



最后更新时间: 2011年1月25日

软件版本号:

**ubuntu: 10.10 openssl: 0.9.8q
lighttpd: 1.4.18**

服务器证书安装配置指南系列之
lighttpd 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. 应用环境.....	3
2. 关于 openssl.....	3
2.1 openssl 简介.....	3
2.2 openssl 下载及安装配置.....	3
3. 申请服务器证书.....	4
3.1 生成私钥.....	4
3.2 生成 csr 请求文件.....	4
4. 下载服务器证书.....	6
4.1 准备下载证书所需信息.....	6
4.2 下载证书.....	6
5. 安装跟证书和服务器证书.....	11
5.1 下载根证书和 CNNIC 中级根证书.....	11
5.2 准备证书链.....	11
5.3 建立证书链文件.....	15
6. 修改配置文件.....	14
6.1 修改 lighttpd.conf.....	14
7. 备份服务器证书.....	17

图表目录

图表一生成密钥命令行.....	4
图表二生成 csr 请求文件.....	4
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.....	10
图表八证书导出向导.....	11
图表九查看根证书 roottest.cer.....	12
图表十查看中级根证书 cnic.cer.....	13

图表十一证书导出向导 (B)	14
图表十二建立证书链文件.....	15

1. 应用环境

系统环境:

Ubuntu10.10 ; lighttpd-1.4.18; openssl-0.9.8q;

证书类型:

可信服务器证书, 申请地址: <http://www.cnnic.cn/jczyfw/wzws/>

2. 关于 openssl

1) openssl 简介

openssl 是一个 Linux/windows 平台下、开放源代码的实现了 SSL 及相关加密技术的软件包。

2) openssl 下载及安装配置

从 openssl 网站下载 openssl-0.9.8q.tar 并安装该版本

```
# ./config --prefix=/usr/local/openssl
```

```
# make
```

```
# make install
```

修改 openssl.cnf 文件:

```
./usr/local/openssl/ssl/openssl.cnf
```

```
dir = /usr/local/openssl/ssl/misc/demoCA      #设定存取凭证的路径
```

```
default_days = 3650      #设定凭证可使用之天数
```

```
default_bits = 2048      #设定密钥长度(bits)
```

以上是配置 openssl。

3. 申请服务器证书

本手册以 1.cnnic.cn 为例

生成私钥

命令格式：**openssl genrsa -des3 -out [keystore _name] key 2048 Generating RSA private key, 2048 bit long modulus**

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 key

如下图所示：



```
root@leon: /usr/openssl
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)

root@leon:/usr/openssl# openssl genrsa -des3 -out 1.cnnic.cn.key 2048 Generating
RSA private key, 2048 bit long modulus
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
Enter pass phrase for 1.cnnic.cn.key:
Verifying - Enter pass phrase for 1.cnnic.cn.key:
```

图表一生成密钥命令行

如上图所示，行命令运后会提示输入两次私钥的密码，结果生成 2048 位的 RSA 私钥，私钥文件名为：1.cnnic.cn.key。

<注：CNNIC 可信服务器证书要求域名证书密钥对最少为 2048 位>

1) 生成 CSR 证书请求文件

命令格式：**openssl req -new -key [keystore_name] -out [csr_name]**

注：[]中的内容为需要输入的参数

- **csr_name**: 表示生成的证书请求文件的文件名
- **keystore_name**: 表示证书密钥库的文件名，扩展名一般为 key

如下图所示：

```
root@leon:/usr/openssl# openssl req -new -key 1.cnnic.cn.key -out m1.cnnic.cn.csr
Enter pass phrase for 1.cnnic.cn.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:beijing
Locality Name (eg, city) []:beijing
Organization Name (eg, company) [Internet Widgits Pty Ltd]:cnnic
```

