



SURFfederatie ADFS-HANDLEIDING
*VOOR AANSLUITING ALS IDENTITY
PROVIDER*

versie 1.2, november 2009

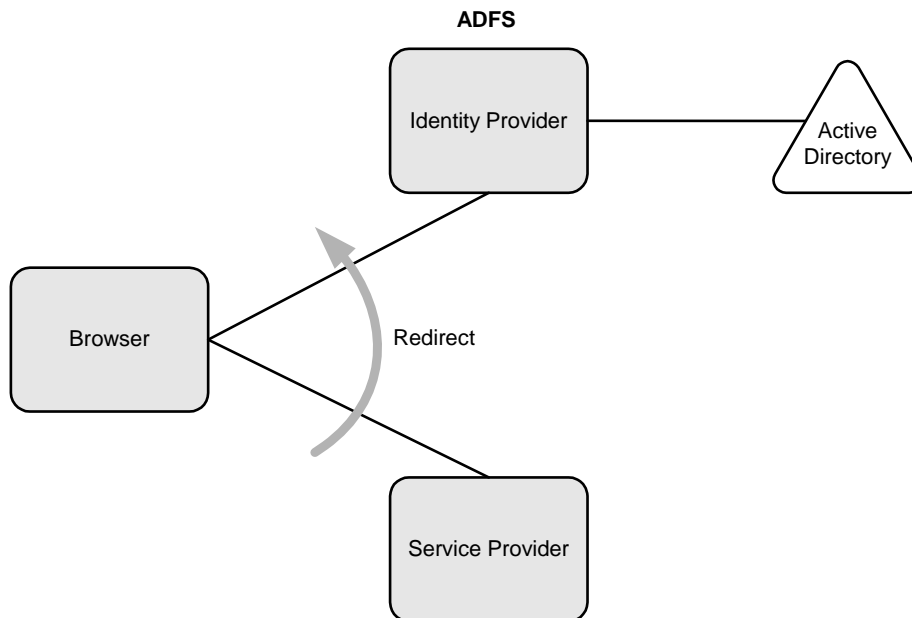
INHOUDSOPGAVE

1. Inleiding.....	3
1.1 Auteurs.....	4
2. Systeemconfiguratie	5
2.1 Inleiding	5
2.2 Windows Server 2003 R2 Enterprise Edition configureren	5
2.3 ADFS service component installeren	6
2.4 ADFS koppelen aan de Active Directory	7
3. ADFS inrichten als Identity PROVIDER	8
3.1 Inleiding	8
3.2 Trust policy configureren	8
3.3 Tokencertificaat exporteren.....	9
3.4 Gegevens opsturen naar SURFfederatie	9
3.5 Gegevens van SURFfederatie configureren	9
3.6 Koppeling testen.....	11
3.7 Tokencertificaat vernieuwen	11
4. Attributen vrijgeven aan de SURFfederatie.....	13
4.1 Inleiding	13
4.2 Organization claims aanmaken	13
4.3 Claim extractions maken	14
4.4 Claim mapping maken	14
4.5 Attributen testen	14
5. Een ADFS Proxy toevoegen	15
5.1 Inleiding	15
5.2 Windows Server 2003 R2 Enterprise Edition configureren	15
5.3 Proxy client certificaat genereren	16
5.4 ADFS proxy component installeren.....	17
5.5 ADFS proxy certificaat importeren	17
5.6 Login pagina aanpassen	18

1. INLEIDING

Als organisatie kunt u aansluiten op de SURFfederatie met het protocol Active Directory Federation Services (ADFS) van Microsoft. U kunt aansluiten op twee manieren:

- als **Identity Provider (IDP)**, in ADFS terminologie 'Account Partner' (AP) genoemd. Bent u IDP, dan is de Active Directory van uw organisatie ontsloten naar de SURFfederatie. Hierdoor kunnen gebruikers in uw Active Directory zich authenticeren voor diensten binnen de SURFfederatie.
- als **Service Provider (SP)**, in ADFS terminologie 'Resource Partner' (RP) genoemd. In deze rol kunt u als organisatie ook diensten aanbieden via de SURFfederatie.



In deze handleiding leest u hoe u uw organisatie aansluit in de rol van Identity Provider, de rol die voor de meeste instellingen van toepassing zal zijn. Er verschijnt ook een handleiding voor aansluiting in de rol van Service Provider.

