中国互联网络信息中心
China Internet Network Information Center

最后更新时间： 2010年12月7日

软 件 版 本 号： windows xp sp3;
apache_2.2.11-win32-x86-openssl-0.9.8i
openssl-0.9.8; vc++6.0;
ActivePerl-5.12.2.1202-MSWin32-x86-293621

服务器证书安装配置指南系列之

apache 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

图表目录

1. 应用环境

系统环境：

windows xp sp3 ;　apache_2.2.11-win32-x86-openssl-0.9.8i; openssl-0.9.8; Perl-5.12.2;　vc++6.0.

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 apache 网站下载 apache_2.2.11-win32-x86-openssl-0.9.8i 并安装该版本 apache http server 包含 openssl 并包含 mod_ssl 模块。配置 OPENSSL_CONF 的变量环境，值为 openssl 里 apps 目录下的 openssl.cnf 文件。

安装 perl 和 vc6，注册环境变量。

然后运行 cmd 进入到 Openssl 根目录，输入 perl Configure VC-WIN32,回车输入 ms\do_ms,然后 cd 到 microsoft visual studio\vc98\bin 目录下执行 vcvars32.bat,最后回到 openssl 目录下执行 nmake –f ms\ntdll.mak 成功之后在 openssl 安装目录下多了几个文件夹并且文件夹下有相关文件。需要把得到的 out32dll 文件夹路径添加到变量环境 path 里。

以上是配置 openssl。

3. 申请服务器证书

本手册以 m1.cnnic.cn 为例，以下命令请使用 开始-运行-cmd 进入 DOS 环境进行

1）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：

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： m1.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〉

