Certificate Generation With XCA

If you aren't able (or willing) to setup openssl on your windows machine, there are various GUI wrappers around the toolset which you might be able to use instead. XCA is an open source wrapper around the OpenSSL toolset which allows you to create keys, csrs and certificates via a GUI and stores all of the generated items in a database file.

First you need to download XCA, which is an open source wrapper around the openssl toolset from:
http://sourceforge.net/projects/xca/

Step by Step Guide

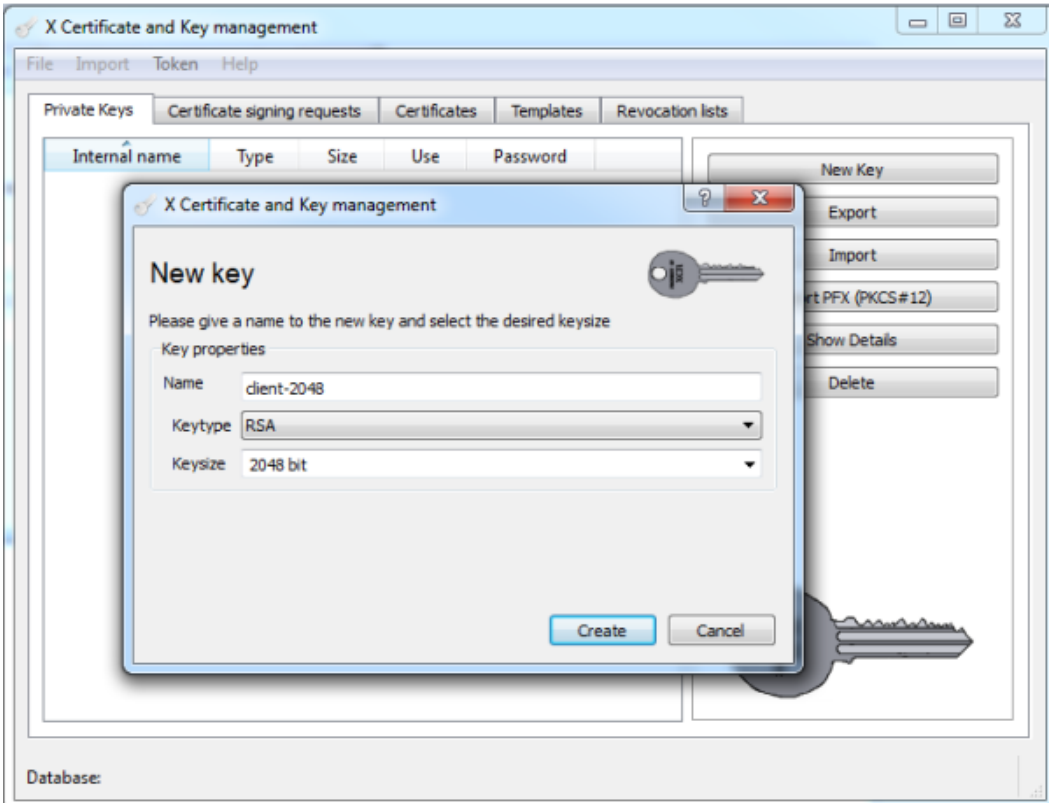
1. Install XCA and run it.
2. Create a new Database,
3. Name it something sensible
4. Save it somewhere appropriate.

This proprietary database is useful for the xca tool only and helps you store your keys, csrs, and certificates, the database file is not used in any part of the process with Betfair.

