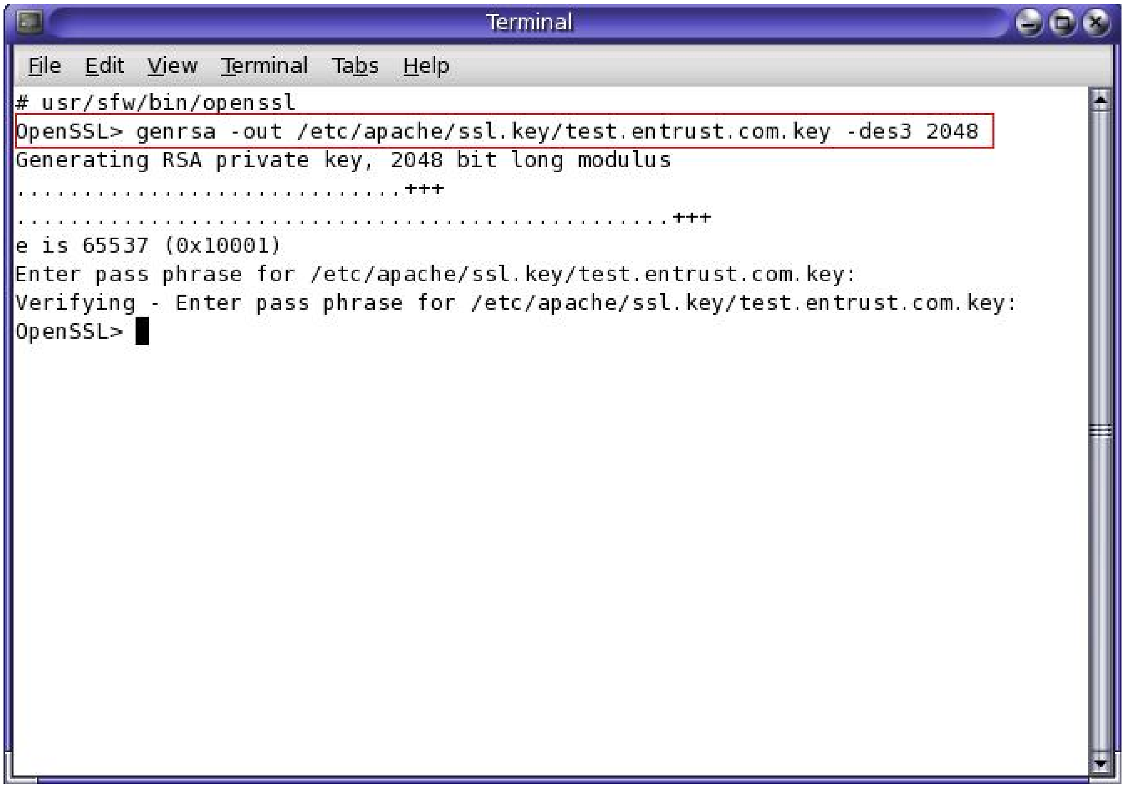
How is a Certificate Signing Request (CSR) generated for Apache HTTP Server using OpenSSL

If you require an SSL certificate to secure a domain hosted using Apache server, you need to first generate a Certificate Signing Request (CSR). To generate a new CSR you need to:

1. Launch command prompt or your system console and run the OpenSSL tool from where it was installed on your system (for example /usr/local/ssl/bin OR usr/sfw/bin as in our test system used for this example).
2. Once openssl is started, generate a new private key to use for securing the domain and to use for generating the new CSR.
   If you have already generated a private key go to step: 3
   To generate a private key use to command:

   genrsa –out <path to key storing directory>/<file name>.key –des3 2048

   you will be asked to provide and verify a password to secure this new private key. Provide this password.



```
# usr/sfw/bin/openssl
OpenSSL> genrsa -out /etc/apache/ssl.key/test.entrust.com.key -des3 2048
Generating RSA private key, 2048 bit long modulus
.............................+++
.................................................+++
e is 65537 (0x10001)
Enter pass phrase for /etc/apache/ssl.key/test.entrust.com.key:
Verifying - Enter pass phrase for /etc/apache/ssl.key/test.entrust.com.key:
OpenSSL>
```

