EAST WEST UNIVERSITY

Cybersecurity, Law, and Ethics (CSE487)

[Summer 2022]

Section: 01

Project Title: Configuration of Certification Authority and Implementation of Transport Layer Security over HTTP

Instructor Name: Rashedul Amin Tuhin

Senior Lecturer, Department of Computer Science and Engineering.

Mini Project Report - 01

Submitted by:

Student ID	Student Name
2019-1-62-001	Rafsan Bari Shafin
2019-1-68-056	Zannatul Mawa
2019-1-60-258	Sabuj Paul

Initial Works:

- Firstly, we must download and install Xampp in our local machine.
- We are creating a folder based on our website domain name ***'baymaxsecureserver'*** in c drive and in the directory, we created a file named ***'fileupload.html'*** where we have written a basic html code.

Configure DNS File:

- Go to ***'C:\xampp\apache\conf\ httpd.conf'*** file and open it in an editor then edit 252 and 253 no. lines.

```
248   # DocumentRoot: The directory out of which you will serve your
249   # documents. By default, all requests are taken from this directory, but
250   # symbolic links and aliases may be used to point to other locations.
251   #
252   DocumentRoot "C:/baymaxSecureServer"
253   <Directory "C:/baymaxSecureServer">
254       #
```

Fig: Configure httpd.conf file

- Go to ***'C:\Windows\System32\drivers\etc\hosts'*** file and open it in an editor and go to the last line add these three lines below.

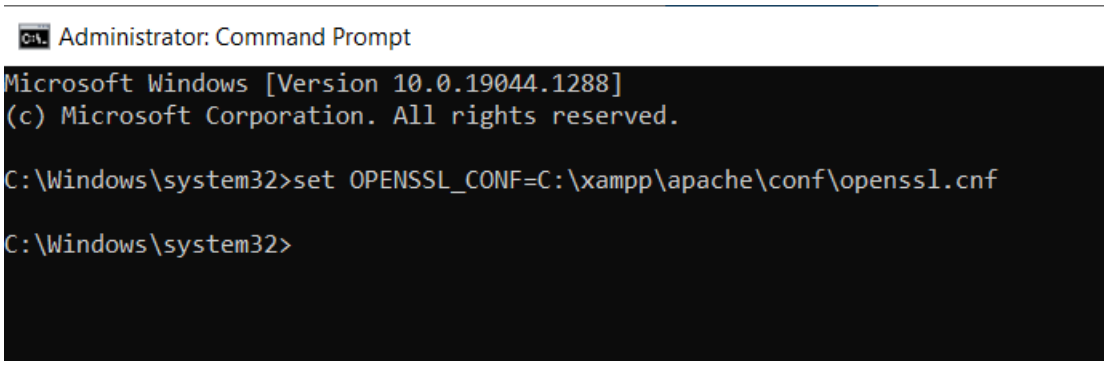
```
# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
127.0.0.1       localhost
127.0.0.1       baymaxsecureserver
127.0.0.1       www.baymaxsecureserver.com
```

Fig: Configure hosts file

Configure OpenSSL environment path:

- Open windows command prompt with ***'Run as Administrator'*** and run this command

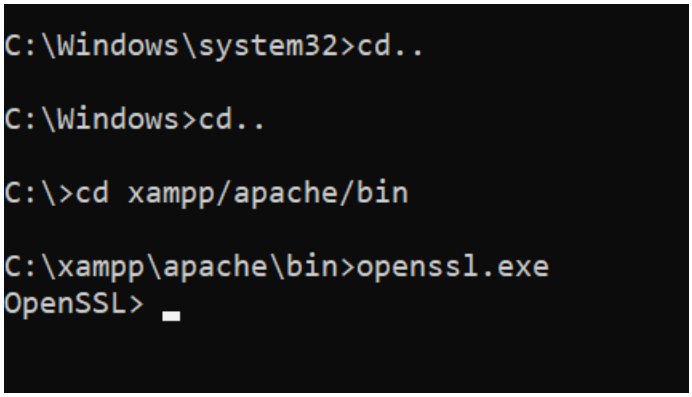
```
set OPENSSL_CONF=C:\xampp\apache\conf\openssl.cnf
```



Creating server certificate:

- In the previous command prompt run these following commands:

1. cd..
2. cd..
3. cd xampp/apache/bin
4. openssl.exe
   You will see an interface like this.



