

SURFnet federation met Novell Access Manager

prepared for

SURFnet

Disclaimer Novell, Inc. makes no representations or warranties with respect to the contents or use of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose.

Trademarks Novell is a registered trademark of Novell, Inc. in the United States and other countries.

* All third-party trademarks are property of their respective owner.

Copyright 2008 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of Novell, Inc.

Novell, Inc.
404 Wyman Street
Waltham
Massachusetts 02451
USA

Novell Nederland B.V.
Barbizonlaan 25
2908 MB Capele a/d Ijssel
Tel: +31 10 286 4444
Fax: +31 10 286 4010

Prepared By Hans-Robert Vermeulen

SURFnet federation met Novell Access Manager—White Paper

December, 2008

Consultants: Hans-Robert Vermeulen

Revision History

Version	Date	Editor	Revisions
0.1	1-08-2007	Hans-Robert Vermeulen	First Draft – based on A-select Liberty
0.2	11-08-2007	Hans-Robert Vermeulen	Second draft – based on A-select Liberty
1.0	27-08-2007	Hans-Robert Vermeulen	Final version – based on A-select Liberty
1.1	12-11-2007	Hans-Robert Vermeulen	Changed the configuration to SAML2
2.0	08/11/07	Hans-Robert Vermeulen	Amended version based on several implementations

Contents

1	Introductie Federatie	1
1.1	Hoe werkt Federatie?	1
1.1.1	Service Providers en Identity Providers	2
1.1.2	Federatie standaarden	2
1.1.3	Transitive en Persistent Federation	4
1.1.4	Metadata	4
2	Federatie in het onderwijs	5
2.1	Federation bij een koppeling met een commerciële externe partij	5
2.2	Federation bij een fusie of ander samenwerkingsverband	5
2.3	Federation voor specifieke projecten	5
3	Novell Access Manager	7
3.1	Introductie Novell Access Manager	7
3.1.1	De Management Server	7
3.1.2	De Identity Server	7
3.1.3	De Access Gateway	7
3.1.4	De Java Agents	8
3.1.5	De SSLVPN server	8
3.2	Federation met Novell Access Manager	8
3.2.1	Attribute sets	8
3.2.2	Profielen	9
3.2.3	User Matching Expressions	9
4	SURFnet Configuratie	10
4.1	Nuttige links	10
4.2	Afspraken met SURFnet	10
4.3	Novell Access Manager als een Identity Provider aan SURFnet koppelen...	11
4.3.1	Stap 1: Certificaten uitwisselen	11
4.3.2	Stap 2: Het aanmaken van een Attribute Set	12
4.3.3	Stap 3: Het aanmaken van een SAML 2.0 Service Provider	13
4.3.4	Stap 4: Het configureren van de SAML 2.0 Service Provider	13
4.3.5	Stap 5: Signing	14
4.3.6	Stap 6: Test de configuratie	14
4.4	Novell Access Manager als een Service Provider aan SURFnet koppelen...	15
4.4.1	Stap 1: Certificaten uitwisselen	15
4.4.2	Stap 2: Het aanmaken van een Attribute Set	16
4.4.3	Stap 3: Het aanmaken van een SAML 2.0 Identity Provider	17
4.4.4	Stap 4: Het configureren van de SAML 2.0 Identity Provider	17
4.4.5	Stap 5: Signing	20
4.4.6	Stap 6: Test de configuratie	20

1 Introductie Federatie

Identity Federatie gaat over het overdragen van identiteitsgegevens tussen twee partijen. Dit kan zowel tussen organisaties en consumenten als tussen organisaties onderling plaatsvinden. Het doel van dit zogenaamde *federatieve identity management* is vrijwel altijd het vertrouwen en/of authenticeren van personen buiten de eigen organisatie.

Een goed voorbeeld van federatie op grote schaal in Nederland is DigiD. Hoewel hier niet één van de geaccepteerde federation standaarden (zie verderop in dit document) wordt gebruikt, is het principe gelijk. Om de authenticiteit van een belastingaangifte te kunnen bewijzen richting de belastingdienst is verificatie van uw identiteit bij een vertrouwde derde partij (DigiD) nodig. De authenticatie (wie) vindt dus extern plaats. De autorisatie (wat) blijft in handen van de belastingdienst.

Een ander goed voorbeeld is de rol die SURFnet wil gaan vervullen binnen de SURFfederatie. De SURFfederatie is een federatieve dienst die onderwijsinstellingen en derden met elkaar kan koppelen. Middels federatie en single sign-on (SSO) zal het voor studenten en medewerkers mogelijk zijn om na het aanmelden bij hun eigen instelling alle diensten (services) van derden te benaderen zonder additioneel in te hoeven loggen. Een groot voordeel voor de studenten die geen extra identiteiten en wachtwoorden hoeven te onthouden.

Naast eindgebruikers ondervinden ook de aangesloten dienstverleners (Service Providers) grote voordelen van federatie. Afhankelijk van de opzet hoeft er namelijk weinig tot wellicht helemaal geen identiteit management plaats te vinden. De onderwijsinstelling (Identity Provider) wordt immers vertrouwd de juiste gegevens aan te leveren, op basis waarvan de dienstverlener toegang tot de relevante informatie kan bieden.

1.1 Hoe werkt Federatie?

Zoals uit bovenstaande introductie blijkt is een federatieve koppeling eigenlijk meer een vertrouwensrelatie tussen minimaal twee partijen. Meestal zullen deze partijen een klant – dienstverlener relatie onderhouden.

De klant is in deze niet altijd gelijk aan de eindgebruiker. Veelal zal een klant een bedrijf, of in ons geval een onderwijsinstelling zijn. De eindgebruikers maken dus gebruik van de diensten die door de dienstverlener worden aangeboden op basis van hun rol binnen een organisatie.

Een groot probleem binnen deze klant – dienstverlener relatie is het onderhoud van identiteiten.

Eindgebruikers moeten weer een andere gebruikersnaam en wachtwoord onderhouden en eventuele extra gegevens (adres, email, etc.) onderhouden.

De dienstverlener moet de gebruikersgegevens beschermen en een eventuele database met deze gegevens aanmelden in het kader van de wet op de persoonsbescherming.

De organisatie is niet gebaat (productiviteitsverlies, helpdesk ondersteuning) bij de problemen die kunnen ontstaan door het bestaan van weer een set identiteitsgegevens in een extern systeem.

Hier biedt federatie een directe oplossing.

Er wordt een vertrouwensrelatie opgebouwd tussen de klant en de dienstverlener, met heldere afspraken over de gegevens die verstrekt moeten worden om een dienst te kunnen benutten.

De klant stuurt alle relevante gegevens van de eindgebruiker mee tijdens de authenticatie, zodat de dienstverlener bijvoorbeeld autorisatie van de gebruiker en facturatie van de gebruikte functionaliteit kan uitvoeren.

Aangezien de dienstverlener de identiteitsgegevens niet hoeft op te slaan, zal er veelal geen relatie met de wet op de persoonsbescherming ontstaan.

De eindgebruiker hoeft geen additionele gebruikersnaam en wachtwoord te onthouden. Zolang hij maar is aangemeld bij het eigen interne systeem zal Single Sign-On worden toegepast. Hiermee wordt de aangeboden dienst een verlenging van het interne systeem.