De procedure voor het aansluiten als IDP bestaat uit de volgende onderdelen:

1. Uw ADFS server systeem configureren voor aansluiting, o.a. Windows Server 2003 R2 Enterprise Edition configureren en ADFS installeren (hoofdstuk 2)
2. De ADFS server inrichten voor aansluiting als IDP voor de SURFfederatie (hoofdstuk 3)
3. Attributen vrijgeven aan de SURFfederatie (hoofdstuk 4)

4. Een ADFS proxy inrichten (hoofdstuk 5)

Dit houdt in dat er 2 verschillende Windows Server 2003 R2 Enterprise Edition machines geconfigureerd worden in deze setup. De ADFS server zal in het AD domein worden opgenomen, de ADFS proxy kan daar buiten staan. De functie van de ADFS proxy kan wellicht gecombineerd worden met andere (IIS) functies op een bestaande machine.

1.1 Auteurs

Deze handleiding is tot stand gekomen door bijdragen van Jan van den Bosch (TU Eindhoven), Jan Michielsen (bureau Hendriks Van der Spek), Peter Swinkels (Fontys Hogescholen), Hans Zandbelt (SURFnet), Joost van Dijk (SURFnet) en Remco Poortinga – van Wijnen (SURFnet).

2. SYSTEEMCONFIGURATIE

2.1 Inleiding

Voordat u de specifieke instellingen voor de SURFfederatie kunt invoeren, moet u uw Windows systeemcomponenten op de ADFS account server juist configureren. Dat gaat in de volgende stappen:

1. Windows Server 2003 R2 Enterprise Edition installeren en configureren, inclusief IIS en Microsoft .NET Framework 2.0 (paragraaf 2.2)
2. De ADFS service component installeren (paragraaf 2.3)
3. ADFS koppelen aan uw Active Directory (paragraaf 2.4)

2.2 Windows Server 2003 R2 Enterprise Edition configureren

1. Installeer Windows Server 2003 R2 Enterprise Edition op de machine die gaat fungeren als ADFS server. Dit kan een bestaande machine zijn, de domain controller, de Active Directory server zelf, of een nieuwe (mogelijk virtuele) machine, zolang deze maar in het Windows domein kan worden opgenomen. Zorg dat het IP-adres van deze server bekend is in DNS, bijvoorbeeld als 'adfs.mycampus.nl'.



Steeds waar in deze handleiding de DNS-naam 'adfs.mycampus.nl' of de identifier 'MyCampus' voorkomt, moet u een zelfgekozen naam invullen. Vul steeds dezelfde naam in.


2. Voeg deze server toe aan het MS Windows domain waar ook de Active Directory server draait (als dit nog niet is gebeurd).
3. Zorg dat de tijd op de machine juist is ingesteld, dus dat hij synchroniseert met een time server. Voor sessie timeouts en ter voorkoming van replay attacks worden namelijk de timestamps in de berichten meegestuurd en gecheckt door de SURFfederatie.
4. Installeer Internet Information Services (IIS) en Microsoft .NET Framework 2.0. Dit doet u via **Start > Control Panel > Add or Remove Programs > Add or Remove Windows Components**.
5. Zorg voor een geldig servercertificaat voor de IIS server, ten behoeve van secure connecties (met behulp van TLS/SSL) naar de ADFS website (adfs.mycampus.nl). De SURFcertificatendienst van SURFnet biedt de mogelijkheid om een servercertificaat af te nemen.

 De methode voor het aanvragen en installeren van het servercertificaat vindt u op Microsoft Technet (<http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS>):

- SSL configureren: kies **Operations Guide > Security in IIS 6.0 > IIS 6.0 Encryption > Configuring Secure Sockets Layer > Configuring SSL on a Web Server or Web Site.**
- Certificaat installeren: kies **Operations Guide > Security in IIS 6.0 > Certificates > Installing Server Certificates.**

2.3 ADFS service component installeren


1. Kies **Start > Control Panel > Add or Remove Programs > Add/Remove Windows Components.**
2. Klik in het venster 'Windows Components Wizard' op **Active Directory Services** en vervolgens op **Details.**

 Als Windows hier (of later in de procedure) vraagt of ASP.NET 2.0 moet worden geïnstalleerd, klik dan op **Yes.**

3. Klik in het venster 'Active Directory Services' op **Active Directory Federation Services (ADFS)**, en vervolgens op **Details.**
4. Selecteer in het venster 'Active Directory Federation Services (ADFS)', de check box **Federation Service** en klik vervolgens op **OK.**
5. Klik op **OK** in het venster 'Active Directory Services'.
6. Klik op **Next** in de Windows Components Wizard.

