Setting up SSL for Apache on openSUSE 11

□□□ Web server □□□ Client □□□□ SSL/TLS.

1. □□□□□□□□□□□□□□ (Certificate of Authority - CA)

$ mkdir /root/ca
$ cd /root/ca

- □□□□□ CA □□□□□□□□□□□□ 2048 bit.

$ openssl genrsa -des3 -out newca.key 2048
Generating RSA private key, 2048 bit long modulus
.................................+++
.................+++
e is 65537 (0x10001)
Enter pass phrase for newca.key: <□□□□□□□□□□□□□□□□□ PEM>
Verifying - Enter pass phrase for newca.key: <□□□□□□□□□□□□□□□□□□□□□ PEM>

- □□□□□ X.509 Certificate □□□□□□□□□ 2 □□ (□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□)

$ openssl req -new -x509 -days 730 -key newca.key -out newca.crt

Enter pass phrase for newca.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]:TH
State or Province Name (full name) [Some-State]:Bangkok
Locality Name (eg, city) []:Thailand
Organization Name (eg, company) [Internet Widgits Pty Ltd]:My Company, LTD.
Organizational Unit Name (eg, section) []:IT
Common Name (eg, YOUR name) []:*.mydomain.com
Email Address []:support@mydomain.com

- □□□□□□□□□□□□ Certificate □□□□□□□□

$ openssl x509 -in newca.crt -text -noout

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
8e:63:fd:8a:a1:a4:77:af
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=TH, ST=Bangkok, L=Thailand, O=My Company, LTD., OU=IT,
CN=*.mydomain.com/emailAddress=support@mydomain.com
Validity
Not Before: Nov 28 06:48:50 2009 GMT
Not After : Nov 28 06:48:50 2011 GMT
Subject: C=TH, ST=Bangkok, L=Thailand, O=My Company, LTD., OU=IT,
CN=*.mydomain.com/emailAddress=support@mydomain.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit):
00:cc:5c:da:bc:ed:08:e6:c4:9a:a4:e9:c0:37:f7:
ea:48:b5:2b:e4:26:00:04:9a:2d:83:35:58:ca:b4:
85:7d:00:5a:da:5b:fc:28:58:38:6b:c5:0a:b2:97:
84:dc:d2:8c:76:4e:a5:e4:1d:36:8c:39:f5:b7:bc:
c9:5c:0f:63:13:7a:99:01:9c:19:d9:be:36:0d:57:
b4:53:ff:59:b1:9c:e0:e5:2b:a7:81:f6:9e:4a:50:
94:dd:75:d1:73:ef:f8:ab:7e:d4:70:ed:45:76:00:
bd:c8:aa:47:e0:c4:eb:8c:15:f8:56:40:23:dc:75:
46:5c:95:24:bb:ba:1e:a0:a4:95:aa:33:40:04:f0:
1d:b6:f0:80:fe:bd:42:38:97:a5:10:27:e5:d7:d0:
12:4d:ba:fa:1a:ed:f9:95:6d:93:5f:18:ab:cd:d0:
c4:5a:cd:e9:7c:e4:b4:bb:71:86:e2:ec:7b:32:87:
f5:13:1b:8e:21:8b:fe:9d:bb:64:0b:87:6e:2e:dc:
4c:da:30:a3:8f:50:a9:0c:b9:2b:2e:12:0f:55:83:
12:ad:df:f2:b4:06:ec:14:2b:00:2c:c1:53:74:a7:
80:93:e4:91:a3:ea:28:6b:45:a2:5b:5c:06:a4:ae:
0a:f0:07:f4:90:c6:e3:e8:ad:da:90:54:46:72:e4:
7f:97
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Key Identifier:
85:B0:D4:A8:8C:9C:7E:AE:EB:54:B9:D5:FF:51:B0:F6:62:30:AF:22
X509v3 Authority Key Identifier:
keyid:85:B0:D4:A8:8C:9C:7E:AE:EB:54:B9:D5:FF:51:B0:F6:62:30:AF:22
DirName:/C=TH/ST=Bangkok/L=Thailand/O=My Company,
LTD./OU=IT/CN=*.mydomain.com/emailAddress=support@mydomain.com
serial:8E:63:FD:8A:A1:A4:77:AF

X509v3 Basic Constraints:

CA:TRUE
Signature Algorithm: sha1WithRSAEncryption
62:eb:b2:1d:13:1f:41:38:95:a2:c4:fc:a6:13:64:fc:b6:dd:
bc:78:65:25:88:3a:cc:e8:0c:0d:4a:7b:e9:5a:8d:d5:06:0d:
04:b1:9e:17:ba:ac:01:96:84:ab:64:5c:73:8a:3c:e8:ee:74:
e9:36:da:d7:27:94:13:47:ae:de:d2:27:d3:48:13:1b:60:c7:
88:53:dc:6d:fe:ef:8d:ab:1d:ab:76:0b:f6:3c:06:1e:0b:92:
94:50:2c:2c:53:6e:1b:6d:f8:c3:c9:01:2b:74:3d:1a:5d:66:
6c:4e:96:fa:0d:81:4d:8a:f9:43:87:0b:94:39:70:ed:d5:0c:
50:d6:40:c8:4a:d0:68:4c:b8:0d:9d:8d:33:1f:97:8e:40:09:
47:c5:a9:77:67:02:11:dc:ce:9e:e1:43:45:49:23:b5:5c:30:
97:26:c9:df:04:fb:19:d3:7b:d3:16:2e:f0:31:1e:62:c2:50:
d5:dc:0f:99:db:38:4b:6c:f0:1c:5b:63:9a:bb:83:11:35:a3:
6c:db:54:6a:c1:81:35:f4:a1:63:3d:e9:51:4e:09:9d:bd:cd:
42:cf:15:2a:cb:05:e6:c9:10:d9:78:02:12:3d:be:73:c1:06:
e5:ef:a9:b2:ee:eb:cb:55:43:a6:e0:f6:6b:55:98:79:69:ec:
a0:8f:f4:41

2. □□□□□□□□□□ □□□□ □□□□□□□□□□□□□□□□□□□□□□□□□□□□ **(Key & Certificate)** □□□□□□□ **Web Server (Apache2)**

$ openssl genrsa -des3 -out ap2server.key 1024

Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)
Enter pass phrase for ap2server.key:
Verifying - Enter pass phrase for ap2server.key:

- □□□□□ **Certificate Signed Request (CSR)**

$ openssl req -new -key ap2server.key -out ap2server.csr

Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)
Enter pass phrase for ap2server.key: <□□□□□□□□>
Verifying - Enter pass phrase for ap2server.key: <□□□□□□□□□□□□□□□□>
linux-wifi:~/ca # openssl req -new -key ap2server.key -out ap2server.csr
Enter pass phrase for ap2server.key:
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]:TH
State or Province Name (full name) [Some-State]:BKK
Locality Name (eg, city) []:THAILAND
Organization Name (eg, company) [Internet Widgits Pty Ltd]:MY COMPANY, LTD.
Organizational Unit Name (eg, section) []:IT
Common Name (eg, YOUR name) []:www.mydomain.com
Email Address []:webmaster@mydomain.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []: <Enter>
An optional company name []: <Enter>

Note: Common Name □□□□□□□□□□□□□□□□□□□□□□□□□□ (FDN)

- □□□□□ **Server Signed Certificate** □□□□□□ **CA** □□□ **CSR**

$ openssl x509 -req -in ap2server.csr -out ap2server.crt -sha1 -CA newca.crt -CAkey newca.key -CAcreateserial -days 730

Signature ok
subject=/C=TH/ST=BKK/L=THAILAND/O=MY COMPANY,
LTD./OU=IT/CN=www.mydomain.com/emailAddress=webmaster@mydomain.com
Getting CA Private Key
Enter pass phrase for newca.key: <□□□□□□□□>

$ openssl x509 -in ap2server.crt -text -noout

Certificate:
 Data:
 Version: 1 (0x0)
 Serial Number:
 9b:b6:4d:a9:d7:3c:15:9e
 Signature Algorithm: sha1WithRSAEncryption
 Issuer: C=TH, ST=Bangkok, L=Thailand, O=My Company, LTD., OU=IT,
CN=*.mydomain.com/emailAddress=support@mydomain.com
 Validity
 Not Before: Nov 28 07:03:33 2009 GMT
 Not After : Nov 28 07:03:33 2011 GMT
 Subject: C=TH, ST=BKK, L=THAILAND, O=MY COMPANY, LTD., OU=IT,
CN=www.mydomain.com/emailAddress=webmaster@mydomain.com

```
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
00:ce:47:b5:e2:e7:8b:6e:c2:6c:7a:3e:fa:d2:cb:
b6:fa:a9:b4:9f:12:db:8f:c7:63:5e:9b:b4:09:cb:
a2:13:11:da:a6:4d:fd:76:b1:b2:4c:cf:c6:e1:95:
0a:00:2c:17:2e:66:82:0d:1d:8f:6d:27:26:0d:ca:
2e:39:54:4e:d2:7e:5b:35:86:e3:17:cb:c7:39:23:
b8:4c:a7:4c:a9:6f:ef:c4:65:75:68:59:c9:19:59:
50:39:83:a0:41:c0:5a:cf:3e:14:b5:4b:72:9b:fc:
49:b3:22:86:8e:0d:73:08:0e:35:65:80:2e:64:a9:
e2:df:c6:3b:31:89:b6:c7:8f
Exponent: 65537 (0x10001)
Signature Algorithm: sha1WithRSAEncryption
b1:58:ca:02:6d:b5:05:60:8d:1a:b8:f0:49:a4:e2:c9:cc:b3:
55:80:8e:28:b4:bc:5b:b1:65:84:6f:1b:ca:5b:79:07:45:47:
47:8c:a6:fd:c1:b6:b0:7f:a1:00:c7:bf:22:c7:82:27:0d:f4:
7e:cd:9a:fc:1c:93:a2:15:26:ca:06:e4:d9:51:58:59:71:a3:
84:59:41:ae:dc:06:6e:2c:e4:e5:a6:48:51:df:6b:2e:21:7b:
96:f0:28:75:df:72:6e:d0:7c:d9:9b:fc:69:b8:ce:23:05:ef:
66:5e:cb:62:16:2f:35:9b:5a:06:79:eb:88:48:2f:f8:4b:10:
31:59:7b:d4:05:c5:03:a8:88:37:c7:1e:37:f1:a3:75:af:9d:
34:9f:b6:0a:3c:5e:b1:a3:d6:a2:d3:70:13:d3:f7:a0:94:ca:
11:46:de:1c:2c:7a:45:25:f2:1f:59:e2:e0:03:12:a1:e0:aa:
65:4e:5e:e6:e4:bf:b3:61:a8:f4:6d:15:ee:f9:e1:e4:10:55:
cd:d3:fb:a1:47:77:8e:24:b3:0e:e5:df:31:04:6d:cb:99:b0:
c6:4f:31:40:10:69:a4:fa:0e:9e:fe:ba:07:20:52:13:9d:d1:
12:d0:9b:85:b7:9e:2d:3a:87:28:fe:5e:fa:16:96:63:cf:73:
62:e3:01:b3
```

