How To Create Self-Signed Certificate?

1- Download and Install XAMPP.

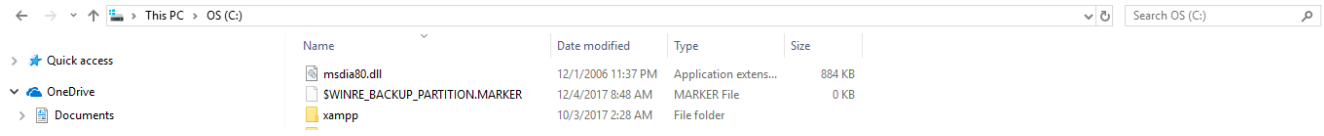
XAMPP is a completely free tool to create local web server, easy to install Apache distribution containing MariaDB, PHP, and Perl. The XAMPP open source package has been set up to be incredibly easy to install and to use.

2- OpenSSL

OpenSSL is a robust, commercial-grade, and full-featured toolkit for the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols. It is also a general-purpose cryptography library.

OpenSSL is licensed under an Apache-style license, which basically means that you are free to get and use it for commercial and non-commercial purposes subject to some simple license conditions.

The XAMPP has openssl as default as enabled when the installation completed. Then we have to go to the folder of xampp where it was installed.



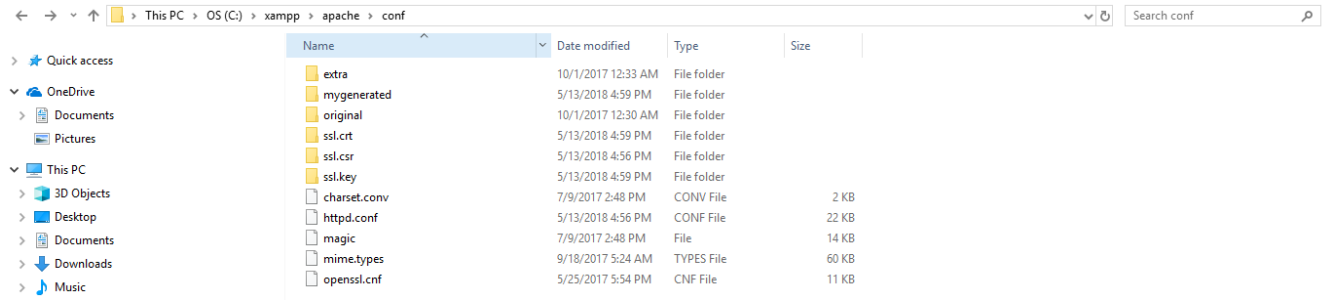
First, we have to run the command line interface.

In this command line interface, we have to test if the openssl is install or not.

If everything is okey, it gives us the date of the openssl is installed on our system then we can continue. Otherwise we have to install openssl.

Firstly in the xampp folder we have to go to the folder as follows

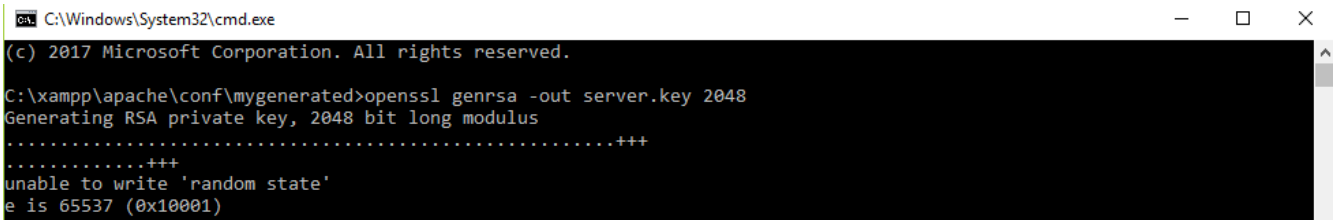
- xampp → apache → conf



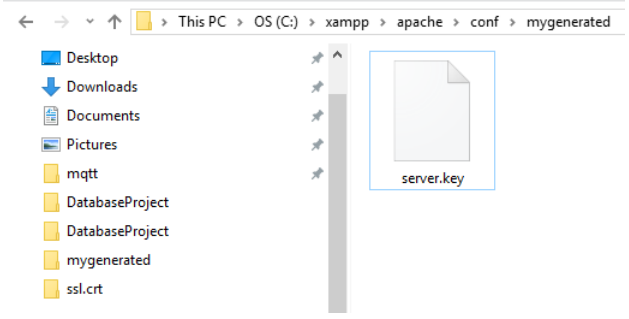
In this folder as we can see we have ssl.crt folder to store the ssl certificates and we have ssl.key folder to store the private keys that we will generate. But I created another folder to create my certificate so I put a name to folder “mygenerated”. Lets navigate to this folder and run cmd in this folder.

Hint (Keys = CTLR + D)

Then in this command line interface we have to first write the commands as follows to create private key.



Then as you can see in the figure below, it will generate a file called server.key and this file will include the private key that generated.



