COMP3334 2023/2024 Semester 2 – Lab 2 – Part 2

Generate private key for the CA:

```
$ openssl ecparam -out ca.key -name prime256v1 -genkey
```

Generate a CSR based on this private key, Section 1 and 3 in this course had a requirement on the Subject name for this CA:

```
$ openssl req -new -key ca.key -out ca.csr -config openssl.cnf
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) [HK]:
State or Province Name (full name) [Kowloon]:
Locality Name (eg, city) []:
Organization Name (eg, company) [PolyU]:
Organizational Unit Name (eg, section) [COMP3334]:
Common Name (e.g. server FQDN or YOUR name) []:COMP3334 ROOT
Certificate Authority
Email Address []:
```

Generate a self-signed certificate out of the CSR, this is the CA certificate:

```
$ openssl req -x509 -key ca.key -in ca.csr -out ca.crt -days 365 -
config openssl.cnf
Warning: Not placing -key in cert or request since request is used
Warning: No -copy_extensions given; ignoring any extensions in the
request
```

Parse the CA certificate:

```
$ openssl x509 -in ca.crt -noout -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            1b:fe:e0:b3:06:41:91:d0:99:88:b5:3f:4a:ad:af:87:e0:85:dd:40
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: C=HK, ST=Kowloon, O=PolyU, OU=COMP3334, CN=COMP3334 ROOT
Certificate Authority
        Validity
            Not Before: Apr  2 10:06:29 2024 GMT
            Not After : Apr  2 10:06:29 2025 GMT
        Subject: C=HK, ST=Kowloon, O=PolyU, OU=COMP3334, CN=COMP3334 ROOT
Certificate Authority
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:aa:8c:bb:3a:b1:f2:c0:f1:b9:26:37:00:79:9d:
                    51:62:db:cd:68:f1:6a:09:28:98:ae:b8:53:97:c1:
                    a7:e2:5b:10:38:d4:9f:dd:23:93:64:37:e3:fa:ef:
                    aa:14:12:f8:9f:fd:eb:76:d5:c2:11:ab:62:60:1a:
                    49:73:e2:6e:fd
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                57:7B:0C:00:B9:7D:2D:3A:99:2C:21:E2:8F:E5:25:C5:65:6D:C8:B4
            X509v3 Authority Key Identifier:
                57:7B:0C:00:B9:7D:2D:3A:99:2C:21:E2:8F:E5:25:C5:65:6D:C8:B4
            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: ecdsa-with-SHA256
    Signature Value:
        30:45:02:21:00:fd:6e:bb:c0:b4:a5:b3:90:36:04:b3:71:90:
        84:46:e9:80:e8:54:62:46:65:c6:26:d6:26:2e:1b:57:a7:48:
        1f:02:20:78:4f:82:90:ff:df:75:a7:f7:80:db:72:42:ba:16:
        f6:ee:1c:53:a6:e3:c7:2a:e6:6b:41:d1:d5:4b:55:fa:20
```

Generate private key for the domain certificate:

```
$ openssl ecparam -out domain.key -name prime256v1 -genkey
```

Generate a CSR based on this private key, note that the subject name had to be your studentID.polyu.edu.hk:

```
$ openssl req -new -key domain.key -out domain.csr -config
openssl.cnf
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) [HK]:
State or Province Name (full name) [Kowloon]:
Locality Name (eg, city) []:
Organization Name (eg, company) [PolyU]:
Organizational Unit Name (eg, section) [COMP3334]:
Common Name (e.g. server FQDN or YOUR name)
[]:12345678d.polyu.edu.hk
Email Address []:
```

Generate a certificate for this domain by making the CA sign the CSR:

```
$ openssl x509 -req -in domain.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -out domain.crt -days 365
Certificate request self-signature ok
subject=C=HK, ST=Kowloon, O=PolyU, OU=COMP3334,
CN=12345678d.polyu.edu.hk
```

Parse the resulting domain certificate:

```
$ openssl x509 -in domain.crt -noout -text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            51:36:f4:65:08:9c:ba:3a:c0:3c:a0:e4:f2:29:e8:a8:52:8b:d2:14
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: C=HK, ST=Kowloon, O=PolyU, OU=COMP3334, CN=COMP3334 ROOT
Certificate Authority
        Validity
            Not Before: Apr  2 10:08:09 2024 GMT
            Not After : Apr  2 10:08:09 2025 GMT
        Subject: C=HK, ST=Kowloon, O=PolyU, OU=COMP3334,
CN=12345678d.polyu.edu.hk
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:1b:30:a1:37:3d:3b:bc:90:30:77:8d:48:75:e3:
                    2d:41:42:54:0f:0c:93:83:a8:17:d8:86:8e:18:4a:
                    22:2f:0c:60:78:ca:3b:5d:8e:18:76:d1:9a:38:38:
                    7d:ea:ca:a5:1b:8f:b6:f8:7e:d7:e8:c3:19:23:33:
                    98:64:e8:67:45
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                2A:4A:5D:2A:2D:51:A0:A1:C7:E9:51:A3:15:DA:25:C4:5C:F7:96:CC
            X509v3 Authority Key Identifier:
                57:7B:0C:00:B9:7D:2D:3A:99:2C:21:E2:8F:E5:25:C5:65:6D:C8:B4
    Signature Algorithm: ecdsa-with-SHA256
    Signature Value:
        30:46:02:21:00:a5:fa:d8:6e:23:4e:8d:79:41:ce:b2:7d:22:
        95:83:9d:4e:57:99:d7:63:07:b5:8c:e6:e9:2a:bc:89:9b:d3:
        3e:02:21:00:8a:6f:ad:f5:24:90:85:0d:44:6e:6d:2b:9d:d5:
        29:0a:51:c5:27:e5:19:35:2a:ce:df:0a:e7:ce:5f:39:64:e4
```