Een service desk hoeft zich niet te bekommeren met weer een extra set aan inlog gegevens en gebruikers die hiervan de naam of het wachtwoord zijn vergeten.
etc.

De voordelen van federatie zijn dus legio.

In de volgende paragrafen worden de onderdelen van federatie en de relatie tussen de onderdelen uitgelegd.

1.1.1 Service Providers en Identity Providers

De termen Service Provider (SP) en Identity Provider (IDP) zijn net al benoemd. In bovenstaande voorbeelden is het duidelijk dat de belastingdienst of bijvoorbeeld SURFnet, Elsevier of Kluwer als dienstverlenende partij fungeert. Binnen de federatie termen zijn zij dus de Service Provider.

De onderwijsinstellingen, of DigiD uit ons voorbeeld fungeren hierbij als de Identity Provider, de partij die de authenticatie uitvoert en de identiteit verifieert.

Een partij kan tevens zowel als IDP als als SP optreden. Een universiteit bijvoorbeeld kan dienstverlener zijn (bijvoorbeeld de bibliotheek) en tegelijkertijd diensten afnemen.

1.1.2 Federatie standaarden

De belangrijkste standaarden op federatie gebied zijn:

- SAML 1.0
- SAML 1.1
- Liberty 1.2
- SAML 2.0
- WS-federation

In de praktijk zullen Liberty 1.2 en SAML 2.0 het meest gebruikt worden. SAML 1.0 en 1.1 worden echter nog door veel producten ondersteund.

Verschillende producten bieden verschillende mogelijkheden. Met Novell Access Manager worden bijvoorbeeld al deze standaarden ondersteund.

Hoewel de federation standaarden al vrij lang bestaan, is federatie zelf pas sinds kort echt in opkomst bij een groter publiek. Dankzij de standaardisatie is het mogelijk om producten van verschillende leveranciers (Novell, Oracle, IBM, A-select, etc.) met elkaar te verbinden. Hoe het een en ander geconfigureerd wordt is echter een totaal verschillend verhaal.

Dit is dan ook meteen een punt waar complexiteit om de hoek komt. Kan een implementatie als Novell Access Manager in 1 keer alle MetaData van een federatieve koppeling inlezen, bij andere producten moet de MetaData worden uitgeplozen en handmatig worden ingevoerd. Dit is natuurlijk foutgevoeliger, maar kan ook voor miscommunicatie zorgen. Ook zullen sommige termen anders zijn gebruikt en zullen gegevens uit Log bestanden niet altijd makkelijk te vergelijken zijn.

Geen probleem als alles functioneert, maar als er iets niet werkt, zullen de beheerders aan beide zijden (zowel aan de IDP als de SP zijde) moeten kijken waar de fout zit. Dit kan de nodige tijd kosten.

1.1.2.1 SAML 1.0 / 1.1

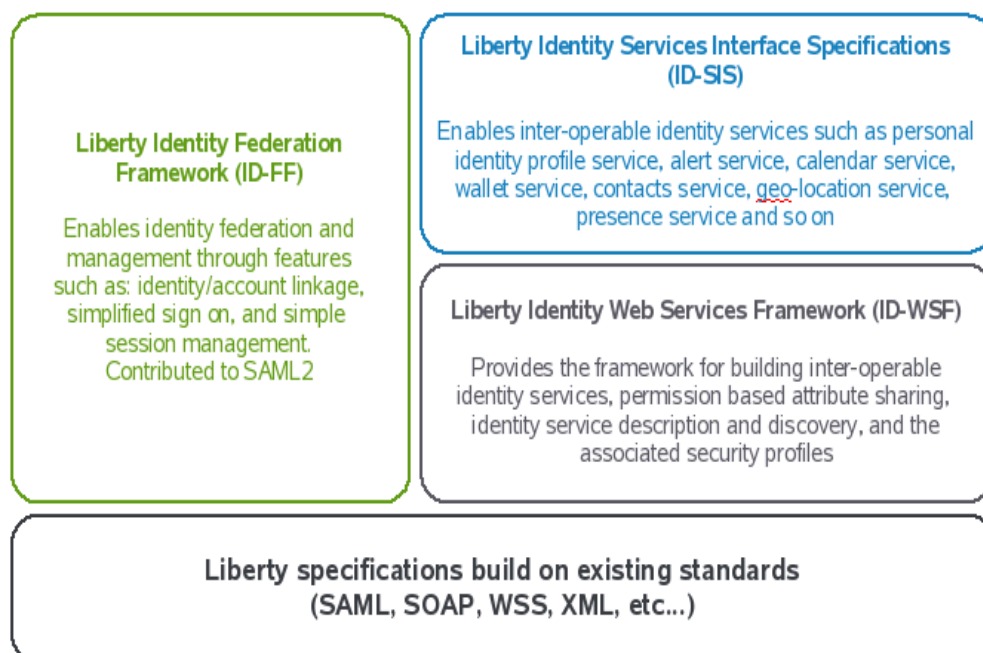
SAML is een OASIS standaard die stamt uit 2002. Meer informatie over de SAML 1.0 en 1.1 standaarden is te vinden op:

<http://www.oasis-open.org/specs/index.php#samlv1.0>

<http://www.oasis-open.org/specs/index.php#samlv1.1>

1.1.2.2 Liberty 1.2

Liberty 1.2 is gedeeltelijk parallel aan SAML 1.1 ontwikkeld. Delen van Liberty 1.2 hebben de basis gevormd voor SAML 2.0 Zo is het Liberty Identity-Federation Framework (ID-FF) aan SAML 2.0 toegevoegd.



Wellicht het grootste voordeel van Liberty is dat deze standaard eind gebruikers veel meer controle kan geven over de informatie (attributen) die gedeeld worden tussen de IDP en SP. Daar waar andere federation standaarden enkel om toestemming voor de federatie vragen gaat Liberty dus verder. In een eCommerce omgeving zou een gebruiker bijvoorbeeld gevraagd kunnen worden of zijn Creditcard gegevens, of persoonlijke adres gegevens gedeeld mogen worden.

In een eBusiness omgeving zal over het algemeen de beheerder bepalen welke gegevens gedeeld worden en biedt Liberty op dit vlak geen voordelen.

Meer informatie is te vinden op:

http://www.projectliberty.org/index.php/liberty/specifications__1

http://www.projectliberty.org/index.php/liberty/liberty_interoperable/interoperable_products

http://www.projectliberty.org/liberty_interoperable/interoperable_products/saml_2_0_test_procedure_v1_0_interoperable_product_table

1.1.2.3 SAML 2.0

De opvolger van SAML 1.1, met daarin onderdelen van Liberty 1.2 verwerkt is SAML 2.0. Dit is de standaard die momenteel het meest gebruikt en geaccepteerd wordt.

Meer informatie is te vinden op:

<http://www.oasis-open.org/specs/index.php#samlv2.0>

<http://www.oasis-open.org/committees/download.php/13525/sstc-saml-exec-overview-2.0-cd-01-2col.pdf>

1.1.3 Transitive en Persistent Federation

Binnen Novell Access Manager kunnen we drie vormen van federation onderscheiden:

- Transitive federation
- Persistent federation – User matching
- Persistent federation – User creation

1.1.3.1 Transitive Federation

Transitive Federation, of vrij vertaald tijdelijke federatie is een manier om zonder fysieke identiteit aan de SP zijde toch federatie tot stand te brengen. Er wordt dus nimmer data van een gebruiker opgeslagen aan de SP zijde, ledere keer dat een gebruiker zichzelf wil aanmelden bij de SP zijde, moet dit via de federatieve koppeling met de IDP gebeuren.

