

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

```
-----
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            4e:f4:30:02:75:98:14:e3:fb:db:dd:d5:9b:b1:9b:f1:73:07:d8:0e
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = IN, ST = JK, L = Jammu, O = IIT JMU, OU = IIT JMU, CN = JAGTI, emailAddress = admin@iitjammu.ac.in
        Validity
            Not Before: Oct 21 20:01:30 2023 GMT
            Not After : Oct 20 20:01:30 2024 GMT
        Subject: C = IN, ST = JK, L = Jammu, O = IIT, OU = IIT JMU, CN = JAGTI, emailAddress = admin@iitjammu.ac.in
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
            Modulus:
                00:c7:d4:5f:32:09:a5:59:df:0b:e4:70:ed:ee:7a:
                e3:27:50:8c:82:20:10:52:54:a5:10:72:79:3a:e0:
                30:e4:7f:4d:db:5a:75:b9:d3:fa:cc:39:05:39:90:
                a5:1b:5d:70:8a:1c:07:b2:dd:c9:b4:84:98:e5:09:
                b5:1b:f4:5b:97:9a:97:44:98:fb:50:21:19:3a:89:
                41:74:b0:1a:9a:0e:cd:37:ef:5e:e5:a0:02:a7:f1:
                cd:24:fc:a2:a2:77:95:f2:f9:00:f8:ab:c0:de:ae:
                3a:20:09:51:89:bd:4e:70:0a:5b:25:87:2c:89:90:
                c5:0e:d2:5b:da:28:b4:24:01:0f:bd:0c:07:ba:87:
                ec:05:ee:47:e7:d2:7d:d2:a0:98:32:dce9:48:53:
                ae:b7:05:fc:5f:34:f1:57:fb:20:e1:ee:77:d1:e1:
                48:f0:79:1c:01:1c:74:20:89:07:0e:1a:f8:ff:0d:
                e8:bd:fc:bd:05:5a:dc:ab:bc:3c:ee:de:b9:3f:4c:
                fd:c4:d0:35:f4:93:dc:03:4d:d0:df:10:5c:85:ba:
                97:b5:3d:d3:cb:15:00:e2:13:ee:ad:00:78:a9:22:
                5c:29:50:0c:ff:f8:18:c2:92:70:d7:97:28:74:5a:
                d1:ae:b3:57:ef:02:eb:ca:7e:53:59:80:cb:02:d0:
                04:b3
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                FA:7F:18:05:AD:13:93:70:D0:93:21:3E:F0:8F:1A:4A:D0:C0:3F:3B
            X509v3 Authority Key Identifier:
                FA:7F:18:05:AD:13:93:70:D0:93:21:3E:F0:8F:1A:4A:D0:C0:3F:3B
            X509v3 Basic Constraints: critical
                CA:TRUE
        Signature Algorithm: sha256WithRSAEncryption
        Signature Value:
            21:3f:cc:c2:97:24:52:02:03:af:0c:3d:e0:23:31:e9:e9:44:
            00:ff:9a:9e:b0:f4:2a:32:3f:e0:49:30:e5:18:cb:87:45:50:
            3a:ca:b7:0a:f4:22:4f:a0:9a:20:a4:00:21:29:0d:45:47:be:
            dc:84:88:b3:ed:42:28:c3:07:85:35:f2:d5:2c:91:4a:01:8f:
            f4:bd:77:ec:9d:41:c5:33:ad:b8:24:77:72:c7:50:a8:b3:a9:
            8b:c9:f0:4c:54:d2:c5:5c:95:1e:7f:be:cc:22:c3:54:a0:c1:
            c2:8c:99:72:08:c3:50:39:55:98:2b:35:cb:ce:08:e4:3f:cf:
            44:aa:fd:08:1f:24:49:1b:0e:04:14:bc:0b:72:b2:13:07:15:
            0e:a5:f3:02:10:e0:1f:ef:1f:9a:3e:07:cf:0d:03:92:8e:00:
            89:c1:0c:58:d2:10:20:0b:be:d0:b4:15:73:55:ee:32:9d:2d:
            90:9d:5e:df:0c:18:99:e8:79:9a:d8:39:50:e7:e2:04:0c:a0:
            4e:88:af:ca:0a:bb:dd:00:3b:3d:0a:7e:5a:9b:81:4e:0f:f7:
            01:a7:4f:53:0d:e8:3d:9f:4a:45:a4:24:22:80:05:9b:91:52:
            77:95:3c:cc:7c:b9:1b:d2:18:bc:24:02:fc:52:78:1a:93:4c:
-----
```

