



最后更新时间: 2010年12月7日

软件版本号: windows xp sp3
orion2.0.5 jdk1.6 jre1.6

服务器证书安装配置指南系列之

Orion 服务器证书安装配置指南

www.cnnic.cn

中国互联网络信息中心 (CNNIC)

地址: 北京中关村南四街四号中国科学院软件园1号楼一层

7*24小时客户服务咨询电话: 86-10-58813000

传真: 86-10-58812666

邮政地址: 北京349信箱6分箱 CNNIC

邮政编码: 100190

目录

1.	关于 keytool.....	3
1.1	keytool 简介.....	3
1.2	keytool 下载及安装.....	3
2.	生成证书请求文件.....	3
2.1	生成私钥.....	3
2.2	生成 csr 请求文件.....	4
3.	下载服务器证书.....	6
3.1	准备下载证书所需信息.....	6
3.2	下载证书.....	6
4.	安装根证书和服务器证书.....	10
4.1	下载根证书及 CNNIC 中级根证书.....	10
4.2	将根证书 root.cer 导入到 keystore 文件.....	10
4.3	将中级 CA 证书 cnic.cer 导入到 keystore 文件.....	11
4.4	将服务器证书 m1.cnic.cn.cer 导入到 keystore 文件.....	13
4.5	查看 keystore 证书.....	13
5.	修改配置配置文件	
5.1	修改 conf 下文件.....	14
5.2	修改 server.xml.....	15
6.	备份服务器证书.....	16

图表目录

图表一	创建私钥.....	4
图表二	生成 csr 文件.....	5
图表三	查看 csr 文件.....	6
图表四	可信服务器证书下载页面.....	7
图表五	填入收到的参考号和授权码以及生成的 csr.....	8
图表六	生成证书.....	9
图表七	格式转换.....	9

图表八 证书导出向导.....	10
图表九 导入根证书.....	11
图表十 导入中级根证书.....	12
图表十一 导入服务器证书.....	13
图表十二 查看 keystore 证书.....	14

1. 关于 keytool

1) keytool 简介

keytool 是用于管理密钥和证书的工具，使用户和管理员能管理自己的公/私钥对以及相关的证书。keytool 将密钥和证书储存到一个 keystore 类型的文件，该文件使用一个密码保护密钥。

2) keytool 下载及安装

请登录 sun 的网站 <http://java.sun.com/javase/downloads/index.jsp> 下载 java 开发包 (JDK)。JDK 中默认安装有 keytool。安装完成后，请配置系统环境变量 JAVA_HOME, 指明 JDK 的安装位置。

2. 生成证书请求文件 CSR

请确保 JAVA_HOME\bin 或者 JRE_HOME\bin 目录存在于 PATH 变量中或直接使用绝对路径调用 keytool 命令。直接使用 keytool 创建证书请求文件需要以下两个步骤：

