EAST WEST UNIVERSITY

Mini Project - 1

Course Title: **Cyber Security, Ethics and Law**

Course Code: **CSE487**

Section No: **3**

Submitted To:

Rashedul Amin Tuhin

Senior Lecturer

Department of Computer Science & Engineering

East West University

Submitted By:

Anika Islam

2019-3-60-008

Shamima Sultana

2018-3-60-099

Md. Amir Hozaifa Bin Zaher

2019-3-60-109

Date of submission:

14 December 2022

Certificate Generation

Changing directory to root folder with superuser access:

sudo -i

Making directories:

mkdir -p ca/{root-ca,sub-ca,server}/{private,newcerts,crl,csr}

Changing mode:

chmod -v 700 ca/{root-ca,sub-ca,server}/private

```
root@amir-VirtualBox:~# chmod -v 700 ca/{root-ca,sub-ca,server}/private
mode of 'ca/root-ca/private' changed from 0755 (rwxr-xr-x) to 0700 (rwx------)
mode of 'ca/sub-ca/private' changed from 0755 (rwxr-xr-x) to 0700 (rwx------)
mode of 'ca/server/private' changed from 0755 (rwxr-xr-x) to 0700 (rwx------)
```

chmod -v 700 ca/{root-ca,sub-ca}/newcerts

```
root@amir-VirtualBox:~# chmod -v 700 ca/{root-ca,sub-ca}/newcerts
mode of 'ca/root-ca/newcerts' changed from 0755 (rwxr-xr-x) to 0700 (rwx------)
mode of 'ca/sub-ca/newcerts' changed from 0755 (rwxr-xr-x) to 0700 (rwx------)
```

Creating index and serial file:

touch ca/{root-ca,sub-ca}/index.txt

touch ca/{root-ca,sub-ca}/serial

echo '01' > ca/root-ca/serial

echo '01' > ca/sub-ca/serial

Generating private key for root CA, sub CA and server:

cd /root/ca/

openssl genrsa -aes256 -out root-ca/private/cakey.pem 4096

```
root@amir-VirtualBox:~/ca# openssl genrsa -aes256 -out root-ca/private/cakey.pem 4096
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................++++
.....................................................................................++++
e is 65537 (0x010001)
Enter pass phrase for root-ca/private/cakey.pem:
Verifying - Enter pass phrase for root-ca/private/cakey.pem:
```

openssl genrsa -aes256 -out sub-ca/private/cakey.pem 4096

```
root@amir-VirtualBox:~/ca# openssl genrsa -aes256 -out sub-ca/private/cakey.pem 4096
Generating RSA private key, 4096 bit long modulus (2 primes)
.................................................++++
.............................++++
e is 65537 (0x010001)
Enter pass phrase for sub-ca/private/cakey.pem:
Verifying - Enter pass phrase for sub-ca/private/cakey.pem:
```

openssl genrsa -out server/private/server.key 2048

```
root@amir-VirtualBox:~/ca# openssl genrsa -out server/private/server.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....................+++++
.................................................+++++
e is 65537 (0x010001)
```

Creating config file for root CA:

cd /root/ca/root-ca

vim root-ca.conf

Paste root-ca.conf **file text from the appendix. Click ESC, :wq and enter to exit**

Creating certificate for root CA:

openssl req -new -x509 -extensions v3_ca -key private/cakey.pem -out cacert.pem -days 3650 -config root-ca.conf

```
root@amir-VirtualBox:~/ca/root-ca# openssl req -new -x509 -extensions v3_ca -key private/cakey.pem -out
cacert.pem -days 3650 -config root-ca.conf
Enter pass phrase for private/cakey.pem:
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) [BD]:
State or Province Name (full name) [Dhaka]:
Locality Name (city, district) [Rampura]:
Organization Name (company) [AcmeCA]:
Organizational Unit Name (department, division) [admin]:
Common Name (hostname, IP, or your name) [rootCA]:
Email Address [admin@acmeca.com]:
```

Default values are accordingly given in the config file.

