FAQ IdP

Op deze pagina vind je alle veelgestelde vragen (FAQ) over Identity Providers of IdP's. Staat jouw vraag er niet tussen en kun je het antwoord ook niet vinden in de rest van de wiki? Stel je vraag dan aan het het SURFconext-team door een mail te sturen naar support@surfconext.nl.

Kunnen uitsluitend bepaalde gebruikersgroepen binnen mijn instelling toegang krijgen tot een dienst?

Dat kan. Bijvoorbeeld met de functionaliteit Autorisatieregels in het SURFconext dashboard kan de SURFconextverantwoordelijke regels aanmaken die specifiek toegang geeft voor bepaalde gebruikers binnen de instelling. In deze wiki lees je over alle mogelijkheden om toegang te beperken tot een bepaalde groep mensen.

Testaccounts binnen SURFconext

Testaccounts zijn toegestaan binnen SURFconext enkel wanneer ze voldoen aan bepaalde eisen. Lees waar testaccounts aan moeten voldoen.

Nieuwsbrieven en alerts

Om de aangesloten instellingen zo goed mogelijk te informeren over SURFconext, verstuurt het SURFconext team verschillende mailings. Dit kan de nieuwsbrief zijn, een aankondiging voor een nieuwe release maar ook nieuws rondom een storing. Op deze pagina staat wat er wordt verstuurd en naar wie: SURFconext mailings.

Kan ik een eigen dienst aanbieden op SURFconext?

Ja, als jouw instelling een SURFnet-contract heeft getekend met bijlage IX is het mogelijk om eigen diensten aan te sluiten op SURFconext zonder nadere contractuele afspraken. Dit kan voor alleen eigen gebruik zijn, of om andere instellingen toegang te geven. In het SURFconext Dashboard vind je onder "Mijn instelling" de gegevens van de SP's die jouw instelling aanbiedt.

Ga voor de technische aansluitinformatie naar Documentation for Service Providers.

SURFconext nieuwsbrief: ontvangstadres wijzigen

Sinds 1 januari 2015 verschijnt de maandelijkse nieuwsbrief van SURFconext. Via deze nieuwsbrief houdt SURFnet alle aangesloten instellingen op de hoogte van de laatste ontwikkelingen rondom SURFconext. Denk hierbij aan nieuwe releases en functionaliteiten, recent aangesloten diensten en interessante bijeenkomsten.
Wij vinden het belangrijk dat de SURFconext contactpersonen van de instelling deze informatie lezen, vandaar dat zij standaard zijn toegevoegd aan de mailinglijst. Mocht je hieraan iets willen wijzigen, neem dan contact op met support@surfconext.nl

Als je geen SURFconext contactpersoon bent en toch graag de nieuwsbrief ontvangt, kun je je aanmelden voor de SURFconext-alert lijst. Via deze mailinglijst wordt naast informatie over storingen ook aankondigingen van nieuwe releases en de nieuwsbrief verspreid. Aanmelden kan via: https://list.surfnet.nl/mailman/listinfo/surfconext-alert .

Welke gebruikers van een organisatie mogen gebruikmaken van SURFconext?

Zie Eisen identiteiten voor meer informatie.

Wat betekent de melding "Invalid signature on idp response"?

Als SURFconext deze melding geeft, ondertekent de IdP zijn SAML-berichten met een certificaat dat bij SURFconext niet bekend is. Dit kan voorkomen als de IdP zijn SAML signing certificaat wijzigt. ADFS kan dit ook automatisch doen.

De IdP-beheerder kan het SURFconext-supportteam vragen om de metadata van de IdP opnieuw in te lezen om het probleem te verhelpen. Beter is het natuurlijk om de situatie te voorkomen. Zie daartoe de volgende vraag.

Kan SURFconext aan mijn IdP doorgeven op welke dienst de gebruiker probeert in te loggen?

SURFconext biedt de mogelijkheid om op basis van een scoping element de zogeheten Issuer in het AuthNRequest (het authenticatie verzoek) mee te geven aan een IdP. Op basis hiervan is het mogelijk toegang tot een bepaalde dienst (of diensten) te autoriseren op de IdP als de IdP dit ondersteunt. Dit mechanisme werkt niet met Microsoft ADFS. Wij stellen dat het op dit moment met de out-of-the-box functionaliteit en door Microsoft ondersteunde en gedocumenteerde functionaliteiten niet mogelijk is gebruik te maken van scoping elementen binnen Microsoft ADFS in combinatie met SURFconext. Met andere producten dan Microsoft is dit wel mogelijk, zoals bijvoorbeeld een IdP op basis van SimpleSAMLphp. Onze partner 2AT heeft een rapport geschreven over het gebruik van scoping met ADFS 4.0.