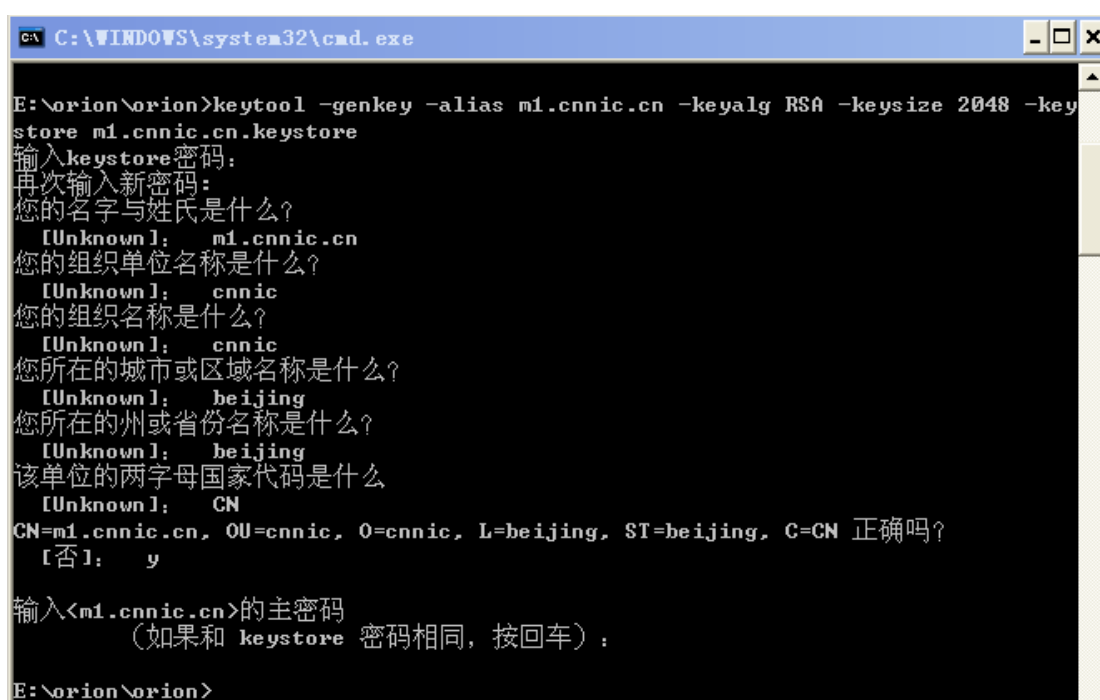
1) 生成私钥

命令格式：`keytool -genkey -alias [alias_name] -keyalg RSA -keysize 2048 -keystore [keystore_name]`

注：[]中的内容为需要输入的参数

- `alias_name`：表示证书的别名
- `keystore_name`：表示证书的密钥库文件名，扩展名一般为 `keystore`

以申请域名 ml.cnnic.cn 的证书请求文件为例，运行情况如下图所示：



```
C:\WINDOWS\system32\cmd.exe
E:\orion\orion>keytool -genkey -alias ml.cnnic.cn -keyalg RSA -keysize 2048 -keystore ml.cnnic.cn.keystore
输入keystore密码:
再次输入新密码:
您的名字与姓氏是什么?
[Unknown]: ml.cnnic.cn
您的组织单位名称是什么?
[Unknown]: cnnic
您的组织名称是什么?
[Unknown]: cnnic
您所在的城市或区域名称是什么?
[Unknown]: beijing
您所在的州或省份名称是什么?
[Unknown]: beijing
该单位的两字母国家代码是什么
[Unknown]: CN
CN=ml.cnnic.cn, OU=cnnic, O=cnnic, L=beijing, ST=beijing, C=CN 正确吗?
[否]: y
输入<ml.cnnic.cn>的主密码
(如果和 keystore 密码相同, 按回车):
E:\orion\orion>
```

图表一 创建私钥

系统提示输入 `keystore` 密码，如不输入密码直接回车则缺省密码为：`changeit`。也可以指定一个新的密码，但一定保存好该密码。

系统提示输入“您的名字与姓氏？”，请输入您要申请域名证书的域名，而不是您的真实名称与姓氏；例如：如果需要为 `www.domain.cn` 申请域名证书就必须输入 `www.domain.cn` 而不能输入 `domain.cn`。通配域名证书请填写通配域名；多域名证书仅需要填写第一个域名名称即；

关于组织单位名称、组织名称、所在城市、所在省份和国家缩写(中国填：CN，其他国家填其缩写)，除国家缩写必须填 CN 外，其余信息均可以是英文或中文。最后，系统要求输入主密码，可以直接回车，使主密码保持与 keystore 密码一致。