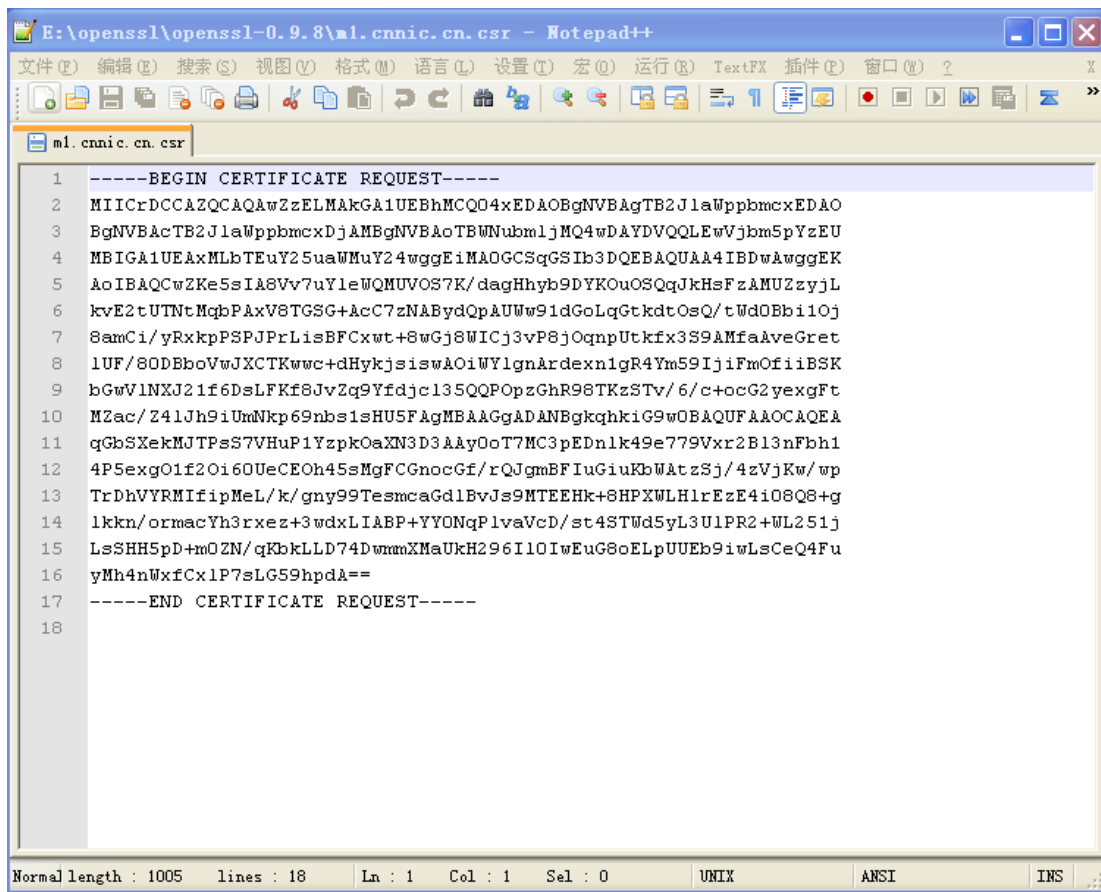
图表二生成 csr 请求文件

上述命令运行后，系统提示输入第一步骤中输入的私钥密码，然后输入 X. 509 证书所要求的字段信息，包括国家(中国添 CN)、省份、所在城市、单位名称、单位部门名称(可以不填直接回车)。 **请注意：除国家缩写必须填 CN 外，其余都可以是英文或中文。**

Common Name 项请输入您要申请域名证书的域名，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可。

请不要输入 Email、口令(challenge password)和可选的公司名称，直接打回车即可。

现在已经成功生成了私钥文件：`1.cnnic.cn.key` 保存在您的服务器中。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：



```
1 -----BEGIN CERTIFICATE REQUEST-----
2 MIICrDCCAQCAwZzELMAkGA1UEBhMCQ04xEDAOBgNVBAGTB2JlaWppbmcxEDAO
3 BgNVBACTB2JlaWppbmcxDjAMBgNVBACTBWNUbm1jMQ4wDAYDVQQLEwVjbm5pYzEU
4 MBIGA1UEAxMLbTEuY25uaWwMuY24wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
5 AoIBAQCwZKe5sIA8Vv7uYleWQNUVOS7K/dagHhyb9DYKouOSQqJkHsFzAMUZzyjL
6 kvE2tUTNtMqbPAxV8TGSg+AcC7zNABydQpAUWw91dGoLqGtKdtOsQ/tWd0Bb11Oj
7 8amCi/yRxpPSPJPrLisBFCxwt+8wGj8WICj3vP8jOqnpUtKfx3S9AMfaAveGret
8 lUF/80DBboVwJXCTKwcc+dHykjsiswAOiWYlgnArdexn1gR4Ym59IjiFmOfiiBSK
9 bGwV1NXJ21f6DsLFKf8JvZq9Yfdjc135QQPOpzGhR98TKzStv/6/c+ocG2yexgFt
10 MZac/Z41Jh9iUmNkp69nbs1sHU5FagMBAAgADANBgkqhkiG9w0BAQUFAAOCQEAA
11 qGbSxekMJTPS7VHuP1YzpkOaXN3D3AAyOoT7MC3pEDnlk49e779Vxr2B13nFbh1
12 4P5exgO1f2Oi60UeCEOh45sMgFCGnocGf/rQJgmBFiUgiuKbWAtzSj/4zVjKw/wp
13 TrDhVYRMIfipMeL/k/gny99TesmcaGdlBvJs9MTEEHk+8HPXWHL1rEzE4i08Q8+g
14 lkkn/ormacYh3rxez+3wdxLIABP+YYONqPlvaVcd/st4STWd5yL3UIPR2+WL251j
15 LsSHH5pD+mOZN/qKbkLLD74DwmmXMaUkH296I10IwEuG8oELpUUEb9iwLsCeQ4Fu
16 yMh4nWxfCx1P7sLG59hpdA==
17 -----END CERTIFICATE REQUEST-----
18
```