Hoe verleng ik het token signingcertificaat van mijn Identity Provider-systeem?

Om de authenticiteit van SAML assertions en authentication responses te verifiëren, gebruik je digitale handtekeningen. Dat betekent dat je ‘signing keys’ moet aanmaken en configureren in je Identity Provider-systeem. Je moet de public signing key publiceren in de vorm van een self-signed certificate in de metadata. De gateway van SURFconext leest deze metadata in, samen met de public key, zodat berichten die van jouw organisatie komen, gevalideerd kunnen worden.

Hoewel SURFconext alleen de public key uit het certificaat gebruikt, vertoont sommige software problemen als er iets mis is met het certificaat, bijvoorbeeld als de geldigheidsduur van het certificaat verloopt. Hieronder lees je aandachtspunten bij het verlopen van token signingcertificaten.

Certificaat verlengen in ADFS 2.0

Bij de installatie van de ADFS server is een self-signed tokencertificaat geïnstalleerd met een standaard geldigheidsduur van 1 jaar. Dit certificaat wordt automatisch vernieuwd voordat de geldigheidsduur is verstreken. Volgens de standaardinstellingen wordt 20 dagen voor het verstrijken van het oude certificaat een nieuw certificaat aangemaakt.

Wij raden je aan om de geldigheidsduur van dit certificaat te verlengen tot bijvoorbeeld 5 jaar, omdat Service Providers elke keer dat een cerificate rollover plaatsvindt het nieuwe certificaat moeten importeren. En tot die tijd zal de dienst onbereikbaar zijn voor jouw gebruikers.

Als je het automatisch gegenereerde token signingcertificaat wilt verlengen en vervangen, moet je de volgende stappen doorlopen:

> Deze stappen zijn bedoeld voor een nieuwe installatie. Voor een bestaande productie-installatie voer je alleen de stappen 1 t/m 3 uit. De langere geldigheidsduur wordt dan pas van kracht na de eerstvolgende (automatische) rollover.

1. Start Windows PowerShell.
2. Laad de ADFS plugin met het commando
   `Add-PSSnapin Microsoft.Adfs.PowerShell`

3. Zet de geldigheidsduur van certificaten op 5 jaar (1825 dagen) met:
   `Set-ADFSProperties -CertificateDuration 1825`
4. Activeer het nieuwe certificaat met:
   `Update-ADFSCertificate -CertificateType Token-Signing -Urgent`
   Voer deze stap alleen uit als de server nog niet in productie is genomen. Voor productieservers wacht je tot het eerstvolgende moment waarop een certificate rollover plaatsvindt.
5. Controleer of het certificaat is verlengd met:
   `Get-ADFSCertificate -CertificateType Token-Signing`
6. De verloopdatum van het certificaat staat vermeld onder 'Not After'.

Certificaat verlengen voor andere Identity Provider-systemen

Voor sommige Identity Provider-systemen (bij voorbeeld SimpleSAMLphp) levert het verlopen van het token signingcertificaat geen problemen op. Bij andere software kan dit wel een probleem geven. Ook als die software de geldigheidsduur van certificaten zelf niet kan aanpassen, kun je waarschijnlijk wel een bestaand certificaat importeren. Het certificaat dat je wilt importeren, maak je dan met een andere tool, zoals OpenSSL.

Met OpenSSL kun je een self-signed tokencertificaat aanmaken. Je doet dat met de volgende commando's:

```
openssl genrsa -out key.pem 2048
openssl req -new -key key.pem -out req.csr -subj '/CN=idp.example.org Signing Certificate'
openssl x509 -req -in req.csr -signkey key.pem -days 1825 -out cert.pem
```

Als een bestaand certificaat moet worden verlengd (in plaats van een nieuw gegenereerd certificaat), gebruik je het commando:

```
openssl x509 -in oldcert.pem -signkey key.pem -days 3650 -out newcert.pem
```

Hoe werkt log out?

Single Log Out (SLO) betekent dat je in één keer uitlogt bij alle Service Providers tegelijk, nadat je bij 1 Service Provider bent uitgelogd. Het is dus precies het tegenovergestelde van Single Sign On.

SURFconext ondersteunt in de praktijk geen Single Log Out. Hiervoor zouden namelijk alle Service Providers bepaalde technische aanpassingen moeten doen op hun systemen. In de praktijk is het onmogelijk om dit af te dwingen en er zeker van te zijn dat een gebruiker ook daadwerkelijk is uitgelogd wanneer deze op uitloggen heeft geklikt bij een willekeurige andere Service Provider. Vanwege de mogelijke veiligheidsissues die dit met zich meebrengt, ondersteunt SURFconext geen SLO.