5. req -newkey rsa:2048 -nodes -keyout server.key -out server.csr

6. Then We have to provide Country Name, State Name, Locality Name, Organization Name, Unit Name, Common Name (www.baymaxsecureserver.com), email address.
7. For checking:
   x509 -signkey server.key -in server.csr -req -days 365 -out server.crt

8. We will see an interface like this:

```
C:\xampp\apache\bin>openssl.exe
OpenSSL> req -newkey rsa:2048 -nodes -keyout server.key -out server.csr
Generating a RSA private key
.....................................................................................+++++
.............+++++
writing new private key to 'server.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]:BD
State or Province Name (full name) [Some-State]:Dhaka
Locality Name (eg, city) []:Dhaka
Organization Name (eg, company) [Internet Widgits Pty Ltd]:East West University
Organizational Unit Name (eg, section) []:CSE
Common Name (e.g. server FQDN or YOUR name) []:www.baymaxsecureserver.com
Email Address []:baymax@live.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:1234
An optional company name []:
OpenSSL> x509 -signkey server.key -in server.csr -req -days 365 -out server.crt
Signature ok
subject=C = BD, ST = Dhaka, L = Dhaka, O = East West University, OU = CSE, CN = www.baymaxsecureserver.com, emailAddress = baymax@live.com
Getting Private key
```

Creating sub root CA certificate:

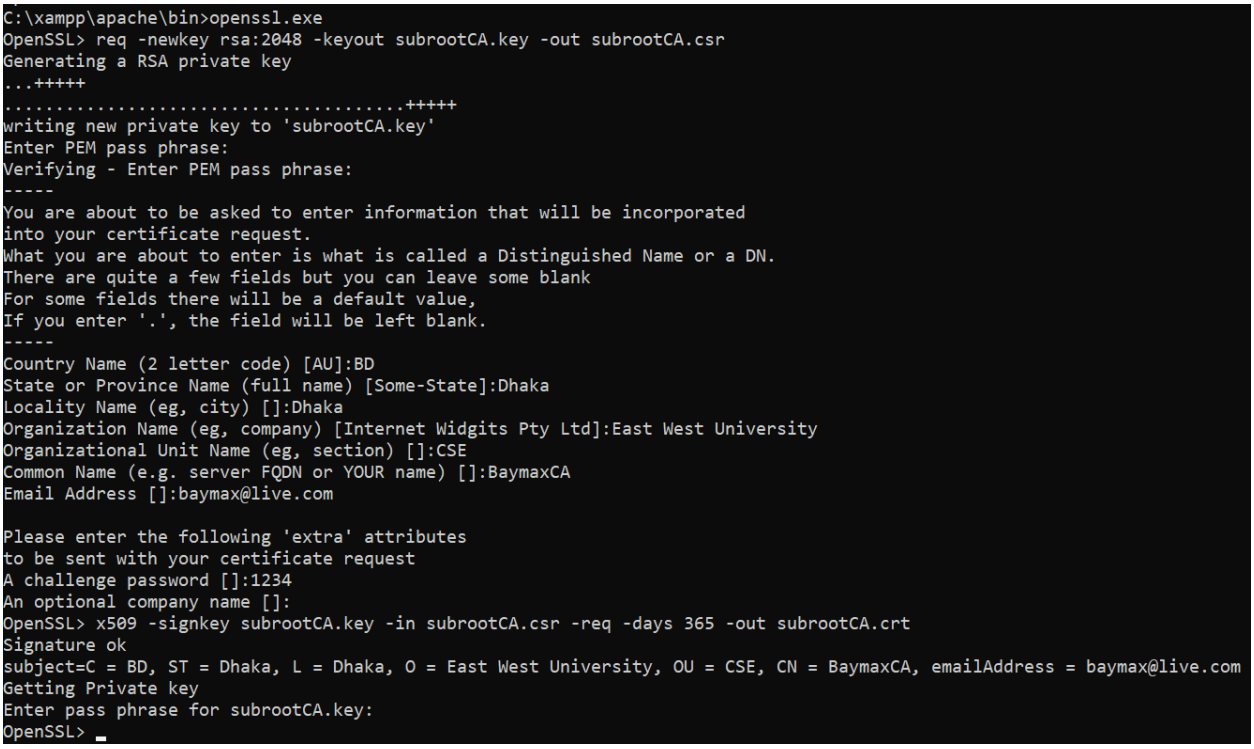
1. Ctrl + C and then type openssl.exe again.

