***OpenSSL – Certificate Creation***

To implement any server that will transfer using HTTPS, you need a certificate. OpenSSL is one way to creates keys and certificates

Steps

openssl genrsa -out key.pem

openssl req -new -key key.pem -out csr.pem

openssl x509 -req -days 9999 -in csr.pem -signkey key.pem -out cert.pem

rm csr.pem

<https://nodejs.org/en/knowledge/HTTP/servers/how-to-create-a-HTTPS-server/>

***Another method:***

|  |  |
| --- | --- |
| ***Commands*** | ***Description*** |
| openssl | Will open an session of openSSL  Note: A OpenSSL > prompt will be displayed |
| genrsa -out ca.key 4096 | Step #1:  Generate the key  (here a file name ***ca.key*** will be created) |
| req -new -x509 -days 1826 -key ca.key -out ca.crt | Step #2:  Create certificate from key file  (from the ***ca.key***, it will create a ***ca.crt*** certificate file)  1826 is the number of days the certificate will be valid (5 years) |
| genrsa -out ia.key 4096 |  |
| req -new -key ia.key -out ia.csr |  |
| X509 -req -days 730 -in ia. |  |

Video: <https://www.youtube.com/watch?v=zwnEmLx2LRs>

Web Site: <https://blog.didierstevens.com/2008/12/30/howto-make-your-own-cert-with-openssl/>

This version appears to produce a certificate correctly dough…

openssl req -newkey rsa:2048 -nodes -keyout key.pem -x509 -days 365 -out certificate.pem

openssl x509 -text -noout -in certificate.pem

<https://www.cloudinsidr.com/content/how-to-install-the-most-recent-version-of-openssl-on-windows-10-in-64-bit/>

***OpenSSL – C Programming***

Also, OpenSSL comes with a library, to facilitate the secure communication.

### Here is a site with code example (*Section OpenSSL API Examples*):

<https://fm4dd.com/openssl/>

Note: In Visual Studio, make sure to

1 - Point the VC++ directories (include and lib) respectively to:

* C:\Program Files\OpenSSL-Win64\include
* C:\Program Files\OpenSSL-Win64\lib

2 – Configure the linker  (Config Properties/Linker/input) and point to lib name:

*capi.lib*

*dasync.lib*

*libapps.lib*

*libcrypto.lib*

*libcrypto\_static.lib*

*libssl.lib*

*libssl\_static.lib*

*libtestutil.lib*

*openssl.lib*

*ossltest.lib*

*padlock.lib*

*uitest.lib*

                Check is there are a bit less lib file required...

***Free Certificate Generation (Web equivalent of OpenSSL)***

<https://fm4dd.com/openssl/>

***NodeJS &https***

[**https://adamtheautomator.com/https-nodejs/**](https://adamtheautomator.com/https-nodejs/)

Note Aug 2023: it can works on my CBSA machine, but it gives a security warning…