

COMPUTING SUBJECT:	Certificates for SSL
TYPE:	Assignment
IDENTIFICATION:	CertificateX509
COPYRIGHT:	<i>Michael Claudius</i>
LEVEL:	Medium
TIME CONSUMPTION:	1-2 hours
EXTENT:	50 lines
OBJECTIVE:	Windows SDK, makecert, pvk2pfx, mmv
PRECONDITIONS:	Computer Networking Ch. 8.5
COMMANDS:	

IDENTIFICATION: CertificateX509/MC

Mission

You are to make a secure connection communication by setting up a server and a client using the secure socket layer (SSL) by sharing the certificate provided by the server. This we shall do in three steps/assignments:

1. CertificateX509 No. 1, Install Windows SDK and investigate the tools *makecert* and *pvk2pfx*
2. CertificateX509 No.2, Create CertificateX509, self-signed X509 Root and Server SSL certificates
3. Secure SocketsC#, Use the certificates and SSLStream for secure socket communication

This assignment is the first Assignment No.1

Purpose

The purpose of this assignment is to install Windows SDK and learn about the tools *mmc*, *makecert* and *pvk2pfx*.

When surfing on the net it is easy to find many descriptions more or less useful, and in more or less updated versions. Here are some:

Useful links for C#:

How to install Window SDK for Windows 10 / 11

<https://dev.windows.com/en-us/downloads/windows-10-sdk>

View certificates using the tool mmc snap in/out

[https://msdn.microsoft.com/en-us/library/ms788967\(v=vs.110\).aspx](https://msdn.microsoft.com/en-us/library/ms788967(v=vs.110).aspx) ;

Description of makecert tool:

[https://msdn.microsoft.com/en-us/library/ms733813\(v=vs.110\).aspx](https://msdn.microsoft.com/en-us/library/ms733813(v=vs.110).aspx)

Description of of pvk2pfx tool:

[https://msdn.microsoft.com/en-us/library/windows/hardware/ff550672\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/hardware/ff550672(v=vs.85).aspx)

Link describing opening command prompt used by Visual studio

[https://msdn.microsoft.com/da-dk/library/ms229859\(v=vs.110\).aspx](https://msdn.microsoft.com/da-dk/library/ms229859(v=vs.110).aspx)

Useful links for Java: Keytool

Solaris Programmers tool to create keys

[Keytool - Key and Certificate Management Tool](#)

Windows Programmers tool to create keys in Java

[Keytool – Key and Certificate Management Tool](#)

1. Install Windows SDK kit

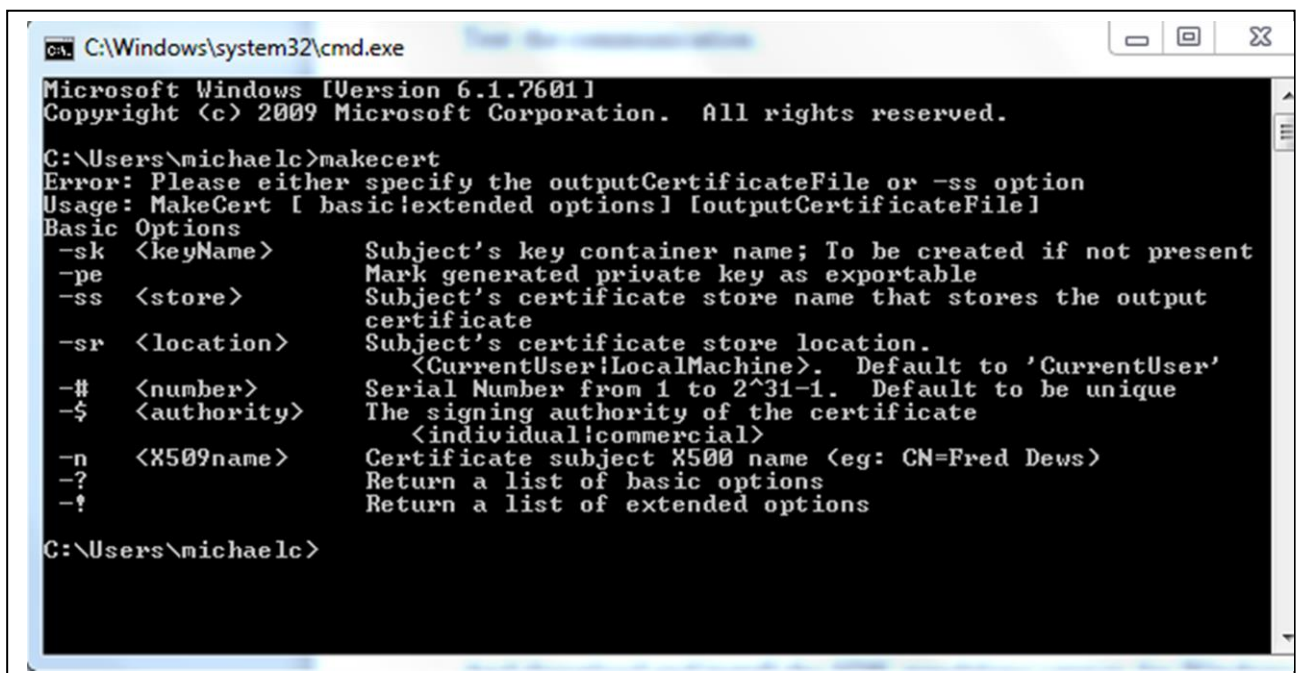
To be able to create certificates for secure socket communication one must use the tool *makecert* and *pvk2pfx* as defined in Window SDK. Therefore you need to install Window SDK for Windows 10/11 if it is not already installed.

