

目录

目录	1
一、 关于 OpenSSL	2
1. OpenSSL 简介	2
2. OpenSSL 下载及安装配置	2
二、 申请服务器证书	3
1. 生成私钥	3
2. 生成 CSR 证书请求文件	4
三、 下载服务器证书	7
1. 准备下载证书所需信息	7
2. 下载证书	7
3. 关于证书的格式转换	10
4. 下载根证书及 CNNIC 中级根证书	12
四、 修改 Apache 配置文件	13
1. 找到 Apache 的配置文件	13
2. 创建证书链	13
3. 修改配置文件	14
五、 特别提示	15

一、关于 OpenSSL

1. OpenSSL 简介

OpenSSL 是一个在 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

登陆 OpenSSL 官方网站: <http://www.openssl.org/>

根据您的操作系统选择下载源代码包或已编译的二进制安装包，Windows 平台建议直接选择下载已编译的二进制安装包，可以节省配置编译环境的时间。这里需要特别说明一下，安装配置 OpenSSL 的这部分操作并不必要在服务器上进行，可以在本地的任意一台 Windows PC 上操作。

二、 申请服务器证书

本手册以 `www.cnnic.cn` 为例，详细讲解利用 OpenSSL 生成私钥以及证书请求文件的每一个步骤。

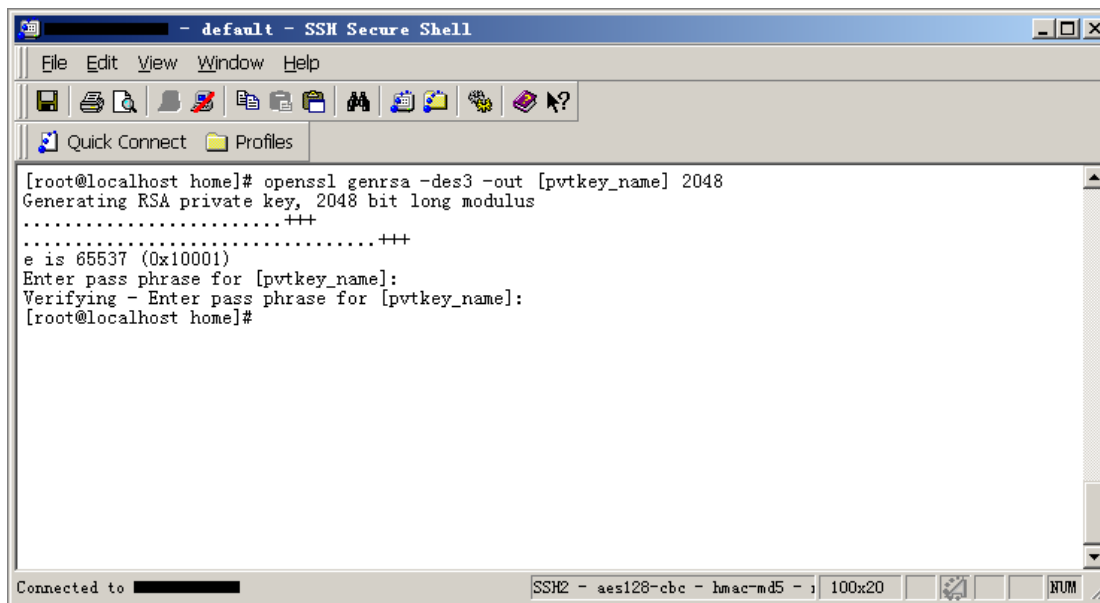
1. 生成私钥

命令格式：`openssl genrsa -des3 -out [pvtkey_name] 2048`

注：[] 中的内容为需要输入的参数

- `pvtkey_name`: 表示证书私钥的文件名，扩展名一般为 `key`

如下图所示：



```
[root@localhost home]# openssl genrsa -des3 -out [pvtkey_name] 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
Enter pass phrase for [pvtkey_name]:
Verifying - Enter pass phrase for [pvtkey_name]:
[root@localhost home]#
```

