Generating a Certificate Signing Request (CSR) using Apache

A CSR is a file containing your certificate application information, including your Public Key.

Generate keys and certificate:

To generate a pair of private key and public Certificate Signing Request (CSR) for a webserver, "server", use the following command:

      openssl req -new -nodes -keyout myserver.key -out server.csr

This creates two files. The file myserver.key contains a private key; do not disclose this file to anyone. Carefully protect the private key.

In particular, be sure to backup the private key, as there is no means to recover it should it be lost. The private key is used as input in the command to generate a Certificate Signing Request (CSR).

You will now be asked to enter details to be entered into your CSR
.
What you are about to enter is what is called a Distinguished Name or a DN.

For some fields there will be a default value, If you enter '.', the field will be left blank.

```
-----
Country Name (2 letter code) [AU]: HK
State or Province Name (full name) [Some-State]: Hong Kong or N/A
Locality Name (eg, city) []:Hong Kong
Organization Name (eg, company) [Internet Widgits Pty Ltd]: MyCompany Ltd
Organizational Unit Name (eg, section) []: IT
Common Name (eg, YOUR name) []: mysubdomain.mydomain.com
Email Address []:
```

Please enter the following 'extra' attributes to be sent with your certificate request

```
A challenge password []:
An optional company name []:
-----
```

Use the name of the webserver as Common Name (CN). If the domain name is mydomain.com append the domain to the hostname (use the fully qualified domain name).

The fields **email address**, **optional company name** and **challenge password** can be left blank for a webserver certificate.

Your CSR will now have been created.