



EAST WEST UNIVERSITY

Department Of CSE

Computer and Cyber-security, Mini Project: 01

Group Number: 113

Title: Securing a networked system with Public Key Infrastructure
(Implementing Transport Layer Security on HTTP for https://
connection)

Course: CSE 487

Section: 01

Submitted By:

Sharmin Akther Rima

ID: 2018-2-60-112

Meftahul Zannat

ID: 2018-2-60-049

Submitted To:

Rashedul Amin Tuhin

Senior Lecturer

Department of CSE, East West University

Step 1:

DNS Configuration:

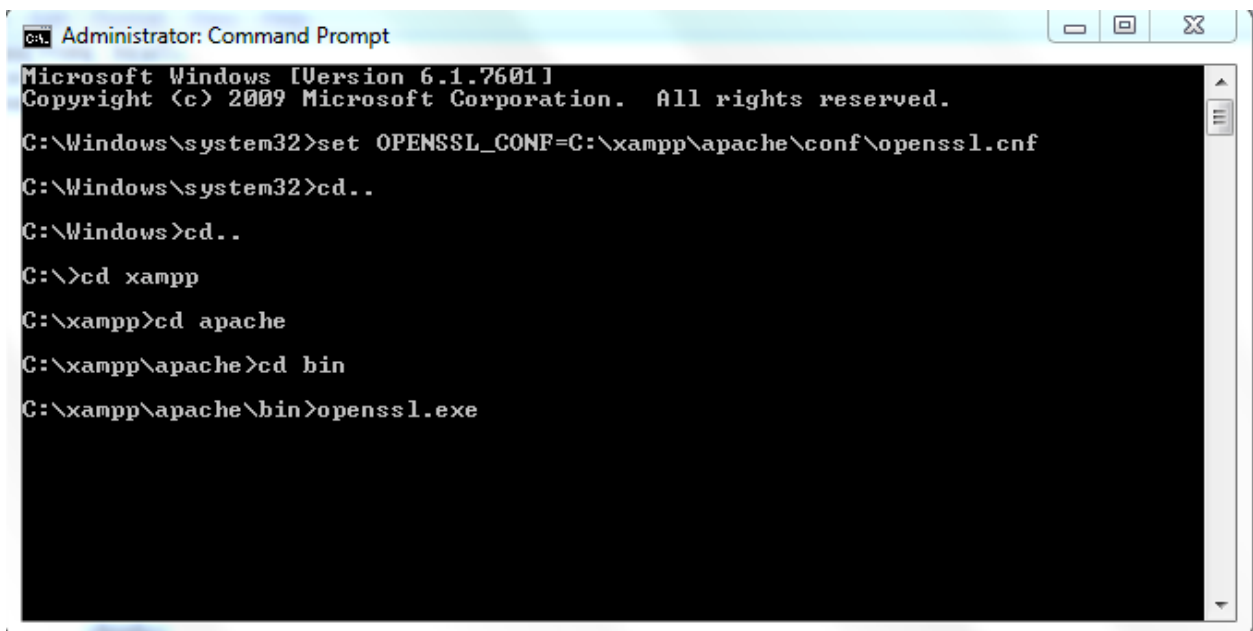
hosts:

127.0.0.1	localhost
127.0.0.1	acmesecureserver
127.0.0.1	www.acmesecureserver.com

Step 2:

For openssl environment path configuration:

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



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

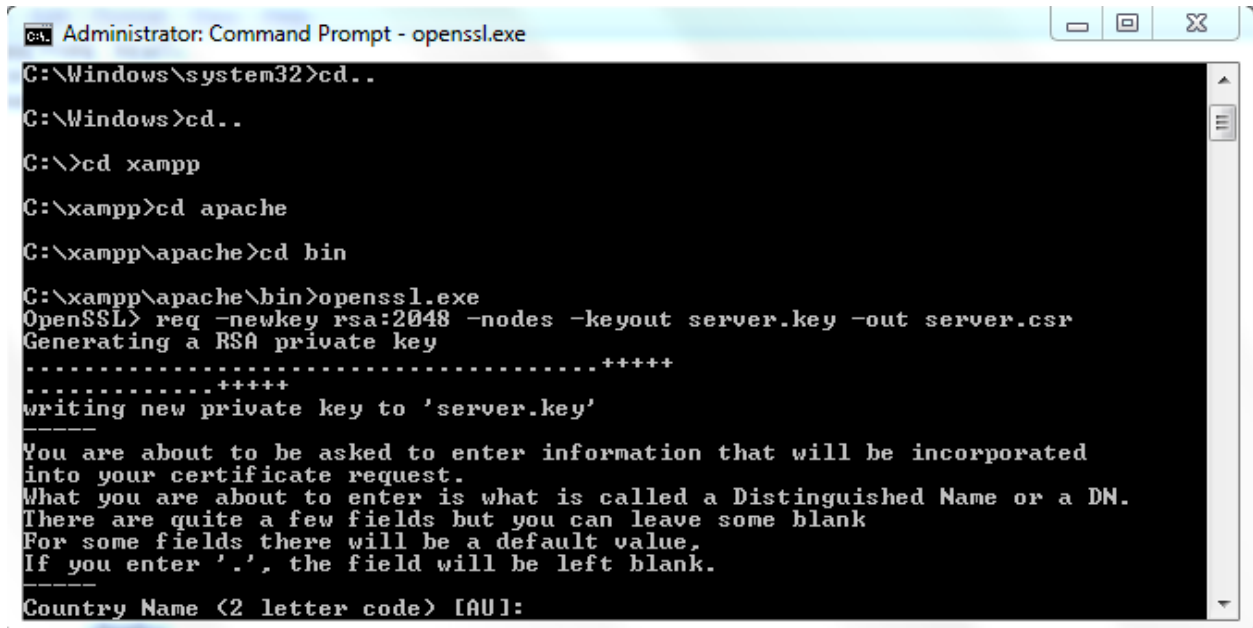
C:\Windows\system32>set OPENSSL_CONF=C:\xampp\apache\conf\openssl.cnf
C:\Windows\system32>cd..
C:\Windows>cd..
C:\>cd xampp
C:\xampp>cd apache
C:\xampp\apache>cd bin
C:\xampp\apache\bin>openssl.exe
```

For creating a server certificate:

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

Common name: www.acmesecureserver.com

~ x509 -signkey server.key -in server.csr -req -days 365 -out server.crt