Equivalent Open SSL Command - Create a public/private RSA key pair using openssl

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

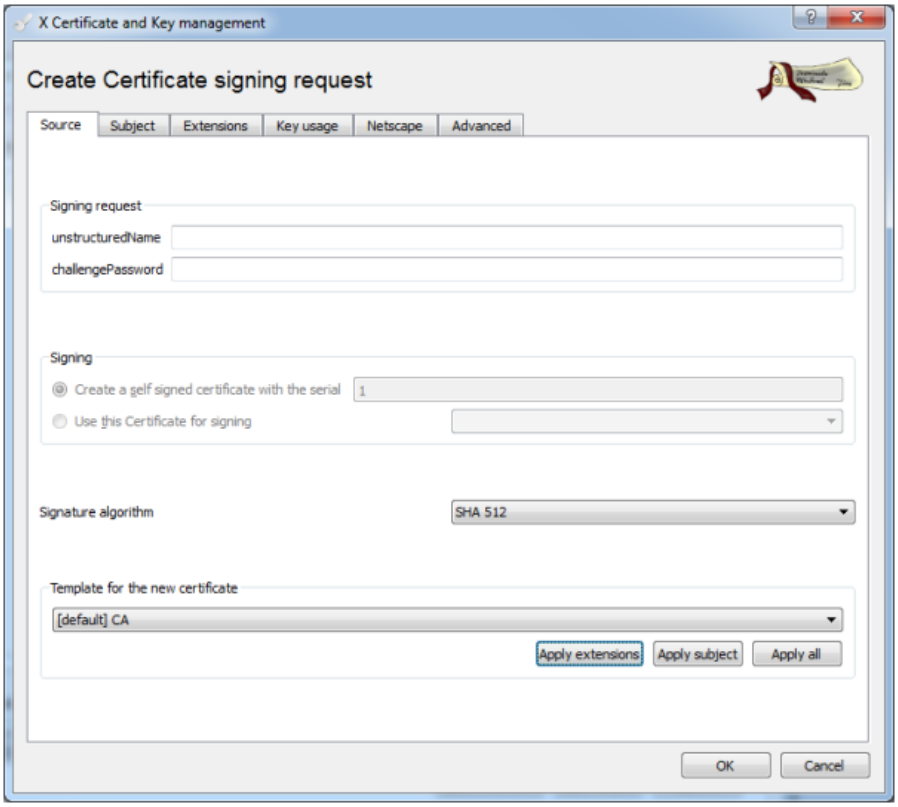
- Create a public/private RSA key pair using xca:



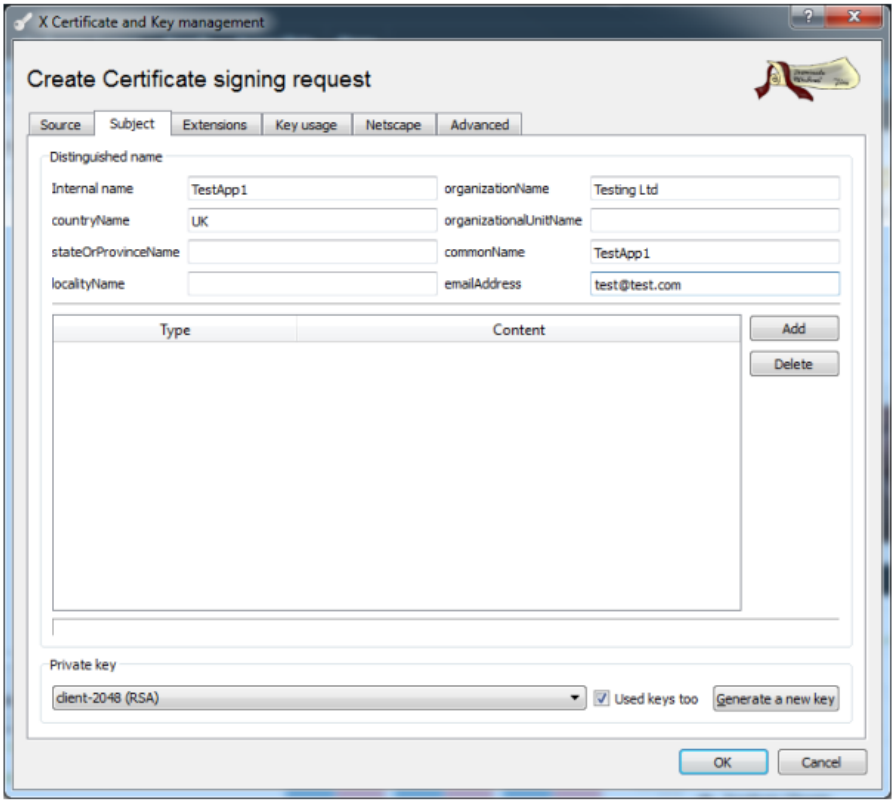
Equivalent Open SSL Command - Create a certificate signing request (CSR).

```
openssl req -new -config openssl.cnf -key client-2048.key -out client-2048.csr
```

