openssl

See cert info

```
openssl x509 -in cert.crt -text -noout
```

Basic use to create self-signed certificate

```
# Generate SSL private key self signed certificate for 10 years
openssl req -x509 -newkey rsa:4096 -sha256 -keyout server.key -out cert.crt -days 3650 -nodes
```

Create request to sign in some trusted CA

```
openssl req -out server.csr -new -sha256 -newkey rsa:4096 -nodes -keyout server.key
cat server.csr
```

than submit CSR to CA

Create request if key already exist

```
openssl req -new -key server.key -out server.csr
```

non-interactive mode example

```
openssl req -new -key server.key -out server.csr -subj "/C=UA/ST=Kyiv/L=Kyiv/O=Company Name/OU=Department name
/CN=example.com" -passin pass:password -passout pass:password
```

Check request

```
openssl req -text -noout -verify -in server.csr
```

Check and use certificate

```
# see the certificate
openssl x509 -in cert.crt -text -noout

# combine certificate and key in pem keypair file
cat server.key server.crt > keypair.pem
```

Check SSL connection

```
openssl s_client -connect server.example.com:443
```

Convert password protected p12 to pem

```
openssl pkcs12 -in key-with-password.p12 -passin pass:password -out key-with-password.pem
```

Remove password from PEM private ssl key

```
openssl rsa -in key-with-password.pem -out key.pem
```