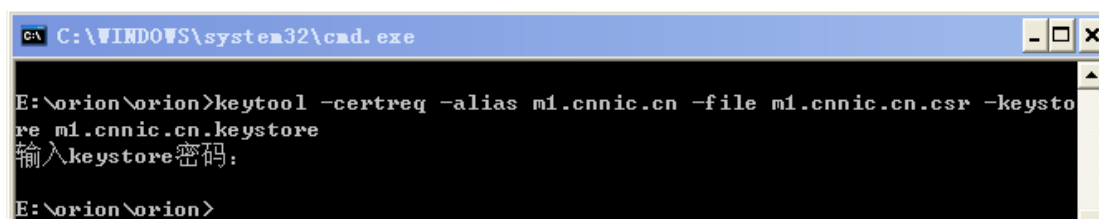
2) 生成 CSR 证书请求文件

命令格式：`keytool -certreq -alias [alias_name] -file [csr_name] -keystore [keystore name]`

注：[] 中的内容为需要输入的参数

- `alias_name`：表示证书的别名
- `csr_name`：表示证书请求文件的名称，扩展名一般为 `csr`
- `keystore_name`：表示证书的密钥库文件名，扩展名一般为 `keystore`

使用上例生成的 keystore 文件，运行情况如下图所示：

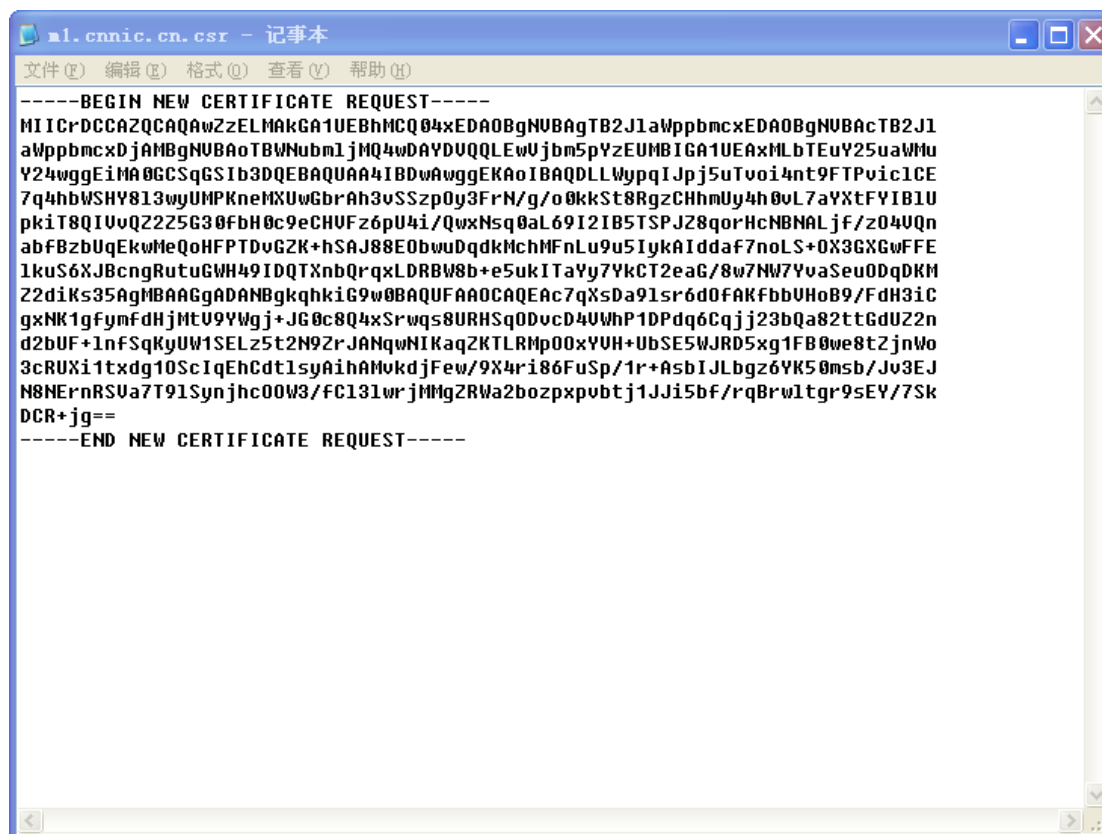


```
C:\WINDOWS\system32\cmd.exe
E:\orion\orion>keytool -certreq -alias m1.cnnic.cn -file m1.cnnic.cn.csr -keystore m1.cnnic.cn.keystore
输入keystore密码:
E:\orion\orion>
```