1.1.3.2 Persistent Federation

Bij Persistent Federation worden twee identiteiten aan elkaar verbonden middels een federatie. Zowel de Identity provider als de Service provider moeten dus over relevante identiteitsinformatie beschikken. Deze identiteiten hoeven niet gelijk te zijn. Veelal zal de gebruiker gevraagd worden om met zijn twee bestaande identiteiten in te loggen waarna deze middels federatie met elkaar verbonden zijn.

Novell Access Manager is in staat om, indien er geen account aan de SP zijde bestaat, automatisch een account aan te maken. Dit account kan op basis van de beschikbare attributen worden gegenereerd.

1.1.4 Metadata

De Metadata van een federatieve koppeling bevat alle relevante gegevens om de koppeling tot stand te kunnen brengen. Per protocol (SAML, Liberty) worden hier de gegevens opgenomen voor bijvoorbeeld:

- Gebruikte certificaten
- URL voor Single Logout
- URL voor Federation Termination
- URL voor Federation Termination Notification
- URL voor Single Sign-On
- etc.

Op basis van deze metadata weten de IDP en SP onderling aan welke URL's zij hun verzoek tot authenticatie, federatie, etc. moeten richten.

2 Federatie in het onderwijs

Zoals uit de eerder genoemde voorbeelden en voordelen reeds is gebleken, blijkt federatie ook een zeer goed toe te passen oplossing binnen het onderwijs. Niet alleen bij universiteiten en hogescholen, maar bij bijna ieder onderwijsinstelling,

Een paar voorbeelden worden in de volgende paragrafen uitgewerkt.

2.1 Federation bij een koppeling met een commerciële externe partij

Er zijn vele (commerciële) aanbieders van content die diensten aan het onderwijs leveren. Denk hierbij bijvoorbeeld aan SURFnet, Kennisnet, Kluwer, Elsevier e.d.

Dit zijn zonder uitzondering partijen waarmee een federatieve koppeling een uitgekende oplossing biedt. U maakt afspraken met de leverancier, uw studenten kunnen gebruik maken van de diensten zonder dat de aanbieder(s) alle nieuwe identiteiten hoeven te beheren.

Een student bevestigt de federatie en kan gebruik maken van de aangeboden diensten. De dienstverlener kan op basis van de attributen binnen de sessie bepalen:

Waar een gebruiker toegang toe krijgt.

Of er logging moet plaatsvinden voor bijvoorbeeld facturatie aan de instelling.
etc.

Een van de attributen kan bijvoorbeeld een studierichting zijn, op basis waarvan specifieke content ontsloten kan worden. Een attribuut kan ook een status weergeven, om bijvoorbeeld een student die net is afgestudeerd gedurende een bepaalde periode toegang te verlenen tot een specifieke banen database.

2.2 Federation bij een fusie of ander samenwerkingsverband

Stel, uw onderwijsinstelling gaat een samenwerkingsverband aan met een andere onderwijsinstelling om de hoek, of in het kader van een uitwisselingsprogramma, met een (studierichting) bij een onderwijsinstelling in het buitenland.

In beide gevallen kan een federatieve koppeling ervoor zorgen dat uw studenten binnen afzienbare tijd toegang kunnen krijgen tot de systemen van de andere instelling en natuurlijk omgekeerd, de studenten van de andere instelling kunnen gebruik gaan maken van uw informatiesystemen.

Dit alles zonder dat u:

Identiteiten moet synchroniseren tussen de partijen

Studenten een extra gebruikersnaam en wachtwoord hoeven te onthouden

Software hoeft te schrijven voor koppelingen.

En dat alles gebaseerd op open standaarden, waardoor het mogelijk is om met ieder instantie een koppeling te realiseren naar uw wensen.

2.3 Federation voor specifieke projecten

Tussen universiteiten en het bedrijfsleven zijn legio samenwerkingsverbanden. Denk hierbij aan onderzoeksprojecten, zoals bijvoorbeeld de samenwerking in het kader van de World Solar Challenge tussen de TU Delft en Nuon. Veel van dit soort projecten vergen een intensieve

samenwerking tussen specifieke projectgroepen binnen de betrokken partijen, waarbij de geheimhouding en beveiliging een struikelblok vormt.

Federation kan ook hier de oplossing zijn waardoor specifieke groepen gebruikers bij elkaars data kunnen, terwijl de rest van de organisatie geen toegang heeft.

Deze oplossing zou mogelijk gemaakt worden door de Access Control van Novell Access Manager in combinatie met federation. Op attribuut niveau kan worden bepaald wie waar toe toegang heeft, waarbij ook voor gebruikers die middels een federatieve koppeling toegang proberen te verkrijgen specifieke eisen kunnen worden gesteld aan bijvoorbeeld de manier van authenticatie (Gebruikersnaam / Wachtwoord, Certificaat, token, of combinatie hiervan.)

3 Novell Access Manager

3.1 Introductie Novell Access Manager

Novell Access Manager is een oplossing waarmee u op veilige wijze toegang kunt verlenen tot interne en externe (web) applicaties. Novell Access Manager biedt u:

Toegang zonder risico's.

Uw gebruikers kunnen op een veilige manier toegang krijgen tot uw web applicaties en interne server applicaties.

Toegang wordt gebaseerd op de rol die een gebruiker heeft binnen de organisatie.

Single Sign-on.

Alle interne wachtwoorden kunnen door Novell Access Manager worden opgeslagen en afgevangen waardoor een gebruiker nog enkel een (sterk beveiligd) wachtwoord hoeft te onthouden.

Vereenvoudigde Federatie.

Zonder additionele software op web servers is het mogelijk federatieve koppelingen op te zetten tussen partijen.

Gecentraliseerd beheer.

Tools om te voldoen aan wettelijke regelgeving.

Novell Access Manager biedt rapportage mogelijkheden om te voldoen aan de Sarbanes-Oxley, HIPAA, Europese Unie en andere privacy wet- en regelgeving.

3.1.1 De Management Server

De Management server bevat de configuratie van de gehele oplossing. Alle afzonderlijke Novell Access Manager componenten melden zich bij de Management Server aan om hun configuratie uit te lezen. Het beheer van de oplossing vindt plaats via een speciale iManager configuratie die ook op de Management Server draait.

3.1.2 De Identity Server

De Identity server verzorgt alle authenticatie en federatie van gebruikers. Hierbij worden gebruikers via eDirectory, SUNone of Active Directory, of een combinatie hiervan aangemeld. LDAP wordt als onderliggend protocol gebruikt.

3.1.3 De Access Gateway

De Access Gateway is een zogenaamde reverse proxy die tussen de gebruiker en de web applicatie staat. Op de Access Gateway wordt alle autorisatie geregeld. Toegang wordt geweigerd of verleend op basis van policies die gekoppeld zijn aan web resources. Toegang kan worden verleend op basis van de rol die een gebruiker binnen de organisatie heeft. Bijvoorbeeld op basis van groepslidmaatschap of bepaalde attributen.

De Access Gateway heeft als voordeel dat er geen additionele software op de webserver hoeft te worden geïnstalleerd.