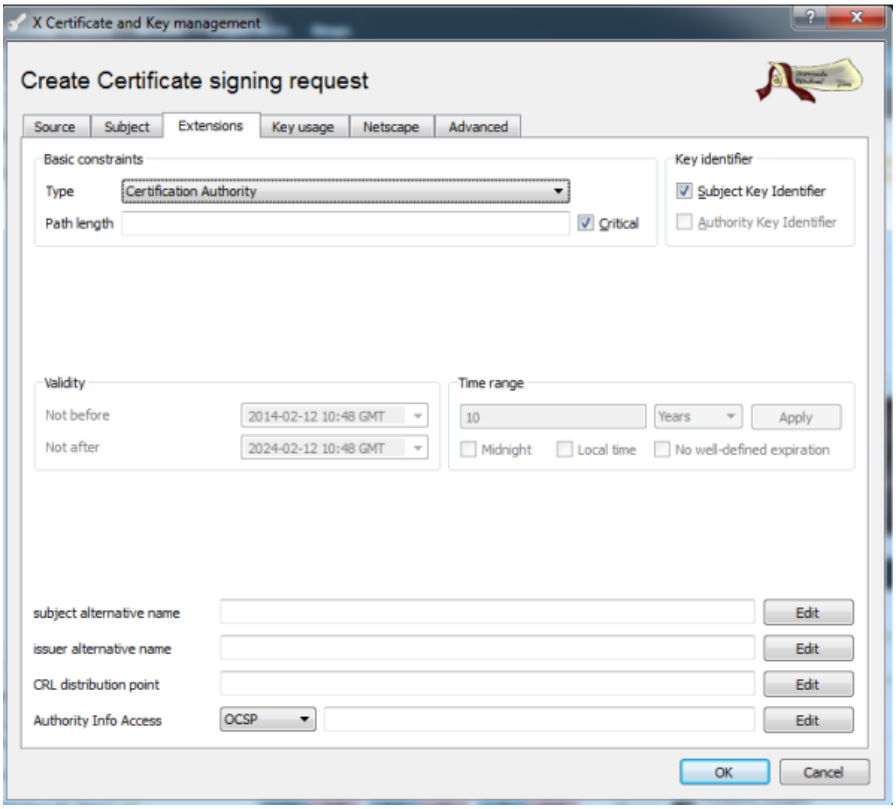
- Select the Certificate signing requests tab and click **New Request**
- Select the CA template and click the **Apply Extensions** button.



- Click on the **Subject** tab and enter the name etc.
- The key that you generated in the first step must be selected (if the key doesn't appear, check the "Used keys tool" box)



- Click on the **Extensions** tab
- Ensure that **Certification Authority** is selected as the type.
- Click OK.

