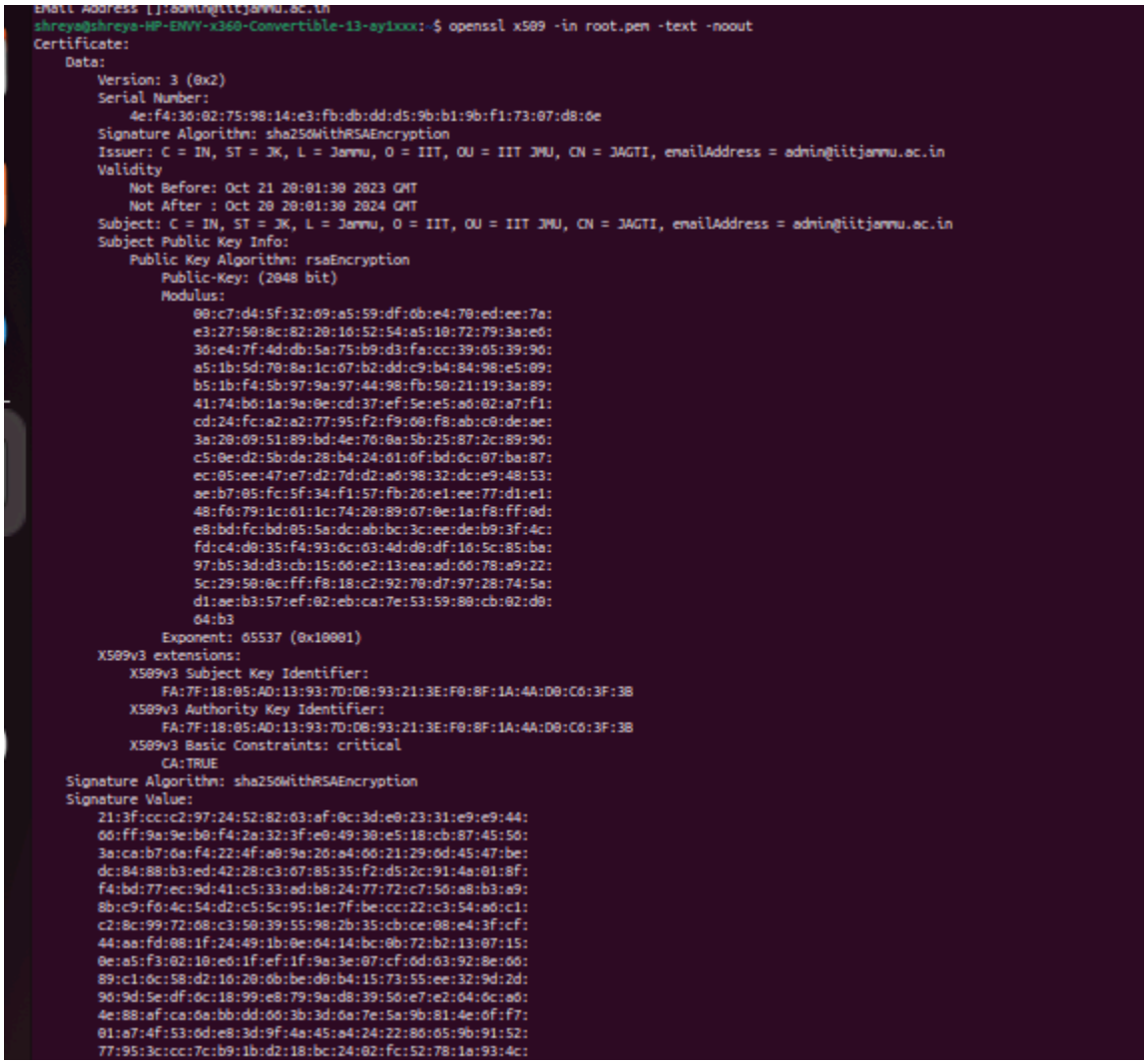
TLS Assignment

1. **Root certificate**

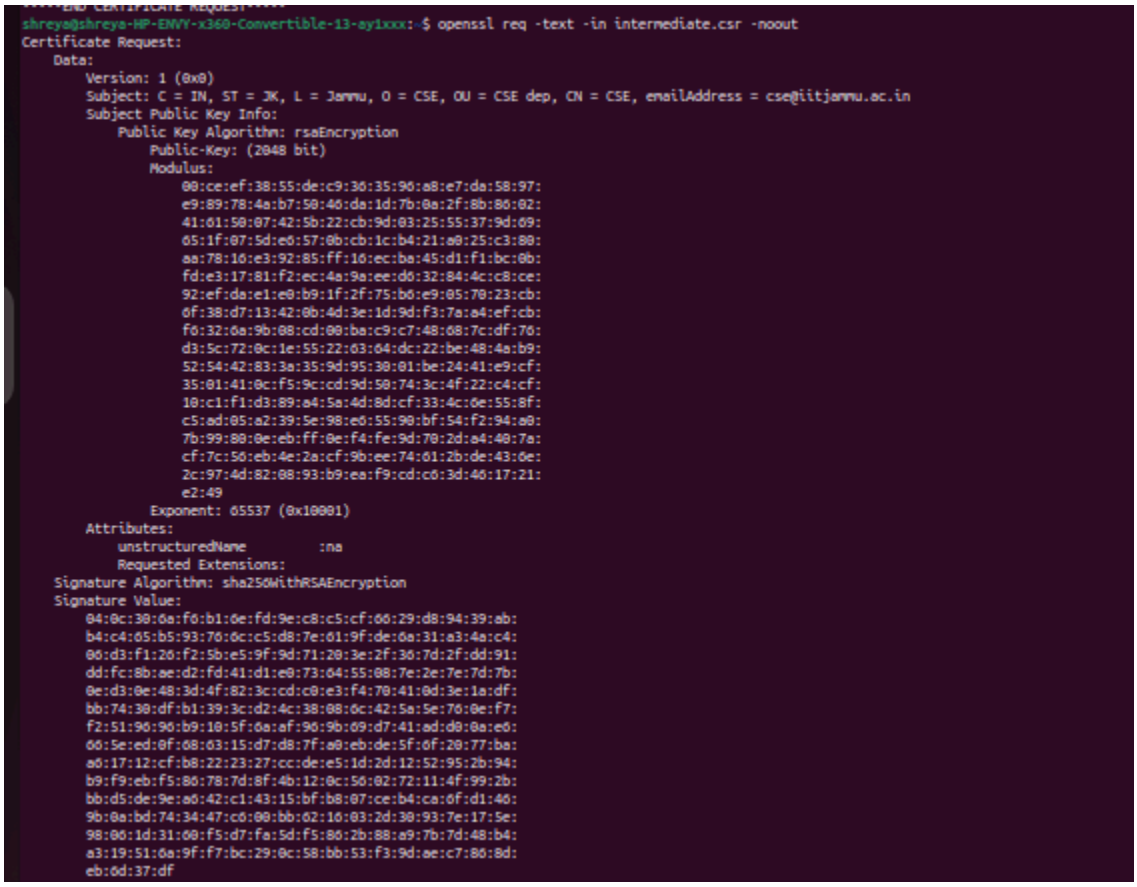
openssl genrsa -out root.key 2048

openssl req -x509 -new -key root.key -days 365 -out root.pem
openssl x509 -in root.pem -text -noout