图表二 生成 csr 文件

系统要求输入第一步骤中填写的 keystore 密码。

生成的 csr 文件为文本文件，可以使用记事本等文本查看工具打开刚刚生成的证书请求文件，如下图所示：



图表三 查看 csr 文件

3. 下载服务器证书

1) 准备下载证书所需信息

参考号与授权码：参考号与授权码是下载证书的密码凭证。当申请的证书通过审核时，用户将接收到由 CNNIC 发送的通过审批的电子邮件通知，该邮件中含有 16 位的参考号与授权码信息，其中参考号与授权码的前 13 位为明文显示，后 3 位为密文显示。审核员会以邮件通知的方式发送后三位的明文显示。

2) 下载证书

登录 CNNIC 可信网络服务中心网页

http://www.cnnic.cn/jczyfw/wzws/xz/201010/t20101027_16322.html

点击页面中部的“可信服务器证书下载”图片链接进入到证书下载页面，如下图所示：

可信服务器证书下载	
点击这里进行在线CSR校验	
参考号：	<input type="text"/>
授权码：	<input type="text"/>
证书请求文件（CSR）：	<p>请把整个CSR文件中 -----BEGIN CERTIFICATE REQUEST----- 和 -----END CERTIFICATE REQUEST----- 之间的内容复制到下边的输入框中</p> <div style="border: 1px solid #ccc; height: 200px; width: 100%;"></div>
<input type="button" value="提交"/> <input type="button" value="重置"/>	

图表四 可信服务器证书下载页面

根据网页上的提示输入“参考号”和“授权码”，将证书请求文件中除去头尾“-----BEGIN NEW CERTIFICATE REQUEST-----”和“-----END NEW CERTIFICATE REQUEST-----”的中间部分内容复制到 CSR 文本框中。结果如下所示：

可信服务器证书下载

[点击这里进行在线CSR校验](#)

参考号：	<input type="text" value="MV4K646JDDHAF6W5"/>
授权码：	<input type="text" value="CJQLNDB7FQSVEJA3"/>

请把整个CSR文件中
-----BEGIN CERTIFICATE REQUEST-----
和
-----END CERTIFICATE REQUEST-----
之间的内容复制到下边的输入框中

```

MIICrDCCAQCAQAwZzELMAkGA1UEBhMCQ04xEDAOBgNVBAGTB2JlaWppbmcxEDAOBgNVBACTB2JlaWppbmcxDjAMBGNVBAoTBWVubmljMQ4wDAYDVQQLEwVjbm5pYzEUMBIGA1UEAxMLbTEuY25uaWUy24wggEiMAOGCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQcwZKe5sIA8Vv7uYleWQMUVOs7K/dagHhyb9DYKOUOSQqJkHsFzAMUzzyjL
kvE2tUTNtMqbpAxV8TGSg+AcC7zNABYdQpAUWw91dGoLqGtktOsQ/tWdOBh10j
8amCi/yRxpPSPJPrLisBFCxwt+8wGj8WICj3vP8jOqnpUtkfx3S9AMfaAveGret
lUF/80DBboVwJXCTKwWC+dHykjsiswAOiWYlgnArdexnigr4Ym59IjIjFmOfiiBSK
bGwVlNXJ21f6DsLFKf8JvZq9Yfdjc135QQPOpzGhR98TKzStv/6/c+ocG2yexgft
Mzac/Z41Jh9iUmNkp69nbs1sHU5FAGMBAAGGADANBgkqhkiG9wOBAQUFAAOCAQEA
qGbSxekMJTPsS7VHuP1YzpkOaxN3D3AAyOoT7MC3pEDnlk49e779Vxr2B13nFbh1
                    
```

