- Certificate Hierarchy
  - Setup a CA
  - Create Sub-CA
  - Create server certificates
  - Create Client Certificate
  - Verify client and server certificates
  - Launch client and server
  - Looking up Services
  - The Green Lock Test

# Certificate Hierarchy

Root certificates / self-signed certificates are not usually used in any application. CAs must provide certificates after due validation of identity.

## Setup a CA

Requires a set of configuration in OpenSSL.

Directory Structure

```
cd cert-hier
mkdir root-ca
cd root-ca
mkdir certs db private
chmod 700 private
touch db/index
openssl rand -hex 16  > db/serial
echo 1001 > db/crlnumber
```

- Certs: location where all issued certificates are stored. Each file here is a certificate
- Db: contains database information.
- Db/index: has the index of all issued certificates.
- Db/serial: serial number of issued certificates. Start with a random number and then the serial number monotonically increases
- Db/crlnumber: Certificate Revocation List numbers
- Private: Contains all the private keys and must be protected

Config file: in cert-hier/root-ca directory

Create root key and CSR request. Take a look at root-ca.conf for configuration details.

==> openssl req -new -config root-ca.conf -out root-ca.csr -keyout private/root-ca.key

```
Generating a RSA private key
.....................................................................................
```

```
.....................................................................................
writing new private key to 'private/root-ca.key'
```

==> ls -al

```
total 32
drwxr-xr-x 5 cybersecurity cybersecurity 4096 Jun 15 12:02 .
drwxr-xr-x 3 cybersecurity cybersecurity 4096 Jun 14 06:18 ..
drwxr-xr-x 2 cybersecurity cybersecurity 4096 Jun 15 11:40 certs
drwxr-xr-x 2 cybersecurity cybersecurity 4096 Jun 15 11:41 db
drwx------ 2 cybersecurity cybersecurity 4096 Jun 15 11:51 private
-rw-r--r-- 1 cybersecurity cybersecurity 2262 Jun 15 12:02 root-ca.conf
-rw-r--r-- 1 cybersecurity cybersecurity 1740 Jun 15 12:02 root-ca.csr
```

==> openssl req -noout -text -in root-ca.csr

Look at “requested extensions”

```
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: C = IN, O = Example, CN = Example.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:
                    00:ed:5b:55:5c:b2:bb:1c:25:c9:64:59:36:31:c7:
                    4e:77:66:87:48:ec:9d:4b:8f:b8:5d:44:4f:98:dd:
                    e0:c1:4f:0d:27:7f:6f:e9:03:c5:4c:5a:76:cb:6b:
                    c6:3d:51:7c:90:1a:ec:44:1c:88:7f:04:d1:af:2c:
                    04:a3:03:35:cb:15:2c:c7:74:06:8d:4c:68:10:cb:
                    4d:c1:a3:27:d2:77:e3:5f:21:72:a0:d1:0e:51:77:
                    80:a0:19:70:d3:7f:01:dc:bb:79:2e:6c:5f:10:dc:
                    be:07:a8:1e:7a:50:cc:ac:aa:6a:bf:9b:52:93:7a:
                    6e:ae:85:27:55:99:4d:68:08:91:d4:f3:b7:9c:fa:
                    55:fb:9b:84:ad:d5:cb:9c:0c:7b:19:34:b0:23:45:
                    e3:86:f9:e6:27:60:5d:b4:12:c1:80:c0:c1:f6:d8:
                    99:5d:90:fb:81:4e:0f:7e:c6:3b:13:58:07:4b:09:
                    22:b6:46:ab:c3:9a:7e:b1:d6:11:d4:a4:84:74:e3:
                    f7:f3:98:33:03:7f:63:e0:4b:94:ac:99:be:d7:86:
                    b5:34:7e:ff:6b:63:35:68:a8:16:f4:5b:9e:17:c2:
                    d2:c0:5f:9a:1d:b3:48:04:98:dc:0c:80:0b:e6:78:
                    ec:95:91:76:7c:e3:9d:3a:65:e5:a5:97:f5:61:a2:
                    1d:4c:5f:ba:38:29:0c:f5:15:a3:20:3c:02:01:33:
                    19:ae:3b:6e:a4:32:6a:25:c1:c8:79:3a:48:10:0a:
                    14:18:11:a1:75:10:e7:15:65:d1:36:f4:34:42:97:
                    34:d0:ff:c4:81:4f:ff:60:e0:71:bd:91:8a:ce:dd:
                    b7:c2:f5:1d:2d:ac:58:8e:92:da:04:b6:31:0f:be:
```

```
                    5f:a3:39:ea:37:70:86:11:78:cf:3e:92:4f:c8:7c:
                    f6:a4:9d:11:a3:63:a3:7d:14:02:43:b4:06:bb:de:
                    c2:d5:d0:0c:5c:bf:c9:a0:36:40:23:8f:1f:34:88:
                    fa:35:b3:47:c8:c3:d0:ce:b9:19:40:23:56:69:37:
                    cf:4e:72:c4:9e:cb:27:c4:50:44:9c:e6:58:97:0f:
                    40:23:e1:d6:62:d8:70:3c:5f:a8:2b:2a:78:54:18:
                    a9:b0:ca:14:e5:6a:24:f0:a4:2e:c8:82:0c:ff:ac:
                    ef:95:72:02:af:a5:7a:b1:03:a7:a0:6f:77:f9:50:
                    90:c8:69:3f:9a:ce:f5:e1:9f:6c:bd:82:85:a2:b9:
                    8e:cf:f3:85:3e:4a:27:95:da:5d:70:50:35:c0:fa:
                    1a:4c:4b:37:90:60:44:f4:6d:e6:96:d0:69:93:b7:
                    e6:a2:04:d9:db:e6:f1:3b:cd:82:31:0b:e7:17:96:
                    a4:d6:8b
                Exponent: 65537 (0x10001)
        Attributes:
        Requested Extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                BB:6D:80:20:31:B4:7D:C1:8D:7B:4F:EE:E2:01:F2:91:DF:09:38:08
    Signature Algorithm: sha256WithRSAEncryption
         d2:12:b7:35:4a:cb:73:ee:19:66:b6:7d:8c:86:ac:16:4e:c4:
         3a:31:b2:03:b5:a9:77:00:33:48:1a:df:fd:2b:57:8a:e6:fe:
         ee:a6:ea:d1:c5:8e:42:89:70:43:cb:f2:f2:29:41:11:a3:98:
         7d:8b:ba:dc:87:79:ff:4e:26:64:d9:a4:6e:28:a6:46:f8:14:
         32:f4:0f:ef:9c:20:a3:ed:bd:68:11:b9:70:6f:05:7f:d3:d1:
         d0:2b:12:0f:41:29:e3:0e:15:67:09:87:db:86:78:0f:82:e2:
         0d:1c:a8:14:0d:9e:3f:a3:f6:da:2c:cc:38:2d:f7:f0:2e:92:
         e6:11:b6:ae:14:a5:0c:b7:73:12:94:bf:ff:f9:92:09:3b:91:
         f5:bc:f1:7e:7e:5e:80:01:a7:6d:10:4d:56:4d:93:5b:2d:c2:
         8e:28:3d:b1:d6:83:a5:06:70:20:5f:9b:0e:1e:8a:26:fd:5c:
         0f:01:42:af:aa:46:6a:9d:11:94:1b:77:69:83:ba:45:47:fd:
         7f:69:4e:3f:1f:7d:c3:5f:4d:ef:0b:22:e6:95:95:f9:58:4e:
         be:b9:27:34:1a:23:4c:56:7c:b8:05:97:0e:a3:d8:d8:88:2c:
         28:02:f7:35:83:b8:ee:9f:a9:04:60:71:84:9a:ea:ab:55:ed:
         bd:4e:4f:cc:f1:a8:1a:bd:3f:b2:c7:67:aa:0b:df:eb:a5:3c:
         64:af:35:0f:58:65:95:07:d3:ee:f4:21:07:11:ba:6c:52:78:
         e5:9f:e8:17:14:75:bc:80:03:56:3f:ac:71:6b:1e:89:4b:cc:
         db:83:19:d3:0a:c1:19:f9:0e:55:7f:bb:2a:01:e0:0e:4f:37:
         61:a8:62:a5:b8:92:fc:85:09:89:b4:bd:8f:7d:6a:56:1f:cf:
         a6:37:24:4a:91:73:d4:bc:3f:d8:5f:9f:4d:70:c0:33:ae:f8:
         6e:e8:96:25:71:0b:74:e6:8f:c6:19:89:ed:34:e5:16:fc:96:
         a3:b9:2d:5d:7b:6e:be:2a:1a:19:7b:00:96:d6:47:66:0e:98:
         ff:bf:92:97:d5:fd:11:c5:4c:f8:ef:96:36:8e:ca:74:ce:5b:
```

```
32:dc:6e:cf:c5:79:a4:f9:a6:f2:b1:42:c6:43:9a:76:42:31:
02:de:ee:a4:4a:f8:bf:e5:e2:3d:19:77:83:29:6a:a0:8c:76:
69:38:f8:a1:bf:9e:03:a6:53:e8:19:a3:89:10:93:df:d3:2d:
66:22:4d:b8:9c:f1:be:46:0c:5a:bb:ef:db:ff:31:1f:90:a9:
47:f3:62:a5:45:96:2a:81:35:e8:73:4f:06:98:34:24:10:47:
72:7b:17:67:14:b3:54:ca
```

Create certificate from the CSR and self sign the certificate.

==> openssl ca -selfsign -config root-ca.conf -in root-ca.csr -out root-ca.crt -extensions ca_ext

```
Using configuration from root-ca.conf
Check that the request matches the signature
Signature ok
Certificate Details:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            2d:0f:e5:f0:00:44:77:c3:e0:31:8d:ba:18:07:c8:bb
        Issuer:
            countryName               = IN
            organizationName          = Example
            commonName                = Example.com
        Validity
            Not Before: Jun 15 06:33:26 2019 GMT
            Not After : Jun 12 06:33:26 2029 GMT
        Subject:
            countryName               = IN
            organizationName          = Example
            commonName                = Example.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:
                    00:ed:5b:55:5c:b2:bb:1c:25:c9:64:59:36:31:c7:
                    4e:77:66:87:48:ec:9d:4b:8f:b8:5d:44:4f:98:dd:
                    e0:c1:4f:0d:27:7f:6f:e9:03:c5:4c:5a:76:cb:6b:
                    c6:3d:51:7c:90:1a:ec:44:1c:88:7f:04:d1:af:2c:
                    04:a3:03:35:cb:15:2c:c7:74:06:8d:4c:68:10:cb:
                    4d:c1:a3:27:d2:77:e3:5f:21:72:a0:d1:0e:51:77:
                    80:a0:19:70:d3:7f:01:dc:bb:79:2e:6c:5f:10:dc:
                    be:07:a8:1e:7a:50:cc:ac:aa:6a:bf:9b:52:93:7a:
                    6e:ae:85:27:55:99:4d:68:08:91:d4:f3:b7:9c:fa:
                    55:fb:9b:84:ad:d5:cb:9c:0c:7b:19:34:b0:23:45:
                    e3:86:f9:e6:27:60:5d:b4:12:c1:80:c0:c1:f6:d8:
```

```
                    99:5d:90:fb:81:4e:0f:7e:c6:3b:13:58:07:4b:09:
                    22:b6:46:ab:c3:9a:7e:b1:d6:11:d4:a4:84:74:e3:
                    f7:f3:98:33:03:7f:63:e0:4b:94:ac:99:be:d7:86:
                    b5:34:7e:ff:6b:63:35:68:a8:16:f4:5b:9e:17:c2:
                    d2:c0:5f:9a:1d:b3:48:04:98:dc:0c:80:0b:e6:78:
                    ec:95:91:76:7c:e3:9d:3a:65:e5:a5:97:f5:61:a2:
                    1d:4c:5f:ba:38:29:0c:f5:15:a3:20:3c:02:01:33:
                    19:ae:3b:6e:a4:32:6a:25:c1:c8:79:3a:48:10:0a:
                    14:18:11:a1:75:10:e7:15:65:d1:36:f4:34:42:97:
                    34:d0:ff:c4:81:4f:ff:60:e0:71:bd:91:8a:ce:dd:
                    b7:c2:f5:1d:2d:ac:58:8e:92:da:04:b6:31:0f:be:
                    5f:a3:39:ea:37:70:86:11:78:cf:3e:92:4f:c8:7c:
                    f6:a4:9d:11:a3:63:a3:7d:14:02:43:b4:06:bb:de:
                    c2:d5:d0:0c:5c:bf:c9:a0:36:40:23:8f:1f:34:88:
                    fa:35:b3:47:c8:c3:d0:ce:b9:19:40:23:56:69:37:
                    cf:4e:72:c4:9e:cb:27:c4:50:44:9c:e6:58:97:0f:
                    40:23:e1:d6:62:d8:70:3c:5f:a8:2b:2a:78:54:18:
                    a9:b0:ca:14:e5:6a:24:f0:a4:2e:c8:82:0c:ff:ac:
                    ef:95:72:02:af:a5:7a:b1:03:a7:a0:6f:77:f9:50:
                    90:c8:69:3f:9a:ce:f5:e1:9f:6c:bd:82:85:a2:b9:
                    8e:cf:f3:85:3e:4a:27:95:da:5d:70:50:35:c0:fa:
                    1a:4c:4b:37:90:60:44:f4:6d:e6:96:d0:69:93:b7:
                    e6:a2:04:d9:db:e6:f1:3b:cd:82:31:0b:e7:17:96:
                    a4:d6:8b
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                BB:6D:80:20:31:B4:7D:C1:8D:7B:4F:EE:E2:01:F2:91:DF:09:38:08
Certificate is to be certified until Jun 12 06:33:26 2029 GMT (3650 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
```