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
```

```
shreya@shreya-HP-ENVY-x360-Convertible-13-ay1xxx: $ openssl req -text -in intermediate.csr -noout
Certificate Request:
Data:
  Version: 1 (0x0)
  Subject: C = IN, ST = JK, L = Jammu, O = CSE, OU = CSE dep, CN = CSE, emailAddress = cse@iitjammu.ac.in
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
    Modulus:
      00:ce:ef:38:55:de:c9:36:35:96:a8:e7:da:58:97:
      e9:89:78:4a:b7:50:46:da:1d:7b:0a:2f:8b:86:02:
      41:01:50:07:42:5b:22:cb:9d:03:25:55:37:9d:09:
      65:1f:07:5d:e0:57:0b:cb:1c:b4:21:a0:25:c3:80:
      aa:78:16:e3:92:85:ff:16:ec:ba:45:d1:f1:bc:0b:
      fd:e3:17:81:f2:ec:4a:9a:ee:d0:32:84:4c:c8:ce:
      92:ef:da:e1:e0:b9:1f:2f:75:b6:e9:05:70:23:cb:
      0f:38:d7:13:42:0b:4d:3e:1d:9d:f3:7a:a4:ef:cb:
      f6:32:6a:9b:08:cd:00:ba:c9:c7:48:08:7c:df:76:
      d3:5c:72:0c:1e:55:22:63:04:dc:22:be:48:4a:b9:
      52:54:42:83:3a:35:9d:95:30:01:be:24:41:e9:cf:
      35:01:41:0c:f5:9c:cd:9d:50:74:3c:4f:22:c4:cf:
      10:c1:f1:d3:89:a4:5a:4d:8d:cf:33:4c:0e:55:8f:
      c5:ad:05:a2:39:5e:98:ed:55:90:bf:54:f2:94:a0:
      7b:99:80:0e:eb:ff:0e:f4:fe:9d:70:2d:a4:40:7a:
      cf:7c:56:eb:4e:2a:cf:9b:ee:74:61:2b:de:43:0e:
      2c:97:4d:82:08:93:b9:ea:f9:cd:c6:3d:46:17:21:
      e2:49
    Exponent: 65537 (0x10001)
  Attributes:
    unstructuredName :na
    Requested Extensions:
  Signature Algorithm: sha256WithRSAEncryption
  Signature Value:
    04:0c:30:6a:f0:b1:0e:fd:9e:c8:c5:cf:66:29:d8:94:39:ab:
    b4:c4:65:b5:93:76:6c:c5:d8:7e:61:9f:de:6a:31:a3:4a:c4:
    00:d3:f1:26:f2:5b:e5:9f:9d:71:20:3e:2f:36:7d:2f:dd:91:
    dd:fc:8b:ae:d2:fd:41:d1:e0:73:04:55:08:7e:2e:7e:7d:7b:
    0e:d3:0e:48:3d:4f:82:3c:cd:c8:e3:f4:70:41:0d:3e:1a:df:
    bb:74:30:df:b1:39:3c:d2:4c:38:08:6c:42:5a:5e:76:0e:f7:
    f2:51:90:90:b9:10:5f:6a:af:90:9b:09:d7:41:ad:d0:0a:e0:
    60:5e:ed:0f:08:03:15:d7:d8:7f:a0:eb:de:5f:0f:20:77:ba:
    a0:17:12:cf:b8:22:23:27:cc:de:e5:1d:2d:12:52:95:2b:94:
    b9:f9:eb:f5:86:78:7d:8f:4b:12:0c:56:02:72:11:4f:99:2b:
    bb:d5:de:9e:a0:42:c1:43:15:bf:b8:07:ce:b4:ca:0f:d1:46:
    9b:0a:bd:74:34:47:c0:00:bb:62:16:03:2d:30:93:7e:17:5e:
    98:00:1d:31:00:f5:d7:fa:5d:f5:86:2b:88:a9:7b:7d:48:b4:
    a3:19:51:6a:9f:f7:bc:29:0c:58:bb:53:f3:9d:ae:c7:86:0d:
    eb:0d:37:df
```