图表五 填入收到的参考号和授权码以及生成的 csr

点击“下载”，如果参考号、授权码和 CSR 均无问题，则显示页面如下所示。

证书下载-证书生成

证书文件：

```

-----BEGIN CERTIFICATE-----
MIIEGzCCAwwGAWIBAgIQEMCXznvJBxWzS5X3sUEd6DANBgkqhkiG9wOBAQUFAADAAyMQswCQYDVQQG
EwJjbjEOMAwGA1UEChMFY25uaWUxZzEzARBgNVBAMTCmNubmljIHJvb3QwHhcNMjAxMjA3MDkzOTAw
WhcNMTEwMjA3MDkzOTAwWjBhMQswCQYDVQQGEwJDTjENMASGA1UECB4EUXdOrDENMASGA1UEBx4E
UxdOrDEOMAwGA1UEChMFY25uaWUxZzEzARBgNVBAsTBWVubmljMRQwEgYDVQQDEwttNS5jbm5pYy5j
bjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALBkp7mWgDxW/u5iV5ZAxRU5Lsr91qAe
HJvONgo645JComQewXMAxRnPKMuS8Ta1RM20ypSDFXxMZIb4BwLVMQAHJ1CkBRbD3VOaguoA2R2
06xD+1Z3QFuLU6PxxqYKL/JHGSk9I8k+suKwEULHC37zAaPxxYgKPe8/yM6qe1S2R/HdL0Ax9oC94a
t62VQX/zQMFuhXAlcJMrDBz50fKSOyKzAA6JZiWCCt17GfWBHhibnOiOIWY5+KIFIpsbBWU1cnb
V/oOwsUp/wm9mr1h92NyXf1BA86nMaFH3xMrNJO//r9z6hwbbJ7GAW0xlpz9niUmH2JSY2Snr2du
                    
```

Web服务器证书请将证书编码框中的内容拷贝，并粘贴到文本中，保存成Web服务器能够识别的格式。

图表六 生成证书

请按页面提示保存，文件名保存为 ml.cnnic.cn.cer。该文件即为申请的证书，如果该证书丢失，就必须进行证书补办。

注意：关于证书的格式转换

从 CNNIC 获得的证书格式为 X509 格式。该将证书文件的扩展名由 txt 改为 cer 或 crt 后，可在 windows 中双击打开查看证书的相关信息。显示信息类似下图所示：



