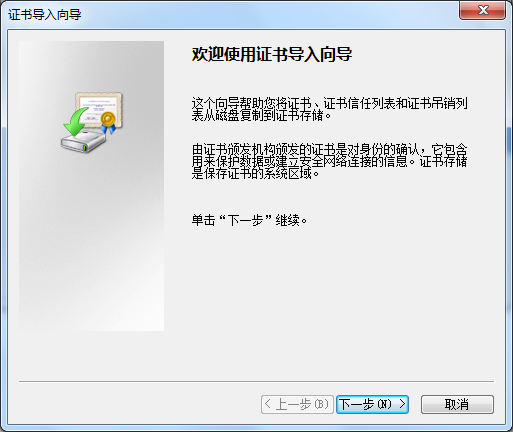
## 私钥导入

选择浏览器中的工具，依次点击Internet选项--->内容--->证书--->导入

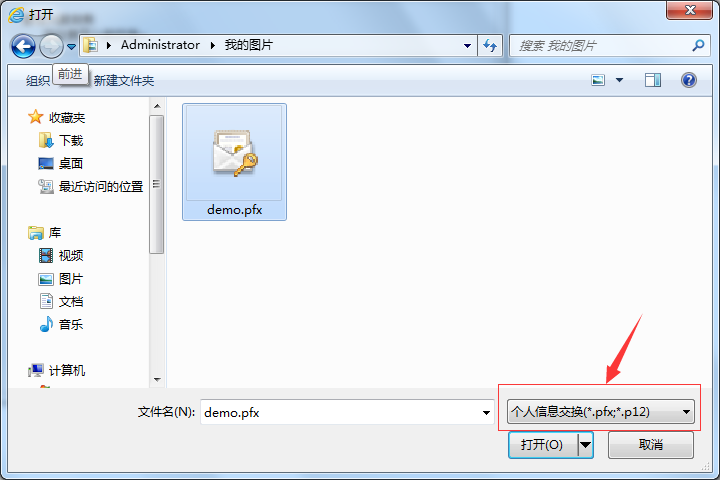




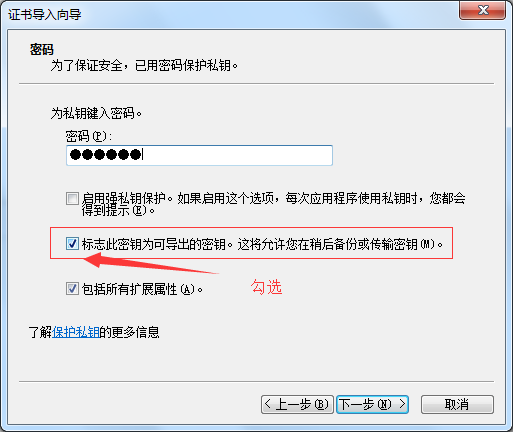
跳出证书导入向导对话框后，根据提示点击下一步



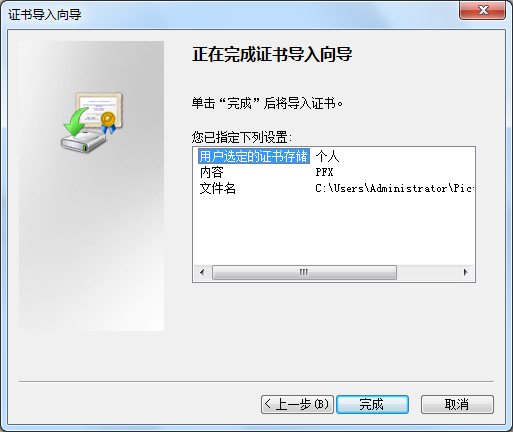
选择“浏览”--->格式修改为“个人信息交换-PKCS #12(.PFX)(P)”找到生成的证书文件，选择打开--->下一步