==> ls -al

```
total 40
drwxr-xr-x 5 cybersecurity cybersecurity 4096 Jun 15 12:04 .
drwxr-xr-x 3 cybersecurity cybersecurity 4096 Jun 14 06:18 ..
drwxr-xr-x 2 cybersecurity cybersecurity 4096 Jun 15 12:04 certs
drwxr-xr-x 2 cybersecurity cybersecurity 4096 Jun 15 12:04 db
```

```
drwx------ 2 cybersecurity cybersecurity 4096 Jun 15 11:51 private
-rw-r--r-- 1 cybersecurity cybersecurity 2262 Jun 15 12:02 root-ca.conf
-rw-r--r-- 1 cybersecurity cybersecurity 3056 Jun 15 11:38 root-ca.conf~
-rw-r--r-- 1 cybersecurity cybersecurity 6900 Jun 15 12:04 root-ca.crt
-rw-r--r-- 1 cybersecurity cybersecurity 1740 Jun 15 12:02 root-ca.csr
```

==> ls -al db

```
total 28
drwxr-xr-x 2 cybersecurity cybersecurity 4096 Jun 15 12:04 .
drwxr-xr-x 5 cybersecurity cybersecurity 4096 Jun 15 12:04 ..
-rw-r--r-- 1 cybersecurity cybersecurity    5 Jun 15 11:41 crlnumber
-rw-r--r-- 1 cybersecurity cybersecurity   89 Jun 15 12:04 index
-rw-r--r-- 1 cybersecurity cybersecurity   20 Jun 15 12:04 index.attr
-rw-r--r-- 1 cybersecurity cybersecurity    0 Jun 15 11:41 index.old
-rw-r--r-- 1 cybersecurity cybersecurity   33 Jun 15 12:04 serial
-rw-r--r-- 1 cybersecurity cybersecurity   33 Jun 15 11:41 serial.old
```

==> ls -al certs

```
total 16
drwxr-xr-x 2 cybersecurity cybersecurity 4096 Jun 15 12:04 .
drwxr-xr-x 5 cybersecurity cybersecurity 4096 Jun 15 12:04 ..
-rw-r--r-- 1 cybersecurity cybersecurity 6900 Jun 15 12:04 2D0FE5F0004477C3E0318DBA1807C8BB.
```

You can see the certificate has been created. You can see inside the certificate using openssl.

## Create Sub-CA

Look at sub-ca.conf, also in root-ca directory.

==> openssl req -new -config sub-ca.conf -out sub-ca.csr -keyout private/sub-ca.key

```
Generating a RSA private key
..............++++
.....................................................................................
writing new private key to 'private/sub-ca.key'
```

==> ls -al private

```
total 16
drwx------ 2 cybersecurity cybersecurity 4096 Jun 15 12:24 .
drwxr-xr-x 5 cybersecurity cybersecurity 4096 Jun 15 12:41 ..
-rw------- 1 cybersecurity cybersecurity 3272 Jun 15 12:02 root-ca.key
-rw------- 1 cybersecurity cybersecurity 3272 Jun 15 12:41 sub-ca.key
```

==> openssl req -noout -text -in sub-ca.csr

```
Certificate Request:
```

```
Data:
    Version: 1 (0x0)
    Subject: C = IN, O = Example, CN = Example SubCA
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
            RSA Public-Key: (4096 bit)
            Modulus:
                00:f3:e6:b0:a4:d9:b8:6d:ae:40:6d:aa:c6:93:d3:
                0b:e9:90:cb:07:4d:b0:5b:bf:75:39:ad:23:c5:ae:
                63:46:1b:3d:18:fd:68:7c:75:4f:4a:7b:a8:99:50:
                90:80:f6:23:94:2e:0a:e1:0f:aa:eb:7f:0a:02:ec:
                00:ec:7a:50:16:ab:3c:8b:97:4d:54:d2:2a:37:a4:
                81:fa:db:46:36:b2:78:0d:b1:f1:1e:08:85:3d:d3:
                f5:8d:f6:f8:20:64:92:4c:71:dd:43:27:34:d1:06:
                b3:30:a1:8b:53:03:9c:68:83:d8:2f:03:94:f5:37:
                bb:90:d6:3e:84:c7:3d:ea:f1:0e:1d:55:6d:0d:1d:
                4c:3a:0a:c9:a6:2f:24:88:3f:a5:ab:b1:c5:bf:93:
                93:27:e9:5f:76:e0:d6:65:4f:c5:c9:8e:26:63:96:
                c2:2a:b9:8c:09:fa:b8:02:7d:9b:25:55:35:55:29:
                38:55:0a:67:2c:c4:35:8a:1d:e0:09:8b:c1:81:9d:
                f2:d5:49:04:a5:ad:d1:ab:32:c8:df:d2:b3:4c:76:
                55:b5:5b:ab:4c:91:89:42:1d:08:6d:fb:54:63:e4:
                56:c5:b9:e8:cd:dc:f5:f0:ac:d6:4d:98:3e:66:f5:
                20:69:9b:1f:b8:96:cd:9a:58:7c:0d:e0:71:ea:9c:
                6e:e1:1d:74:2f:c5:57:1b:94:6d:07:b9:40:dc:ef:
                96:bd:a5:d2:dc:14:8c:d7:0a:2d:58:c7:b4:aa:3c:
                af:21:e0:30:01:32:7d:7f:7a:1d:10:e3:20:6c:d9:
                ee:e3:74:1b:6d:20:27:c1:bd:ca:b8:7e:5b:57:a3:
                4b:68:f5:1c:25:8a:32:6a:8c:74:6b:e0:2c:17:39:
                c4:0b:6a:2c:de:76:4a:60:f5:b9:09:99:36:a1:23:
                6a:62:2b:07:4c:b6:49:1f:b8:55:cc:c5:68:1c:4a:
                62:be:b4:9d:b5:1e:12:18:3b:14:f6:36:f1:d7:1d:
                d6:fd:fc:51:d6:af:96:ff:36:fa:9e:d0:78:2b:c9:
                96:cd:82:22:11:15:2e:68:aa:32:d9:2f:ee:5a:ed:
                ce:ee:17:d7:dd:51:f8:85:ff:3e:93:5c:fe:f6:d7:
                d7:f2:46:5c:16:6a:70:33:d7:59:96:0f:4b:49:bc:
                2e:25:77:66:ab:69:ae:fc:b3:bf:78:96:47:51:81:
                2a:14:b5:ad:5d:15:bf:2e:6f:b8:ce:6d:fd:a4:2a:
                63:da:69:7b:5d:1d:73:26:c2:2d:51:5d:44:92:84:
                48:82:53:98:02:5c:81:63:53:a4:49:4a:77:1a:e4:
                92:77:71:4e:84:5e:e3:cd:15:9c:0d:58:fe:39:91:
                b3:7f:25
            Exponent: 65537 (0x10001)
    Attributes:
    Requested Extensions:
        X509v3 Basic Constraints: critical
```

```
            CA:TRUE
        X509v3 Key Usage: critical
            Certificate Sign, CRL Sign
        X509v3 Subject Key Identifier:
            DD:C4:4A:9E:ED:9B:87:2A:56:E0:FB:8C:6C:F5:C1:2C:79:D3:26:97
Signature Algorithm: sha256WithRSAEncryption
     1c:6c:99:89:f8:31:03:66:f2:4f:26:01:c2:db:bb:82:27:1d:
     fa:fe:4c:c4:8a:00:50:67:aa:29:ef:10:29:e9:fd:3c:6a:81:
     9c:8f:72:a2:49:94:e4:75:38:df:63:ee:19:3e:dc:2a:f7:0a:
     dd:e6:01:3c:6a:64:84:3a:85:89:72:4f:61:5c:54:bb:e0:1d:
     90:ec:f3:04:f8:c5:78:77:b1:b4:f6:4e:a2:c5:7b:67:24:3c:
     da:e6:83:2a:12:84:88:8b:d9:f2:99:d0:7c:f7:ed:97:17:f8:
     d2:0a:80:fe:8b:a9:ce:4b:9f:26:c0:e5:11:45:28:35:50:e4:
     39:b4:3a:ea:93:2c:6f:76:00:5f:c8:31:6c:7e:66:fd:11:4f:
     b2:7f:dd:8e:00:64:c5:6d:2a:a1:70:cb:eb:e4:9d:3a:96:ef:
     3b:75:ee:e6:38:6d:bb:cf:cc:fb:d9:0e:3a:72:68:af:87:a3:
     77:92:94:3c:f6:e5:04:1e:8e:a7:39:5d:4e:86:0b:b6:c1:16:
     41:97:95:30:ce:c8:df:d1:df:eb:e8:df:1a:c0:dd:a6:e6:a6:
     07:38:10:28:d2:99:51:47:8b:95:13:81:e2:cf:64:f1:2c:f3:
     ae:2f:1c:d2:25:6b:c4:14:9b:0a:b9:57:3e:a4:92:0d:b9:e6:
     2a:0f:ac:50:e0:9f:b1:66:79:89:07:cc:b3:3f:ef:4a:eb:cc:
     e0:e4:cf:49:9c:19:4a:59:c9:9e:f0:03:76:20:47:71:08:26:
     25:a9:1d:66:64:32:44:b8:64:79:2b:87:bb:f8:95:c1:5f:17:
     2f:a3:f1:d1:58:ff:14:78:41:33:db:7b:dd:f6:a8:fe:93:75:
     64:25:c2:60:2b:86:5f:25:62:46:5a:77:53:56:da:cb:6c:8e:
     e1:7f:fb:8d:94:95:3e:ad:df:56:a0:76:7d:a5:e0:88:d3:29:
     03:d1:1a:56:3b:07:53:d0:41:30:c4:39:73:07:3b:22:be:46:
     ea:c5:e0:61:a3:a5:0a:ed:90:1e:9c:da:23:70:ca:45:04:41:
     8d:2d:53:63:33:08:c8:71:57:5e:2f:89:4e:a0:84:3c:ca:4b:
     06:33:04:bc:3a:50:c7:6f:d3:cd:af:2f:08:47:1f:96:81:ad:
     06:58:cc:b2:6b:d2:42:f2:ed:2c:74:a4:11:83:73:6e:b9:da:
     0e:b3:44:e9:40:5e:67:f9:3f:41:2a:a5:74:ea:1b:69:bb:9e:
     18:69:6d:6c:7f:99:f2:ed:32:65:37:78:10:70:f8:7a:6b:53:
     b2:78:e2:23:78:c2:b3:db:87:9e:9e:cc:21:00:c3:ce:7b:91:
     bd:99:19:ab:23:13:9f:5d
```