Creating config file for sub CA:

cd /root/ca/sub-ca

vim sub-ca.conf

Paste sub-ca.conf **file text from the appendix. Click ESC, :wq and enter to exit**

Creating certificate for sub CA:

openssl req -new -key private/cakey.pem -sha256 -out csr/sub-ca.csr -config sub-ca.conf

Generating certificate signing request (CSR) for sub CA:

```
root@amir-VirtualBox:~/ca/sub-ca# openssl req -new -key private/cakey.pem -sha256 -out csr/sub-ca.csr
-config sub-ca.conf
Enter pass phrase for private/cakey.pem:
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) [BD]:
State or Province Name (full name) [Dhaka]:
Locality Name (city, district) [Rampura]:
Organization Name (company) [AcmeCA]:
Organizational Unit Name (department, division) [subadmin]:
Common Name (hostname, IP, or your name) [subCA]:
Email Address [subadmin@acmeca.com]:
```

Default values are accordingly given in the config file.

Generating sub CA certificate from sub CA CSR and root CA:

cd ../root-ca

openssl ca -extensions v3_intermediate_ca -days 3652 -notext -in ../sub-ca/csr/sub-ca.csr -out ../sub-ca/cacert.pem -config root-ca.conf

```
root@amir-VirtualBox:~/ca/root-ca# openssl ca -extensions v3_intermediate_ca -days 3652 -notext -in ..
/sub-ca/csr/sub-ca.csr -out ../sub-ca/cacert.pem -config root-ca.conf
Using configuration from root-ca.conf
Enter pass phrase for /root/ca/root-ca/private/cakey.pem:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'BD'
stateOrProvinceName   :PRINTABLE:'Dhaka'
localityName          :PRINTABLE:'Rampura'
organizationName      :PRINTABLE:'AcmeCA'
organizationalUnitName:PRINTABLE:'subadmin'
commonName            :PRINTABLE:'subCA'
Certificate is to be certified until Nov 24 11:35:56 2032 GMT (3652 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
```

Generating certificate signing request (CSR) for server:

cd ../server

openssl req -key private/server.key -new -sha256 -out csr/server.csr

```
root@amir-VirtualBox:~/ca/server# openssl req -key private/server.key -new -sha256 -out csr/server.csr

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) []:Rampura
Organization Name (eg, company) [Internet Widgits Pty Ltd]:www.verysecureserver.com
Organizational Unit Name (eg, section) []:serveradmin
Common Name (e.g. server FQDN or YOUR name) []:www.verysecureserver.com
Email Address []:info@verysecureserver.com

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

Generating server certificate from server CSR and sub CA:

openssl ca -config ../sub-ca/sub-ca.conf -extensions server_cert -days 365 -notext -in csr/server.csr -out cert.pem

```
root@amir-VirtualBox:~/ca/server# openssl ca -config ../sub-ca/sub-ca.conf -extensions server_cert -da
ys 365 -notext -in csr/server.csr -out cert.pem
Using configuration from ../sub-ca/sub-ca.conf
Enter pass phrase for /root/ca/sub-ca/private/cakey.pem:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'BD'
stateOrProvinceName   :ASN.1 12:'Dhaka'
localityName          :ASN.1 12:'Rampura'
organizationName      :ASN.1 12:'www.verysecureserver.com'
organizationalUnitName:ASN.1 12:'serveradmin'
commonName            :ASN.1 12:'www.verysecureserver.com'
Certificate is to be certified until Nov 25 11:38:46 2023 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
```

Server Creation and Saving Certificate

Mapping hostname to IP:

echo "127.0.0.2 www.verysecureserver.com" >> /etc/hosts

Server Creation:
Download and install xampp
Modify index.php **file located in** /opt/lampp/htdocs **and provide php code for the server:**
sudo -s

gedit /opt/lampp/htdocs/index.php

Modify httpd-ssl.conf **in** /opt/lampp/etc/extra**:**
gedit /opt/lampp/etc/extra/httpd-ssl.conf
Replace 106 line with this:
SSLCertificateFile "/root/ca/server/cert.pem"
Replace 116 line with this:
SSLCertificateKeyFile "/root/ca/server/private/server.key"
Replace 137 line with this:
SSLCACertificateFile "/root/ca/sub-ca/cacert.pem"
These indicate the server certificate, private key and the CA cert

For redirecting http to https:
gedit httpd-xampp.conf
Append the following at the end:

