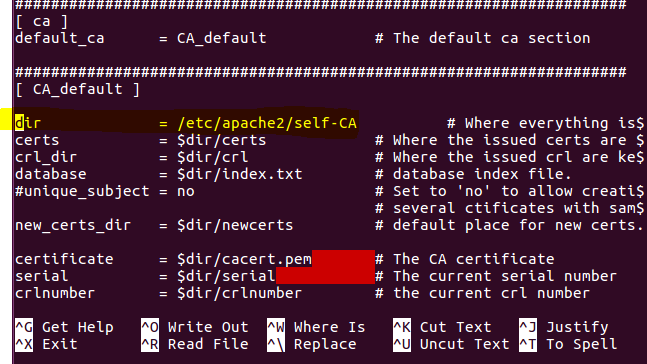
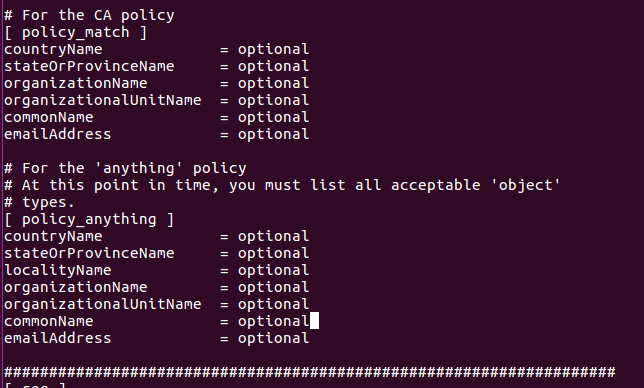
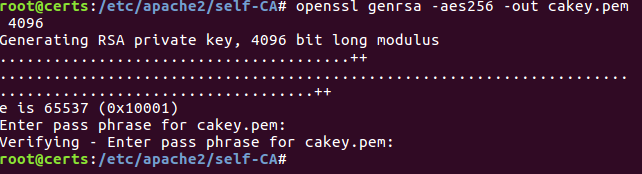
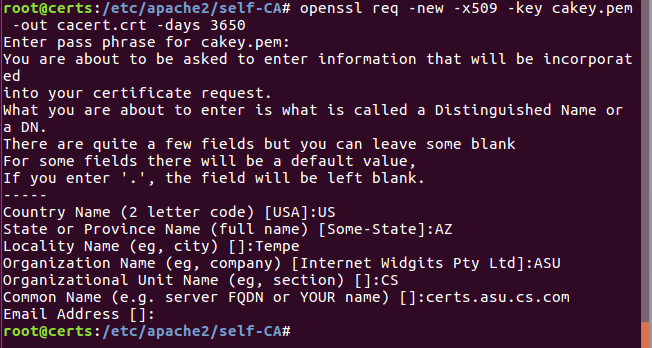
Create a certificate authority using OpenSSL on Linux (Ubuntu)

1. On the terminal verify Openssl is installed. (on Ubuntu it comes by default)
2. Use command “which openssl”
3. Then locate the openssl.cnf file using the command “locate openssl.cnf”.
4. Go to the location /etc/ssl (openssl.cnf is present at this location.)
5. Sudo -s to change to the root mode.
6. Create a directory named self-CA inside /etc/apache2 to store our certificates. Open the openssl.cnf file and change the directory to /etc/apache2/self-CA under the CA\_Default section. Openssl will look into this directory for certificates.   
   
7. Also I have changed the CA policy match to optional (Since this is a lab assignment). But in a production network they have to match.   
   
8. Change the host to “certs.asu.cs.com” using the command - hostname certs.asu.cs.com. Also make the change inside the /etc/hosts file accordingly.
9. Now go to the /etc/apache2/self-CA location. First generate a RSA private key which will be used to sign the root certificates.

