| | |
|---|---|
| **COMPUTING SUBJECT:** | Root and Server Certificates |
| **TYPE:** | Assignment |
| **IDENTIFICATION** | CertificateX509 No. 2 |
| **COPYRIGHT:** | *Michael Claudius* |
| **LEVEL:** | Medium |
| **TIME CONSUMPTION:** | 1-2 hours |
| **EXTENT:** | 50 lines |
| **OBJECTIVE:** | mekecert , pvk2pfx, mmc commands |
| **PRECONDITIONS:** | Computer Networking Ch. 8.5 |
| **COMMANDS:** | |

**IDENTIFICATION:** CertificateX509 No.2 /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 self-signed X509 Root and Server SSL certificates
3. Secure SocketsC#, Use the certificates and SSLStream for secure socket communication

You have already done the first assignment and this assignment is the Assignment No.2

Purpose

For developing and testing one can create self-signed certificates (e.g. SSL certificates for Root, server and clients) instead of just buying them from Verisign or other providers. This is the purpose of this assignment.

.

*Useful links*

http://stackoverflow.com/questions/9982865/sslstream-example-how-do-i-get-certificates-that-work

http://stackoverflow.com/questions/14214396/how-to-create-a-certificate-to-use-with-sslstream-authenticateasserver-without-i

http://www.codeproject.com/Articles/25677/Simple-WCF-X-Certificate

http://www.jayway.com/2014/09/03/creating-self-signed-certificates-with-makecert-exe-for-development/

The Mission

In the following you can either follow the instructions given in the link:

http://www.jayway.com/2014/09/03/creating-self-signed-certificates-with-makecert-exe-for-development/

where they are running a .cmd batch file created in Notepad or just typing the commands in the Command Prompt (cmd).
In the following I explain the last mentioned method and for details on what goes on you can also look at the link given above.

1. Root certificate: creation

First Create your own new folder for your certificates e.g. C:\Certificates
Start a dos prompt as administrator: Click: start -> search -> cmd
Position in the folder for certificates, type: cd certificates
*Type* (by copy and paste):

```
makecert -r -pe -n "CN=RootCA" -cy authority -sv RootCA.pvk  RootCA.cer
```

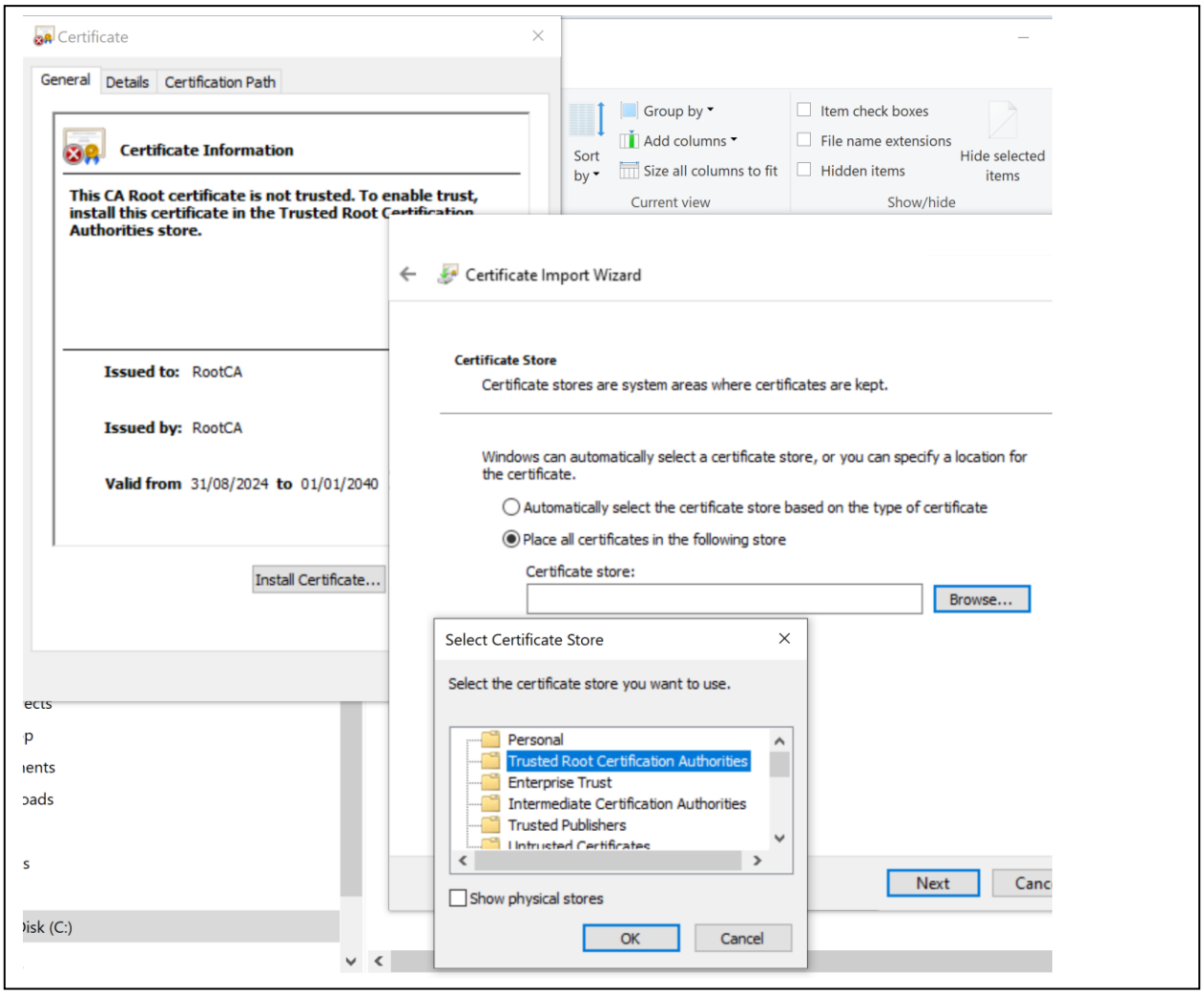
On the way you will be prompted for some passwords (use simple ones like *secret*)
*Type*: dir
And you will see you have created two files: a .cer file (a X.509 certificate with public key) and a .pvk file (with the private key).
Now Copy the public and private key from .pvk and .cer into an .pfx file (personal information exchange)
*Type*: (by copy and paste):

```
pvk2pfx -pvk RootCA.pvk  -spc RootCA.cer -pfx RootCA.pfx -po mysecret
```