==> openssl ca -config root-ca.conf -in sub-ca.csr -out sub-ca.crt -extensions sub_ca_ext

```
Using configuration from root-ca.conf
Check that the request matches the signature
Signature ok
Certificate Details:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
```

```
    2d:0f:e5:f0:00:44:77:c3:e0:31:8d:ba:18:07:c8:bc
Issuer:
    countryName               = IN
    organizationName          = Example
    commonName                = Example.com
Validity
    Not Before: Jun 15 07:18:31 2019 GMT
    Not After : Jun 12 07:18:31 2029 GMT
Subject:
    countryName               = IN
    organizationName          = Example
    commonName                = Example SubCA
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
        RSA Public-Key: (4096 bit)
        Modulus:
            00:f3:e6:b0:a4:d9:b8:6d:ae:40:6d:aa:c6:93:d3:
            0b:e9:90:cb:07:4d:b0:5b:bf:75:39:ad:23:c5:ae:
            63:46:1b:3d:18:fd:68:7c:75:4f:4a:7b:a8:99:50:
            90:80:f6:23:94:2e:0a:e1:0f:aa:eb:7f:0a:02:ec:
            00:ec:7a:50:16:ab:3c:8b:97:4d:54:d2:2a:37:a4:
            81:fa:db:46:36:b2:78:0d:b1:f1:1e:08:85:3d:d3:
            f5:8d:f6:f8:20:64:92:4c:71:dd:43:27:34:d1:06:
            b3:30:a1:8b:53:03:9c:68:83:d8:2f:03:94:f5:37:
            bb:90:d6:3e:84:c7:3d:ea:f1:0e:1d:55:6d:0d:1d:
            4c:3a:0a:c9:a6:2f:24:88:3f:a5:ab:b1:c5:bf:93:
            93:27:e9:5f:76:e0:d6:65:4f:c5:c9:8e:26:63:96:
            c2:2a:b9:8c:09:fa:b8:02:7d:9b:25:55:35:55:29:
            38:55:0a:67:2c:c4:35:8a:1d:e0:09:8b:c1:81:9d:
            f2:d5:49:04:a5:ad:d1:ab:32:c8:df:d2:b3:4c:76:
            55:b5:5b:ab:4c:91:89:42:1d:08:6d:fb:54:63:e4:
            56:c5:b9:e8:cd:dc:f5:f0:ac:d6:4d:98:3e:66:f5:
            20:69:9b:1f:b8:96:cd:9a:58:7c:0d:e0:71:ea:9c:
            6e:e1:1d:74:2f:c5:57:1b:94:6d:07:b9:40:dc:ef:
            96:bd:a5:d2:dc:14:8c:d7:0a:2d:58:c7:b4:aa:3c:
            af:21:e0:30:01:32:7d:7f:7a:1d:10:e3:20:6c:d9:
            ee:e3:74:1b:6d:20:27:c1:bd:ca:b8:7e:5b:57:a3:
            4b:68:f5:1c:25:8a:32:6a:8c:74:6b:e0:2c:17:39:
            c4:0b:6a:2c:de:76:4a:60:f5:b9:09:99:36:a1:23:
            6a:62:2b:07:4c:b6:49:1f:b8:55:cc:c5:68:1c:4a:
            62:be:b4:9d:b5:1e:12:18:3b:14:f6:36:f1:d7:1d:
            d6:fd:fc:51:d6:af:96:ff:36:fa:9e:d0:78:2b:c9:
            96:cd:82:22:11:15:2e:68:aa:32:d9:2f:ee:5a:ed:
            ce:ee:17:d7:dd:51:f8:85:ff:3e:93:5c:fe:f6:d7:
            d7:f2:46:5c:16:6a:70:33:d7:59:96:0f:4b:49:bc:
            2e:25:77:66:ab:69:ae:fc:b3:bf:78:96:47:51:81:
```

```
                    2a:14:b5:ad:5d:15:bf:2e:6f:b8:ce:6d:fd:a4:2a:
                    63:da:69:7b:5d:1d:73:26:c2:2d:51:5d:44:92:84:
                    48:82:53:98:02:5c:81:63:53:a4:49:4a:77:1a:e4:
                    92:77:71:4e:84:5e:e3:cd:15:9c:0d:58:fe:39:91:
                    b3:7f:25
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            Authority Information Access:
                CA Issuers - URI:http://root-ca.example.com/root-ca.cr
                OCSP - URI:http://ocsp.root-ca.example.com:9080

            X509v3 Authority Key Identifier:
                keyid:BB:6D:80:20:31:B4:7D:C1:8D:7B:4F:EE:E2:01:F2:91:DF:09:38:08

            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://root-ca.example.com/root-ca.crl

            X509v3 Extended Key Usage:
                TLS Web Client Authentication, TLS Web Server Authentication
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Name Constraints:
                Permitted:
                  DNS:example.com
                  DNS:example.org
                Excluded:
                  IP:0.0.0.0/0.0.0.0
                  IP:0:0:0:0:0:0:0:0/0:0:0:0:0:0:0:0

            X509v3 Subject Key Identifier:
                DD:C4:4A:9E:ED:9B:87:2A:56:E0:FB:8C:6C:F5:C1:2C:79:D3:26:97
Certificate is to be certified until Jun 12 07:18:31 2029 GMT (3650 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
```

==> ls -al certs

```
total 24
drwxr-xr-x 2 cybersecurity cybersecurity 4096 Jun 15 12:48 .
```

```
drwxr-xr-x 5 cybersecurity cybersecurity 4096 Jun 15 12:48 ..
-rw-r--r-- 1 cybersecurity cybersecurity 6900 Jun 15 12:04 2D0FE5F0004477C3E0318DBA1807C8BB.
-rw-r--r-- 1 cybersecurity cybersecurity 8186 Jun 15 12:48 2D0FE5F0004477C3E0318DBA1807C8BC.
```

==> cat db/index

```
V   290612063326Z       2D0FE5F0004477C3E0318DBA1807C8BB    unknown /C=IN/O=Example/CN=Examp
V   290612071831Z       2D0FE5F0004477C3E0318DBA1807C8BC    unknown /C=IN/O=Example/CN=Examp
```

==> cat db/serial

```
2D0FE5F0004477C3E0318DBA1807C8BD
```

==> cat db/serial.old

```
2D0FE5F0004477C3E0318DBA1807C8BC
```

==> ls -al

```
total 60
drwxr-xr-x 5 cybersecurity cybersecurity 4096 Jun 15 12:48 .
drwxr-xr-x 4 cybersecurity cybersecurity 4096 Jun 15 12:13 ..
drwxr-xr-x 2 cybersecurity cybersecurity 4096 Jun 15 12:48 certs
drwxr-xr-x 2 cybersecurity cybersecurity 4096 Jun 15 12:48 db
drwx------ 2 cybersecurity cybersecurity 4096 Jun 15 12:24 private
-rw-r--r-- 1 cybersecurity cybersecurity 2263 Jun 15 12:48 root-ca.conf
-rw-r--r-- 1 cybersecurity cybersecurity 3056 Jun 15 11:38 root-ca.conf~
-rw-r--r-- 1 cybersecurity cybersecurity 6900 Jun 15 12:04 root-ca.crt
-rw-r--r-- 1 cybersecurity cybersecurity 1740 Jun 15 12:02 root-ca.csr
-rw-r--r-- 1 cybersecurity cybersecurity 2945 Jun 15 12:48 sub-ca.conf
-rw-r--r-- 1 cybersecurity cybersecurity 2944 Jun 15 12:40 sub-ca.conf~
-rw-r--r-- 1 cybersecurity cybersecurity 8186 Jun 15 12:48 sub-ca.crt
-rw-r--r-- 1 cybersecurity cybersecurity 1740 Jun 15 12:41 sub-ca.csr
```

How do you distinguish between self-signed certificate and a CA issued certificate? The difference is in the presence of the "X509v3 Authority Key Identifier" extension. Its value will be different from the value of the "X509v3 Subject Key Identifier" extension. If they are the same or if the "Authority Key Identifier" extension is not present, then it is a self-signed certificate.

## Create server certificates

We will now create certificates for server and client. We will not do this in the root-ca folder since they are not managed by the CA. Instead they are managed by the user/application/customer.

==> cd cert-hier

==> openssl genrsa -out serverkey.key

```
Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................................+++++
```

```
.....................................................................+++++
e is 65537 (0x010001)
```

==> openssl rsa -pubout -out serverpubkey.key -in serverkey.key

```
writing RSA key
```

==> ls -al

```
total 20
drwxr-xr-x 3 cybersecurity cybersecurity 4096 Jun 15 12:58 .
drwxr-xr-x 6 cybersecurity cybersecurity 4096 Jun 12 20:30 ..
drwxr-xr-x 5 cybersecurity cybersecurity 4096 Jun 15 12:48 root-ca
-rw------- 1 cybersecurity cybersecurity 1679 Jun 12 20:32 serverkey.key
-rw-r--r-- 1 cybersecurity cybersecurity  451 Jun 12 20:33 serverpubkey.key
```

Create a CSR

==> openssl req -new -config server-coolcompany.conf -key serverkey.key -out server-coolcompany.csr

==> openssl req -in server-coolcompany.csr -noout -text

```
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: CN = www.coolcompany.example, emailAddress = admin@coolcompany.example, O =
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:a5:8b:ec:35:4c:fb:5c:46:9f:4e:a5:be:7b:32:
                    c4:17:a0:d3:09:88:01:5e:36:04:f1:7d:c1:98:31:
                    35:ea:62:ad:22:4a:5d:19:bd:0f:0f:f0:3a:f5:ca:
                    66:ee:b0:a1:85:4f:af:b7:3a:d7:9d:60:5f:cd:b6:
                    5f:fd:0f:db:94:5b:02:4f:e4:ad:b6:25:0d:25:bb:
                    ce:55:86:27:2b:3e:57:df:72:1a:79:04:29:b5:dc:
                    a5:23:5a:ff:48:72:a4:88:fb:fb:d3:f1:5c:1a:c4:
                    05:e6:e0:b9:56:0e:c8:91:8e:fb:66:9d:68:67:e5:
                    ca:ae:45:4c:e4:6b:05:6f:68:eb:6b:0c:05:d4:de:
                    7b:40:f9:27:30:94:0f:ab:41:75:d1:38:9e:9c:04:
                    49:b1:9c:47:97:e6:70:ae:35:7a:e1:79:12:bd:50:
                    71:53:73:49:51:af:c0:73:f7:21:e8:75:a3:99:49:
                    b7:0d:7f:df:4b:64:a0:4c:5c:a3:6a:dc:1f:17:6c:
                    dd:00:a9:05:2e:7d:db:fc:ab:5a:65:17:e0:75:5f:
                    77:b2:70:aa:97:be:02:6f:10:44:29:e3:31:b5:4b:
                    b7:94:da:ba:23:75:4d:0c:b9:78:77:0e:65:aa:65:
                    8a:a5:c1:11:5c:6e:1e:96:27:22:20:20:15:de:96:
                    a5:c3
                Exponent: 65537 (0x10001)
```

```
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
         6d:ee:a9:49:0c:f5:4f:cb:18:b3:2a:5f:fe:e2:ae:14:d1:68:
         d8:20:d4:c5:72:a4:54:d4:a6:34:c7:1a:b4:8f:45:55:29:96:
         3c:33:42:ac:68:3d:cc:4c:83:c8:06:79:d1:91:37:0f:1f:38:
         df:61:8f:0f:41:36:a3:9c:bb:35:40:f7:e0:70:1f:e4:7a:84:
         e7:f1:c7:1f:19:da:14:4e:12:09:d2:90:47:3a:82:7b:ac:48:
         72:c4:95:d9:a5:b8:cf:2c:5e:fa:db:a6:dc:a4:41:20:92:8c:
         4c:c7:c9:7d:f3:1b:28:10:7e:0b:85:18:5a:12:36:e3:1b:1a:
         b4:a7:a2:b6:d2:42:17:d8:fe:91:46:57:76:6f:f0:c2:5a:19:
         86:e0:31:15:e7:73:16:30:9e:a8:72:bc:c6:a2:6c:10:c4:76:
         64:26:25:38:dc:e8:48:92:c1:3f:10:9d:d9:cd:da:25:66:45:
         37:e1:58:57:0b:05:aa:9f:80:a8:a1:a7:58:e8:9f:ef:d4:9d:
         12:09:47:95:eb:8a:32:38:07:07:23:0a:90:24:a6:55:87:0d:
         4d:46:d5:f0:db:7b:c2:f1:17:24:43:1c:ba:38:35:5a:2e:18:
         95:81:90:68:3c:85:cc:6b:dd:1d:ea:65:d9:2b:7f:d0:0e:5f:
         6a:33:04:a8
```

Get Server certificate issued by the SubCA.