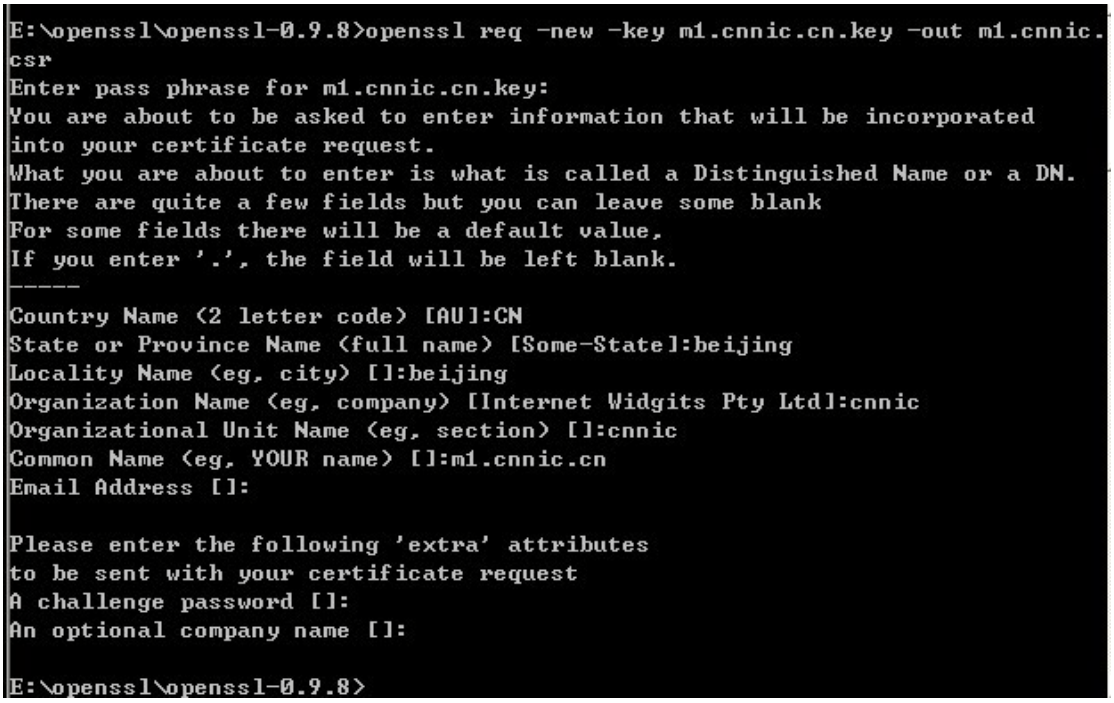
2）生成 CSR 证书请求文件

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：



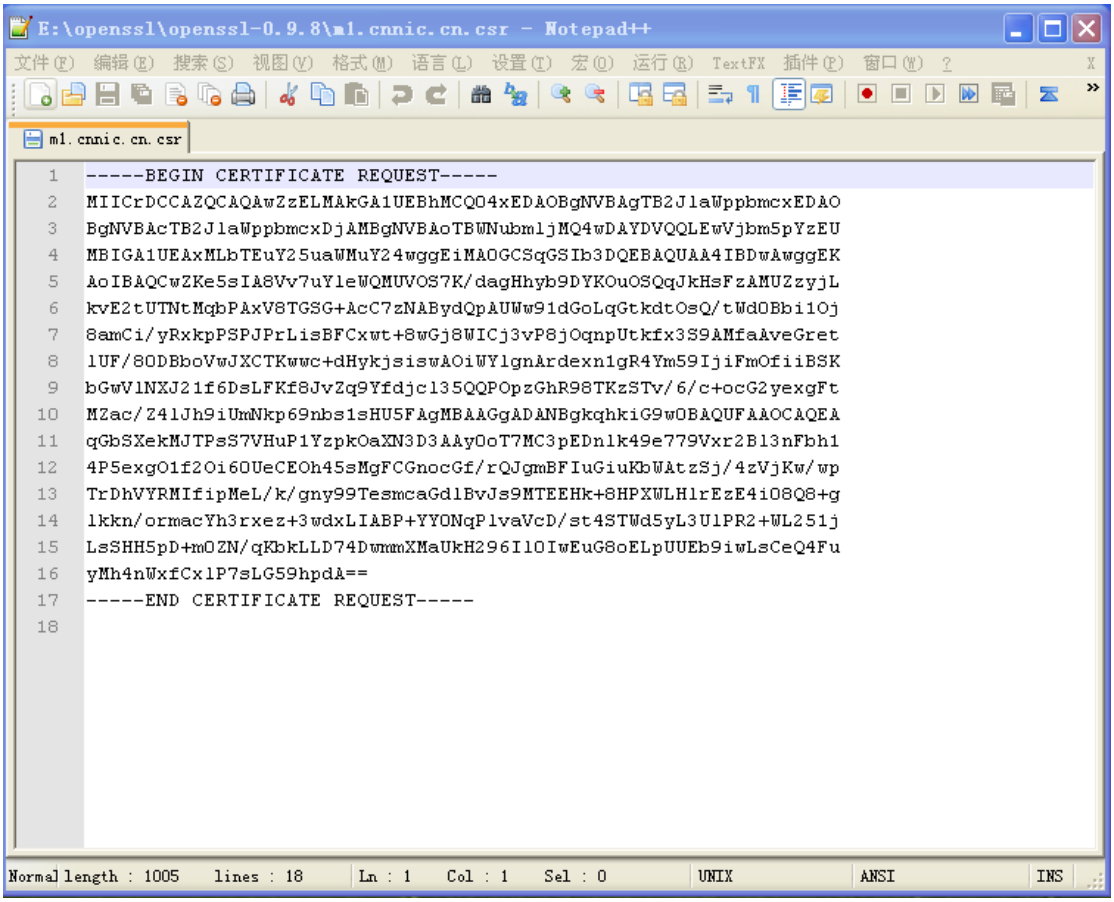
图表二　生成 csr 请求文件

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：m1.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：