De Access Gateway vertaalt Identity Server authenticaties naar standaard HTTP headers, waarmee de meeste web applicaties overweg kunnen. Het is tevens mogelijk om authenticatie naar achterliggende systemen op basis van web formulieren (naam en wachtwoord op de web pagina) te automatiseren.

3.1.4 De Java Agents

Novell Access Manager biedt IBM WebSphere, BEA WebLogic en JBoss agents die autorisatie en toegang bieden tot servlets en Enterprise JavaBeans (EJBs). Deze agents gebruiken Java Authentication and Authorization Service (JAAS), Java Authorization Contract voor Containers (JACC) en interne Web-server APIs voor authenticatie. Tezamen leveren zij granulaire, policy-gebaseerde autorisatie en toegang tot servlets en EJBs.

3.1.5 De SSLVPN server

Novell Access Manager biedt een Secure Sockets Layer Virtual Private Network (SSL VPN), een Linux-gebaseerde dienst die beveiligde toegang biedt tot niet HTTP gebaseerde applicaties. Deze dienst deelt sessie informatie met de Access Gateway, waardoor Single Sign-on mogelijk is naar de achterliggende applicaties. De SSLVPN server ondersteunt client-integrity checking om ervoor te zorgen dat specifieke bedrijfssoftware, zoals firewalls of virus scanners aanwezig zijn voordat toegang wordt verleend..

3.2 Federation met Novell Access Manager

Zoals eerder genoemd, ondersteunt Novell Access Manager 3.0 de meest gangbare federatieve protocollen. Zowel als Identity Provider, alsook als Service Provider is Novell Access Manager eenvoudig te configureren. Wel blijft het van belang duidelijke afspraken te maken met de te koppelen partij over de benodigde attributen, het te gebruiken protocol, en de specifieke instellingen die hieraan verbonden zijn.

Zo is het bijvoorbeeld mogelijk om federation via Artifact of Post te laten plaatsvinden. Bij gebruik van de Artifact methodiek, communiceren de IDP en SP rechtstreeks met elkaar. Dit is over het algemeen een veiligere methode als de Post methode, waarbij de browser van de gebruiker optreedt als intermediair en alle communicatie via de browser van de gebruiker loopt.

Zo zijn er veel keuzes die kunnen worden gemaakt. Verderop in dit document staat een beschrijving van de koppeling met SURFnet en de gekozen instellingen. In veel gevallen zijn dit de standaard instellingen, echter afhankelijk van uw wensen en de mogelijkheden bij de tegenpartij zou er in de praktijk van kunnen worden afgeweken.

Hieronder worden de verschillende, Novell Access Manager specifieke, onderdelen die geconfigureerd moeten worden voor een federatieve koppeling besproken.

3.2.1 Attribute sets

Een Attribute set is een verzameling van attributen zoals naam, email adres, geboortedatum, etc. Een Service Provider kan vragen om attributen. Een Identity Provider kan attributen meegeven met de authenticatie. Bij Liberty is het mogelijk om een gebruiker toestemming te laten geven voor de overdracht van (afzonderlijke) attributen.

Het is afhankelijk van de gekoppelde diensten welke attributen moeten worden uitgewisseld. De gebruikersnaam zal bijvoorbeeld altijd noodzakelijk zijn, echter overige gegevens zijn alleen voor specifieke doeleinden noodzakelijk.

Een attribute set is enkel een verzameling van attributen. Bij de configuratie van de SP of IDP wordt uiteindelijk bepaald welke attributen werkelijk gebruikt worden. Pas als er aan beide ziden (SP en IDP) een match is zullen deze attributen ook daadwerkelijk uitgewisseld worden. Bijvoorbeeld, cn, full name en email address worden door de IDP aangeboden. De SP vraagt om cn, email address en credit card. In dit scenario zullen dus enkel de cn en het email adres worden uitgewisseld.

SURFnet wenst (in ieder geval voor hun test omgeving) minimaal de cn of uid van de gebruiker te ontvangen. Dit is een normale minimale vereiste, aangezien de Service Provider moet weten wie er toegang wil krijgen.

3.2.1.1 Attribute Mapping

Hoewel veel is gestandaardiseerd, toch zullen we niet altijd dezelfde taal praten. Om dit probleem op te lossen is het mogelijk om attribute mapping uit te voeren. Hierbij kan een specifiek attribuut, bekend onder NaamX binnen het lokale systeem vertaald worden naar NaamY voor communicatie met het gekoppelde systeem.

Het is hierdoor bijvoorbeeld mogelijk om het CN attribuut te mappen naar het UID attribuut, of om custom LDAP attributen zoals een studentnummer te koppelen aan een meer algemeen of overeengekomen attribuut.

3.2.2 Profielen

De beschikbare attributen voor de Attribute set komen bij Novell Access Manager uit de volgende profielen:

- Personal Profile
- Employee Profile
- Custom Profile
- LDAP Attribute Profile

De eerste drie profielen staan onder de “Web Service Provider” link van de Liberty tab van de Identity Server. het LDAP profiel staat onder de “LDAP Attribute Mapping” link van de Liberty tab van de Identity Server.

3.2.3 User Matching Expressions

User Matching Expressions worden gebruikt om federatieve gebruikers te koppelen aan bestaande gebruikers.

Door attributen te vergelijken kunnen SP en IDP bijvoorbeeld een match leggen tussen twee bestaande identiteiten. De complexiteit van een User Matching Expression hangt af van enerzijds de beschikbare attributen aan de IDP zijde en anderzijds de beschikbare attributen aan de SP zijde. Het zal niet in alle gevallen mogelijk zijn een match te leggen met bestaande gebruikers. Een paar voorbeelden.

Jan van den Broek, Jan01 aan de IDP zijde kan gekoppeld worden met Broekvd_J aan de SP zijde op basis van een gelijke voornaam, achternaam en email adres.

Het kan echter ook het geval zijn dat aan de IDP zijde de achternaam als “van den Broek” wordt weggeschreven, terwijl aan de SP zijde het bestaande account onder “Broek, van den” is weggeschreven. Nu wordt het al moeilijker om een match te leggen.

Indien er geen match gevonden is, en automatische account creatie (user provisioning) niet aangezet kan of mag worden, dan kan de gebruiker gevraagd worden om eenmalig in te loggen bij de SP. Hierdoor wordt de federatie tussen beide accounts tot stand gebracht. Hierna zal de gebruiker altijd automatisch ingelogd worden.

4 SURFnet Configuratie

4.1 Nuttige links

De volgende URLs zijn van belang voor de configuratie:

De algemene SURFnet SURFfederatie website:

<http://federatie.SURFnet.nl/>

De Metadata van de productieomgeving van SURFnet:

Voor SAML 2.0 Identity Providers:

<http://federatie.surfnet.nl/metadata-sfs-sp-saml20-signed.xml>

Voor SAML 2.0 Service Providers:

<http://federatie.surfnet.nl/metadata-sfs-idp-saml20-signed.xml>

De Metadata van de testomgeving van SURFnet:

Voor SAML 2.0 Identity Providers:

<https://wayf-test.surfnet.nl/wayf-test-saml20-metadata-sp.xml>

Voor SAML 2.0 Service Providers:

<https://wayf-test.surfnet.nl/wayf-test-saml20-metadata-idp.xml>

4.2 Afspraken met SURFnet

Alvorens aan de configuratie te beginnen is het slim om contact op te nemen met SURFnet via het volgende email adres: federatie-beheer@SURFnet.nl

SURFnet heeft inmiddels duidelijke eisen gesteld ten aanzien van de aansluiting. Zo zult u een overeenkomst met SURFnet moeten tekenen, waarbij een aantal zaken formeel wordt afgehandeld.

