# HowTo generate a CSR


2020-06-06

# Contents

# 1 Certificate Signing Requst (CSR)

The CSR is needed by a Certificate Authorithy (CA) to sign the public key.

The basic usage is:

- Create your own private key
- Create with this private key a CSR
- Send your CSR to CA
- CA signs your public key and returns it to you

# 2 Creating a CSR

There are quite a few ways to create a CSR.

For inexpierenced user we recommend using the open source gui xca [https://www.hohnstaedt.de/xca/index.php/download] (https://www.hohnstaedt.de/xca/index.php/download). See HowTo use XCA for a detailed description.

For people using a command line tool OpenSSL Source Code is recommended which is already installed in most Unix distributions. For Windows it is available in CygWin for Windows.

The following line will generate a new private key and the CSR.

```
openssl req -new -newkey rsa:4096 -nodes -keyout mykey.key -out mycsr.csr
```

You will get this output on your screen:

```
# Generating a 2048 bit RSA private key
# ..............................................++++++
# ............................++++++
# writing new private key to 'privkey.pem'
# -----
# You are about to be asked to enter information that will be incorporated
# into your certificate request.
# What you are about to enter is what is called a Distinguished Name or a DN.
# There are quite a few fields but you can leave some blank
# For some fields there will be a default value,
# If you enter '.', the field will be left blank.
# -----
```

Afterwards you are prompted for some information. Please leave most of them empty as our CA is not using it or they may cause problems signing the public key.

```
# Country Name (2 letter code) [AU]:
# State or Province Name (full name) [Some-State]:
# Locality Name (eg, city) []:
# Organization Name (eg, company) [Internet Widgits Pty Ltd]:
# Organizational Unit Name (eg, section) []:
```

Depending wether your are creating a client certificate or a server certificate add either your name as given in your account or your domain name.

```
# Common Name (eg, YOUR name) []:example.com
# Email Address []:
```

Do not fill the next prompts.

```
# Please enter the following 'extra' attributes
# to be sent with your certificate request
# A challenge password []:
# An optional company name []:
```

Now the private key ‘mykey.key’ and the csr ‘mycsr.csr’ are available.