Vereiste attributen

Als een gebruiker wil inloggen bij een dienst via SURFconext wordt deze doorgestuurd naar de loginpagina van zijn organisatie, zodat hij lokaal kan authenticeren. Soms wil de dienst graag weten wie die gebruiker is, zodat hij de dienst kan personaliseren (welkom Jan Jansen) of autorisaties kan uitvoeren (bijvoorbeeld ander aanbod voor student / medewerker). De informatie die de Service Provider hiervoor nodig heeft, noemen we ook wel attributen (of claims in de ADFS-wereld). Deze attributen worden vanuit de organisatie, via SURFconext, aan de Service Provider doorgegeven. Elk attribuut bevat een bepaalde waarde die iets zegt over de gebruiker, bijvoorbeeld een naam of een e-mailadres.

Op je Identity Provider-systeem configureer je welke attributen SURFconext ontvangt van jouw organisatie.

Benodigde attributen

Verschillende diensten gebruiken verschillende attributen, soms ook met een andere attribuutnaam voor een bepaald gegeven . Om problemen voor je gebruiker te voorkomen, configureer je in ieder geval alle hieronderstaande attributen. Deze zijn veel in gebruik bij de verschillende dienstaanbieders. Meestal kunnen die direct uit een corresponderend veld uit je interne directory komen.

Het is belangrijk op te merken dat SURFconext privacybewust is opgezet en dat een service provider alleen die attributen krijgt die die service provider nodig heeft (en dus niet al onderstaande waardes). Ook heeft de SURFconext-verantwoordelijke van de instelling altijd het laatste woord over het koppelen aan een dienst. Als de SURFconext-verantwoordelijke vindt dat een dienst te veel attributen vraagt en daarmee niet voldoet aan de privacy wensen van de instelling, wordt er niet gekoppeld. De door de identity provider ingestelde en attributen blijven in beheer en onder verantwoording van de instelling ongeacht hoeveel en welke je definieert in je identity provider.

Attribuutnaam	Voorbeeldwaarde	Omschrijving	Noot
`urn:mace:dir:attribute-def:uid`	`s12489345`	De unieke code (gebruikersnaam) waarmee de gebruiker inlogt bij je organisatie	*
`urn:mace:terena.org:attribute-def:schacHomeOrganization`	`uniharderwijk.nl`	Een unieke identificatie voor deze organisatie, identiek voor alle gebruikers. Dit is in de vorm van een de door de organisatie geregistreerde domeinnaam, meestal het hoofddomein van de instelling.	*
`urn:mace:dir:attribute-def:displayName`	`Jan de Vries`	De volledige naam van de gebruiker.	
`urn:mace:dir:attribute-def:cn`	`Jan de Vries`	De volledige naam van de gebruiker, identiek aan displayName, beide zijn door elkaar in gebruik.	
`urn:mace:dir:attribute-def:givenName`	`Jan`	Voornaam van de gebruiker.	
`urn:mace:dir:attribute-def:sn`	`de Vries`	Achternaam van de gebruiker, inclusief eventuele tussenvoegsels.	
`urn:mace:dir:attribute-def:mail`	`jan.devries@uniharderwijk.nl`	E-mailadres van de gebruiker.	
`urn:mace:dir:attribute-def:eduPersonPrincipalName`	`s12489345@uniharderwijk.nl`	Globaal unieke identifier voor een gebruiker. Deze identifier dient globaal uniek gemaakt te worden d.m.v. van het toevoegen van de in schacHomeOrganization gebruikte domeinnaam.	
`urn:mace:dir:attribute-def:eduPersonAffiliation`	`employee`	Of de gebruiker 'student' of 'employee' is. Meerdere waarden voor één gebruiker zijn mogelijk, alleen vastgestelde termen toegestaan.	
`urn:mace:dir:attribute-def:eduPersonScopedAffiliation`	`employee@uniharderwijk.nl`	Zelfde waarde als eduPersonAffiliation, maar met domeinnaam uit schacHomeOrganization erachter. Beide vormen zijn naast elkaar in gebruik.	

Voor uitgebreide documentatie over syntax en semantiek van elk van deze attributen, zie Attributen in SURFconext (NL). Daar vind je ook welke attributen SURFconext nog meer ondersteunt, die nodig kunnen zijn voor specifieke service providers die ze vereisen.

* De attributen met deze noot zijn technisch noodzakelijk voor *elke* login op SURFconext en inloggen is dan ook onmogelijk als ze niet gezet zijn.

Attributen vrijgeven vanuit je IDM-systeem

Hoe het vrijgeven van attributen precies werkt voor de meest voorkomende Identity Management systemen, kun je lezen in de handleidingen voor ADFS, SimpleSAMLphp en NetIQ Access Manager.