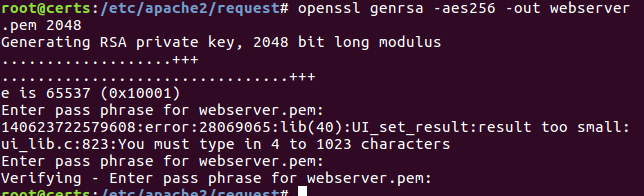
**Create root CA private key**

Command – openssl genrsa –aes256 –out cakey.pem 4096   
  
  


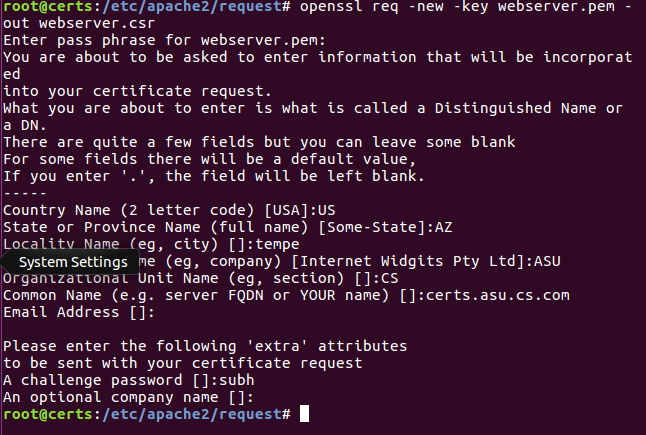
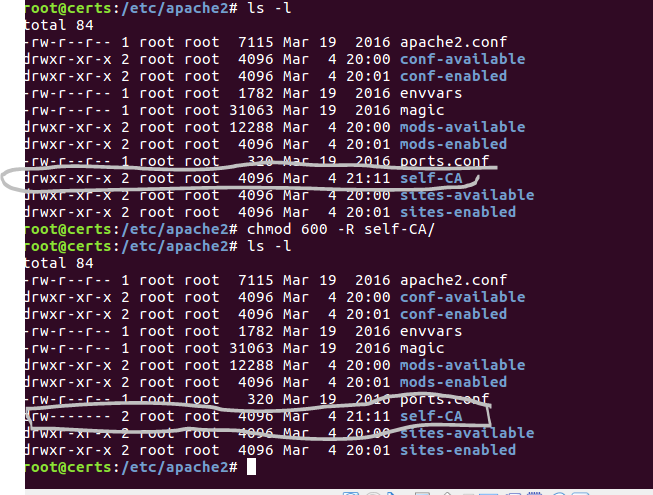
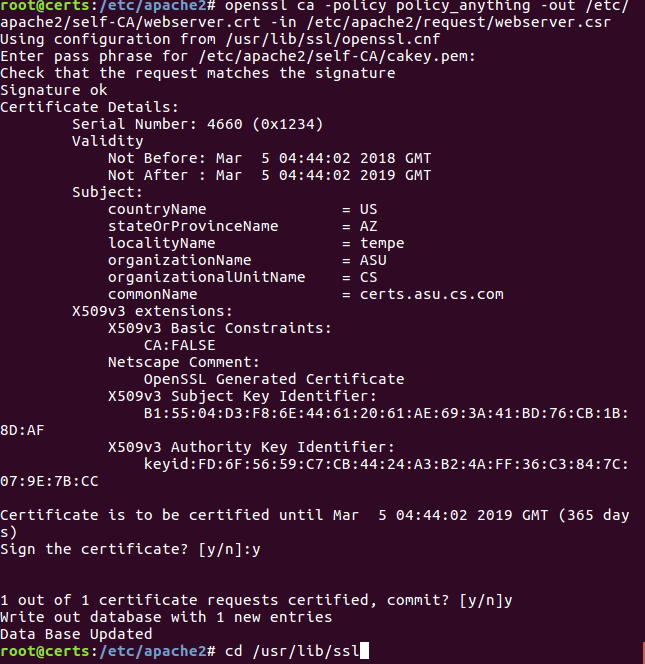
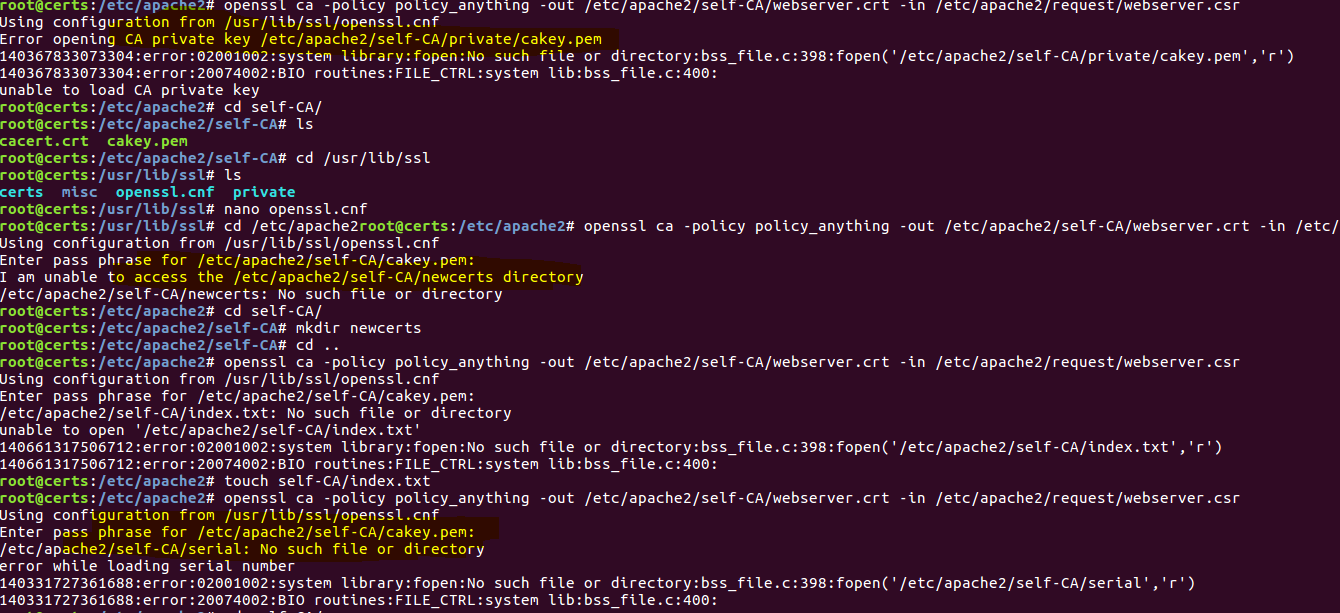
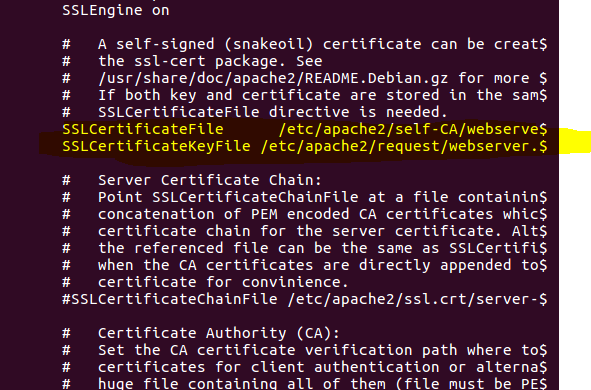