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：

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：

图表五　填入收到的参考号和授权码以及生成的 csr

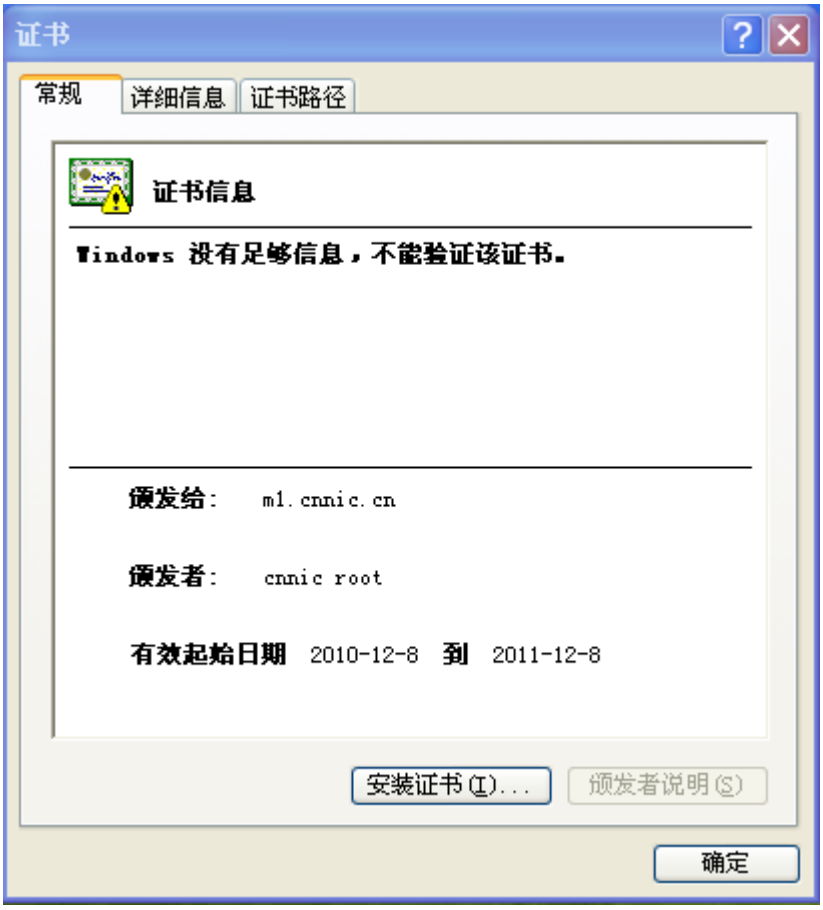
点击“提交”，如果参考号、授权码和 CSR 均无问题，则显示页面如下所示：

图表六　生成证书

