1. generate the private key:

```
$ openssl genrsa -des3 -out company-ca.key 2048
```

Be very careful with that one, it must have a password and must never be transmitted.

2. now create the (self-signed) CA certificate itself:

```
$ openssl req -new -x509 -days 3650 -subj '/C=CH/ST=SO/L=SO/O=IT/CN=Company' -key company-ca.key -out company-ca.crt
```

3. Create server certificate

```
$ openssl genrsa -des3 -out server.key 2048

$ openssl rsa -in server.key -out server.key

$ openssl req -new -nodes -key server.key -days 3650 -out /tmp/server.csr -subj '/C=CH/ST=SO/L=SO/O=IT/CN=server.domain.net'

$ openssl x509 -days 3650 -req -in /tmp/server.csr -CA company-ca.crt -CAkey company-ca.key -CAcreateserial -out server.crt
```

4. Create client certificate

```
$ openssl genrsa -des3 -out client.key 2048

$ openssl rsa -in client.key -out client.key

$ openssl req -new -nodes -key client.key -days 3650 -out /tmp/client.csr -subj '/C=CH/ST=SO/L=SO/O=IT/CN=*.domain.net'

$ openssl x509 -days 3650 -req -in /tmp/client.csr -CA company-ca.crt -CAkey company-ca.key -CAcreateserial -out client.crt
```