==> cd root-ca

==> openssl ca -config sub-ca.conf -in ../server-coolcompany.csr -out ../server-coolcompany.crt -extensions server_ext

```
Using configuration from sub-ca.conf
Check that the request matches the signature
Signature ok
The organizationName field is different between
CA certificate (Example) and the request (My Cool Company Ltd)
```

Config file prevents us from issuing arbitrary certificates. Re-create the CSR.

==> openssl req -new -config server-example.conf -key serverkey.key -out server-example.csr

==> ls -al

```
total 36
drwxr-xr-x 3 cybersecurity cybersecurity 4096 Jul  4 22:00 .
drwxr-xr-x 8 cybersecurity cybersecurity 4096 Jul  4 21:07 ..
drwxr-xr-x 5 cybersecurity cybersecurity 4096 Jul  4 21:32 root-ca
-rw-r--r-- 1 cybersecurity cybersecurity  191 Jul  4 21:50 server-coolcompany.conf
-rw-r--r-- 1 cybersecurity cybersecurity 1102 Jul  4 21:52 server-coolcompany.csr
-rw-r--r-- 1 cybersecurity cybersecurity  165 Jul  4 21:58 server-example.conf
-rw-r--r-- 1 cybersecurity cybersecurity 1070 Jul  4 22:00 server-example.csr
-rw------- 1 cybersecurity cybersecurity 1679 Jul  4 21:48 serverkey.key
-rw-r--r-- 1 cybersecurity cybersecurity  451 Jul  4 21:48 serverpubkey.key
```

==> openssl req -in server-example.csr -noout -text

```
Certificate Request:
    Data:
        Version: 1 (0x0)
        Subject: CN = 127.0.0.1, emailAddress = admin@coolcompany.example, O = Example, OU =
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:a5:8b:ec:35:4c:fb:5c:46:9f:4e:a5:be:7b:32:
                    c4:17:a0:d3:09:88:01:5e:36:04:f1:7d:c1:98:31:
                    35:ea:62:ad:22:4a:5d:19:bd:0f:0f:f0:3a:f5:ca:
                    66:ee:b0:a1:85:4f:af:b7:3a:d7:9d:60:5f:cd:b6:
                    5f:fd:0f:db:94:5b:02:4f:e4:ad:b6:25:0d:25:bb:
                    ce:55:86:27:2b:3e:57:df:72:1a:79:04:29:b5:dc:
                    a5:23:5a:ff:48:72:a4:88:fb:fb:d3:f1:5c:1a:c4:
                    05:e6:e0:b9:56:0e:c8:91:8e:fb:66:9d:68:67:e5:
                    ca:ae:45:4c:e4:6b:05:6f:68:eb:6b:0c:05:d4:de:
                    7b:40:f9:27:30:94:0f:ab:41:75:d1:38:9e:9c:04:
                    49:b1:9c:47:97:e6:70:ae:35:7a:e1:79:12:bd:50:
                    71:53:73:49:51:af:c0:73:f7:21:e8:75:a3:99:49:
                    b7:0d:7f:df:4b:64:a0:4c:5c:a3:6a:dc:1f:17:6c:
                    dd:00:a9:05:2e:7d:db:fc:ab:5a:65:17:e0:75:5f:
                    77:b2:70:aa:97:be:02:6f:10:44:29:e3:31:b5:4b:
                    b7:94:da:ba:23:75:4d:0c:b9:78:77:0e:65:aa:65:
                    8a:a5:c1:11:5c:6e:1e:96:27:22:20:20:15:de:96:
                    a5:c3
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
         75:32:3c:51:e8:00:fe:a4:5b:99:7a:08:4e:c8:f3:6b:45:7b:
         78:e4:cb:fa:0a:fd:55:ae:9e:5c:74:e8:17:47:22:e9:bb:be:
         4a:18:a3:10:fc:aa:86:09:81:1f:36:cf:86:db:40:21:ec:74:
         7f:63:cb:e1:a6:0d:c4:f1:14:20:60:62:c7:89:f8:e4:85:f4:
         b6:b7:c3:10:76:1b:ad:d4:98:df:31:ed:21:31:70:12:b8:54:
         ab:20:c2:81:af:d5:6f:bf:4e:2a:6a:86:7d:a1:86:8d:37:63:
         f2:bd:f7:bc:ac:0a:39:31:57:ac:f6:c5:22:f1:7e:e2:20:17:
         b2:92:cd:a4:97:32:aa:62:58:0d:82:9b:b9:b1:1e:2c:5d:ce:
         5e:66:48:f7:c0:0d:a6:84:4e:06:ab:33:5c:88:53:8f:40:5e:
         7d:47:46:7d:db:1c:d0:5a:87:6c:46:89:87:7c:66:5b:6c:32:
         40:06:50:97:7e:69:94:86:f4:f9:88:f8:62:1f:2a:59:d9:ef:
         6b:38:fb:81:d2:2b:33:0f:b5:65:ef:d7:fa:64:a8:f5:5a:f6:
         06:c9:2d:ac:83:08:5d:16:88:b5:22:b5:66:81:44:25:2a:99:
         be:90:cd:9b:e0:84:e2:30:6b:e6:39:7b:df:52:2b:6e:4f:be:
```

```
10:41:26:ef
```

Now switch to the CA and issue the certificate

==> cd root-ca

==> openssl ca -config sub-ca.conf -in ../server-example.csr -out ../server-example.crt -extensions server_ext

```
Using configuration from sub-ca.conf
Check that the request matches the signature
Signature ok
Certificate Details:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            7d:2b:5b:7f:9f:30:c3:b2:38:c6:e5:19:82:f0:c2:88
        Issuer:
            countryName               = IN
            organizationName          = Example
            commonName                = Example SubCA
        Validity
            Not Before: Jul  4 16:31:49 2019 GMT
            Not After : Jul  3 16:31:49 2020 GMT
        Subject:
            countryName               = IN
            stateOrProvinceName       = Tamil Nadu
            organizationName          = Example
            organizationalUnitName    = Finance
            commonName                = 127.0.0.1
            emailAddress              = admin@coolcompany.example
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:a5:8b:ec:35:4c:fb:5c:46:9f:4e:a5:be:7b:32:
                    c4:17:a0:d3:09:88:01:5e:36:04:f1:7d:c1:98:31:
                    35:ea:62:ad:22:4a:5d:19:bd:0f:0f:f0:3a:f5:ca:
                    66:ee:b0:a1:85:4f:af:b7:3a:d7:9d:60:5f:cd:b6:
                    5f:fd:0f:db:94:5b:02:4f:e4:ad:b6:25:0d:25:bb:
                    ce:55:86:27:2b:3e:57:df:72:1a:79:04:29:b5:dc:
                    a5:23:5a:ff:48:72:a4:88:fb:fb:d3:f1:5c:1a:c4:
                    05:e6:e0:b9:56:0e:c8:91:8e:fb:66:9d:68:67:e5:
                    ca:ae:45:4c:e4:6b:05:6f:68:eb:6b:0c:05:d4:de:
                    7b:40:f9:27:30:94:0f:ab:41:75:d1:38:9e:9c:04:
                    49:b1:9c:47:97:e6:70:ae:35:7a:e1:79:12:bd:50:
                    71:53:73:49:51:af:c0:73:f7:21:e8:75:a3:99:49:
```

```
                    b7:0d:7f:df:4b:64:a0:4c:5c:a3:6a:dc:1f:17:6c:
                    dd:00:a9:05:2e:7d:db:fc:ab:5a:65:17:e0:75:5f:
                    77:b2:70:aa:97:be:02:6f:10:44:29:e3:31:b5:4b:
                    b7:94:da:ba:23:75:4d:0c:b9:78:77:0e:65:aa:65:
                    8a:a5:c1:11:5c:6e:1e:96:27:22:20:20:15:de:96:
                    a5:c3
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            Authority Information Access:
                CA Issuers - URI:http://sub-ca.example.com/sub-ca.crt
                OCSP - URI:http://ocsp.sub-ca.example.com:9081

            X509v3 Authority Key Identifier:
                keyid:07:CE:A9:EE:BA:4B:86:F2:F4:79:05:37:99:59:DD:F3:43:A2:DE:AC

            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://sub-ca.example.com/sub-ca.crl

            X509v3 Extended Key Usage:
                TLS Web Client Authentication
            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Subject Key Identifier:
                B2:45:C4:C7:2A:FC:0E:55:10:7B:90:67:06:DE:C4:12:CF:C5:D5:A7
Certificate is to be certified until Jul  3 16:31:49 2020 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
```

==> ls -al db

```
total 36
drwxr-xr-x 2 cybersecurity cybersecurity 4096 Jul  4 22:01 .
drwxr-xr-x 5 cybersecurity cybersecurity 4096 Jul  4 21:32 ..
-rw-r--r-- 1 cybersecurity cybersecurity    5 Jul  4 21:10 crlnumber
-rw-r--r-- 1 cybersecurity cybersecurity  331 Jul  4 22:01 index
-rw-r--r-- 1 cybersecurity cybersecurity   20 Jul  4 22:01 index.attr
-rw-r--r-- 1 cybersecurity cybersecurity   20 Jul  4 21:32 index.attr.old
-rw-r--r-- 1 cybersecurity cybersecurity  180 Jul  4 21:32 index.old
-rw-r--r-- 1 cybersecurity cybersecurity   33 Jul  4 22:01 serial
```

```
-rw-r--r-- 1 cybersecurity cybersecurity   33 Jul  4 21:32 serial.old
```

==> ls -al certs/

```
total 32
drwxr-xr-x 2 cybersecurity cybersecurity 4096 Jul  4 22:01 .
drwxr-xr-x 5 cybersecurity cybersecurity 4096 Jul  4 21:32 ..
-rw-r--r-- 1 cybersecurity cybersecurity 6900 Jul  4 21:21 7D2B5B7F9F30C3B238C6E51982F0C286.
-rw-r--r-- 1 cybersecurity cybersecurity 7812 Jul  4 21:32 7D2B5B7F9F30C3B238C6E51982F0C287.
-rw-r--r-- 1 cybersecurity cybersecurity 6427 Jul  4 22:01 7D2B5B7F9F30C3B238C6E51982F0C288.
```

Look at the certificate and verify everything looks good.