图表一 生成私钥

如上图所示，运行命令后会两次提示输入私钥的密码，此密码请牢记，将是您以后访问该私钥的依据。至此，2048 位的 RSA 私钥就已经生成了，私钥文件名为：`[pvtkey_name]`。该文件会存在于您运行 OpenSSL 命令时所处的文件夹位置。

<注：CNNIC 服务器证书要求 2048 位密钥长度>

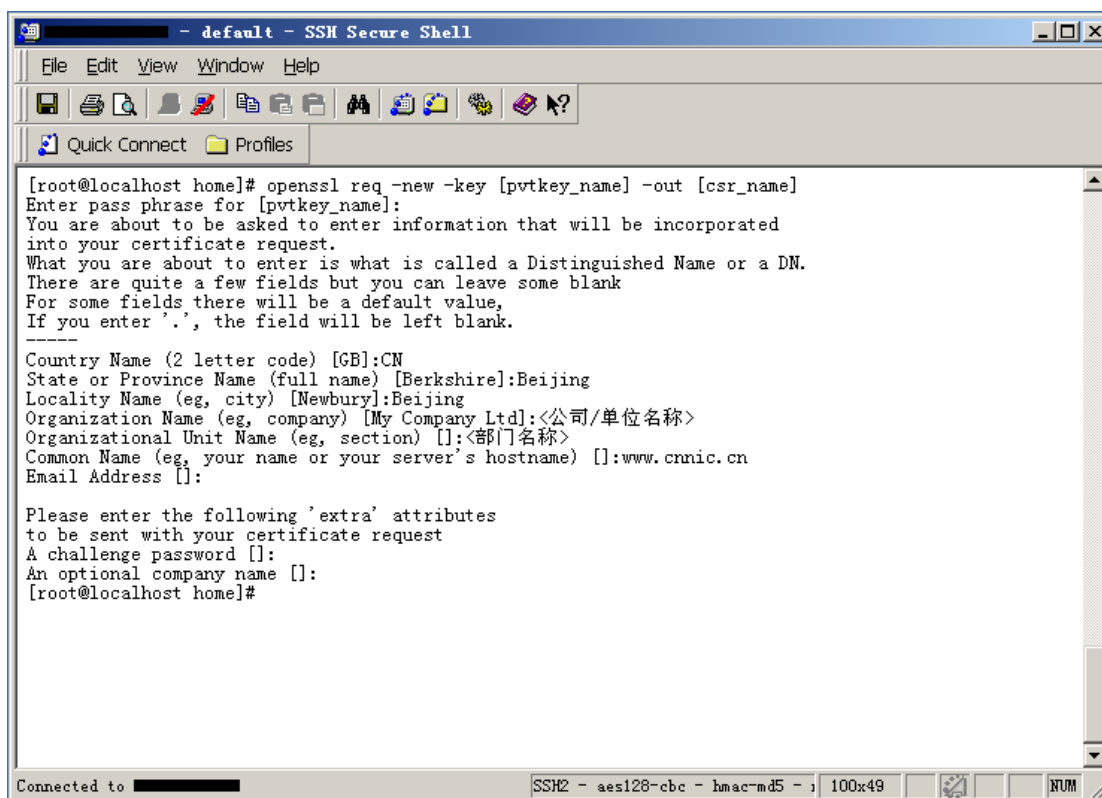
2. 生成 CSR 证书请求文件

命令格式：`openssl req -new -key [pvtkey_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
- `pvtkey_name`: 表示证书私钥的文件名，扩展名一般为 `key`