U komt nu in het venster 'Federation Service'.

7. Selecteer onder 'Token-signing certificate' de optie **Create a self-signed token-signing certificate.**

 Met het token-signing certificaat worden de authenticatiegegevens die de ADFS service naar de SURFfederatie stuurt, digitaal ondertekend. Dit certificaat moet u daarom naar de SURFfederatie sturen. U doet dit in paragraaf 3.4.

 Het aangemaakte token-signing certificaat is 1 jaar geldig, daarna moet u een nieuw certificaat aanmaken en installeren. SURFnet zal u tijdig waarschuwen als het certificaat bijna verloopt. Hoe u een nieuw certificaat, met langere geldigheidsduur, kunt aanmaken en installeren wordt beschreven in paragraaf 3.7.

8. Selecteer onder 'Trust policy' de optie **Create a new trust policy** en klik op **Next.**

9. Er kan nu worden gevraagd waar de installatiefiles zich bevinden. Geef de juiste locatie op, bijvoorbeeld 'R2 Installation Folder\cmpnents\r2' en klik op **OK**.
10. Sluit de procedure af door in het venster 'Completing the Windows Components Wizard' op **Finish** te klikken.

2.4 ADFS koppelen aan de Active Directory

1. Kies **Start > All Programs > Administrative Tools > Active Directory Federation Services**.
2. Dubbelklik op **Federation Service**, dubbelklik op **Trust Policy**, dubbelklik op **My Organization**. Klik met de rechtermuisknop op **Account Stores**, kies **New** en klik op **Account Store**.
3. Klik op **Next** in het venster 'Welcome to the Add Account Store Wizard'.
4. Selecteer in het venster 'Account Store Type' de optie **Active Directory** en klik op **Next**.
5. Selecteer in het venster 'On the Enable this Account Store' de optie **Enable this account store** en klik op **Next**.
6. Klik op **Finish** in het venster 'Completing the Add Account Store Wizard'.

3. ADFS INRICHTEN ALS IDENTITY PROVIDER

3.1 Inleiding

Het inrichten van ADFS als Identity Provider voor de SURFfederatie bestaat uit de volgende stappen:


1. De trust policy configureren (paragraaf 3.2)
2. Het tokencertificaat naar een bestand exporteren (paragraaf 3.3). U moet dit tokencertificaat naar de SURFfederatie sturen. Het garandeert dat de uitwisseling van authenticatiegegevens veilig verloopt.
3. De noodzakelijke gegevens naar de SURFfederatie sturen (paragraaf 3.4)
4. De gegevens van de SURFfederatie configureren (paragraaf 3.5)
5. Koppeling testen (paragraaf 3.6)

Voor het vrijgeven van autorisatiekenmerken of attributen, wellicht vereist voor het benaderen van bepaalde diensten, is een extra stap noodzakelijk. Deze wordt beschreven in hoofdstuk 4.

Na verloop van tijd zal het tokencertificaat vernieuwd moeten worden, het aanmaken en configureren hiervan wordt beschreven in paragraaf 3.7.

3.2 Trust policy configureren

1. Kies **Start > All Programs > Administrative Tools > Active Directory Federation Services**.
2. Dubbelklik op **Federation Service**, klik met de rechtermuisknop op **Trust Policy** en klik op **Properties**.
3. Selecteer de tab **General**.
4. Vul onder 'Federation Service URI' de tekst **urn:federation:MyCampus** in. **MyCampus** is de naam van uw organisatie. Gebruik hiervoor alleen ASCII-letters.
5. Vul onder 'Federation Service endpoint URL' de tekst **https://adfs.mycampus.nl/adfs/ls/** in. **adfs.mycampus.nl** is de DNS-naam die u bij het installeren van Windows Server 2003 R2 gekozen hebt (zie paragraaf 2.2).

 **Let op:** vergeet de laatste slash (/) niet.

6. Selecteer de tab **Display name tab**.
7. Typ onder 'Display name for this trust policy' de naam **MyCampus** in, waarin **MyCampus** de naam van uw organisatie is. Klik op **OK**.