==> openssl x509 -in server-example.crt -noout -text

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            7d:2b:5b:7f:9f:30:c3:b2:38:c6:e5:19:82:f0:c2:8b
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = IN, O = Example, CN = Example SubCA
        Validity
            Not Before: Jul  4 17:10:09 2019 GMT
            Not After : Jul  3 17:10:09 2020 GMT
        Subject: C = IN, ST = Tamil Nadu, O = Example, OU = Finance, CN = 127.0.0.1, emailAd
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:a5:8b:ec:35:4c:fb:5c:46:9f:4e:a5:be:7b:32:
                    c4:17:a0:d3:09:88:01:5e:36:04:f1:7d:c1:98:31:
                    35:ea:62:ad:22:4a:5d:19:bd:0f:0f:f0:3a:f5:ca:
                    66:ee:b0:a1:85:4f:af:b7:3a:d7:9d:60:5f:cd:b6:
                    5f:fd:0f:db:94:5b:02:4f:e4:ad:b6:25:0d:25:bb:
                    ce:55:86:27:2b:3e:57:df:72:1a:79:04:29:b5:dc:
                    a5:23:5a:ff:48:72:a4:88:fb:fb:d3:f1:5c:1a:c4:
                    05:e6:e0:b9:56:0e:c8:91:8e:fb:66:9d:68:67:e5:
                    ca:ae:45:4c:e4:6b:05:6f:68:eb:6b:0c:05:d4:de:
                    7b:40:f9:27:30:94:0f:ab:41:75:d1:38:9e:9c:04:
                    49:b1:9c:47:97:e6:70:ae:35:7a:e1:79:12:bd:50:
                    71:53:73:49:51:af:c0:73:f7:21:e8:75:a3:99:49:
                    b7:0d:7f:df:4b:64:a0:4c:5c:a3:6a:dc:1f:17:6c:
                    dd:00:a9:05:2e:7d:db:fc:ab:5a:65:17:e0:75:5f:
                    77:b2:70:aa:97:be:02:6f:10:44:29:e3:31:b5:4b:
                    b7:94:da:ba:23:75:4d:0c:b9:78:77:0e:65:aa:65:
                    8a:a5:c1:11:5c:6e:1e:96:27:22:20:20:15:de:96:
                    a5:c3
```

```
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            Authority Information Access:
                CA Issuers - URI:http://sub-ca.example.com/sub-ca.crt
                OCSP - URI:http://ocsp.sub-ca.example.com:9081

            X509v3 Authority Key Identifier:
                keyid:07:CE:A9:EE:BA:4B:86:F2:F4:79:05:37:99:59:DD:F3:43:A2:DE:AC

            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://sub-ca.example.com/sub-ca.crl

            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Subject Key Identifier:
                B2:45:C4:C7:2A:FC:0E:55:10:7B:90:67:06:DE:C4:12:CF:C5:D5:A7
    Signature Algorithm: sha256WithRSAEncryption
         a2:d5:43:f8:e5:eb:91:de:7e:d7:c9:74:f1:81:13:34:a7:39:
         83:8a:70:d5:94:b0:8f:8c:10:f8:33:0e:91:f8:81:cb:ac:e7:
         a9:8c:91:82:6b:92:45:94:0b:e7:38:2d:d9:6a:62:bd:bd:b3:
         15:75:18:6b:9a:cd:8a:e4:7e:28:f4:30:76:bb:8d:3e:63:16:
         41:66:3f:77:ca:31:e2:e8:1a:ce:a6:d2:d8:5c:20:2f:a3:da:
         43:91:08:97:9e:f0:60:9e:82:36:5e:fb:1d:1a:cb:64:95:67:
         68:3b:9d:79:c1:f4:c2:54:88:db:de:b2:af:b6:cb:fc:47:27:
         0b:ec:cc:b8:a6:ae:43:8c:7c:bd:87:96:45:1b:1c:10:64:5d:
         eb:73:a2:7f:7f:bb:ef:1f:8c:b4:b5:52:cd:52:29:be:82:a9:
         27:ef:dd:ab:68:f6:95:29:ad:b2:02:7e:7a:60:fb:05:cc:15:
         88:a7:2d:64:ef:00:f1:58:c4:cb:47:65:2a:45:a2:4f:a3:1e:
         ba:3e:c3:fa:d2:1a:ab:51:69:a0:17:38:1c:04:ef:1c:d3:25:
         be:3f:a0:96:9b:25:1c:de:9a:06:ed:8e:e8:d5:ca:5c:e1:ba:
         03:d0:21:3a:47:41:d8:89:5b:43:a7:bf:97:98:2f:41:8f:d2:
         96:a9:b5:06:05:3d:a9:9b:a9:da:77:49:58:25:c3:a6:9e:2f:
         84:d7:59:59:df:03:9a:0c:8f:06:95:0e:29:4a:e6:34:e5:f0:
         38:11:92:3e:2a:6b:d4:27:eb:60:a1:9c:01:1e:14:4e:9a:af:
         8a:19:ee:16:15:01:80:64:cc:73:73:69:82:ad:c9:f1:62:3d:
         51:93:a6:ba:3d:4d:c3:94:b7:3c:13:44:b7:34:c8:b9:9a:4e:
         1d:70:1e:42:46:57:65:ff:53:5e:ae:17:8d:c7:3e:7d:7c:87:
         dc:4c:52:d7:a3:ee:5b:0d:83:84:68:72:3e:d3:ba:60:30:7f:
         d1:5b:d8:4c:b7:1d:e9:d5:16:ff:63:67:cf:76:7d:4d:19:a0:
         28:94:04:7c:b8:62:59:15:9d:bc:4f:a0:e6:2c:ce:12:a9:03:
```

```
45:43:be:d1:fd:d6:a8:b6:db:7c:c8:ab:94:2b:15:b0:a2:80:
e7:06:bc:70:21:d3:a9:af:8b:f0:f8:05:0b:15:2d:e0:25:e6:
13:34:f7:e4:75:d3:d9:6a:75:ff:5c:bc:f1:f6:bd:ad:d5:00:
ab:88:bc:f4:dc:54:11:e4:6e:4e:a2:62:8d:16:51:fe:58:e8:
fe:a0:f8:92:bb:70:20:4e:74:54:c1:f5:03:dd:44:2a:7b:b3:
db:c4:4c:68:f3:57:a3:ea
```

## Create Client Certificate

==> cd cert-hier

==> openssl genrsa -out clientkey.key 4096

```
openssl genrsa -out clientkey.key 4096
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................................................................++++
.....................................................................................
e is 65537 (0x010001)
```

==> openssl req -new -config client-example.conf -key clientkey.key -out client-example.csr

==> openssl req -in client-example.csr -noout -text

SubCA has to issue certificate

==> cd root-ca

==> openssl ca -config sub-ca.conf -in ../client.csr -out ../client.crt -extensions client_ext

```
Using configuration from sub-ca.conf
Check that the request matches the signature
Signature ok
Certificate Details:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            7d:2b:5b:7f:9f:30:c3:b2:38:c6:e5:19:82:f0:c2:89
        Issuer:
            countryName               = IN
            organizationName          = Example
            commonName                = Example SubCA
        Validity
            Not Before: Jul  4 16:41:36 2019 GMT
            Not After : Jul  3 16:41:36 2020 GMT
        Subject:
            countryName               = IN
            stateOrProvinceName       = Delhi
```

```
    organizationName          = Example
    organizationalUnitName    = HR
    commonName                = 127.0.0.1
    emailAddress              = admin@coolcompany.example
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
        RSA Public-Key: (4096 bit)
        Modulus:
            00:d7:9e:e4:e8:ef:2b:93:9a:3e:61:1a:8d:d6:1d:
            68:37:10:61:1f:8b:17:28:6b:81:37:dd:63:0f:d7:
            df:61:07:dc:a2:43:ba:17:3a:be:79:03:ff:46:4e:
            23:6d:0b:e4:7c:0d:a9:11:a7:cd:c6:30:81:34:b6:
            f7:a7:60:8e:ad:57:ee:78:85:02:9d:7c:54:7b:53:
            b2:bd:42:8a:c4:32:bd:00:98:87:37:e5:a4:27:b4:
            53:ae:b8:81:27:ec:64:f5:d9:c2:76:46:7a:ed:39:
            dd:77:91:99:a8:1f:ad:fa:a3:2f:a7:44:d8:c3:88:
            09:2f:2a:d5:8e:96:43:2b:d1:b9:ed:23:0d:f4:61:
            41:f8:0d:52:41:64:40:0b:01:63:47:06:d3:81:44:
            32:e8:54:43:f8:5d:fb:24:70:42:df:6c:36:c5:fe:
            de:86:77:7b:91:52:09:b5:c8:b4:e5:02:9b:5b:33:
            7a:02:1d:d8:16:ec:1a:cf:0e:44:e3:d2:c0:39:5d:
            d4:53:97:3e:f2:18:f0:48:75:ec:17:73:67:dc:40:
            80:61:33:22:e8:b2:60:9c:98:4b:82:7f:d9:55:d5:
            8c:cd:fb:9a:05:9f:4c:0d:d6:d2:0d:c1:a4:27:19:
            de:4b:f4:9e:ec:0d:17:c2:73:f7:c4:92:5d:8f:54:
            5b:f6:cd:b3:b4:00:47:4f:75:e5:2e:30:5b:bc:be:
            90:81:bb:bf:3e:cf:75:b8:21:f0:cd:ad:b6:29:ab:
            3a:2c:7f:1a:6f:d4:9d:df:9f:f5:c9:b5:ae:48:7f:
            0d:62:a1:8b:30:28:42:90:aa:9f:61:d1:82:3e:d8:
            ba:66:ac:15:cc:fa:0d:be:09:ff:78:b6:a5:98:77:
            bd:eb:44:3f:08:3a:55:f1:63:4f:4b:1a:40:90:76:
            d1:b2:bb:f4:d3:dc:4c:04:0d:89:72:b0:72:28:fb:
            29:31:31:cb:5c:0e:9a:91:8d:41:3f:3a:12:9e:25:
            7d:c4:7b:c4:d2:dd:66:51:6d:6a:45:79:97:d6:59:
            4a:7b:d7:0c:14:5b:a5:27:9e:bb:3c:c3:8c:db:df:
            e6:db:4b:1b:b4:55:97:8e:fc:bb:29:42:f3:99:ab:
            cc:d9:d2:78:12:81:69:e6:60:c6:6a:23:dd:07:14:
            1a:d0:ec:89:57:9b:b9:82:c0:95:13:f8:3f:7e:da:
            bd:9e:d7:b0:ab:26:38:a4:be:da:34:4f:35:a0:3d:
            69:b5:b4:a6:90:47:e0:bd:31:15:9a:c2:d7:fa:1b:
            94:7e:a5:1e:58:f9:40:19:8b:19:e9:c0:90:80:95:
            18:0d:2c:a0:aa:6d:3e:f1:0d:71:35:30:9f:87:5c:
            56:b2:e9
        Exponent: 65537 (0x10001)
X509v3 extensions:
    Authority Information Access:
```

```
                CA Issuers - URI:http://sub-ca.example.com/sub-ca.crt
                OCSP - URI:http://ocsp.sub-ca.example.com:9081

            X509v3 Authority Key Identifier:
                keyid:07:CE:A9:EE:BA:4B:86:F2:F4:79:05:37:99:59:DD:F3:43:A2:DE:AC

            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://sub-ca.example.com/sub-ca.crl

            X509v3 Extended Key Usage:
                TLS Web Client Authentication, TLS Web Server Authentication
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Subject Key Identifier:
                03:4A:E1:F8:93:95:3A:47:BB:BF:EC:16:4A:66:F6:3A:E3:C1:DB:AE
Certificate is to be certified until Jul  3 16:41:36 2020 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
```

==> ls -al certs

```
total 40
drwxr-xr-x 2 cybersecurity cybersecurity 4096 Jul  4 22:11 .
drwxr-xr-x 5 cybersecurity cybersecurity 4096 Jul  4 21:32 ..
-rw-r--r-- 1 cybersecurity cybersecurity 6900 Jul  4 21:21 7D2B5B7F9F30C3B238C6E51982F0C286.
-rw-r--r-- 1 cybersecurity cybersecurity 7812 Jul  4 21:32 7D2B5B7F9F30C3B238C6E51982F0C287.
-rw-r--r-- 1 cybersecurity cybersecurity 6427 Jul  4 22:01 7D2B5B7F9F30C3B238C6E51982F0C288.
-rw-r--r-- 1 cybersecurity cybersecurity 7937 Jul  4 22:11 7D2B5B7F9F30C3B238C6E51982F0C289.
```

==> openssl x509 -noout -text -in client-example.crt

## Verify client and server certificates

==> cd cert-hier

==> ls -al

```
total 64
drwxr-xr-x 3 cybersecurity cybersecurity 4096 Jul  4 22:11 .
drwxr-xr-x 8 cybersecurity cybersecurity 4096 Jul  4 21:07 ..
```