如下图所示：



图表二 生成 csr 文件

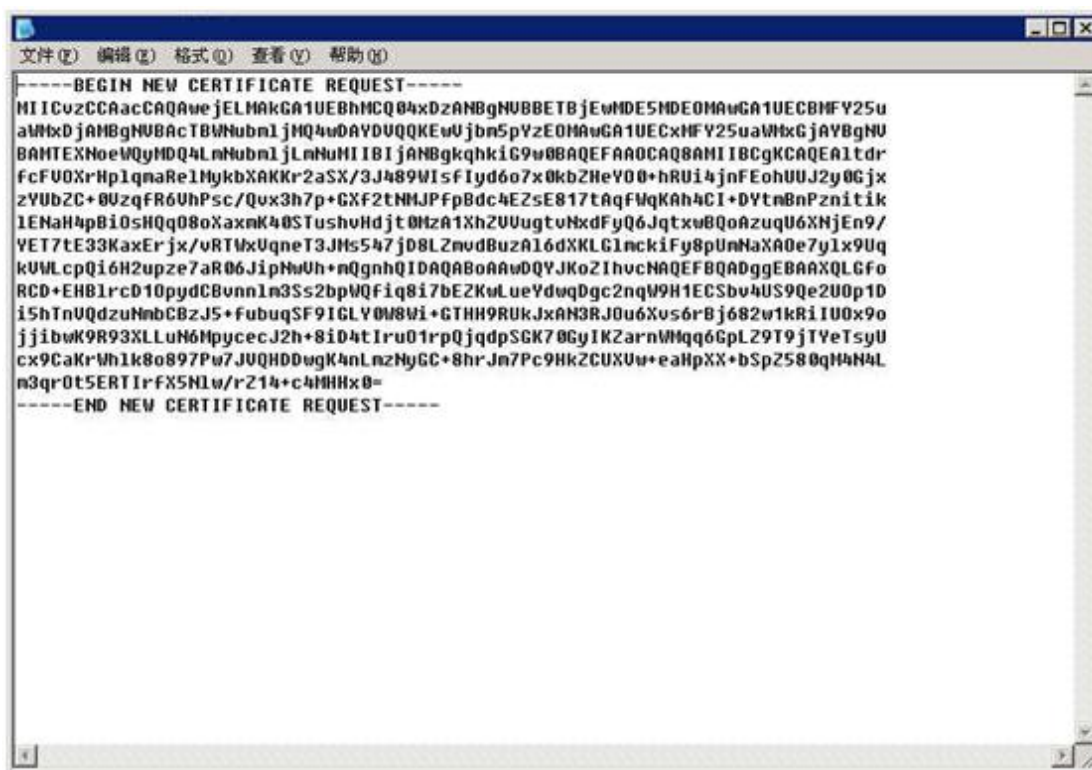
上述命令运行后，按照系统提示，首先输入私钥密码，然后按提示顺序输入 X.509 证书所要求的字段信息，包括国家(中国为 CN)、省份、所在城市、单位名称、单位部门名称(可以不填直接回车)。 **请注意：除国家名称一项必须填写二**

字母国家代码外，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完整域名，而不是您的真实名称与姓氏，例如：如果需要为 www.cnnic.cn 申请域名证书就必须输入 www.cnnic.cn 而不能输入 cnnic.cn。如果申请通配域名证书，则输入通配域名的形式，通配符为“*”，如：*.cnnic.cn；如果申请多域名证书，则输入多域名中第一个域名即可。

