

Relatie SURF (SURFconext) en Kennisnet (Entree)

Kennisnet biedt met de [Entree Federatie](#) een federatie aan voor het funderend en middelbaar beroepsonderwijs (mbo). SURFconext biedt een federatie aan voor het middelbaar beroeps- en hoger onderwijs en wetenschap. Het mbo is dus doelgroep van beide federaties.

Hieronder geven we aan hoe instellingen en diensten hier concreter mee om kunnen gaan, en daarna ook nog achtergrondinformatie over waarom de twee federaties naast elkaar bestaan en niet aan elkaar gekoppeld zijn.

Doelgroep federatie							
	PO	VO	MBO	HBO	WO	Research	UMC
Entree	✓	✓	✓				
SURFconext			✓	✓	✓	✓	✓

Samenvatting

- De Entree Federatie en SURFconext zijn technisch niet aan elkaar gekoppeld.
- Een mbo-instelling sluit aan op zowel Entree als SURFconext, via één Identity Provider-installatie zijn beide federaties eenvoudig naast elkaar te ontsluiten.
- Een dienstaanbieder kiest afhankelijk van de doelgroep van de dienst voor een aansluiting op Entree of op SURFconext, of in uitzonderlijke gevallen, op beide.

Voor instellingen (identity providers)

De overlap tussen de federaties geldt alleen voor mbo-instellingen. Andere instellingen kunnen sowieso maar aansluiten op één van de federaties.

Om aansluiten eenvoudig te houden spreken SURFconext en Entree hetzelfde technische protocol voor identity providers (SAML 2.0). Een mbo-instelling heeft dus voldoende aan één softwareproduct voor de identity provider-koppeling met beide. In dit product worden vervolgens twee configuraties opgenomen met daarin de juiste URLs en attributsets die bij de respectievelijke federatie horen. Deze koppelingen vereisen in het algemeen weinig onderhoud nadat ze eenmaal gemaakt zijn en via deze koppelingen kunnen honderden diensten gebruikt worden.

Voor dienstaanbieders (service providers)

De dienstaanbieder bepaalt op basis van haar doelgroep op welke federatie ze aansluit. Zie daarvoor de tabel bovenaan de pagina.

Sluit aan op één federatie

Enkele voorbeelden:

1. Bedien je mbo en hbo? Dan is SURFconext een passende keuze.
2. Bedien je vo en mbo? Dan is Entree geschikt.
3. Bedien je uitsluitend mbo? Dan zijn beide federaties geschikt.

Aansluiten op beide federaties

Alleen diensten die een heel brede doelgroep hebben, dat wil zeggen, bijvoorbeeld zowel vo als hbo onder hun klanten hebben, dienen op beide federaties aan te sluiten. Technisch gezien lijken de koppelingen op elkaar dus dit is mogelijk met dezelfde software en protocollen. De ontvangen attributen zullen wel anders zijn.

Het is aan de dienstaanbieder om vervolgens de gebruiker de juiste ingang op te sturen bij het inloggen. Deze UX-keuzes hangen erg af van de opzet en werking van de dienst zelf. Als er bijvoorbeeld al bekend is voor welke instelling de inlog bedoeld is, dan kan de juiste federatie aangeboden worden. Een keuzescherf "inloggen voortgezet en middelbaar onderwijs" versus "inloggen hogescholen en universiteiten", waarna de gebruiker naar de juiste federatie wordt gestuurd, is ook denkbaar. De dienst kan ook zelf een lijst met alle ondersteunde instellingen ("where are you from"-scherf) maken en onderhouden, en onderwater de gebruiker richting de corresponderende federatie sturen.

Achtergrond

De federaties lijken qua architectuur op elkaar en gebruiken ook dezelfde technische protocollen. Er zijn echter ook significante (functionele) verschillen, in bijvoorbeeld de doelgroep, typen eindgebruikers, organisatie van aangesloten instellingen, type aangesloten diensten, al dan niet internationale samenwerking en welke informatie uitgewisseld wordt. Zo richt Entree zich voor een belangrijk deel op scholieren en op de onderwijs-use case. SURFconext heeft een andere doelgroep en faciliteert bijvoorbeeld ook internationaal samenwerkende wetenschappers. Elk van de twee is dus optimaal ingericht voor de eigen functionele eisen, die maar gedeeltelijk overlappen.

In het verleden is er een pilot geweest met het technisch koppelen van beide federaties, zodat diensten aangesloten op Entree ook gebruikt konden worden door instellingen van SURFconext. De redenen om hier niet verder mee te gaan:

- Het gebruik van de pilot is maar heel beperkt gebleken. Sindsdien is het mbo ook aangesloten op SURFconext. Zoals hierboven beschreven is er daarmee voor maar een heel klein aantal diensten nog van toepassing dat ze op beide zouden moeten aansluiten.
- Entree en SURFconext ondersteunen nu dezelfde technische protocollen, zodat die gevallen waarin er toch op twee aangesloten moet worden, dezelfde software gebruikt kan worden, met alleen andere configuratie.
- Integratie of koppeling van twee proxy's achter elkaar is niet triviaal en zou een flinke investering vereisen.
- In onze ervaring is de federatie al een complex geheel waarin het nu soms al onduidelijk is voor instellingen waar of waarom iets fout gaat of niet werkt. Bij het achter elkaar schakelen van twee proxy's neemt de complexiteit van de keten toe en de transparantie van wat er waar gebeurt af. Die extra complexiteit lijkt op dit moment niet gerechtvaardigd voor de mogelijke opbrengst.

Kennisnet en SURF zijn en blijven in regulier contact over goede afstemming tussen de federaties. Hierbij hebben we het bijvoorbeeld over:

- Rolverdeling helder maken tussen de doelgroepen van instellingen en dienstaanbieders.
- Zorgen dat onze koppelingen technisch hetzelfde werken.
- Afstemming van attributsets. Zo is nu het ECK ID ook beschikbaar in SURFconext.
- Verkennen gezamenlijk optrekken met nieuwe ontwikkelingen zoals eduID.

Afbouw pilot

Het laatste resterend gebruik van de pilot-koppeling wordt in de zomer van 2024 beëindigd. Service providers op Entree die gebruikers van SURFconext laten inloggen, kunnen (ook) aan SURFconext koppelen. Een instelling krijgt dan vanuit SURFconext het verzoek of ze inderdaad die service provider die eerst via Entree liep nu via SURFconext wil koppelen en kan besluiten of ze dat inderdaad wil (blijven) toestaan. Voor het overige is er van instellingen geen actie vereist.