3.3 Tokencertificaat exporteren

1. Kies **Start > All Programs > Administrative Tools > Active Directory Federation Services**. Klik met rechtermuisknop op **Federation Service**, en klik op **Properties**.
2. Selecteer de tab **General** en klik op **View**.
3. Selecteer de tab **Details** en klik op **Copy to file**.
4. Klik op **Next** in het venster 'Welcome to the Certificate Export Wizard'.
5. Selecteer in het venster 'Export Private Key' de optie **No, do not export the private key** en klik op **Next**.
6. Selecteer in het venster 'Export File Format' de optie **Base-64 encoded X.509 (Cer.)** en klik op **Next**.
7. Voer in het venster 'File to Export' de bestandnaam **C:\MyCampus_ts.cer** in. Klik vervolgens op **Next**.
8. Klik in het venster 'Completing the Certificate Export Wizard' op **Finish**.

3.4 Gegevens opsturen naar SURFfederatie

Stuur de volgende gegevens naar SURFnet, via federatie-beheer@surfnet.nl.

- De federatie-identificer: de naam die u hebt opgegeven in stap 3 van paragraaf 3.2 (**urn:federation:MyCampus**).
- De federatie-endpoint URL: de URL die u hebt ingevoerd in stap 4 van paragraaf 3.2 (**https://ads.mycampus.nl/ads/ls/**).
- Het bestand met het tokencertificaat dat u in paragraaf 3.3 hebt gegenereerd.

3.5 Gegevens van SURFfederatie configureren

Voor de SURFfederatiekoppeling gebruikt u hetzelfde type gegevens als die u opgestuurd hebt in paragraaf 3.3. Deze gegevens gebruikt u om de SURFfederatie als service provider toe te voegen aan de ADFS service.

Het gaat om de volgende gegevens:

- De federatie-identificer van de SURFfederatie: **urn:federation:surfnet:sfs**
- De federatie-endpoint URL van de account provider service van de SURFfederatie: **https://wayf.surfnet.nl/federate/wsfed1x**

Het configureren gaat als volgt:

1. Kies **Start > All Programs > Administrative Tools > Active Directory Federation Services**.
2. Dubbelklik op **Federation Service**, dubbelklik op **Trust Policy**, dubbelklik op **Partner Organizations**, klik met de rechtermuisknop op **Resource Partners**, selecteer **New** en klik op **Resource Partner**.
3. Klik op **Next** in het venster 'Welcome to the Add Resource Partner Wizard pagina'.
4. Selecteer in het venster 'Import Policy File' de optie **No** en klik op **Next**.
5. Vul in het venster 'Resource Partner Details' onder 'Display name' de naam **SURFfederatie** in.
6. Vul onder 'Federation Service URI' de federatie-identificer van de SURFfederatie in: **urn:federation:surfnet:sfs**.



Let op: deze identificer is hoofdlettergevoelig.

7. Vul onder 'Federation Service endpoint URL' de federatie-endpoint URL van de SURFfederatie in: **https://wayf.surfnet.nl/federate/wsfed1x**. Klik vervolgens op **Next**.
8. Selecteer in het venster 'Federation Scenario' de optie **Federated Web SSO** en klik op **Next**.
9. Selecteer in het venster 'Resource Partner Identity Claims' de checkbox **UPN Claim** en klik op **Next**. (Indien gewenst kunt u met SURFnet overleggen over een ander type te gebruiken claim).
10. Selecteer in het venster 'Select UPN Suffix' de optie **Pass all UPN domain suffixes through unchanged**. Klik op **Next**.
11. Selecteer in het venster 'Enable this Resource Partner' de checkbox **Enable this resource partner** en klik op **Next**.
12. Klik op **Finish** in het venster 'Completing the Add Resource Partner Wizard'.

Mocht u een configuratie maken voor de test omgeving van de SURFfederatie dan zijn de gegevens als volgt:

- Federatie identificer: **urn:federation:surfnet:sfs-test**
- Federatie URL: **https://wayf-test.surfnet.nl/federate/wsfed1x**

Beide koppelingen, zowel voor productie als test omgeving kunnen eventueel tegelijkertijd als verschillende resource partners worden geconfigureerd op dezelfde ADFS server.

3.6 Koppeling testen

Wanneer u de hele inrichtingsprocedure hebt uitgevoerd en SURFnet meldt dat de configuratie van uw gegevens is ingevoerd op de SURFfederatie-servers, is uw ADFS-installatie al gereed om te authenticeren in de SURFfederatie. Dit kunt u testen door op een test service in te loggen, bijvoorbeeld via <https://wayf.surfnet.nl/attributes>.

Voor de testomgeving is de URL van deze test service: <https://wayf-test.surfnet.nl/attributes>.