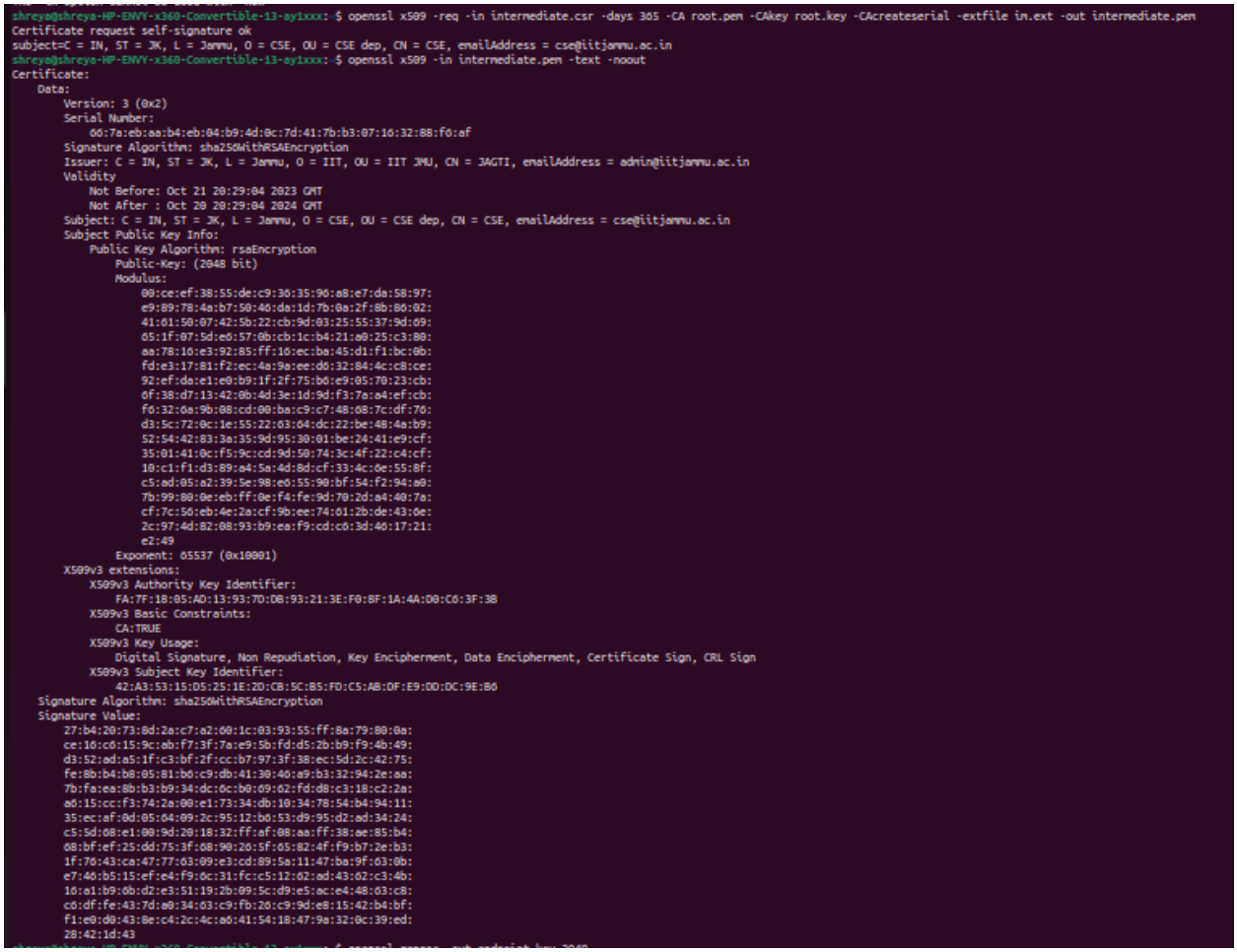


1. Intermediate certificate
   openssl genrsa -out intermediate.key 2048

openssl req -new -key intermediate.key -out intermediate.csr -nodes
openssl req -text -in intermediate.csr -noout

