Documentatie voor Identity Providers

Via de SURFconext-infrastructuur beschikken onderzoekers, medewerkers en studenten over clouddiensten van verschillende aanbieders. Authenticatie, autorisatie, groepsbeheer en afspraken over privacy en beveiliging worden zo veel mogelijk centraal geregeld. SURFconext neemt je werk uit handen: er is één koppeling nodig in plaats van een aparte koppeling per dienst.

Wil je dat gebruikers van jouw instelling toegang krijgen tot clouddiensten? Dan kan je als Identity Provider aansluiten op SURFconext. Lees verder en ontdek wat je allemaal moet doen om als Identity Provider te koppelen met SURFconext en daar vervolgens optimaal gebruik van te maken.

Deze handleiding is bedoeld voor Identity Providers en beschrijft:

- De basisprincipes van SURFconext
- Hoe je als instelling de Identity Provider aansluit op SURFconext
- Hoe je beschikbare diensten activeert
- Hoe je kunt samenwerken via SURFconext
- Informatie over hoe je de Identity Provider beheert
- Wie je kan helpen tijdens het aansluitproces
- Welke mailings er zijn met betrekking tot SURFconext en hoe je jezelf kunt abonneren
- Veel gestelde vragen IdP

Voordelen SURFconext:

- Door 1 koppeling te maken met SURFconext, regelt de instelling in 1 keer de toegang tot alle op SURFconext gekoppelde diensten (die de instelling wil gebruiken)
- De instelling heeft geen onderhoud meer aan zelfgebouwde koppelingen
- De instelling biedt met SURFconext studenten en medewerkers altijd en overal toegang: thuis, onderweg en in het buitenland
- SURFconext kan de informatieverplichting (consent) over het delen van persoonsgegevens met dienstaanbieders overnemen
- Eenmaal aangesloten op de SURFconext, kan de instelling sneller en eenvoudiger aansluiten op nieuwe diensten
- De instelling kan gebruik maken van alle SURFconext diensten, zoals SURFsecureID, gastgebruik, groepmanagement, rijkere autorisatie etc
- Een instelling kan gebruikers van andere instellingen toegang geven tot geleverde diensten (de instelling treedt dan op als een aanbieder)
- SURFconext is gebaseerd op open standaarden (SAML/OpenID Connect)
- Gebruikersaccounts + wachtwoorden blijven bij de instelling (en gaan niet naar de dienst)
- Vertrouwen: gebruikte protocollen zorgen voor 'technisch vertrouwen', oftewel de zekerheid dat de berichten bij de juiste partij belanden en niet te onderscheppen (lees: te veranderen) zijn.
- Inzage in statistieken (hoeveel logins, welke dienst, hoeveel unieke gebruikers, etc.)

Voordelen voor eindgebruikers:

- Met de inloggegevens van de eigen instelling kun je inloggen op alle gekoppelde diensten, ook bij andere instellingen, ook buiten Nederland
- Je hoeft niet elke keer een nieuw account aan te maken, veilige wachtwoorden te bedenken en te managen etc.
- SURFconext zorgt dat je niet voor elke dienst opnieuw hoeft in te loggen (Single Sign-on)
- De kans dat je/een wachtwoord uitlekt en wordt misbruikt is kleiner, omdat het wachtwoord alleen bij de eigen instelling (en niet bij een aanbieder) ingevoerd wordt
- Je identiteit wordt alleen bekend als dat noodzakelijk is, zoals bij toetsen (SURFnet streeft met aanbieders naar doorgifte van zo weinig mogelijk gegevens)
- Je privacy is beter beschermd, want leveranciers moeten zich houden aan de policy van SURFconext (waarin o.a. veel aandacht voor privacy & data-beveiliging) + consent (inzage in welke attributen over de lijn gaan en evt. het weigeren daarvan)