TCS certificates for MS SQL Server

Just spent some time figuring out why a Microsoft SQL Server didn't grok my fresh TCS certificate.

Generating key materials

I did this on a host with OpenSSL. Also possible on the Windows host but I will write about that later.

```
openssl req -newkey rsa:2048 -keyout server.key -out server.csr -subj /CN=hayek.terena.org/
```

I submitted the signing request to the SURFnet web site, and after a few hours, and jumping through the Domain Control Validation hoops, I got a signed certificate (`cert-11988-hayek.terena.org.pem`) back, and the chain, which consists of 3 certificates concatenated into one file (`chain-11988-hayek.terena.org.pem`).

Then combined all certificates into one file, and created a PFX from these materials:

```
cp server.pem all.pem
cat chain.pem >> all.pem
openssl pkcs12 -export -inkey server.key -in all.pem -out server.pfx
```

Adding the key and certificates

Copy this file to the Windows server, and run `mmc`, then add the Certificates snap-in.

When it asks for who to manage certificates, select an account that the SQL Server has access to.

In our case that was the "Local System" account, and we were running the snap-in as Administrator, so all is well.

Expand: Console Root -> Certificates (Local Computer) -> Personal.

Right-click -> All Tasks -> Import.

Now navigate to the pfx file and import it. Include all extended properties.

I kept **Mark this key as exportable** unchecked, as I already have the key material in PEM format in a different place.

We don't need this, and any malicious export attempt will be more difficult this way.

Configuring MS SQL Server to use the certificate

Our box runs Microsoft SQL Server 2008 R2. Run the **SQL Server Configuration Manager**, expand the **SQL Server Network Configuration**, and right-click **Protocols for MSSSQLSERVER** (or whatever your instance is called).

On the Certificate tab you should be able to see your certificate.

In my case nothing would show up 😞

According to How to: Enable Encrypted Connections to the Database Engine (SQL Server Configuration Manager), **the name of the certificate must be the fully qualified domain name (FQDN) of the computer**. The TCS certificates we use can only contain a valid FQDN as the Subject's Common Name (CN), so this was correct. I checked permissions and those seemed to be OK as well.

It turned out that the server did not have a **Full Computer Name** yet... duh.

After fixing that the certificate showed up and everything worked. After setting **Protocols for MSSSQLSERVER** to **Yes**, I checked with Wireshark and indeed no more plain text queries 🙂.

PS: you can also use this certificate to secure other stuff, like Remote Desktop.