```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            24:4a:09:ca:f7:22:8b:ed:a1:fc:76:22:49:a3:0e:b1:34:1f:08:ba
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = PK, ST = Islamabad, L = Islamabad, O = SecureChat CA, CN = SecureChat
Root CA
        Validity
            Not Before: Nov 16 19:16:33 2025 GMT
            Not After : Nov 14 19:16:33 2035 GMT
        Subject: C = PK, ST = Islamabad, L = Islamabad, O = SecureChat CA, CN =
SecureChat Root CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:d9:f1:55:b8:3a:df:c0:a5:83:e2:63:42:03:5c:
                    e0:c4:d0:da:d4:5f:e4:70:24:36:11:25:ee:31:19:
                    90:11:d7:31:8e:f7:72:96:6c:ec:dd:53:ee:b6:fe:
                    cf:74:9c:d7:aa:60:32:78:88:34:75:a2:c4:da:be:
                    f9:ea:19:24:cf:22:23:22:42:20:d4:a7:e8:cf:91:
                    e8:8f:63:27:2b:cb:f2:3a:1c:a7:22:93:68:76:4f:
                    23:7d:f1:d0:69:eb:93:a4:0d:9b:ab:4d:f9:f3:af:
                    85:2f:3b:f8:76:b9:b9:bb:28:92:96:a5:8a:76:24:
                    2b:47:f5:fe:c2:6a:67:26:69:d9:70:d2:b4:ac:80:
                    ed:15:3c:a8:46:ea:84:d8:be:57:c5:16:9e:15:d7:
                    09:9b:66:e6:33:92:17:cb:6a:5a:16:99:d0:5a:45:
                    09:24:c0:a0:d1:de:e0:8f:8b:93:fe:51:25:b1:8f:
                    d1:a2:af:55:86:41:55:b9:15:b1:bb:27:a3:6c:d9:
                    7e:f9:ea:8f:27:f6:14:2e:98:79:ca:ec:08:72:15:
                    80:41:02:1c:68:3e:e2:81:5b:c0:c9:fb:25:95:d7:
                    00:90:2f:56:39:63:3e:82:ab:1b:6b:f1:1a:60:7b:
                    df:3a:51:ba:6c:49:6b:8c:af:46:fc:81:15:50:b1:
                    8f:d3
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        8f:b9:bc:32:10:f7:ec:57:ff:f0:59:ee:cc:40:1a:b0:6e:7a:
        b2:26:92:f8:95:93:52:1f:89:cb:b4:a3:a9:e7:9a:19:0e:ea:
        39:0c:83:0c:15:97:1b:7b:25:1a:e5:a1:e3:16:c7:b6:c5:7d:
        97:5e:17:97:b5:2f:52:93:ca:4e:38:77:7e:0e:eb:5a:95:73:
        18:78:c8:5a:3e:7c:49:35:de:e1:53:f1:c7:ef:e2:38:ae:29:
        8d:3e:6f:19:1b:58:56:27:55:38:5b:7d:51:81:cf:e2:4c:17:
        36:f9:24:c4:c4:f5:ca:73:75:95:f8:fa:40:6e:51:81:b5:56:
```

e6:c0:90:0d:4b:b1:6b:45:fe:14:fb:f7:e7:3a:aa:65:fa:15:
d5:97:9f:37:5f:95:a3:e5:9d:77:04:4d:11:f6:de:15:ab:ed:
b0:29:44:90:d2:6a:d7:68:ca:17:32:44:f8:54:24:5a:2f:c1:
a8:27:02:9e:a7:17:b2:dc:12:11:c2:b7:67:8c:1c:f7:af:21:
7e:a3:c7:3f:a1:6b:32:5e:a7:4c:9b:63:aa:10:ce:10:d2:3c:
b4:80:d8:18:cd:1a:4f:99:05:38:ac:d5:aa:a6:10:8e:5d:4a:
75:fb:3d:bb:f7:b9:1f:48:da:90:df:ef:37:b6:e2:cb:ee:33:
84:75:a9:68

Client cert text:

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
6d:48:13:1d:1b:01:14:02:c7:74:cf:06:ae:db:6a:90:31:0e:03:73
Signature Algorithm: sha256WithRSAEncryption
Issuer: C = PK, ST = Islamabad, L = Islamabad, O = SecureChat CA, CN = SecureChat Root CA
Validity
Not Before: Nov 16 19:17:47 2025 GMT
Not After : Nov 16 19:17:47 2026 GMT
Subject: C = PK, ST = Islamabad, O = SecureChat Entity, CN = client
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:a4:9e:d9:a2:2a:ec:5e:36:ff:c5:68:f0:b1:36:
aa:76:93:9d:cd:46:5e:15:b3:b2:a4:19:90:f2:16:
f9:cc:2e:9b:97:1f:e4:38:44:8d:f4:6d:30:fe:72:
d4:f1:81:2e:c2:ac:76:a1:e9:64:1c:04:66:48:98:
a7:30:af:f2:e1:4e:ef:1e:2a:7c:b7:27:7f:9e:71:
25:45:f5:a4:da:b4:da:a9:7b:1c:c9:aa:33:26:1d:
eb:89:02:f9:0b:f9:f6:8f:f6:e2:e7:30:67:ec:48:
d6:98:d4:8f:66:2c:e1:99:2f:61:21:78:54:cf:b4:
c7:02:9a:51:90:ec:1c:4b:8f:5f:32:f4:06:93:4f:
c4:67:95:c7:72:aa:07:fc:68:c0:29:2b:5b:7e:e8:
bf:fd:fd:34:a2:c0:50:b7:49:fb:77:0f:6b:f4:4d:
58:6c:b6:4b:dd:30:fb:95:c8:47:58:e6:8d:aa:ee:
82:47:d9:18:cd:24:43:2d:57:37:8e:0d:27:eb:68:
91:cd:47:7e:84:2b:b9:7e:67:82:0f:0c:e9:8b:51:
11:ed:65:d5:70:0d:d8:a5:76:de:f1:53:6c:57:97:
eb:b3:90:b1:42:f7:57:fb:59:c1:59:0d:4b:c9:18:
71:8a:fd:74:aa:d8:84:87:cf:8d:db:62:94:5b:35:
dc:a1
Exponent: 65537 (0x10001)
Signature Algorithm: sha256WithRSAEncryption

```
    Signature Value:
        6d:a7:c2:dd:f1:a9:e5:e0:e3:fe:ea:ad:36:00:bf:80:f9:c2:
        1d:fc:c8:18:aa:68:c1:cf:78:af:81:e3:93:e9:4c:90:71:38:
        c8:cd:7d:98:a7:23:5e:bd:1d:32:d1:e6:9d:42:1a:63:98:92:
        4e:cf:2c:10:ae:e7:85:ac:11:2b:b0:ae:5b:55:9f:25:af:02:
        82:2c:29:f4:5a:ca:56:80:d8:70:3c:78:71:e6:02:1c:2a:43:
        d8:f6:29:f2:5a:5a:2a:77:6e:bd:57:23:6f:aa:cc:ae:1e:9d:
        03:86:a7:2b:6c:17:77:91:07:3e:99:78:c2:cc:45:1a:02:d7:
        c8:cf:3c:90:c8:91:e6:59:1b:b2:db:b4:9e:cc:04:e6:05:ec:
        4a:af:4c:9f:39:e2:06:a4:57:9f:8a:79:ae:89:f7:2b:aa:39:
        3b:6f:14:35:f9:19:01:00:ae:46:56:3e:cd:e3:5d:41:9a:98:
        f2:bb:ee:ef:29:ae:e6:72:e7:0c:81:9c:e5:2a:9b:e4:fe:b3:
        e3:e8:84:b8:3a:c8:11:c1:0e:c1:d0:16:23:21:ae:17:60:12:
        9b:a4:21:68:14:f4:c0:d2:f6:ab:23:ab:e7:74:2c:5f:94:58:
        cb:70:8b:9d:e1:05:fb:eb:3f:9c:62:ea:6c:72:8f:df:1e:6d:
        01:91:f6:39