First check that you can run *makecert* from the command prompt.

Start a dos-prompt.

Just Start -> cmd

Give the command *makecert*:



```
cmd. C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\michaelc>makecert
Error: Please either specify the outputCertificateFile or -ss option
Usage: MakeCert [ basic|extended options] [outputCertificateFile]
Basic Options
-sk <keyName>      Subject's key container name; To be created if not present
-pe              Mark generated private key as exportable
-ss <store>       Subject's certificate store name that stores the output
                  certificate
-sr <location>    Subject's certificate store location.
                  <CurrentUser!LocalMachine>. Default to 'CurrentUser'
-# <number>       Serial Number from 1 to 2^31-1. Default to be unique
-$ <authority>    The signing authority of the certificate
                  <individual!commercial>
-n <X509name>     Certificate subject X500 name (eg: CN=Fred Dews)
-?              Return a list of basic options
-!              Return a list of extended options

C:\Users\michaelc>
```

Also try to check out the *pvk2pfx* command in the same way.

If it works all is fine and you just jump to next assignment.

If a command is not recognized you must check if you have SDK installed and then change the environment variable Path.

****To be repeated****

Lookup the paths:

C:\Program Files\Windows Kits\10.0\bin\x64)

C:\Program Files (x86)\Windows Kits\10\bin\10.0.19041.0\x64

Or something similar and see if you can recognize the application *makecert* and *pv2pfx*.

IF YES:

Set your environment variable Path to include present working directory (.) and your folder with the Windows SDK it (e.g.

C:\Program Files\Windows Kits\10.0\bin\x64

C:\Program Files (x86)\Windows Kits\10\bin\10.0.19041.0\x64

Then try to run commands again.

For more details see the Appendix (at the end of the assignment) on Environmental variables.

IF NO:

Use the link:

<https://developer.microsoft.com/en-us/windows/downloads/sdk-archive>

And download and install the SDK standalone version for Windows 10 or 11.
Then repeat the instructions given above.

2. Investigate makecert and pvk2pfx tools

What is the purpose of *makecert* ?

Explain the various options like -sky -n -r etc.

What is the purpose of *pvk2pfx* ?

Explain the various options like -pvk -f etc.

Wonder how many of these are important.....

Tip: Make use of the following links

Description of *makecert* tool:

[https://msdn.microsoft.com/en-us/library/ms733813\(v=vs.110\).aspx](https://msdn.microsoft.com/en-us/library/ms733813(v=vs.110).aspx)

Description of *pvk2pfx*:

[https://msdn.microsoft.com/en-us/library/windows/hardware/ff550672\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/hardware/ff550672(v=vs.85).aspx)

