

**Edukoppeling**

Identificatie en authenticatie

(concept)

Edustandaard

21 december 2016

**Inhoudsopgave**

[1. Inleiding 3](#_Toc470073346)

[1.1. Doel en doelgroep van dit document 3](#_Toc470073347)

[2. Overzicht SAAS-model 4](#_Toc470073348)

[3 Identificatie van de eindpartij 5](#_Toc470073349)

[3.1 Header vs body 5](#_Toc470073350)

[3.2 Externe vs interne bus 6](#_Toc470073351)

[3.3 Register Instellingen en Opleidingen (RIO) 7](#_Toc470073352)

[3.4 Juridische entiteit 8](#_Toc470073353)

[3.5 Organisatie Identificerend Nummer (OIN) 9](#_Toc470073354)

# Inleiding

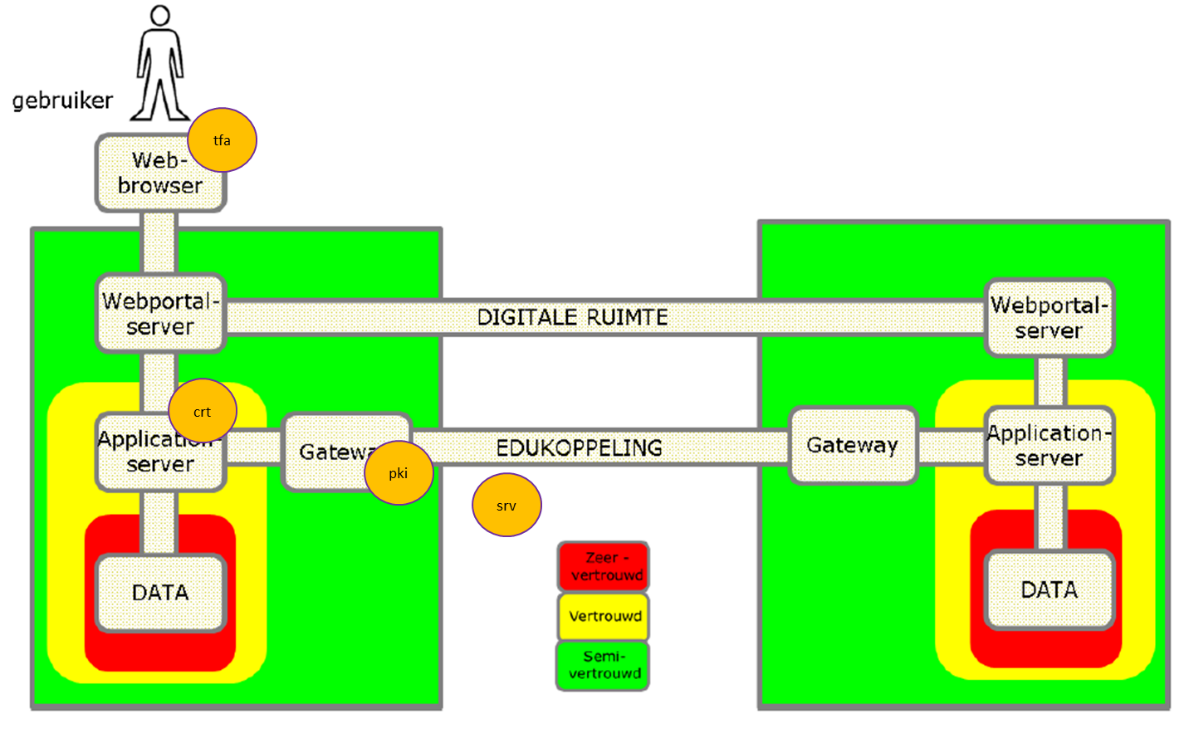
Deze notitie is het resultaat van de actiepunt 43 van de werkgroep Edukoppeling over het verduidelijken van het toepassen van het Organisatie Identificerende Nummer (OIN) nu en in het nieuwe RIO model. Mogelijk wordt dit in een volgende versie uitgebreid tot een notitie voor een nadere toelichting op het SAAS-model dat (actiepunt 49).

