How to create a self signed or official ssl tls certificate without questions asked (non-interactive) on the command line interface

Goal:

- create a x509 server certificate for use in TLS (ssl)
- self signed (not official, not trusted by default)
- includes multiple alternative (alias) DNS hostnames (virtual hosts)
- includes administrative email contact
- create new or reuse a host's private key
- non interactive (no questions asked)
- no passphrases for private key
- works on UBUNTU 20.04 LTS and similar

Generate self signed server certificate incl. new private key

To create a new private key + self signed certificate use:

```
openssl req \
  -x509 \
  -sha256 \
  -nodes  \
  -days 3650 \
  -newkey rsa:4096 \
  -keyout youtHostnameHere.key \
  -out youtHostnameHere.SELFSIGNED.$(date +%F).crt \
  -subj
"/C=CountryCode/ST=StateCode/L=LocationCity/O=yourOrganisationOrFqdn/OU=your
OrganisationalUnitOrFqdn/CN=your.FqdnHost.name/emailAddress=your@email.tld/"
\
  -addext subjectAltName=DNS:www.your.FqdnHost.name \
  -addext 'subjectAltName=DNS:*.your.FqdnHost.name' \
  -addext subjectAltName=DNS:more.FqdnHost.name
```

To read/show a certificate in human readable format use:

```
openssl x509 -text -noout -in yourNewCertificateFileToDisplay | more
```

Generate (unprotected) private key only:

```
openssl genrsa -out yourFqdnHostname.key 2048
```

To view/show private key in a more human readable format use:

```
openssl rsa -text -in ourFqdnHostname.key  | more
```

Request official server certificate using existing private key (csr)

```
openssl req \
  -new \
  -key yourKeyFile.key \
  -out youtHostnameHere.SELFSIGNED.$(date +%F).crt \
  -subj
"/C=CountryCode/ST=StateCode/L=LocationCity/O=yourOrganisationOrFqdn/OU=your
OrganisationalUnitOrFqdn/CN=your.FqdnHost.name/emailAddress=your@email.tld/"
\
  -addext subjectAltName=DNS:www.your.FqdnHost.name \
  -addext 'subjectAltName=DNS:*.your.FqdnHost.name' \
  -addext subjectAltName=DNS:more.FqdnHost.name
```

To view/show CSR in human readable format use:

```
openssl req -text -noout -in yourCsrFileHere.csr | more
```

Self sign a given csr

WARNING: This does NOT pass through the alternative DNS hostnames to the certificate!!! Also the `-addext` option is not available within x509 context. So this section is mostly useless atm. For better control set up a full blown CA and use the `openssl ca` context instead.

```
openssl x509 \
  -req
  -sha256
  -days 3650
  -in yourCsrFileHere.csr
  -signkey yourKeyFile.key
  -out youtHostnameHere.SELFSIGNED.$(date +%F).crt
```

---

linux, cli, crt, csr, key, openssl, ca, certificate, ssl, tls, cli, command, line, commandline