图表三查看 csr 文件

4. 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面

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”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"/>
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> <pre>MIICrDCCAZQCAQAwZzELMAkGA1UEBhMCQ04xEDAOBgNVBAGTB2JlaWppbmcxEDAOBgNVBACjB2JlaWppbmcxDjAMBgNVBAoTBWVudm1lMQ4wDAYDVQQLEwVjb250YzEUMBIA1UEAxMLbTEuY25uaWVudm1lMQ4wDAYDVQQQAQAA4IBDwAwggEKAoIBAQcwZKe5sIA8Vv7uYleWQMUVOs7K/dagHhyb9DYKOUOSQqJkHsFzAMUZzyjLkvE2tUTNtMqbPaxV8TGSg+AcC7zNABYdQpAUWw91dGoLqGtktOsQ/tWd0Ebi1Oj8amCi/yRxpPSPJPrLisBFCxwt+8wGj8WICj3vP8jOqnpUtkfx3S9AMfaAveGret1UF/80DBbcVwJXCTKwcc+dHykjsiswAOiWYlgnArdeXn1gR4Ym59IjiFmOfiiBSKbGwVlNXJ21f6DsLFKf8JvZq9Yfdjc135QQPOpzGhR98TKzStv/6/c+ocG2yexgFtMZac/Z41Jh9iUmNkp69nbs1sHU5FAGMBAAGgADANBgkqhkiG9w0BAQUFAAOCAQEAqGbSxekMJTPsS7VHuP1YzpkOaxN3D3AAyOoT7MC3pEDnlk49e779Vxr2B13nFbh1</pre>
<input type="button" value="提交"/> <input type="button" value="重置"/>	