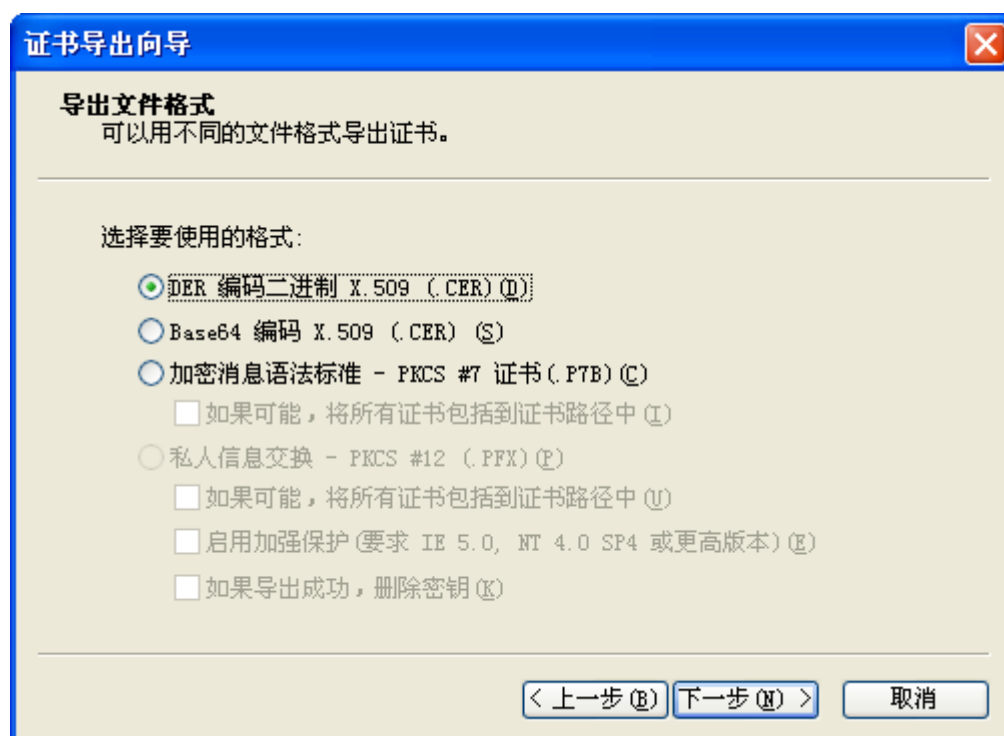
图表七 格式转换

X509 格式的证书利用 windows 提供的图形界面操作工具可以另存为以下两种编码格式：

- BASE64 编码格式：该格式的证书可以用记事本打开
- DER 编码格式：二进制格式

在上图中，点击“详细信息”->“复制到文件”后，即可以根据提示点击“下

一步”利用证书导出向导导出需要格式的证书，如下图所示：



图表八 证书导出向导

4. 安装根证书和服务器证书

1) 下载根证书及CNNIC中级根证书

下载地址：

快速证书：http://www.cnnic.cn/jczyfw/wzws/ksym/ksxz/201105/t20110524_21055.html

标准证书：http://www.cnnic.cn/jczyfw/wzws/bzcx/xz/201010/t20101027_16322.html

EV证书：<http://www.cnnic.cn/jczyfw/wzws/kxEV/xz/>

将 CNNIC 中级根证书文件名保存为“CNNIC.cer”，将根证书文件名保存为“root.cer”（本例用的测试根证书，名为 roottest.cer）。

2) 将根证书 root.cer 导入到 Keystore 文件

命令格式：**keytool -import -trustcacerts -alias root -file root.cer -keystore**

[keystore_name]

注：[]中的内容为需要输入的参数

- **keystore_name**：表示保存证书私钥的文件名，扩展名一般为 keystore

```

C:\WINDOWS\system32\cmd.exe

E:\orion\orion>keytool -import -trustcacerts -alias roottest -file roottest.cer
-keystore m1.cnnic.cn.keystore
输入keystore密码:
所有者:CN=cnnic root, O=cnnic, C=cn
签发人:CN=cnnic root, O=cnnic, C=cn
序列号:349c0001
有效期: Sat Apr 28 14:53:54 CST 2007 至Wed Apr 28 14:53:54 CST 2027
证书指纹:
    MD5:12:3F:2F:19:D3:0F:35:6A:55:C4:68:63:55:D8:72:7E
    SHA1:92:D6:C4:DC:BD:89:EB:3B:A9:F7:63:F2:46:59:5E:1B:7A:68:A9:45
    签名算法名称:SHA1withRSA
    版本: 3

扩展:

#1: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#2: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
  DigitalSignature
  Non_repudiation
  Key_Encipherment
  Data_Encipherment
  Key_Agreement
  Key_CertSign
  Cr1_Sign
]

#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
  KeyIdentifier [
    0000: FF 68 78 A7 CF BA B4 3B 72 25 8D AA D0 5B A5 F4 .hx....;r%...[...
    0010: 90 D0 F4 BF .....
  ]
]

#4: ObjectId: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
  SSL CA
  S/MIME CA
  Object Signing CA]

#5: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
  KeyIdentifier [
    0000: FF 68 78 A7 CF BA B4 3B 72 25 8D AA D0 5B A5 F4 .hx....;r%...[...
    0010: 90 D0 F4 BF .....
  ]
]

信任这个认证? [否]: y
认证已添加至keystore中

E:\orion\orion>

```

图表九 导入根证书

3) 将中级CA证书CNNIC.cer导入keystore文件

命令格式：**keytool -import -v -trustcacerts -storepass [password] -alias**

[ca_cert] -file CNNIC.cer -keystore [keystore_name]