De enige echt veilige vorm van SLO is (en blijft) het volledig afsluiten van je browser. Met volledig bedoelen we dat de gebruiker alle vensters en tabbladen moet sluiten en dat de browserapplicatie dus helemaal is afgesloten. Alleen het sluiten van de tabbladen van diensten waar je bent ingelogd via SURFconext is niet voldoende om overal uit te loggen.

Het is essentieel om de gebruikers van jouw organisatie goed te informeren over hoe zij veilig moeten uitloggen, zeker tijdens het gebruik op een publieke of terminalpc of de computer van een ander.

Advies

We adviseren je daarom om al bij het inloggen op de webpagina's te vermelden dat de enige veilige vorm van uitloggen het volledig afsluiten van je browser is.

Op deze pagina staan richtlijnen beschreven voor hoe je de login pagina het beste kan vormgeven.

Meer informatie

Zie ook: https://wiki.shibboleth.net/confluence/display/CONCEPT/SLOIssues. Of lees het blog 'Damn you Single Sign On' van SURFnet.

Wat gebeurt er met de gegevens van gebruikers van SURFconext?

De gegevens van de gebruikers blijven in beheer van de organisatie waar ze studeren of werken. Door SURFconext te gebruiken, hoeven inlognamen en wachtwoorden niet worden doorgegeven aan Service Providers. Soms worden er wel attributen (gebruikerskenmerken), zoals naam, doelgroep en opleiding van gebruikers uitgewisseld. Service Providers kunnen hun aanbod daarmee afstemmen op de behoeften van de gebruikers.

SURFconext zorgt ervoor dat alleen de informatie die nodig is, wordt doorgestuurd naar Service Providers. Bij het inloggen ontvangt SURFconext persoonsgegevens van de instelling. SURFconext stuurt deze door naar de Service Provider. Hierbij is SURFconext dus het doorgeefluik.

Organisaties, Service Providers en SURFconext slaan de gegevens op in logfiles. Het doel van deze logfiles is beperkt tot het beheer van de dienst, interne controle van de processen en beveiliging. Dit betekent dat de gegevens in de logfiles alleen voor een bepaalde termijn worden bewaard. Meer informatie over privacy lees je op Privacy en Privacy en persoonsgegevens.

Hoelang worden de gegevens bewaard die ik via SURFconext doorstuur?

Persoonsgegevens mogen niet langer bewaard worden dan nodig is voor het doel waarvoor ze zijn verzameld. Instellingen maken hier zelf afspraken over met dienstaanbieders.

SURFconext
De bewaartermijnen van gegevens die door de dienst SURFconext worden opgeslagen, kan je terugvinden op: https://profile.surfconext.nl/my-surfconext De bewaartermijnen staan ook genoemd in Bijlage A8 in de Verwerkersovereenkomst die SURFnet met instellingen heeft afgesloten.

Hoe waarborgt SURFconext mijn privacy?

Op technisch vlak waarborgen wij de privacy door de gegevens te versleutelen voordat ze worden verzonden.

Maar om de privacy daadwerkelijk te waarborgen, maken wij met alle deelnemers aan SURFconext duidelijke afspraken, zodat de gegevens alleen gebruikt worden voor het doel dat we hebben afgesproken.

De afspraken op het gebied van privacy staan in de ‘Privacy Best Practice’. Dit document is gebaseerd op de Algemene Verordening Gegevensbescherming (AVG). In de Privacy Best Practice staat het doel waarvoor persoonsgegevens worden verzameld. Het gebruiken van persoonsgegevens is alleen toegestaan als het noodzakelijk is om dat specifieke doel te bereiken, bijvoorbeeld autorisatie of personalisatie. Daarbij krijgen alleen personen die het echt nodig hebben, toegang tot de persoonsgegevens.

De transparantie voor de gebruiker over het gebruik van zijn persoonsgegevens, wordt gewaarborgd door hem hierover te informeren zodra hij een dienst benadert via SURFconext. Ook zijn er maximale bewaartermijnen voor persoonsgegevens vastgesteld en worden SURFconext-deelnemers verplicht om beveiligingsmaatregelen te nemen om misbruik van de gegevens te voorkomen. Meer informatieMeer informatie over privacy lees je op Privacy en Privacy en persoonsgegevens.

Wat is de procedure voor het wijzigen of vervangen (migreren) van een Identity Provider-systeem?

Wij raden je aan om wijzigingen in het Identity Provider-systeem zoveel mogelijk te vermijden. Dit omdat er vrijwel altijd sprake is van een verstoring van de diensten. Die verstoring varieert van 1 werkdag tot 2 weken.

Helaas is het soms onvermijdelijk om iets te veranderen aan je Identity Provider-systeem of aan de configuratie daarvan. Bijvoorbeeld als je overstapt naar een ander softwarepakket, of verhuist naar een andere server.

