



??

????? - Certificate Authority (CA)?????????????SSL????????? Server ? Root ?????

?????????????????????? Verisign ??

CA ???? Linux ? Windows ?????????? Linux ????Windows ?????????? Windows ???Certificate Service?

?????

- [Apache ???? SSL ??](#)
- [Configure vsftpd with SSL](#)
- [Symantec \(??? VeriSign\) ????????](#)
- [?? Linux CA ? Windows IIS ????????](#)

Let's Encrypt

- [How To Secure Apache with Let's Encrypt on Ubuntu 16.04](#)
- [SSL For Free ?? SSL ?????????? Let's Encrypt ??????????](#)
- [How to Use Let's Encrypt to Install Free SSL Certificates on Your Linux VPS](#)
- [Apache with Let's Encrypt Certificates on CentOS 8](#)
- [How to manage Let's Encrypt SSL/TLS certificates with certbot](#)
- [certbot](#)

Test SSL - ?????????? SSL ??????????

- <https://www.tecmint.com/testssl-sh-t...x-commandline/>
- <https://github.com/drwetter/testssl.sh>
- <https://testssl.sh/>
- <https://www.ssllabs.com/sslltest/>

Monitoring SSL

- <https://certificatemonitor.org>  
Source code: <https://github.com/RaymiiOrg/certifi...expiry-monitor>
- <https://alerts.httpsop.com>

????????????(self-signed)

????????????

?????	?????
?????(Private Key)	xxx.key

??????(CSR)	xxx.csr
Server ???	xxx_SERVER.crt
Root ???(?? CA ??)	xxxCA_ROOT.crt

??????

- openssl

??????

```
cd /etc/pki
mkdir -m 0755 mypbxCA/
mkdir -m 0755 private/ certs/ newcerts/ crl/
```

- mypbxCA ????????
- private ????????
- certs ????????
- newcerts ??? PEM ?
- crl ??????????????

?? openssl ???

```
cp /etc/pki/tls/openssl.cnf /etc/pki/mypbxCA/openssl.my.cnf
chmod 0600 /etc/pki/mypbxCA/openssl.my.cnf
touch /etc/pki/mypbxCA/index.txt
echo '01' > /etc/pki/mypbxCA/serial
```

?? CA(Root) ?? ? Private key

???????????????????? CA ?????????????????(??)????????? OSSLAB CA, Alang CA????? your-name CA

```
cd /etc/pki/mypbxCA
openssl req -config openssl.my.cnf -new -x509 -extensions v3_ca -keyout private/my-nameCA_ROOT.key
-out certs/my-nameCA_ROOT.crt -days 1825
```

Enter PEM pass phrase: <??????>

...

... <????>

Common Name (eg, your name or your server's hostname) []: <????? your-name CA????????????????????>

>

???????????????

????????????

1. private/my-nameCA\_ROOT.key ??????????????????
2. certs/my-nameCA\_ROOT.crt ?? ROOT ??????????????????

?? openssl ???

?? CARoot ????????????

?? /etc/pki/mypbxCA/openssl.my.cnf?

[ CA\_default ]

```
dir          = .          # ??? <==
certs       = $dir/certs  # Where the issued certs are kept
crl_dir     = $dir/crl    # Where the issued crl are kept
database    = $dir/index.txt # database index file.
#unique_subject = no      # Set to 'no' to allow creation of
                        # several certificates with same subject.
new_certs_dir = $dir/newcerts # default place for new certs.

certificate = $dir/certs/my-nameCA_ROOT.crt # ??? <==
serial      = $dir/serial # The current serial number
crlnumber   = $dir/crlnumber # the current crl number
                        # must be commented out to leave a V1 CRL
crl         = $dir/crl.pem # The current CRL
private_key = $dir/private/my-nameCA_ROOT.key # ??? <==
RANDFILE    = $dir/private/.rand # private random number file
```

???? Server ??

?? Server ??????(Private key)???????(CSR)

cd /etc/pki/mypbxCA

```
openssl req -config openssl.my.cnf -new -nodes -keyout private/this-is-my-host_SERVER.key -out
this-is-my-host_SERVER.csr
```

```
Country, State, Locality, Organization <????????? CARoot ??????>????????????????????? *.crt ??????
# openssl x509 -in certs/alongCA_ROOT.crt -noout -text
```

????????????

Common Name?<????????????????????? FQDN>

A challenge password []: <?????????????????????>

????????????

1. private/this-is-my-host\_SERVER.key Server ????
2. this-is-my-host\_SERVER.csr Server ????????(CSR)

????(?????????????????)

```
chown root:asterisk /etc/pki/mypbxCA/private/this-is-my-host_SERVER.key
chmod 0440 /etc/pki/mypbxCA/private/this-is-my-host_SERVER.key
```

??(??)????? CSR ?

??? CARoot ?????????? Server ??????????????

- ?????????? CARoot ??????
- ?? CSR ?????????????? CARoot ?????????????? Country, State, Locality,.....?????????????????

cd /etc/pki/mypbxCA

```
openssl ca -config openssl.my.cnf -in this-is-my-host_SERVER.csr -out certs/this-is-my-host_SERVER.crt
```

Using configuration from openssl.my.cnf

Enter pass phrase for ./private/this-is-my-host\_ROOT.key: <????? Root ??????????????????????>

Certificate is to be certified until Jul 29 03:40:03 2013 GMT (365 days)

Sign the certificate? [y/n]: <??y?????????????????>

1 out of 1 certificate requests certified, commit? [y/n] <?? y>

????????????? 365 ?????????? -days 3650

?????????????

1. certs/**this-is-my-host\_SERVER.crt** Server ???
2. newcerts/**01.pem** ??? Server ?????????????? serial ??????????