3. Use the openssl tool to generate your new CSR from the private key
   To generate your new CSR using openssl use the following command:

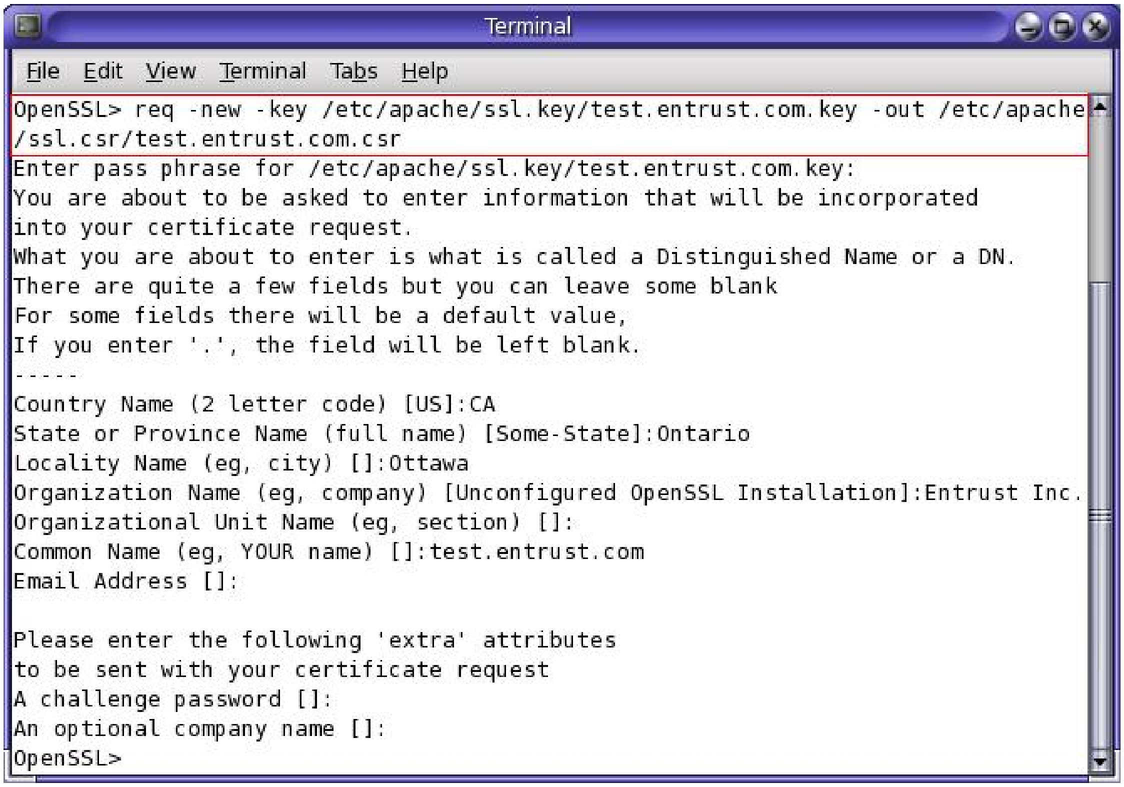
   req –new –key <private key directory>/<private key>.key –out <CSR directory>/<CSR file name>.csr

   You will be asked to provide the password for the private key file so enter it.

You will be asked to enter the Distinguished Name (DN) to be defined in the CSR as follows (**mandatory fields are: country, organization name, and common name**):

Attribute	Prefix	Description	Example
Country/Region	**c**	**Business location - country**	**CA**
State/Province	st	Business location – state/province	Ontario
City/Locality	l	Business location - city	Ottawa
Organizational Unit	ou	Department in the organization	
Organization	**o**	**Organization's legal business name**	**Entrust Inc.**
Common name	**cn**	**Domain to be secured by certificate**	**test.entrust.com**

