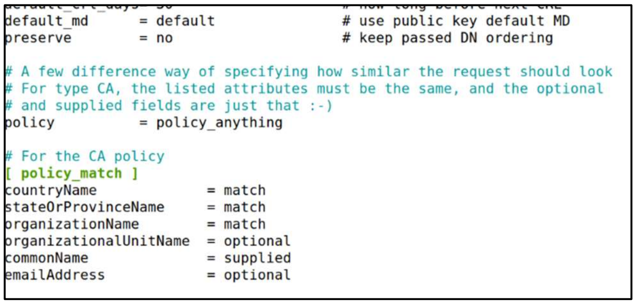
Lab 6 Assignment

Submitted by: Rishabh Pahwa (110091645)

Part 1: Create server public-key and its certificate

1) Copy /usr/lib/ssl/openssl.cnf to your current working directory and make the following change to this file:
"policy = policy_match" to "policy = policy_anything"



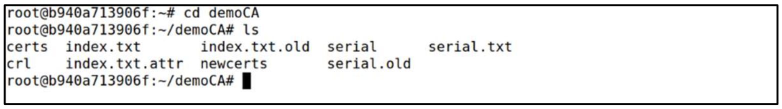
```
default_md      = default               # use public key default MD
preserve        = no                    # keep passed DN ordering

# A few difference way of specifying how similar the request should look
# For type CA, the listed attributes must be the same, and the optional
# and supplied fields are just that :-)
policy          = policy_anything

# For the CA policy
[ policy_match ]
countryName             = match
stateOrProvinceName     = match
organizationName        = match
organizationalUnitName  = optional
commonName              = supplied
emailAddress            = optional
```

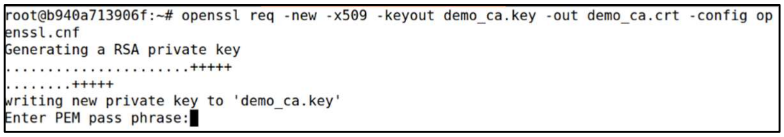
2) Create a new directory demoCA in the current directory. Then, do the following.

- Create new directories certs, crl and newcerts in demoCA and empty files index.txt and serial:

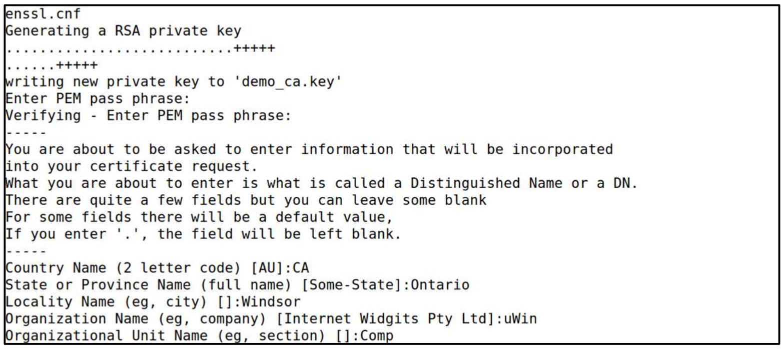


```
root@b940a713906f:~# cd demoCA
root@b940a713906f:~/demoCA# ls
certs  index.txt       index.txt.old  serial      serial.txt
crl    index.txt.attr  newcerts       serial.old
root@b940a713906f:~/demoCA# 
```

- Generate a self-signed certificate for our certificate authority (CA):



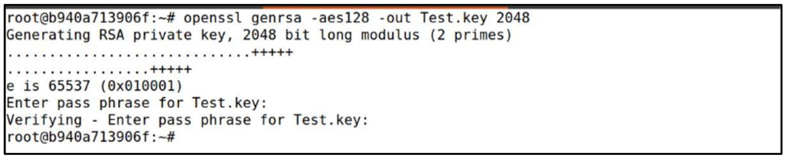
```
root@b940a713906f:~# openssl req -new -x509 -keyout demo_ca.key -out demo_ca.crt -config op
enssl.cnf
Generating a RSA private key
......................+++++
........+++++
writing new private key to 'demo_ca.key'
Enter PEM pass phrase:
```



```
enssl.cnf
Generating a RSA private key
..........................+++++
......+++++
writing new private key to 'demo_ca.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
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]:CA
State or Province Name (full name) [Some-State]:Ontario
Locality Name (eg, city) []:Windsor
Organization Name (eg, company) [Internet Widgits Pty Ltd]:uWin
Organizational Unit Name (eg, section) []:Comp
```

