COMPUTING SUBJECT:	Certificates for SSl
TYPE:	Assignment
IDENTIFICATION:	CertificateX509
COPYRIGHT:	*Michael Claudius*
LEVEL:	Medium
TIME CONSUMPTION:	1-2 hours
EXTENT:	50 lines
OBJECTIVE:	Windows SDK, makecert, pvk2pfx, mmc
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, Install Windows SDK and investigate the tools *mmc, makecert* & *pvk2pfx*
2. CreateCertificateX509, Create self-signed X509 Root and Server SSL certificates
3. Secure SocketsC#, Use the certificates and SSLStream for secure socket communication

This assignment is the Assignment No.1

Purpose

The purpose of this assignment is to install Windows SDK and learn about the tools *mmc*, *makecer*t 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
https://developer.microsoft.com/da-dk/windows/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 ;

Description of makecert tool:
https://docs.microsoft.com/en-us/windows/win32/seccrypto/makecert

Description of of pvk2pfx tool:
https://docs.microsoft.com/en-us/windows-hardware/drivers/devtest/pvk2pfx

Link describing opening command prompt used by Visual studio
https://msdn.microsoft.com/da-dk/library/ms229859(v=vs.110).aspx

Description of thumbprint
https://www.thesslstore.com/blog/ssl-certificate-still-sha-1-thumbprint/

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, see if you can find a path like:

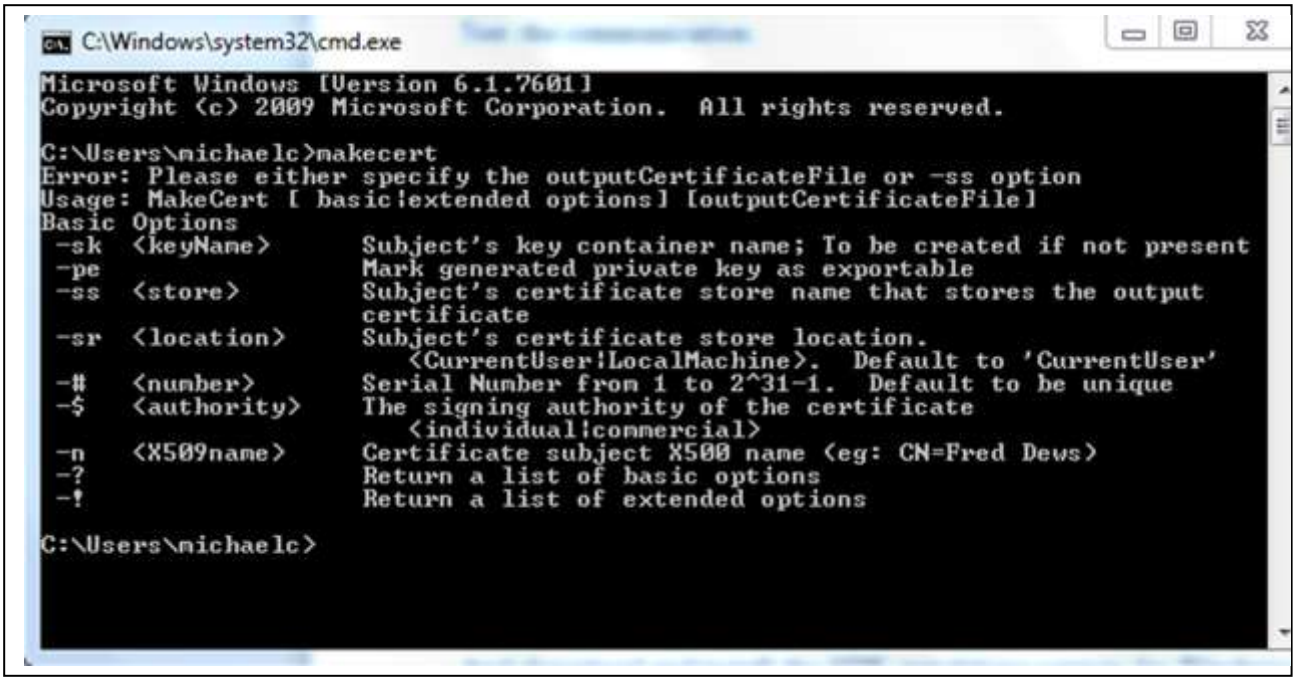
C:\Program Files(x86)\Windows Kits\10\bin\10.0.xxxx\x64 (xxxx=fx18041)

If not install Window SDK for Windows 10, if you have not done it already. Use the link:

https://developer.microsoft.com/da-dk/windows/downloads/windows-10-sdk/

And download and install the SDK standalone version for Windows 10.

Then check that you can access and run *makecert* from the command prompt.
Start a command-prompt.
Click Start -> Programs -> Accessories -> Command prompt
Or just Start -> cmd
Give the command *makecert:*



Also try to check out the *pvk2pfx* command in the same way. If a command is not recognized you must change the environment variables PATH (Path) and maybe CLASSPATH.