Maar ook het wijzigen van de inhoud van een attribuut, het vervangen van het certificaat of het aanpassen van de URL van de metadata valt onder een wijziging van je Identity Provider-systeem. Al deze veranderingen hebben impact op de diensten die de gebruikers van je organisatie gebruiken via SURFconext. Vaak zijn 1, meerdere, of alle diensten tijdelijk niet te gebruiken, bijvoorbeeld omdat de gebruikers van je organisatie niet kunnen inloggen. De duur van deze onderbrekingen varieert sterk.

Neem daarom altijd eerst contact op met het SURFconext-team (support@surfconext.nl) om de wijziging(en) met ons te spreken, en om samen de impact te bepalen.

Meer informatie over de procedure voor het vervangen (migreren) van een Identity Provider-systeem lees je bij Veranderingen aanbrengen bestaande Identity Provider.

Waarom moet de tijd op mijn IdP zo precies kloppen?

Om allerhande replay-aanvallen te voorkomen, hanteren SURFconext en de meeste SP-software stricte tijdslimieten voor de geldigheid van SAML-assertions. Als de tijd van een IdP niet correct is, kan het gebeuren dat de assertion die SURFconext van de IdP ontvangt buiten het geldigheidsinterval valt dat in die assertion is gedefinieerd. SURFconext zal de assertion dan niet accepteren, en de gebruiker een foutmelding tonen.

De tijd op de server kan up-to-date worden gehouden door via het ntp-protocol te synchroniseren met een aantal internetservers. Op de meeste Linux-systemen kan de tijd gesynchroniseerd worden door het package `ntp` (of `ntp-server`) te installeren. Op Windows-systemen is de gebruikelijk procedure dat de PDC emulator als autoritieve tijdbron voor de domein fungeert. De PDC emulator synchroniseert dan met servers op het internet of met een hardware-device (typisch GPS), en de overige hosts halen hun tijd op bij de PDC emulator. Zie de Microsoft Knowledge Base voor meer informatie.

Wat is het attribuut eduPersonTargetedID?

Het attribuut eduPersonTargetedID is een kopie van de Subject -> NameID welke door SURFconext zelf wordt gezet. Als een Identity Provider de eduPersonTargetedID zelf zet, wordt deze altijd overschreven door SURFconext.

Dit attribuut is in het leven geroepen omdat de Subject -> NameID zelf geen onderdeel is van de SAML v2.0-respons en dus niet gebruikt kan worden. Als SURFconext het attribuut eduPersonTargetedID plaatst, kan de Subject -> NameID wel worden gebruikt.

Je hoeft dit attribuut niet zelf toe te voegen aan je Identity Provider-systeem, omdat SURFconext dit attribuut automatisch vult.

Wat doet SURFconext?

SURFconext bouwt een nieuw NameID op uit schacHomeOrganization + UID. Je ziet deze terug als 'subject' in de debug-pagina van het Engineblok op https://engine.surfconext.nl/authentication/sp/debug. Voorts bepaalt ook het NameIDformat hoe de NameID naar de Service Provider wordt gestuurd. Deze kan zijn:

```
urn:oasis:names:tc:SAML:2.0:nameid-format:transient
urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified
```

Het transient format is het meest veilig (eenmalige unieke code die per sessie en per Service Provider anders is), daarna het persistent format (unieke code die over meerdere sessies, over meerdere Service Providers en voor langere tijd geldig is) en de unspecified variant is het minst veilig (waarin de UID en de schacHomeOrganization zichtbaar zijn). Deze laatste wordt in verband met inbreuk op de privacy niet meer toegestaan.

Per Service Provider kan worden bepaald wat het NameIDformat is. Je kunt dit onder andere bekijken met de SAML tracer, een plugin voor FireFox. Op deze pagina staat beschreven hoe je SAML tracer kunt gebruiken.

Op de debug-pagina van SURFconext (https://engine.surfconext.nl/authentication/sp/debug) zal je na het inloggen geen eduPersonTargetedID attribuut zien. Dit komt doordat deze pagina alleen informatie laat zien voordat deze gemanipuleerd is (dus voordat SURFconext het eduPersonTargetedID-attribuut heeft gezet).

Aan welke eisen moeten de entitlement-attributen voldoen voor de TERENA Personal Certificate Service?

Om een persoonscertificaat te kunnen aanvragen via de TERENA Personal Certificate Services (https://www.digicert.com/sso) moeten de vrijgegeven attributen aan extra eisen voldoen.

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

Dit attribuut moet gevuld zijn met een waarde die per persoon uniek is en eindigt met de domeinnaam van de betreffende instelling.

Voor een medewerker van de Universiteit van Tilburg is dat bijvoorbeeld @uvt.nl.