Daarnaast heeft SURFnet een duidelijke beschrijving van de benodigde attributen gemaakt. Al deze informatie is op <http://federatie.SURFnet.nl/> terug te vinden.

Het is van belang om met SURFnet de volgende onderwerpen te bespreken om de koppeling met de SURFfederatie te realiseren:

Uitwisseling metadata en certificaten.

Van welke diensten wilt u gebruik gaan maken?

Uitwisseling van attributen (basis en gerelateerd aan de specifieke diensten.)

Specifieke URLs om de configuratie te kunnen testen.

De naamgeving die SURFnet gaat hanteren en waaronder uw organisatie terug is te vinden op de login pagina van SURFnet.

Een contact persoon om uw configuratie mee te kunnen testen.

Uitwisseling van LOG files bij eventuele problemen met de configuratie.

SURFnet biedt meerdere opties om te verbinden, zowel via de proprietary manier van A-select, alsook via gestandaardiseerde federatie protocollen. Voor Novell Access Manager is het van belang dat SURFnet de SAML 2.0 standaard officieel ondersteund.

Dit document zal de koppeling tussen Novell Access Manager en SURFnet op basis van SAML 2.0 beschrijven.

Novell Access Manager kan aan SURFnet gekoppeld worden als Service Provider (SP) of als Identity Provider (IDP.) Het is ook mogelijk om beide rollen te vervullen.

Fungeren als een IDP is bijvoorbeeld aan de orde als een Universiteit of hoge school diensten van SURFnet of een van de aangesloten partners, de zogenaamde Service Providers, wil afnemen.

Wilt uw instantie zelf ook diensten aanbieden aan andere partijen, dan zult u (ook) een configuratie als SP moeten inrichten.

Voordat u kunt koppelen met SURFnet zullen onderlinge afspraken gemaakt moeten worden tussen de onderwijsinstelling of diensten aanbieder en SURFnet. Onderstaande configuratie is dus een richtlijn en zal alleen tot stand kunnen komen in samenwerking met SURFnet.

4.3 Novell Access Manager als een Identity Provider aan SURFnet koppelen

Deze configuratie is bijvoorbeeld aan de orde als een Universiteit of hoge school diensten van SURFnet of een van de aangesloten partners, de zogenaamde Service Providers, wil afnemen.

4.3.1 Stap 1: Certificaten uitwisselen

Als eerste stap moeten er certificaten worden uitgewisseld. Novell Access Manager kan indien de tegenpartij dit toelaat rechtstreeks de Public key van een Certificate Authority (de trusted root) uitlezen. Als dit niet mogelijk is kan de tegenpartij een DER of PEM export van dit certificaat aanleveren.

Zorg er in ieder geval altijd voor dat:

- De Certificate Authority van de tegenpartij wordt geïmporteerd en toegevoegd aan de NIDP trust store.

- Eventueel ook expliciet het Server certificate van de tegenpartij wordt geïmporteerd en toegevoegd aan de NIDP trust store.

4.3.1.1 Exporteren van de trusted root aan de Novell Access Manager zijde

SURFnet is in staat om de benodigde certificaat informatie uit de metadata van uw configuratie te halen. Vraagt SURFnet echter om een export, dan kunt u de volgende stappen doorlopen.

Selecteer binnen iManager het onderdeel "Certificates" onder Novell Access Manager.

- Klik op de "Trusted Roots" tab

- Klik op de juiste Trusted Root (Standaard de Config-CA)

- Klik op "Export Public Certificate"

- Selecteer het gewenste formaat (DER of PEM)

- Het bestand zal nu als een download via de browser worden aangeboden.

Standaard is de Config-CA gegenereerd door de Management Server. Er kan echter ook volledig met externe certificaten gewerkt worden van bijvoorbeeld Thawt, Verisign, etc.

Het certificaat dient aangeboden te worden aan SURFnet, zodat zij deze in hun configuratie kunnen opnemen.

4.3.1.2 Importeren van de ontvangen trusted root van SURFnet

De trusted root van de productie omgeving is te downloaden via <http://federatie.surfnet.nl/sfs-signing-certificate.pem>

Om dit certificaat te importeren moeten de volgende stappen worden doorlopen.

Selecteer binnen iManager het onderdeel "Certificates" onder Novell Access Manager.

- Klik op de "Trusted Roots" tab

Klik op "Import"

Geef het certificaat een naam, bijvoorbeeld SurfSNS-CA.

Browse naar het certificaat en selecteer dat

Klik op OK.

De Trusted Root wordt nu toegevoegd.

Vervolgens moeten we de Trusted Root nog aan de NIDP Trust Store toevoegen.

Plaats een vinkje voor het zojuist geïmporteerde certificaat

Klik op "Add Trusted Roots to Trust Stores"

Klik op het "Select Keystore" icoon rechts in het pop-up scherm

Plaats een vinkje voor de NIDP-truststore

Klik twee maal op OK.

Note: Binnen de test omgeving van SURFnet wordt gebruik gemaakt van zogenaamde self-signed certificaten. Hierdoor is het mogelijk om het certificaat rechtstreeks uit de metadata te importeren.

Ga hiervoor naar de metadata URL van SURFnet en kopieer alle gegevens tussen de `<ds:X509Certificate>` en `</ds:X509Certificate>` XML tags.

In plaats van de eerder beschreven stap "Browse naar het certificaat en selecteer dat" kun je nu deze data plakken in het scherm. Let er wel op dat je de data tussen de volgende tags toevoegt:

```
-----BEGIN CERTIFICATE-----
```

```
<hier het certificaat>
```

```
-----END CERTIFICATE-----
```

4.3.2 Stap 2: Het aanmaken van een Attribute Set

Selecteer binnen iManager het onderdeel "Identity Server" onder Novell Access Manager.

Klik op de "Shared Settings" tab.

Klik op "New" onder de Attribute Sets.

Geef de Attribute Set een naam, bijvoorbeeld SURFnetFederatie

Klik vervolgens op "New" om attributen toe te voegen. Hierbij kunnen attributen uit de verschillende profielen worden gekozen.

Over het algemeen zullen de attributen die we als IDP gaan aanbieden aan SURFnet uit onze LDAP directory komen. In dit voorbeeld zullen we dan ook de volgende LDAP attributen aan SURFnet aanbieden door deze in de Attribute Set op te nemen:

LDAP attribute: cn

LDAP attribute: sn

LDAP attribute: givenName

LDAP attribute: email

Let ook op de mapping. SURFnet kan bijvoorbeeld verlangen dat het attribuut **urn:mace:dir:attribute-def:mail** wordt verzonden, terwijl uw LDAP server het attribuut Studentmail kent. Selecteer hiervoor uw LDAP attribuut en vul bij de mapping de gewenste SURFnet notatie in.

De gewenste notatie en de benodigde attributen zijn terug te vinden op <http://www.surfnet.nl/nl/Thema/SURFfederatie/over/Pages/Attributenschema.aspx>

Let er op dat u niet de korte notaties gebruikt (uid, cn, givenName) maar de notatie zoals deze verderop op de pagina van SURFnet wordt weergegeven. Bijvoorbeeld:

```
urn:mace:dir:attribute-def:uid
```

urn:mace:dir:attribute-def:sn
 urn:mace:dir:attribute-def:givenName
 etc.