## Doel en doelgroep van dit document

Dit document heeft als doel ondersteuning te bieden bij Edukoppeling implementaties en is bedoeld voor medewerkers die bij de (technische) implementatie van Edukoppeling betrokken zijn. Het gaat hierom werknemers (ontwikkelaars, architecten, projectmanagers, informatiemanagers etc.) werkzaam bij onderwijsgerelateerde organisaties. De lezer van dit document willen wij vragen om zaken die ontbreken of onduidelijk zijn te melden bij de beheerder van Edukoppeling (<https://www.edustandaard.nl/standaarden/afspraken/afspraak/edukoppeling/1.2/>).

# 2. Overzicht SAAS-model

In figuur 1 is schematisch een beeld geschetst van ketensamenwerking. De school is vertegenwoordig in deze figuur als de organisatie die mensen in dienst heeft (de gebruiker) die de onderwijskundige of administratieve processen uitvoeren. Door de samenwerking worden zij ondersteund in hun handelen. De organisatie kan zelf zijn dataverzameling, zijn applicaties en servers inrichten, maar vaker zien we dat als een clouddienst wordt afgenomen.



In de Edukoppeling architectuur zijn de elementen beschreven waaruit deze samenwerking bestaat. Een korte samenvatting:

* In de front-office logt de medewerker van de eindorganisatie in met een federatieve sleutel (two factor authenticatie of tfa). De authenticatiefederatie is een onafhankelijke partij die ook de delegatierelatie tussen medewerker en school kan valideren;
* Het certificeringsschema (crt) is een set van normen opgesteld om de veiligheid van de klantomgeving in de cloud te garanderen;
* In de backoffice worden gegevens uitgewisseld. Vaak gebeurt dat in opdracht van de eindpartij door een applicatieve bewerker in de cloud (SAAS). Dit is de partij die de uitwisseling feitelijk uitvoert. We onderscheidende volgende communicatiefuncties bij de servicerequester en bij de serviceprovider:
  + Requester: Het serviceregister (srv) bevat ‘adresseringsinformatie’ voor de requester. Door de eindorganisatie is vastgelegd, door een medewerker met tfa, waar een bepaalde service kan worden aangeroepen.
  + Provider: Een PKI-certificaat van de requester wordt gebruikt om de identiteit met zekerheid vast stellen. Het serviceregister (srv) bevat ‘machtigingsinformatie’ die door de serviceprovider kan worden gecontroleerd.

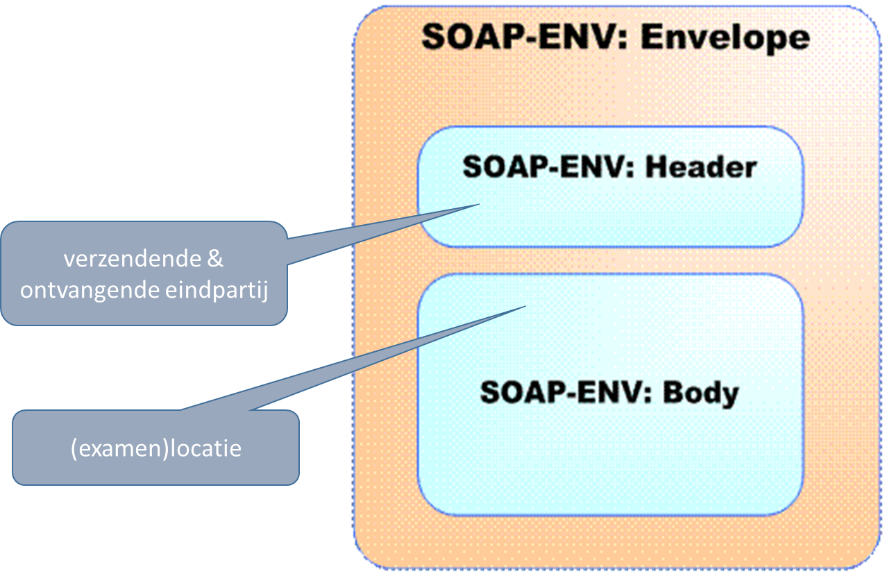
In de volgende paragraaf wordt ingegaan op de identificatie van de eindpartij met een OIN op basis waarvan de cloud-leverancier kan routeren achter de voordeur.

