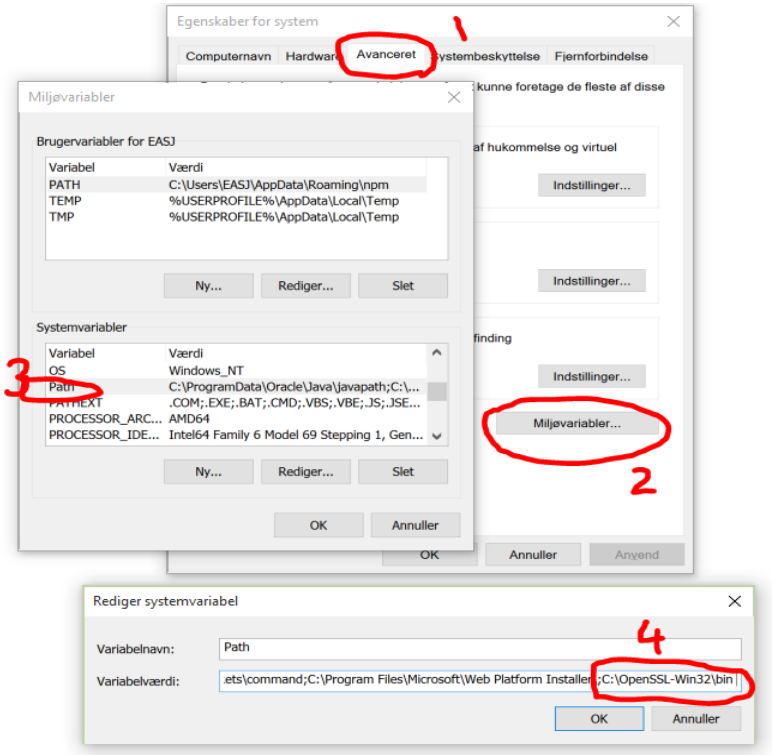
Week 38 Labs

Lab5

The following steps will enable you to create your own certificate on a windows machine using OpenSSL command line tool.

1. First, download OpenSSL tool. From : https://slproweb.com/products/Win32OpenSSL.html if it still works otherwise search for "OpenSSL for windows"
2. Unzip it anywhere on your computer and Install it.
3. **Open cmd 'windows command prompt' and type openssl if it works then skip the steps 4-12**
4. Add the path to **openssl/bin** directory to your path variable.
5. (What do you mean?). "hmmm back to nursery".
6. I mean! If you have unzipped/put your openssl in **C:** drive then the path to its bin directory will be **C:\openssl\bi**n OR **C:\Program Files\openssl\bin** OR **C:\OpenSSLwin32\bin ….**
7. Put this path to your windows path variable. (Where can I find it?)
8. Press the windows key and R key (this will bring up the run box)
9. Type in **sysdm.cpl** OR **control sysdm.cpl** and press Ok
10. In this new window choose Advance and then Click on Environment variables
11. On newer versions of windows you can click on new button to put a new path
12. In the system variable window double click the path variable and append a semicolon and the path to your openssl/bin (for example; C**:\OpenSSL-Win32\bin**) directory to it.
13. Click OK, OK and Ok



(Were those steps necessary?) “No. Not at all”. It will enable you to run openssl from any directory you run your **cmd (command line tool)** from.

You can run the windows **cmd** from a particular directory/folder by **Right clicking** in the directory/folder while keeping the **Shift key** down. Now choose **Open Command window here**.

This way you can create your keys/certificate exactly where you want it.

Now you are ready to create your private public keys. Type the following in your command window. There is an error on this line correct it. You can find information about OpenSSL commands here: https://www.openssl.org/docs/manmaster/apps/openssl.html

Openssl –req –x509 –days 365 –newkey rsa:2048 –keyout my-private-key.pem –out my-cert.pem

- Explain the above openssl command, the options and other params
- Find five more openssl options and explain them
- FIX the ERROR; If you encounter an ERROR: unable to write random state

Now execute the following command

openssl pkcs12 –export –in my-cert.pem –inkey my-private-key.pem –out my-keys-container.pfx

- Explain the above openssl command, the options and other params

Now Run the following command and Explain, in detail, what does it do?

openssl pkcs12 -in my-keys-container.pfx -clcerts -nokeys -out my-public-cert-key.pem