# Generating certificates

You can generate certificates to use withTLS using a third-party tool such as OpenSSL or Keytool.

This guide explains how to useOpenSSL to generate certificates when the Common Name (CN) is either thepublic DNS or anIP address . Before you begin, ensure OpenSSL is installed.

## Public DNS as CN

Follow these steps to use a public DNS as CN.

### Generating a CA certificate

1. Generate a key file calledtessera_ca.key
2. :
3. openssl genrsa -out tessera_ca.key 2048
4. Generate a certificate authority (CA) certificate calledtessera_ca.pem
5. that usestessera_ca.key
6. :
7. openssl req -x509 -new -nodes -key tessera_ca.key -sha256 -days 1024 -out tessera_ca.pem

### Generating a new certificate for a node

We recommend each node has its own certificate. To generate the certificate:

1. Generate a key file calledtessera_cer.key
2. :
3. openssl genrsa -out tessera_cer.key 2048
4. Generate a certificate signing request (CSR) calledtessera_cer.csr
5. :
6. openssl req -new -key tessera_cer.key -out tessera_cer.csr
7. Answer each prompt for information to be added to the certificate request. Ensure the value you specify for CN matches the host public DNS so the requests from the server are accepted. The name is also specified in the configuration file for thenodeurl
8. andclienturl
9. options.

info If running onlocalhost , make surelocalhost is specified in CN. 1. Generate a certificate calledtessera_cer.pem 2. signed by the CA certificate: 3. openssl x509 -req -in tessera_cer.csr -CA tessera_ca.pem -CAkey tessera_ca.key -CAcreateserial -out tessera_cer.pem -days 500 -sha256

## IP address as CN

Follow these steps to use a public IP address as CN.

### Updating theopenssl.cnf

file

1. Find theopenssl.cnf
2. file, and create a copy of it.
3. In your copy of theopenssl.cnf
4. file, find the[req]
5. section, and add:
6. req_extensions = v3_req
7. [ v3_req ]
8. basicConstraints = CA:FALSE
9. keyUsage = nonRepudiation, digitalSignature, keyEncipherment
10. subjectAltName = @alt_names
11. [alt_names]
12. DNS.1 =
13. DNS.2 =
14. IP.1 =
15. IP.2 =
16. For each DNS you want to use as an alternate name, specify aDNS.n
17. entry.
18. For each IP address you want as an alternate IP address, specify anIP.n

19. entry.
20. note
21. When running onlocalhost
22. , include127.0.0.1
23. as a listed IP address.

## Generating a new CSR for a node

1. Run the following command. Substitute your values for all variables.
2. openssl req -new -key tessera_cer.key -out tessera_cer.csr -config/openssl.cnf

3. Test whether the certificate was generated with the expected subject alternative names:

4. Command

5. Output example

openssl req -text -noout -in tessera_cer.csr [...] Requested Extensions: X509v3 Subject Alternative Name: DNS:, DNS:, IP Address:, IP Address: [...]

## Generating a new certificate

1. Run the following command. Substitute your values for all variables.
2. openssl x509 -req -in tessera_cer.csr -CA tessera_ca.pem -CAkey tessera_ca.key -CAcreateserial -out tessera_cer.pem -days 500 -sha256 -extfile /openssl.cnf -extensions v3_req

3. Test whether the generated certificate contains the subject alternative names:

4. Command

5. Output example

openssl x509 -in tessera_cer.pem -text -noout [...] X509v3 extensions: X509v3 Subject Alternative Name: DNS:, DNS:, IP Address:, IP Address: [...] Edit this page Last updatedonNov 29, 2023 byJoshua FernandesPrevious AWS Secrets Manager keys Next Configure