图五填入收到的参考号和授权码以及生成的 csr

点击“提交”，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-----
MIIEGzCCAwoGAWIBAgIQEMCXznvJBxWzS5X3sUEd6DANBgkqhkiG9w0BAQUFADAYMQswCQYDVQQG
EwJjbjEOMAwGA1UEChMFY25uaWMxEzARBgNVBAMTCmNubmljIHJvb3QwHhcNMTAxMjA3MDkzOTAw
WhcNMTExMjA3MDkzOTAwWjBhMQswCQYDVQQGEwJDTjENMAsGA1UECB4EUXdOrDENMAsGA1UEBx4E
UxdOrDEOMAwGA1UEChMFY25uaWMxEzARBgNVBAsTBWNUbmljMRQwEgYDVQQDEwtMS5jbm5pYy5j
bjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALBkp7mvgDxW/u5iV5ZAxRU5Lsr91qAe
HJvONgo645JComQewXMAxRnPKMuS8Ta1RM2Oyps8DFXxMZIb4BwLvMOAHJ1CkBRbD3VOaguo2R2
06xD+1Z3QFuLU6PxqYKL/JHGSk9I8k+suKwEULHC37zAaPxYgKPe8/yM6qe1S2R/HdL0Ax9oC94a
t62VQX/zQMFuhXAlcJMrDBz5OfKSOyKzAA6JZiWCCt17GfWBHhibn0iOIWY5+KIF IpsbBWU1cnb