```
Administrator: Command Prompt - openssl.exe
C:\Windows\system32>cd..
C:\Windows>cd..
C:\>cd xampp
C:\xampp>cd apache
C:\xampp\apache>cd bin
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]:
```

For creating a sub root CA certificate:

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

Common Name: AcmeCA

~ x509 -signkey subrootCA.key -in subrootCA.csr -req -days 365 -out subrootCA.crt

For creating a root CA certificate:

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

Common Name: Acme-RootCA

```
Administrator: Command Prompt - openssl.exe
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]:EWU
Organizational Unit Name (eg, section) []:CSE
Common Name (e.g. server FQDN or YOUR name) []:Acme-RootCA
Email Address []:cyber487@gmail.com
OpenSSL>
```

domain.ext:

authorityKeyIdentifier=keyid,issuer

basicConstraints=CA:FALSE

subjectAltName = @alt_names

[alt_names]

DNS.1 =www.acmesecureserver.com

DNS.2 =127.0.0.1

```
$ hosts domain.ext X
C: > xampp > apache > bin > domain.ext
1
2 authorityKeyIdentifier=keyid,issuer
3 basicConstraints=CS:FALSE
4 subjectAltName = @alt_names
5 [alt_names]
6 DNS.1 =www.acmesecureserver.com
7 DNS.2 =127.0.0.1
8
```

root.ext:

authorityKeyIdentifier=keyid,issuer

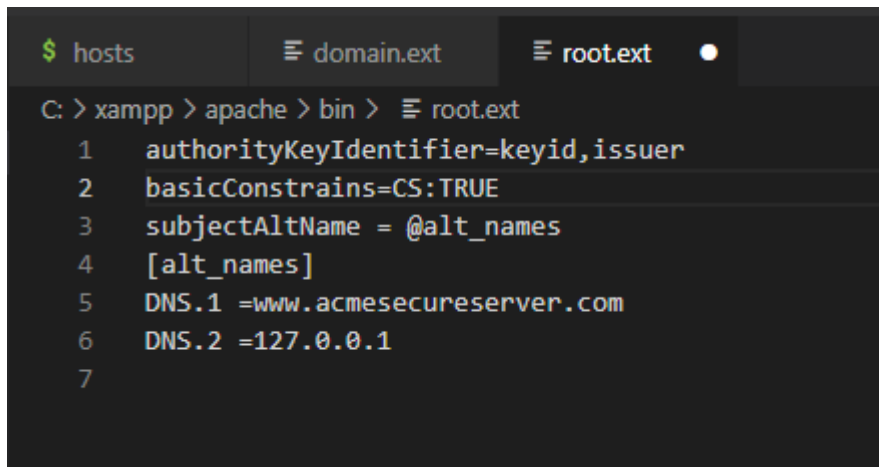
basicConstraints=CA:TRUE

subjectAltName = @alt_names

[alt_names]

DNS.1 =www.acmesecureserver.com

DNS.2 =127.0.0.1

A screenshot of a terminal window with a dark background. At the top, there are three tabs: '\$ hosts', 'domain.ext', and 'root.ext' (which is active and has a white dot). Below the tabs, the terminal shows the command 'C: > xampp > apache > bin > root.ext' followed by a numbered list of six lines of text: 1 authorityKeyIdentifier=keyid,issuer, 2 basicConstraints=CS:TRUE, 3 subjectAltName = @alt_names, 4 [alt_names], 5 DNS.1 =www.acmesecureserver.com, 6 DNS.2 =127.0.0.1, and 7 (an empty line).**Signing subrootCA certificate with rootCA certificate:**

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

For checking the subrootCa certificate:

~ x509 -text -noout -in subrootCA.crt

~ x509 -in subrootCA.crt -outform der -out subrootCA.der

Exporting the subrootCA key file in subrootCA pfx file:

~ pkcs12 -inkey subrootCA.key -in subrootCA.crt -export -out subrootCA.pfx

Signing server certificate with subrootCA 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

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

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

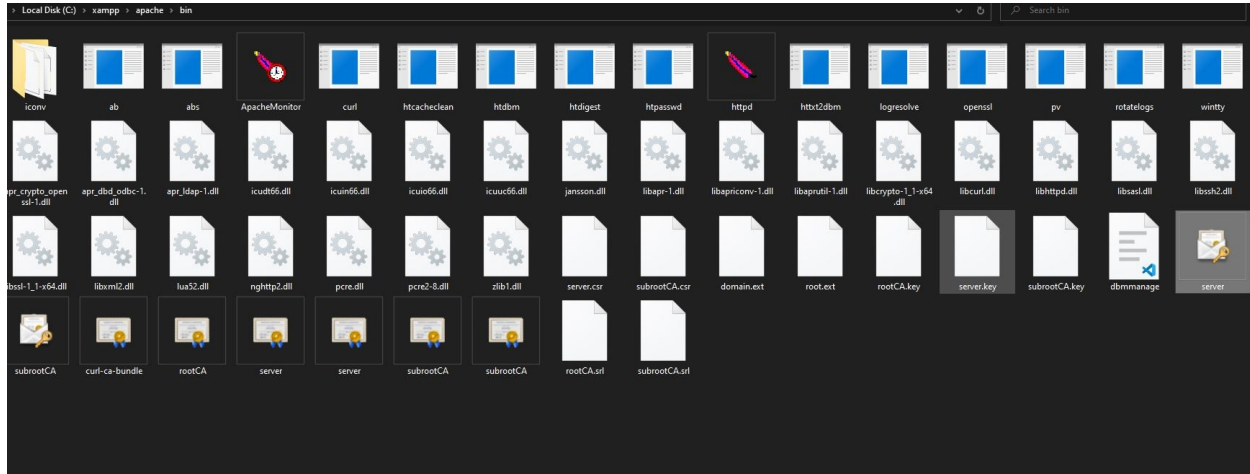
Replacing the RSA encryption from the server and subrootCA key for setting the validity:

~ rsa -in server.key -out server.key

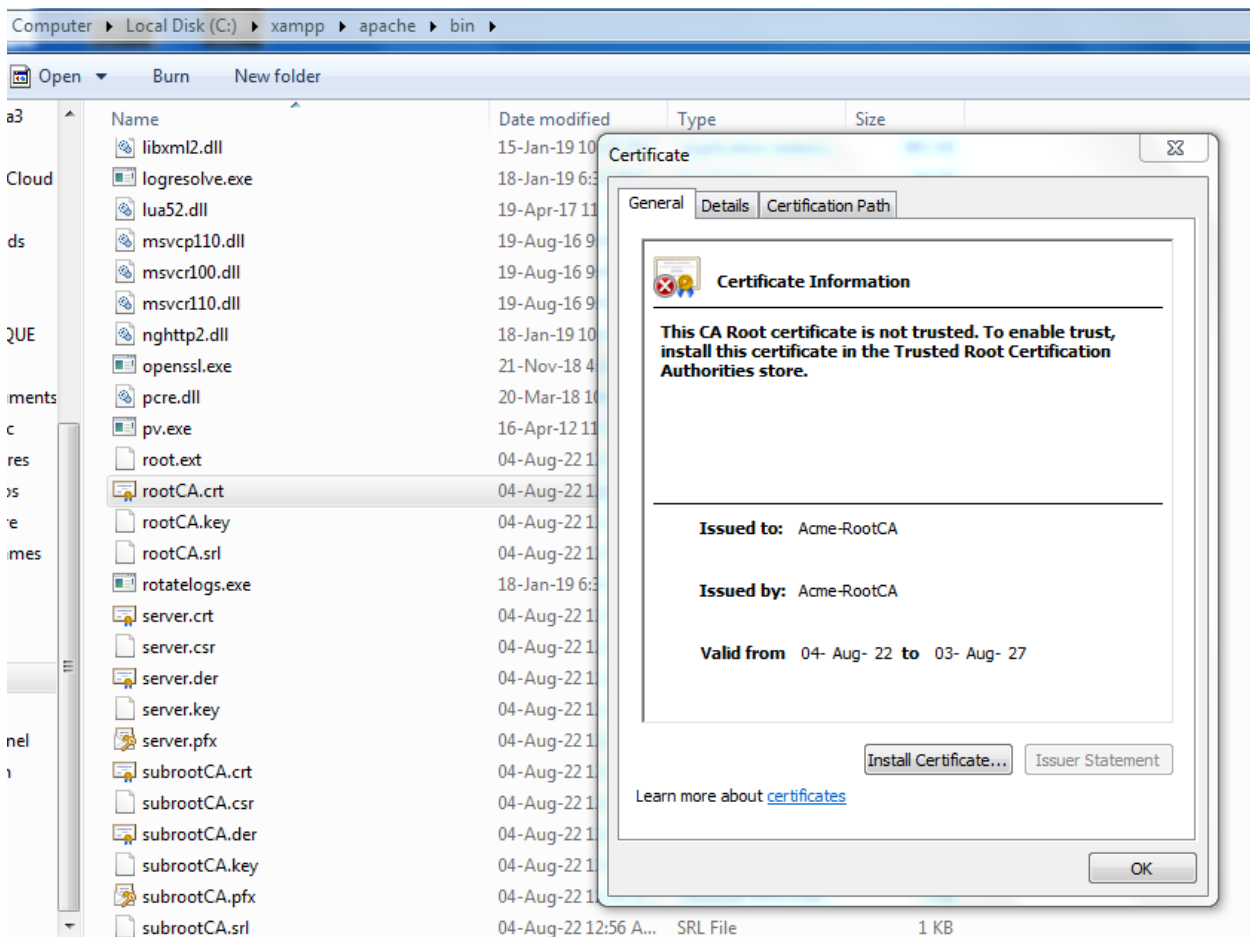
~ rsa -in subrootCA.key -out subrootCA.key

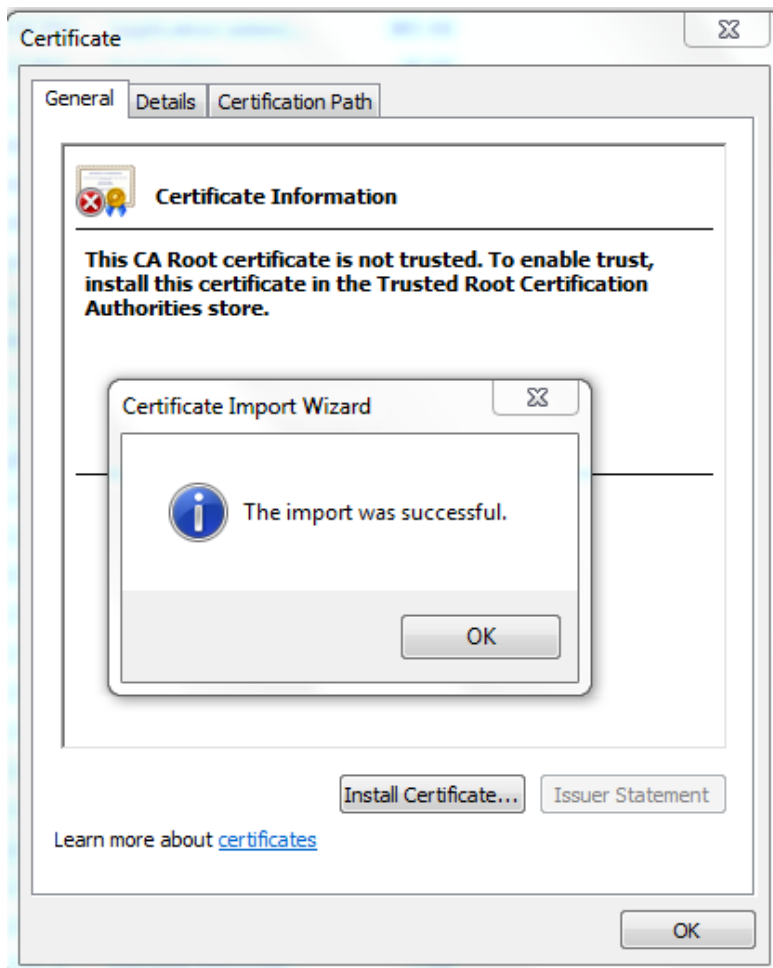
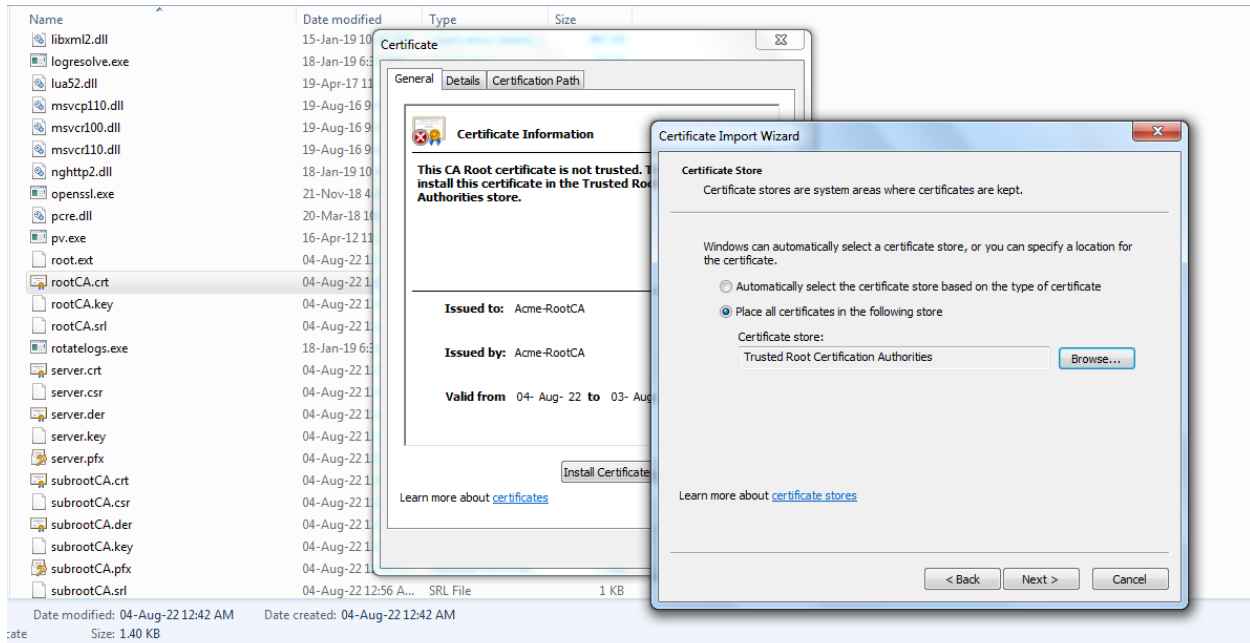
```
OpenSSL> x509 -in subrootCA.crt -outform der -out subrootCA.der
OpenSSL> pkcs12 -inkey subrootCA.key -in subrootCA.crt -export -out subrootCA.pfx
7480:error:08064066:object identifier routines:OBJ_create:oid exists:crypto\obje
cts\obj_dat.c:698:
Enter pass phrase for subrootCA.key:
Enter Export Password:
Verifying - Enter Export Password:
OpenSSL> x509 -req -CA subrootCA.crt -CAkey subrootCA.key -in server.csr -out se
rver.crt -days 365 -CAcreateserial -extfile domain.ext
Signature ok
