Dat is weer balen. Na het intikken van een heel artikel drukte ik per ongeluk op de "back" toets. Heel het artikel weer verdwenen. Het zou wel mooi zijn als er een automatische save-optie in het Joomla-cms zou zitten. De backtoets in Firefox=Alt + pijltje links.

Zoals in het artikel "ISA en HTTP_VIA Header" aangeven kan ik met de N82 met ActiveSync bij de Exchange Server komen, echter dit was me nog niet gelukt via een SSL verbinding. De reden dat het nog niet is gelukt komt omdat het installeren en de eisen aan het certificaat anders zijn dan die voor de Windows Mobile pda's. De Nokia N82 heeft als OS Symbian versie 9.0. Een certificaat uit SelfSSL kreeg ik met geen mogelijkheid op de telefoon. Uiteindelijk is het wel gelukt maar dan anders, de hoe-procedure beschrijf ik hieronder. Deze site heb ik ter inspiratie gebruikt.

Benodigdheden

- Windows 2003 + IIS (waar de active sync site op staat)
- Linux/Ubuntu server
- Mail for Exchange geïnstalleerd op Nokia N82 en reeds werkend voor HTTP

Stappenplan

1. Installeer openssl op ubuntu met het volgende commando op de Ubuntu server
   sudo apt-get install openssl
2. Maak benodigde directories en bestanden aan (ga eerst in /**etc**/**ssl** staan)
   sudo mkdir keys
   sudo mkdir requests
   sudo mkdir certs
   sudo mkdir demoCA
   sudo touch database.txt
   sudo mkdir demoCA/newcerts
   sudo mkdir demoCA/private
   sudo touch demoCA/index.txt
   sudo echo "01" >> demoCA/serial
3. Maak een private key
   sudo openssl genrsa -des3 -out keys/rootca.key 1024

   Generating RSA private key, 1024 bit long modulus
   .....++++++
   .....++++++

e is 65537 (0x10001)
Enter pass phrase for keys/rootca.key: <type hier een woord/zin (soort password), onthoud deze
Verifying - Enter pass phrase for keys/rootca.key: < en nog een keer ter verificatie

4. Maak het root-certificaat aan

sudo openssl req -config openssl.cnf -new -x509 -days 1001 -key keys/rootca.key -out certs/rootca.cer

Enter pass phrase for keys/rootca.key: < type hier het woord/ de zin die gebruikt is bij het maken van de private key.
Country Name (2 letter code) [AU] < type de landcode, bijv. NL
State or Province Name (full name) [Some-State]: <type de provicienaam of . "punt" om deze leeg te laten
Locality Name (eg, city) []: < type de naam van de stad, bijv Rotterdam
Organization Name (eg, company) [Internet Widgits Pty Ltd]: < type de naam van de organisatie, bijv. Private Certs Ltd
Organizational Unit Name (eg, section) []: <type de organisatienaam of . "punt" om deze leeg te laten
Common Name (eg, YOUR name) []: <type de naam van de Root-CA (zo komt deze in de lijst van certificaten te staan, bijv: mine.nu
Email Address []: <type een emailadres, ter info, bijv: info@arjan.mine.nu

5. Converteer het gemaakte certificaat naar DER-formaat. (nodig voor Windows)

sudo openssl x509 -in certs/rootca.cer -outform DER -out certs/rootca.der

6. Verzoek aanmaken certificaat (dit op IIS Website ActiveSync) zie: Microsoft Knowledge Base Article Q228821 .
7. Kopieer het request bestand naar /**etc/ssl/requests** (WinScp)

8. Signeer het request op de ubuntu-server

sudo openssl ca -policy policy_anything -config openssl.cnf -cert certs/rootca.cer -in requests/certreqamn.txt -keyfile keys/rootca.key -days 360 -out certs/certamn.cer