```
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
```

```

shreya@shreya-HP-ENVY-x360-Convertible-13-ay1xxx: $ openssl x509 -req -in intermediate.csr -days 365 -CA root.pem -CAkey root.key -CAcreateserial -extfile in.ext -out intermediate.pem
Certificate request self-signature ok
subject=C = IN, ST = JK, L = Jammu, O = CSE, OU = CSE dep, CN = CSE, emailAddress = cse@iitjammu.ac.in
shreya@shreya-HP-ENVY-x360-Convertible-13-ay1xxx: $ openssl x509 -in intermediate.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0d:7a:eb:aa:b4:eb:04:b9:4d:0c:7d:41:7b:b3:07:10:32:88:f0:af
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = IN, ST = JK, L = Jammu, O = IIT, OU = IIT JMU, CN = JAGTI, emailAddress = admin@iitjammu.ac.in
        Validity
            Not Before: Oct 21 20:29:04 2023 GMT
            Not After: Oct 20 20:29:04 2024 GMT
        Subject: C = IN, ST = JK, L = Jammu, O = CSE, OU = CSE dep, CN = CSE, emailAddress = cse@iitjammu.ac.in
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
            Modulus:
                00:ce:ef:38:55:de:c9:30:35:90:a8:e7:da:58:97:
                e9:89:78:4a:b7:50:40:da:1d:7b:0a:2f:8b:80:02:
                41:01:50:07:42:5b:22:cb:9d:03:25:55:37:9d:09:
                05:1f:07:5d:e0:57:0b:cb:1c:b4:21:a0:25:c3:80:
                aa:78:10:e3:92:85:ff:10:ec:ba:45:d1:f1:bc:0b:
                fd:e3:17:81:f2:ec:4a:9a:ee:d0:32:84:4c:c8:ce:
                92:ef:da:e1:e0:b9:1f:2f:75:b0:ep:05:70:72:cb:
                0f:38:df:13:42:00:4d:3e:1d:9d:f3:7a:e4:ef:cb:
                f6:32:0a:9b:08:cd:00:bac:9c:7:48:00:7c:df:70:
                d3:5c:72:0c:1e:55:22:03:04:dc:22:be:48:4a:b9:
                52:54:42:83:3a:35:9d:95:30:01:be:24:41:e9:cf:
                35:01:41:0c:f5:9c:cd:9d:50:74:3c:4f:22:c4:cf:
                10:c1:f1:d3:89:a4:5a:4d:8d:cf:33:4c:0e:55:8f:
                c5:ad:05:a2:39:5e:98:e0:55:90:bf:54:f2:94:a0:
                7b:99:80:0e:eb:ff:0e:f4:fe:9d:70:2d:a4:40:7a:
                cf:7c:50:eb:4e:2a:cf:9b:ee:74:01:2b:de:43:0e:
                2c:97:4d:82:08:93:b9:ea:f9:cd:c0:3d:40:17:21:
                e2:49
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                FA:7F:18:05:AD:13:93:70:0B:93:21:3E:F0:8F:1A:4A:D0:C0:3F:3B
            X509v3 Basic Constraints:
                CA:TRUE
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                42:A3:53:15:05:25:1E:20:CB:5C:85:F0:C5:AB:DF:E9:DD:DC:9E:80
        Signature Algorithm: sha256WithRSAEncryption
        Signature Value:
            27:b4:20:73:8d:2a:c7:a2:00:1c:03:93:55:ff:8a:79:80:0a:
            ce:10:c0:15:9c:0b:f7:3f:7a:e9:5b:fd:d5:2b:b9:f9:4b:49:
            d3:52:ad:a5:1f:c3:bf:2f:cc:b7:97:3f:38:ec:5d:2c:42:75:
            fe:0b:b4:80:05:81:b0:c9:d0:41:30:40:a9:b3:32:94:2e:aa:
            7b:fa:ea:0b:b3:b9:34:dc:0c:b0:69:02:fd:d8:c3:18:c2:2a:
            e0:15:cc:f3:74:2a:00:e1:73:34:db:10:34:78:54:b4:94:11:
            35:ec:ef:0d:05:04:09:2c:95:12:bd:53:d9:95:d2:ad:34:24:
            c5:5d:08:e1:00:9d:20:18:32:ff:af:88:aa:ff:38:ae:85:b4:
            08:bf:ef:25:dd:75:3f:08:90:26:5f:05:82:4f:f9:b7:2e:b3:
            1f:70:43:ca:47:77:03:09:e3:cd:89:5a:11:47:ba:9f:03:0b:
            e7:40:b5:15:ef:e4:f9:0c:31:fc:c5:12:02:ad:43:02:c3:4b:
            10:a1:b9:0b:d2:e3:51:19:2b:09:5c:d9:e5:ac:e4:48:03:c8:
            c0:df:fe:43:7d:a0:34:03:c9:f0:20:c9:9d:e8:15:42:b4:bf:
            f1:e0:d0:43:8e:c4:2c:4c:a0:41:54:18:47:9a:32:0c:39:ed:
            28:42:1d:43

```

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