subject=C = BD, ST = Dhaka, L = Dhaka, O = EWU, OU = CSE, CN = ww.acmesecureserv
er.com, emailAddress = cyber487@gmail.com
Getting CA Private Key
7480:error:08064066:object identifier routines:OBJ_create:oid exists:crypto\obje
cts\obj_dat.c:698:
Enter pass phrase for subrootCA.key:
OpenSSL> x509 -in server.crt -outform der -out server.der
OpenSSL> pkcs12 -inkey server.key -in server.crt -export -out server.pfx
Enter Export Password:
Verifying - Enter Export Password:
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>
```

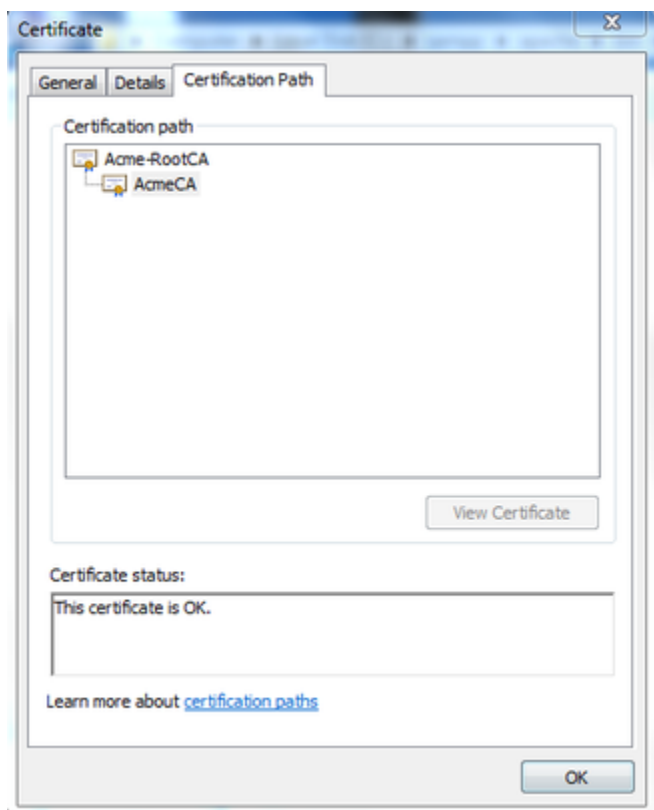
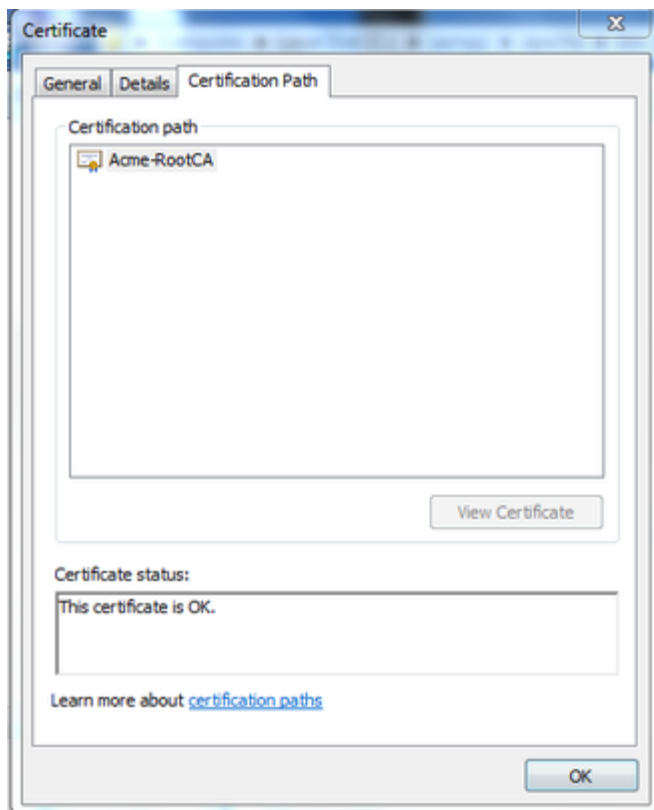
After executing these commands, we will have certificates:

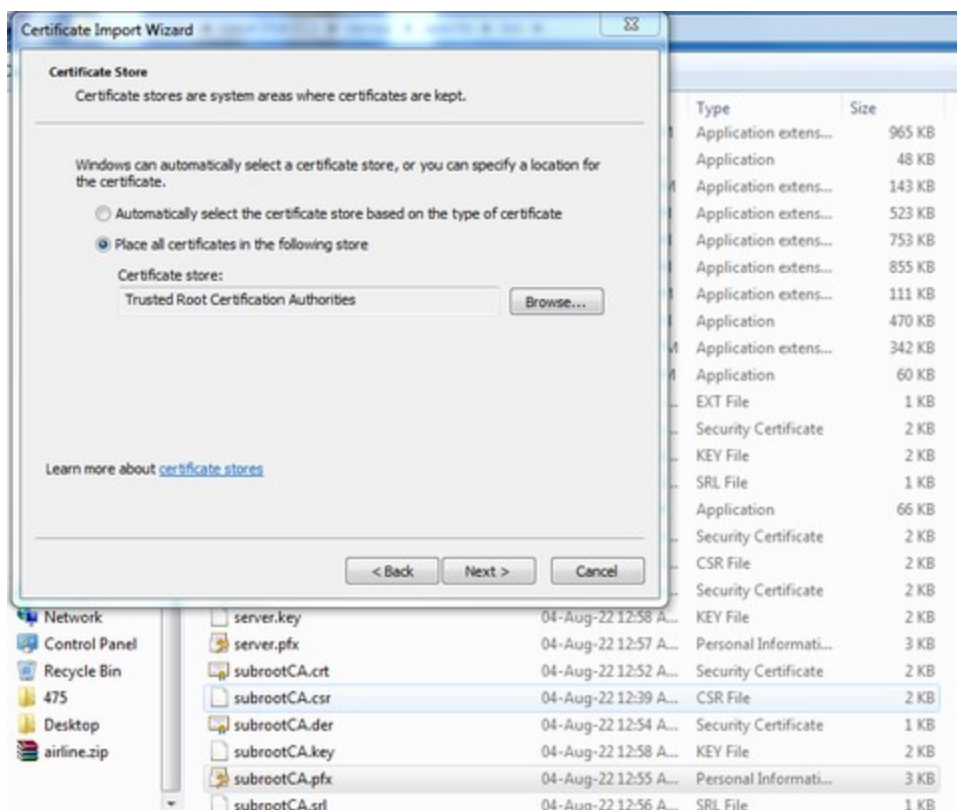
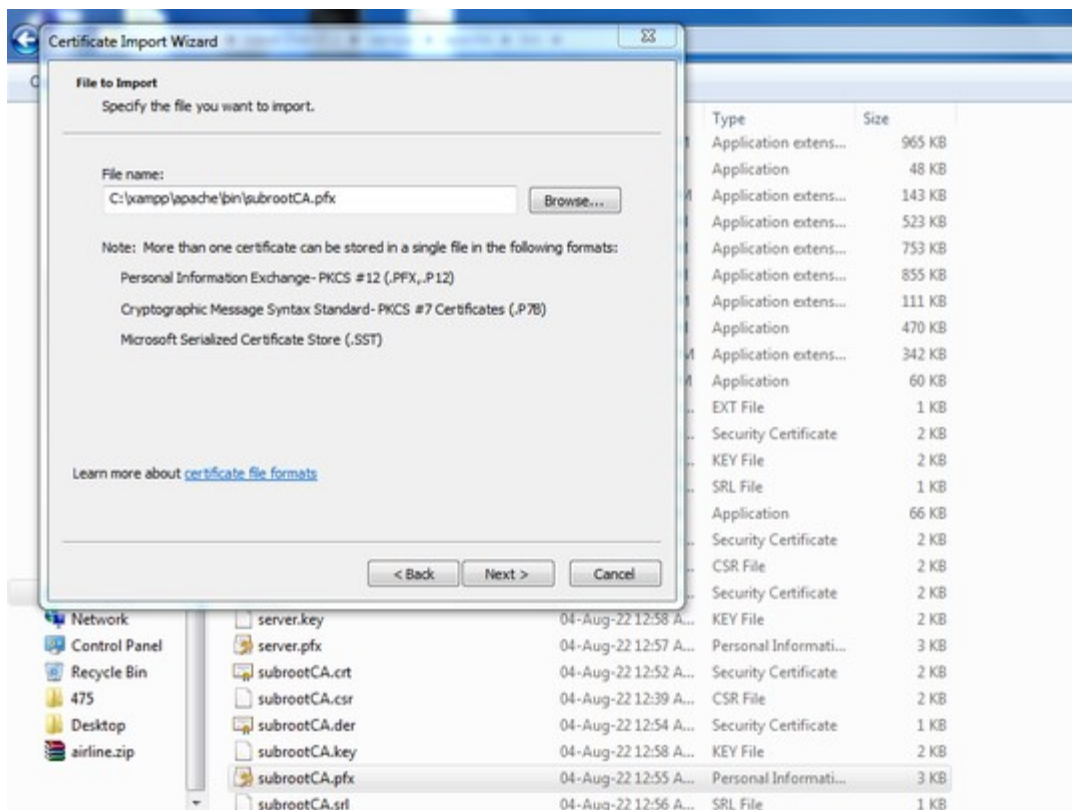


Now importing all certificate :

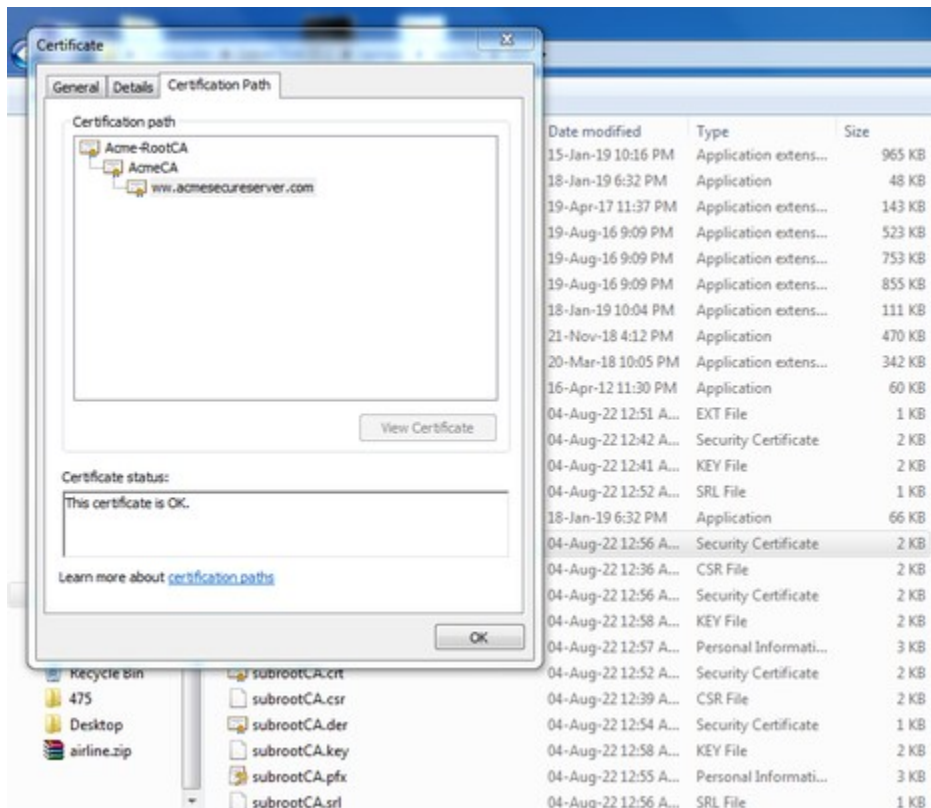








logresolve.exe	18-Jan-19 6:32 PM	Application	48 KB
lua52.dll	19-Apr-17 11:37 PM	Application extens...	143 KB
msvcp110.dll	19-Aug-16 9:09 PM	Application extens...	523 KB
msvcr100.dll	19-Aug-16 9:09 PM	Application extens...	753 KB
msvcr110.dll	19-Aug-16 9:09 PM	Application extens...	855 KB