Email Address、challenge password、optional company name 请直接按回车键跳过，不需要输入任何信息。

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：



```

-----BEGIN NEW CERTIFICATE REQUEST-----
MIICvzCCAacCAQAwjELMAkGA1UEBhMCQ04xDzANBgNVBETBjEwMDE5MDE0MAUwGA1UECBMFY25u
aWVhDjAMBgNVBACITWlubmljHQ4wDAYSUQKQEWjbn5pYzE0MAUwGA1UECmFhY25uYWxkLmN1
BAHTEXNoeWQyMDQ4LnubmljLnubmljLmN1IjEjANBgkqhkiG9w0BAQEFAAOCQA8AMIIBCgKCAQEA
ltdrFcfU0XrHplqnaRe1MykbXAKKr2aSX/3J489WIsfIyd6o7x0kb2HeY00+hRUi4jnFEohUUJ2y0Gjx
zYUub2C+0UzqFR6UhPsc/Qvx3h7p+GXF2tNMJPfpBdc4EZsE817tAqfWqKAh4CI+DYtnBnPznitk
lENaH4pBi0sHQq08oXaxnK40STushvHdjt0HzA1XhZUUugtVhXdfYQ6JqtxwBQoAzU6XNjEn9/
YET7tE33KaxErjx/vRTVxUqneT3JHs547jd8LZnudBuzA16dXKLGlnckiFy8pUnNaXA0e7y1x9Uq
kUMLcpQi6H2upze7aR06JipNvUh+nQgnhQIDAQABoAAwDQYJKoZIhvcNAQEFBQADggEBAAXQLGfo
RCD+EHB1rcD10pydCBvnnl3Ss2bpWQfiq8i7bE2KwLueYdwqDgc2nqW9H1ECSbv4US9Qe2U0p1D
i5hTnUQdzuNmbCBzJ5+FubuqSF91GLV0M8wi+GTHH9RUKJxAN3RJ0u6Xus6rBj682w1kRiIU0x9o
jjjibwK9R93XLLuH6MpycecJ2h+8iD4tIruD1rpQjqdpSGK70GyIKZarnWHqq6GpLZ9T9jTYeTsyU
cx9CaKrWh1k8o897Pw7JUQHDDwgK4nLnzNyGC+8hrJm7Pc9HkZCUXUw+eahpXX+bSpZ580qH4N4L
n3qr0t5ERTIrFX5Nlw/rZ14+c4MHHX0=
-----END NEW CERTIFICATE REQUEST-----

```

图表三 查看 csr 文件

三、 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 官网，进入 CNNIC 服务器证书下载中心页面：

<http://www.cnnic.net.cn/jczyfw/fwqzs/fwqzsxxzx/>

点击相应的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="MV4K646JDDHAF8W5"/>
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>MIICrDCCAZQCAQAwZzELMAkGA1UEBhMCQ04xEDAOBgNVBAGTB2JlaWppbmcxEDAOBgNVBAcTB2JlaWppbmcxDjAMBgNVBAoTBWNum1jMQ4wDAYDVQQLewVjbm5pYzEU MBIGAlUEAxMLbTEuY25uaWMuY24wgwEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK AoIBAQcwZKe5sIA8Vv7uYleWQMUvos7K/dagHhyb9DYKouOSQ qJkHsFzAMUZzyjL kvE2tUTNtMqbPaxV8TGSg+AcC7zNABYdQpAUWw91dGoLqGtktOsQ/tWd0Bbi1Oj 8amCi/yRxkpPSPJPrLisBFCxwt+8wGj8WICj3vP8jOqnpUtkf x3S9AMfaAveGret lUF/80DBboVwJXCTKwcc+dHykjsiswAOiWYlgnArdeXn1gR4Y m59IjiFmOfiiBSK bGwVlNXJ21f6DsLFKf8JvZq9Yfdjc135QQPOpzGhr98TKzStv /6/c+ocG2yexgFt MZac/Z4lJh9iUmNkp69nbs1sHU5FAGMBAAGGADANBgkqhkiG9 wOBAQUFAAOCAQEA qGbSXekMJTPsS7VHuP1YzpkOaXN3D3AAyOoT7MC3pEDnlk49e 779Vxr2B13nFbh1</pre>
<input type="button" value="提交"/> <input type="button" value="重置"/>	