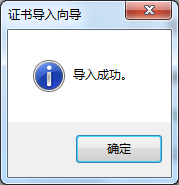
输入之前设置的证书口令，勾选第二选项--->下一步--->下一步





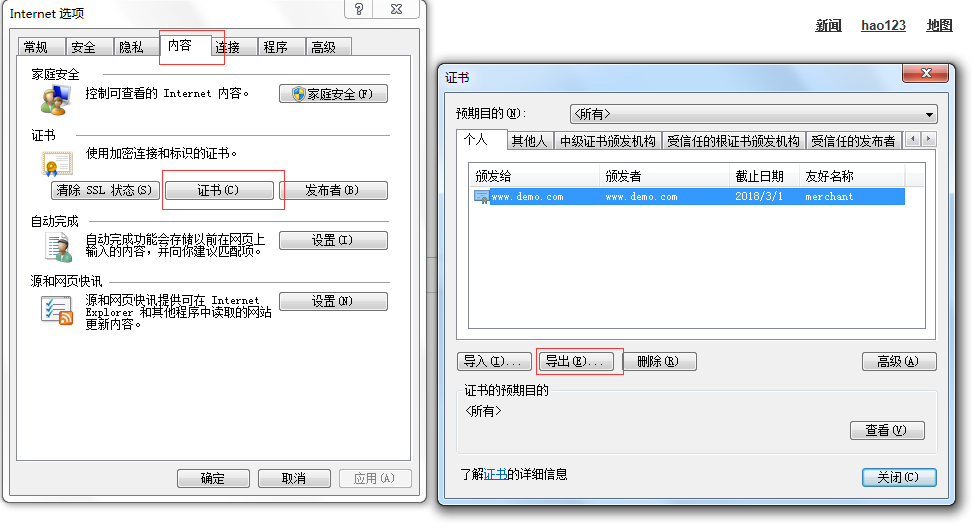
确认设置后，点击完成

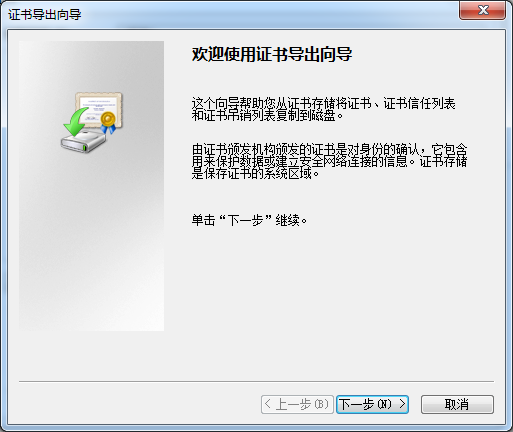
点击确定，私钥证书导出完成。



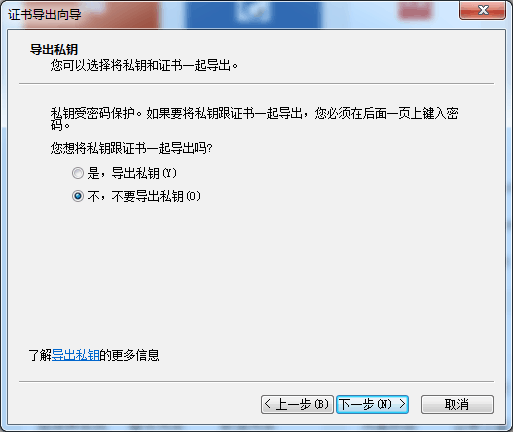
## 公钥导出

选择浏览器中的工具，依次点击Internet选项--->内容--->证书--->导出

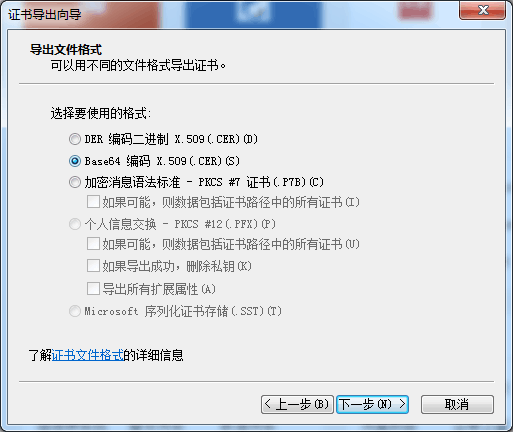


