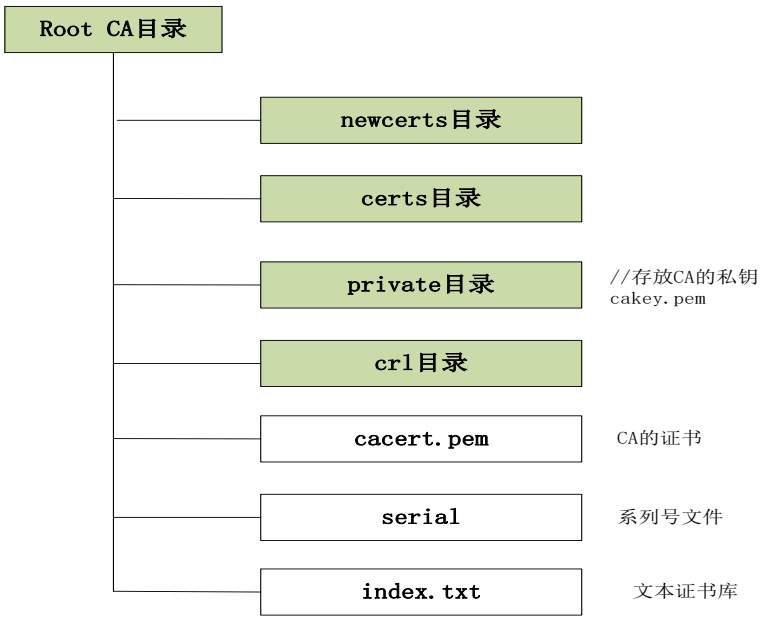
How to make SSL Certificates

The structure of CA，like below：



Comments:

newcerts // it is used to store new certificates,filename is the serial number, suffix ispem
certs // reserved first
private // it is used to store private key of CA, if no special private key, CA will use this private key to issue
crl //reserved first
serial //When CA is issued, it is used for serial umber
Index.txt // the library of text CA

Certificates making：

Create CA directory

1. Please copy ca.pl(attached in email) into C:\Program Files\Apache Software Foundation\Apache2.X\bin

Open cmd(command line in your PC), enter into path C:\Program Files\Apache Software Foundation\Apache2.X\bi, run perl ca.pl –newca, after running successfully, it will create a demoCA folder in current path

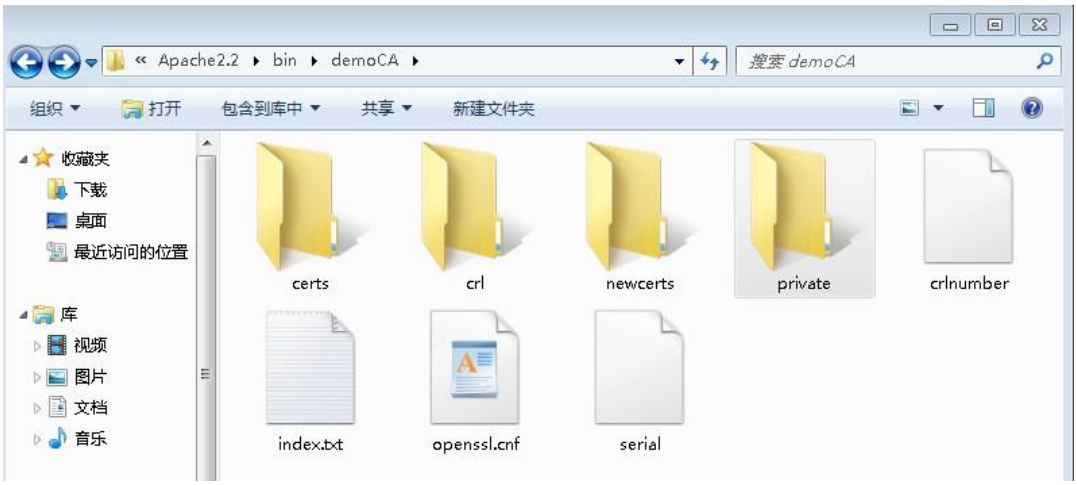
In demoCA path, please create a file named serial without any suffix, then open it by Ultra edit, write 01 in it, save and exist.