Using configuration from openssl.cnf
Enter pass phrase for keys/rootca.key: < type hier het woord/ de zin die gebruikt is bij het maken van de private key.
Check that the request matches the signature
Signature ok
Certificate Details:
Serial Number: 2 (0x2)
Validity
Not Before: Sep 1 13:37:12 2008 GMT
Not After : Aug 27 13:37:12 2009 GMT
Subject:
countryName = NL
stateOrProvinceName = ZH
localityName = Rotterdam
organizationName = PM

```
        organizationalUnitName    = OU
        commonName                = naamwebsite.domainextensie
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        Netscape Comment:
            OpenSSL Generated Certificate
        X509v3 Subject Key Identifier:
            A0:28:10:98:44:8E:E9:EF:02:70:78:6B:7B:F4:3D:01:C1:E9:A3:73
        X509v3 Authority Key Identifier:
            keyid:16:00:FC:DC:BA:C7:7D:F6:5F:88:3A:46:87:E0:5E:64:7D:28:7A:86

Certificate is to be certified until Aug 27 13:37:12 2009 GMT (360 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

9. Converteer het gemaakte certificaat naar DER-formaat. (dit is nodig voor Windows)
   sudo openssl x509 -in certs/certamn.cer -out certs/x509amn.cer
10. Kopieer de certificaten **rootca.der** en **x509amn.cer** uit **etcsslcerts** naar de windows opgeving waar het request is aangemaakt en maak daar het request verder af. Importeer ook het **rootca.der** in de certificatestorage van de computer.

11. Plaats het **rootca.der** bestand in de hoofdirectory van de webserver waarop op het certificate is geïnstalleerd (de ActiveSync website). Zorg dat deze site ook bereikbaar is met http

12. Voeg in IIS op de website de mimetype "**application/x-x509-ca-cert**" toe met als extensie" **.der**"
    (Properties website > Tabblad HTTP Headers> Button Mime Types...> New...)
13. Surf met de Noka N82 naar **http://naamwebsite.domainextensie/rootca.der**

Een **"Save Certificate"** melding verschijnt nu met de informatie in het root certificaat
Kies **Save**
Een **"New certificate might be unsecure. Save anyway?"** melding verschijnt nu.
Kies **Save**
Nu krijg je de mogelijkheid om het label aan te passen
Kies **Ok**

Een mogelijkheid tot **"Certificate uses**" verschijnt nu.
Enter Internet
Enter Onlinecert. checking

Enter Vpn
OK

Certificate Saved!

14. Voer op de Nokia N82 de volgende handeling uit **> Menu > Mfe >Mail for Exchange > Options**
> Edit Profile
> Connection
> Secure connection = Yes
> Save
15. Voer op de Nokia N82 de volgende handeling uit **Options > Synchronise > Select**, Als alles goed is gegaan dan lukt de synchronisatie over SSL

Test mogelijkheid:
Een middels bovenstaande procedure aangemaakt root-certificaat is op te halen bij http://arjan.mine.nu/rootca.der
Als je deze importeert en plaatst (automatisch) in je "trustedroot certificate storage" dan kan je over een ssl-beveiligde verbinding waar geen foutmelding meer voor verschijnt het nummer Master of Puppets van Metallica downloaden op
deze
link. Veel luisterplezier toegewenst.

Naschrift:

Met bovenstaande handelingen krijg je een zelf aangemaakt certificaat voor op je exchange omgeving. Voor de sterkte van de encryptie maakt het niks uit of je deze zelf hebt aangemaakt of hebt gekocht. Wel is het erg omslachting om zo'n self-certificaat in browsers te krijgen en zeker als je een ssl pagina aanbied aan anderen, onbekenden, iedereen op internet, is het ondoenlijk. Om dit ongemak te voorkomen kan je dan beter een certificaat kopen bij een van de aanbieders op internet die aangeven dat hun certificaten door de meeste (>95%) browsers worden vertrouwd. Dan blijft er enkel het stukje IIS-configuratie over en hoef je niet met Openssl aan de slag. Als het echter voor eigen gebruik is of in ieder geval beperkt gebruik dan is een zelf aangemaakt root-certificaat met daarbij een certificaat voor server-authticatie een betere methode. Wie vertrouwd er bijvoorbeeld nu een certificaat als deze is uitgeven door iemand op
deze
lijst? Okay, je moet ergens vanuit gaan als het om vetrouwen gaat maar met de huidige samenleving durf ik er geen vergif op in te nemen dat er geen dag komt dat https:/mijn.postbank.nl niet de echte https://mijn.postbank.nl is en dat je hier niet eens een

certificaatwaarschuwing van krijgt.Een door de postbank zelf uitgegeven root-certificaat zou dat wel doen. Op voorwaarde dan dat je alle standaard aanwezige certificaten verwijderd, dat dan weer wel. hmmm Toch niet helemaal helaas, hier kom ik nog op terug.