```

An optional company name []:na
shreyas@shreya-HP-ENVY-x360-Convertible-13-ay1xxx: $ openssl req -text -in endpoint.csr -noout
Certificate Request:
Data:
  Version: 1 (0x0)
  Subject: C = IN, ST = UP, L = Unnao, O = endpoint, OU = local, CN = local, emailAddress = shreyathour@iitjammu.ac.in
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
    Modulus:
      00:ac:95:4a:10:03:2b:8f:50:81:8d:0c:a1:91:37:
      e0:e7:fd:00:9b: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:
      d0:a2:d2:f4:08:4a:a9:ef:20:80:4a:9f:e4:9d:7f:
      80:bf:dd:0c: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:c0:07:5a:32:9f:0f:78:7c:30:2c:ab:
      bb:da:09:d9:27:34:0a:20:1d:4e:5f:11:a8:aa:70:
      10:00:5f:11:b5:42:a3:80:bd:ef:c7:d5:04:80:7b:
      dc:c3:7c:87:a0:01:0d:08:c0:09:5c:e0:75:ee:01:
      05:3b:2b:d5:ea:a0:52:f5:ed:01:37:55:eb:20:c7:
      d0:f2:5a:94:8f:4c:44:d9:43:e7:2f:ac:14:e1:c8:
      7a:c5:ee:ff:54:0e:f2:c0: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:82:01:
      cd:ba:19:7f:ae:8e:73:a5:c7:10:cd:d9:1c:4b:0d:
      ad:29
    Exponent: 65537 (0x10001)
  Attributes:
    unstructuredName: na
  Requested Extensions:
  Signature Algorithm: sha256WithRSAEncryption
  Signature Value:
    52:92:ee:03:d7:b6:c1:70:c4:f7:07:2d:50:5e:e4:70:5d:a5:
    b5:97:7e:10:5b:27:b3:0f:c8:e3:1e:84:8e:b2:b6:c2:d5:80:
    c9:bc:11:f8:5d:21:d8:ec:91:90:e0:1e:30:d5:07:52:8f:b8:
    74:7e:b9:dd:4d:d7:cc:e7:84:10:09:ad:59:d4:53:22:9d:7d:
    bd:58:5b:b6:c3:48:c2:bf:7c:33:eb:af:02:e3:75:25:fad3:
    0a:52:00:df:c1:ba:12:31:da:47:e1:30:78:1b:bf:85:8a:50:
    4e:0f:15:00:f2:a4:73:54:4a:4e:2e:b5:c0:7b:0a:88:e2:53:
    2b:4b:7a:a9:aa:b7:0c:04:89:35:cb:29:be:d1:90:23:73:cb:
    ab:ce:eb:bc:09:74:f9:72:71:01:ed:08:47:87:5b:23:35:3f:
    e3:00:5b:da:2c:c2:bd:0f:4b:78:30:2c:8d:93:98:5b:43:51:
    00:31:00:03:e7:7f:17:90:94:15:71:0f:e7:e0:29:05:44:20:
    ad:3b:fe:7f:02:ac:3f:53:3a:15:09:90:7f:bd:d7:00:ca:55:
    19:35:e0:25:03:4e:eb:b4:5d:f2:8b:df:7e:90:35:21:72:3e:
    d9:ec:28:d0:33:98:7b:df:c2:0b:80:77:ef:ce:d0:e3:6c:f4:
    02:4e:b6:fb

```

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 305 -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:c0:09:b0:cc:52:23:19:35:a5:1d:0e:0f:a7:dc:70:40:f4
