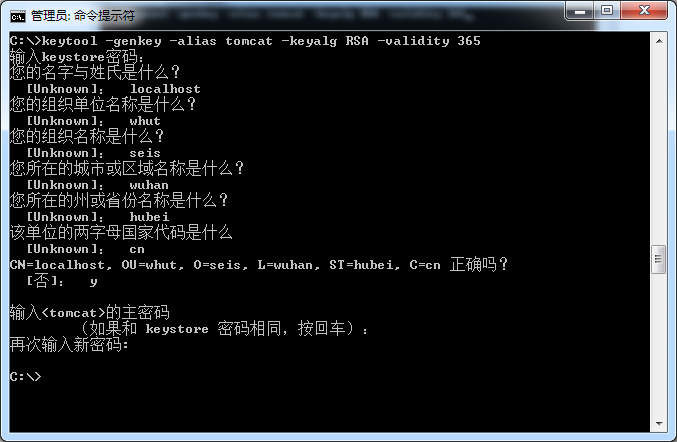
1. 打开命令行，建议在c盘根目录操作：

keytool -genkey -alias tomcat -keyalg RSA -validity 365

如果已经存在tomcat别名，可以删除操作：

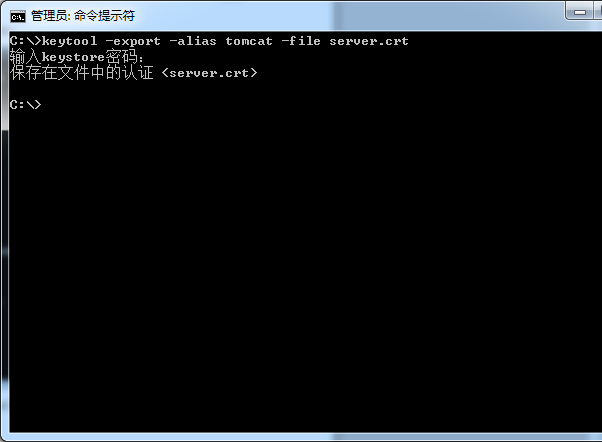
keytool -delete -alias tomcat -keyalg RSA



注意：“名字与姓氏”填写：localhost，否则cas client在验证的时候会报localhost no match错误，密码默认是:changeit

1. 证书导出保存

keytool -export -alias tomcat -file server.crt



密码：changeit

1. 证书导入到jdk

keytool -import -file localhost.crt -keystore "C:/Program Files (x86)/Java/jdk1.6.0\_43/jre/lib/security/cacerts" -alias cas



密码：changeit

Jdk路径根据自己电脑情况调整，默认情况“C:/Program Files (x86)/Java/jdk1.6.0\_43”

1. Tomcat配置

（1）打开tomcat的conf目录server.xml配置文件，将下面配置的注释去掉：

<!--

  <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"

             maxThreads="150" scheme="https" secure="true"

             clientAuth="false" sslProtocol="TLS" />

-->

即删除 <!—和 -->

（2）注意，如果是两个tomcat进行测试，需要修改这里的8443端口，避免连个tomcat的端口占用冲突

1. 部署cas-server
2. 将cas.war拷贝到tomcat的webapp目录，启动tomcat
3. 通过浏览器访问 <https://localhost:8443/cas>即可以访问服务，注意端口
4. 查看cert store中已经安装的证书

keytool -list -v -keystore "%JAVA\_HOME%/jre/lib/security/cacerts" -alias tomcat -storepass changeit

keytool -export -keystore "C:/Program Files (x86)/Java/jdk1.6.0\_43/jre/lib/security/cacerts" -alias tomcat -*storepass* changeit

keytool -genkeypair -alias "cas" -keyalg "RSA" -keystore cas.keystore

keytool -import -file localhost.crt -keystore "C:/Program Files (x86)/Java/jdk1.6.0\_43/jre/lib/security/cacerts" -alias cas