

# OAuth 2.0 / OIDC

- Inleiding
- Verantwoordelijkheden
- Metagegevens
- Logout

# Inleiding

Dit document beschrijft de manier waarop een Service Provider (SP) een federatie met de Identity Provider (IdP) van de Universiteit via het OAuth 2.0 OpenID Connect (OAuth 2.0 en OIDC) protocol kan realiseren. De benodigde informatie, en voorwaarden worden in dit document beschreven.

# Verantwoordelijkheden

De aanvrager is gemandateerd om namens de applicatie eigenaar een federatie tussen de Service Provider en Identity Provider aan te vragen. De applicatie eigenaar is formeel eindverantwoordelijk en dient zelf een functioneel en technisch team aan te stellen voor werkzaamheden aan de Service Provider die voortvloeien uit de totstandkoming van deze federatie<sup>[1]</sup>.

Wijzigingen aan de kant van de applicatie moeten worden afgestemd met het Identity and Access Management (IAM) team via de ITS Servicedesk. Soms zijn er ook wijzigingen aan de kant van de Identity Provider. In dat geval neemt het IAM team contact op met de aangewezen functioneel beheerder(s) van de applicatie.

Het IAM team communiceert niet direct met leveranciers. Contact met een leverancier over de federatie dient te allen tijde via een medewerker van de Universiteit Utrecht te verlopen. Dit kan de applicatie eigenaar dan wel een functioneel beheerder zijn.

---

<sup>[1]</sup> Hierbij kan bijvoorbeeld gedacht worden aan de implementatie en het onderhouden van de gebruikte OAuth 2.0 en OpenID Connect softwarebibliotheek van de Service Provider.

# Metagegevens

## Metadata Identity Provider

De metadata van de Identity Provider kan via de volgende URL's worden verkregen:

Productie	<a href="https://login.uu.nl/nidp/oauth/nam/.well-known/openid-configuration">https://login.uu.nl/nidp/oauth/nam/.well-known/openid-configuration</a>
Acceptatie	<a href="https://login.acc.uu.nl/nidp/oauth/nam/.well-known/openid-configuration">https://login.acc.uu.nl/nidp/oauth/nam/.well-known/openid-configuration</a>

Hier is informatie te vinden over ondersteunde algoritmen, autorisatie endpoints, scopes, response types, response modes, en authenticatie methoden.

## Client configuration

Voor het registreren van de Service Provider als client application zijn de volgende gegevens benodigd:

Parameter	Vereist/ Optioneel	Beschrijving	Waarden
Client name	Vereist	Naam van de Service Provider	
Redirect URIs	Vereist	Redirect URI waarden	
Application type	Optioneel	Web/native	
Grants required	Vereist	Gewenste grants	
Token types	Vereist	Gewenste token types	

# Logout

## Introductie

Op [deze](#) en [deze](#) pagina's vind je meer informatie over de gebruikte specificaties. Deze specificaties zijn leidend, de tekst hieronder geldt als een versimpelde **conceptuele** uitleg. Deze tekst moet niet gebruikt worden als leidraad voor een implementatie. Daarvoor verwijzen we naar de eerder genoemde specificaties.

## Beknopte uitleg

Net zoals bij SAML2.0 Single Logout is het met OpenID Connect mogelijk om vanuit een Relying Party (RP) en vanuit een OpenID Provider (OP) uit te loggen.

Voor het gemak beschrijven we deze implementaties als **Relying Party initiated Logout** en **OpenID Provider initiated Logout** en noemen we de OpenID Provider (OP) een Identity Provider (IdP).

### **Relying Party initiated Logout (specificatie: OpenID Connect RP-Initiated Logout 1.0)**

1. De browser stuurt een uitlog verzoek naar de Relying Party.
2. De Relying Party stuurt de browser van de gebruiker door naar de uitlogpagina van de Identity Provider.
3. De Identity Provider beëindigt de gebruikerssessie en stuurt het uitlogverzoeken naar andere Relying Party's en leidt de browser optioneel door naar de uitlogpagina van de Relying Party.

### **OpenID Provider initiated Logout (specificatie: OpenID Connect Front-Channel Logout 1.0)**

1. De browser stuurt het uitlogverzoek naar de Identity Provider.
2. De Identity Provider toont een uitlogpagina met één of meerdere **<iframe>** elementen met de logout URI's van de Relying Party's waarmee de eindgebruiker een sessie heeft.
3. De browser roept alle **<iframe>** elementen aan en initieert per Relying Party één uitlogverzoek.
4. De Relying Party ontvangt het uitlogverzoek en beëindigen de sessie met de gebruiker.

In tegenstelling tot SAML2.0 Single Logout (m.u.v. een asynchrone logout) is er bij bovengenoemde implementaties geen garantie dat de sessie bij de Relying Party beëindigd is.

## Implementatie

Een aantal factoren waar een beheerder en/of ontwikkelaar van een Relying Party rekening mee moet houden zijn:

- Het gebruik van security headers t.b.v. **<iframe>** elementen zoals (maar niet uitsluitend): X-Frame-Options, Content-Security-Policy, etc. op de uitlogpagina (frontchannel\_logout\_uri).
- Het verschil tussen een frontchannel\_logout\_uri en post\_logout\_redirect\_uri.
- Het vermelden van de frontchannel\_logout\_session\_required indien de waarde 'true' is.
- Bij het gebruik van een post\_logout\_redirect\_uri is een id\_token\_hint verplicht.

## Testen

Het Identity Provider /.well-known/openid-configuration endpoint adverteert ondersteuning voor onderstaande instellingen. Dit houdt in dat als jouw applicatie deze instellingen automatisch inleest er mogelijk onbedoeld gebruik gemaakt wordt van de mogelijkheid om uit te kunnen loggen. Om een correcte werking van de OpenID Connect implementatie te garanderen doen wij een dringend verzoek om dit te controleren.

Via een TOPdesk melding kan verzocht worden om jouw geregistreerde applicatie op de Identity Provider te voorzien van tenminste een logout\_redirect\_uri en optioneel een post\_logout\_redirect\_uri.

Onderstaande elementen zijn t.o.v. de productie omgeving toegevoegd aan het /.well-known/openid-configuration endpoint:

- end\_session\_endpoint: https://login.<acc>.uu.nl/nidp/oauth/v1/nam/end\_session
- frontchannel\_logout\_session\_supported: true
- frontchannel\_logout\_supported: true