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、授权码和证书请求文件均无问题，则显示页面如下所示。

| 证书下载-证书生成

证书文件：	<pre> -----BEGIN CERTIFICATE----- MIIEGzCCAwOgAwIBAgIQEMCXznvJBxWzSSX3sUEd6DANBgkqhkiG9w0BAQUFADAyMQswCQYDVQQG EwJjbjEOMAwGA1UEChMFY25uaWMxEzARBgNVBAMTCmNubmljIHJvb3QwHhcNMTAxMjA3MDkzOTAw WhcNMTEwMjA3MDkzOTAwWjBhMQswCQYDVQQGEwJDTjENMAsGA1UECB4EUXdOrDENMAsGA1UEBx4E UxdOrDEOMAwGA1UEChMFY25uaWMxEzARBgNVBAsTBWVubmljMRQwEgYDVQQDEwttMS5jbm5pYy5j bjCCASIwdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALBkp7mWgDxW/u5iV5ZAxRU5Lsr91qAe HJv0Ngo645JComQewXMxRnPKMuS8Ta1RM2Oyps8DFXxMzIb4BwLvMOAHJ1CkBRbD3VOaguoA2R2 06xD+1Z3QFuLU6PxqYKL/JHGsk9I8k+suKwEULHC37zAaPxYgKPe8/yM6qe1S2R/HdLOAx9oC94a t62VQX/zQMFuhXAlcJMrDBz50fKSOyKzAA6JZiWCCcT17GfWBHhibn0iOIWY5+KIF IpsbBWWU1cnb V/oOwsUp/wm9mr1h92NyXf1BA86nMaFH3xMrNJO//r9z6hwbbJ7GAWOxlpz9niUmH2JSY2Snr2du </pre>
-------	--