请按页面提示保存，文件名保存为 m1.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：

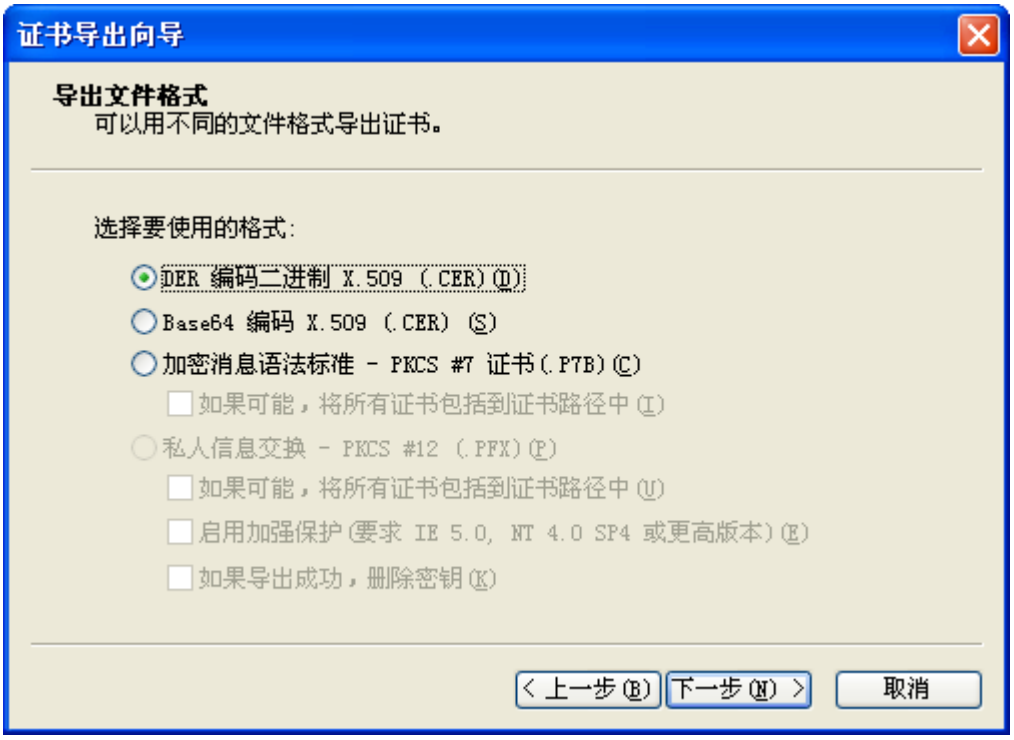


图表七　格式转换

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

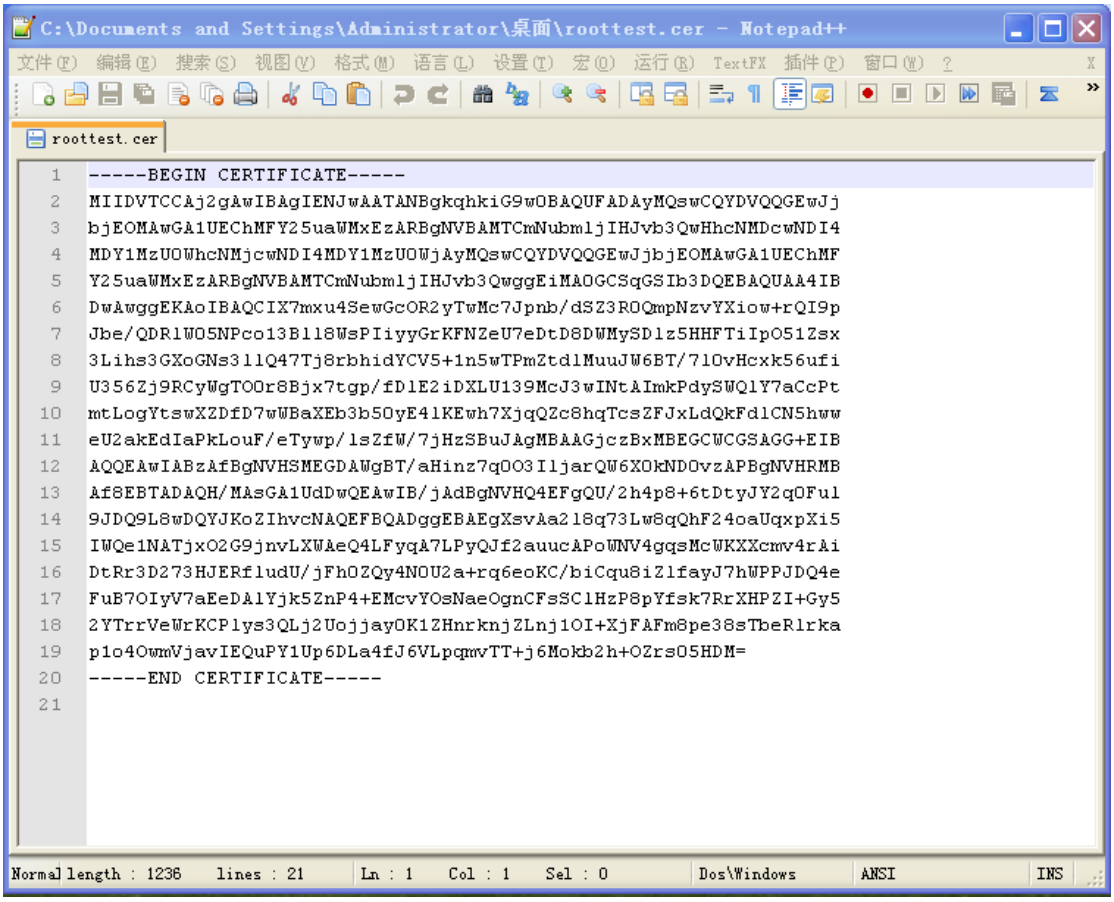
标准证书：http://www.cnnic.cn/jczyfw/wzws/bzkx/xz/201010/t20101027_16322.html