Note: SURFnet heeft afspraken gemaakt met de diverse Service Providers (Kluwer, Elsevier, etc.) over de te gebruiken attributen. Door deze standaardisatie wordt wildgroei voorkomen en zult u ten alle zijden slechts een beperkte hoeveelheid attributen aan hoeven leveren. Momenteel zijn er 15 attributen die SURFnet selectief naar de betrokken Service Providers doorstuurt.

4.3.3 Stap 3: Het aanmaken van een SAML 2.0 Service Provider

Omdat uw Novell Access Manager configuratie als Identity Provider naar SURFnet toe gaat fungeren en dus SURFnet als een Service Provider gaat fungeren, moet u binnen Novell Access Manager een Service Provider configuratie aanmaken waarin u de gegevens van de SURFnet zijde configureert.

Selecteer binnen iManager het onderdeel "Identity Server" onder Novell Access Manager.

Klik op de "Edit" link onder Configuration.

Klik op "New" onder de SAML 2.0 tab en selecteer Service Provider.

Voer een naam in, bijvoorbeeld SURFnetSP en voer de metadata URL in, of plak de metadata in het tekst veld en klik op "Next."

Controleer of de juiste certificaat gegevens aanwezig zijn en klik op "Next."

De SP is nu aangemaakt maar moet nog worden geconfigureerd.

4.3.4 Stap 4: Het configureren van de SAML 2.0 Service Provider

De configuratie van een externe SP heeft niet veel om handen.

Selecteer binnen iManager het onderdeel "Identity Server" onder Novell Access Manager.

Klik op de "Edit" link onder Configuration.

Klik op de zojuist aangemaakte Service Provider onder de SAML 2.0 tab (SURFnetSP.)

Klik op de Access tab. De instellingen moeten hier standaard zijn, zoals weergegeven in onderstaande figuur.

Security

Encrypt assertions
 Encrypt name identifiers

SOAP Back Channel Security Method

Message Signing
 Mutual SSL
 Basic Authentication

Send:

Name:
 Password:

Verify:

Name:
 Password:

Klik op Attributes

Selecteer de eerder aangemaakte Attribute Set en voeg de attributen toe die je mee wilt of moet sturen. Dit zijn waarschijnlijk alle attributen die zijn opgenomen in de Attribute Set.

Klik op Authentication

Authentication response binding moet voor SURFnet op Post staan.

Persistent en Transient identifier format staan beiden geselecteerd. Persistent is de default (standaard instelling)

Use proxied requests en Provide discovery services staan beiden aan (standaard instelling)

Authentication response binding:

Supported identity formats	Use	Default
Persistent identifier format:	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Transient identifier format:	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Use proxied requests

Sla alle instellingen op en klik op "Update All" in de Identity Server iManager task.

4.3.5 Stap 5: Signing

Als extra beveiliging (naast communicatie over een SSL verbinding) moet signing worden aangezet.

Selecteer binnen iManager het onderdeel "Identity Server" onder Novell Access Manager.

Klik op de "Edit" link onder Configuration.

Under "Identity Provider" enable "Require Signed Authentication Requests"

Under "Identity Consumer" enable both "Require Signed Assertions" and "Sign Authentication Requests"

Note: Indien er na het zetten van de "Require Signed Authentication Requests" optie een 300101008 foutmelding wordt afgegeven op de communicatie tussen de Identity Server en de Access Gateway, dan moeten de volgende acties worden uitgevoerd die er voor zorgen dat tussen de Identity Server en de Access Gateway de metadata opnieuw wordt uitgewisseld.

Ga naar Access Gateways

Klik op Edit

Klik op Reverse Proxy / Authentication

Zet de optie voor "identity Server Cluster" op [none]

Ok / Apply Changes / Update All.

Volg de prompt op en doe ook een Update All op de Identity Server.

Ga terug naar Access Gateways

Klik op Edit

Klik op Reverse Proxy / Authentication

Voeg de Identity Server weer toe.

Ok / Apply Changes / Update All.

Volg de prompt op en doe ook een Update All op de Identity Server.

4.3.6 Stap 6: Test de configuratie

Open een verse browser en ga naar de volgende URL om de koppeling te testen:

Voor de Test omgeving is dit: <https://wayf-test.surfnet.nl/attributes>

Voor de Productie omgeving is dit <https://espee.surfnet.nl/attributes>

Selecteer uit de lijst jouw organisatie. SURFnet heeft aan hun zijde Novell Access Manager als Identity server geconfigureerd. SURFnet geeft deze configuratie een naam, waarschijnlijk de naam

van jouw organisatie en door hierop te klikken kun je alle SURFnet diensten benaderen terwijl de authenticatie door jouw Novell Access Manager systeem wordt afgehandeld.

Je wordt na het aanklikken van de eigen organisatie dan ook doorgestuurd naar jouw Identity Server voor authenticatie. Log in met een gebruiker en als alles aan beide kanten goed is geconfigureerd wordt je terug gerouteerd naar SURFnet en de aangevraagde dienst. In dit geval zul je exact zien welke attributen en welke waarden worden doorgegeven.

4.4 Novell Access Manager als een Service Provider aan SURFnet koppelen

Deze configuratie is bijvoorbeeld aan de orde als een Universiteit of hoge school zelf diensten wil aanbieden aan andere onderwijsinstellingen via SURFnet.

4.4.1 Stap 1: Certificaten uitwisselen

Stap 1 is gelijk aan stap 1 voor de IDP configuratie. Heeft u reeds een SURFnet koppeling gemaakt met Novell Access Manager als de IDP, dan kunt u deze stap overslaan en doorgaan bij Stap 2.

Als eerste stap moeten er certificaten worden uitgewisseld. Novell Access Manager kan indien de tegenpartij dit toelaat rechtstreeks de Public key van een Certificate Authority (de trusted root) uitlezen. Als dit niet mogelijk is kan de tegenpartij een DER of PEM export van dit certificaat aanleveren.

Zorg er in ieder geval altijd voor dat:

- De Certificate Authority van de tegenpartij wordt geïmporteerd en toegevoegd aan de NIDP trust store.

- Eventueel ook expliciet het Server certificate van de tegenpartij wordt geïmporteerd en toegevoegd aan de NIDP trust store.

4.4.1.1 Exporteren van de trusted root aan de Novell Access Manager zijde

Selecteer binnen iManager het onderdeel "Certificates" onder Novell Access Manager.

- Klik op de "Trusted Roots" tab

- Klik op de juiste Trusted Root (Standaard de Config-CA)

- Klik op "Export Public Certificate"

- Selecteer het gewenste formaat (DER of PEM)

- Het bestand zal nu als een download via de browser worden aangeboden.

Standaard is de Config-CA gegenereerd door de Management Server. Er kan echter ook volledig met externe certificaten gewerkt worden van bijvoorbeeld Thawt, Verisign, etc.

Het certificaat dient aangeboden te worden aan SURFnet, zodat zij deze in hun configuratie kunnen opnemen.

4.4.1.2 Importeren van de ontvangen trusted root van SURFnet

De trusted root is te downloaden via <http://federatie.surfnet.nl/sfs-signing-certificate.pem>

Om dit certificaat te importeren moeten de volgende stappen worden doorlopen.