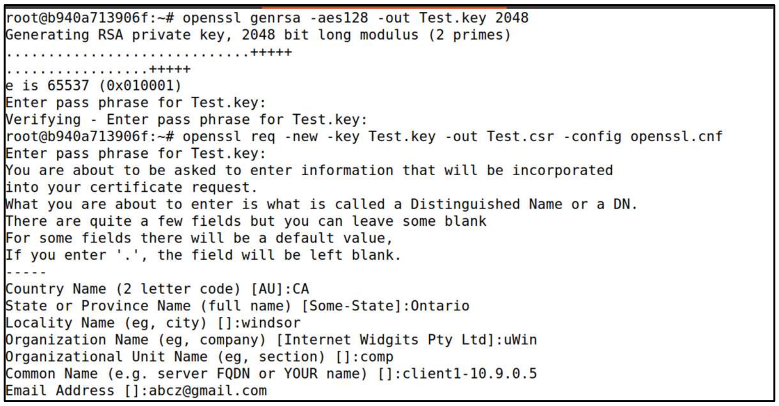
- Create a certificate for our test TLS server, signed by our authority's key demo_ca.key.

1. Generate a RSA private key for TLS server.

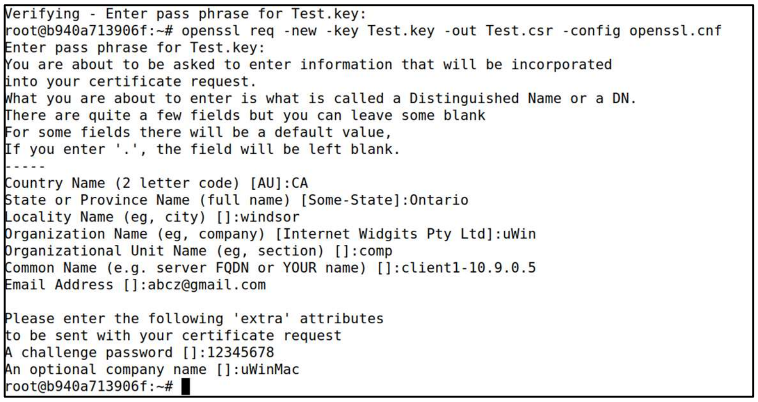


```
root@b940a713906f:~# openssl genrsa -aes128 -out Test.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
............................+++++
................+++++
e is 65537 (0x010001)
Enter pass phrase for Test.key:
Verifying - Enter pass phrase for Test.key:
root@b940a713906f:~#
```

2. Generate a certificate signing request:



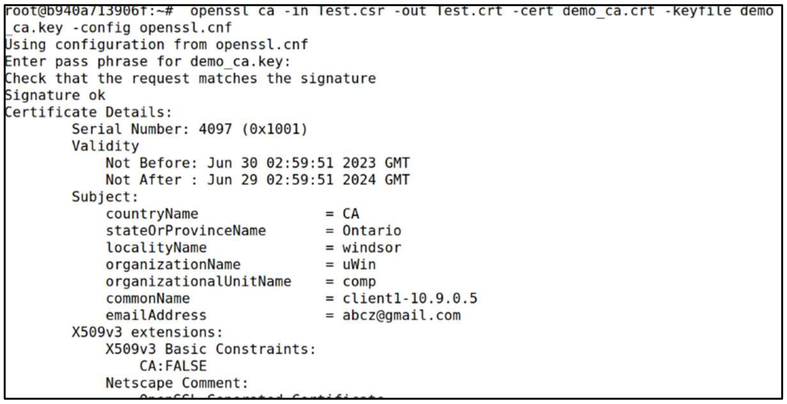
```
root@b940a713906f:~# openssl genrsa -aes128 -out Test.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
............................+++++
................+++++
e is 65537 (0x010001)
Enter pass phrase for Test.key:
Verifying - Enter pass phrase for Test.key:
root@b940a713906f:~# openssl req -new -key Test.key -out Test.csr -config openssl.cnf
Enter pass phrase for Test.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]:CA
State or Province Name (full name) [Some-State]:Ontario
Locality Name (eg, city) []:windsor
Organization Name (eg, company) [Internet Widgits Pty Ltd]:uWin
Organizational Unit Name (eg, section) []:comp
Common Name (e.g. server FQDN or YOUR name) []:client1-10.9.0.5
Email Address []:abcz@gmail.com
```