2. Copy openssl.cnf into demoCA folder

Openssl.cnf

(openssl.cnf file original path：
C:\Program Files\Apache Software Foundation\Apache2.x\conf)

You can find below folder and files in demoCA folder:



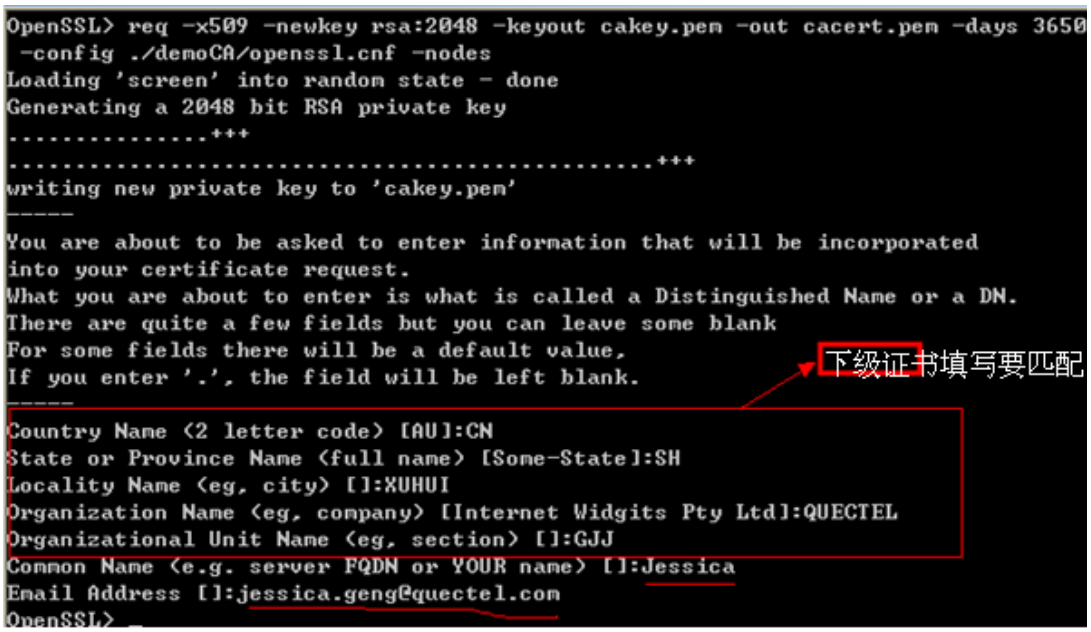
Generate self - signed root certificates and Root key

1. Open cmd, enter into C:\Program Files\Apache Software Foundation\Apache2.x\bin path, excute Openssl.exe, then execute following command:
req -x509 -newkey rsa:2048 -keyout ./demoCA/cakey.pem -out cacert.pem –days 3650 -config ./demoCA/openssl.cnf -nodes

Command description：
–days 3650 // The certificate's valid time is 365 days by default, this is set to 3650 (10 years, can be greater than 3650, according to the conditions set)
-x509 // Will generate a self-signed certificate, namely the root certificate
-newkey // Will generate a new CSR file, this option should take parameters, if generated RSA private key file, the parameter is a number specifying the private key file name of the bit
-keyout // show the filename of the created new private key file. If this option is not set,

will use the file name specified in the config file
-nodes // The generated private key file will not be encrypted
-config // the file name which used for config file