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

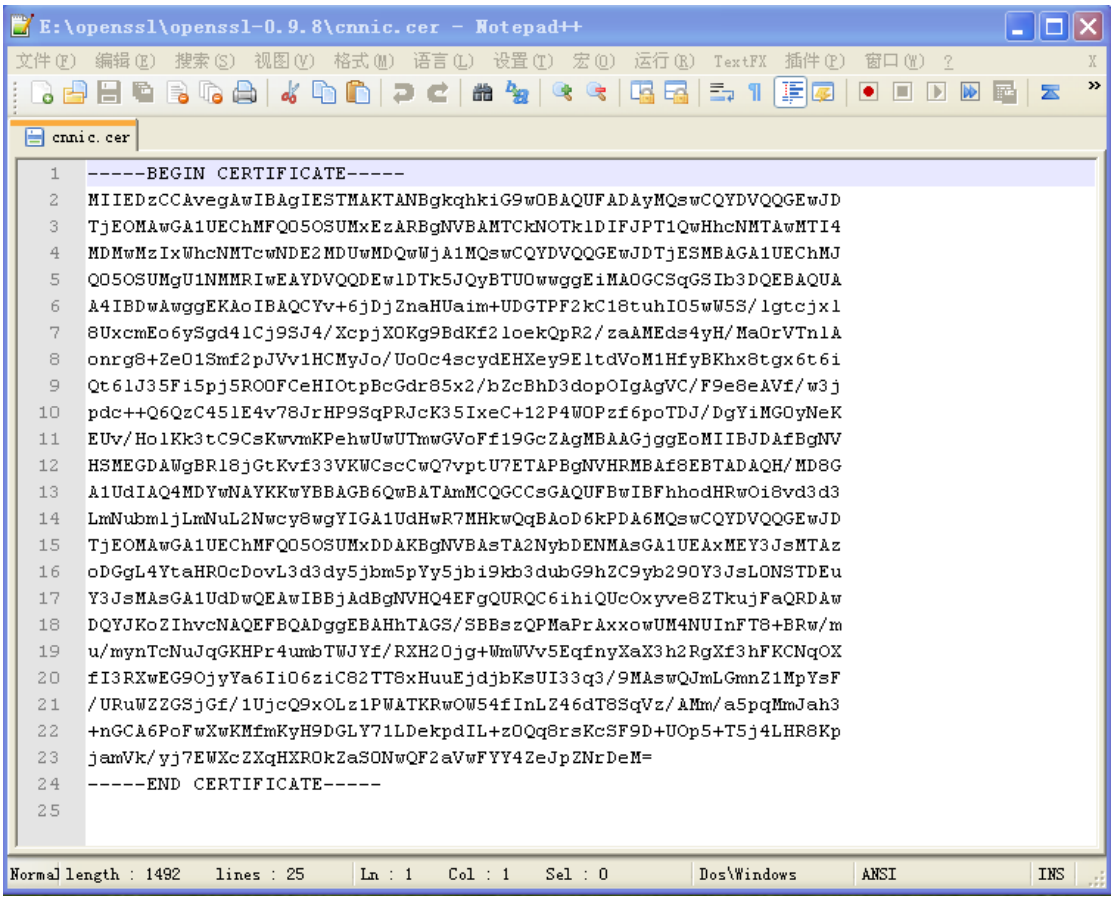
将 CNNIC 中级根证书文件名保存为“CNNIC.cer”，将根证书文件名保存为“root.cer”。