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。

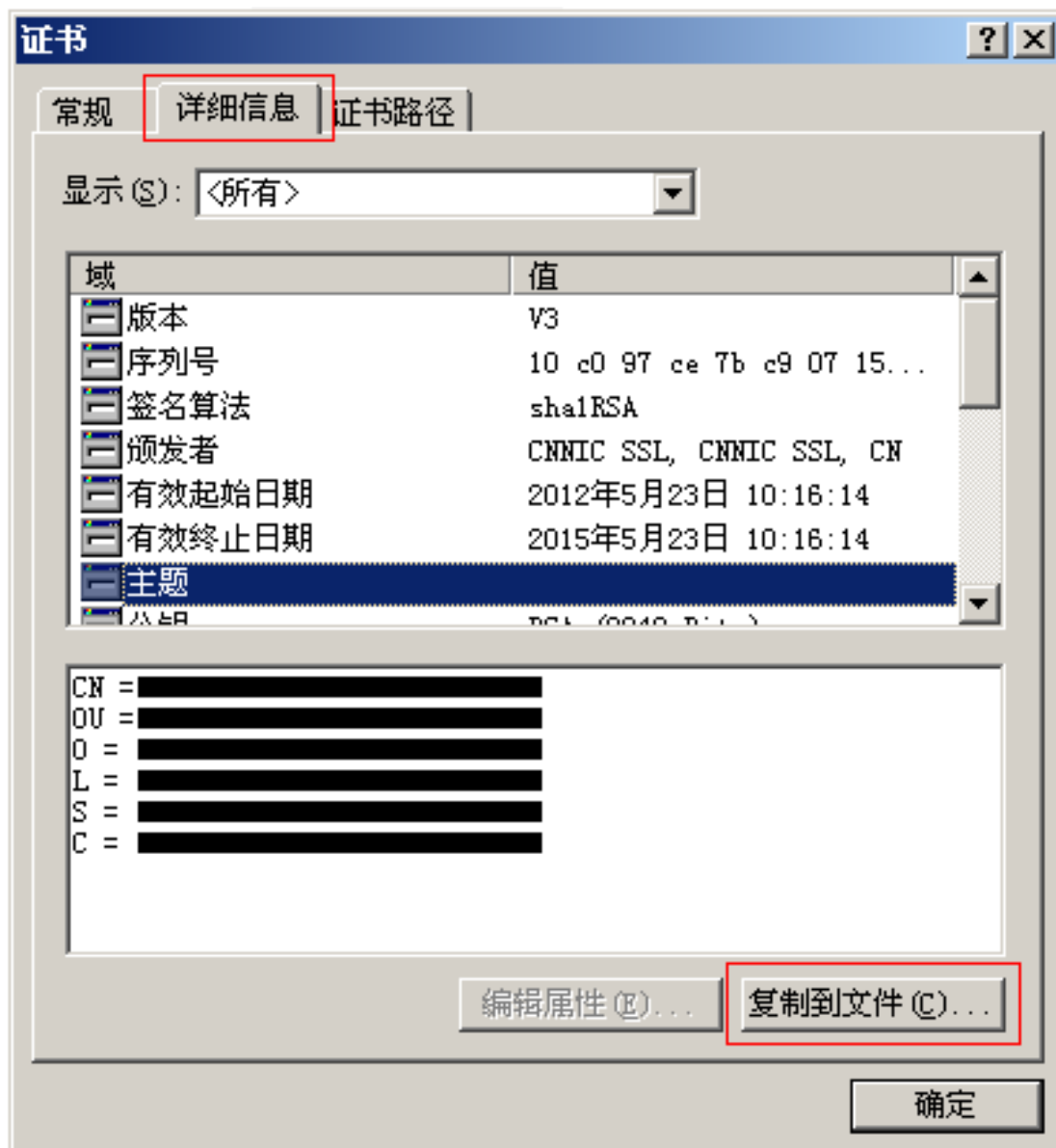
| 保存

图表六 生成证书

请按页面提示将文本框中的内容拷贝下来，粘贴到一个文本文档中保存，为文件起一个方便记忆的名字，以.cer为后缀。您也可以直接点击保存，自动下载一个名为WebCert.cer的文件，该文件即为申请的证书。**请妥善保存该文件，如果该证书丢失，就必须进行证书补发操作，此操作可能会有相应费用产生。**

3. 关于证书的格式转换

从CNNIC获得的证书格式为X.509格式。该将证书文件的扩展名改为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：