On the way you will be prompted for the passwords for subject key and private key (*mysecret*).
Don't forget your keys.
Now you have three files in the certificate directory.

2. Root certificate: making it “trusted”

Now we shall install the certificate RootCA.cer in the Trusted Root Certification -> Certificates
Use Windows explorer and open the RootCA.cer file by double-clicking.




Click: Install Certificate
Choose: Browse
Select: Trusted Root Certification Authorities
Follow the steps (next, ok, finish) and you have now installed the certificate.
See the difference by opening the RootCA.cer file again by double-clicking.

3. Server certificate: Creation

Next we create a certificate to handle SSL on the server and this certificate is signed by the RootCA authority.

```
makecert -ic RootCA.cer -iv RootCA.pvk -n "CN= FakeServerName " -pe -sky exchange -sv ServerSSL.pvk ServerSSL.cer
```

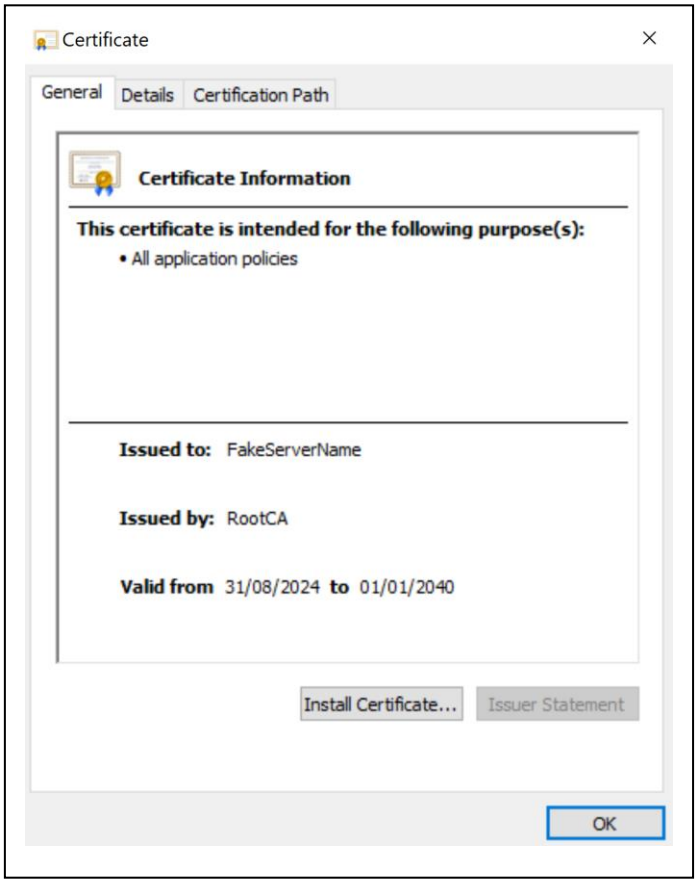
Again you will be asked for keys and also the issuer's key, which is the one you choose when creating RootCA.
*Type*: dir
And you will see you have created to files: a .cer file (a X.509 certificate with public key) and .pvk file (with the private key).
Now copy the public and private key from .pvk and .cer into an .pfx file (personal information exchange)
*Type*: (by copy and paste):

```
pvk2pfx -pvk ServerSSL.pvk  -spc ServerSSL.cer -pfx ServerSSL.pfx -po mysecret
```

On the way you will be prompted for the passwords for subject key and private key (*secret*).
Don't forget your keys/passwords.
Now you have three more files in the certificate directory.

4. Server certificate: making it “trusted”

First open ServerSSL.cer by double-clicking, notice that it has already been automatically installed.




Secondly, we shall install the certificate ServerSSL.pfx in the Personal Certificates
Open the ServerSSL.pfx file by double-clicking.
Follow the procedure just like before. Remember that the private key for .pfx file is the password stated by the -po option (*mysecret*).
Then see the difference by opening the ServerSSL.cer file again by double-clicking.

Now we are ready to use the certificates in C# programs in the next assignment SecureSocketC.

5. 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 ;

Try local computer and personal account. See if you can find ”FakeSerName”.

*Guess you will be surprised how many certificates you have accepted!!*