```
-rw-r--r-- 1 cybersecurity cybersecurity  153 Jul  4 22:06 client-example.conf
-rw-r--r-- 1 cybersecurity cybersecurity 7937 Jul  4 22:11 client-example.crt
-rw-r--r-- 1 cybersecurity cybersecurity 1744 Jul  4 22:09 client-example.csr
-rw------- 1 cybersecurity cybersecurity 3243 Jul  4 22:07 clientkey.key
drwxr-xr-x 5 cybersecurity cybersecurity 4096 Jul  4 21:32 root-ca
-rw-r--r-- 1 cybersecurity cybersecurity  191 Jul  4 21:50 server-coolcompany.conf
-rw-r--r-- 1 cybersecurity cybersecurity 1102 Jul  4 21:52 server-coolcompany.csr
-rw-r--r-- 1 cybersecurity cybersecurity  165 Jul  4 21:58 server-example.conf
-rw-r--r-- 1 cybersecurity cybersecurity 6427 Jul  4 22:01 server-example.crt
-rw-r--r-- 1 cybersecurity cybersecurity 1070 Jul  4 22:00 server-example.csr
-rw------- 1 cybersecurity cybersecurity 1679 Jul  4 21:48 serverkey.key
-rw-r--r-- 1 cybersecurity cybersecurity  451 Jul  4 21:48 serverpubkey.key
```

==> openssl verify -purpose sslserver server-example.crt

```
C = IN, ST = Tamil Nadu, O = Example, OU = Finance, CN = 127.0.0.1, emailAddress = admin@coo
error 20 at 0 depth lookup: unable to get local issuer certificate
error server-example.crt: verification failed
```

==> openssl verify -CAfile root-ca/sub-ca.crt -purpose sslserver server-example.crt

```
C = IN, O = Example, CN = Example SubCA
error 2 at 1 depth lookup: unable to get issuer certificate
error server-example.crt: verification failed
```

OpenSSL complains that it does not know the certificate chain. We need to inform openssl that certain certificates – the root certificate specifically and possibly more – are intrinsically trusted. These trusted certificates are inserted into a trust store.

We create a trust store by concatenating all the certificates in the chain into a single file.

==> cat root-ca/root-ca.crt root-ca/sub-ca.crt > ca-chain.crt

==> cat ca-chain.crt | grep Subject

```
Subject: C=IN, O=Example, CN=Example.com
Subject Public Key Info:
    X509v3 Subject Key Identifier:
Subject: C=IN, O=Example, CN=Example SubCA
Subject Public Key Info:
    X509v3 Subject Key Identifier:
```

Now verify the certificates

==> openssl verify -purpose sslserver -CAfile ca-chain.crt server-example.crt

```
server-example.crt: OK
```

==> openssl verify -purpose sslclient -CAfile ca-chain.crt client-example.crt

```
client-example.crt: OK
```

### Launch client and server

We can now use these certificates to launch a TLS server and client. This is a sample client and server with openssl.

==> openssl s_server -cert server-example.crt -key serverkey.key

Server is now ready to accept connections:

```
Using default temp DH parameters
ACCEPT
```

Lets start the client.

==> openssl s_client

Server throws out a bunch of messages:

```
-----BEGIN SSL SESSION PARAMETERS-----
MHOCAQECAgMEBAITAgQg5Ra8tgXNpuJ0WBjz4duVOkiuZ24SOKH+UE7tdkh19W4E
MBVwxTHT4ezv8BxOnzFI6zFd39yw9nJ3AE/wWoFkJwjFE1HDvzv5B6vbFlnTdgjl
9KEGAgRdHi6LogQCAhwgpAYEBAEAAACuBgIEItzu2Q==
-----END SSL SESSION PARAMETERS-----
Shared ciphers:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256:EC
Signature Algorithms: ECDSA+SHA256:ECDSA+SHA384:ECDSA+SHA512:Ed25519:Ed448:RSA-PSS+SHA256:RS
Shared Signature Algorithms: ECDSA+SHA256:ECDSA+SHA384:ECDSA+SHA512:Ed25519:Ed448:RSA-PSS+SH
Supported Elliptic Groups: X25519:P-256:X448:P-521:P-384
Shared Elliptic groups: X25519:P-256:X448:P-521:P-384
---
No server certificate CA names sent
CIPHER is TLS_AES_256_GCM_SHA384
Secure Renegotiation IS supported
```

This is the TLS session setup information.

The client complains that it cannot verify the authenticity of the server's certificate. We need the trust chain!

```
CONNECTED(00000003)
depth=0 C = IN, ST = Tamil Nadu, O = Example, OU = Finance, CN = 127.0.0.1, emailAddress = a
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 C = IN, ST = Tamil Nadu, O = Example, OU = Finance, CN = 127.0.0.1, emailAddress = a
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:C = IN, ST = Tamil Nadu, O = Example, OU = Finance, CN = 127.0.0.1, emailAddress = admi
   i:C = IN, O = Example, CN = Example SubCA
```

```
---
Server certificate
[server's certificate]
```

Lets terminate the client (hit ^C) and use the chain as the truststore.

==> openssl s_client -CAfile ca-chain.crt

The certificate chain is now verified fine, but there is another error. We will not look

```
CONNECTED(00000003)
depth=2 C = IN, O = Example, CN = Example.com
verify return:1
depth=1 C = IN, O = Example, CN = Example SubCA
verify return:1
depth=0 C = IN, ST = Tamil Nadu, O = Example, OU = Finance, CN = 127.0.0.1, emailAddress = a
verify return:1
---
Certificate chain
 0 s:C = IN, ST = Tamil Nadu, O = Example, OU = Finance, CN = 127.0.0.1, emailAddress = admi
   i:C = IN, O = Example, CN = Example SubCA
---
Server certificate

-----BEGIN CERTIFICATE-----
MIIFaTCCA1GgAwIBAgIQfStbf58ww7I4xuUZgvDCizANBgkqhkiG9w0BAQsFADA3
MQswCQYDVQQGEwJJTjEQMA4GA1UECgwHRXhhbXBsZTEWMBQGA1UEAwwNRXhhbXBs
ZSBTdWJDQTAeFw0xOTA3MDQxNzEwMDlaFw0yMDA3MDMxNzEwMDlaMIGEMQswCQYD
VQQGEwJJTjETMBEGA1UECAwKVGFtaWwgTmFkdTEQMA4GA1UECgwHRXhhbXBsZTEQ
MA4GA1UECwwHRmluYW5jZTESMBAGA1UEAwwJMTI3LjAuMC4xMSgwJgYJKoZIhvcN
AQkBFhlhZG1pbkBjb29sY29tcGFueS5leGFtcGxlMIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEApYvsNUz7XEafTqW+ezLEF6DTCYgBXjYE8X3BmDE16mKt
IkpdGb0PD/A69cpm7rChhU+vtzrXnWBfzbZf/Q/blFsCT+SttiUNJbvOVYYnKz5X
33IaeQQptdylI1r/SHKkiPv70/FcGsQF5uC5Vg7IkY77Zp1oZ+XKrkVM5GsFb2jr
awwF1N57QPknMJQPq0F10TienARJsZxHl+ZwrjV64XkSvVBxU3NJUa/Ac/ch6HWj
mUm3DX/fS2SgTFyjatwfF2zdAKkFLn3b/KtaZRfgdV93snCql74CbxBEKeMxtUu3
lNq6I3VNDLl4dw5lqmWKpcERXG4eliciICAV3palwwIDAQABo4IBITCCARowcQYI
KwYBBQUHAQEEZTBjMDAGCCsGAQUFBzAChiRodHRwOi8vc3ViLWNhLmV4YW1wbGUu
Y29tL3N1Yi1jYS5jcnQwLwYIKwYBBQUHMAGGI2h0dHA6Ly9vY3NwLnN1Yi1jYS5l
eGFtcGxlLmNvbTo5MDgxMB8GA1UdIwQYMBaAFAfOqe66S4by9HkFN5lZ3fNDot6s
MAwGA1UdEwEB/wQCMAAwNQYDVR0fBC4wLDAqoCigJoYkaHR0cDovL3N1Yi1jYS5l
eGFtcGxlLmNvbS9zdWItY2EuY3JsMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA4GA1Ud
DwEB/wQEAwIFoDAdBgNVHQ4EFgQUskXExyr8DlUQe5BnBt7EEs/F1acwDQYJKoZI
hvcNAQELBQADggIBAKLVQ/jl65HeftfJdPGBEzSnOYOKcNWUsI+MEPgzDpH4gcus
56mMkYJrkkWUC+c4LdlqYr29sxV1GGuazYrkfij0MHa7jT5jFkFmP3fKMeLoGs6m
0thcIC+j2kORCJee8GCegjZe+x0ay2SVZ2g7nXnB9MJUiNvesq+2y/xHJwvszLim
rkOMfL2HlkUbHBBkXetzon9/u+8fjLS1Us1SKb6CqSfv3ato9pUprbICfnpg+wXM
```

```
FYinLWTvAPFYxMtHZSpFok+jHro+w/rSGqtRaaAXOBwE7xzTJb4/oJabJRzemgbt
jujVylzhugPQITpHQdiJWOOnv5eYLOGPOpaptQYFPambqdp3SVglw6aeL4TXWVnf
A5oMjwaVDilK5jTl8DgRkj4qa9Qn62ChnAEeFE6ar4oZ7hYVAYBkzHNzaYKtyfFi
PVGTpro9TcOUtzwTRLc0yLmaTh1wHkJGV2X/U16uF43HPn18h9xMUtej7lsNg4Ro
cj7TumAwf9Fb2Ey3HenVFv9jZ892fU0ZoCiUBHy4YlkVnbxPoOYszhKpA0VDvtH9
1qi223zIq5QrFbCigOcGvHAh06mvi/D4BQsVLeAl5hM09+R109lqdf9cvPH2va3V
AKuIvPTcVBHkbk6iYo0WUf5Y6P6g+JK7cCBOdFTB9QPdRCp7s9vETGjzV6Pq
-----END CERTIFICATE-----
subject=C = IN, ST = Tamil Nadu, O = Example, OU = Finance, CN = 127.0.0.1, emailAddress = a

issuer=C = IN, O = Example, CN = Example SubCA

---
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: RSA-PSS
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 1945 bytes and written 391 bytes
Verification: OK
---
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 0 (ok)
---
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol  : TLSv1.3
    Cipher    : TLS_AES_256_GCM_SHA384
    Session-ID: 15B2DD6D76BABE5AF375961EE0C40F7A9DBBB6FE6F811530BE23D6C97FEC01D2
    Session-ID-ctx:
    Resumption PSK: AC5045E1554082E795CE6107712E1C01943182F29A2B7FCD76E44D4C9595D053FF4243E9
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
    0000 - 5e aa 0b 95 a6 b4 01 c9-32 43 01 43 bb 9d c6 fb   ^.......2C.C....
    0010 - b4 e0 20 39 b6 3c 6c ec-ae 82 35 5b 7f 0f 3f 95   .. 9.<l...5[..?.
    0020 - 59 54 69 45 2a 1e be 9d-9f 0b b2 7a 0e 25 17 56   YTiE*......z.%.V
```

```
    0030 - d2 98 b5 62 1e 20 33 e7-7b 10 ae 6d 3b 9d 29 05   ...b. 3.{..m;.).
    0040 - ea 06 ee 88 6b bf 78 48-c5 99 6e 63 19 d1 52 62   ....k.xH..nc..Rb
    0050 - a1 7c 6b 3e 86 75 41 f8-92 b4 97 a9 be ca e2 c8   .|k>.uA.........
    0060 - 3e 40 f5 c4 2f d0 35 db-b7 19 13 80 c5 9c 6e 2c   >@../.5.......n,
    0070 - 87 e6 1e ab e8 bc b6 73-41 78 f8 d0 e0 5e 12 e9   .......sAx...^..
    0080 - 8a d6 e7 3a c5 33 ad 6f-0d ca 29 7b a1 3b d7 85   ...:.3.o..){.;..
    0090 - c4 b3 20 97 4a cc ff ae-66 97 46 9b 3f 02 fc a2   .. .J...f.F.?...
    00a0 - c7 16 51 51 f4 1b 07 e0-f8 29 2b 08 40 94 b0 9a   ..QQ.....)+.@...
    00b0 - 9a e6 3e 77 74 7e 30 09-3e 1c fd b0 96 45 c6 e1   ..>wt~0.>....E..
    00c0 - 3e 1c 38 43 1f 95 c2 59-71 6f 40 62 54 c0 18 8f   >.8C...Yqo@bT...