Server cert text:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            01:d1:9a:49:75:b2:e6:c2:bc:f4:d1:88:db:4f:53:d5:86:b4:70:b5
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = PK, ST = Islamabad, L = Islamabad, O = SecureChat CA, CN = SecureChat
Root CA
        Validity
            Not Before: Nov 16 19:17:47 2025 GMT
            Not After : Nov 16 19:17:47 2026 GMT
        Subject: C = PK, ST = Islamabad, O = SecureChat Entity, CN = localhost
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b6:8b:42:ab:46:4b:e6:71:94:1b:66:c4:a5:4a:
                    9d:f4:5c:7a:73:ec:d8:d3:b0:c4:08:5c:d0:cb:ad:
                    87:96:f0:8a:1b:7b:26:fd:41:fd:df:bd:cb:af:7b:
                    76:be:d7:8b:ae:68:ec:e9:b2:fe:05:c1:3c:19:92:
                    85:f8:18:b9:52:fe:f6:eb:0a:e9:0b:8c:9f:c0:38:
                    a3:41:54:08:77:4c:36:4b:be:af:54:7d:fb:5c:0e:
                    fe:c5:97:88:c6:e1:b2:b5:f6:71:2d:8e:68:51:66:
                    f0:db:95:1f:e9:ff:33:2a:2a:74:e2:78:51:13:2b:
                    7a:71:40:da:9f:f4:c9:5a:8c:05:16:bb:5f:ab:85:
                    49:8f:bd:bd:ed:b7:8e:89:e2:59:50:86:a3:e0:d6:
                    85:90:67:fb:59:bc:45:9d:8b:b9:6e:ad:e0:f0:7c:
                    e4:47:fb:de:38:79:82:05:f8:28:0a:7f:75:13:db:
                    39:1b:6d:ab:c1:bf:24:d5:93:7a:12:c8:e2:00:e5:
```

f5:aa:87:fb:58:f6:0b:58:21:16:91:47:fe:7e:a7:
67:45:5f:9f:67:4c:e2:9c:d7:1c:98:d1:ea:a6:7f:
25:e9:17:20:48:a2:01:43:34:61:6e:13:37:fe:27:
99:5f:14:fa:65:56:be:8e:0e:b9:dc:31:54:4c:ef:
16:ad
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Alternative Name:
DNS:localhost
Signature Algorithm: sha256WithRSAEncryption
Signature Value:
70:0e:8d:94:9f:af:bc:74:d0:83:a9:88:fa:3f:3a:2b:73:f6:
38:a1:cb:71:43:0e:93:72:f9:d7:fa:f7:78:5b:10:33:c2:56:
13:ca:73:3f:27:06:60:26:fb:58:42:46:f0:e0:4b:2a:09:0a:
2b:65:51:da:48:03:c3:6c:10:a1:24:43:bd:91:25:3b:fe:68:
3e:a5:be:c8:7b:af:96:a5:7f:be:c6:80:35:1a:0e:bb:e9:9b:
43:d8:ea:0a:7e:81:1a:57:31:78:d0:54:7b:3f:43:7f:1b:5c:
b2:fd:5d:54:6a:fd:e5:e4:5a:c0:81:8f:9f:f3:95:63:86:d0:
8f:68:12:a1:b2:23:81:51:f2:af:4e:d2:b8:65:e8:f8:e1:67:
9b:7f:c2:03:ac:be:e2:09:a1:b2:2f:75:d3:dc:57:fb:60:57:
18:a3:0a:23:03:df:ab:16:85:d1:08:e9:65:04:2e:d5:02:41:
23:b3:0f:30:ac:7e:87:1b:ff:4a:5f:ba:8b:14:e8:5c:ad:bd:
bb:5b:42:f3:a3:e5:ec:bb:85:ea:7b:a9:20:53:ba:28:8b:97:
47:9b:ac:a3:e9:f2:29:b4:f0:06:c2:47:3c:4f:df:f2:7c:90:
d3:97:a8:69:50:f0:e7:60:75:af:0b:c8:39:7e:8a:70:0d:60:
3d:10:8f:19