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）：

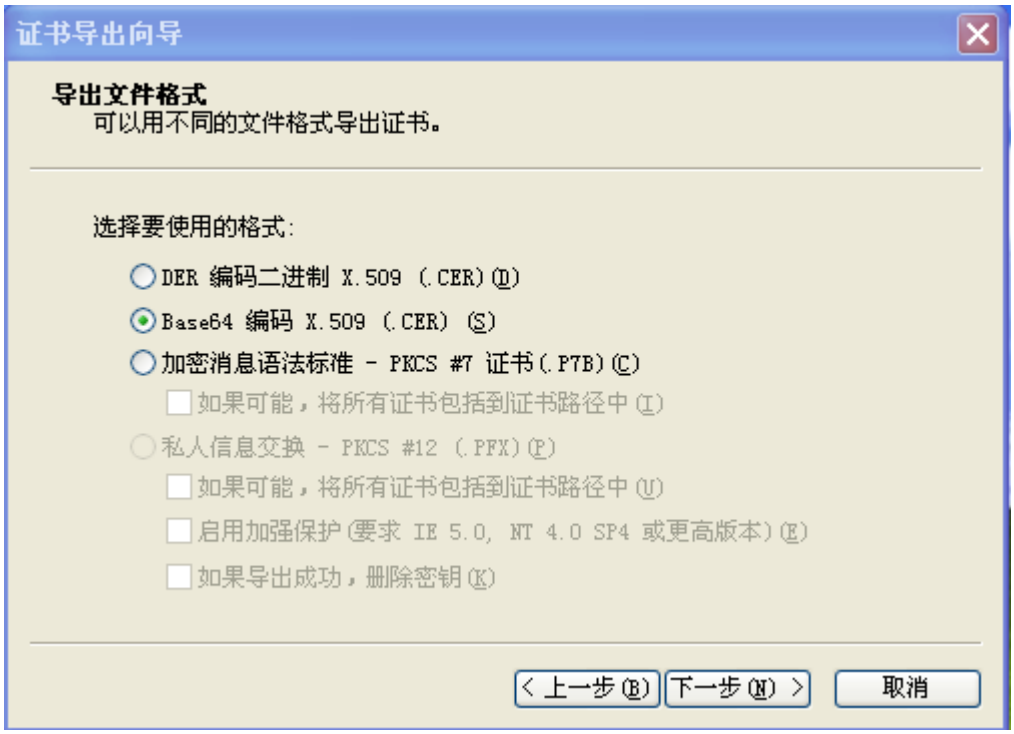


图表九　查看根证书 roottest.cer



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：

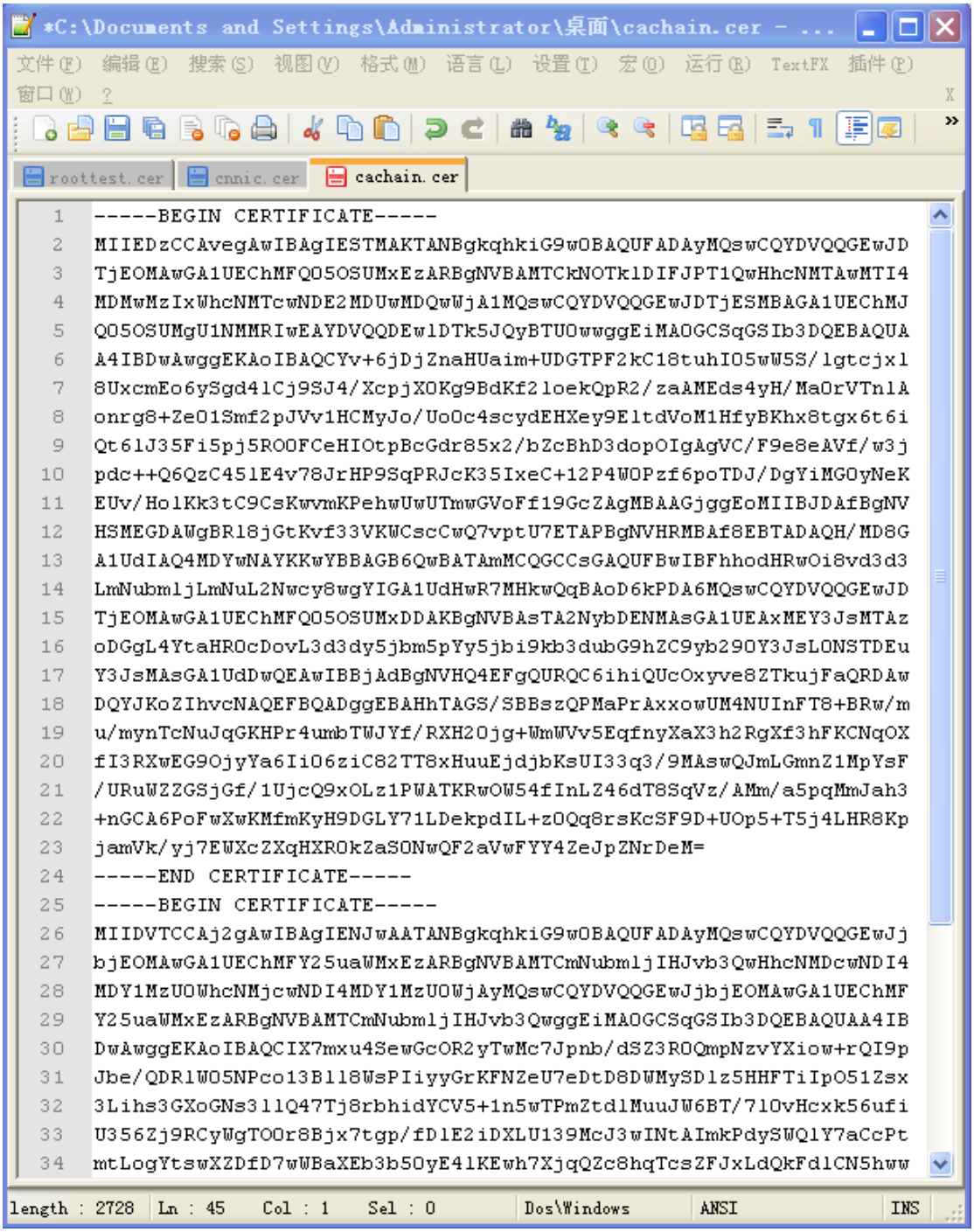


图表十一　证书导出向导（B）

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：



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
3. registrars.cnnic.cn.cer　　CNNIC 颁发的证书（Base64 格式）