Note: Do not use a challenge password.



```
OpenSSL> req -new -key /etc/apache/ssl.key/test.entrust.com.key -out /etc/apache
/ssl.csr/test.entrust.com.csr
Enter pass phrase for /etc/apache/ssl.key/test.entrust.com.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) [US]:CA
State or Province Name (full name) [Some-State]:Ontario
Locality Name (eg, city) []:Ottawa
Organization Name (eg, company) [Unconfigured OpenSSL Installation]:Entrust Inc.
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:test.entrust.com
Email Address []:

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

4. Now you should have a new CSR for your domain ready to be used. The content of this CSR is what you need to submit to Entrust when you are requesting/generating your SSL certificate. The CSR file should contain content similar to this:

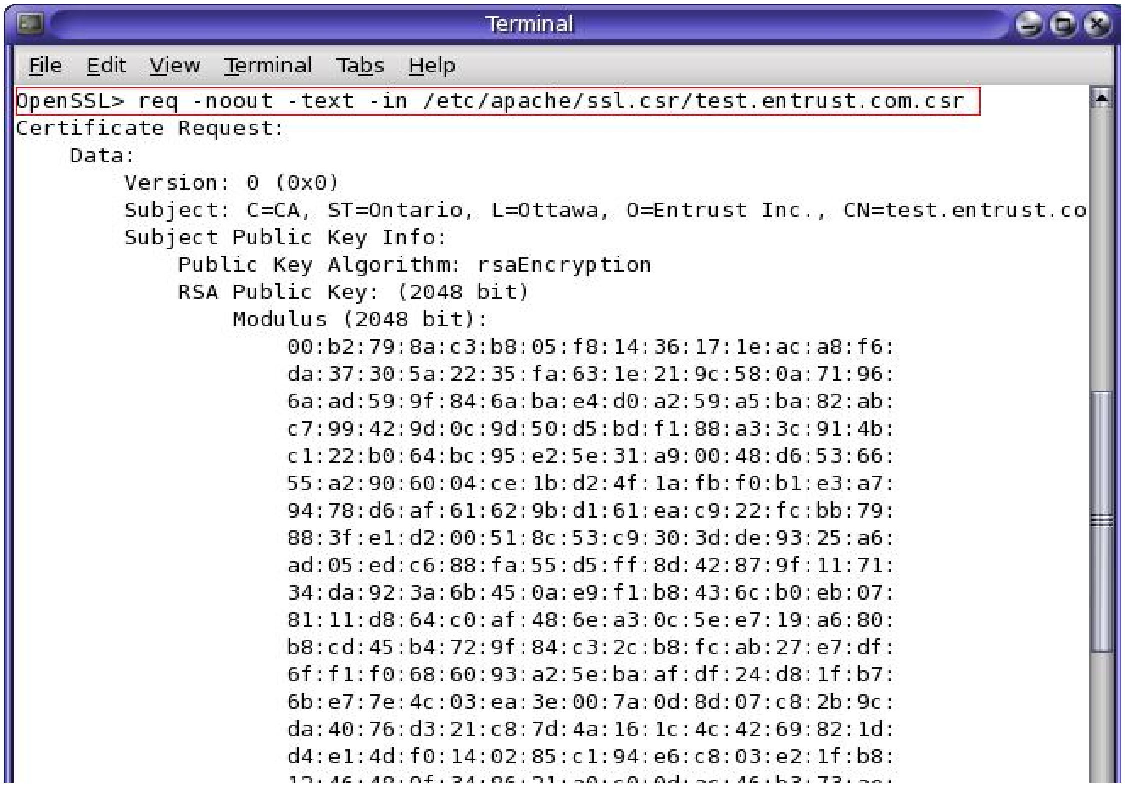
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIEhDCCA2wCAQAwgYAxCzAJBgNVBAYTAkNBMRAwDgYDVQQIDAdPbnRhcmlvMQ8w
DQYDVQQHDAZPdHRhd2ExFTATBgNVBAoMDEVudHJ1c3QgSW5jLjEZMBcGA1UECwwQ
Q2VydGlmaWNhdGUgRGVwLjEcMBoGA1UEAwwTaWlzN2NlcnQuZW50cnVzdC5jYTCC
.
.

.

OOqRZhp/bkDjEWW+OO1Z7hAnB1gcN4t1Q7TO3gZwyO9Yarv7gkPXCsCIMwJkhmzB
X4n6sJ5KGAUQj+Qx6VDeyTzG6w8hTvXH0lLxVb7LYg12vcrt2O3wKdBwRdcPNtLO
8nK2lCzuiMwL+cM8XJroaYCtr8A8mDHLCTQHy1y5PReZ2wYIChPWVwzzrhWo7XZ5
Vmcczl6amkU=
-----END NEW CERTIFICATE REQUEST-----

5. To verify the content of your new CSR, run the following openssl command:
   req –noout –text –in <path to CSR file>/<file name>.csr

   This will display the information specified in the CSR file in plain text format.



