SSO Koppelingen met Pleio

Introductie

Single Sign-On (SSO) koppelingen zijn mechanismen die gebruikers in staat stellen om met één set inloggegevens toegang te krijgen tot meerdere applicaties of diensten. Er zijn twee hoofdvarianten van SSO koppelingen: OpenID Connect (OIDC) en Security Assertion Markup Language (SAML). Hoewel Pleio beide soorten SSO koppelingen ondersteunt, gaat de voorkeur sterk uit naar OIDC. Deze voorkeur is gebaseerd op de verwachting dat meer overheidsinstellingen zullen afstappen van SAML ten gunste van OIDC, vanwege zijn modernere en flexibelere architectuur.

Focus op OIDC Koppelingen

Gezien de verschuiving in de voorkeur van SSO-technologieën, focust dit document zich op het opzetten en troubleshooten van OIDC koppelingen met Pleio via de Account service. OIDC biedt een efficiënte en gestandaardiseerde wijze voor authenticatie processen, wat het een aantrekkelijke keuze maakt voor hedendaagse digitale toepassingen.

Technische Achtergrond

- Account service: De productieomgeving is te vinden op account.pleio.nl, en de testomgeving op account.pleio-test.nl. De code is open source en is te vinden op onze Gitlab onder de applicatienaam Concierge.
- Frontend: Om een koppeling te testen maken we gebruik van developertesting.pleio.nl (productie) en review.pleio-test.nl (test).
- Voor de flow van authenticatie zijn de onderstaande bestanden relevant:
    - `/core/oidc/views.py`
    - `/core/oidc/auth.py`
    - `/core/oidc/user_factory.py`

- Mozilla Django OIDC Library: Concierge maakt gebruik van deze library. Bestanden van belang:
  - `/mozilla_django_oidc/auth.py`
  - `/mozilla_django_oidc/views.py`

Opzetten van een OIDC Koppeling

Contact met het Pleio Team

Voor het opzetten van een OIDC koppeling kunt u contact opnemen met het Pleio team. Wij voorzien u van de benodigde informatie en ondersteuning.

Identificatie van Rollen

- Identity Provider (IDP): De IDP is de partij die de identiteit van de gebruikers verifieert. In een OIDC-koppeling stuurt de IDP het ID Token en, indien van toepassing, het Access Token naar de Service Provider na succesvolle authenticatie van de gebruiker.
- Service Provider (SP): Pleio fungeert als de Service Provider. De SP vertrouwt op de IDP om gebruikers te authenticeren en stuurt gebruikers naar de IDP voor het inlogproces.

Aanmaken van Client ID en Secret

- Na het ontvangen van de callback URL van het Pleio team, dient u een client ID en secret te genereren.
- Het is aanbevolen om het secret via een veiliger kanaal dan e-mail te delen, zoals via een beveiligde berichtenservice.

Vereisten van de Identity Provider (IDP)

De IDP dient het Pleio team te voorzien van de volgende informatie:

- "Well-Known/Openid-Configuration" Endpoint: Dit endpoint bevat configuratie-informatie die nodig is voor het opzetten van de koppeling.
- Token, JWKS en Authorize Endpoint: Als het "well-known/openid-configuration" endpoint niet beschikbaar is, moeten deze afzonderlijke endpoints samen met het signing algoritme verstrekt worden.

Gebruikersgegevens en Claims

- Pleio verwacht dat de 'sub' en 'email' claim minimaal aanwezig zijn in het token.
- De 'sub' bepaalt, in combinatie met een identifier voor de koppeling, of het de eerste keer is dat een gebruiker inlogt met de koppeling.
- Bij de eerste inlog wordt er een gebruiker aangemaakt in het systeem van Pleio, met als 'email' de meegestuurde 'email' claim.
- Voor het 'name' veld van de nieuwe gebruiker wordt gekeken naar claims in de volgende volgorde: 'preferred_username', 'nickname', 'name', 'given_name'. Bij afwezigheid van deze claims wordt de 'name' gebaseerd op het e-mailadres.
- Bij bestaande gebruikers worden de 'email' en 'name' velden geüpdatet als er nieuwe waarden worden meegestuurd in het token voor deze claims.

Belangrijke Aandachtspunten

Controle van Client ID en Secret

- Het komt vaak voor dat er verwarring ontstaat over de juiste client ID. Men haalt soms verschillende IDs,, zoals de Application ID, Object ID, en anderen, door elkaar.
- Zorg ervoor dat de juiste client ID en secret worden meegestuurd. Deze zijn cruciaal voor het succesvol functioneren van de SSO koppeling.
- Bij twijfel, stuur een screenshot van de omgeving waar de client ID en secret zijn gegenereerd. Dit stelt het Pleio team in staat om zelf te controleren en te bevestigen of de correcte gegevens zijn verstrekt.

Veelgestelde Vragen (FAQ)

Wat is het verschil tussen OIDC en SAML?

OIDC is gebaseerd op OAuth 2.0 en gebruikt JSON Web Tokens (JWT) voor identiteitsinformatie, terwijl SAML een oudere standaard is die XML gebruikt voor het uitwisselen van authenticatie- en autorisatiegegevens.

Waarom heeft Pleio een voorkeur voor OIDC boven SAML?

De voorkeur voor OIDC komt door zijn modernere architectuur, flexibiliteit, en de verwachting dat meer overheidsinstellingen naar deze technologie zullen migreren.

Hoe veilig zijn OIDC koppelingen?

OIDC koppelingen zijn zeer veilig mits correct geconfigureerd, met mechanismen als SSL/TLS voor data encryptie en secure token handling.

Kan Pleio naast OIDC ook SAML koppelingen ondersteunen?

Ja, Pleio ondersteunt beide typen koppelingen, maar de focus en aanbeveling ligt bij OIDC vanwege de genoemde voordelen.

Wat zijn de voornaamste stappen voor het opzetten van een OIDC koppeling met Pleio?

Het proces omvat voorbereidende gesprekken met de IDP, het bepalen van een shortname, het communiceren van callback URL's voor clientID en secret, en het configureren van de koppeling in Pleio admin.

Hoe worden gebruikersgegevens behandeld in OIDC?

Gebruikersgegevens worden veilig uitgewisseld via tokens, met minimale vereiste claims zoals 'sub' (subject) en 'email'.

Wat als er problemen zijn tijdens het authenticatieproces?

Concierge's logs kunnen worden gefilterd op de shortname van de koppeling voor gerichte analyse en troubleshooting. Deze FAQ-sectie biedt antwoorden op veelvoorkomende vragen.

Informatieve Bron over OIDC

Voor meer inhoudelijke informatie over hoe OIDC werkt, bekijk deze YouTube video: OpenID Connect In Depth.