6. 修改配置文件

1) 增加mod_ssl模块

默认情况下 Apache HTTP Server 2.2.11 的安装目录中 conf 下的 httpd.conf 中的 mod_ssl 模块是被注释的，处于未启用状态，如下图所示：

```
#LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
#LoadModule proxy_http_module modules/mod_proxy_http.so
#LoadModule rewrite_module modules/mod_rewrite.so
LoadModule setenvif_module modules/mod_setenvif.so
#LoadModule speling_module modules/mod_speling.so
#LoadModule ssl_module modules/mod_ssl.so
#LoadModule status_module modules/mod_status.so
#LoadModule substitute_module modules/mod_substitute.so
#LoadModule unique_id_module modules/mod_unique_id.so
#LoadModule userdir_module modules/mod_userdir.so
#LoadModule usertrack_module modules/mod_usertrack.so
#LoadModule version_module modules/mod_version.so
#LoadModule vhost_alias_module modules/mod_vhost_alias.so
```

图表十三　被注释的 mod_ssl 模块

因此需要将其前端的注释符#去掉，以启用 mod_ssl 模块。

```
#LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
#LoadModule proxy_http_module modules/mod_proxy_http.so
#LoadModule rewrite_module modules/mod_rewrite.so
LoadModule setenvif_module modules/mod_setenvif.so
#LoadModule speling_module modules/mod_speling.so
LoadModule ssl_module modules/mod_ssl.so
#LoadModule status_module modules/mod_status.so
#LoadModule substitute_module modules/mod_substitute.so
#LoadModule unique_id_module modules/mod_unique_id.so
#LoadModule userdir_module modules/mod_userdir.so
#LoadModule usertrack_module modules/mod_usertrack.so
#LoadModule version_module modules/mod_version.so
#LoadModule vhost_alias_module modules/mod_vhost_alias.so
```

图表十四 启用 mod_ssl 模块

2) 导入ssl配置文件

默认情况下 Apache HTTP Server 2.2.11 的安装目录中 conf 下的 httpd.conf 中的 httpd-ssl.conf 是被注释的，处于未导入状态，如下图所示：

```
# Secure (SSL/TLS) connections
#Include conf/extra/httpd-ssl.conf
```

图表十五　被注释的 httpd-ssl.conf

因此需要将其前端的注释符#去掉，以导入 ssl 的配置文件，如下图所示：

```
# Secure (SSL/TLS) connections
Include conf/extra/httpd-ssl.conf
```

