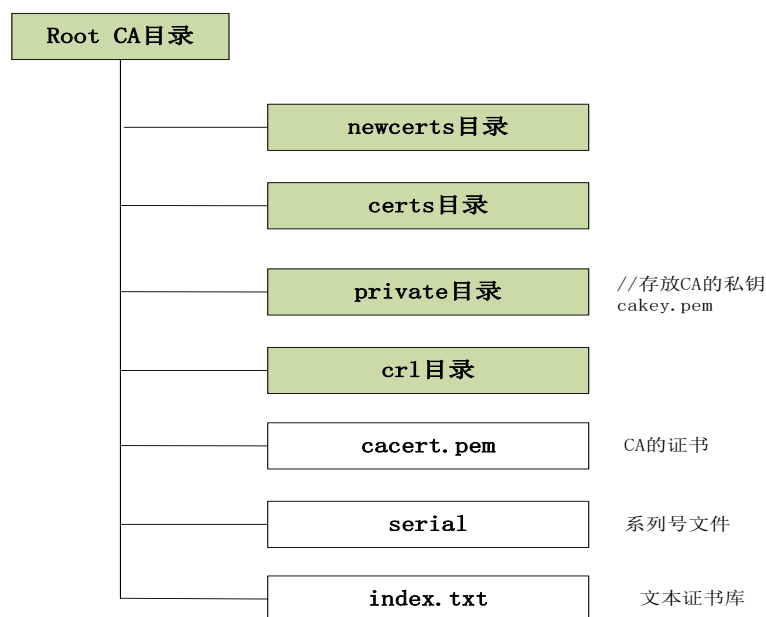


How to make SSL Certificates

The structure of CA, like below:



Comments:

newcerts // it is used to store new certificates,filename is the serial number, suffix is pem
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 number
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\bin, 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

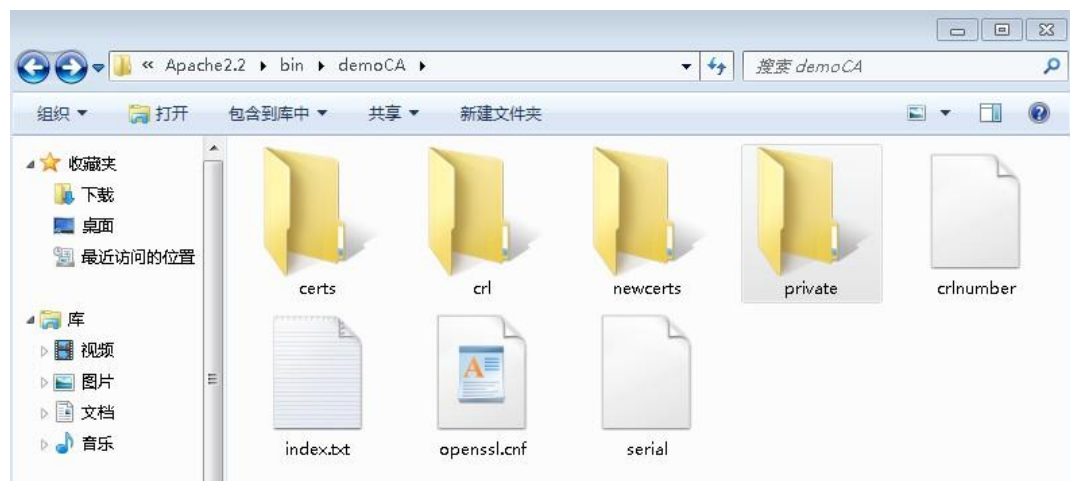


Openssl.cnf

(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
```

```
C:\Documents and Settings\Administrator.QUECTEL-JESSICA>cd C:\Program Files\Apache Software Foundation\Apache2.2\bin\  
C:\Program Files\Apache Software Foundation\Apache2.2\bin>openssl.exe  
OpenSSL> █
```

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

```
OpenSSL> req -x509 -newkey rsa:2048 -keyout cakey.pem -out cacert.pem -days 3650
-config ./demoCA/openssl.cnf -nodes
Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'cakey.pem'
-----
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]:SH
Locality Name <eg, city> []:XUHUI
Organization Name <eg, company> [Internet Widgits Pty Ltd]:QUECTEL
Organizational Unit Name <eg, section> []:GJJ
Common Name <e.g. server FQDN or YOUR name> []:Jessica
Email Address []:jessica.geng@quectel.com
OpenSSL>
```

下级证书填写要匹配

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, especially the red part below(email address should be different):

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

```
OpenSSL> req -new -newkey rsa:2048 -out ./demoCA/user_cert_req.pem -keyout ./demoCA/user_key.pem -config ./demoCA/openssl.cnf -nodes
Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to './demoCA/user_key.pem'
-----
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]:SH
Locality Name <eg. city> []:XUHUI
Organization Name <eg. company> [Internet Widgits Pty Ltd]:QUECTEL
Organizational Unit Name <eg. section> []:GJJ
Common Name <e.g. server FQDN or YOUR name> []:Jessica_user1
Email Address []:jessica.geng@quectel.com
-----
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:1234
An optional company name []:1234
```

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
```

```
OpenSSL> ca -in ./demoCA/user_cert_req.pem -out ./demoCA/user_cert.pem -extensions
ns usr_cert -notext -config ./demoCA/openssl.cnf
Using configuration from ./demoCA/openssl.cnf
Loading 'screen' into random state - done
Check that the request matches the signature
Signature ok
Certificate Details:
  Serial Number: 1 (0x1)
  Validity
    Not Before: Oct 21 08:19:12 2013 GMT
    Not After : Oct 21 08:19:12 2014 GMT
  Subject:
    countryName           = CN
    stateOrProvinceName   = SH
    organizationName      = QUECTEL
    organizationalUnitName = GJJ
    commonName            = Jessica_user1
    emailAddress          = jessica.geng@quectel.com
  X509v3 extensions:
    X509v3 Basic Constraints:
      CA:FALSE
    Netscape Comment:
      OpenSSL Generated Certificate
    X509v3 Subject Key Identifier:
      05:00:1D:1B:84:8E:DF:B1:28:66:64:8D:BE:28:9B:37:F2:65:6B:57
    X509v3 Authority Key Identifier:
      keyid:BB:D7:3C:F4:E8:6B:17:71:AF:9A:DB:8A:2C:AB:5F:91:6B:EF:A1:5
9
Certificate is to be certified until Oct 21 08:19:12 2014 GMT (365 days)
Sign the certificate? [y/n]:y
```

Create finished.

ca.crt.pem- root certificate

ca.key.pem- root certificate's private key

user_cert.pem- user certificate

user_key.pem- user certificate's private key

