

Woordenlijst

- [Access Control List \(ACL\)](#)
- [Attribuut](#)
- [Authenticatie](#)
- [Authenticatiemiddel](#)
- [Autorisatie](#)
- [Gebruiker](#)
- [Hub en spoke setup](#)
- [Identificatie](#)
- [Identifier](#)
- [Identiteit](#)
- [Identity management](#)
- [Identity Provider](#)
- [Lifecycle management](#)
- [Samenwerkingsorganisatie](#)
- [Service Provider \(SP\)](#)
- [SAML](#)
- [Single Sign On-toegang](#)
- [SLS](#)
- [Trust framework](#)
- [User consent](#)
- [WAYF \(Where are you from\)](#)

Access Control List (ACL)

Een lijst die SURFconext bijhoudt, waarin staat welke Identity Providers toegang hebben tot een Service Provider.

Attribuut

Attributen zijn kenmerken van gebruikers, zoals naam, e-mailadres en organisatie. Voor het authenticeren en autoriseren van gebruikers wordt gebruikgemaakt van deze attributen.

SURFnet hanteert daarin het principe van 'minimal disclosure' en geeft alleen gegevens van gebruikers door die noodzakelijk zijn voor het gebruik van een dienst. Elke instelling die een dienst wil gebruiken, moet expliciet akkoord geven voor het doorgeven van de attributen.

Authenticatie

Bij authenticatie laat de gebruiker zien dat hij beschikt over een authenticatiemiddel dat hoort bij een bepaalde account en identiteit.

De identiteit is vooraf op een andere manier vastgesteld (identificatie). Het doel van de authenticatie is om te laten zien dat de gebruiker is wie hij zegt te zijn. Strikt genomen kan echter alleen worden vastgesteld dat een gebruiker tijdens de authenticatie het bij een identiteit horende authenticatiemiddel heeft gebruikt.

Authenticatiemiddel

Een voorziening die een gebruiker aanwendt om zich te authenticeren bij een dienst.

Voorbeelden zijn een combinatie van een gebruikersnaam en een wachtwoord (basisauthenticatie) of een gebruikersnaam en een certificaat, tokens met wachtwoord (sterke authenticatie).

Autorisatie

Autorisatie is het toekennen van bevoegdheden. Op basis van bepaalde gegevens wordt bijvoorbeeld bepaald tot welke diensten een gebruiker toegang heeft. Dat kan gebeuren op basis van de rol die een gebruiker heeft binnen een project of organisatie. Zo kan een uitgeverij bepaalde publicaties beschikbaar stellen aan specifieke medewerkers van een bepaalde onderwijsinstelling. Daarvoor is aanvullende informatie behorend bij een identiteit nodig, zoals bijvoorbeeld de functie die een medewerker heeft ('attributen').

Gebruiker

Een lid van de Identity Provider (bijvoorbeeld een student of medewerker).

Hub en spoke setup

Een hub en spoke setup is een systeem van verbanden in de vorm van een spakenwiel, waarbij al het verkeer langs de spaken gaat naar een hub in het midden (in ons geval de SURFconext-hub)

Identificatie

Identificatie is het vaststellen van de identiteit van een gebruiker, bijvoorbeeld door de gebruiker zijn rijbewijs of paspoort te laten tonen. De identiteit wordt vervolgens gebruikt om een account van de gebruiker bij de Identity Provider te creëren.

Identifier

Een label (meestal een string of tekst) waarmee je een entiteit (een gebruiker, object o.i.d.) aanduidt. Dit maakt het mogelijk om naar een entiteit te verwijzen. Zo'n entiteit heeft meestal meerdere identifiers die in verschillende contexten nuttig kunnen zijn (denk aan: uid, ePPN enz.).

Identiteit

Een identiteit bepaalt één of meer van de volgende zaken:

- wie de gebruiker is (er heeft identificatie plaatsgevonden);
- welke authenticatiemiddelen de gebruiker kan gebruiken;
- of de gebruiker geautoriseerd is voor toegang tot een dienst, liefst door middel van rollen;
- welk profiel de gebruiker heeft zodat diensten op maat geleverd kunnen worden.

Een identiteit heeft een uniek kenmerk ('unique identifier').

Identity management

Het geheel van processen en techniek voor het beheer en gebruik van elektronische identiteiten.

Identity Provider

Een organisatie die gegevens verstrekt over de identiteit van de gebruiker waardoor authenticatie van de gebruiker mogelijk is.

Lifecycle management

De periode vastleggen en beheren waarbinnen iemand een dienst mag gebruiken. Denk daarbij aan een account dat alleen voor een bepaalde periode gebruikt kan worden door geautoriseerde personen. Zolang jouw studenten en medewerkers bij jouw organisatie studeren of werken mogen ze diensten van SURFnet gebruiken. Zodra zij klaar zijn met hun studie of niet meer werkzaam zijn bij jouw organisatie, moet hen de toegang tot SURFnet-diensten worden onzegd.

Samenwerkingsorganisatie

Groepen gebruikers verspreid over meerdere organisaties die samenwerken en samen een eigen organisatie vormen.

Service Provider (SP)

Een Service Provider is een organisatie die via SURFnet diensten of content aanbiedt die via het internet toegankelijk zijn. Denk aan webshops, videodiensten, uitgevers, maar bijvoorbeeld ook onderwijsinstellingen die lesmodules aan studenten van andere onderwijsinstellingen aanbieden.

SAML

Security Assertion Markup Language (SAML) is een gestandaardiseerde taal die wordt gebruikt om binnen en tussen federaties informatie uit te wisselen.

Single Sign On-toegang

Eenmaal aanmelden en vervolgens met dezelfde gebruikersnaam en wachtwoord toegang hebben tot alle diensten, zonder je nog een keer aan te hoeven melden.

SLS

Richtlijnen vanuit SURFnet over de beschikbaarheid en bereikbaarheid diensten.

Trust framework

Een certificaat dat Service Providers en Identity Providers ondertekenen om aan te geven dat ze de identiteit, beveiliging en het privacybeleid van SURFconext vertrouwen en vice versa.

User consent

De functionaliteit waarmee de gebruiker expliciet toestemming kan geven voor het uitwisselen van persoonsgegevens met externe Service Providers. SURFconext biedt deze 'user consent'-functionaliteit aan, zodat instellingen kunnen voldoen aan de Algemene Verordening Gegevensbescherming ([AVG](#)).

WAYF (Where are you from)

Inlogscherm waarin je moet selecteren van welke organisatie je afkomstig bent, zodat je daar kunt authenticeren.