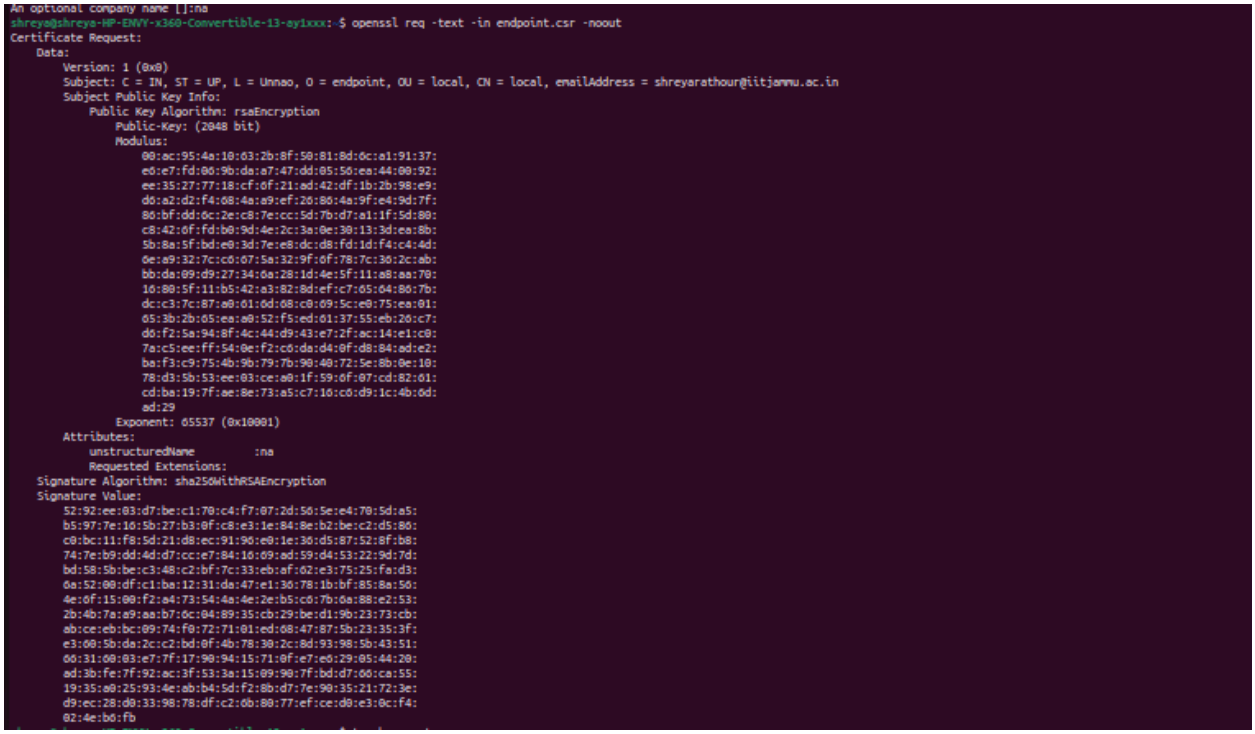


touch im.ext
openssl x509 -req -in intermediate.csr -days 365 -CA root.pem -CAkey root.key -CAcreateserial -extfile im.ext -out intermediate.pem
openssl x509 -in intermediate.pem -text -noout



2. EndPoint Certificate

   openssl genrsa -out endpoint.key 2048
   openssl req -new -key endpoint.key -out endpoint.csr -nodes
   openssl req -text -in endpoint.csr -noout