3.7 Tokencertificaat vernieuwen

Het in sectie 2.3 (stap 7) aangemaakte self-signed tokencertificaat heeft een standaard geldigheidsduur van een jaar en zal dus op een gegeven moment vernieuwd moeten worden. SURFnet zal u tijdig waarschuwen (ruim een maand van tevoren) dat het tokencertificaat binnenkort zal verlopen.

De makkelijkste procedure om dit certificaat te vernieuwen bestaat uit het creëren van een nieuw self-signed certificate met behulp van OpenSSL en deze te installeren op de ADFS server. Aan dit nieuwe certificaat kan direct ook een langere geldigheidsduur dan een jaar worden meegegeven; het onderstaande voorbeeld creëert een certificaat dat 10 jaar geldig is.

Een self-signed certificaat kan genereerd worden met OpenSSL¹ op de volgende wijze:

1. `openssl req -x509 -nodes -days 3650 -newkey rsa:1024 -keyout adfs.key -out adfs.cer`
2. `openssl pkcs12 -export -inkey adfs.key -in adfs.cer -out adfs.pfx`
<kies een wachtwoord dat bij het importeren moet worden gebruikt>
3. Open de Microsoft Management Tool met **Start > Run** en door ``mmc`` in te voeren. Voeg een console toe door te kiezen voor **File > Add/Remove Snap-in...** en kies voor **Standalone > Add...** Kies **Certificates** uit de lijst van **Available Standalone Snap-ins** en selecteer **Add**. Kies dan de optie **Computer Accounts** uit de opties voor het type certificaten dat de snap-in gaat beheren, kies **Next** en kies de optie **Local Computer** als de computer die beheerd gaat worden door deze snap-in. Kies dan achtereenvolgens **Finish**, **Close** en **Ok**.
4. Navigeer in de console naar **Certificates (Local Computer) > Personal > Certificates**, klik op de rechtermuisknop en kies **All Tasks > Import**. Browse naar de `adfs.pfx` file (NB: niet de `.cer` file) en klik op **Next**. Geef

¹ Een OpenSSL installer voor Windows is beschikbaar via: <http://www.slproweb.com/products/Win32OpenSSL.html>

het wachtwoord uit stap 2., klik achtereenvolgens op **Next**, **Next** en **Finish**, en sluit de console af (hoeft niet te worden opgeslagen).

5. Voordat het nieuwe tokencertificaat geactiveerd kan worden moet deze ook bij SURFnet bekend (en geconfigureerd) zijn, stuur daarom de uit stap 1 komende publieke certificaat (adfs.cer bestand) naar federatie-beheer@surfnet.nl. SURFnet zal terugmelden wanneer het nieuwe tokencertificaat aan de SURFnet kant geïnstalleerd is.



Let op: Vanaf dit moment zijn er aan de kant van SURFnet twee tokencertificaten geldig, zowel de 'oude' als de nu nog niet actieve 'nieuwe', waardoor de overgang naar het nieuwe certificaat naadloos kan verlopen. Vergeet daarom niet aan SURFnet te melden wanneer u de overgang daadwerkelijk heeft gemaakt, zodat ook aan SURFnet kant het oude tokencertificaat kan worden opgeruimd.

Na melding dat het certificaat bij SURFnet is geïnstalleerd kunt u het nieuwe tokencertificaat activeren/selecteren voor gebruik:

1. Kies **Start > All Programs > Administrative Tools > Active Directory Federation Services**. Klik met rechtermuisknop op **Federation Service**, en klik op **Properties**.
2. Selecteer de tab **General** en klik op **Select**.
3. Selecteer uit de lijst van certificaten het tokencertificaat dat u in de vorige stap 4 heeft geïnstalleerd en klik op **OK**.
4. Kies in het pop-up venster dat vraagt of de private key door het account van de ADFS service gelezen mag worden op **Yes**.
5. Kies **Apply**, in het pop-up venster **Yes**, en klik vervolgens op **OK**.
6. Meld aan SURFnet dat het nieuwe tokencertificaat actief is.

4. ATTRIBUTEN VRIJGEVEN AAN DE SURFFEDERATIE

4.1 Inleiding

Claims zijn attributen die de authenticatieservice na een geslaagde authenticatie van een gebruiker kan toevoegen aan het authenticatietoken. Voorbeelden van attributen zijn het e-mailadres van de gebruiker of de naam van een groep waar de gebruiker lid van is. Ze worden door de ADFS accountservice uitgegeven.