```
OpenSSL> req -noout -text -in /etc/apache/ssl.csr/test.entrust.com.csr
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=CA, ST=Ontario, L=Ottawa, O=Entrust Inc., CN=test.entrust.co
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:b2:79:8a:c3:b8:05:f8:14:36:17:1e:ac:a8:f6:
                    da:37:30:5a:22:35:fa:63:1e:21:9c:58:0a:71:96:
                    6a:ad:59:9f:84:6a:ba:e4:d0:a2:59:a5:ba:82:ab:
                    c7:99:42:9d:0c:9d:50:d5:bd:f1:88:a3:3c:91:4b:
                    c1:22:b0:64:bc:95:e2:5e:31:a9:00:48:d6:53:66:
                    55:a2:90:60:04:ce:1b:d2:4f:1a:fb:f0:b1:e3:a7:
                    94:78:d6:af:61:62:9b:d1:61:ea:c9:22:fc:bb:79:
                    88:3f:e1:d2:00:51:8c:53:c9:30:3d:de:93:25:a6:
                    ad:05:ed:c6:88:fa:55:d5:ff:8d:42:87:9f:11:71:
                    34:da:92:3a:6b:45:0a:e9:f1:b8:43:6c:b0:eb:07:
                    81:11:d8:64:c0:af:48:6e:a3:0c:5e:e7:19:a6:80:
                    b8:cd:45:b4:72:9f:84:c3:2c:b8:fc:ab:27:e7:df:
                    6f:f1:f0:68:60:93:a2:5e:ba:af:df:24:d8:1f:b7:
                    6b:e7:7e:4c:03:ea:3e:00:7a:0d:8d:07:c8:2b:9c:
                    da:40:76:d3:21:c8:7d:4a:16:1c:4c:42:69:82:1d:
                    d4:e1:4d:f0:14:02:85:c1:94:e6:c8:03:e2:1f:b8:
                    12:46:48:0f:34:86:21:a0:c0:0d:ac:46:b3:73:ac:
```

6. Open the generated .csr file containing the newly created Certificate signing Request (CSR) and copy its content into the specified field when you are requesting a certificate from Entrust.
   <u>Note:</u> you need to copy the full CSR including the
   -----BEGIN NEW CERTIFICATE REQUEST-----
   and the
   -----END NEW CERTIFICATE REQUEST-----
   lines. Make sure that here are no trailing spaces or carriage returns in the CSR.

For more information about OpenSSL see: http://www.openssl.org/docs/apps/openssl.html

How is the Server Certificate installed in Apache (OpenSSL)?

After you receive the secure certificate pickup link from Entrust, follow the instructions below to install your new certificate in Apache server.

1. Pick up your Entrust Certificate through the secure pickup link that is sent to you. Copy and paste the certificate that is displayed into a text editor.
   The certificate should look like this:

   ```
   -----BEGIN CERTIFICATE-----
   MIIETTCCAzWgAwIBAgIESyDyzjANBgkqhkiG9w0BAQUFADCBsTELMAkGA1UE
   BhMCVVMxFjAUBgNVBAoTDUVudHJ1c3QsIEluYy4xOTA3BgNVBAsTMHd3dy5l
    .
    .
    .
   Fr4NBGoyp0TvTLv9/mIyijCD+AVs+U7vY20nTPeGUsKAFI+u0Hy7MduF8Pt2
   8lwRdW7dJnvVl+igWtI/0yXfZahFsPDCl1naLrhazeritKllugMtCXqWlRmA
   uyCntu+draHBu/JihC8135lB8XvhYaZlbg==
   -----END CERTIFICATE-----
   ```

   Make sure to copy these lines:

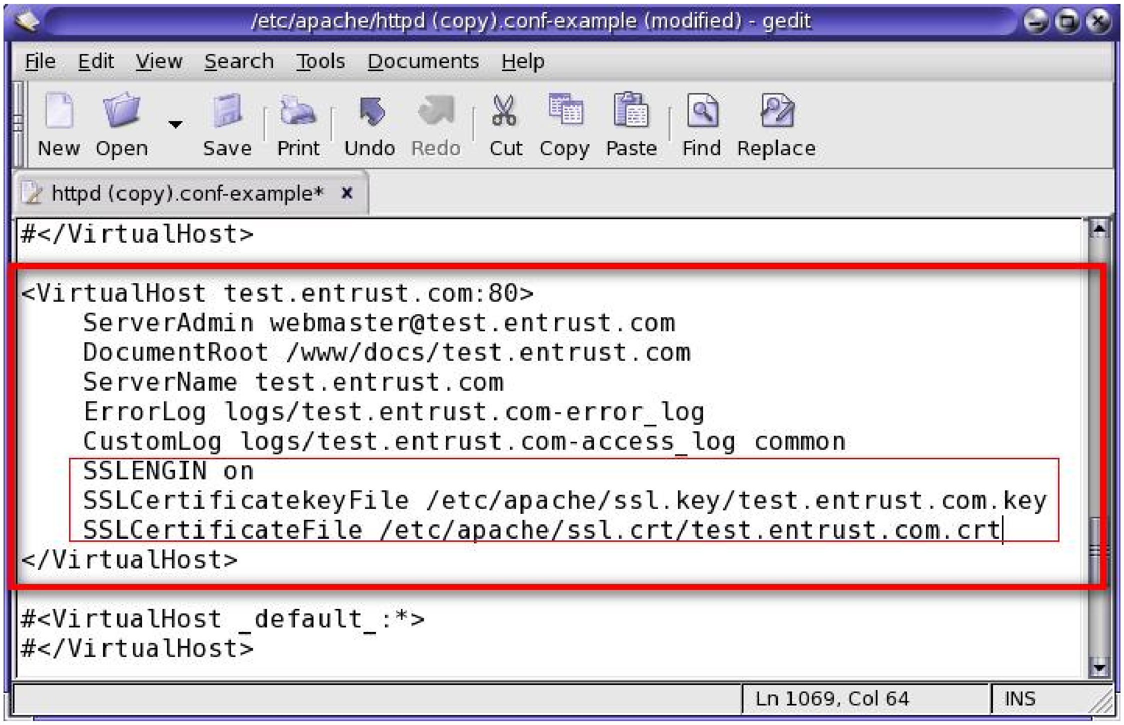
   ```
   -----BEGIN CERTIFICATE-----