2. Certificate related information's configuration, an example like below

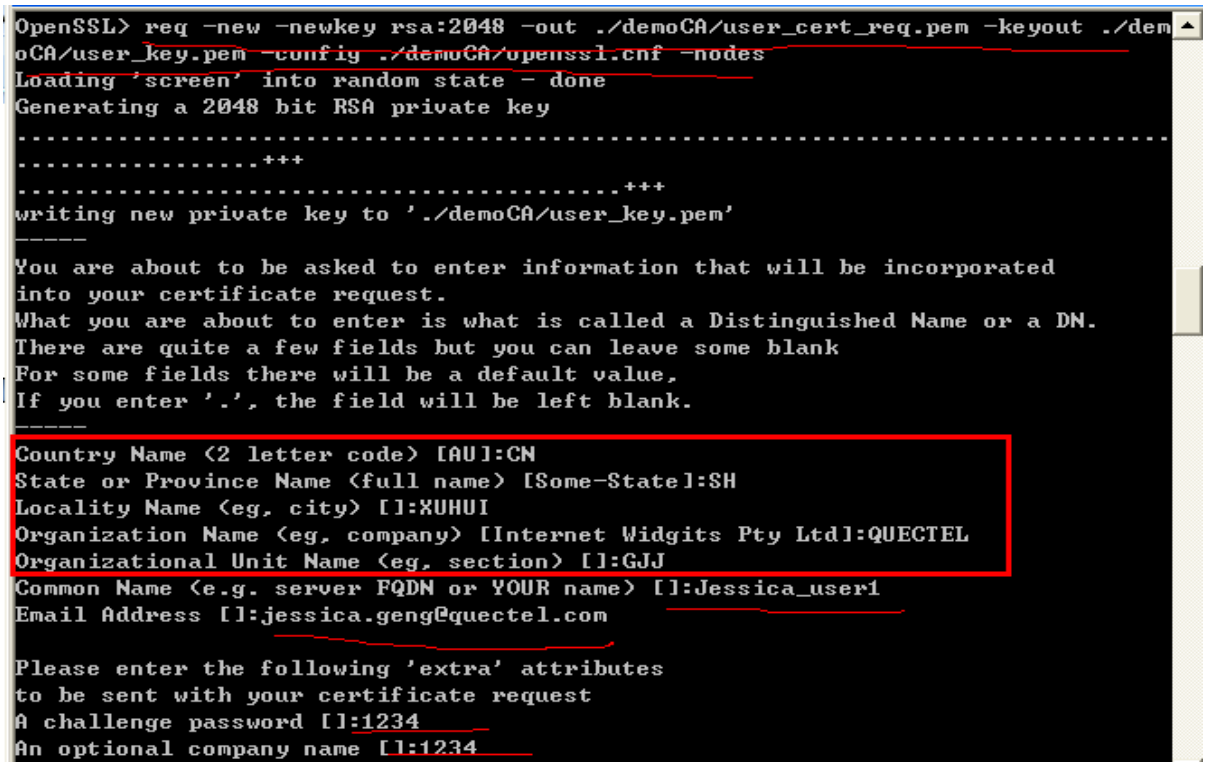


Note: The information should be matched with Subordinate certificates.

3. Generates a User Certificate Request
Open cmd, enter into C:\Program Files\Apache Software Foundation\Apache2.x\bin path, excute Openssl.exe, then execute the following command:
req -new -newkey rsa:2048 -out ./demoCA/user_cert_req.pem
-keyout ./demoCA/user_key.pem -config ./demoCA/openssl.cnf –nodes

Please note：
The following contents of root certificate should be matched with user certificate, expecially the red part below(email address should be different):

```
[ policy_match ]
countryName             = match
stateOrProvinceName     = match
organizationName        = match
organizationalUnitName  = optional
commonName              = supplied
emailAddress            = optional
```