V/oCwsUp/wm9mr1h92NyXf1BA86nMaFH3xMrNJO//r9z6hwbbJ7GAW0xlpz9niUmH2JSY2Snr2du

```

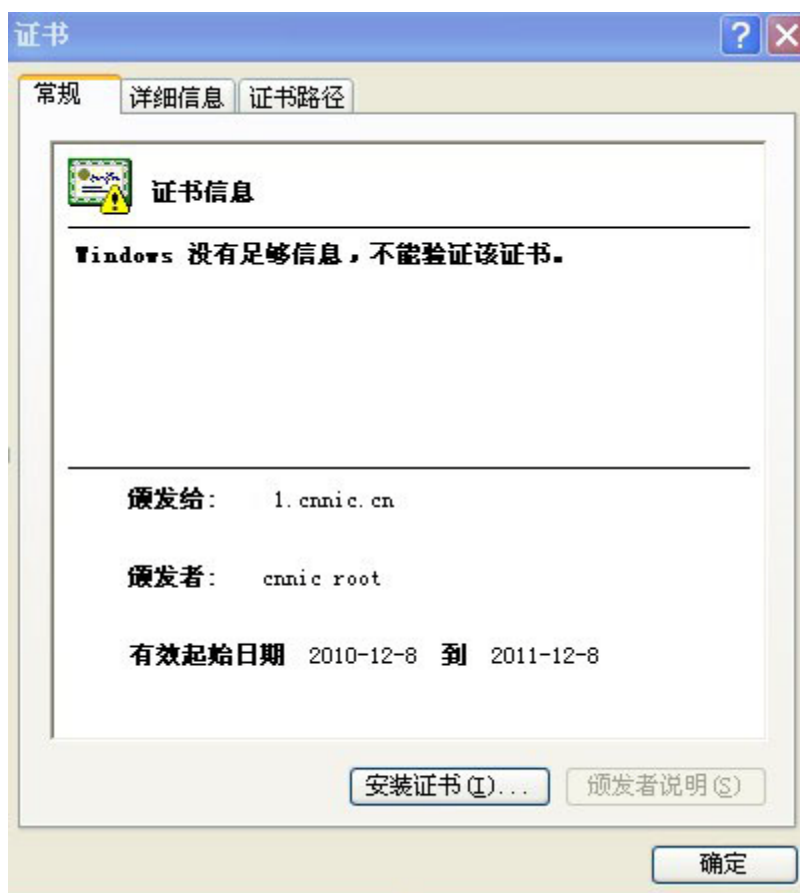
Web服务器证书请将证书编码框中的内容拷贝，并粘贴到文本中，保存成Web服务器能够识别的格式。

图表六生成证书

请按页面提示保存，文件名保存为 1.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：

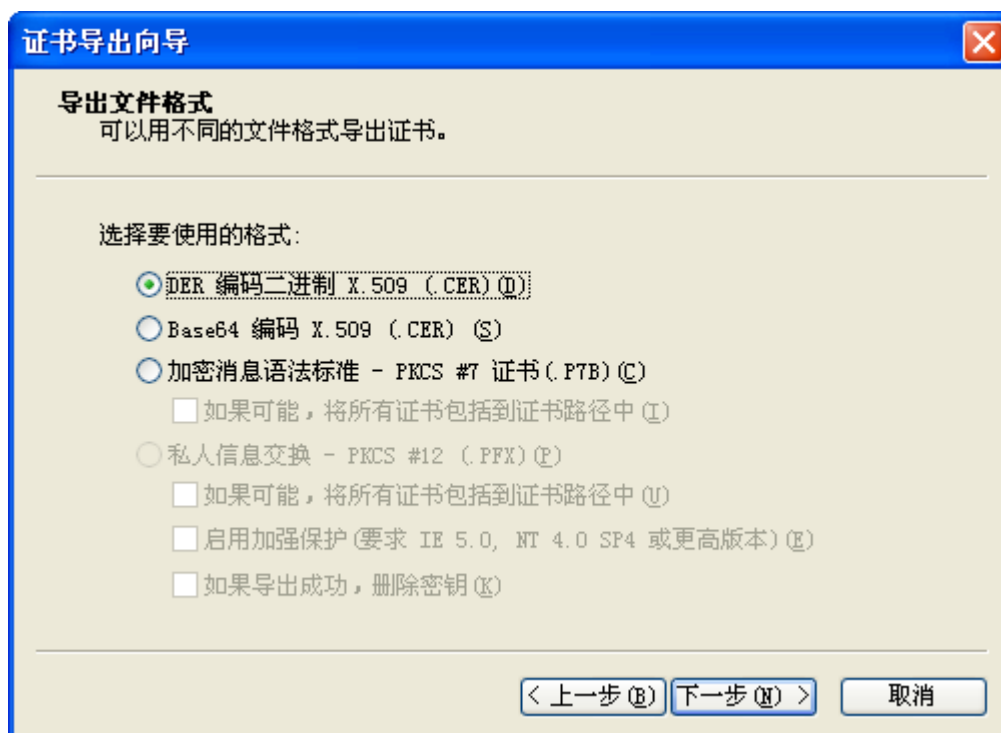


图表七格式转换

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 (A)

5. 安装根证书和服务证书

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

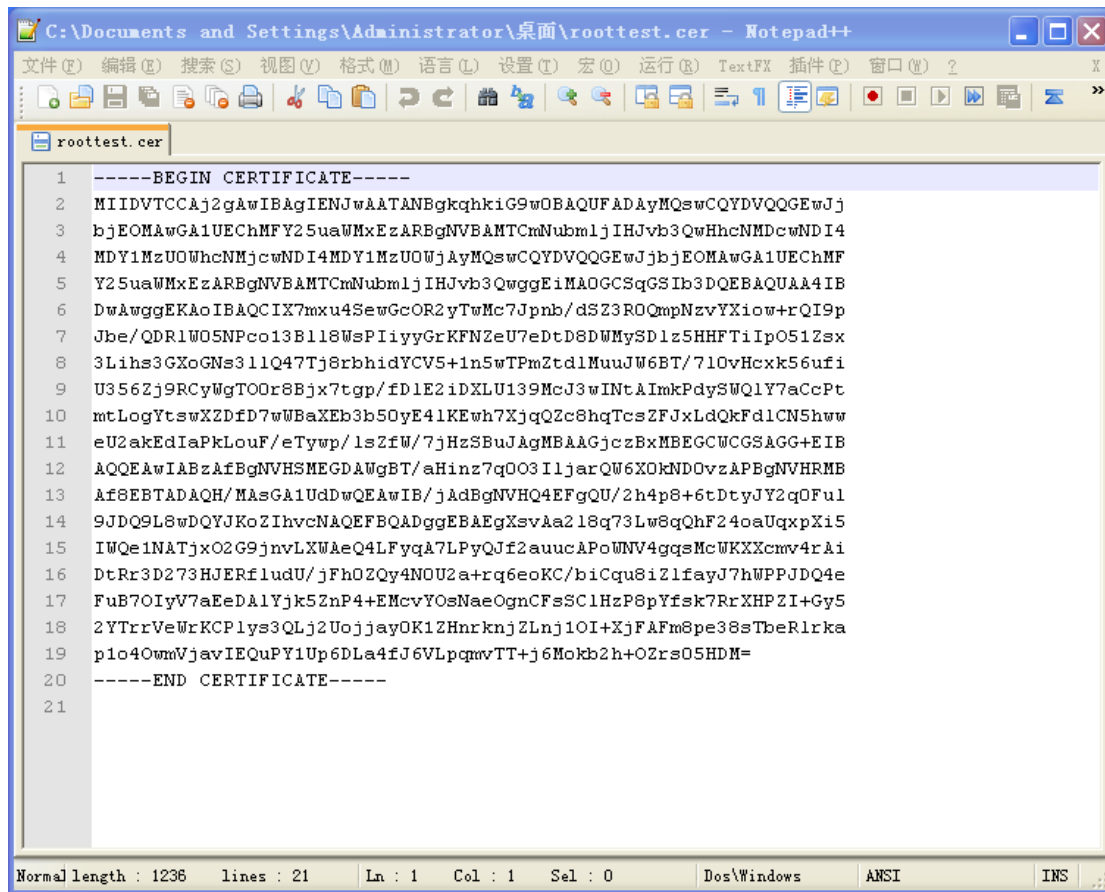
标准证书: http://www.cnnic.cn/jczyfw/wzws/bzcx/xz/201010/t20101027_16322.html

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”。

2) 准备证书链

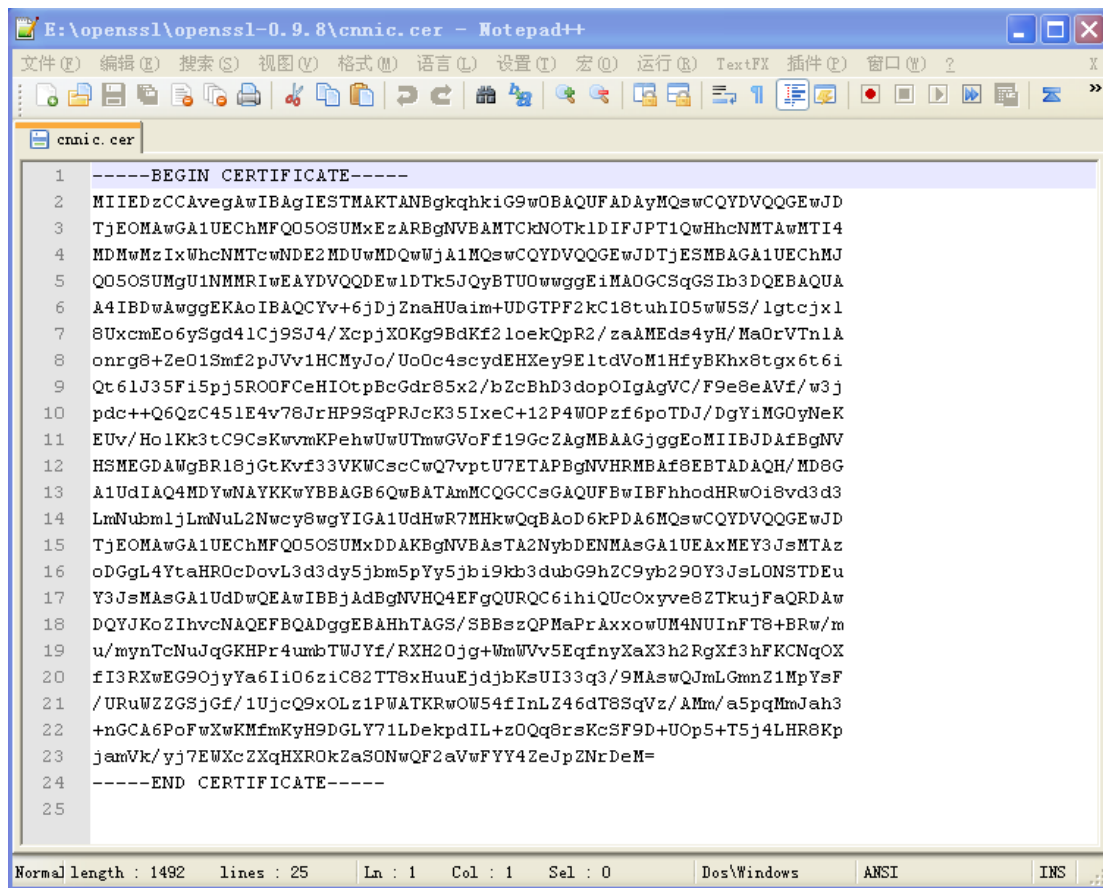
使用文本编辑工具（如 notepad）将 root.cer 和 CNNIC.cer 分别打开，分别显示如下图所示（本例用的测试根证书，名为 roottest.cer）：