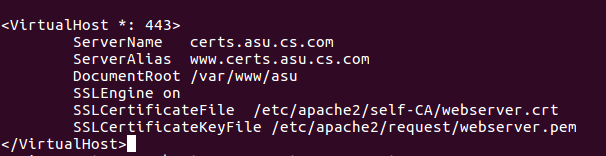
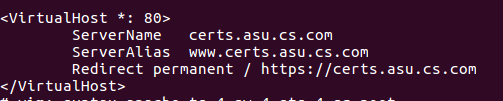
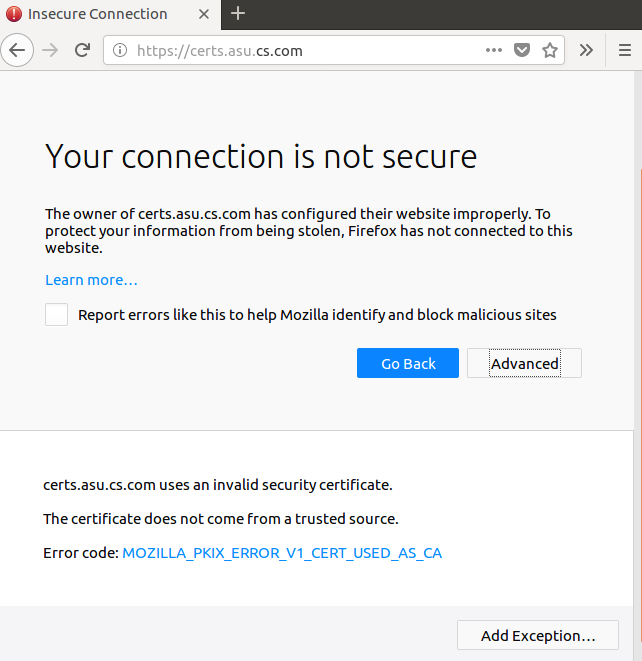
1. Now create a Root Certificate using the private key. While creating the root cert it will ask below details. Root certificate is valid for 10 years.   
   command : openssl req –new –x509 –key cakey.pem –out cacert.crt –day 3650