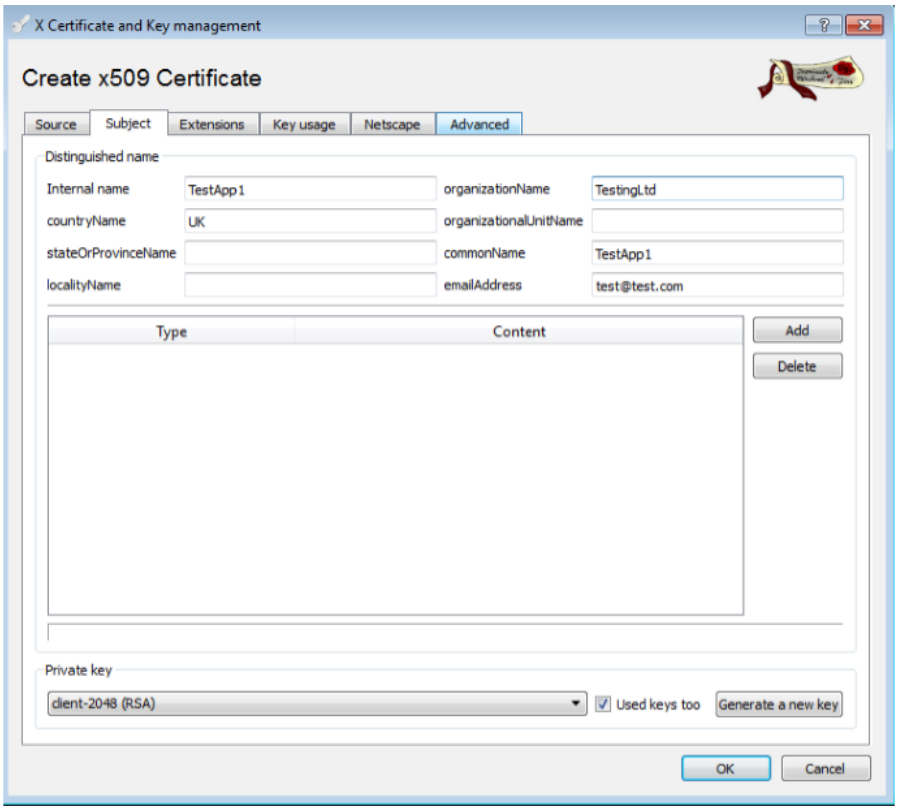


Equivalent Open SSL Command - Self-sign the certificate request to create a certificate

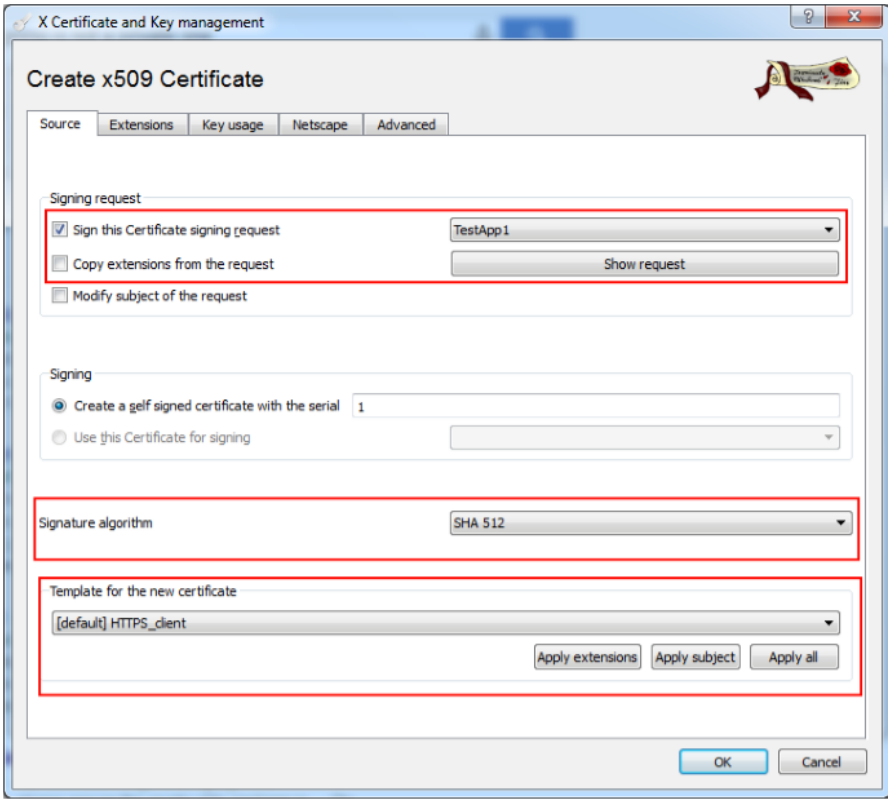
```
openssl x509 -req -days 365 -in client-2048.csr -signkey client-2048.key -out client-2048.crt -extfile openssl.cnf -extensions ssl_client
```

We will now create and sign a certificate from the first two steps:

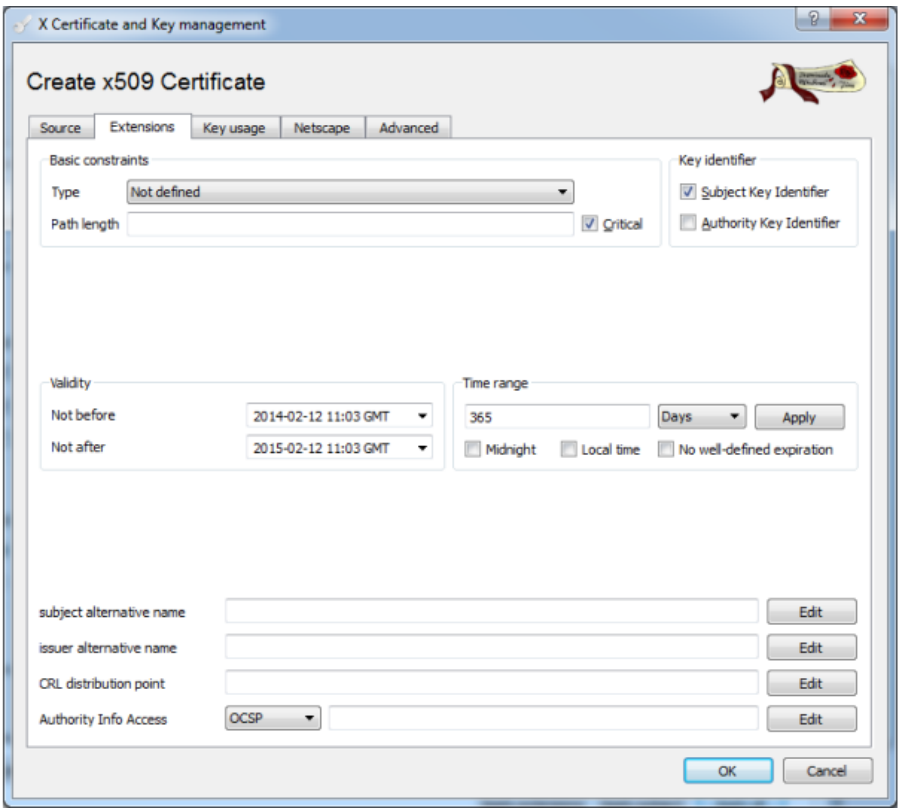
- Click the Certificates Tab and click New Certificate
- Click on the **Subject** tab and enter the name etc.
- The key that you generated in the first step must be selected (if the key doesn't appear, check the "Used keys tool" box)



- Click on the **Source** tab and select the parameters shown below:



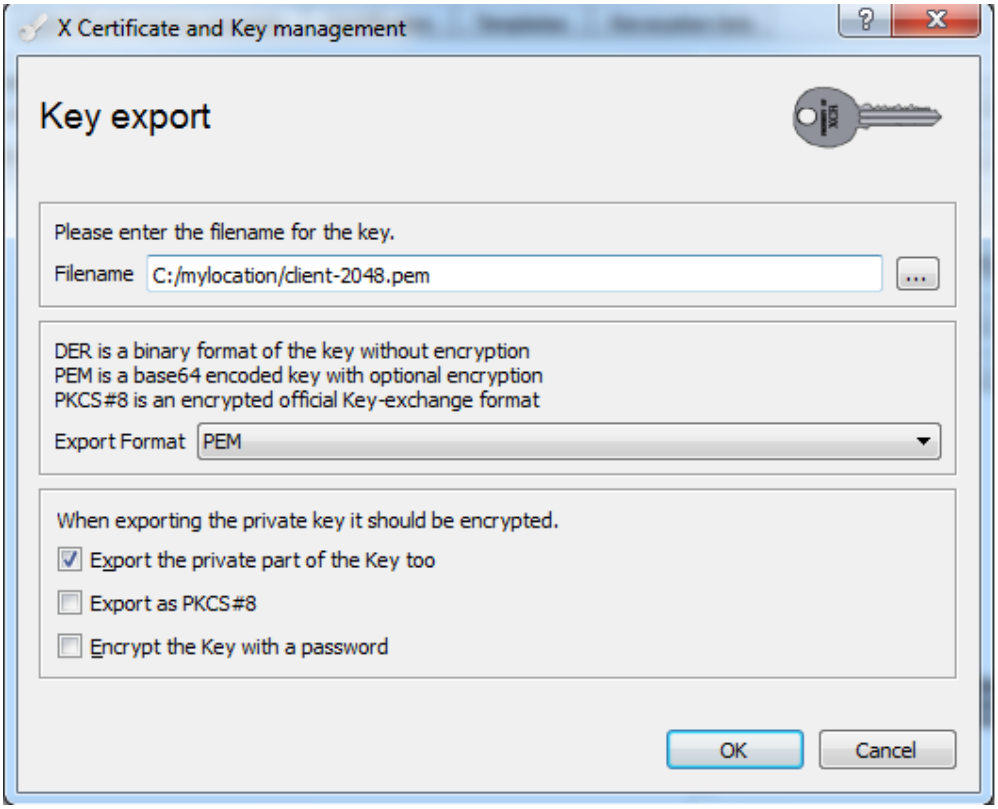
- You should make sure that your CSR is selected but that “Copy extensions from the request” is unticked and that you have selected the [default] HTTPS_client and pressed the “Apply extensions” button.