Selecteer binnen iManager het onderdeel "Certificates" onder Novell Access Manager.

- Klik op de "Trusted Roots" tab

- Klik op "Import"

- Geef het certificaat een naam, bijvoorbeeld SurfSNS-CA.

- Browse naar het certificaat en selecteer dat

Klik op OK.

De Trusted Root wordt nu toegevoegd.

Vervolgens moeten we de Trusted Root nog aan de NIDP Trust Store toevoegen.

Plaats een vinkje voor het zojuist geïmporteerde certificaat

Klik op "Add Trusted Roots to Trust Stores"

Klik op het "Select Keystore" icoon rechts in het pop-up scherm

Plaats een vinkje voor de NIDP-truststore

Klik twee maal op OK.

Note: Binnen de test omgeving van SURFnet wordt gebruik gemaakt van zogenaamde self-signed certificaten. Hierdoor is het mogelijk om het certificaat rechtstreeks uit de metadata te importeren.

Ga hiervoor naar de metadata URL van SURFnet en kopieer alle gegevens tussen de <ds:X509Certificate> en </ds:X509Certificate> XML tags.

In plaats van de eerder beschreven stap "Browse naar het certificaat en selecteer dat" kun je nu deze data plakken in het scherm. Let er wel op dat je de data tussen de volgende tags toevoegt:

-----BEGIN CERTIFICATE-----

<hier het certificaat>

-----END CERTIFICATE-----

4.4.2 Stap 2: Het aanmaken van een Attribute Set

Indien u reeds een SURFnet koppeling gemaakt met Novell Access Manager als de IDP, dan kunt u kiezen of u deze wilt (her)gebruiken of dat u een nieuwe Attribute Set aanmaakt. Zorg er in ieder geval voor dat u weet welke attributen u nodig heeft om uw service te kunnen verlenen en om eventuele logging / facturatie of toegang tot achterliggende systemen mogelijk te maken.

U kunt bijvoorbeeld verlangen dat de volgende attributen worden meegezonden:

Naam van de onderwijsinstelling

Email adres van de gebruiker

Common name (cn) van de gebruiker

Voor- en achternaam van de gebruiker

De beschikbare attributen zijn terug te vinden op

<http://www.surfnet.nl/nl/Thema/SURFfederatie/over/Pages/Attributenschema.aspx>

Het is aan te raden om u te beperken tot de op deze web pagina genoemde lijst met attributen. Is dit niet mogelijk, dan zult u in contact moeten treden met SURFnet voor eventuele toevoegingen, bovendien zal ieder instelling vervolgens het extra attribuut moeten aanleveren, hetgeen een aanpassing in hun configuratie betekend.

Selecteer binnen iManager het onderdeel "Identity Server" onder Novell Access Manager.

Klik op de "Shared Settings" tab.

Klik op "New" onder de Attribute Sets.

Geef de Attribute Set een naam.

Klik vervolgens op "New" om attributen toe te voegen. Hierbij kunnen attributen uit de verschillende profielen worden gekozen.

Over het algemeen zullen we de attributen die we als SP gaan vragen / verlangen als LDAP attributen beschikbaar moeten komen, bijvoorbeeld:

LDAP attribute: cn

LDAP attribute: sn
LDAP attribute: givenName
LDAP attribute: email

Let ook op de mapping. SURFnet kan bijvoorbeeld het attribuut **urn:mace:dir:attribute-def:mail** zenden, terwijl uw LDAP server het attribuut mail kent. Selecteer hiervoor uw LDAP attribuut en vul bij de mapping de werkelijke SURFnet notatie in.

4.4.3 Stap 3: Het aanmaken van een SAML 2.0 Identity Provider

Omdat uw Novell Access Manager configuratie als Service Provider naar SURFnet toe gaat fungeren zal dus SURFnet als een Identity Provider gaat fungeren. U moet binnen Novell Access Manager hiervoor een Identity Provider configuratie aanmaken waarin u de gegevens van de SURFnet zijde configureert.

Note: Deze configuratie is complexer dan de SP configuratie die eerder is besproken. U zult keuzes moeten maken omtrent:

- Het aanmaken van identiteiten.
- Het matchen van bestaande gebruikers
- De gewenste authenticatie methode.
- etc.

Het is aan te bevelen om vooraf samen met Novell Consulting of een partner een gedegen ontwerp te maken.

Selecteer binnen iManager het onderdeel "Identity Server" onder Novell Access Manager.

Klik op de "Edit" link onder Configuration.

Klik op "New" onder de SAML 2.0 tab en selecteer Identity Provider.

Voer een naam in, bijvoorbeeld SURFnetIDP en voer de metadata URL (<http://federatie.SURFnet.nl/metadata-sfs-idp-saml20-signed.xml>) in, of plak de metadata in het tekst veld en klik op "Next."

Controleer of de juiste certificaat gegevens aanwezig zijn en klik op "Next."

De IDP is nu aangemaakt maar moet nog worden geconfigureerd.

4.4.4 Stap 4: Het configureren van de SAML 2.0 Identity Provider

De configuratie van een Identity Provider is redelijk complex.

Selecteer binnen iManager het onderdeel "Identity Server" onder Novell Access Manager.

Klik op de "Edit" link onder Configuration.

Klik op de zojuist aangemaakte Identity Provider onder de SAML 2.0 tab (SURFnetIDP.)

Klik op de Access tab. Het vinkje voor "Advertise on Login page" zorgt ervoor dat er op de login pagina van Novell Access Manager een SURFnet link wordt geplaatst, identiek aan de "Display Name." Hiermee kunnen gebruikers later aangeven dat zij via de SURFnet federatie willen aanmelden.

De security instellingen moeten hier standaard zijn, zoals weergegeven in onderstaande figuur.

Security

Encrypt name identifiers

SOAP Back Channel Security Method

Message Signing

Mutual SSL

Basic Authentication

Send:

Name:

Password:

Verify:

Name:

Password:

Klik op Attributes

Selecteer de eerder aangemaakte Attribute Set en voeg de attributen toe die je wilt of moet ontvangen.

Klik op Authentication. Dit gedeelte is het meest complexe deel van de configuratie. Er zijn vele keuze mogelijkheden en deze zullen hier voor het merendeel worden besproken. Voor een goed ontwerp blijft het aan te raden om een partner of Novell Consulting in te schakelen.

De optie "Allow users to federate" bepaalt of er gebruik gemaakt wordt van persistent of transient federation. Schakel deze optie uit voor Transient federation en schakel hem in voor Persistent Federation. Bij Persistent Federation worden fysieke accounts aan beide zijden aan elkaar gekoppeld. Bij Transient federation wordt authenticatie toegestaan, maar wordt er geen link gelegd naar een lokale gebruiker.

Transient federation kan een zeer valide (en eenvoudige) optie zijn. Het zal van uw situatie en de aan te bieden diensten afhangen of u dit kunt gebruiken. In het verdere voorbeeld gaan we uit van Persistent federation.

De optie "Allow after authentication" mag uitgeschakeld worden.

De optie "Allow before authentication" geeft aan dat er een federatieve koppeling tussen twee gebruikers mag worden opgezet gebaseerd op de authenticatie gegevens die van de IDP worden ontvangen. Deze optie moet bij Persistent Federation worden aangezet en verlangt de configuratie van de opties binnen het "User Identification Methods" kader.