2. req -newkey rsa:2048 -keyout subrootCA.key -out subrootCA.csr

3. Then We have to provide Country Name, State Name, Locality Name, Organization Name, Unit Name, Common Name (www.baymaxsecureserver.com), email address.

4. For checking:
   x509 -signkey subrootCA.key -in subrootCA.csr -req -days 365 -out subrootCA.crt

5. We will see an interface like this:



Creating root CA certificate:

1. Ctrl + C and then type openssl.exe again.

2. req -x509 -sha256 -days 1825 -newkey rsa:2048 -keyout rootCA.key -out rootCA.crt

3. Then We have to provide Country Name, State Name, Locality Name, Organization Name, Unit Name, Common Name (www.baymaxsecureserver.com), email address.

4. We will see an interface like this:

```
C:\xampp\apache\bin>openssl.exe
OpenSSL> req -x509 -sha256 -days 1825 -newkey rsa:2048 -keyout rootCA.key -out rootCA.crt
Generating a RSA private key
.....................................+++++
.+++++
writing new private key to 'rootCA.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]:BD
State or Province Name (full name) [Some-State]:Dhaka
Locality Name (eg, city) []:Dhaka
Organization Name (eg, company) [Internet Widgits Pty Ltd]:East West University
Organizational Unit Name (eg, section) []:CSE
Common Name (e.g. server FQDN or YOUR name) []:Baymax-RootCA
Email Address []:baymax@live.com
OpenSSL>
```

```
OpenSSL> x509 -req -CA rootCA.crt -CAkey rootCA.key -in subrootCA.csr -out subrootCA.crt -days 365 -CAcreateserial -extfile root.ext
Signature ok
subject=C = BD, ST = Dhaka, L = Dhaka, O = East West University, OU = CSE, CN = BaymaxCA, emailAddress = baymax@live.com
Getting CA Private Key
Enter pass phrase for rootCA.key:
OpenSSL>
```

Configure those certificates:

- Go to ***'C:\xampp\apache\bin'*** and create a file name ***'domain.ext'*** and paste the following code:

```
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
subjectAltName = @alt_names
[alt_names]
DNS.1 =www.verysecureserver.com
DNS.2 =127.0.0.1
```

- Go to ***'C:\xampp\apache\bin'*** and create a file name ***'root.ext'*** and paste the following code:

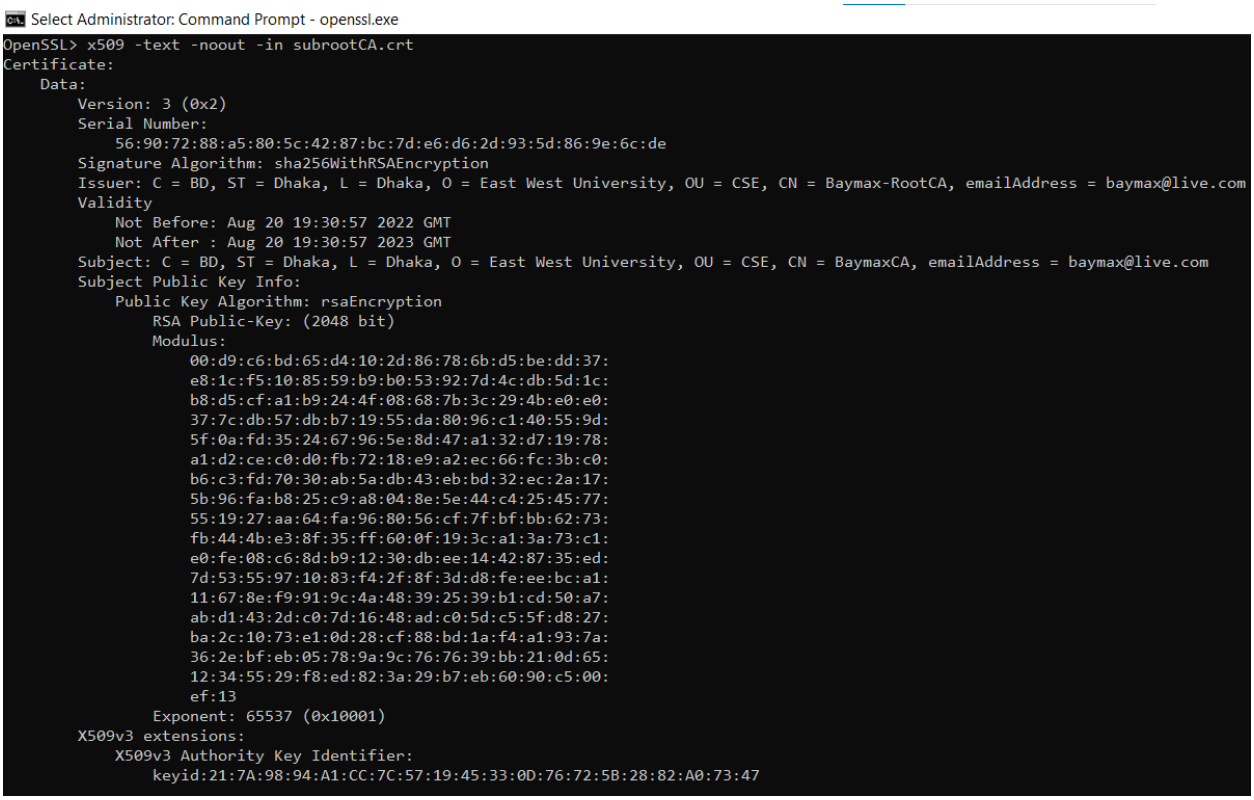
```
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:TRUE
subjectAltName = @alt_names
[alt_names]
DNS.1 =www.verysecureserver.com
DNS.2 =127.0.0.1
```

Signing sub root CA certificate with root CA certificate:

- `x509 -req -CA rootCA.crt -CAkey rootCA.key -in subrootCA.csr -out subrootCA.crt -days 365 -CAcreateserial -extfile root.ext`