A) Set your environment variable Path to include present working directory (.) and your folder with the Windows SDK it (e.g. C:\Program Files(x86)\Windows Kits\10.0\bin\x64)
F*or more details; See the Appendix on environment variables at the end of this document.*

Maybe

B) Set your environment variable CLASSPATH to include the folder (working directory '.' - dot). Not in Windows 10!.

2. Investigate makecert and pvk2pfx tools

What is the purpose of *makecert* ?
Explain the various options like -sk -n -sr 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://docs.microsoft.com/en-us/windows/win32/seccrypto/makecert

Description of *pvk2pfx*:
https://docs.microsoft.com/en-us/windows-hardware/drivers/devtest/pvk2pfx

3. Certificate repository

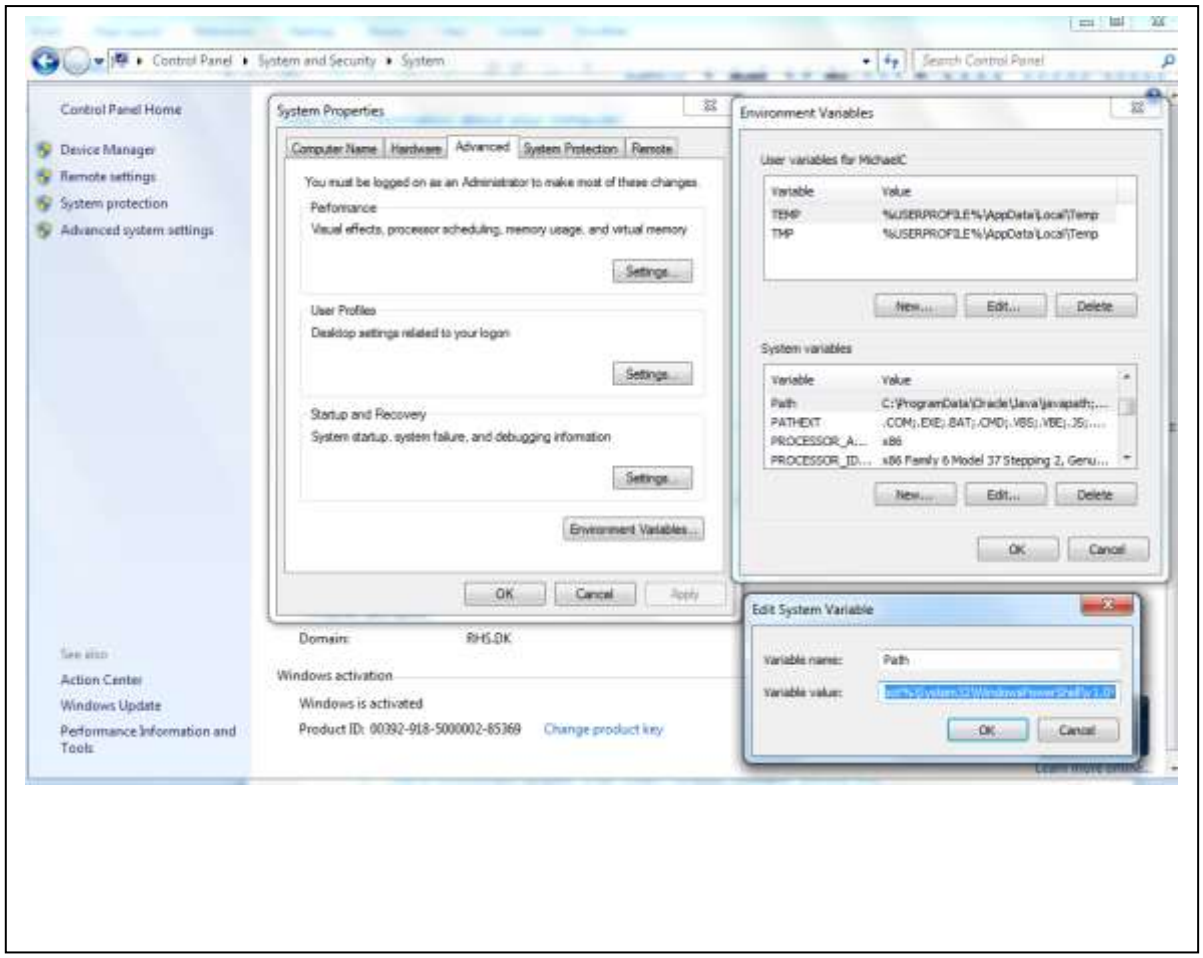
Use both the Internet browser and/or the tool *mmc* snap in/out to find out which certificates you already have on your computer.
Furthermore, take a close look at some of the trusted certificates and on localhost.

Tip: Make use of the following link
https://msdn.microsoft.com/en-us/library/ms788967(v=vs.110).aspx ;

Guess you will be surprised!

Environment variables Path and CLASSPath

1. Select Start -> Control Panel
2. Choose System and Security -> System
3. Click Advanced system settings > Advanced tab
4. Click on Environment Variables, and under System Variables, find **Path**, and click on it.



5. Click on Edit and in the Edit windows, modify **Path** by adding the directory of the respective file to the value for **Path**. 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!!
6. Click OK everywhere
7. Reopen Command prompt window, and run the command again.

   Maybe you will have to restart your computer….