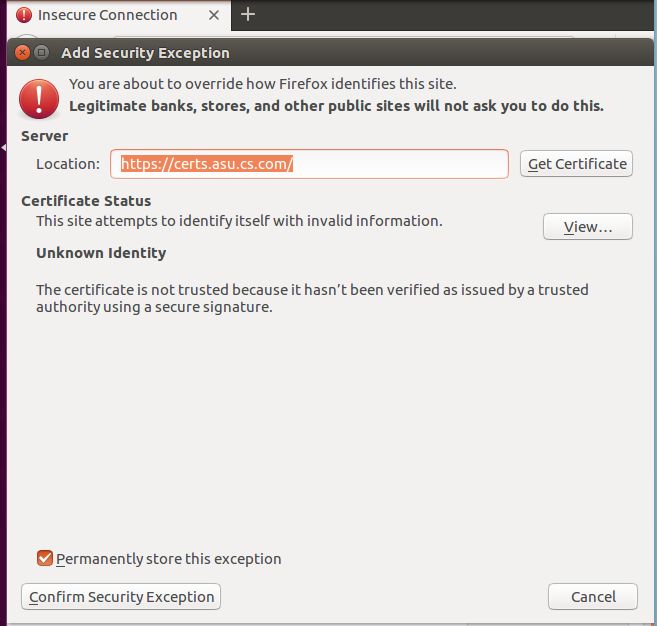


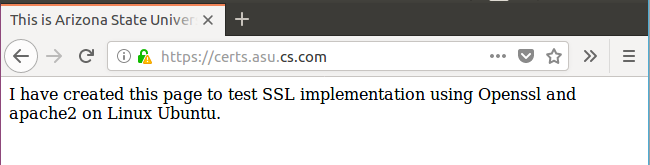
1. **A webserver will request the root CA for a certificate where the webserver will have its public key. First, the webserver will create its private key.**