3. Certificate repository

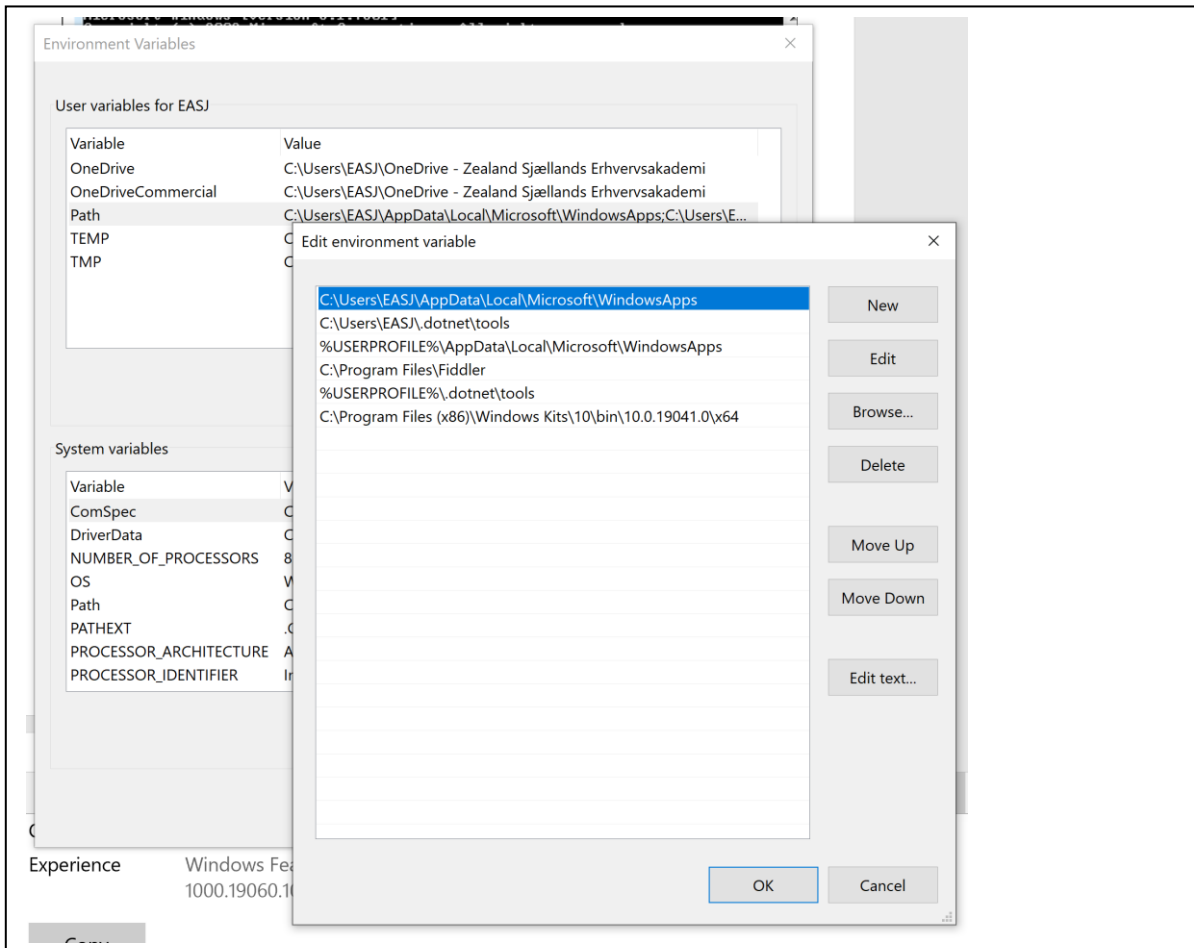
Use both the Internet browser and the tool *mmc snap in/out* to find out which certificates you already have on your computer.

View certificates: [https://msdn.microsoft.com/en-us/library/ms788967\(v=vs.110\).aspx](https://msdn.microsoft.com/en-us/library/ms788967(v=vs.110).aspx) ;

Guess you will be surprised!

Environmental variables PATH and CLASSPATH

1. Select Start -> Control panel
2. Choose System Security -> System
3. Find the Setting Environment Variables, choose **Path**, and click on it.



4. In the Edit windows, modify **Path** by creating new paths with the location of the files to be added.
If you do not have the item **Path**, you may select to add a new variable and add **Path** as the name and the location of the class as the value. Remember the semicolons as splitter characters!
5. Click OK everywhere
6. Reopen Command prompt window, and do the assignment again

Maybe you will have to restart your computer....

Comments to teacher

I found pvk2pfx in C:\Program Files (x86)\Windows Kits\10\bin\10.0.19041.0\x86