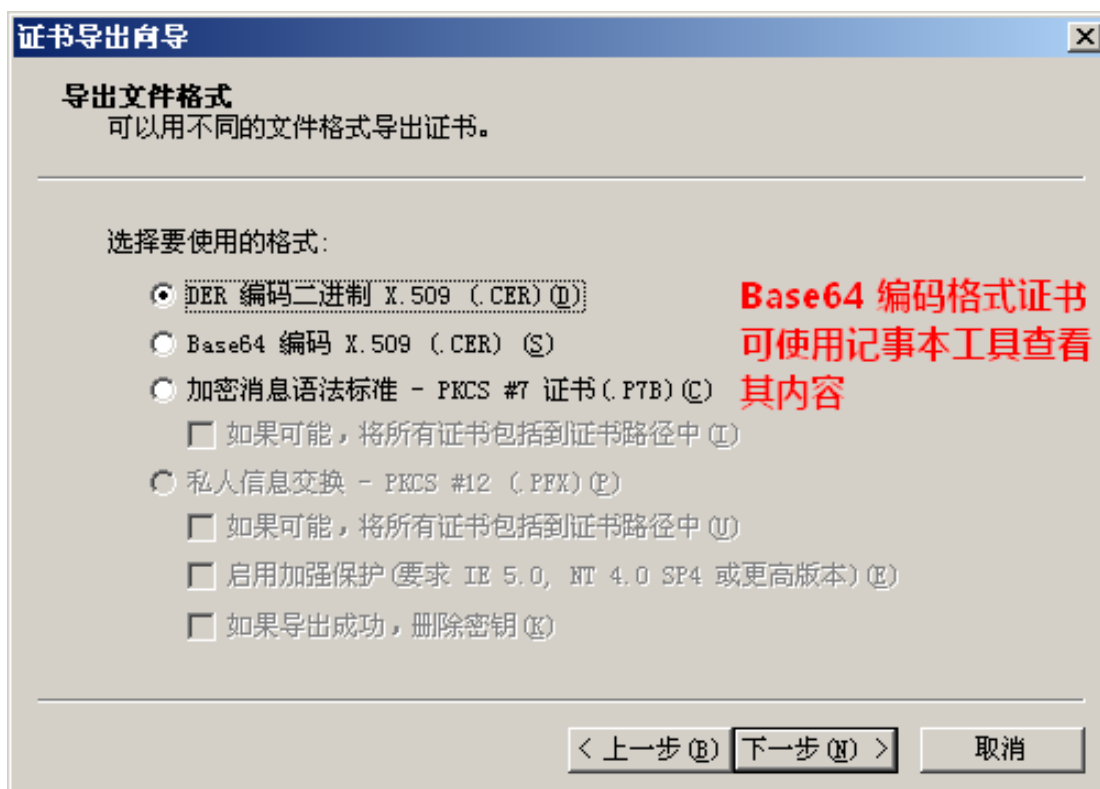
图表七 格式转换

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. 下载根证书及 CNNIC 中级根证书

根证书及 CNNIC 中级根证书下载地址：

<http://www.cnnic.net.cn/jczyfw/fwqzs/fwqzsxzzx/>

根据购买产品类型，点击相应的链接下载根证书以及中级根证书，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”。

四、修改 Apache 配置文件

1. 找到 Apache 的配置文件

首先确认您的 Apache 安装目录所在位置,打开该安装目录下的 conf 目录,并在 conf 目录下找到 httpd.conf 文件以及 extra 目录下的 httpd-ssl.conf 文件,这两个文件就是稍后所需要修改的 Apache 的配置文件,您可以文本方式打开它们并进行编辑。

2. 创建证书链

这里要用到您之前步骤所下载的中级根证书和根证书文件,首先创建一个名为 cert_chain.cer 的空文本文档,然后依次将 cnic.cer(中级根证书)、root.cer(根证书)两个文件以文本方式打开,将其中全部内容(包括“-----BEGIN CERTIFICATE-----”和“-----END CERTIFICATE-----”,每串证书代码之间均需要使用回车换行分隔)依次复制到新建的 cert_chain.cer 文档中。完成后的 cert_chain.cer 中应包含两段代码,大致结构如下图所示:



```
-----BEGIN CERTIFICATE-----
MIIEOzCCAvegAwIBAgIESTHAKTANBgkqhkiG9w0BAQUFADAgMQuCQYDVQQGEwJD
TjEONHAvGA1UEChMFQ0S0UHxEzARBgNVBAHTCkN0Tkd1DIFJPT1QwHhcNMTA1I4
:
:
中级根证书
+nGCA6PoFuXvKHFnKyH9DGLY71LDeKpdIL+z0Qq8rsKcSF9D+U0p5+T5j4LHR8Kp
janUk/yj7EMXcZxqHXR0kZaS0HwQF2aUwFYY4ZeJp2HrDeH=
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIDUTCCAj2gAwIBAgIESTHAKTANBgkqhkiG9w0BAQUFADAgMQuCQYDVQQGEwJD
TjEONHAvGA1UEChMFQ0S0UHxEzARBgNVBAHTCkN0Tkd1DIFJPT1QwHhcNMDc0NDU2
:
:
根证书
buXF6iFUiZx9FX+Y9QCJ7u0EwFyWtcUG6kbghUM2G8kS1sHNzYDzAgE8yGnLRUhj
2JTQ7IU0004R2FSCjKY9ri4i1AnIX0o8gV0VKg0XF1UJ24pBgp5nmxE=
-----END CERTIFICATE-----
```

图表九 证书链

至此，证书链文件已创建完成，将该证书链文件连同之前步骤生成的私钥文件以及下载的服务器证书文件一起，复制到 Apache 安装目录 conf 文件夹下，下面就可以来修改配置文件了。

3. 修改配置文件

首先打开 httpd.conf 文件，找到以下内容：

```
#LoadModule ssl_module modules/mod_ssl.so
#Include conf/extra/httpd-ssl.conf
```