```
<IfModule mod_rewrite.c>
   RewriteEngine On

   # Redirect /xampp folder to https
   RewriteCond %{HTTPS} !=on
   RewriteCond %{REQUEST_URI} /
   RewriteRule ^(.*) https://%{SERVER_NAME}$1 [R,L]
</IfModule>
```

Save and exit

Run Xampp:
sudo -s
cd /opt/lampp/
./manager-linux-x64.run
Click on start on Manage Servers => Apache Web Server.

Checking with curl:
curl https://www.verysecureserver.com
This will show error, since CA certificates are not provided.
sudo -i
cp -T /root/ca/root-ca/cacert.pem /usr/local/share/ca-certificates/acmerootca.crt
cp -T /root/ca/sub-ca/cacert.pem /usr/local/share/ca-certificates/acmesubca.crt
update-ca-certificates -v
CA certificates are now provided.
Checking with curl will show the html file:

curl https://www.verysecureserver.com

Uploading CA certificates to a browser: (Mozilla)
cp -T /root/ca/root-ca/cacert.pem ~amir/acmerootca.crt
cp -T /root/ca/sub-ca/cacert.pem ~amir/acmesubca.crt

Here amir **is the username of the PC.**
Go to Preferences => Search cert => View Certificates => Authorities => Import => acmerootca.crt => **Tick on both checkbox => OK**
=> Import => acmesubca.crt => **Do not tick on both checkbox => OK.**

Clear the browser and restart.
Now there should be the security padlock symbol.

DNS

For static IP:

Go to Oracle VirtualBox software => File => Host Network Manager => Click the first option and properties => Untick DHCP server.

Turn off your virtual machines.

For both client and host pc:

Setting virtual network:

Select your virtual machine => Settings => Network => Adapter 1 => Tick Enable Network Adapter => Attached to: Host-only Adapter =>Advanced => Promiscuous Mode => Allow VMs => Adapter 2 => Tick Enable Network Adapter => Attached to: NAT

Turn on your host virtual machine.

Go to Settings => Select the first network => IPv4 => Manual => Addresses => Address: 192.168.56.199 => Network: 255.255.255.0 => Gateway: 192.168.56.1 => DNS => Turn off Automatic => DNS: 192.168.56.1 => Apply => Turn the network off and on

Turn on your client virtual machine.

Go to Settings => Select the first network => IPv4 => Manual => Addresses => Address: 192.168.56.101 => Network: 255.255.255.0 => Gateway: 192.168.56.1 => DNS => Turn off Automatic => DNS: 192.168.56.1 => Apply => Turn the network off and on

Turn off your client virtual machine.

192.168.56.199 is the host IP.

192.168.56.101 is the client IP.

From host PC:

Turn the network of to access internet, (for example: using apt install command)

Installing bind9:

sudo -i

sudo apt install bind9

Checking machine status:

hostnamectl status

```
  Static hostname: amir-VirtualBox
        Icon name: computer-vm
          Chassis: vm
       Machine ID: 3f6dc438e0d34b619e62c51d0845adb6
          Boot ID: 0f69734714c44cd9a4fe0ce9d680559a
   Virtualization: oracle
 Operating System: Ubuntu 20.04.2 LTS
           Kernel: Linux 5.15.0-52-generic
     Architecture: x86-64
```

Edit the hosts file to the following:

gedit /etc/hosts

```
1 192.168.56.199 amir-VirtualBox.verysecureserver.com amir-VirtualBox
2
3 # The following lines are desirable for IPv6 capable hosts
4 ::1     ip6-localhost ip6-loopback
5 fe00::0 ip6-localnet
6 ff00::0 ip6-mcastprefix
7 ff02::1 ip6-allnodes
8 ff02::2 ip6-allrouters
```

Editing named.conf.options **file:**

cd /etc/bind

gedit named.conf.options

```
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        // forwarders {
        //      0.0.0.0;
        // };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation auto;

        listen-on-v6 { any; };
        recursion yes;
        listen-on { 192.168.56.199; };
        allow-transfer { none; };
        forwarders {
                192.168.56.1;
        };
};
```

Following is the code which is added:

```
recursion yes;
listen-on { 192.168.56.199; };
allow-transfer { none; };
forwarders {
        192.168.56.1;
};
```

Editing named.conf.local **file:**

gedit named.conf.local

```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

// forward lookup zone
zone "verysecureserver.com" IN {
        type master;
        file "/etc/bind/db.verysecureserver.com";
};

// reverse lookup zone
zone "56.168.192.in-addr.arpa" IN {
        type master;
        file "/etc/bind/db.56.168.192";
};

```

Following is the code which is added:

```
// forward lookup zone
zone "verysecureserver.com" IN {
        type master;
        file "/etc/bind/db.verysecureserver.com";
};

// reverse lookup zone
zone "56.168.192.in-addr.arpa" IN {
        type master;
        file "/etc/bind/db.56.168.192";
};
```

Checking config file:

named -checkconf

Creating and editing db.verysecureserver.com **file:**

cp db.local db.verysecureserver.com

gedit db.verysecureserver.com

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns1.verysecureserver.com. root.verysecureserver.com. (
                              2                 ; Serial
                         604800                 ; Refresh
                          86400                 ; Retry
                        2419200                 ; Expire
                         604800 )               ; Negative Cache TTL
;
@       IN      NS      ns1.verysecureserver.com.
ns1     IN      A       192.168.56.199
www     IN      A       192.168.56.199
@       IN      A       192.168.56.199
```

Following code is used:

```
;
; BIND data file for local loopback interface
;
$TTL  604800
@     IN    SOA   ns1.verysecureserver.com. root.verysecureserver.com. (
                        2           ; Serial
                     604800         ; Refresh
                      86400         ; Retry
                     2419200        ; Expire
                      604800 )      ; Negative Cache TTL
;
@     IN    NS    ns1.verysecureserver.com.
ns1   IN    A     192.168.56.199
www   IN    A     192.168.56.199
@     IN    A     192.168.56.199
```

Creating and editing db.56.168.192 **file:**

cp db.127 db.56.168.192

gedit db.56.168.192

```
1 ;
2 ; BIND reverse data file for local loopback interface
3 ;
4 $TTL    604800
5 @       IN      SOA     ns1.verysecureserver.com. root.verysecureserver.com. (
6                                 1                 ; Serial
7                            604800                 ; Refresh
8                             86400                 ; Retry
9                           2419200                 ; Expire
10                           604800 )       ; Negative Cache TTL
11 ;
12 @       IN      NS      ns1.verysecureserver.com.
13 199     IN      PTR     ns1.verysecureserver.com.
14 199     IN      PTR     www.verysecureserver.com.
15
```

Following code is used:

```
;
; BIND reverse data file for local loopback interface
;
$TTL   604800
@      IN      SOA    ns1.verysecureserver.com. root.verysecureserver.com. (
                             1             ; Serial
                        604800                  ; Refresh
                         86400                  ; Retry
                        2419200                 ; Expire
                         604800 )       ; Negative Cache TTL
;
@      IN      NS     ns1.verysecureserver.com.
199    IN      PTR    ns1.verysecureserver.com.
199    IN      PTR    www.verysecureserver.com.
```

Restarting bind9 and checking status:

service bind9 restart

service bind9 status

Deleting and linking resolv.conf **file:**

rm /etc/resolv.conf

ln -sf /run/systemd/resolve/resolv.conf /etc/resolv.conf

gedit /etc/resolv.conf

```
1 # This file is managed by man:systemd-resolved(8). Do not edit.
2 #
3 # This is a dynamic resolv.conf file for connecting local clients directly to
4 # all known uplink DNS servers. This file lists all configured search domains.
5 #
6 # Third party programs must not access this file directly, but only through the
7 # symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,
8 # replace this symlink by a static file or a different symlink.
9 #
10 # See man:systemd-resolved.service(8) for details about the supported modes of
11 # operation for /etc/resolv.conf.
12
13 # No DNS servers known.
14 nameserver 192.168.56.199
15 search localdomain
```

Following code is added:

nameserver 192.168.56.199
search localdomain

gedit /etc/nsswitch.conf

```
1 # /etc/nsswitch.conf
2 #
3 # Example configuration of GNU Name Service Switch functionality.
4 # If you have the `glibc-doc-reference' and `info' packages installed, try:
5 # `info libc "Name Service Switch"' for information about this file.
6
7 passwd:         files systemd
8 group:          files systemd
9 shadow:         files
10 gshadow:        files
11
12 hosts:          files dns mdns4_minimal [NOTFOUND=return] myhostname
13 networks:       files
14
15 protocols:      db files
16 services:       db files
17 ethers:         db files
18 rpc:            db files
19
20 netgroup:       nis
```