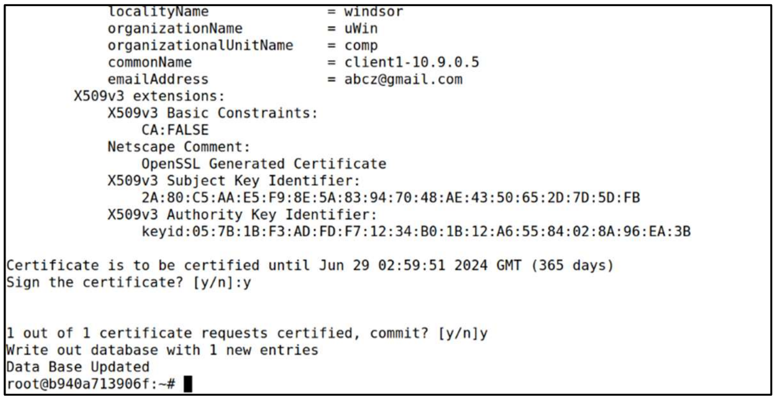
```
Verifying - Enter pass phrase for Test.key:
root@b940a713906f:~# openssl req -new -key Test.key -out Test.csr -config openssl.cnf
Enter pass phrase for Test.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is 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]:CA
State or Province Name (full name) [Some-State]:Ontario
Locality Name (eg, city) []:windsor
Organization Name (eg, company) [Internet Widgits Pty Ltd]:uWin
Organizational Unit Name (eg, section) []:comp
Common Name (e.g. server FQDN or YOUR name) []:client1-10.9.0.5
Email Address []:abcz@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:12345678
An optional company name []:uWinMac
root@b940a713906f:~# █
```

3. Generate the certificate for TLS server:



```
root@b940a713906f:~#  openssl ca -in Test.csr -out Test.crt -cert demo_ca.crt -keyfile demo
_ca.key -config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for demo_ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4097 (0x1001)
        Validity
            Not Before: Jun 30 02:59:51 2023 GMT
            Not After : Jun 29 02:59:51 2024 GMT
        Subject:
            countryName               = CA
            stateOrProvinceName       = Ontario
            localityName              = windsor
            organizationName          = uWin
            organizationalUnitName    = comp
            commonName                = client1-10.9.0.5
            emailAddress              = abcz@gmail.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
```

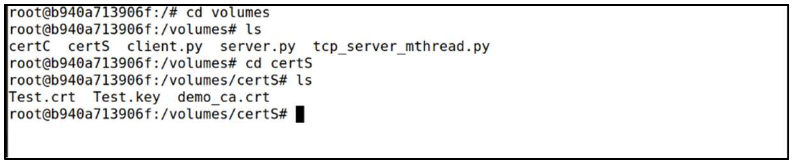


```
            localityName              = windsor
            organizationName          = uWin
            organizationalUnitName    = comp
            commonName                = client1-10.9.0.5
            emailAddress              = abcz@gmail.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                2A:80:C5:AA:E5:F9:8E:5A:83:94:70:48:AE:43:50:65:2D:7D:5D:FB
            X509v3 Authority Key Identifier:
                keyid:05:7B:1B:F3:AD:FD:F7:12:34:B0:1B:12:A6:55:84:02:8A:96:EA:3B

Certificate is to be certified until Jun 29 02:59:51 2024 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
root@b940a713906f:~# 
```