touch ep.ext
openssl x509 -req -in endpoint.csr -CA intermediate.pem -CAkey intermediate.key -days 365 -extfile ep.ext -out endpoint.pem
openssl x509 -in endpoint.pem -text -noout

```
shreya@shreya-HP-ENVY-x360-Convertible-13-ay1xxx:~$ openssl x509 -req -in endpoint.csr -CA intermediate.pem -CAkey intermediate.key -days 365 -extfile ep.ext -out endpoint.pem
Certificate request self-signature ok
subject=C = IN, ST = UP, L = Unnao, O = endpoint, OU = local, CN = local, emailAddress = shreyarathour@iitjammu.ac.in
shreya@shreya-HP-ENVY-x360-Convertible-13-ay1xxx:~$ openssl x509 -in endpoint.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            22:dc:27:c6:09:b6:cc:52:23:19:35:a5:1d:6e:0f:a7:dc:70:40:f4
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = IN, ST = JK, L = Jammu, O = CSE, OU = CSE dep, CN = CSE, emailAddress = cse@iitjammu.ac.in
        Validity
            Not Before: Oct 21 20:44:33 2023 GMT
            Not After : Oct 20 20:44:33 2024 GMT
        Subject: C = IN, ST = UP, L = Unnao, O = endpoint, OU = local, CN = local, emailAddress = shreyarathour@iitjammu.ac.in
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:ac:95:4a:10:63:2b:8f:50:81:8d:6c:a1:91:37:
                    e6:e7:fd:06:9b:da:a7:47:dd:05:50:ea:44:00:92:
                    ee:35:27:77:18:cf:0f:21:ad:42:df:1b:2b:98:e9:
                    d6:a2:d2:f4:68:4a:a9:ef:26:86:4a:9f:e4:9d:7f:
                    86:bf:dd:6c:2e:c8:7e:cc:5d:7b:d7:a1:1f:5d:80:
                    c8:42:0f:fd:b0:9d:4e:2c:3a:0e:30:13:3d:ea:8b:
                    5b:8a:5f:bd:e0:3d:7e:e8:dc:d8:fd:1d:f4:c4:4d:
                    0e:a9:32:7c:c6:07:5a:32:9f:0f:78:7c:36:2c:ab:
                    bb:da:09:d9:27:34:6a:28:1d:4e:5f:11:a8:aa:70:
                    10:80:5f:11:b5:42:a3:82:8d:ef:c7:65:64:86:7b:
                    dc:c3:7c:87:a0:61:0d:68:c0:09:5c:e0:75:ea:01:
                    65:3b:2b:65:ea:a0:52:f5:ed:61:37:55:eb:26:c7:
                    d6:f2:5a:94:8f:4c:44:d9:43:e7:2f:ac:14:e1:c0:
                    7a:c5:ee:ff:54:0e:f2:c6:da:d4:0f:d8:84:ad:e2:
                    ba:f3:c9:75:4b:9b:79:7b:90:40:72:5e:8b:0e:10:
                    78:d3:5b:53:ee:03:ce:a0:1f:59:0f:07:cd:82:61:
                    cd:ba:19:7f:ae:8e:73:a5:c7:16:c6:d9:1c:4b:6d:
                    ad:29
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                42:A3:53:15:D5:25:1E:2D:CB:5C:B5:FD:C5:AB:DF:E9:DD:DC:9E:B6
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment
            X509v3 Subject Alternative Name:
                DNS:localhost, IP Address:127.0.0.1
            X509v3 Subject Key Identifier:
                3A:B8:7D:49:4F:AC:5B:4B:F5:16:4F:BA:B5:44:C9:A9:DD:78:0C:AD
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        4b:a2:b0:05:16:47:e1:e7:6f:f7:0b:a6:bb:31:bc:95:c7:f7:
        4b:5b:5a:52:01:e8:8d:b8:96:e5:0d:1a:1c:62:65:c1:e6:50:
        4c:02:bc:05:45:37:6b:05:27:a2:cd:39:c8:bd:03:d2:a3:77:
        6a:8f:15:78:1c:07:ac:dc:f0:44:5d:55:58:58:df:f2:f3:4f:
        9c:bd:5b:f4:79:94:b4:9e:16:48:f4:48:73:2f:5f:6e:d7:32:
        23:4c:1a:43:bd:d9:2b:e7:50:b5:e6:1c:eb:02:f3:c3:b2:62:
        b2:d2:c0:0b:bc:37:4e:76:64:bb:1d:f0:c6:3e:00:49:4a:a2:
        ee:e7:0e:4f:d9:be:c6:fc:23:de:ad:30:fc:86:94:b3:a7:ba:
        b9:99:7b:72:71:f8:40:d1:a9:00:6e:9f:5e:11:b7:39:55:bf:
        fa:1d:12:0f:f3:87:09:00:7e:36:99:b7:72:d5:af:1f:1c:f4:
        dd:65:fc:3c:78:ce:b8:4d:f1:1e:ac:ee:85:e6:1d:56:90:c9:
        ba:69:c6:48:d8:fa:e2:cf:e4:38:86:38:19:f1:bd:9d:28:4e:
        63:38:be:82:81:c3:f2:3d:38:df:49:d9:65:92:3d:17:49:b9:
        e5:82:e7:10:06:7a:63:93:2e:03:1c:aa:d3:76:28:19:2f:c3:
        a3:97:b9:de
```

cat endpoint.pem intermediate.pem root.pem>chain.pem
openssl verify -show_chain -CAfile chain.pem endpoint.pem

```
shreya@shreya-HP-ENVY-x360-Convertible-13-ay1xxx:~$ cat endpoint.pem intermediate.pem root.pem>chain.pem
shreya@shreya-HP-ENVY-x360-Convertible-13-ay1xxx:~$ openssl verify -show_chain -CAfile chain.pem endpoint.pem
endpoint.pem: OK
Chain:
depth=0: C = IN, ST = UP, L = Unnao, O = endpoint, OU = local, CN = local, emailAddress = shreyarathour@iitjammu.ac.in (untrusted)
depth=1: C = IN, ST = JK, L = Jammu, O = CSE, OU = CSE dep, CN = CSE, emailAddress = cse@iitjammu.ac.in
depth=2: C = IN, ST = JK, L = Jammu, O = IIT, OU = IIT JMU, CN = JAGTI, emailAddress = admin@iitjammu.ac.in
```