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

De waarde van het commonName (cn) attribuut moet de achternaam in het identiteitsbewijs bevatten en mag daarnaast voornaam of initialen bevatten.

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

De eduPersonEntitlement is een multivalued attribuut. Dat wil zeggen dat dit attribuut meerdere waarden mag hebben. Gebruikers die een certificaat mogen aanvragen hebben de waarde '`urn:mace:terena.org:tcs:personal-user`' in dit attribuut staan. Alleen accounts van echte personen mogen deze attribuutwaarde krijgen. Het mogen dus geen testaccounts of functionele accounts zijn. Bovendien moeten deze personen een geldig identiteitsbewijs hebben laten zien (face-to-face). Voor personeel in loondienst is dat automatisch al het geval.

Log in op de debug-pagina van SURFconext om te controleren of jouw account de juiste attributen levert. Meer informatie over het toevoegen van dit attribuut lees je bij Hoe geef ik het eduPersonEntitlement attribuut mee?

Voorbeeld

Name	Value
`urn:mace:dir:attribute-def:eduPersonPrincipalName`	john@university.nl
`urn:mace:dir:attribute-def:mail`	John.Doe@university.nl
`urn:mace:dir:attribute-def:cn`	John Doe
`urn:mace:dir:attribute-def:eduPersonEntitlement`	`urn:mace:terena.org:tcs:personal-user`
`urn:mace:terena.org:attribute-def:schacHomeOrganization`	university.nl

Voor administrators werd in het verleden nog een tweede waarde gebruikt: '`urn:mace:terena.org:tcs:personal-admin`'. Deze is tegenwoordig niet meer nodig en kan veilig verwijderd worden waar nog aanwezig.

Hoe wordt het UID-attribuut door SURFconext en aangesloten diensten gebruikt?

Een van de attributen in het schema van SURFconext is het UID attribuut (`urn:mace:dir:attribute-def:uid`) Op welke wijze wordt dat gebruikt binnen SURFconext door de aangesloten diensten?

- SURFconext gebruikt de waarde van het UID-attribuut als onderdeel van de primaire identifier voor gebruikers in SURFconext. Om precies te zijn in een combinatie met de waarde van het schacHomeOrganization-attribuut (`urn:mace:terena.org:attribute-def:schacHomeOrganization`).
  De reden dat wij UID gebruiken is omdat UID per definitie uniek is binnen een organisatie. UID is een van de twee vereiste attributen die een identity provider moet leveren om aan te kunnen sluiten op SURFconext (zie ook: Vereiste attributen).
- Als een Service Provider er om vraagt (en de Identity Provider toestemming geeft) kan deze ook het UID-attribuut krijgen. SURFconext geeft op dat moment de waarde door die door de Identity Provider is aangeleverd. Sommige Service Providers zullen dit atribuut gebruiken als (basis voor) een identifier. Het komt zelden voor dat dit attribuut aan een gebruiker getoond word.
- Naast bovenstaand 'interne' gebruik binnen SURFconext, geven wij standaard ook een identifier (de zogenaamde SAML name-ID) aan Service Providers. Deze Identifier is persistent, en niet rechtstreeks tot de gebruiker te herleiden voor de dienst. De identifier is gebaseerd op de door door de instellingen geleverde UID. Diverse diensten gebruiken deze name-ID (of het afgeleide attribuut 'eduPersonTargetedID') als identifier, en wij moedigen Service Providers aan specifiek dat te gebruiken, in plaats van het UID-attribuut.

Kijk voor meer informatie over attributen op de pagina Attributen in SURFconext (NL).

Hoe voeg ik het eduPersonAffiliation-attribuut toe?

Het '`urn:mace:dir:attribute-def:eduPersonAffiliation`'-attribuut geeft aan welke relatie je als gebruiker hebt met jouw organisatie. SURFspot gebruikt dit attribuut bijvoorbeeld om je naar de juiste 'winkel' te sturen.

Voor studenten heeft dit attribuut de waarde 'student'. Voor medewerkers heeft dit attribuut de waarde 'employee'. De naam en de waarde van dit attribuut zijn hoofdlettergevoelig.

Wil je controleren of dit attribuut voor jou als gebruiker goed wordt doorgegeven? Log dan in op de debug-pagina van SURFconext: https://engine.surfconext.nl/authentication/sp/debug.

Attribuut vrijgeven in ADFS 2.0

Identity Providers die ADFS 2.0 gebruiken, kunnen het vrijgeven van attributen regelen via de GUI. Zorg er eerst voor dat alle studenten in een Windows Security Group zitten, en alle medewerkers in een andere Windows Security Group. Op basis van de Windows Security-groepen voeg je conditioneel een attribuut met een bepaalde waarde toe. Dat gebeurt met een 'Send Group Membership as a Claim'-rule.