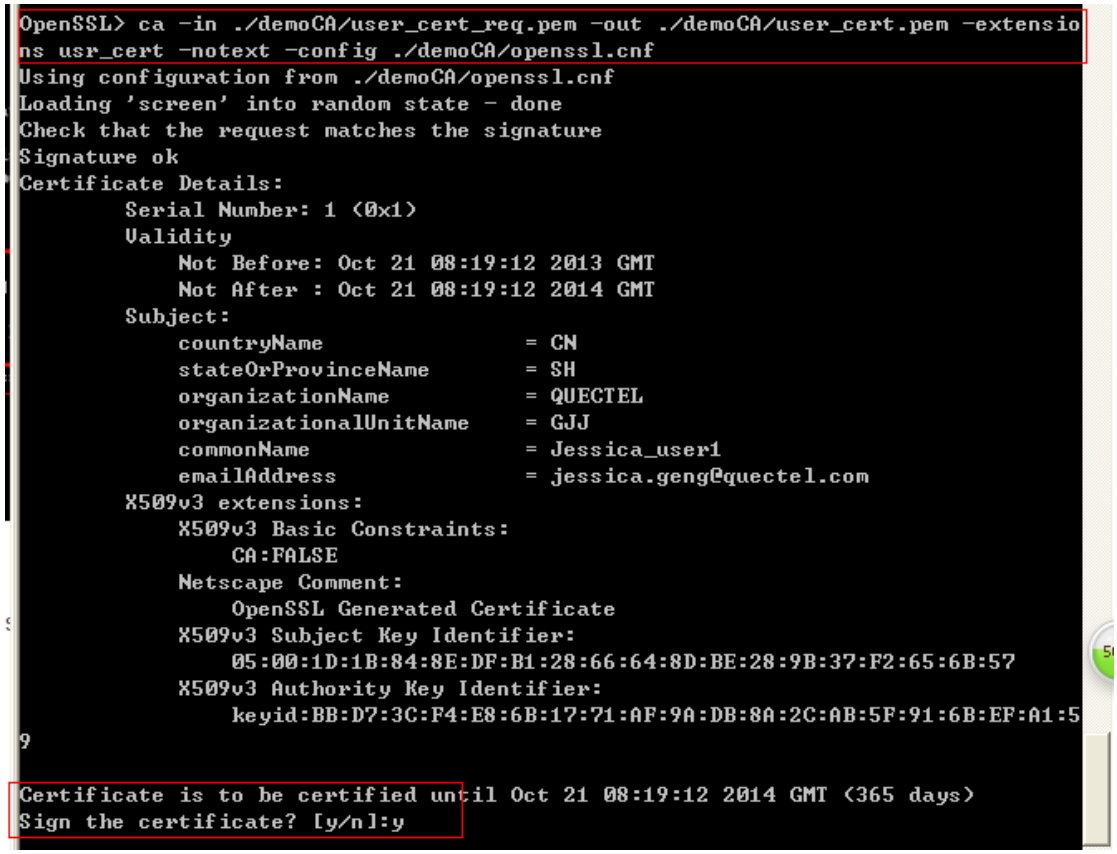


4. Please put cakey.pem in path demoCA\private, and put cacert.pem file from \bin directory to demoCA directory.

5. Create user certificate

Use cmd , enter into C:\Program Files\Apache Software Foundation\Apache2.x\bin，execute Openssl.exe, then execute following command：

ca -in ./demoCA/user_cert_req.pem -out ./demoCA/user_cert.pem -extensions usr_cert -notext -config ./demoCA/openssl.cnf



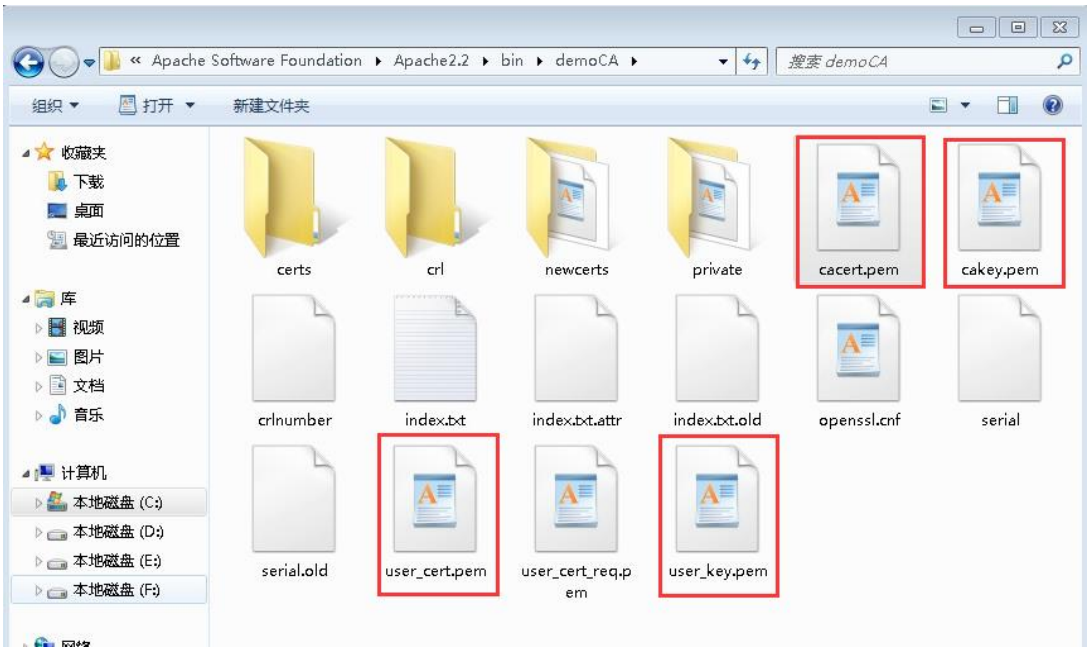
Create finished.

cacert.pem- root certificate

cakey.pem- root certificate’s private key

user_cert.pem- user certificate

user_key.pem- user certificate’s private key


Apache Software Foundation ▸ Apache2.2 ▸ bin ▸ demoCA ▸
搜索 demoCA
组织
打开
新建文件夹
收藏夹
下载
桌面
最近访问的位置
库
视频
图片
文档
音乐
计算机
本地磁盘 (C:)
本地磁盘 (D:)
本地磁盘 (E:)
本地磁盘 (F:)
certs
crl
newcerts
private
cacert.pem
cakey.pem
crlnumber
index.txt
index.txt.attr
index.txt.old
openssl.cnf
serial
serial.old
user_cert.pem
user_cert_req.pem
user_key.pem