nghttp2.dll	18-Jan-19 10:04 PM	Application extens...	111 KB
openssl.exe	21-Nov-18 4:12 PM	Application	470 KB
pcre.dll	20-Mar-18 10:05 PM	Application extens...	342 KB
pv.exe	16-Apr-12 11:30 PM	Application	60 KB
root.ext	04-Aug-22 12:51 A...	EXT File	1 KB
rootCA.crt	04-Aug-22 12:42 A...	Security Certificate	2 KB
rootCA.key	04-Aug-22 12:41 A...	KEY File	2 KB
rootCA.srl	04-Aug-22 12:52 A...	SRL File	1 KB
rotatelog.exe	18-Jan-19 6:32 PM	Application	66 KB
server.crt	04-Aug-22 12:56 A...	Security Certificate	2 KB
server.csr	04-Aug-22 12:36 A...	CSR File	2 KB
server.der	04-Aug-22 12:56 A...	Security Certificate	2 KB
server.key	04-Aug-22 12:58 A...	KEY File	2 KB
server.pfx	04-Aug-22 12:57 A...	Personal Informati...	3 KB
subrootCA.crt	04-Aug-22 12:52 A...	Security Certificate	2 KB
subrootCA.csr	04-Aug-22 12:39 A...	CSR File	2 KB
subrootCA.der	04-Aug-22 12:54 A...	Security Certificate	1 KB
subrootCA.key	04-Aug-22 12:58 A...	KEY File	2 KB
subrootCA.pfx	04-Aug-22 12:55 A...	Personal Informati...	3 KB
subrootCA.srl	04-Aug-22 12:56 A...	SRL File	1 KB



Step 3 :

Creating certificate:

Configuring httpd-vhosts:

```
<VirtualHost *:443>
```

```
    DocumentRoot "C:/acmesecureserver/"
```

```
    ServerName acmesecureserver
```

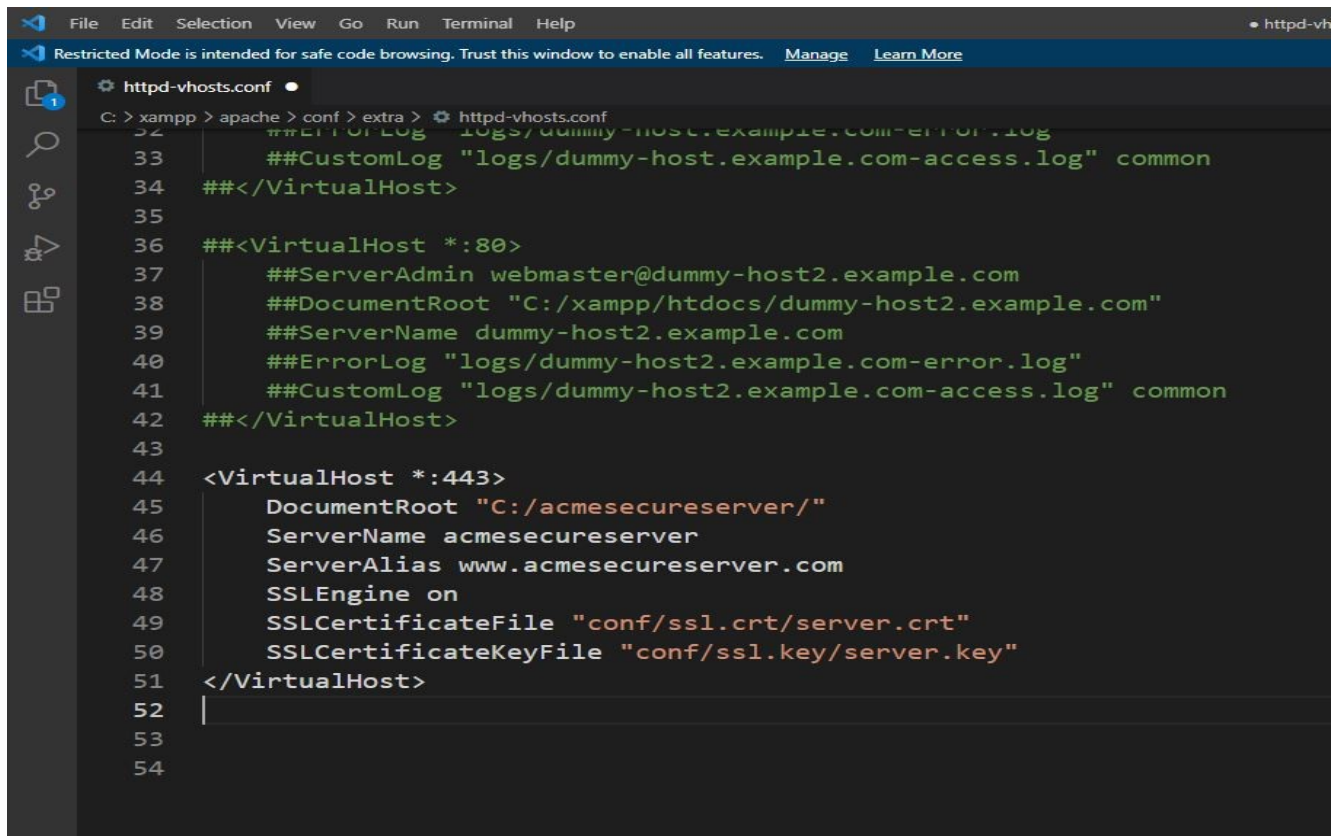
```
    ServerAlias www.acmesecureserver.com
```