注：[]中的内容为需要输入的参数

- password: 表示私钥的保护口令
- ca_cert: 表示中级 CA 证书文件名
- keystore_name: 表示保存证书私钥的文件名，扩展名一般为 keystore

```

C:\WINDOWS\system32\cmd.exe
E:\orion\orion>keytool -import -trustcacerts -alias cnnic -file cnnic.cer -key
ore m1.cnnic.cn.keystore
输入keystore密码:
所有者:CN=CNNIC SSL, O=CNNIC SSL, C=CN
签发人:CN=CNNIC ROOT, O=CNNIC, C=CN
序列号:49330029
有效期: Thu Jan 28 11:03:21 CST 2010 至Sun Apr 16 13:00:40 CST 2017
证书指纹:
    MD5:27:63:91:3F:CC:40:A4:54:33:EE:F6:BC:91:25:A7:86
    SHA1:D2:2D:35:F0:4B:55:40:7E:A3:DF:F1:7D:2A:96:CC:A3:59:AC:B8:02
    签名算法名称:SHA1withRSA
    版本: 3

扩展:
#1: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints: [
  CA:true
  PathLen:2147483647
]
#2: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
  Key_CertSign
  Crl_Sign
]
#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
  KeyIdentifier [
    0000: 45 00 BA 8A 18 90 51 C3   B1 CA F7 BC 65 39 2E 8C   E.....Q.....e9..
    0010: 56 90 44 30                               U.D0
  ]
]
#4: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
  [DistributionPoint:
    [CN=crl1, OU=crl, O=CNNIC, C=CN]
  ], DistributionPoint:
    [URIName: http://www.cnnic.cn/download/rootcrl/CRL1.crl]
]
  
```

```
#5: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
  [CertificatePolicyId: [1.3.6.1.4.1.29836.1.1]
  [PolicyQualifierInfo: [
    qualifierID: 1.3.6.1.5.5.7.2.1
    qualifier: 0000: 16 18 68 74 74 70 3A 2F 2F 77 77 77 2E 63 6E 6E ..http://w
ww.cnn
0010: 69 63 2E 63 6E 2F 63 70 73 2F ic.cn/cps/

]] ]
]

#6: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 65 F2 31 AD 2A F7 F7 DD 52 96 0A C7 02 C1 0E EF e.1.*...R.....
0010: A6 D5 3B 11 ...;
]
]

信任这个认证? [否]: y
认证已添加至keystore中

E:\orion\orion>
```

图表十 导入中级根证书

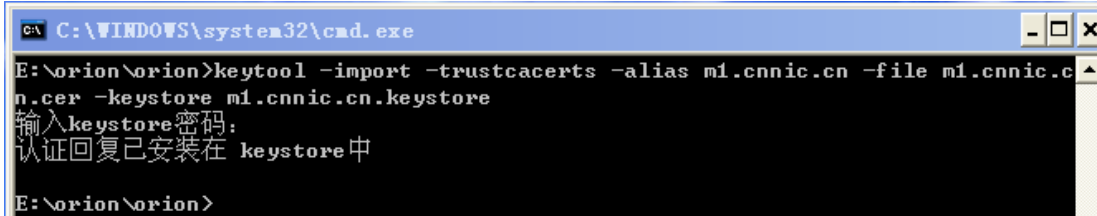
4) 将服务器证书m1.cnnic.cn.cer导入keystore文件

命令格式: **keytool -import -v -trustcacerts -storepass [password] -alias**

[alias_name] -file [server_cert] -keystore [keystore_name]

注: []中的内容为需要输入的参数

- password: 表示私钥的保护口令
- server_cert: 表示服务器证书文件名
- alias_name: 表示私钥的别名
- keystore_name: 表示证书密钥库的文件名, 扩展名一般为 keystore



```
C:\WINDOWS\system32\cmd.exe
E:\orion\orion>keytool -import -v -trustcacerts -alias m1.cnnic.cn -file m1.cnnic.c
n.cer -keystore m1.cnnic.cn.keystore
输入keystore密码:
认证回复已安装在 keystore中

E:\orion\orion>
```