De attributen die binnen de SURFfederatie kunnen worden gebruikt, vindt u hier: <http://www.surffederatie.nl/attributenschema>. In dit hoofdstuk worden er drie besproken: *urn:mace:dir:attribute-def:eduPersonEntitlement*, *urn:mace:dir:attribute-def:cn* en *urn:mace:dir:attribute-def:uid*. Deze fungeren slechts als voorbeeld; overleg met SURFnet over de specifieke attributen die uw organisatie nodig heeft voor het benaderen van diensten in de SURFfederatie.

Claims worden in drie stappen geconfigureerd:

1. De organization claims die u als organisatie nodig hebt (paragraaf 4.2)
2. Claim extractions maken, die informatie uit Active Directory halen om de organization claims te vullen (paragraaf 4.3). Het gaat bijvoorbeeld om specifieke attributen of lidmaatschap van bepaalde groepen.
3. Een claim mapping maken (paragraaf 4.4). Hiermee wordt bepaald:
 - welke claims naar de SURFfederatie gestuurd
 - welke naam deze claims krijgen
4. Attributen testen (paragraaf 4.5)

4.2 Organization claims aanmaken

1. Kies **Start > All Programs > Administrative Tools > Active Directory Federation Services**.
2. Dubbelklik op **Federation Service**, dubbelklik op **Trust Policy**, dubbelklik op **My Organization**, klik met de rechtermuisknop op **Organization Claims**, selecteer **New** en klik op **Organization Claims**.
3. Vul onder 'Claim Name' de naam **eduPersonEntitlement** in.
4. Selecteer de optie **Custom claim** en klik op **OK**.
5. Herhaal stap 3 en 4 voor de attributen *cn* en *uid*.

4.3 Claim extractions maken

1. Kies **Start > All Programs > Administrative Tools > Active Directory Federation Services**.
2. Dubbelklik op **Federation Service**, dubbelklik op **Trust Policy**, dubbelklik op **My Organization**, dubbelklik op **Account Stores**, klik met de rechtermuisknop op **Active Directory**, selecteer **New** en klik op **Create a Custom Claim Extraction**.
3. Vul onder 'Attribute' de naam `extensionAttribute1` in.
4. Kies onder 'Map to this Organization Claim' de optie **edupersonEntitlement**.
5. Herhaal stap 1 tot en met 4 voor de attributen *cn* en *uid*. Vul daarbij de volgende waarden in:
 - *cn*: attribute = Common Name, Map to this Organization Claim = **cn**
 - *uid*: attribute = `samAccountName`, Map to this Organization Claim = **uid**

4.4 Claim mapping maken



Voor de claimnamen moet het gestandaardiseerde attributenschema van SURFfederatie worden gehanteerd. Stem dit af met de SURFfederatie.

1. Kies **Start > All Programs > Administrative Tools > Active Directory Federation Services**.
2. Dubbelklik op **Federation Service**, dubbelklik op **Trust Policy**, dubbelklik op **Partner Organizations**, dubbelklik op **Resource Partners**, klik met de rechtermuisknop op **SURFfederatie**, selecteer **New** en klik op **New Outgoing Custom Claim Mapping**.
3. Selecteer onder 'Organization group claims' de optie **eduPersonEntitlement**.
4. Vul onder 'Outgoing claim name' de naam `urn:mace:dir:attribute-def:duPersonEntitlement` in.
5. Herhaal deze procedure voor de claims *cn* en *uid*, met respectievelijke outgoing claim names: `urn:mace:dir:attribute-def:cn`, `urn:mace:dir:attribute-def:uid`.

4.5 Attributen testen

U kunt nu weer van de test service van SURFnet gebruikmaken (<https://wayf.surfnet.nl/attributes>) om te testen of uw attributen goed worden vrijgegeven en doorgegeven.

5. EEN ADFS PROXY TOEVOEGEN

5.1 Inleiding

Het is sterk aanbevolen om `voor` de ADFS server nog een ADFS proxy in te richten die het verkeer van buitenaf doorstuurt naar de ADFS server. Dit heeft de volgende voordelen:

- De ADFS server dient in het Windows domein te worden opgenomen maar moet in de standaard oplossing wel van buitenaf bereikbaar te zijn. Door een ADFS proxy op te nemen in het netwerk, kan de ADFS server afgeschermd blijven van de buitenwereld, en kan de proxy, die niet in het AD domein hoeft te worden opgenomen, in het DMZ worden geplaatst
- Een proxy kan geconfigureerd worden om een login pagina met de look-and-feel van de instelling te tonen aan de gebruiker, in plaats van de standaard popup prompt die de ADFS server laat zien; dit verbetert de herkenbaarheid van de login voor de eindgebruiker en helpt phishing te voorkomen, ondermeer door het toepassen van een geldig SSL server certificaat. Ook kan op deze wijze extra tekst op de login pagina getoond worden waarmee gebruikers worden geholpen met het inloggen, iets dat niet mogelijk is met de standaard ADFS popup username/password prompt.

