Vertrouwde diensten voor onderzoekers automatisch koppelen

Er zijn wereldwijd zo'n 2200 diensten beschikbaar die gekoppeld kunnen worden via SURFconext en andere onderwijs- en onderzoeksfederaties. Iedere dienst apart op betrouwbaarheid beoordelen en koppelen: dat is veel werk. Gevolg: veel diensten worden niet gekoppeld, gebruikers kunnen niet inloggen met hun instellingsaccount en zoeken een onveiliger en onhandiger alternatief.

De entity categories *Research & Scholarship (R&S)* en *Code of Conduct* brengen uitkomst. Valt een dienst in beide categorieën dan krijgt hij het stempel "Betrouwbaar" van SURFconext. En kun jij hem als instelling ook vertrouwen, en automatisch beschikbaar stellen aan je gebruikers. Wat houden deze entity categories in en wat zeggen ze over de betrouwbaarheid van een dienst?

Wat zijn entity categories?

Via SURFconext en andere onderwijs- en onderzoeksfederaties van landen waar SURFnet mee samenwerkt (via eduGAIN), zijn in totaal meer dan 2200 diensten beschikbaar om te koppelen. Om het overzicht te behouden zijn diensten daarom geklassificeerd in zogehete*n entity categories* op basis van gedeelde eigenschappen. Er zijn veel verschillende entity categories, waarvan de meest relevante op deze pagina verder worden toegelicht. 2 daarvan zijn voor het aspect betrouwbaarheid van belang en die behandelen we daarom hier: *Research & Scholarship (R&S)*, een categorie diensten voor het ondersteunen van wetenschap en onderzoek, en *Code of Conduct*, een categorie diensten die expliciet verklaart te voldoen aan de AVG.

Research & Scholarship

Gedeelde kenmerken

De categorie *Research & Scholarship (R&S)* is opgezet om de beheerlast van het koppelen van individuele diensten te reduceren. Deze categorie bevat diensten met de volgende gedeelde kenmerken:

1. Het doel van de dienst is het **ondersteunen van wetenschap en onderzoek**
2. De dienst gebruikt **een vaste, gelimiteerde set attributen** voor authenticatie en autorisatie
3. Een Service Provider krijgt zo'n label niet zo maar: **de federatie waar de dienst oorspronkelijk vandaan komt controleert of de Service Provider in aanmerking komt**

Diensten sneller en makkelijker beschikbaar maken

Het doel van deze categorie diensten is het automatisch beschikbaar maken van deze diensten voor gebruikers (bijv. onderzoekers). Wetenschappers en onderzoekers hoeven hierdoor niet langer per losse dienst een aanvraag in te dienen bij de SURFconext-verantwoordelijke, die vervolgens niet langer per dienst hoeft te beoordelen of bijvoorbeeld de gevraagde attributen redelijk zijn; dat is immers van tevoren al bepaald voor de gehele categorie. Dit scheelt een hoop werk voor de SURFconext-verantwoordelijke en zorgt voor enorme tijdswinst voor wetenschappers en onderzoekers.

Door als instelling deze categorie te ondersteunen worden alle diensten binnen R&S automatisch beschikbaar gesteld aan (evt alleen een deel van) de gebruikers van jouw instelling.

Vaste, beperkte set attributen

R&S bevat alleen attributen waarmee wetenschappelijke samenwerking mogelijk wordt gemaakt. Een dienst kan alleen in aanmerking komen voor R&S als er gebruik wordt gemaakt van een (combinatie van) deze attributen. Minder mag natuurlijk altijd, maar indien een dienst *meer* attributen vereist, dan zal de dienst dat afzonderlijk met alle instellingen moeten afspreken. Automatisch koppelen werkt in dat geval niet.

De volgende attributen mogen door een R&S-dienst worden gebruikt:

1. Een (technische) identifier van de gebruiker (`eduPersonPrincipalName` - voldoende als deze gegarandeerd niet opnieuw wordt toegewezen aan andere gebruikers; anders óók `eduPersonTargetedID`)
2. Een herkenbare naam van de gebruiker (`displayName` en/of `givenName` + `sn`)
3. Een e-mail adres van de gebruiker (`mail`)
4. (Optioneel) De rol van de gebruiker binnen de instelling (`eduPersonScopedAffiliation`)

Voor meer achtergrondinformatie over deze attributen, zie Attributen in SURFconext (NL).