Om dit attribuut vrij te geven, moet de volgende stappen doorlopen:

1. Open de ADFS 2.0 Management utility.
2. Selecteer 'ADFS 2.0 -> Service -> Claim Descriptions'.
3. Kies 'Add Claim Description...'.
4. Vul de Display name met 'eduPersonAffiliation' en de 'Claim identifier' met '`urn:mace:dir:attribute-def:eduPersonAffiliation`'.
5. Kies 'OK'.
6. Selecteer 'ADFS 2.0 -> Trust Relationships -> Relying Party Trusts'.
7. Selecteer 'SURFconext' en kies voor 'Edit Claim Rules...'.
8. Kies 'Add Rule...'.
9. Kies 'Send Group Membership as a Claim' en kies 'Next'.
10. Vul de 'Claim rule name' met 'eduPersonAffiliation student', de 'User's group' met de Security Group waarin de studenten zitten en de 'Outgoing claim value' met 'student' en kies 'OK'.
11. Kies nogmaals 'Add Rule...'.
12. Kies 'Send Group Membership as a Claim' en kies 'Next'.
13. Vul de 'Claim rule name' met 'eduPersonAffiliation employee', de 'User's group' met de Security Group waarin de medewerkers zitten en de 'Outgoing claim value' met 'employee' en kies 'OK'.

Hoe geef ik het eduPersonEntitlement-attribuut mee?

Diensten die het '`urn:mace:dir:attribute-def:eduPersonEntitlement`'-attribuut gebruiken, kunnen hiermee zien wat de toegangsrechten van een bepaalde gebruiker zijn. Het wordt bijvoorbeeld gebruikt door de TERENA Certificate Services:

- https://mijncertificaat.surfnet.nl/
- https://tcs-escience-portal.terena.org/

Zie ook het antwoord op de vraag Aan welke eisen moeten de entitlement-attributen voldoen voor de TERENA Personal Certificate Service?.

Attribuut vrijgeven in ADFS 2.0

Het eduPersonEntitlement-attribuut is een een multi-value string. Het kan dus meer dan 1 waarde doorgeven. In het geval van 'AD' als 'attribute store' moet je dus een AD-veld gebruiken dat multi-value strings ondersteunt. Daar zijn er niet zo veel van. Een goede keuze is bijvoorbeeld altSecurityIdentities.

Om het eduPersonEntitlement/attribuut vrij te geven, moet je de volgende stappen doorlopen:

Op de federatie (ADFS)-server:

1. Open 'ADFS 2.0 management console'.
2. Ga naar 'AD FS 2.0 -> Service -> Claim Descriptions'.
3. Kies 'Add Claim Description ...'
    a. Display name: `urn:mace:dir:attribute-def:eduPersonEntitlement`
    b. Claim type: `urn:mace:dir:attribute-def:eduPersonEntitlement`
    c. Belangrijk! Selecteer beide checkmarks bij 'Publish this claim description ...' Doe dit bij alle 'Claim Descriptions' die je zelf hebt toegevoegd.
4. Kies 'Finish'.
5. Ga naar AD FS 2.0: 'Trust Relationships -> Relying Party Trusts'. Klik de productiesettings aan (die met 'Display Name SURFconext').
6. Kies 'Edit Claim Rules ...'
7. Kies 'Add Rule : Next'
    a. Voer de naam in voor de rule, bijvoorbeeld 'Persoon eduPersonEntitlement'
    b. Attribute store: Active Directory
    c. LDAP Attribute: altSecurityIdentities
    d. Outgoing Claim Type: `urn:mace:dir:attribute-def:eduPersonEntitlement`
8. Kies 'Finish'.

Op de domein controller:

1. Vul in AD meerdere waardes in voor de gebruiker in het veld 'altSecurityIdentities'. Bijvoorbeeld:
    a. `urn:mace:terena.org:tcs:personal-admin`
    b. `urn:mace:terena.org:tcs:escience-user`
    c. `urn:mace:terena.org:tcs:escience-admin`
    d. `urn:mace:terena.org:tcs:personal-user`
2. Controleer de werking via https://engine.surfconext.nl/authentication/sp/debug. De waardes moeten als volgt op aparte regels staan:
    a. `urn:mace:dir:attribute-def:eduPersonEntitlement urn:mace:terena.org:tcs:personal-admin`
    b. `urn:mace:dir:attribute-def:eduPersonEntitlement urn:mace:terena.org:tcs:escience-user`
    c. `urn:mace:dir:attribute-def:eduPersonEntitlement urn:mace:terena.org:tcs:escience-admin`
    d. `urn:mace:dir:attribute-def:eduPersonEntitlement urn:mace:terena.org:tcs:personal-user`

Hoe geef ik het schacHomeOrganization-attribuut mee?