Het inrichten van een ADFS proxy bestaat uit de volgende stappen

1. Windows Server 2003 R2 Enterprise Edition installeren en configureren, inclusief IIS en Microsoft .NET Framework 2.0 (paragraaf 5.2)
2. Een client certificaat genereren voor de proxy (paragraaf 5.3)
3. De ADFS proxy component installeren (paragraaf 5.4)
4. ADFS proxy certificaat importeren op ADFS account server (paragraaf 5.5)
5. Het aanpassen van de login pagina (paragraaf 5.6).

Het toevoegen van een proxy is ook beschreven op:

<http://blogs.technet.com/adfs/archive/2008/06/10/adding-an-adfs-proxy-server.aspx>

5.2 Windows Server 2003 R2 Enterprise Edition configureren

1. Installeer Windows Server 2003 R2 Enterprise Edition op de machine die gaat fungeren als ADFS proxy. Dit kan een bestaande machine zijn, of een nieuwe (mogelijk virtuele) machine. Zorg dat het IP-adres van deze server in DNS op de volgende wijze geregistreerd wordt: extern zal

'adfs.mycampus.nl' moeten resolvable naar de proxy, en intern zal 'adfs.mycampus.nl' nog steeds naar de ADFS server resolvable.

- i Het testen van de proxy kan verlopen door op een client machine tijdelijk de HOSTS file aan te passen naar de nieuwe situatie.
- 2. Zorg dat de tijd op de machine juist is ingesteld, dus dat hij synchroniseert met een time server.
- 3. Installeer Internet Information Services (IIS). Dit doet u via **Start > Control Panel > Add or Remove Programs > Add or Remove Windows Components**.
- 4. Zorg voor een geldig servercertificaat voor de IIS server, ten behoeve van secure connecties (met behulp van TLS/SSL) naar de ADFS proxy (adfs.mycampus.nl). NB: dit kan dus hetzelfde certificaat zijn als eerder geïnstalleerd op de ADFS server.

5.3 Proxy client certificaat genereren

De ADFS proxy zal authenticatie verzoeken doorsturen naar de ADFS server over een HTTPS verbinding. Om dit te kunnen doen moet de proxy zich kunnen authenticeren met een SSL client certificaat. Dit client certificaat en de bijbehorende private key dient te worden aangemaakt op de proxy en het publieke certificaat dient te worden geïmporteerd op de ADFS server. Het client certificaat kan een willekeurig certificaat zijn, maar een self-signed certificaat kan genereerd worden met OpenSSL² op de volgende wijze:


- 5. `openssl req -x509 -nodes -days 3650 -newkey rsa:1024 -keyout proxy.key -out proxy.cer`
- 6. `openssl pkcs12 -export -inkey proxy.key -in proxy.cer -out proxy.pfx`
<kies een wachtwoord dat bij het importeren moet worden gebruikt>
- 7. Open de Microsoft Management Tool met **Start > Run** en door ``mmc`` in te voeren. Voeg een console toe door te kiezen voor **File > Add/Remove Snap-in...** en kies voor **Standalone > Add...** Kies **Certificates** uit de lijst van **Available Standalone Snap-ins** en selecteer **Add**. Kies dan de optie **Computer Accounts** uit de opties voor het type certificaten dat de snap-in gaat beheren, kies **Next** en kies de optie **Local Computer** als de computer die beheerd gaat worden door deze snap-in. Kies dan achtereenvolgens **Finish**, **Close** en **Ok**.
- 8. Navigeer in de console naar **Certificates (Local Computer) > Personal > Certificates**, klik op de rechtermuisknop en kies **All Tasks > Import**. Browse naar de proxy.pfx file (NB: niet de .cer file) en klik op **Next**. Geef

² Een OpenSSL installer voor Windows is beschikbaar via:
<http://www.slproweb.com/products/Win32OpenSSL.html>

het wachtwoord uit stap 2., klik achtereenvolgens op **Next**, **Next** en **Finish**, en sluit de console af (hoeft niet te worden opgeslagen).

