

## Agenda Edustandaard werkgroep Edukoppeling

Leden: Edwin Verwoerd (Edu-V), Robert Kars (DUO), Maarten Kok (SBB), Patrick van der Veer (SURF, OEAPI), Brian Domnisse (Kennisnet, voorzitter), Erwin Reinhoud (Kennisnet, BES), Dennis Grootendorst (Studielink, Npuls), René Rutte (Paragin, OKE), Tom Kirchjunger (Topicus, VDOD), Peter Leijnse (SURF, Npuls)

Agendalid: Joël de Bruin (MBO Digitaal), Noor Ferket (VDOD), HP Köhler (Edu-V), Kees van Ginkel (Topicus, OKE)

### Datum en locatie

20 mei 2026, 10:00-13:00

Locatie: Bar Beton, Kiosk, Perron 4/5, Amersfoort CS

Agenda en stukken staan op:

1. Opening / mededelingen / Verslag van 30 maart 2026
2. Bespreken wijzigingsvoorstel OAuth profiel (DUO) - Referentie onderwijsorganisatie (edu-to en edu-from) (edu-to en edu-from)
3. Bespreken nieuwe versie OAuth – Voorschrift rond private\_key\_jwt
4. Vaststellen CloudEvents profiel
5. Bespreken conceptversie Edukoppeling Architectuur (werkdokument)
6. Wvttk

### 1. Opening / mededelingen / verslag

Actiepunt #134

Er is nog eens met beheer IBP werkgroep gesproken en we hebben een tekstvoorstel in de Edukoppeling Architectuur opgenomen (zie Testbeleid).

Verslag van 30 maart 2026

Verslag is te vinden op teams: [2026-03-30 Verslag- Edustandaard Werkgroep Edukoppeling.docx](#)

### 2. Bespreken wijzigingsvoorstel OAuth profiel (DUO) – Referentie onderwijsorganisatie (edu-to en edu-from)

Er is een OAuth-profiel ([2026-05-05 Edukoppeling - OAuth client credentials profiel voor RESTful APIs.docx](#)) opgesteld op basis van het eerder besproken werkdokument. Er moet nog een optie voor mandaat/delegatie<sup>1</sup> gegevens worden toegevoegd mee te geven in de JWT voor clientauthenticatie en/of het Access Token. DUO heeft vorige keer kort voor de bijeenkomst een concept met de leden van de werkgroep gedeeld. Tijdens het overleg zijn er verschillende opmerkingen gemaakt waarna besloten wordt dat er een nieuw wijzigingsvoorstel wordt ingediend op welke punten DUO het huidige Edukoppeling OAuth-profiel wil aanvullen of wijzigen. Dit nieuwe voorstel ([Wijzigingsvoorstel OAuth2.0 \(0.1\).docx](#)) willen we graag met de leden bespreken zodat we op korte termijn het profiel kunnen aanpassen en als concept publiceren.

---

<sup>1</sup> Edu-to en edu-from, zie [Wijzigingsvoorstel OAuth2.0 \(0.1\).docx](#)

# edustandaard

## 3. Bespreken nieuwe versie OAuth – Voorschrift rond private\_key\_jwt

Het OAuth profiel is op een aantal punten aangepast. De belangrijkste betreffen voorschriften rond de JWT<sup>2</sup> (private\_key\_jwt) bij clientauthenticatie.

- MUST: Bij registratie en verloop of wijziging van het certificaat, deelt de API-afnemer een JWK met de API-aanbieder.
- MAY: Een client kan in de JWT de jwk opnemen zolang sleutel informatie al bij API-aanbieder is geregistreerd
- SHOULD: Als er meerdere sleutels in de JWK zitten dan moet in de JWT de kid parameter meegegeven worden.
- MUST: JWT-header moet een iss-claim bevatten (clientid van client die het token creëert)
- MUST: JWT-header moet een sub-claim bevatten (clientid van client die het token creëert)
- MUST: JWT-header moet een iat-claim bevatten met de tijd waarop het token was gecreëerd
- MUST: JWT-header moet een exp-claim bevatten, na deze tijd mag het token niet geaccepteerd worden door de AS
- MUST: JWT-header moet een jti-claim bevatten en is uniek per request naar het token endpoint.
- MUST: JWT-header moet een aud-claim bevatten met de waarde van de 'issuer identifier'<sup>3</sup> (de identifier van de Authorization Server<sup>4</sup>).

## 4. Vaststellen CloudEvents profiel

Er is door Dennis op basis van het eerder besproken werkdocument (Asynchrone communicatie via RESTful API) een Edukoppeling CloudEvents profiel ([2026-05-20 Edukoppeling - CloudEvents profiel \(asynchrone communicatie via RESTful APIs\).docx](#)) opgesteld. De eerdere opmerkingen van de leden zijn hierin verwerkt. We streven ernaar om dit profiel samen met het OAuth-profiel op korte termijn te kunnen publiceren. We vragen jullie om de wijzigingen door te nemen en de commentaren. Lees met name de voorschriften in hoofdstuk 4 en hoofdstuk 8.4.

## 5. Bespreken conceptversie Edukoppeling Architectuur (werkdocument)

Er is een eerste versie van een architectuur werkdocument opgesteld (zie [2026-05-20 Edukoppeling - Architectuur 3.0 \(concept\).docx](#)). Dit is echt nog een conceptversie. We zijn nieuwsgierig of dit een beetje in de juiste richting is. We vragen ons af of het de juiste onderdelen bevat, wat ontbreekt, wat is onvolledig, wat moet weg. We streven ernaar om voor het najaar een nieuw architectuurdocument te kunnen publiceren.

In de architectuur is een paragraaf rond testbeleid opgenomen (actiepunt #134). Dit leek, na overleg met de voorzitter van de IBP werkgroep toch even de meest efficiënte route om wat gewenst wordt meer concreet te maken. Testbeleid kan heel breed zijn en zeker met

---

<sup>2</sup> Zie ook verslag van 30 maart 2026

<sup>3</sup> OpenID Foundation adviseert om bij private\_key\_jwt de issuer identifier (AS Metadata spec RFC8414) als aud te gebruiken als mitigatie tegen misbruik. Zie [2025-01-22-private\\_key\\_jwt-aud-issues.pptx](#) en [draft-ietf-oauth-rfc7523bis-06 - Updates to OAuth 2.0 JSON Web Token \(JWT\) Client Authentication and Assertion-Based Authorization Grants](#). Zie besluit [2026-03-30 Verslag- Edustandaard Werkgroep Edukoppeling.docx](#)

<sup>4</sup> Bijvoorbeeld de URL van het token endpoint

# edustandaard

voorschriften voor verschillende omgevingen. Zowel de Edukoppeling werkgroep als die van IBP heeft maar een beperkte scope. Als onderdeel van de architectuur bespreken we graag nog even of we met deze eerste aanzet rond een testbeleid op de goede weg zijn of niet.

## 6. Wvttk