Code of Conduct

Om er zeker van de zijn dat de persoonsgegevens die worden uitgewisseld ten behoeve van federatieve authenticatie en autorisatie goed beschermd zijn, is een tweede *entity category* in het leven geroepen. Deze heet de *GÉANT Data Protection Code of Conduct (CoCo)*, en bevat alleen Service Providers die expliciet hebben verklaard te voldoen aan de (strenge) eisen uit de Europese wet- en regelgeving rond gegevensbescherming. Hiermee garanderen Service Providers dat zij de ontvangen persoonsgegevens (attributen) alleen gebruiken voor het mogelijk maken van federatieve authenticatie en autorisatie en het leveren van de dienst. Bijvoorbeeld: een (wetenschappelijke) wiki heeft een naam en e-mailadres nodig om onderlinge samenwerking mogelijk te maken.

Verwerkersovereenkomst niet nodig

Het uitgangspunt van R&S en CoCo is dat de Service Provider die de persoonsgegevens ontvangt geen *verwerker* is die de persoonsgegevens verwerkt in expliciete opdracht van de instelling, maar *verantwoordelijke*. Een verwerkersovereenkomst is dus niet nodig voor diensten die vallen onder de entity categories R&S en CoCo. Uitzonderingen zijn in specifieke gevallen natuurlijk mogelijk: in dat geval gaan de afspraken die de instelling met de dienst maakt altijd voor.

Voor alle diensten die onder R&S vallen geldt **gerechtvaardigd belang** als grondslag voor het verwerken van persoonsgegevens voor de authenticatie en autorisatie van de gebruiker. Met andere woorden, door R&S te gebruiken is het uitwisselen van een minimale set attributen die nodig is voor het mogelijk maken van federatieve authenticatie en autorisatie ten behoeve van diensten voor wetenschap en onderzoek gegrond. REFEDS heeft als eigenaar van deze entity category uitgebreid de juridische aspecten van R&S getoetst.bronnen

Extra bronnen met juridische achtergrondinformatie
• Een uitgebreide juridische analyse van de grondslag voor R&S (Engels) • Een blogpost van de juridisch adviseur van JISC (NREN uit het VK) over federatieve login en de AVG (Engels)

Enkele voorbeelden van diensten die binnen R&S en CoCo vallen

• **CERN Service Provider Proxy** (https://cern.ch/login)
  • CERN, bekend van onder andere de Large Hadron Collider en de ontdekking van het higgsboson, werkt met wetenschappers van over de hele wereld, verspreid over honderden verschillende instellingen.
• **BBMRI-ERIC** (http://www.bbmri-eric.eu/)
  • BBMRI is een Europese infrastructuur voor onder andere biologische data. Via BBMRI wordt iedereen die te maken heeft met biomedisch onderzoek samengebracht onder 1 infrastructuur.
• **ELIXIR research infrastructure AAI** (https://www.elixir-czech.cz/)
  • De Tsjechische node van het Elixir-project verzorgt een duurzame oplossing voor de opslag van onderzoeksdata uit de Life Sciences. Via deze infrastructuur wordt de opgeslagen data beschikbaar gesteld aan anderen en worden daarvoor verschillende tools, maar ook trainingen, aangeboden.
• **DARIAH AAI** (https://www.dariah.eu/)
  • DARIAH is een Europese infrastructuur voor de geesteswetenschappen. Via deze infrastructuur worden verschillende diensten die verspreid door Europa te vinden zijn, gecombineerd onder 1 paraplu.

Meedoen?

Diensten die in beide categorieën vallen worden als "Betrouwbaar" beschouwd. Deze diensten kun je via SURFconext automatisch koppelen aan je Identity Provider, zodat de beheerlast een stuk lager wordt en daarmee ook het leven van bepaalde gebruikers. Gebruikers hoeven dan namelijk niet meer een losse aanvraag te doen voor een dienst; zij kunnen gewoon direct inloggen (uiteraard na het geven van consent!).

Heeft jouw instelling gebruikers die hier mogelijk van kunnen profiteren? Vraag het automatisch koppelen voor jouw Identity Provider aan via SUR Fconext Dashboard of support@surfconext.nl.