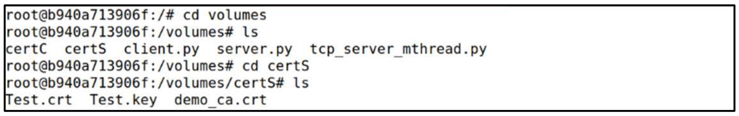
4. Copy your certificate **Test.crt** and **Test.key** to a folder **certS** in the shared folder **volumes**



```
root@b940a713906f:/# cd volumes
root@b940a713906f:/volumes# ls
certC  certS  client.py  server.py  tcp_server_mthread.py
root@b940a713906f:/volumes# cd certS
root@b940a713906f:/volumes/certS# ls
Test.crt  Test.key  demo_ca.crt
root@b940a713906f:/volumes/certS# 
```

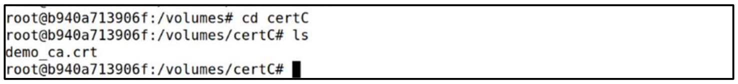
5. Copy *demo_ca.crt* to folder (such as **certC**) in the shared folder **volumes**.

CertS files:



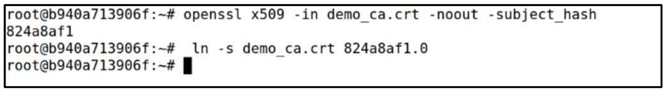
```
root@b940a713906f:/# cd volumes
root@b940a713906f:/volumes# ls
certC  certS  client.py  server.py  tcp_server_mthread.py
root@b940a713906f:/volumes# cd certS
root@b940a713906f:/volumes/certS# ls
Test.crt  Test.key  demo_ca.crt
```

CertC files:



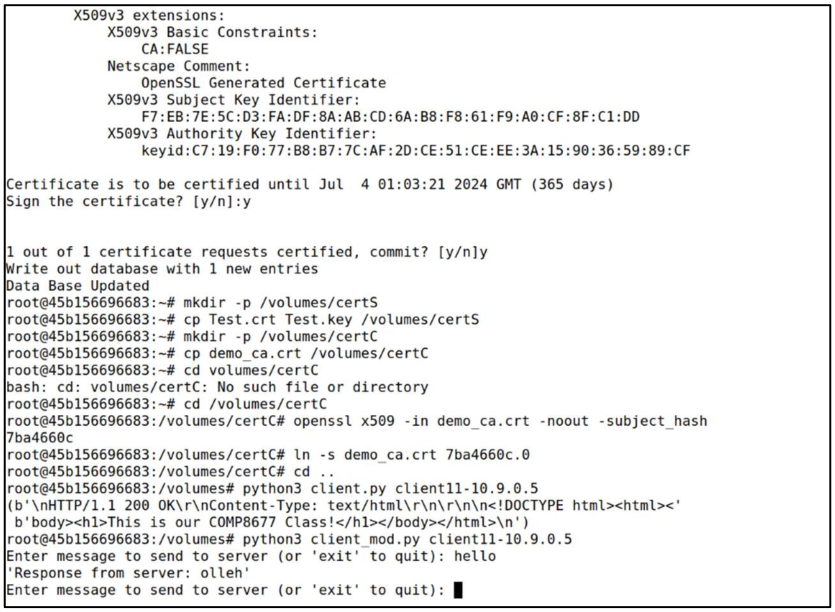
```
root@b940a713906f:/volumes# cd certC
root@b940a713906f:/volumes/certC# ls
demo_ca.crt
root@b940a713906f:/volumes/certC# █
```

Calculating hash value and using it to create symbolic link:



```
root@b940a713906f:~# openssl x509 -in demo_ca.crt -noout -subject_hash
824a8af1
root@b940a713906f:~#  ln -s demo_ca.crt 824a8af1.0
root@b940a713906f:~# █
```