```
1 -----BEGIN CERTIFICATE-----
2 MIIDVTCCAj2gAwIBAgIENJwAATANBgkqhkiG9w0BAQUFADAyMQswCQYDVQQGEwJj
3 bjEOMAwGA1UEChMFY25uaWMxEzARBgNVBAMTCmNubmljIHJvb3QwHhcNMDcwNDI4
4 MDY1MzU0WmcNMjcwNDI4MDY1MzU0WjAyMQswCQYDVQQGEwJbjEOMAwGA1UEChMF
5 Y25uaWMxEzARBgNVBAMTCmNubmljIHJvb3QwggEiMAOGCSqGSIb3DQEBAQUAA4IB
6 DwAwggEKAAoIBAQCIX7mxu4SewGcOR2yTwMc7Jpnb/dS23ROQmpNzvYXiw+rQI9p
7 Jbe/QDR1W05NPFco13B118WspIiyyGrKFNzeU7eDtD8DWMYSD1z5HHFTiIp051Zsx
8 3Lhs3GXoGns311Q47Tj8rbhidYCV5+1n5wTPm2tdlMuuJW6BT/71OvHcxk56ufi
9 U356Zj9RCyWgTODr8Bjx7tgp/fD1E2iDXLU139McJ3wINTAImkPdySWQ1Y7aCcPt
10 mtLogYtswXZDfd7wWbAXEb3b50yE41KEwh7XjqQZc8hqTcsZFJxLdQkFdlCN5hww
11 eU2akEdIaPkLouF/eTywp/1sZfW/7jHzSBuJAgMBAAGjczBxMBEGCWCgsAGG+EIB
12 AQEAAIABzAfBgNVHSMEGDAWgBT/aHinz7q003I1jarQW6X0kND0vzAPBgNVHRMB
13 Af8EBTADAQH/MAsGA1UdDwQEAwIB/jAdBgNVHQ4EFgQU/2h4p8+6tDtyJY2q0Fu1
14 9JDQ9L8wDQYJKoZIhvcNAQEFBQADggEBAEgXsvAa218q73Lw8qQhF24oaUqxpXi5
15 IWQe1NATjx02G9jnvLXWæQ4LFyqA7LPyQJf2auucAPoWNV4gqsMcWKKXcmv4rAi
16 DtRr3D273HJERfludU/jFhOZQy4NOU2a+rq6eoKC/biCqu8iZ1fayJ7hWPPJDQ4e
17 FuB7OIyV7aEeDAlYjk5ZnP4+EMcvYOsNaeOgnCFsSC1HzP8pYfsk7RrXHPZI+Gy5
18 2YTrrVeWrKCPlys3QLj2UoJJayOK1ZHnrknjZLnj1OI+XjFAFm8pe38sTbeRlrka
19 p1o4OmwVjavIEQuPY1Up6DLa4fJ6VLpqmvTT+j6Mokb2h+OZrs05HDM=
20 -----END CERTIFICATE-----
21
```

Normal length : 1236 lines : 21 Ln : 1 Col : 1 Sel : 0 Dos\Windows ANSI INS

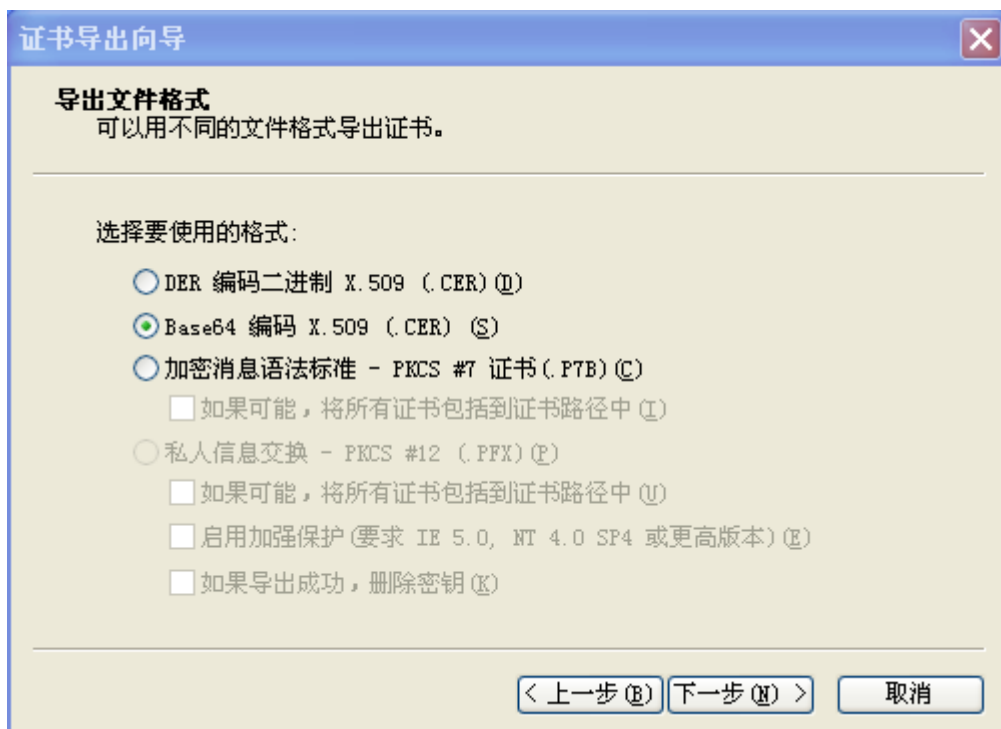
图表九查看根证书 roottest.cer