5.4 ADFS proxy component installeren


1. Kies **Start > Control Panel > Add or Remove Programs > Add/Remove Windows Components**.
2. Klik in het venster 'Windows Components Wizard' op **Active Directory Services** en vervolgens op **Details**.
3. Klik in het venster 'Active Directory Services' op **Active Directory Federation Services (ADFS)**, en vervolgens op **Details**.
4. Selecteer in het venster 'Active Directory Federation Services (ADFS)', de check box **Federation Service Proxy** en klik vervolgens op **OK**.

 Als Windows hier (of later in de procedure) vraagt of ASP.NET 2.0 moet worden geïnstalleerd, klik dan op **Yes**.

5. Klik op **OK** in het venster 'Active Directory Services'.
6. Klik op **Next** in de Windows Components Wizard.

U komt nu in het venster 'Federation Service Proxy'.

7. Selecteer onder 'Select client authentication certificate' het client server certificaat dat u eerder bij 5.3 hebt gegenereerd. Als er wordt gevraagd om de rechten om de private key te lezen, bevestig deze vraag dan.

 Met het client certificaat wordt de informatie die de ADFS proxy naar de ADFS server stuurt, digitaal ondertekend. Dit certificaat kan een self-signed certificaat zijn, zolang de uitgever van het certificaat maar als een trusted CA wordt opgenomen in de ADFS server zoals beschreven in paragraaf 5.5.

8. Vul onder 'Federation Service Domain Name System host name' de DNS naam van de ADFS account server in: `adfs.mycampus.nl`. Merk op dat deze naam dus (intern) moet resoluten naar de ADFS account server, eventueel door de HOSTS file aan te passen.
9. Er kan nu worden gevraagd waar de installatiefiles zich bevinden. Geef de juiste locatie op, bijvoorbeeld 'R2 Installation Folder\cmpnents\r2' en klik op **OK**.
10. Sluit de procedure af door in het venster 'Completing the Windows Components Wizard' op **Finish** te klikken.

5.5 ADFS proxy certificaat importeren

1. Kopieer de proxy.cer file uit paragraaf 5.3 naar de ADFS server.

2. Kies **Start > All Programs > Administrative Tools > Active Directory Federation Services**.
3. Open de Microsoft Management Tool met **Start > Run** en door `mmc` in te voeren. Voeg een console toe door te kiezen voor **File > Add/Remove Snap-in...** en kies voor **Standalone > Add...** Kies **Certificates** uit de lijst van **Available Standalone Snap-ins** en selecteer **Add**. Kies dan de optie **Computer Accounts** uit de opties voor het type certificaten dat de snap-in gaat beheren, kies **Next** en kies de optie **Local Computer** als de computer die beheerd gaat worden door deze snap-in. Kies dan achtereenvolgens **Finish**, **Close** en **Ok**.
4. Navigeer in de console naar **Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates**, klik op de rechtermuisknop en kies **All Tasks > Import**. Browse naar de proxy.cer file en klik op **Next**. Klik achtereenvolgens op **Next**, **Next** en **Finish**, en sluit de console af (hoeft niet te worden opgeslagen).
5. Dubbelklik op **Federation Service**, dubbelklik op **Trust Policy**, kies met de rechtermuisknop **Properties**, kies het tabblad **FSP Certificates** en selecteer het zojuist geïmporteerde certificaat.

U kunt nu weer van de test service van SURFnet gebruikmaken (<https://wayf.surfnet.nl/attributes>) om te testen of de koppeling werkt.

5.6 Login pagina aanpassen

De standaard login pagina op de ADFS proxy kan nu worden aangepast naar de look-and-feel van uw instelling, door de file **C:\ADFS\sts\Is\clientlogon.aspx** te wijzigen.

Zie voor aanwijzingen ook: [http://msdn.microsoft.com/en-us/library/bb625464\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/bb625464(VS.85).aspx).

Bij voorkeur dient hier tekst te worden opgenomen over:

- de manier waarop gebruikers moeten inloggen, bijv. in welk formaat de user identifier moet worden ingevoerd (bijv. "student nummers" of "NetID")
- een waarschuwing dat (bijv. bij gebruik op publieke terminals), uitloggen alleen voor 100% gegarandeerd kan worden door de browser af te sluiten
- dat bij het inloggen moet worden gelet op een geldige HTTPS URL op de juiste server