- □□□□□□ **Certificate** □□□□□□□□□□□□□□□□□□ **Apache**

```
$ cp ap2server.crt /etc/apache2/ssl.crt/
$ cp ap2server.key /etc/apache2/ssl.key/
$ cp newca.crt /etc/apache2/ssl.crt/
```

3. □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

```
$ mkdir /srv/www/htdocs/ssl-site
$ cd /srv/www/htdocs/ssl-site
```

- □□□□□□□□□□ **index.html** □□□□□□□□□□□□□□□□□□

$ vi index.html

```
<html>
<head><title>SSL Testing</title></head>
<body>
<center>
Encrypted!
</center>
</body>
</html>
```

$ cd ..
$ chown wwwrun.www ssl-site/ -R

4. □□□□□□□ Apache Web Server □□□□□□□□□□□□□□□□ SSL

- □□□□□ virtual host □□□□□□□□□□□□□□□□□□□ template

$ cp /etc/apache2/vhosts.d/vhost-ssl.template /etc/apache2/vhosts.d/ssl-site.conf

$ vi /etc/apache2/vhosts.d/ssl-site.conf

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□.

```
<VirtualHost _default_:443>

 #  General setup for the virtual host
 DocumentRoot "/srv/www/htdocs"
 ServerName www.mydomain.com:443
 ServerAdmin webmaster@mydomain.com
 ErrorLog /var/log/apache2/error_log
 TransferLog /var/log/apache2/access_log
 #   SSL Engine Switch:
 #   Enable/Disable SSL for this virtual host.
 SSLEngine on
 SSLCipherSuite
ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
 SSLCertificateFile /etc/apache2/ssl.crt/ap2server.crt
 SSLCertificateKeyFile /etc/apache2/ssl.key/ap2server.key
 SSLCertificateChainFile /etc/apache2/ssl.crt/newca.crt

 <Directory "/srv/www/htdocs/ssl-site">
 Options Indexes
```

AllowOverride None
Allow from from all
Order allow,deny
</Directory>

□□□□□□□ Save □□□□ Restart Apache

5. Load SSL module

$ vi /etc/sysconfig/apache2

APACHE_SERVER_FLAGS="**SSL**"

- Restart Web Server

$ rcapache2 restart

6. □□□□□

- □□□□ □Browser Mozilla Firefox □□□□ IE □□□□□

URL: www.mydomain.com/ssl-site


Certificate Viewer:"www.mydomain.com"
General
Details
Could not verify this certificate for unknown reasons.
Issued To
Common Name (CN) www.mydomain.com
Organization (O) MY COMPANY, LTD.
Organizational Unit (OU) IT
Serial Number 00:9B:B6:4D:A9:D7:3C:15:9E
Issued By
Common Name (CN) *.mydomain.com
Organization (O) My Company, LTD.
Organizational Unit (OU) IT
Validity
Issued On 28/11/2009
Expires On 28/11/2011
Fingerprints
SHA1 Fingerprint AA:80:0D:BE:42:D7:95:14:A0:B1:95:2D:97:D8:F3:97:5C:81:9D:03
MD5 Fingerprint 1C:B1:E2:58:3A:32:0F:E3:A9:CC:CD:C4:CA:47:E9:1F
Close