Het 'urn:mace:terena.org:attribute-def:schacHomeOrganization'-attribuut identificeert de organisatie van een gebruiker. De waarde van dit attribuut is een RFC1035-domeinaam, bijvoorbeeld 'surfnet.nl'. Voor alle gebruikers van een Identity Provider heeft dit attribuut dezelfde waarde. De waarde die je toekent, is het hoofddomein van de organisatie.

Attribuut vrijgeven in ADFS 2.0

Voor Identity Providers die ADFS 2.0 gebruiken, kunnen het vrijgeven van attributen regelen via de GUI. De truc is om een 'Send Group Membership as a Claim' te gebruiken met als groep 'Domain Users'. Het attribuut wordt dan aan alle gebruikers toegevoegd.

Om dit attribuut vrij te geven moet je de volgende stappen doorlopen:

1. Open de ADFS 2.0 Management utility.
2. Selecteer 'ADFS 2.0' -> 'Service' -> 'Claim Descriptions'.
3. Kies 'Add Claim Description...'.
4. Vul de 'Display name' met 'schacHomeOrganization' en de 'Claim identifier' met '`urn:mace:terena.org:attribute-def:schacHomeOrganization`'.
5. Kies 'OK'.
6. Selecteer 'ADFS 2.0' -> 'Trust Relationships' -> 'Relying Party Trusts'.
7. Selecteer 'SURFconext' en kies voor 'Edit Claim Rules...'.
8. Kies 'Add Rule...'.
9. Kies 'Send Group Membership as a Claim' en kies 'Next'.
10. Vul de 'Claim rule name' met 'schacHomeOrganization', de 'User's group' met 'Domain Users' en de 'Outgoing claim value' met de gewenste waarde en kies 'OK'.

Attribuut vrijgeven in SimpleSAMLphp

Je voegt een attribuut met een constante waarde toe door het bestand 'config/config.php' te wijzigen. Voeg in deze file het volgende toe, onder de entry voor 'authproc.idp':

```
10=> array(
    'class'=> 'core:AttributeAdd',
    'urn:mace:terena.org:attribute-def:schacHomeOrganization'=> array('example.org')
),
```

Vul voor 'example.org' de gewenste waarde van het schacHomeOrganization attribuut in.

De index in de 'authproc.idp' moet uniek zijn. In het voorbeeld is deze 10. Is die waarde al in gebruik? Kies dan een andere.

Zie de simpleSAMLphp-documentatie voor meer informatie: http://simplesamlphp.org/docs/stable/core:authproc_attributeadd.

Hoe geef ik student- of personeelsnummers door via SURFconext?

Sinds februari 2014 ondersteunt SURFconext het `schacPersonalUniqueCode` attribuut om instellingsspecifieke student- en personeelsnummers door te geven aan SPs. Om dit attribuut te leveren, moet er per instelling een deel van de betreffende namespace worden gereserveerd. Neem daarom contact op met support@surfconext.nl als u dit attribuut wilt gaan gebruiken.

Kan ik TMG gebruiken als proxy voor ADFS 2.0?

Je kunt TMG gebruiken als proxy voor ADFS 2.0. In de installatiehandleiding voor het aansluiten van een Active Directory Federation Services (ADFS) 2.0 Identity Provider op SURFconext staat hoe je een proxyserver inricht op basis van ADFS. Er zijn diverse instellingen die al een MS Thread Management Gateway (TMG) hebben, en deze als proxy gebruiken in plaats van de ADFS-proxy.

Er is (nog) geen handleiding die speciaal voor SURFconext beschrijft hoe je TMG configureert. Op Microsoft Technet staat wel een artikel dat de installatie beschrijft: http://social.technet.microsoft.com/wiki/contents/articles/7877.configuring-tmg-as-an-ad-fs-2-0-proxy.aspx

⚠ Let er bij het configureren van de proxy op dat je de SAML 2.0-metadata zonder authenticatie beschikbaar maakt. Het gaat hier om de url: https://<yourdomein>/FederationMetadata/2007-06/FederationMetadata.xml.

Waar is de SURFguest IdP gebleven?

In het verleden faciliteerde SURFnet de toegang van externen tot online diensten via een eigen gast-IdP: SURFguest

Sinds september 2013 maakt SURFnet voor het faciliteren van gasttoegang tot op SURFconext aangesloten diensten gebruik van: Onegini. Onegini is een nieuwe manier van inloggen waarbij een gebruiker zijn social account (Facebook, Twitter, LinkedIn, Google) gebruikt. Gebruikers hoeven zo geen aparte gebruikersnaam en wachtwoord meer te onthouden.

Wat is de rol van gast-IdP Onegini?

Wat is Onegini?