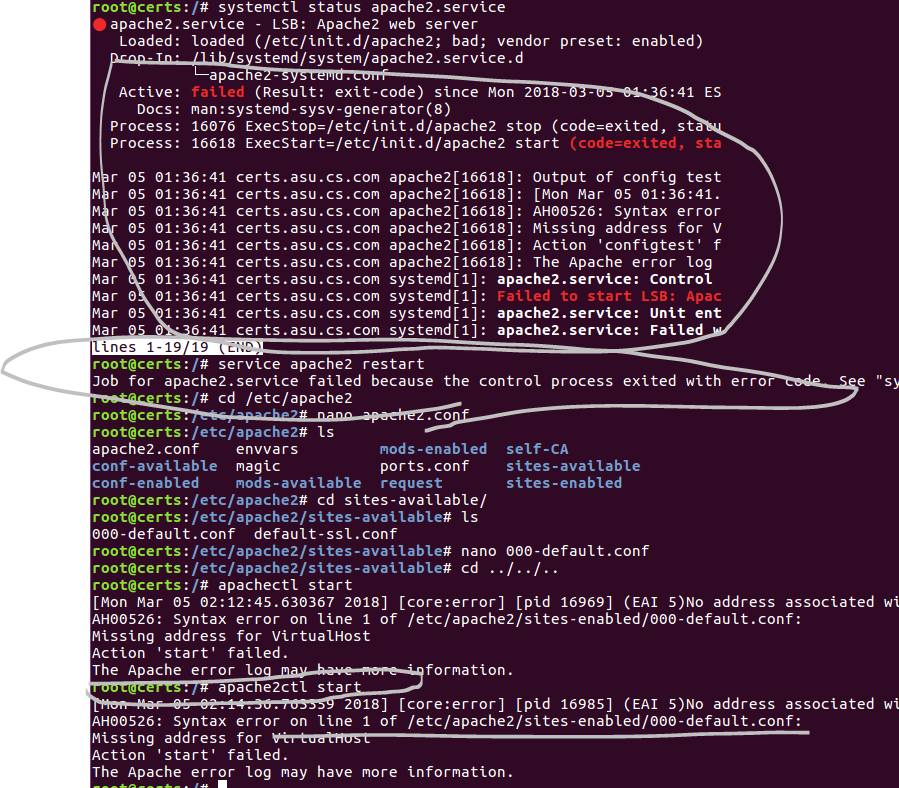
(I have created a request folder where the webserver will generate its private key)

1. **Generate CSR: The webserver generates a certificate signing request using its private key.   
     
   command: openssl req –new –key webserver.pem –out webserver.csr**
2. Change the permission of the self-CA folder so that no one else can make any changes.   
   
3. Now the Root-CA has to sign the Certificate Signing Request from the webserver.   
   command: openssl ca –policy policy\_anything –out /etc/apache2/self-CA/webserver.crt –in   
   /etc/apache2/request/webserver.csr  
     
   Since it is a test CA, we are putting policy\_anything.   
     
   
4. I realized few things while signing the csr as the root ca. First, create folders to hold certs, requests as per the structure of openssl.cnf file with in /usr/lib/ssl. I faced many errors since those folders were not present while signing the csr.   
     
   I had to create missing folders and I also had to make some adjustments in the openssl.cnf file within /usr/lib/ssl
5. Configure the web server to use the certificate.   
   Go to the path /etc/apache2/sites-available. Open default-ssl.cnf file.   
   (\*apache2.conf need not to be modified. )  
   Edit the path to the certificate and the private key of the webserver.  
   
6. To the 000-deafult.conf file inside /etc/apache2/sites-available, add a virtualhost as below.  
   
7. Add following for redirection of HTTP to HTTPS.  
   
8. Since it is a self-signed certificate, the browser shows the warning. But go ahead and add to exception.   
   



Now I am able to access my test website securely (https).  


Lesson Learned: many times I faced the error “Unable to start LSB” while restarting the apache2. It may happen due to wrong configuration in any of the apache conf file. Use apache2ctl start command every time you make any changes to conf file.



How to remove apache on Ubuntu:

Sudo -s

Service apache2 stop

apt-get purge apache2 apache2-utils apache2.2-bin apache2-common

apt-get autoremove

Finally, check if there is any configuration files or manual pages belonging to Apache2, which are still not removed.

Whereis apache2

Remove all of them using command : rm –rf /etc/apache2 (each path)

How to install apache2 on Ubuntu:

sudo a2ensite example.com.conf

sudo a2dismod mpm\_event

sudo a2enmod mpm\_prefork

Openssl key generation <https://jamielinux.com/docs/openssl-certificate-authority/online-certificate-status-protocol.html>

<https://rietta.com/blog/2012/01/27/openssl-generating-rsa-key-from-command/>

Openssl CA <https://www.youtube.com/watch?v=oCl0gzLPPMI>

<https://www.youtube.com/watch?v=Ei-ah2ruEkM>

A very good tutorial on how to enable virtual host in apache - <https://www.digitalocean.com/community/tutorials/how-to-set-up-apache-virtual-hosts-on-ubuntu-16-04>