    Start Time: 1562260669
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol  : TLSv1.3
    Cipher    : TLS_AES_256_GCM_SHA384
    Session-ID: 55EF5206942344ED00C65638750230EC64FC29489D21A4EE549C5F5BC63F4D29
    Session-ID-ctx:
    Resumption PSK: E990FDF5EAEB48300379B4A8E5B44FB0DBE62D7BD3D81A8193167689F28FA70A26EDD9C0
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
    0000 - 5e aa 0b 95 a6 b4 01 c9-32 43 01 43 bb 9d c6 fb   ^.......2C.C....
    0010 - 7a 91 bf 3a fb 4c b5 5a-e9 4f e9 5d 8c 98 43 01   z..:.L.Z.O.]..C.
    0020 - e5 5c 98 33 5b bd 26 50-5f bb f9 64 c7 d7 85 f3   .\.3[.&P_..d....
    0030 - 2a 69 9d 33 cf d2 30 7f-f7 00 fb ed 46 96 38 e0   *i.3..0.....F.8.
    0040 - 1f 87 92 bc 75 1a bc 24-41 3a 13 bf 22 5f 8a df   ....u..$A:.."_..
    0050 - c6 13 b6 c9 8e 5c 24 d8-3e a0 ea 2a e5 3d 9d 9f   .....\$.>..*.=..
    0060 - 55 14 77 10 01 74 c1 66-6b 76 af 39 2d 59 c8 69   U.w..t.fkv.9-Y.i
    0070 - fa 86 4d 37 a2 fe 0c 09-04 bc 38 94 86 b4 d6 8f   ..M7......8.....
    0080 - b7 ff 47 8d 28 78 a7 6b-db 0e bb c0 b8 b9 75 6a   ..G.(x.k......uj
    0090 - e3 0b 80 48 44 37 e2 8e-16 c2 af 9f ea 04 bb bd   ...HD7..........
    00a0 - 94 e4 a6 70 35 ac 46 88-7e 58 dc fc 46 fa 95 05   ...p5.F.~X..F...
    00b0 - 76 00 5b ce a1 0b 0d ac-a9 67 df 75 2f 5e 2f 68   v.[......g.u/^/h
    00c0 - ef dd d2 ee e9 62 c9 e6-f5 47 0b 5e 95 db d0 75   .....b...G.^...u

    Start Time: 1562260669
```

```
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
```

You can now type anything you want and see the messages going through.

You can also have separate certificates for the client and this will be sent to the server as well.

```
Client: openssl s_client -CAfile ca-chain.crt -cert client.crt -key clientkey.key
```

## Looking up Services

Lets look at a few different websites and see their structure. Use the browser to confirm the certificate used.

==> openssl s_client -connect www.google.com:443

```
CONNECTED(00000003)
depth=2 OU = GlobalSign Root CA - R2, O = GlobalSign, CN = GlobalSign
verify return:1
depth=1 C = US, O = Google Trust Services, CN = Google Internet Authority G3
verify return:1
depth=0 C = US, ST = California, L = Mountain View, O = Google LLC, CN = www.google.com
verify return:1
---
Certificate chain
 0 s:C = US, ST = California, L = Mountain View, O = Google LLC, CN = www.google.com
   i:C = US, O = Google Trust Services, CN = Google Internet Authority G3
 1 s:C = US, O = Google Trust Services, CN = Google Internet Authority G3
   i:OU = GlobalSign Root CA - R2, O = GlobalSign, CN = GlobalSign
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIDzzCCAregAwIBAgIQdPYVxCOhXWMVUkOLZFXqnDANBgkqhkiG9w0BAQsFADBU
MQswCQYDVQQGEwJVUzEeMBwGA1UEChMVR29vZ2xlIFRydXN0IFNlcnZpY2VzMSUw
IwYDVQQDExxHb29nbGUgSW50ZXJuZXQgQXV0aG9yaXR5IEczMB4XDTE5MDUyMTIw
MzYyN1oXDTE5MDgxMzIwMzEwMFowaDELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNh
bGlmb3JuaWExFjAUBgNVBAcMDU1vdW50YWluIFZpZXcxEzARBgNVBAoMCkdvb2ds
ZSBMTEMxFzAVBgNVBAMMDnd3dy5nb29nbGUuY29tMFkwEwYHKoZIzj0CAQYIKoZI
zj0DAQcDQgAE+jWY5QtTAGfkOHUOm7aHEVSU2y49257lB3UeYIzQLVUJK0t9povp
PUDLD9O2nQasokEAoraQ2iyhOzQjf+AdSqOCAVIwggFOMBMGA1UdJQQMMAoGCCsG
AQUFBwMBMA4GA1UdDwEB/wQEAwIHgDAZBgNVHREEEjAQgg53d3cuZ29vZ2xlLmNv
bTBoBggrBgEFBQcBAQRcMFowLQYIKwYBBQUHMAKGIWh0dHA6Ly9wa2kuZ29vZy9n
c3IyL0dUU0dJQUczLmNydDApBggrBgEFBQcwAYYdaHR0cDovL29jc3AucGtpLmdv
```

```
b2cvR1RTR0lBRzMwHQYDVR0OBBYEFIE1UfZ0ZyASTNszZS2WKVJ2OEbhMAwGA1Ud
EwEB/wQCMAAwHwYDVR0jBBgwFoAUd8K4UJpndnaxLcKG0IOgfqZ+ukswIQYDVR0g
BBowGDAMBgorBgEEAdZ5AgUDMAgGBmeBDAECAjAxBgNVHR8EKjAoMCagJKAihiBo
dHRwOi8vY3JsLnBraS5nb29nL0dUU0dJQUczLmNybDANBgkqhkiG9w0BAQsFAAOC
AQEAICO5bbLAn9Illlm7Jgp/SDy3otnKvxmNEV2dbyfJaZQocumRfBJqrEHf1eiq
o5AEp+h+yus7QGuy+Rw1e/5f90sQM4GgIAqyv1x9tqsO95+M94yIp1xRXXW4qrUV
2l7OSAifG3BMyp+lCKLcKXnnvHm3upuXlnKu5BrnNOlycbMyNhdZ27TYtqYRDBqr
xsAjvblEqiaRjJVHKQ5Iai4fdbJwpVq3DxgpXyiFrpCC1Hn/Ug5sebCMD1Ic3iVK
7cVAjYybf773LfN7AgQpAWurqvtOAmeeV1SSkXYSW4fXbevkFa1pSKXEtm2mn4QZ
yEUcGFEfuhlMf7MGE9jeUOsSHA==
-----END CERTIFICATE-----
subject=C = US, ST = California, L = Mountain View, O = Google LLC, CN = www.google.com

issuer=C = US, O = Google Trust Services, CN = Google Internet Authority G3

---
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: ECDSA
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 2408 bytes and written 396 bytes
Verification: OK
---
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 256 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 0 (ok)
---
```

Yahoo:

==> openssl s_client -connect www.yahoo.com:443

```
CONNECTED(00000003)
depth=2 C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert High Assurance EV Roo
verify return:1
depth=1 C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert SHA2 High Assurance S
verify return:1
depth=0 C = US, ST = California, L = Sunnyvale, O = Oath Inc, CN = *.www.yahoo.com
verify return:1
---
Certificate chain
```

```
 0 s:C = US, ST = California, L = Sunnyvale, O = Oath Inc, CN = *.www.yahoo.com
   i:C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert SHA2 High Assurance Serv
 1 s:C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert SHA2 High Assurance Serv
   i:C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert High Assurance EV Root C
 2 s:C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert SHA2 High Assurance Serv
   i:C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert High Assurance EV Root C
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIJHzCCCAegAwIBAgIQCJCo+qXyE8vjILXtpTJnkjANBgkqhkiG9w0BAQsFADBw
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMS8wLQYDVQQDEyZEaWdpQ2VydCBTSEEyIEhpZ2ggQXNz
dXJhbmNlIFNlcnZlciBDQTAeFw0xOTA1MDEwMDAwMDBaFw0xOTEwMjgxMjAwMDBa
MGMxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMRIwEAYDVQQHEwlT
dW5ueXZhbGUxETAPBgNVBAoTCE9hdGggSW5jMRgwFgYDVQQDDA8qLnd3dy55YWhv
by5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCkM1GHoSo/9oKj
PqENo9GMbP5yvtXZQoi8doHlLkHOGToMV90U+zKxfobAGYlJYV4kJjCxHXg/8FU0
AYvHVcs+VhicEGaSIUZ6p1T87YqqKC5x7QSUMk+ffmHA0Y75bMqOogmy4o6p+7fq
t4qaW1XHm0a3vXCZNFAz2nrJg3RI8bcCFbdP4mFccHuDH31s9gNJDFKD/qgaB29p
gR+uLOX/T8REDHVDtIfaDHE9WpPxeqdwltDQieGlg4Bm40jJDcHA7u0gpVnlTX77
0JajcqGguTXIpAqQJH14iHDE8oqSvFJF0Hy3xZTl4cn/LqvHBzvdYYMu6RCaKNvG
fqhKJSzvAgMBAAGjggXAMIIFvDAfBgNVHSMEGDAWgBRRaP+QrwIHdTzM2WVkYqIS
uFlyOzAdBgNVHQ4EFgQUrpm7KbnCAMUN1HOkiQNiNVmUAZswggLpBgNVHREEggLg
MIIC3IIPKi53d3cueWFob28uY29tghBhZGQubXkueWFob28uY29tgg4qLmFtcC55
aW1nLmNvbYIMYXUueWFob28uY29tggxiZS55YWhvby5jb22CDGJyLnlhaG9vLmNv
bYIPY2EubXkueWFob28uY29tghNjYS5yb2dlcnMueWFob28uY29tggxjYS55YWhv
by5jb22CEGRkbC5mcC55YWhvby5jb22CDGRlLnlhaG9vLmNvbYIUZW4tbWFrdG9v
Yi55YWhvby5jb22CEWVzcGFub2wueWFob28uY29tggxlcy55YWhvby5jb22CD2Zy
LWJlLnlhaG9vLmNvbYIWZnItY2Eucm9nZXJzLnlhaG9vLmNvbYISZnJvbnRpZXIu
eWFob28uY29tggxmci55YWhvby5jb22CDGdyLnlhaG9vLmNvbYIMaGsueWFob28u
Y29tgg5oc3JkLnlhaG9vLmNvbYIXaWRlYW5ldHNldHRlci55YWhvby5jb22CDGlk
LnlhaG9vLmNvbYIMaWUueWFob28uY29tggxpbi55YWhvby5jb22CDGl0LnlhaG9v
LmNvbYIRbWFrdG9vYi55YWhvby5jb22CEm1hbGF5c2lhLnlhaG9vLmNvbYIMbWJw
LnlpbWcuY29tggxteS55YWhvby5jb22CDG56LnlhaG9vLmNvbYIMcGgueWFob28u
Y29tggxxYy55YWhvby5jb22CDHJvLnlhaG9vLmNvbYIMc2UueWFob28uY29tggxz
Zy55YWhvby5jb22CDHR3LnlhaG9vLmNvbYIMdWsueWFob28uY29tggx1cy55YWhv
by5jb22CEXZlcml6b24ueWFob28uY29tggx2bi55YWhvby5jb22CDXd3dy55YWhv
by5jb22CCXlhaG9vLmNvbYIMemEueWFob28uY29tgg9oay5yZC55YWhvby5jb22C
D3R3LnJkLnlhaG9vLmNvbTAOBgNVHQ8BAf8EBAMCBaAwHQYDVR0lBBYwFAYIKwYB
BQUHAwEGCCsGAQUFBwMCMHUGA1UdHwRuMGwwNKAyoDCGLmh0dHA6Ly9jcmwzLmRp
Z2ljZXJ0LmNvbS9zaGEyLWhhLXNlcnZlci1nNi5jcmwwNKAyoDCGLmh0dHA6Ly9j
cmw0LmRpZ2ljZXJ0LmNvbS9zaGEyLWhhLXNlcnZlci1nNi5jcmwwTAYDVR0gBEUw
QzA3BglghkgBhv1sAQEwKjAoBggrBgEFBQcCARYcaHR0cHM6Ly93d3cuZGlnaWNl
cnQuY29tL0NQUzAIBgZngQwBAgIwgYMGCCsGAQUFBwEBBHcwdTAkBggrBgEFBQcw
AYYYaHR0cDovL29jc3AuZGlnaWNlcnQuY29tME0GCCsGAQUFBzAChkFodHRwOi8v
Y2FjZXJ0cy5kaWdpY2VydC5jb20vRGlnaUNlcnRTSEEySGlnaEFzc3VyYW5jZVNl
```

