Dienst Uitvoering Onderwijs
Ministerie van Onderwijs, Cultuur en Wetenschap

CONCEPT/~~VERTROUWELIJK~~/~~DEFINITIEF~~

Directie
DFS-ICT-RNE

Afdeling
Facet

Contactpersoon
René Bosscher
Software Architect
rene.bosscher@duo.nl

Datum
06-05-2026

Bijlagen
nvt

Betreft: Wijzigingsvoorstel OAuth2.0

Versie 0.1

Inhoudsopgave

1 Aanleiding

Op 30-03-2026 heeft een werkgroep bijeenkomst plaatsgevonden t.b.v. Edustandaard Werkgroep Edukoppeling. Tijdens de werkgroep bijeenkomst (en een aantal gesprekken daarna) zijn er zijn vragen gesteld als onderdeel van het onderwerp ‘OAuth profiel’ rond de optionele extra claims die in het OAuth token opgenomen kunnen worden t.b.v. routering en mandaatvalidatie.

Met dit document wordt een wijzigingsvoorstel gedaan om dat deel in het profiel te verbeteren.

2 Wijzigingsverzoek

2.1 Openstaande vragen

2.1.1 Naamgeving custom claims

Voor de uitwerking van het OAuth profiel zijn vragen gesteld over de naamgeving van de voorgestelde custom claims t.b.v. routering en mandaatvalidatie en de mogelijke risico's op interoperabiliteitsproblemen.

Momenteel zijn de custom claims 'act' en 'pdi' voorgesteld. Als we dit als publieke claims beschouwen, dan zouden deze ook geregistreerd moeten zijn of worden bij IANA. Of we houden deze claims private en schrijven een format voor in de vorm van een URI.

In een vorig overleg is ook de optie genoemd om de edu-from en edu-to van het REST-SaaS profiel over te nemen.

Deze paragraaf de aanleiding voor wijzigingsverzoek 2.2.1

2.1.2 Optie om RAR te ondersteunen

Tijdens de vorige bijeenkomst van de werkgroep op 30-03-2026 is een alternatieve optie voorgesteld voor het meegeven van routering en mandaatvalidatie gegevens.

De RAR (RFC 9396 - OAuth 2.0 Rich Authorization Requests) beschrijft een methodiek om vergelijkbare gegevens mee te sturen zonder dat er custom claims in het token request meegestuurd hoeven te worden. De custom claims zouden dan als key/value attributen in een stukje JSON meegestuurd moeten worden via een extra URL parameter 'authorization_details'. Voorwaarde is wel dat deze key/value attributen worden opgenomen in het access token dat opgeleverd wordt door de AS.

Met opmerkingen [DG1]: Dit is in ieder geval een mature standaard. Dat staat nog even naast adoptie.

De openstaande vraag uit het vorige overleg, en de terugkoppeling uit de PoC, is de adoptie van de standaard in main-stream (open-source) IAM systemen.

Deze paragraaf de aanleiding voor wijzigingsverzoek: 2.2.2

2.2 Gewenste wijziging(en)

De gewenste wijzigingen om in het OAuth profiel door te voeren zijn:

2.2.1 Aanpassing optionele custom claims

In de beschrijving van de custom claims t.b.v. een token request en access token is het gewenst om het volgende aan te passen:

- Custom claim 'act' wordt hernoemd naar 'edu-from' met als format: "urn:edukoppeling:oin:XXXXXXXXXXXXXXXXXXXX"
- Custom claim 'pdi' wordt hernoemd naar 'edu-to' met als format: "urn:edukoppeling:oin:XXXXXXXXXXXXXXXXXXXX"

2.2.2 Optionele RAR ondersteuning

Het is gewenst om in het profiel de optie op te nemen dat een implementerende partij naast de al beschreven optionele custom claims ook kan kiezen voor de toepassing van de RAR voor een token request en access token.

Bij de RAR moet dan de extra URL parameter 'authorization_details' meegestuurd worden bij een token request i.p.v. de optionele custom claims in het token request jwt. Daarnaast moeten de key/value attributen van de URL parameter

'authorization_details' opgenomen worden in de access token die door de AS wordt uitgegeven.

Voorbeeld met een URL parameter 'authorization_details':

```
POST /oauth2/token HTTP/1.1
Host: server.example.com
Content-Type: application/x-www-form-urlencoded
HTTP request parameters:
* REQUIRED  grant_type=client_credentials
* REQUIRED  &client_assertion_type=urn:ietf:params:oauth:client-assertion-type:jwt-bearer
* REQUIRED  &client_assertion=<JWT met claims>
* OPTIONAL  &scope="nl-test-admin-flow-0 nl-test-admin-flow-2-3-4"
* OPTIONAL  &authorization_details=[
{
  "type": "edukoppeling_mandaat",
  "edu-from": "urn:edukoppeling:oin:XXXXXXXXXXXXXXXXXXXX",
  "edu-to": "urn:edukoppeling:oin:XXXXXXXXXXXXXXXXXXXX"
}
```

Voorbeeld met een 'authorization_details' in het access token:

```
{
  "iss": "https://m2m.facet.onl/oauth2/token",
  "sub": "XXXXXXXXXXXXXXXXXXXX",
  ...
  "authorization_details": [
    {
      "type": "edukoppeling_mandaat",
      "edu-from": "urn:edukoppeling:oin:XXXXXXXXXXXXXXXXXXXX",
      "edu-to": "urn:edukoppeling:oin:XXXXXXXXXXXXXXXXXXXX"
    }
  ]
}
```

Met opmerkingen [RR2]: Verfijningsvoorstel:

```
{
 "iss": "00000001802514306000",
 "sub": "00000001802514306000",
 "aud": "https://koppelvlak.duo.nl/oauth/token",
 "jti": "a8f3b2c1-...",
 "exp": 1712484300,
 "urn:edukoppeling:dienstaanbieder:oin":
"00000001802514306000",
 "urn:edukoppeling:dienstafnemer:oin":
"00000004012345678000"
}
```

Waarbij:
Volgens industry standard gebruik iss EN sub beide het client id bevatten
"aud" bevat de url van het token endpoint
Extra claims staan niet genest in het object omdat niet alle servers/libraries nesting van claims out-of-the-box ondersteunen.
De claims dienstaanbieder/dienstafnemer heb ik voor dit voorbeeld toegevoegd, maar ik ben wel voorstander om in de claim duidelijk te maken waar die claim voor staat.

Mijn voorstel is dus om het standaard deel van het JWT token ook echt standaard te houden voor standaardisatie over de verschillende standaarden heen en de extra claims zo eenvoudig maar wel expliciet genoeg op te nemen.

Met opmerkingen [KR3R2]: Hoi Rene Rutte. Het gaat hier om het access token dat je krijgt van de auth server. In de issuer moet dan toch gewoon de auth server zelf opgenomen zijn? In het private key JWT op het request snap ik het wel maar daar gaat dit voorbeeld niet over. Verder wel eens met je opmerking