?????? Server ???

cd /etc/pki/mypbxCA

```
openssl x509 -in certs/this-is-my-host_SERVER.crt -noout -text
```

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 1 (0x1)

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=TW, ST=MyPBX, L=TC, O=Home, CN=this.is.my.host

Validity

Not Before: Jul 28 04:19:52 2012 GMT

Not After : Jul 28 04:19:52 2013 GMT

Subject: C=TW, ST=myPBX, L=Taichung, O=Home, OU=Net, CN=this.is.my.host

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:bc:8c:81:3e:b3:5b:30:f9:52:43:86:48:b8:18:
92:10:4f:63:c8:57:52:41:9b:40:b6:09:db:a4:82:
6c:79:56:c4:4e:a6:e6:48:69:9a:9e:6f:e7:6e:13:
32:9e:d3:cc:95:ea:56:5c:17:84:76:56:aa:3a:92:
45:41:32:0a:af:b2:ea:ae:c0:7a:8b:5d:af:ad:8e:
07:5f:c9:36:2e:47:c9:fe:1b:4d:a4:fa:00:b0:34:
46:f1:b4:00:51:dd:1f:69:18:94:79:c9:4b:22:c4:
6a:d3:49:5d:2e:14:92:4a:46:79:95:0a:1a:05:00:
77:ce:1a:30:9e:2d:c8:39:93

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints:

CA:FALSE

Netscape Comment:

OpenSSL Generated Certificate

X509v3 Subject Key Identifier:

5C:FF:F7:F0:69:80:E0:2F:16:39:98:7E:18:6E:83:12:14:46:69:53

X509v3 Authority Key Identifier:

keyid:37:E7:1F:96:48:52:C7:D2:E9:32:31:F8:42:00:04:C3:89:D1:A0:FE

Signature Algorithm: sha1WithRSAEncryption

b3:3d:4b:22:f3:89:c1:84:08:a0:5d:a6:3a:d0:ca:57:3c:02:
1b:d4:f4:3c:5d:f3:f8:dd:8d:b6:19:8d:e9:1d:7c:3e:ba:28:
8d:df:7d:a2:3f:90:9e:34:47:37:a7:17:28:4c:3b:a8:c2:da:
81:ae:00:13:9a:fa:dd:c5:ba:56:06:06:9a:e7:e2:47:c1:9b:
eb:56:58:f9:4d:00:53:42:80:cc:e8:17:80:46:e4:d0:65:2c:
c3:f0:5a:d5:2c:3d:a3:1e:89:4d:19:57:03:d7:a0:93:c4:77:
87:03:8b:7c:17:9d:ee:92:08:b4:2e:a2:aa:a3:99:18:5b:f8:
a9:f8

?? PKCS#12 ????)

???? Apache ? SSL ??????(SSLVerifyClient require)????????????????????

????)

??? Root ??????)

openssl pkcs12 -export -clcerts -in certs/my-nameCA\_ROOT.crt -inkey private/my-nameCA\_ROOT.key
-out my-nameCA\_ROOT.p12

????my-nameCA\_ROOT.p12 (???? .p12)

NOTE:

???? CARoot ?????

???? Export ?????????????????????

????)

???? Cient ??????? CARoot ??????? PKCS#12

??? CARoot ??????? (?? CSR ?????????? CARoot ???????)?

openssl x509 -in certs/my-nameCA\_ROOT.crt -noout -text

Certificate:

....

Issuer: C=TW, ST=MyPBX, L=TC, O=Home, CN=this.is.my.host

...

Subject: C=TW, ST=MyPBX, L=TC, O=Home, CN=this.is.my.host

...

??

- C - Country
- ST - State or Province Name
- L - Locality Name
- O - Organization Name
- CN - Comman Name

?? Client ????? CSR

openssl req -config openssl.my.cnf -new -nodes -keyout private/this-is-my-host\_CLIENT.key -out this-is-my-host\_CLIENT.csr

Enter PEM pass phrase: <?? CLIENT?????>

?????? CARoot ?????????????????

A challenge password [] <??????>

?? Client CSR

openssl ca -config openssl.my.cnf -in this-is-my-host\_CLIENT.csr -out certs/this-is-my-host\_CLIENT.crt

Enter pass phrase for... <?? CARoot ????>

...

Certificate is to be certified until Jul 29 03:40:03 2013 GMT (365 days)

Sign the certificate? [y/n]: <??y????????????????>

1 out of 1 certificate requests certified, commit? [y/n] <?? y>

???????????????? -days 3650

????? PKCS12

```
openssl pkcs12 -export -clcerts -in certs/this-is-my-host_CLIENT.crt -inkey private/
this-is-my-host_CLIENT.key -out this-is-my-host_CLIENT.p12
```

NOTE:

???????????????? -days 3650

?? \*.csr ???????????? CARoot ????????????????????

????????? CARoot ??????

?? pkcs12 ??????? Export ????????????????????????

?????????????????

?????????? CA ?????????????????????? Key?CSR?? CRT ??????

? Nginx ??????

```
mkdir /etc/nginx/ssl
```

```
openssl req -x509 -nodes -days 3650 -newkey rsa:2048 -keyout /etc/nginx/ssl/
raida13-cloudcoin-global.key \
-out /etc/nginx/ssl/raida13-cloudcoin-global.crt
```

for Apache?

```
openssl genrsa -out my-test-web.key 2048
```

```
openssl req -new -key my-test-web.key -out my-test-web.csr
```

```
openssl x509 -req -days 3650 -in my-test-web.csr -signkey my-test-web.key -out my-test-web.crt
```