跳出证书导出向导对话框后，根据提示点击下一步

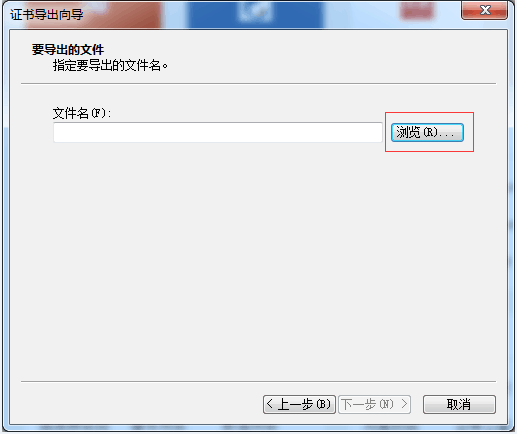
选择“不，不要导出私钥”

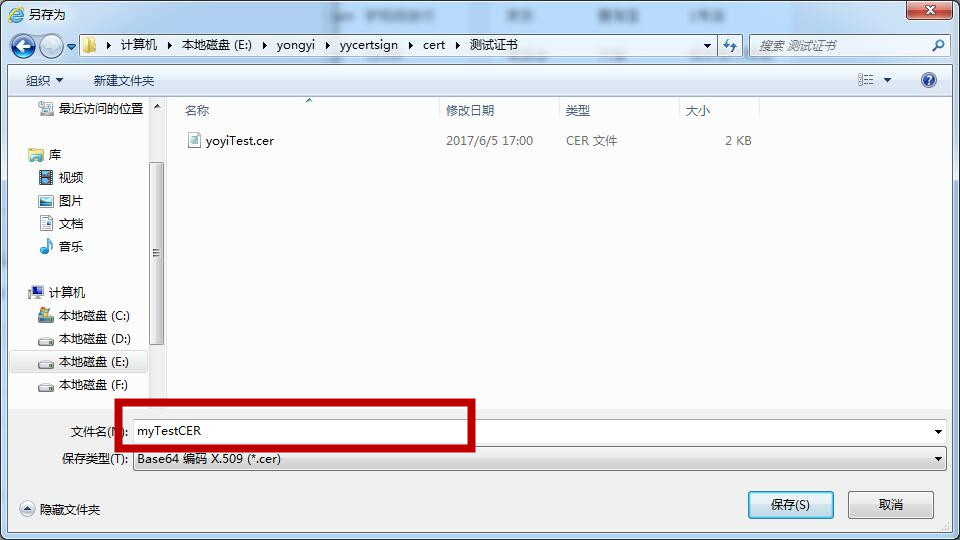


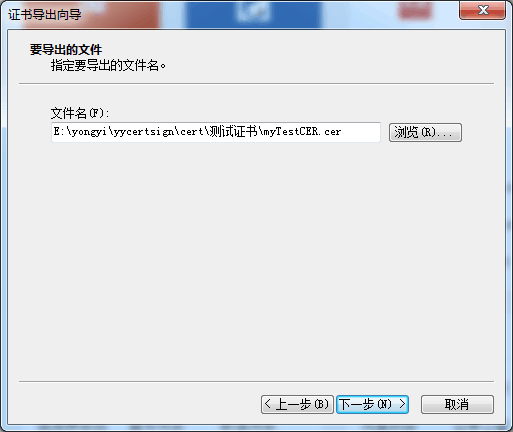
选择Base64编码 X.509(.CER)(S)---> 下一步



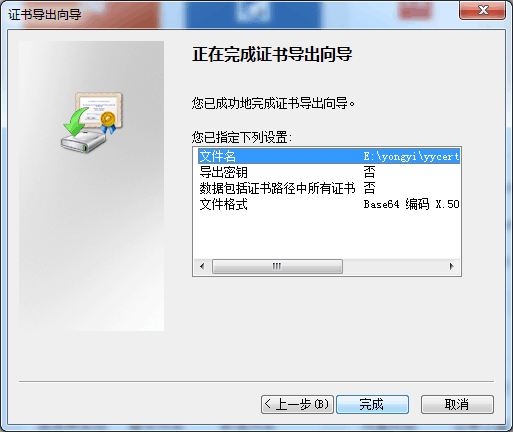
点击浏览选择想要保存证书的路径及文件名--->下一步







点击完成



点击确定，公钥证书导出完成。