Explanation of the commands:

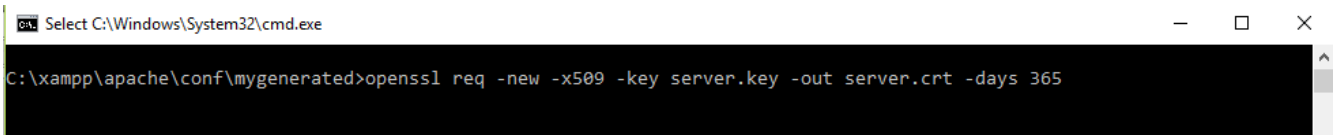
openssl = it is a tool and we will use it to create certificate

genrsa = that means generate a private key

-out server.key = is the name of the file will be created to hold the private key

2048 = means 2048 bit, it is a type of the private key that we will generated

Then in this command line interface we have to write another command that will create certificate.



-new -x509 = the command to create self-signed certificates

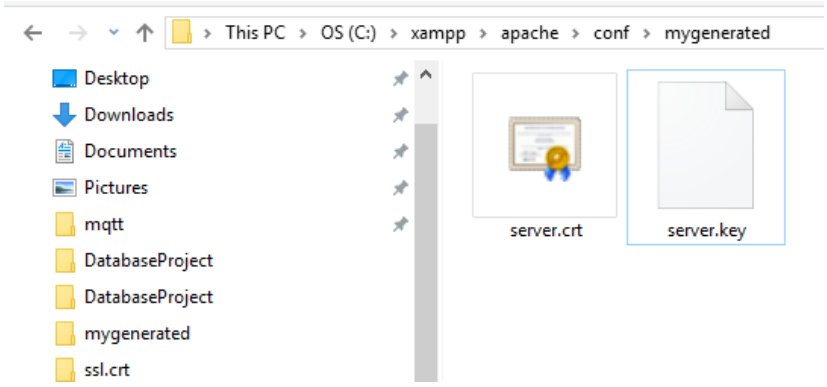
-key server.key = the private key file

-out server.crt = the certificate file will be generated

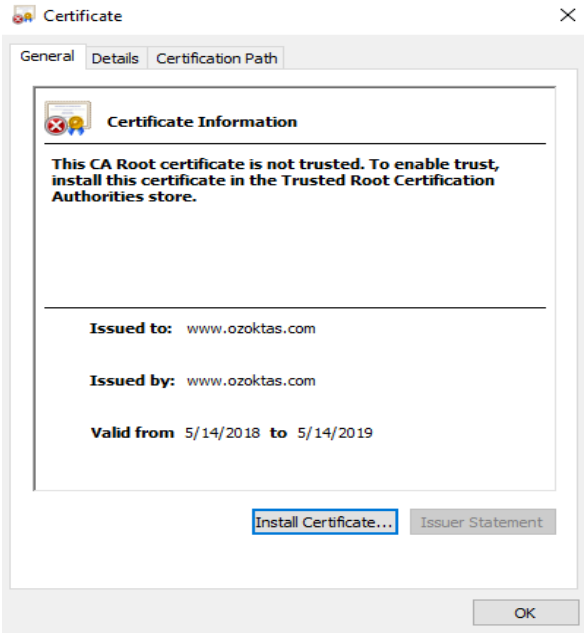
-days 365 = the days we want to be sure that this certificate will be valid

Then it will asked the information we want to put to this certificate.

Then as you can see in the figure below, it will generate a certificate based on the given private key file.

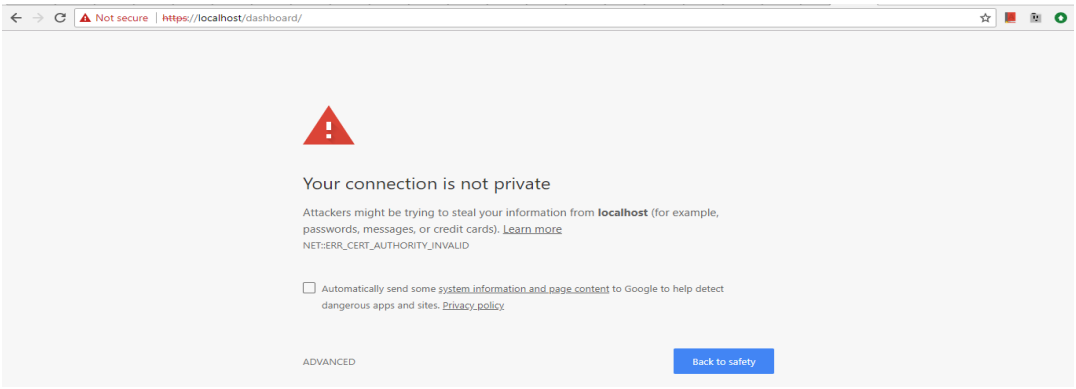


When we click to the created certificate it gives us the information about it.



After all, we have to put the server.key file into the folder “ssl.key” in the folder of xampp/apache/conf and server.crt file into the folder “ssl.crt”.

Then if we try to go the **https://localhost** from our browser it will say that “Your connection is not private”.



If we click to the **NET::ERR_CERT_AUTHORITY_INVALID** it will explain us what is the problem as you can see in the figure below.