```
cnZlckNBLmNydDAMBgNVHRMBAf8EAjAAMIIBAwYKKwYBBAHWeQIEAgSB9ASB8QDv
AHYA7ku9t3XOYLrhQmkfq+GeZqMPfl+wctiDAMR7iXqo/csAAAFqdMSsygAABAMA
RzBFAiEA+x2otregfacyFT3PRD33cgNQWIi4yrR0kBAtnCZsn2kCIDrHp/xP6zwD
dsGqEjSINAE9jmKrgo/elELKjftwT83lAHUAh3W/51l8+IxDmV+9827/Vo1HVjb/
SrVgwbTq/16ggw8AAAFqdMSt5gAABAMARjBEAiAB4YV22p0U22BJh5roMLNgx+Ms
h2VIEz0Jz56BSmtv6gIgP2dSVn2gw61bntjp9yGGR14Lyj5Q+LwTlVXmvNrlW1sw
DQYJKoZIhvcNAQELBQADggEBALAFKLcI0WP4KM5SSnQniOi0Y3lVaVCRsEX40aIp
2vA1oPnrN+Y1ZvheFnZXfT2wlfbvEW4RBIT2NBm7z+adVldZ+lQE56qgng+Tab/j
bccWlpHioITDQHkILEZEi4jpD6L3A55OfJtOtanYF4ZriagYW7XUmaHGsKEgAJ7N
OsqsXud1I8L/DYkokttQnbiPvl+3jNnwlq4vbHvYJMBHTr9vwUJHRpLyGkpD7cwn
FRqHMK/+/gxjRr+GgNgA5UwjptyEwzfiXlHpOgYhawSS/pJphxjpNpnwbfozwo4j
ThR/tNqj9qhqwdtKQKNYEhyQNipodImwdKGcDIOC77cgj/A=
-----END CERTIFICATE-----
subject=C = US, ST = California, L = Sunnyvale, O = Oath Inc, CN = *.www.yahoo.com

issuer=C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert SHA2 High Assurance Se

---
No client certificate CA names sent
Peer signing digest: SHA512
Peer signature type: RSA
Server Temp Key: ECDH, P-256, 256 bits
---
SSL handshake has read 5461 bytes and written 441 bytes
Verification: OK
---
New, TLSv1.2, Cipher is ECDHE-RSA-AES128-GCM-SHA256
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES128-GCM-SHA256
    Session-ID: 76FB83457B0CE42A7F7CDBD0F50BD61571AEAC775FE14C4EBB71A14D9EC1A480
    Session-ID-ctx:
    Master-Key: 401286615C602006D81ECDD084B315F9E4E82D191D7B47E505BC6D9A13625870202B086ECB61
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
    0000 - fe 50 93 c2 15 c5 09 58-7e 15 72 c2 57 99 d6 7a   .P.....X~.r.W..z
    0010 - 57 e4 83 5c 97 ff fd 83-67 d7 20 d5 9d d6 15 91   W..\....g. .....
    0020 - f5 8b 5a 9c 7a 80 db 7b-f3 17 36 fd 9d a3 3d b2   ..Z.z..{..6...=.
```

```
    0030 - 8c ec ab b8 0c 82 b8 35-41 8a 87 c7 1f 53 2e 34   .......5A....S.4
    0040 - 6b be c6 d2 a4 ba 3b af-8e 5b 8b 89 78 56 70 67   k.....;..[..xVpg
    0050 - fe 73 96 6e ca 10 5f 88-ce e1 3e 5d 6b 4b 75 ba   .s.n.._...>]kKu.
    0060 - cb fc d3 a2 9f bf 2f 04-9e 59 31 70 6f 21 6b 63   ....../..Y1po!kc
    0070 - 89 3d 03 06 9a 3c da 72-33 37 37 a7 f2 0f a5 6f   .=...<.r377....o
    0080 - a1 08 66 49 e7 81 7d c8-17 87 27 a4 d7 6a 14 6d   ..fI..}...'..j.m
    0090 - e4 38 fd 63 cf 20 4f be-39 ec a2 75 d9 bb 74 b8   .8.c. O.9..u..t.
    00a0 - ba 72 7c b3 9a 62 90 29-9b 28 45 0b 42 19 4a c8   .r|..b.).(E.B.J.
    00b0 - b4 3d 22 59 a8 ae a8 da-20 b8 22 6b 95 b2 44 91   .="Y.... ."k..D.
    00c0 - a7 4b d6 dc ce 9e 50 7b-dc 09 9e 43 fb e7 e0 dd   .K....P{...C....

    Start Time: 1560830113
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
    Extended master secret: no
---
^C
```

### The Green Lock Test

You can compare the cert downloaded via openssl to the cert information you get from the browser. Download the certificate from the browser's Green Lock.

==> openssl x509 -in yahoo.crt -text -noout

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            08:90:a8:fa:a5:f2:13:cb:e3:20:b5:ed:a5:32:67:92
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert SHA2 High Ass
        Validity
            Not Before: May  1 00:00:00 2019 GMT
            Not After : Oct 28 12:00:00 2019 GMT
        Subject: C = US, ST = California, L = Sunnyvale, O = Oath Inc, CN = *.www.yahoo.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:a4:33:51:87:a1:2a:3f:f6:82:a3:3e:a1:0d:a3:
                    d1:8c:6c:fe:72:be:d5:d9:42:88:bc:76:81:e5:2e:
                    41:ce:19:3a:0c:57:dd:14:fb:32:b1:7e:86:c0:19:
                    89:49:61:5e:24:26:30:b1:1d:78:3f:f0:55:34:01:
                    8b:c7:55:cb:3e:56:18:9c:10:66:92:21:46:7a:a7:
                    54:fc:ed:8a:aa:28:2e:71:ed:04:94:32:4f:9f:7e:
                    61:c0:d1:8e:f9:6c:ca:8e:a2:09:b2:e2:8e:a9:fb:
```

```
            b7:ea:b7:8a:9a:5b:55:c7:9b:46:b7:bd:70:99:34:
            50:33:da:7a:c9:83:74:48:f1:b7:02:15:b7:4f:e2:
            61:5c:70:7b:83:1f:7d:6c:f6:03:49:0c:52:83:fe:
            a8:1a:07:6f:69:81:1f:ae:2f:45:ff:4f:c4:44:0c:
            75:43:b4:87:da:0c:71:3d:5a:93:f1:7a:a7:70:96:
            d0:d0:89:e1:a5:83:80:66:e3:48:c9:0d:c1:c0:ee:
            ed:20:a5:59:e5:4d:7e:fb:d0:96:a3:72:a1:a0:b9:
            35:c8:a4:0a:90:24:7d:78:88:70:c4:f2:8a:92:bc:
            52:45:d0:7c:b7:c5:94:e5:e1:c9:ff:2e:ab:c7:07:
            3b:dd:61:83:2e:e9:10:9a:28:db:c6:7e:a8:4a:25:
            2c:ef
        Exponent: 65537 (0x10001)
X509v3 extensions:
    X509v3 Authority Key Identifier:
        keyid:51:68:FF:90:AF:02:07:75:3C:CC:D9:65:64:62:A2:12:B8:59:72:3B

    X509v3 Subject Key Identifier:
        AE:99:BB:29:B9:C2:00:C5:0D:D4:73:A4:89:03:62:35:59:94:01:9B
    X509v3 Subject Alternative Name:
        DNS:*.www.yahoo.com, DNS:add.my.yahoo.com, DNS:*.amp.yimg.com, DNS:au.yahoo
    X509v3 Key Usage: critical
        Digital Signature, Key Encipherment
    X509v3 Extended Key Usage:
        TLS Web Server Authentication, TLS Web Client Authentication
    X509v3 CRL Distribution Points:

        Full Name:
          URI:http://crl3.digicert.com/sha2-ha-server-g6.crl

        Full Name:
          URI:http://crl4.digicert.com/sha2-ha-server-g6.crl

    X509v3 Certificate Policies:
        Policy: 2.16.840.1.114412.1.1
          CPS: https://www.digicert.com/CPS
        Policy: 2.23.140.1.2.2

    Authority Information Access:
        OCSP - URI:http://ocsp.digicert.com
        CA Issuers - URI:http://cacerts.digicert.com/DigiCertSHA2HighAssuranceServer

    X509v3 Basic Constraints: critical
        CA:FALSE
    CT Precertificate SCTs:
        Signed Certificate Timestamp:
            Version   : v1 (0x0)
```

```
                Log ID    : EE:4B:BD:B7:75:CE:60:BA:E1:42:69:1F:AB:E1:9E:66:
                            A3:0F:7E:5F:B0:72:D8:83:00:C4:7B:89:7A:A8:FD:CB
                Timestamp : May  1 19:00:07.498 2019 GMT
                Extensions: none
                Signature : ecdsa-with-SHA256
                            30:45:02:21:00:FB:1D:A8:B6:B7:A0:7D:A7:32:15:3D:
                            CF:44:3D:F7:72:03:50:58:88:B8:CA:B4:74:90:10:2D:
                            9C:26:6C:9F:69:02:20:3A:C7:A7:FC:4F:EB:3C:03:76:
                            C1:AA:12:34:88:34:01:3D:8E:62:AB:82:8F:DE:94:42:
                            CA:8D:FB:70:4F:CD:E5
            Signed Certificate Timestamp:
                Version   : v1 (0x0)
                Log ID    : 87:75:BF:E7:59:7C:F8:8C:43:99:5F:BD:F3:6E:FF:56:
                            8D:47:56:36:FF:4A:B5:60:C1:B4:EA:FF:5E:A0:83:0F
                Timestamp : May  1 19:00:07.782 2019 GMT
                Extensions: none
                Signature : ecdsa-with-SHA256
                            30:44:02:20:01:E1:85:76:DA:9D:14:DB:60:49:87:9A:
                            E8:30:B3:60:C7:E3:2C:87:65:48:13:3D:09:CF:9E:81:
                            4A:6B:6F:EA:02:20:3F:67:52:56:7D:A0:C3:AD:5B:9E:
                            D8:E9:F7:21:86:47:5E:0B:CA:3E:50:F8:BC:13:95:55:
                            E6:BC:DA:E5:5B:5B
    Signature Algorithm: sha256WithRSAEncryption
         b0:05:28:b7:08:d1:63:f8:28:ce:52:4a:74:27:88:e8:b4:63:
         79:55:69:50:91:b0:45:f8:d1:a2:29:da:f0:35:a0:f9:eb:37:
         e6:35:66:f8:5e:16:76:57:7d:3d:b0:95:f6:ef:11:6e:11:04:
         84:f6:34:19:bb:cf:e6:9d:56:57:59:fa:54:04:e7:aa:a0:9e:
         0f:93:69:bf:e3:6d:c7:16:96:91:e2:a0:84:c3:40:79:08:2c:
         46:44:8b:88:e9:0f:a2:f7:03:9e:4e:7c:9b:4e:b5:a9:d8:17:
         86:6b:89:a8:18:5b:b5:d4:99:a1:c6:b0:a1:20:00:9e:cd:3a:
         ca:ac:5e:e7:75:23:c2:ff:0d:89:28:92:db:50:9d:b8:8f:be:
         5f:b7:8c:d9:f0:96:ae:2f:6c:7b:d8:24:c0:47:4e:bf:6f:c1:
         42:47:46:92:f2:1a:4a:43:ed:cc:27:15:1a:87:30:af:fe:fe:
         0c:63:46:bf:86:80:d8:00:e5:4c:23:a6:dc:84:c3:37:e2:5e:
         51:e9:3a:06:21:6b:04:92:fe:92:69:87:18:e9:36:99:f0:6d:
         fa:33:c2:8e:23:4e:14:7f:b4:da:a3:f6:a8:6a:c1:db:4a:40:
         a3:58:12:1c:90:36:2a:68:74:89:b0:74:a1:9c:0c:83:82:ef:
         b7:20:8f:f0
```