```
1 -----BEGIN CERTIFICATE-----
2 MIIEDzCCAVEgAwIBAgIESTMAKTANBgkqhkiG9w0BAQUFADAYMQswCQYDVQQGEwJD
3 TjEOMAwGA1UEChMFQ05OSUMxEzARBgNVBAMTCkNOTk1DIFJPT1QwHhcNMTAwMTI4
4 MDMwMzIxWhcNMTEwNDE2MDUwMDQwWjA1MQswCQYDVQQGEwJDTjESMBAGA1UEChMJ
5 Q05OSUMGU1NMMRIwEAYDVQQDEw1DTk5JQyBTU0wggEiMAOGCSqGSIb3DQEBAQUA
6 A4IBDwAwggEKAAoIBAQCYv+6jdJZnaHUaim+UDGTPF2kC18tuhI05wW5S/lgtcjx1
7 8UxcmEo6ySgd41Cj9SJ4/XcpjXOKg9BdKf2loeKqR2/zaAMEds4yH/MaOrVTn1A
8 onrg8+Ze01Smf2pJVv1HCMyJo/Uo0c4scydEHXey9E1tdVoM1HfyBKhx8tgx6t6i
9 Qt61J35F15pj5RODFCeHI0tpBcGdr85x2/bZcBhD3dopOlgAgVC/F9e8eAVf/w3j
10 pdc++Q6QzC451E4v78JrHP9SqrJcK35Ixc+12P4WOPzf6poTDJ/DgYiHG0yNeK
11 EUv/Ho1Kk3tC9CsKvwmKPeWUwUTmwGVof19GcZAgMBAAgJggEoMIIBJDAfBgNV
12 HSMGDAWgBR18jGtKvf33VKWCscCwQ7vptU7ETAPBgNVHRMBAf8EBTADAQH/MD8G
13 A1UdIAQ4MDYwNAYKKwYBBAg6QwBATAmMCQGCCsGAQUFBwIBFhhodHRwOi8vd3d3
14 LmNubmljLmNubU2Nwcy8wYyYGA1UdHwR7MHkwQwBAoD6kPDA6MQswCQYDVQQGEwJD
15 TjEOMAwGA1UEChMFQ05OSUMxDDAKBgNVBAsTA2NybdENMAsGA1UEAxMEY3JsmTAz
16 oDgGL4YtaHR0cDovL3d3dy5jbm5pYy5jb29kb3dubG9hZC9yb290Y3JsmLONSTDEu
17 Y3JsmAsGA1UdDwQEAwIBBjAdBgNVHQ4EFgQURQC6ih1QUcOxyve8ZTKujFaQRDAw
18 DQYJKoZIhvcNAQEFBQADggEBAHhTAGS/SBBSzQPMAPrAxxowUM4NUInFT8+BRw/m
19 u/mynTcNuJqGKHP4umbTWJYf/RXH2Ojg+WmWVv5EqfnyXaX3h2RgXf3hFKCNqOX
20 fI3RXwEG9OjyYa6Ii06ziC82TT8xHuuEjdbKsUI33q3/9MASwQJmLGmmZ1MpYsF
21 /URuWZZGSjGf/1UjcQ9xOLz1PWATKRwOW54fInLZ46dT8Sqvz/AMm/a5pqMmJah3
22 +nGCA6PoFwXwKmfKyH9DGLY71LDekpdIL+z0Qq8rsKcSF9D+UOp5+T5j4LHR8Kp
23 jamVk/yj7EWXcZXqHXROkZaSONwQF2aVwFYY4ZeJpZNRDeM=
24 -----END CERTIFICATE-----
25
```

图表十查看中级根证书 cnnic.cer

注意：在用 notepad 打开 roottes.cer 的时候可能会出现乱码，这样我们就先直接打开 roottest.cer --详细信息--复制到文本，选择 Base64 编码 X.509，如下图：



图表十一证书导出向导 (B)

下一步，替换之前的 roottest.cer 文件即可。

3) 建立证书链文件

使用文本编辑工具新建一个文件 cachain.cer，将 root.cer 和 CNNIC.cer 中的内容拷贝进去并保存，注意 CNNIC.cer 的内容在前，root.cer 的内容在后，显示如下图所示：