   -----END CERTIFICATE-----
   ```

   Also ensure that there are no trailing spaces or carriage returns. **Save the text file using a .crt file extension**.

2. Open your server's **HTTPD.CONF** file and locate your virtual host entry for the domain to be secured by this certificate and make sure that SSL is enabled for it
   ```
   SSLEngine on
   ```

3. Add the following lines under the virtual host entry in the HTTPD.CONF file:
   ```
   SSLCertificateKeyFile <path to private key>/<private key file>.key
   SSLCertificateFile <path to certificate file>/<certificate file>.crt
   ```


/etc/apache/httpd (copy).conf-example (modified) - gedit
File Edit View Search Tools Documents Help
New Open Save Print Undo Redo Cut Copy Paste Find Replace
httpd (copy).conf-example*
Ln 1069, Col 64
INS

```
#</VirtualHost>

<VirtualHost test.entrust.com:80>
    ServerAdmin webmaster@test.entrust.com
    DocumentRoot /www/docs/test.entrust.com
    ServerName test.entrust.com
    ErrorLog logs/test.entrust.com-error_log
    CustomLog logs/test.entrust.com-access_log common
    SSLENGIN on
    SSLCertificatekeyFile /etc/apache/ssl.key/test.entrust.com.key
    SSLCertificateFile /etc/apache/ssl.crt/test.entrust.com.crt
</VirtualHost>

#<VirtualHost _default_:*>
#</VirtualHost>
```

Optional Step for Linux Redhat user:

If you are using the bundled version of apache that comes with Linux Redhat, do the following:

Replace the certificate in the localhost.crt file with the new certificate you have received. It is best to backup the localhost.crt file and then rename it to something. Then copy the new cert to localhost.crt.

You will need to stop and start your website for the changes to take effect.