分别删除行首的配置语句注释符号“#”，并保存退出。

再打开 conf/extra 目录中的 httpd-ssl.conf 文件，分别找到以下内容：

```
SSLCertificateFile "..您的 apache 的安装路径/conf/server.crt"
SSLCertificateKeyFile "..您的 apache 的安装路径/conf/server.key"
#SSLCertificateChainFile "..您的 apache 的安装路径/conf/server-ca.crt"
```

分别将这三条配置语句做以下修改：

```
SSLCertificateFile "..您的 apache 的安装路径/conf/WebCert.cer"
```

“WebCert.cer”是您下载的服务器证书文件。

```
SSLCertificateKeyFile "..您的 apache 的安装路径/conf/[pvtkey_name]"
```

“[pvtkey_name]”是您之前步骤生成的私钥文件，具体文件名以您的命名为准。

```
SSLCertificateChainFile "..您的 apache 的安装路径/conf/cert_chain.cer"
```

首先删除行首注释符号“#”，“cert_chain.cer”是您刚刚创建的证书链文件，包含中级根证书以及根证书代码。

修改完毕保存退出后，您可以尝试启动 Apache 服务，测试是否可以正常通过 https 方式访问您的域名。**测试成功后请务必妥善备份您的证书私钥文件以及服务器证书（链）文件。**

五、 特别提示

如果您的中间件环境（Nginx、Apache 等）是在 Windows 系统上搭建起来的，那么您在按照本手册进行操作后，在证书部署环节可能会遇到一些小问题，具体表现为 SSL/HTTPS 所使用的端口（例如 443 端口）无法启动，这时请不要紧张，我们这里为您提供了解决方案。

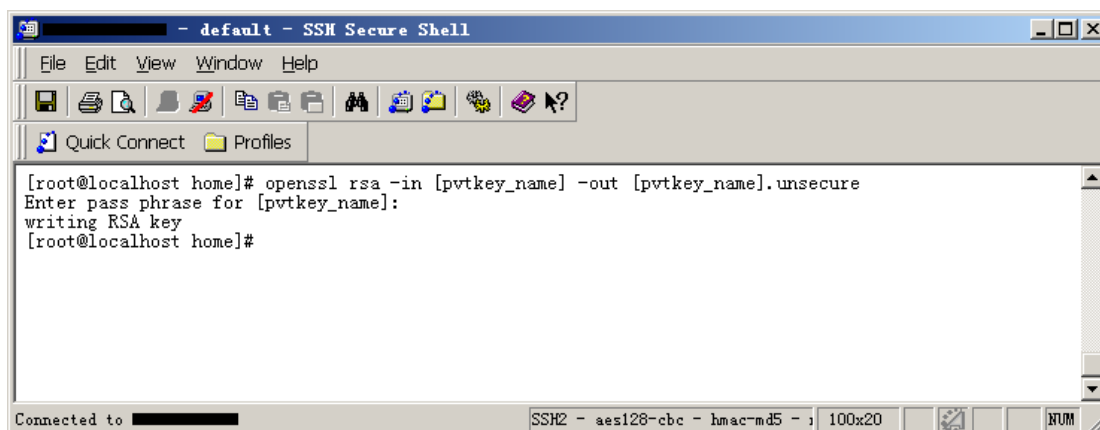
您只需要去掉私钥中的 DES 加密即可，具体您可以执行以下命令：

```
openssl rsa -in [pvtkey_name] -out [pvtkey_name].unsecure
```

注：[] 中的内容为需要输入的参数

- pvtkey_name: 表示证书私钥的文件名，扩展名一般为 key

如下图所示：



图表十 去掉私钥中的 DES 加密

这时候您就已经成功的去掉了私钥文件的 DES 加密，在私钥所在文件夹下会新生成一个后缀为 unsecure 的私钥文件，今后在访问这个新私钥文件时就不需要输入密码了，这也意味着您需要更加小心保存您的私钥文件。

接下来您只需要把新生成的没有密码的私钥文件配置到您的中间件中，如果

没有其他配置问题，SSL/HTTPS 便可以正常启动并监听预设端口。