Following code is used at line 12:

hosts: files dns mdns4_minimal [NOTFOUND=return] myhostname

From any (Host or Client) PC:
Checking forward lookup:
nslookup www.verysecureserver.com
Checking reverse lookup:
nslookup 192.168.56.199

***To get padlock symbol in the client PC, you will similarly have to upload the certificates in to the browser,**

Firewall

Installing Firewall:

sudo apt install ufw

Allowing only ports 80, 443, 53:

ufw default allow outgoing

ufw default deny incoming

ufw enable

ufw allow 80

ufw allow 443

ufw allow 53

Checking status:

ufw status

```
root@amir-VirtualBox:~# ufw status
Status: active

To                         Action      From
--                         ------      ----
80                         ALLOW       Anywhere
443                        ALLOW       Anywhere
53                         ALLOW       Anywhere
80 (v6)                    ALLOW       Anywhere (v6)
443 (v6)                   ALLOW       Anywhere (v6)
53 (v6)                    ALLOW       Anywhere (v6)
```

IDS

From host PC:

Install snort:

sudo apt-get install snort

Enter values: enp0s3, 192.168.56.199/24

cd /etc/snort

cp snort.conf test_snort.conf

sudo gedit test_snort.conf

At line 52: ipvar HOME_NET 192.168.56.199

save and exit

sudo nano /etc/snort/rules/local.rules

Append this:

alert tcp any any -> $HOME_NET any (flags:S; msg: "DoS attack is happening!"; flow:stateless; detection_filter: track by_dst, count 70, seconds 10; sid: 100001; rev: 1;)

save and exit

Testing conf file:

sudo snort -T -i enp0s3 -c /etc/snort/test_snort.conf

Running snort:

sudo snort -A console -q -i enp0s3 -c /etc/snort/test_snort.conf

From client PC:

Installing hping3:

sudo apt install hping3 -y

Attacking host PC:

sudo hping3 192.168.56.199 -q -n -d 120 -S -p 80 --flood --rand-source

On the host PC, it will show the DoS attack warning. *CTRL + C to end the task.

Appendix

root-ca.conf file code:

```
#
# OpenSSL configuration file.
#

# Establish working directory.

dir                     = /root/ca/root-ca

[ ca ]
default_ca              = CA_default

[ CA_default ]
serial                  = $dir/serial
database                = $dir/index.txt
new_certs_dir           = $dir/newcerts
certificate             = $dir/cacert.pem
private_key             = $dir/private/cakey.pem
default_days            = 730
default_crl_days        = 30
default_md              = sha256
preserve                = no
email_in_dn             = no
nameopt                 = default_ca
certopt                 = default_ca
policy                  = policy_match

[ policy_match ]
countryName             = match
stateOrProvinceName     = optional
organizationName        = optional
organizationalUnitName  = optional
commonName              = supplied
emailAddress            = optional

[ req ]
default_bits            = 4096              # Size of keys
default_keyfile         = key.pem           # name of generated keys
default_md              = sha256            # message digest algorithm
string_mask             = nombstr           # permitted characters
distinguished_name      = req_distinguished_name
req_extensions          = v3_ca

[ req_distinguished_name ]
```

```
# Variable name             Prompt string
#-------------------------   ----------------------------
countryName                 = Country Name (2 letter code)
countryName_min             = 2
countryName_max             = 2
stateOrProvinceName         = State or Province Name (full name)
localityName                = Locality Name (city, district)
0.organizationName          = Organization Name (company)
organizationalUnitName      = Organizational Unit Name (department, division)
commonName                  = Common Name (hostname, IP, or your name)
commonName_max              = 64
emailAddress                = Email Address
emailAddress_max            = 40

# Default values for the above, for consistency and less typing.
# Variable name             Value
#-------------------------   ----------------------------
countryName_default         = BD
stateOrProvinceName_default  = Dhaka
localityName_default        = Rampura
0.organizationName_default   = AcmeCA
organizationalUnitName_default = admin
commonName_default                = rootCA
emailAddress_default      = admin@acmeca.com

[ v3_ca ]
basicConstraints            = critical, CA:TRUE
subjectKeyIdentifier        = hash
authorityKeyIdentifier      = keyid:always,issuer:always
keyUsage                    = critical, digitalSignature, cRLSign, keyCertSign


[ v3_req ]
basicConstraints            = CA:FALSE
subjectKeyIdentifier        = hash


[ crl_ext ]
authorityKeyIdentifier      = keyid:always,issuer:always


[ v3_intermediate_ca ]
subjectKeyIdentifier        = hash
authorityKeyIdentifier      = keyid:always,issuer:always
basicConstraints            = critical, CA:true, pathlen:0
keyUsage                    = critical, digitalSignature, cRLSign, keyCertSign
```

```
authorityInfoAccess         = OCSP;URI:http://192.168.56.199:8888
nsCaRevocationUrl           = http://192.168.56.199/sub-ca-certs/carevok.crl


[ server_cert ]
basicConstraints            = CA:FALSE
nsCertType                  = server
nsComment                   = "OpenSSL Generated Server Certificate"
subjectKeyIdentifier        = hash
authorityKeyIdentifier      = keyid,issuer:always
keyUsage                    = critical, digitalSignature, keyEncipherment
extendedKeyUsage            = serverAuth
```