```

1 -----BEGIN CERTIFICATE-----
2 MIIEEDzCCAvAgAwIBAgIESTMAKTANBgkqhkiG9wOBAQUFADAYMQswCQYDVQGEwJD
3 TjEOMAwGA1UEChMFQ05OSUMxEzARBgNVBAMTCkNOTk1DIFJPT1QwHhcNMTAwMTI4
4 MDMwMzIxWncNMTCwNDE2MDUwMDQwWjA1MQswCQYDVQGEwJDTjESMBAGA1UEChMJ
5 Q05OSUMGU1NMMRIwEAYDVQDEw1DTk5JQyBTU0wggEiMAOGCSqGSIb3DQEBAQUA
6 A4IBDwAwggEKAoIBAQC9Yv+6jDjZnaHUaim+UDGTPF2kC18tuhIO5wW5S/lgtcjx1
7 8UxcmEo6ySgd4lCj9SJ4/XcpjXOKg9BdKf2loekQpR2/zaAMEds4yH/MaOrVtnlA
8 onrg8+Ze01Smf2pJVv1HcMyJo/UoOc4scydEHXey9E1tdVoM1HfyBkx8tgx6t6i
9 Qt6lJ35Fi5pj5ROOFceHIOTpBcGdr85x2/bZcBhD3dopOIgAgVC/F9e8eAVf/w3j
10 pdc++Q6QzC451E4v78JrHP9SQRJcK35IxeC+12P4WOPzf6poTDJ/DgYiMGOyNeK
11 EUv/HolKk3tC9CsKwvmKPeHwUwUTmwGVoFf19GcZAgMBAAGjggEoMIIBJDAfBgNV
12 HSMEDGAWgBR18jGtKvf33VKWCscCwQ7vptU7ETAPBgNVHRMBAf8EBTADAQH/MD8G
13 A1UdIAQA4MDYwNAyKkYBBAGB6QwBATAmMCQGCCsGAQUFBwIBFhhodHRwOi8vd3d3
14 LmNubmljLmNubmljLnwcy8wggYIGA1UdHwR7MHkwQqBAoD6kPDA6MQswCQYDVQGEwJD
15 TjEOMAwGA1UEChMFQ05OSUMxDDAKBgNVBAsTA2NybdENMAsGA1UEAxMEY3J5MTAz
16 oDGgL4YtaHROcDovL3d3dy5jbM5pYy5jb19kb3dubG9hZC9yb290Y3JsLONSTDEu
17 Y3JsMAsGA1UdDwQEAwIBBjAdBgNVHQ4EFgQURQC6ihiQUcOxyve8ZTkujFaQRDAw
18 DQYJKoZIhvcNAQEFBQADggEBAHhTAgS/SBBszQPMaPrAxxowUM4NUInFT8+BRw/m
19 u/mynTcNuJqGKHP4umbTWJYf/RXH20jg+WmWVv5EqfnyXaX3h2RgXf3hFKCNqOX
20 fI3RXwEG90jyYa6Ii06ziC82TT8xHuuEjdjbKsUI33q3/9MAswQJmLgmnZ1MpYsF
21 /URuWZzGSjGf/1UjCQ9xOLz1PWATKRwOW54fInLZ46dT8SqVz/AMm/a5pqMmJah3
22 +nGCA6PoFwXwKfmKyH9DGLY71LDekpdIL+zOQq8rsKcSF9D+UOp5+T5j4LHR8Kp
23 jamVk/yj7EWXc2XqHXROkZaSONwQF2aVwFYY4ZeJpZnrDeM=
24 -----END CERTIFICATE-----
25 -----BEGIN CERTIFICATE-----
26 MIIDVTCCAj2gAwIBAgIENJwAATANBgkqhkiG9wOBAQUFADAYMQswCQYDVQGEwJj
27 bjEOMAwGA1UEChMFY25uaWMxEzARBgNVBAMTCmNubmljIHJvb3QwHhcNMDCwNDI4
28 MDY1MzU0WncNMjcwNDI4MDY1MzU0WjA1MQswCQYDVQGEwJjbjEOMAwGA1UEChMF
29 Y25uaWMxEzARBgNVBAMTCmNubmljIHJvb3QwggEiMAOGCSqGSIb3DQEBAQUAA4IB
30 DwAwggEKAoIBAQCIX7mxu4SewGcOR2yTwmC7Jpnb/dsZ3ROqmpNzvYxiow+rQI9p
31 Jbe/QDR1W05NPco13B118WsPIiyyGrKFNZeU7eDtD8DWMYSD1z5HHFTiIp051Zsx
32 3LihS3GXoGNS31lQ47Tj8rbhidYCV5+1n5wTPmZtdlMuuJW6BT/710vHcxk56ufi
33 U356Zj9RCyWgTOOr8Bjx7tgp/fDlE2iDXLU139McJ3wIntAImkPdySWQ1Y7aCcPt
34 mtLogYtswXZDf7wWBaXEB3b50yE41KEwh7XjqQZc8hqTcsZFJxLdQkFd1CN5hw

```

图表十二建立证书链文件

至此，配置 SSL 需要的如下文件均已准备好：

1. cachain.cer 证书链文件
2. registrars.cnnic.cn.key 使用 OpenSSL 创建的私钥
3. registrars.cnnic.cn.cer CNNIC 颁发的证书（Base64 格式）

6. 修改配置文件

1) 修改lighttpd.conf

#vi /usr/lighttpd/etc/lighttpd.conf 修改前要备份这个文件

加入下面信息:

```
$SERVER["socket"] == "theos.in:443" {  
  
ssl.engine = "enable"  
  
ssl.pemfile = "/etc/lighttpd/theos.in/theos.in.cer"  
  
ssl.ca-file = "/etc/lighttpd/theos.in/CA_issuing.crt"  
  
server.name = "theos.in"  
  
server.document-root = "/home/lighttpd/theos.in/https"  
  
server.errorlog = "/var/log/lighttpd/theos.in/serror.log"  
  
accesslog.filename = "/var/log/lighttpd/theos.in/saccess.log" }
```

其中,

ssl.engine = "enable" : 打开 lighttpd ssl 开关

ssl.pemfile = "/usr/local/lighttpd/theos.in/theos.in.cer" - 你的 cer 文件

ssl.ca-file = "/usr/local/lighttpd/theos.in/CA_issuing.crt" - 你的证书链文件

保存并关闭这个文件。重启 lighttpd 服务器(会提示你输入 SSL private key 的密码):

如果分配了 443 端口作为 https 服务端点,且域名解析配置正确,此时可以在浏览器地址栏输入: <https://1.cnnic.cn> (申请证书的域名)测试您的 SSL 证书是否安装成功。

7. 备份服务器证书

只需备份好服务器证书文件 1.cnnic.cn.cer

私钥保存文件 1.cnnic.cn.key 即可。