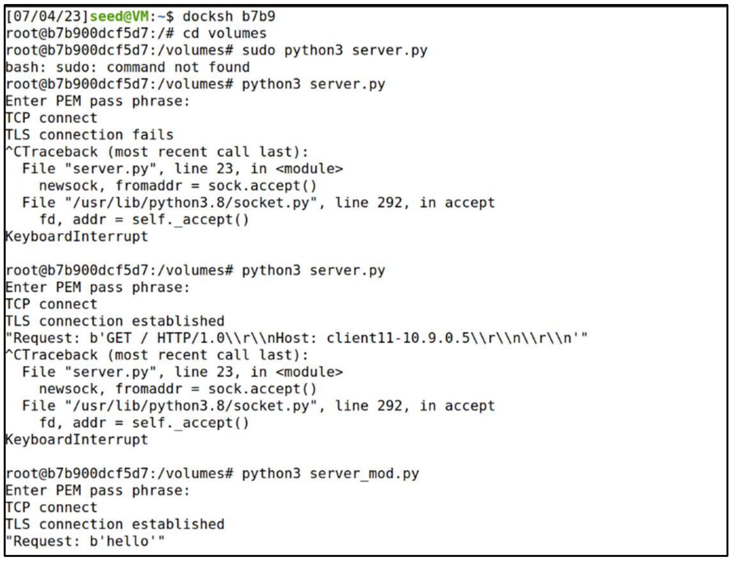
Part 2: TLS Client and Server Communication



```
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                F7:EB:7E:5C:D3:FA:DF:8A:AB:CD:6A:B8:F8:61:F9:A0:CF:8F:C1:DD
            X509v3 Authority Key Identifier:
                keyid:C7:19:F0:77:B8:B7:7C:AF:2D:CE:51:CE:EE:3A:15:90:36:59:89:CF

Certificate is to be certified until Jul  4 01:03:21 2024 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
root@45b156696683:~# mkdir -p /volumes/certS
root@45b156696683:~# cp Test.crt Test.key /volumes/certS
root@45b156696683:~# mkdir -p /volumes/certC
root@45b156696683:~# cp demo_ca.crt /volumes/certC
root@45b156696683:~# cd volumes/certC
bash: cd: volumes/certC: No such file or directory
root@45b156696683:~# cd /volumes/certC
root@45b156696683:/volumes/certC# openssl x509 -in demo_ca.crt -noout -subject_hash
7ba4660c
root@45b156696683:/volumes/certC# ln -s demo_ca.crt 7ba4660c.0
root@45b156696683:/volumes/certC# cd ..
root@45b156696683:/volumes# python3 client.py client11-10.9.0.5
(b'\nHTTP/1.1 200 OK\r\nContent-Type: text/html\r\n\r\n\n<!DOCTYPE html><html><'
 b'body><h1>This is our COMP8677 Class!</h1></body></html>\n')
root@45b156696683:/volumes# python3 client_mod.py client11-10.9.0.5
Enter message to send to server (or 'exit' to quit): hello
'Response from server: olleh'
Enter message to send to server (or 'exit' to quit): █
```



```
[07/04/23]seed@VM:~$ docksh b7b9
root@b7b900dcf5d7:/# cd volumes
root@b7b900dcf5d7:/volumes# sudo python3 server.py
bash: sudo: command not found
root@b7b900dcf5d7:/volumes# python3 server.py
Enter PEM pass phrase:
TCP connect
TLS connection fails
^CTraceback (most recent call last):
  File "server.py", line 23, in <module>
    newsock, fromaddr = sock.accept()
  File "/usr/lib/python3.8/socket.py", line 292, in accept
    fd, addr = self._accept()
KeyboardInterrupt

root@b7b900dcf5d7:/volumes# python3 server.py
Enter PEM pass phrase:
TCP connect
TLS connection established
"Request: b'GET / HTTP/1.0\\r\\nHost: client11-10.9.0.5\\r\\n\\r\\n'"
^CTraceback (most recent call last):
  File "server.py", line 23, in <module>
    newsock, fromaddr = sock.accept()
  File "/usr/lib/python3.8/socket.py", line 292, in accept
    fd, addr = self._accept()
KeyboardInterrupt

root@b7b900dcf5d7:/volumes# python3 server_mod.py
Enter PEM pass phrase:
TCP connect
TLS connection established
"Request: b'hello'"
```