- For Checking:

```
x509 -text -noout -in subrootCA.crt
```



```
            X509v3 Basic Constraints:
                CA:TRUE
            X509v3 Subject Alternative Name:
                DNS:www.baymaxsecureserver.com, DNS:127.0.0.1
    Signature Algorithm: sha256WithRSAEncryption
         1e:8c:ef:a2:24:7a:6f:40:32:73:85:e5:9c:b6:11:06:8d:81:
         44:d5:84:ac:bf:20:53:80:77:76:0f:34:6d:43:7b:75:4b:60:
         09:1d:8e:a5:bb:71:d3:aa:74:35:c2:0f:32:c7:9c:35:46:54:
         33:15:99:3a:78:8a:aa:07:4a:3e:ae:8a:98:45:d9:fd:6b:98:
         ac:8e:85:c8:83:6b:18:93:b6:23:23:c4:93:a2:eb:3e:d6:34:
         4f:ef:3a:e1:fd:51:af:9c:71:d8:96:f5:45:fc:e2:d5:75:02:
         3c:d8:f3:2f:b1:19:7e:bb:ae:a0:69:71:9b:19:75:47:7b:28:
         56:0c:a8:ce:89:cd:b4:83:ad:d0:b5:e5:1f:8d:bd:59:f5:81:
         2a:0c:c4:1b:d3:81:a9:ce:a1:6d:43:04:50:94:29:52:39:52:
         b4:e2:55:8d:cf:0b:c7:08:7a:5d:63:5c:48:73:a1:75:e9:fb:
         a5:44:6d:ff:e9:f1:48:e9:ab:c1:b6:d9:8e:c8:c3:4d:b7:5b:
         5a:e9:0b:94:88:69:13:da:24:e5:d0:51:2e:5b:58:a8:ad:88:
         6a:96:90:d0:e7:66:f8:40:ba:20:ef:a5:c9:cc:47:31:ef:8f:
         45:9f:79:bb:c3:c8:8c:2e:ae:cd:6f:8b:bf:86:bb:d3:8e:af:
         0d:7b:72:d1
OpenSSL>
```

Exporting the sub root CA key file in sub root CA pfx file:

- `x509 -in subrootCA.crt -outform der -out subrootCA.der`
- `pkcs12 -inkey subrootCA.key -in subrootCA.crt -export -out subrootCA.pfx`

```
OpenSSL> x509 -in subrootCA.crt -outform der -out subrootCA.der
OpenSSL> pkcs12 -inkey subrootCA.key -in subrootCA.crt -export -out subrootCA.pfx
15992:error:08064066:object identifier routines:OBJ_create:oid exists:crypto\objects\obj_dat.c:699:
Enter pass phrase for subrootCA.key:
Enter Export Password:
Verifying - Enter Export Password:
OpenSSL>
```

Signing server certificate with sub root CA certificate:

- `x509 -req -CA subrootCA.crt -CAkey subrootCA.key -in server.csr -out server.crt -days 365 -CAcreateserial -extfile domain.ext`
- `x509 -in server.crt -outform der -out server.der`

```
OpenSSL> x509 -req -CA subrootCA.crt -CAkey subrootCA.key -in server.csr -out server.crt -days 365 -CAcreateserial -extfile domain.ext
Signature ok
subject=C = BD, ST = Dhaka, L = Dhaka, O = East West University, OU = CSE, CN = www.baymaxsecureserver.com, emailAddress = baymax@live.com
Getting CA Private Key
15992:error:08064066:object identifier routines:OBJ_create:oid exists:crypto\objects\obj_dat.c:699:
Enter pass phrase for subrootCA.key:
OpenSSL> x509 -in server.crt -outform der -out server.der
OpenSSL>
```

Exporting the server key file in the server .pfx file:

- `pkcs12 -inkey server.key -in server.crt -export -out server.pfx`

```
OpenSSL> pkcs12 -inkey server.key -in server.crt -export -out server.pfx
Enter Export Password:
Verifying - Enter Export Password:
OpenSSL>
```

Replacing the RSA encryption from the server and sub root CA key for setting the validity:

- `rsa -in server.key -out server.key`
- `rsa -in subrootCA.key -out subrootCA.key`

```
OpenSSL> rsa -in server.key -out server.key
writing RSA key
OpenSSL> rsa -in subrootCA.key -out subrootCA.key
Enter pass phrase for subrootCA.key:
writing RSA key
OpenSSL>
```

Now we have to install those certificates. Go to ***'C:\xampp\apache\bin'*** and install ***rootCA.crt*** and ***subrootCA.pfx***.