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = IN, ST = JK, L = Jammu, O = 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:10:03:2b:8f:50:81:8d:0c:a1:91:37:
                e0:e7:fd:00:90: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:
                d0:a2:d2:f4:08:4a:a9:ef:26:80:4a:9f:e4:9d:7f:
                80:bf:dd:0c: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:c0:07:5a:32:9f:0f:78:7c:36:2c:ab:
                bb:de:09:d9:27:34:0a:28:1d:4e:5f:11:a8:aa:70:
                10:80:5f:11:b5:42:a3:82:8d:ef:c7:05:04:86:7b:
                dc:c3:7c:87:a0:01:0d:08:c0:09:5c:e0:75:ea:01:
                05:3b:2b:05:ea:a0:52:f5:ed:01:37:55:eb:20:c7:
                d0:f2:5a:94:8f:4c:44:d9:43:e7:2f:ac:14:e1:c0:
                7a:c5:ee:ff:54:0e:f2:c0: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:82:01:
                cd:ba:19:7f:ae:8e:73:a5:c7:16:c0: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:0F:E9:DD:DC:9E:B0
            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:F5:10:4F:BA:B5:44:C9:A9:DD:78:0C:AD
        Signature Algorithm: sha256WithRSAEncryption
        Signature Value:
            4b:a2:b0:05:10:47:e1:e7:0f:f7:0b:a0:bb:31:bc:95:c7:f7:
            4b:5b:5a:52:01:e8:8d:b8:90:e5:0d:1a:1c:02:05:c1:e0:50:
            4c:02:bc:05:45:37:0b:05:27:a2:cd:39:c8:bd:03:d2:a3:77:
            0a:8f:15:78:1c:07:ac:dc:f6:44:5d:55:58:58:df:f2:f3:4f:
            9c:bd:5b:f4:79:94:b4:9e:10:48:f4:48:73:2f:5e:0e:d7:32:
            23:4c:1a:43:bd:d9:2b:e7:50:b5:e0:1c:eb:02:f3:c3:b2:02:
            b2:d2:c9:0b:bc:37:4e:70:04:bb:1d:f0:c0:3e:00:49:4a:a2:
            ee:e7:0e:4f:d9:be:c0:fc:23:de:ad:30:fc:80:94:b3:a7:ba:
            b9:99:7b:72:71:f8:40:d1:a9:00:0e:9f:5e:11:b7:39:55:bf:
            fa:1d:12:0f:f3:87:09:00:7e:30:99:b7:72:d5:af:1f:1c:f4:
            dd:05:fc:3c:78:ce:b8:4d:f1:1e:ac:ee:85:e0:1d:50:90:c9:
            ba:09:cd:48:d8:fa:e2:cf:ed:38:80:38:19:f1:bd:9d:28:4e:
            03:38:be:82:01:c3:f2:3d:38:df:49:d9:05:92:3d:17:49:b9:
            e5:82:e7:10:00:7a:03:93:2e:03:1c:aa:d3:70:28:19:2f:c3:
            a3:97:b9:6e

```

```

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 JMU, CN = JAGTI, emailAddress = admin@iitjammu.ac.in

```