Onegini is een nieuwe manier van inloggen waarbij een gebruiker zijn social account (Facebook, Twitter, LinkedIn, Google) gebruikt. De gebruiker hoeft dan geen aparte gebruikersnaam en wachtwoord meer te onthouden.

Wat is het verschil tussen een gast-account en een instellingsaccount?

Onegini accounts zijn gebaseerd op social accounts (Facebook/LinkedIn/Google/Twitter). Dat noemen we ook wel ‘self asserted accounts’. Dat betekent dat de identiteit door de gebruikers zelf is opgegeven en niet geverifieerd is. Dit betekent dat je geen zekerheid hebt over de juistheid van de identiteit die de gebruiker heeft opgegeven. Dit resulteert in een laag ‘Level of Assurance’ (LoA). Dit is anders dan bij de uitgifte van een instellingsaccount door een universiteit of hogeschool, waar een uitgebreid identificatieproces aan vooraf gaat.

Sommige Service Providers besluiten daarom om gast-gebruikers minder rechten in hun applicatie te geven dan gebruikers met een instellingsaccount. Dit verschilt echter per Service Provider.

Welke Service Providers staan gastgebruik toe?

Een beperkt aantal Service Providers staat gastgebruik via Onegini toe. Wanneer een Service Provider Onegini heeft opgenomen in het selectiescherm met Identity Providers (ook wel WAYF ‘Where are you From’ genoemd), ondersteunt hij gastgebruik.

Waar kan ik documentatie over Onegini voor eindgebruikers en Service Providers vinden?

Op de SURFnet wiki staat meer informatie over Onegini die toegespitst is op:

Eindgebruikers

Service Providers

Hoe is de rolverdeling tussen Onegini & SURFconext?

SURFconext heeft een contract met Onegini voor het leveren van een applicatie voor gasttoegang tot applicaties van derden op basis van een social account. In dat contract zijn goede afspraken gemaakt over de continuïteit van Onegini, de service levels en hoe Onegini omgaat met privacy en beveiliging van data.

Meer informatie over Onegini:

Meer informatie over Onegini kan je vinden op Onegini.

Foutmeldingen bij links direct vanuit Office-applicaties

Als links direct zijn opgenomen in MS Office-applicaties zoals Word, Excel of Powerpoint, kunnen deze bij sommige SP's een foutmelding genereren inzake ontbrekende cookies. Dit komt door een bug/feature van deze producten die content proberen voor te laden en vervolgens een browser te lanceren, zonder de cookies van de oorspronkelijke request. Dit is een bekend issue met enige vorm van federatieve log-in in Office-documenten. Het gebeurt alleen bij SP's die meteen redirecten naar SURFconext wanneer een specifieke URL wordt aangevraagd.

Een client-side oplossing is om MS Office up te graden naar een versie die "Modern Authentication" ondersteunt. Zie Using Office 365 Modern Authentication with Office Clients van Microsoft voor meer informatie.

Alternatief, de SP is misschien een staat een workaround voor clients te implementeren. Dor het detecteren van de User Agent, kan de SP Office forceren om meteen op juiste wijze de browser te lanceren. Zie hier en hier voor enkele suggesties. Hoe dan ook, dit moet gebeuren aan de kant van de SP.

Inloggen in de Google Chrome-browser

> Let op: dit gaat niet over het gebruik van Chrome in het algemeen om in te loggen met SURFconext, maar specifiek om de in de browser ingebouwde functie om je aan te melden bij Chrome zelf, zodat bookmarks etc gesynchroniseerd kunnen worden.

Chrome biedt de mogelijkheid om je aan te melden bij de browser zelf. Dit stuurt een authenticatierequest naar Google om in te loggen met je Google-account. Voor instellingen die Google Apps for Education afnemen, is het daardoor in theorie ook mogelijk om hier het instellingsaccount voor te gebruiken. Er zijn situaties bekend waarin dit werkt. Echter, we krijgen regelmatig meldingen van complicaties die gebruikers tegenkomen als ze dit proberen te doen. Veelal worden die veroorzaakt door het feit dat het inloggen-in-Chrome-zelf via aparte ingebouwde beperkte browserfunctionaliteit gaat. Deze lijkt niet zo robuust te zijn inzake bijvoorbeeld sessiemanagement, en is niet goed te debuggen met bijvoorbeeld extensions omdat deze niet werken in deze conext van Chrome. SURFconext support kan hier dus weinig betekenen om dit te ondersteunen als het mis gaat. Met de informatie die we wel hebben lijkt het er op dat er niets is dat SURFconext specifiek zou kunnen veranderen om dit probleem op te lossen. Instellingen kunnen uiteraard zelf proberen via hun eigen logging en tools te achterhalen of het ergens schort. Ook is het wellicht mogelijk gebruik te maken van hun supportcontacten bij Google.