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
Robert.kars@duo.nl

Datum
23-03-2026

Bijlagen
nvt

Betreft: Aanvulling op OAuth2.0

Versie 0.4

Inhoudsopgave

1 Inleiding

Vanuit de werkgroep Edukoppeling wordt gewerkt aan een nieuw profiel gebruikmakende van OAuth2.0. Er is al een basis OAuth2.0 profiel gemaakt, maar dat moet nog aangevuld worden met optionele toevoegingen zodat het ook bruikbaar wordt voor aanvullende validaties.

In dit document wordt een voorstel toegelicht voor optionele toevoegingen op het OAuth profiel voor de ondersteuning van mandaatcontroles.

2 Uitgangspunten

Dit document is geschreven vanuit het scenario waarbij gegevensuitwisseling plaatsvindt van systeem-A (client) naar systeem-B (server). Optioneel kan dit onder het mandaat van een onderwijsinstelling plaatsvinden. Het valideren van een mandaat is geen onderdeel van het OAuth profiel, maar het profiel moet daar wel optioneel bruikbaar voor zijn.

2.1 De basis

- Deze aanvulling gaat uit van het actuele Edukoppeling oauth profiel. De lezer wordt geacht dit profiel te kennen; zonder die kennis is dit document mogelijk moeilijk te begrijpen

2.2 Actoren en systemen

In dit document worden de volgende aanvullende actoren onderkend:

- Onderwijsinstelling of ander rechtspersoon welke verwerkingsverantwoordelijke en bevoegdheidhouder is;

NB. De gegevensuitwisseling wordt in dit document in één richting uitgewerkt, maar een systeem kan de rol van client en server tegelijk invullen voor een gegevensuitwisseling in twee richtingen.

2.3 Mandaatregister

Binnen de werkgroep is besloten het centrale mandatenregister (OSR) optioneel te maken. Partijnen mogen het inzetten maar het is niet verplicht. Deze aanvulling moet dan ook in beide situaties inzetbaar zijn.

Hoe een mandaatregister geïmplementeerd wordt, is dus buiten de scope van dit document.

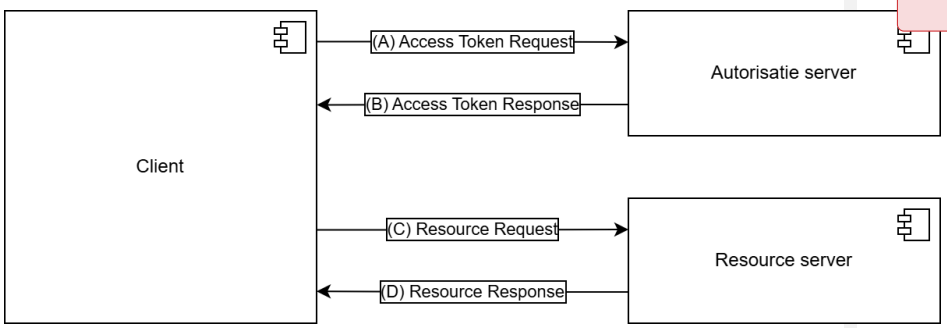
3 OAuth2.0 profiel toevoegingen

Met opmerkingen [DG1]: Mijn indruk is dat dergelijke JWT-claims wel binnen de standaard vallen, echter dat het niet heel gebruikelijk is om binnen een token-request aanvullende claims te leveren en die te valideren. De ondersteuning vanuit open source pakketten voor autorisatieservers vereist al snel custom implementatie.

Ik ben benieuwd of andere deze indruk ook delen.

Zoals aangegeven wordt de client credential flow gebruikt zoals beschreven in de actuele Edukoppeling specificatie. Om relaties met formele partij <<**term even overnemen van Edukoppeling, bedoeld wordt, school, instelling etc>>** aan te kunnen geven worden de volgende claims toegevoegd

3.1 Client Credentials Flow



De vier flows worden hieronder in meer detail beschreven.

3.1.1 (A) Access Token Request

Een client vraagt een access-token aan bij de autorisatie-server. Hierbij worden optioneel de volgende claims aan de private key JWT toegevoegd:

Met opmerkingen [DG2]: Beschouwen we dit als private of public claims conform de JWT RFC?

Claim	Naam	Oorsprong	Verplichting	Voorbeeld	Toelichting
act (sub (string))	Actor	Custom claim	WANT	"0000000700038SS00000"	Een unieke identificatie van het subject namens wie dit verzoek wordt gestuurd. Invulling: OIN. *NB. Vergelijkbaar met EDU-FROM*
Pdi (sub (string))	Publisher Delegator Id	Custom claim	WANT	"0000000700038SS00000"	Een unieke identificatie van het subject voor wie het bericht bedoeld is Invulling: OIN. *NB. Vergelijkbaar met EDU-TO*

De JWT-payload zou er als onderstaand uit kunnen zien.

```
{
  "iss": "https://m2m.mbo-sis.nl/oauth2/token",
  "sub": "00000003743434240000",
  "aud": "https://m2m.facet.onl/oauth2/token",
  "jti": "a3a2fc6e-29e3-4b4d-9284-615982c213c4",
  "iat": "1516238941",
  "exp": "1516239022",
  "act": {
    "sub": "00000007000038SS00000"
  },
  "pdi": {
    "sub": "00000007000038SS00000"
  }
}
```

3.1.2 (B) Access Token Response

Als de AS de controle met succes heeft uitgevoerd – en de mandaat- danwel autorisatiecontrole met positief resultaat heeft uitgevoerd, dan stuurt de autorisatie-server een access-token terug naar de client. Daarin worden de optionele custom claims uit bovenstaand voorbeeld onveranderd in het access token overgenomen. Daarmee geeft de AS aan dat de relatie akkoord bevonden is.

3.1.3 (C) Resource Request

Het access-token wordt, inclusief de optionele claims meegenomen bij het request naar de resource server. Deze kan, en moet, de claims valideren en op basis daarvan de juiste gegevens retourneren.

3.1.4 (D) Resource Response

De resource-server stuurt de gevraagde resource terug naar de client middels een standaard response. Hierbij wordt geen JWT gebruikt