sub-ca.conf file code:

```
#
# OpenSSL configuration file.
#

# Establish working directory.

dir                     = /root/ca/sub-ca

[ ca ]
default_ca              = CA_default

[ CA_default ]
serial                  = $dir/serial
database                = $dir/index.txt
new_certs_dir           = $dir/newcerts
certificate             = $dir/cacert.pem
private_key             = $dir/private/cakey.pem
x509_extensions         = usr_cert
default_days            = 730
default_crl_days        = 30
default_md              = sha256
preserve                = no
email_in_dn             = no
nameopt                 = default_ca
certopt                 = default_ca
policy                  = policy_match

[ policy_match ]
countryName             = match
```

```
stateOrProvinceName         = optional
organizationName            = optional
organizationalUnitName      = optional
commonName                  = supplied
emailAddress                = optional

[ req ]
default_bits                = 4096                # Size of keys
default_keyfile             = key.pem             # name of generated keys
default_md                  = sha256              # message digest algorithm
string_mask                 = nombstr             # permitted characters
distinguished_name          = req_distinguished_name
req_extensions              = v3_req

[ req_distinguished_name ]
# Variable name             Prompt string
#-------------------------   ------------------------------
countryName                 = Country Name (2 letter code)
countryName_min             = 2
countryName_max             = 2
stateOrProvinceName         = State or Province Name (full name)
localityName                = Locality Name (city, district)
0.organizationName          = Organization Name (company)
organizationalUnitName      = Organizational Unit Name (department, division)
commonName                  = Common Name (hostname, IP, or your name)
commonName_max              = 64
emailAddress                = Email Address
emailAddress_max            = 40

# Default values for the above, for consistency and less typing.
# Variable name             Value
#-------------------------   ------------------------------
countryName_default         = BD
stateOrProvinceName_default  = Dhaka
localityName_default        = Rampura
0.organizationName_default   = AcmeCA
organizationalUnitName_default = subadmin
commonName_default                = subCA
emailAddress_default      = subadmin@acmeca.com

[ v3_ca ]
basicConstraints            = critical, CA:TRUE
subjectKeyIdentifier        = hash
authorityKeyIdentifier      = keyid:always,issuer:always
keyUsage                    = critical, digitalSignature, cRLSign, keyCertSign
```

```
[ v3_req ]
basicConstraints          = CA:FALSE
subjectKeyIdentifier       = hash

[ crl_ext ]
authorityKeyIdentifier     = keyid:always,issuer:always

[ v3_OCSP ]
basicConstraints          = CA:FALSE
keyUsage                = nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage          = OCSPSigning

[ usr_cert ]
basicConstraints          = CA:FALSE
subjectKeyIdentifier       = hash
authorityKeyIdentifier     = keyid,issuer:always


[ v3_intermediate_ca ]
subjectKeyIdentifier       = hash
authorityKeyIdentifier     = keyid:always,issuer:always
basicConstraints          = critical, CA:true, pathlen:0
keyUsage                  = critical, digitalSignature, cRLSign, keyCertSign


[ server_cert ]
basicConstraints          = CA:FALSE
nsCertType                = server
nsComment                 = "OpenSSL Generated Server Certificate"
subjectKeyIdentifier      = hash
authorityKeyIdentifier     = keyid,issuer:always
keyUsage                  = critical, digitalSignature, keyEncipherment
extendedKeyUsage          = serverAuth
```