```
    SSLEngine on
```

```
    SSLCertificateFile "conf/ssl.crt/server.crt"
```

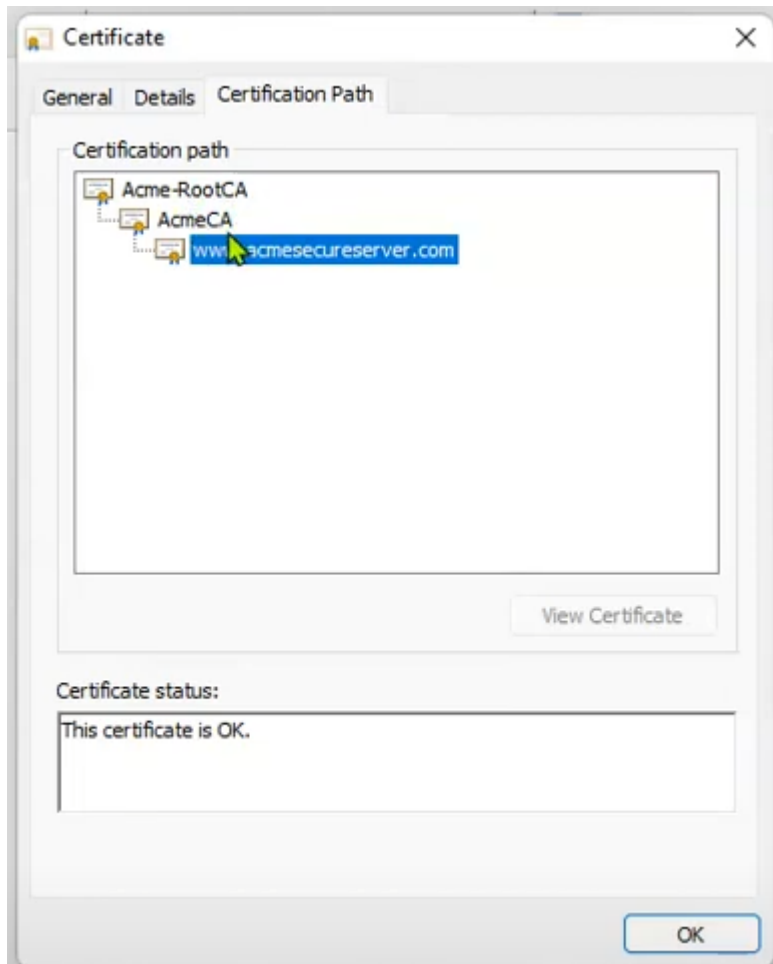
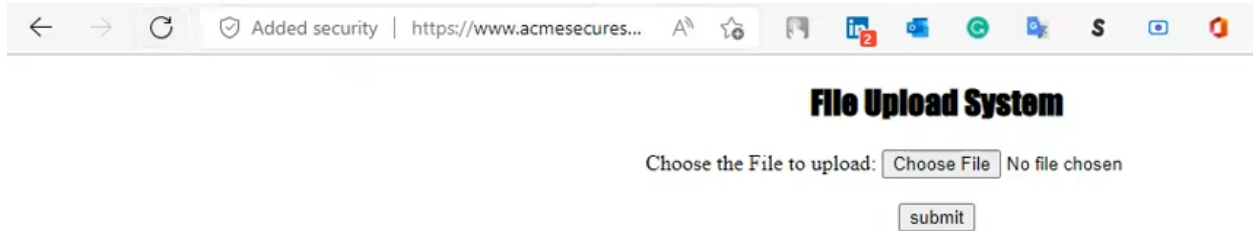
```
    SSLCertificateKeyFile "conf/ssl.key/server.key"
```

```
</VirtualHost>
```



```
File Edit Selection View Go Run Terminal Help
Restricted Mode is intended for safe code browsing. Trust this window to enable all features. Manage Learn More
httpd-vhosts.conf
C: > xampp > apache > conf > extra > httpd-vhosts.conf
32  ##ErrorLog logs/dummy-host.example.com-error.log
33  ##CustomLog "logs/dummy-host.example.com-access.log" common
34  ##</VirtualHost>
35
36  ##<VirtualHost *:80>
37  ##ServerAdmin webmaster@dummy-host2.example.com
38  ##DocumentRoot "C:/xampp/htdocs/dummy-host2.example.com"
39  ##ServerName dummy-host2.example.com
40  ##ErrorLog "logs/dummy-host2.example.com-error.log"
41  ##CustomLog "logs/dummy-host2.example.com-access.log" common
42  ##</VirtualHost>
43
44  <VirtualHost *:443>
45      DocumentRoot "C:/acmesecureserver/"
46      ServerName acmesecureserver
47      ServerAlias www.acmesecureserver.com
48      SSLEngine on
49      SSLCertificateFile "conf/ssl.crt/server.crt"
50      SSLCertificateKeyFile "conf/ssl.key/server.key"
51  </VirtualHost>
52
53
54
```

After installing all the certificates:



Step 4:

Revocation of certificate:

Open openssl.exe to revoke the certificate issued to acmesecureserver.com from the AcmeCA →

```
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
```

subrootCA.conf:

```
[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 = Acme
[ 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.acmesecureserver.com

DNS.2 = 127.0.0.1