图表十六　去掉注释启用 httpd-ssl.conf

3)　修改httpd-ssl.conf

在apache—conf—extra-- httpd-ssl.conf中找到如下片段

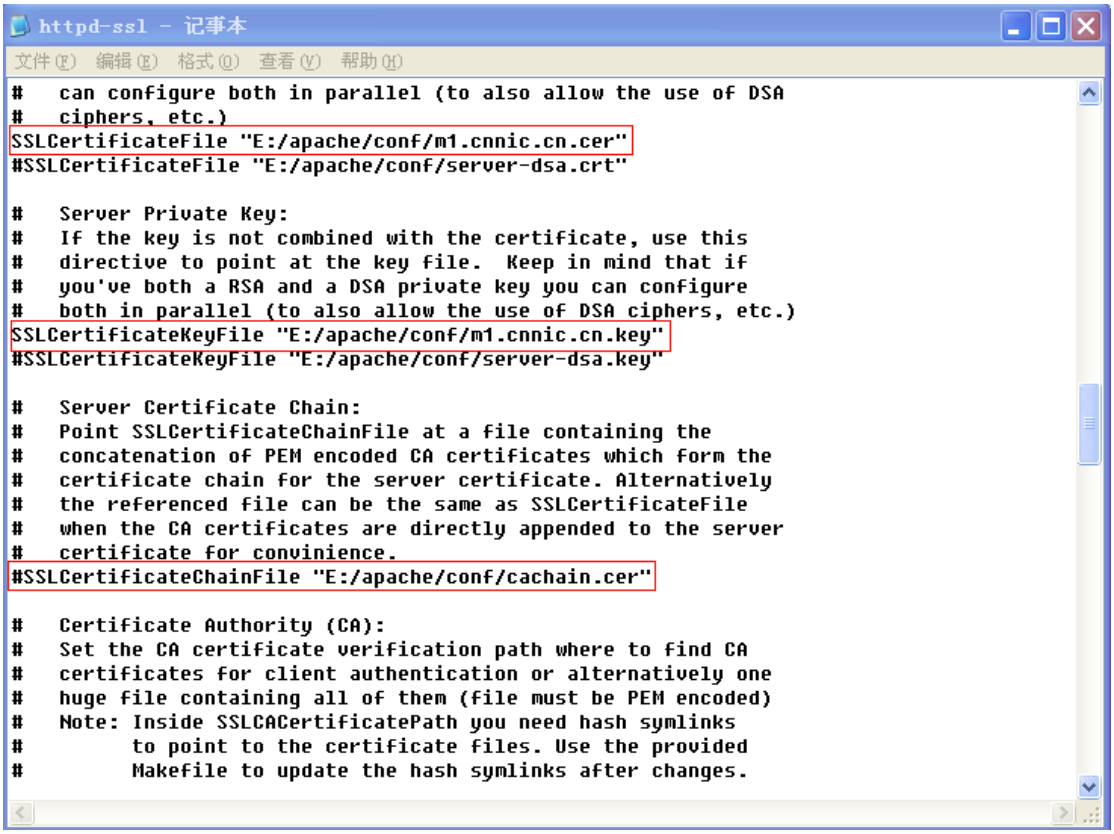
```
#   Server Certificate:
#   Point SSLCertificateFile at a PEM encoded certificate.  If
#   the certificate is encrypted, then you will be prompted for a
#   pass phrase.  Note that a kill -HUP will prompt again.  Keep
#   in mind that if you have both an RSA and a DSA certificate you
#   can configure both in parallel (to also allow the use of DSA
#   ciphers, etc.)
SSLCertificateFile "C:/Program Files/Apache Software Foundation/Apache2.2/conf/server.crt"
#SSLCertificateFile "C:/Program Files/Apache Software Foundation/Apache2.2/conf/server-dsa.crt"

#   Server Private Key:
#   If the key is not combined with the certificate, use this
#   directive to point at the key file.  Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile "C:/Program Files/Apache Software Foundation/Apache2.2/conf/server.key"
#SSLCertificateKeyFile "C:/Program Files/Apache Software Foundation/Apache2.2/conf/server-dsa.key"

#   Server Certificate Chain:
#   Point SSLCertificateChainFile at a file containing the
#   concatenation of PEM encoded CA certificates which form the
#   certificate chain for the server certificate. Alternatively
#   the referenced file can be the same as SSLCertificateFile
#   when the CA certificates are directly appended to the server
#   certificate for convinience.
#SSLCertificateChainFile "C:/Program Files/Apache Software Foundation/Apache2.2/conf/server-ca.crt"
```

图表十七　修改前的 httpd-ssl.conf

其中，SSLCertificateFile 指明证书的存放路径，SSLCertificateKeyFile 指明私钥的存放路径，SSLCertificateChainFile 指明根证书与中级根证书链的存放路径。

将以上三个指令的值更改为实际证书、私钥、证书链的存放路径，保存文件。

举例来说，假设 cachain.cer，m1.cnnic.cn.key，m1.cnnic.cn.cer 三个文件存放在 Apache HTTP Server 的 conf 目录中，则将 httpd-ssl.conf 文件中相关部分修改为入下图所示（红色框部分）：



图表十八　红色框内为修改的地方

上图所示修改使用的是相对于 conf 目录的相对路径，也可更改为相对于硬盘的绝对路径

最后，重启 Apache HTTP Server 服务使之生效。

如果分配了 443 端口作为 https 服务端口，且域名解析配置正确，此时可以在浏览器地址栏输入：https://m1.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 m1.cnnic.cn.cer

私钥保存文件 m1.cnnic.cn.key 即可。