De opties binnen het "User Identification Methods" kader moeten als volgt worden ingesteld:

Zowel de "User Matching Method" alsook de "User Provisioning Method" geconfigureerd.

4.4.4.1 User Matching Method

De User matching method moet dusdanig geconfigureerd worden dat een match te maken is op een attribuut. Het is aan te raden om bijvoorbeeld het email adres hiervoor te gebruiken.

Matching is alleen van belang als er gebruikers via de federatieve koppeling binnen kunnen komen die al een lokaal account hebben. Dit zal bijvoorbeeld kunnen gebeuren als er meerdere IDP koppelingen zijn gedefinieerd. Binnen de SURFnet configuratie lijkt dit echter niet logisch.

Het volgende voorbeeld beschrijft een matching rule die matcht op enkel het email adres, of op een combinatie van voornaam, achternaam en geboortedatum.

Klik op de knop naast "User Matching Method"

Selecteer bij “User Matching Expression” <New User Matching Expression>
 Geef de mathcing expression een naam. Bijvoorbeeld “Match op naam en datum of email”
 Klik op het Plus icoon binnen “Logical Group 1” en selecteer LDAP Attribute:mail
 Klik op “New Logical Group”
 Klik op het Plus icoon binnen “Logical Group 2” en selecteer LDAP Attribute:sn
 Klik op het Plus icoon binnen “Logical Group 2” en selecteer LDAP Attribute:givenName
 Klik op het Plus icoon binnen “Logical Group 2” en selecteer LDAP Attribute:dob
 Select Finish

Note: Hou er rekening mee dat niet alle attributen reeds beschikbaar zijn. Via Identity Server / Shared Settings / Custom Attributes / LDAP Attribute Names / New kunnen overige LDAP attributen worden toegevoegd. Bijvoorbeeld een geboortedatum zoals in bovenstaande voorbeeld gebruikt.

Selecteer bij “If match not found” de optie “Automatically provision user account.”
 Voeg de gewenste user stores toe waarbinnen naar een match moet worden gezocht.
 Klik op ok.

4.4.4.2 User Provisioning Method

Klik op de knop naast “User Provisioning Method”
 Selecteer alle Required Attributes. Bijvoorbeeld sn en givenName, of email

Note: Let op dat alle attributen die je hier kiest ook daadwerkelijk door de IDP worden meegezonden en ook daadwerkelijk in stap 2 en stap 4 / Attributes worden meegenomen. Indien een van de attributen **niet** wordt ontvangen zal er **nooit** provisioning plaats vinden.

Selecteer alle Optional Attributes. Deze attributen zullen bij de aan te maken gebruiker worden opgeslagen. Het is niet erg als een of meerdere attributen ontbreken.

Bij “Define user name creation” wordt bepaald hoe de User ID wordt opgebouwd. Enkel de Required Attributes zijn hier beschikbaar.

Zet de maximum length op 10

Selecteer Automatically create user name

Selecteer bij Segment1 het gewenste attribuut (bijvoorbeeld givenName) en ene lengte van 4

Selecteer eventueel een Junction

Selecteer bij Segment2 het gewenste attribuut (bijvoorbeeld sn) en ene lengte van 4

Enable de optie “Ensure name is unique.”

Bij deze configuratie wordt dus voor de gebruiker Piet Paulusma een User ID van PietPau opgebouwd, eventueel gevolgd door een volgnummer van 2 posities om hem uniek te maken binnen het systeem.

In het volgende scherm kunnen de standaard waardes gehanteerd worden. In dit geval “Automatically create password.”

Als laatste moet ene User Store en context gedefinieerd worden waarbinnen de accounts worden opgeslagen. Eventueel kan de optie “Delete user provisioning accounts if federation is terminated” worden aangevinkt.

Terug op de Authentication pagina moeten de volgende instellingen nog worden gezet:

Binnen het “User Identification Methods” kader moet “Automatically provision unknown user” enabled worden. Dit zorgt ervoor dat alle gebruikers die via de

SURFnet federatieve koppeling worden aangemeld automatisch een UserID krijgen binnen de LDAP directory

Bij "Authentication Context" kunnen we de optie "Do not specify" hanteren. Hierbij wordt de IDP (SURFnet en daarmee de overige aangesloten instellingen) expliciet vertrouwd.

Note: Het is ook mogelijk om een specifiek contract of type te selecteren. Deze configuratie valt echter buiten de scope van dit document.

Binnen het "Options" kader worden de volgende instellingen gemaakt:

"Response protocol binding" op "POST."

"Allowable IDP proxy indirections" op "Let IDP Decide."

"Force authentication at Identity Provider" en "Use automatic introduction" beiden disabled.

Sla alle instellingen op en klik op "Update All" in de Identity Server iManager task.

4.4.5 Stap 5: Signing

Stap 5 is gelijk aan stap 5 voor de IDP configuratie. Heeft u reeds een SURFnet koppeling gemaakt met Novell Access Manager als de IDP, dan kunt u deze stap overslaan en doorgaan bij Stap 6.

Als extra beveiliging (naast communicatie over een SSL verbinding) moet signing worden aangezet.

Selecteer binnen iManager het onderdeel "Identity Server" onder Novell Access Manager.

Klik op de "Edit" link onder Configuration.

Under "Identity Provider" enable "Require Signed Authentication Requests"

Under "Identity Consumer" enable both "Require Signed Assertions" and "Sign Authentication Requests"

Note: Indien er na het zetten van de "Require Signed Authentication Requests" optie een 300101008 foutmelding wordt afgegeven op de communicatie tussen de Identity Server en de Access Gateway, dan moeten de volgende acties worden uitgevoerd die er voor zorgen dat tussen de Identity Server en de Access Gateway de metadata opnieuw wordt uitgewisseld.

Ga naar Access Gateways

Klik op Edit

Klik op Reverse Proxy / Authentication

Zet de optie voor "identity Server Cluster" op [none]

Ok / Apply Changes / Update All.

Volg de prompt op en doe ook een Update All op de Identity Server.

Ga terug naar Access Gateways

Klik op Edit

Klik op Reverse Proxy / Authentication

Voeg de Identity Server weer toe.

Ok / Apply Changes / Update All.

Volg de prompt op en doe ook een Update All op de Identity Server.

4.4.6 Stap 6: Test de configuratie

Open een verse browser en ga naar de login pagina van de service die u gaat aanbieden via de SURFnet federatie.

Op de login pagina van Novell Access Manager zal een link staan met de naam die u in stap 3 aan de IDP configuratie heeft gegeven.

Klik op deze link en u zult worden doorverwezen naar een SURFnet pagina. Hier kunt u selecteren via welke IDP u zich wilt aanmelden.

Authenticatie zou vervolgens succesvol moeten zijn.

Note: Er zijn vele mogelijkheden om de aan te bieden dienst binnen Novell Access Manager te configureren. Afhankelijk van de dienst zelf (moet er een identity injection worden uitgevoerd, of een form fill,) het gewenste beveiligingsnivo (moet men beschikken over een token, of is naam en wachtwoord voldoende) en diverse andere variabelen kunnen er variaties op bovenstaande configuratie nodig zijn.

Wederom luidt hier het advies dat het verstandig is om de hulp van een partner of Novell Consulting in te roepen.

<End of Document>