图表十一 导入服务器证书

5) 查看keystore证书

命令格式: **keytool -list -keystore [keystore_name]**

注：[]中的内容为需要输入的参数

- keystore_name: 表示证书密钥库的文件名，扩展名一般为 keystore

```

C:\WINDOWS\system32\cmd.exe
E:\orion\orion>keytool -list -keystore m1.cnnic.cn.keystore
输入keystore密码:

Keystore 类型: JKS
Keystore 提供者: SUN

您的 keystore 包含 3 输入

cnnic, 2010-12-9, trustedCertEntry,
认证指纹 <MD5>: 27:63:91:3F:CC:40:A4:54:33:EE:F6:BC:91:25:A7:86
m1.cnnic.cn, 2010-12-9, PrivateKeyEntry,
认证指纹 <MD5>: CA:C2:29:E3:52:A0:2B:FC:7F:66:4B:24:C2:F3:EA:3A
roottest, 2010-12-9, trustedCertEntry,
认证指纹 <MD5>: 12:3F:2F:19:D3:0F:35:6A:55:C4:68:63:55:D8:72:7E

E:\orion\orion>

```

图表十二 查看 keystore 证书

5. 修改配置文件

1) 修改 conf 下文件

将 Orion 安装目录的 conf 文件夹下的 default-web-site.xml 复制一份，另存为 secure-web-site.xml，与 default-web-site.xml 放在相同路径下。用记事本打开 secure-web-site.xml 进行如下修改（粗体部分为需要增加内容），SSL 访问使用的端口不可使用与普通 HTTP 监听端口相同的端口号，因此本例中改为 8443

```

<?xml version="1.0"?>
<!DOCTYPE web-site PUBLIC "Orion Web-site" "http://www.orionserver.com/dtds/web-site.dtd">
<web-site host="[ALL]" port="8443" display-name="Default Orion WebSite" secure="true">
    <ssl-config keystore="e:\orion\orion\m1.cnnic.cn.keystore"
keystore-password="keystorePassword" />
    <!-- The default web-app for this site, bound to the root -->
    <default-web-app application="default" name="defaultWebApp" />
    <!-- Uncomment this to activate the news app -->
    <!-- <web-app application="news" name="news-web" root="/news" /> -->
    <!-- Access Log, where requests are logged to -->

```

```
<access-log path="../log/default-web-access.log" />
</web-site>
```

请检查和修改 keystoreFile 的路径是否正确和 keystore 密码是否正确，修改并保存配置文件。

2) 修改 server.xml

用记事本打开 config/server.xml 文件，将刚刚修改保存的 secure-web-site.xml 的路径配置入其中（参见粗体部分内容）

```
<?xml version="1.0"?>
<!DOCTYPE application-server PUBLIC "Orion Application Server Config"
"http://www.orionserver.com/dtds/application-server.dtd">
<application-server application-directory="../applications"
  deployment-directory="../application-deployments">
  <rmi-config path="./rmi.xml" />
  <!-- JMS-server config link, uncomment to activate the JMS service -->
  <!-- <jms-config path="./jms.xml" /> -->
  <log>
    <file path="../log/server.log" />
  </log>
  <global-application name="default" path="application.xml" />
  <global-web-app-config path="global-web-application.xml" />
  <web-site path="./default-web-site.xml" />
  <web-site path="e:\orion\orion\config\secure-web-site.xml" />
  <!-- Compiler, activate this to specify an alternative compiler such
    as jikes for EJB/JSP compiling. -->
  <!-- <compiler executable="jikes" classpath="/myjdkdir/jre/lib/rt.jar" /> -->
</application-server>
```

保存配置文件，重新启动 Orion。如果使用 8443 端口作为 https 服务且域名解析正确，则可在浏览器地址栏输入：<https://ml.cnnic.cn:8443> 测试您的域名证

书是否安装成功。

6. 备份服务器证书

服务器证书及私钥都保存在 `keystore` 文件里面，保存并备份 `keystore` 文件即可。