- Copy from that location ***'server.crt'*** and replace with ***'C:\xampp\apache\conf\ssl.crt\server.crt'***
- Copy from that location ***'server.csr'*** and replace with ***'C:\xampp\apache\conf\ssl.csr\server.csr'***
- Copy from that location ***'server.key'*** and replace with ***'C:\xampp\apache\conf\ssl.key\server.key'***

Lastly, go to ***'C:\xampp\apache\conf\extra\httpd-vhosts.conf'*** and open in an editor and add these lines of code at the last for configuring ***httpd-vhosts***:

```
<VirtualHost *:443>
        DocumentRoot "C:/baymaxSecureServer/"
        ServerName baymaxsecureserver
        ServerAlias www.baymaxsecureserver.com
        SSLEngine on
        SSLCertificateFile "conf/ssl.crt/server.crt"
        SSLCertificateKeyFile "conf/ssl.key/server.key"
</VirtualHost>
```

Revocation of certificate:

- Go to ***'C:\xampp\apache\bin'*** location and create file named ***'subrootCA.conf'*** where this code will be written:

```
[ca]
default_ca = CA_default
[CA_default]
dir =C:/xampp/apache/bin
certs = $dir
crl_dir = $dir
new_certs_dir = $dir
database = $dir/index.txt
serial = $dir/serial.txt
RANDFILE = $dir/private/.rand
private_key = $dir/subrootCA.key
certificate = $dir/subrootCA.crt
crlnumber = $dir/crlnumber.txt
crl = $dir/crl/ca.crl
default_crl_days = 30
default_md = sha256
name_opt = ca_default
cert_opt = ca_default
default_days = 365
preserve = no
```

```
policy = policy_loose
[ policy_strict ]
countryName = supplied
stateOrProvinceName = supplied
organizationName = supplied
organizationalUnitName = optional
commonName = supplied
emailAddress = optional
[ policy_loose ]
countryName = optional
stateOrProvinceName = optional
localityName = optional
organizationName = optional
organizationalUnitName = optional
commonName = supplied
emailAddress = optional
[ req ]
# Options for the req tool, man req.
default_bits = 2048
distinguished_name = req_distinguished_name
string_mask = utf8only
default_md = sha256
# Extension to add when the -x509 option is used.
x509_extensions = v3_ca
[ req_distinguished_name ]
countryName = Country Name (2 letter code)
stateOrProvinceName = State or Province Name
localityName = Locality Name
0.organizationName = Organization Name
organizationalUnitName = Organizational Unit Name
commonName = Common Name
emailAddress = Email Address
countryName_default = BD
stateOrProvinceName_default = Dhaka
0.organizationName_default = EWU
[ v3_ca ]
# Extensions to apply when createing root ca
# Extensions for a typical CA, man x509v3_config
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, digitalSignature, cRLSign, keyCertSign
[ v3_intermediate_ca ]
```

```
# Extensions to apply when creating intermediate or sub-ca
# Extensions for a typical intermediate CA, same man as above
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
#pathlen:0 ensures no more sub-ca can be created below an intermediate
basicConstraints = critical, CA:true, pathlen:0
keyUsage = critical, digitalSignature, cRLSign, keyCertSign
crlDistributionPoints = @crl_dist_points
[ server_cert ]
# Extensions for server certificates
basicConstraints = CA:FALSE
nsComment = "OpenSSL Generated Server Certificate"
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer:always
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth
subjectAltName = @alt_names
[alt_names]
DNS.1 = www.baymxsecureserver.com
DNS.2 = 127.0.0.1
```

- Now we have to create some files in the same directory named ***index.txt***, ***serial.txt*** and ***crlnumber.txt***

➢ Open openssl.exe to revoke the certificate issued to verysecureserver.com from the Acme CA

```
ca -config subrootCA.conf -revoke server.crt
```

➢ To generate revocation crl file

```
ca -config subrootCA.conf -gencrl -out rev.crl
```

➢ To see the revocation file in the form of text

```
crl -in rev.crl -noout -text
```

DNS Configuration Using Bind9:

- **First we have to install bind9 from the below link and configure it like the 2 no video**
  - ♦ https://www.isc.org/bind/
  - ♦ https://www.youtube.com/watch?v=fsrny8RADZM