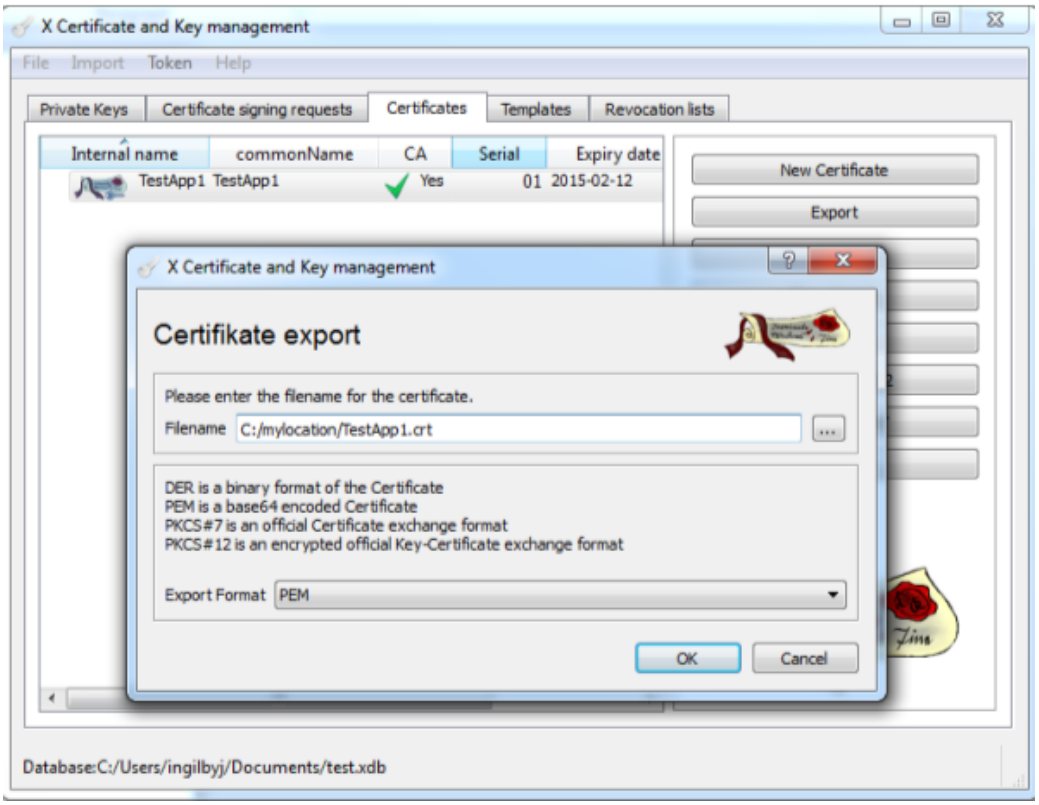


You can then press OK to create the self-signed certificate.

Next we need to export the key and the certificate for use in our application.

- Export the private key and Certificate. These files should be used in the authentication process and should be referred to in your code where the private key (the .pem file) and certificate file (the .crt file) are mentioned. You can also export to other formats such as PKCS 12 depending upon the format expected by your language/library of choice.





You should upload the .crt file exported to the My Security page on Betfair.com to allow this certificate access to your account.