# Identificatie van de eindpartij

De eindpartij is de juridische entiteit of een onderdeel daarvan die uitwisselt in kader van dienstverlening of een wettelijke taak. In dit hoofdstuk wordt behandeld hoe binnen Edukoppeling per bericht eenduidig kan worden vastgesteld wie beide eindpartijen, de verzender en de ontvanger, zijn.

## 3.1 Header vs body

Edukoppeling is gebaseerd op SOAP. Een bericht bestaat uit daarin uit 2 onderdelen, een header en een body.



|  |
| --- |
| Principe 1. Functie en logistiek zijn gescheiden in respectievelijk body en header.  (of anders gezegd: Edukoppeling heeft geen boodschap aan de boodschap) |

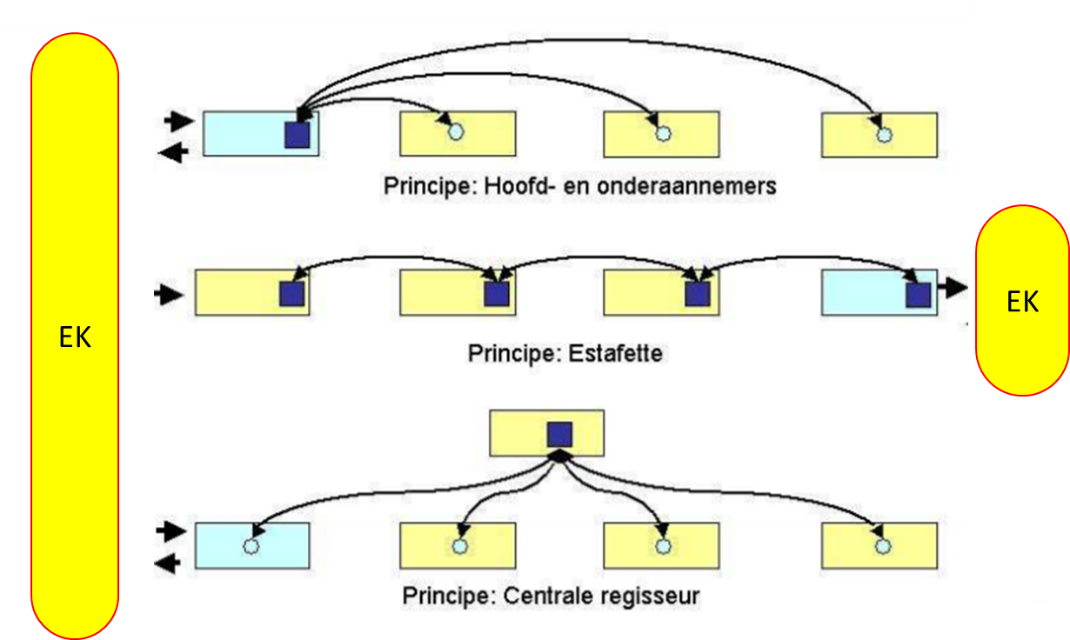
De header wordt gebruikt voor de logistiek. Met de verzender en ontvanger wordt aangeduid voor wie de inhoud in de body afkomstig is of is bedoeld. Als de eindpartij een SAAS-leverancier heeft ingeschakeld wordt deze informatie gebruikt om de body te verwerken in de correcte klantomgeving/tenant.

Als het functioneel is om iets over de organisatie te vermelden, iets wat de verwerkende applicatie moet weten, dan gebeurt dat in de body van het bericht. Bijvoorbeeld in BRON-PO/VO worden leerlingen ingeschreven per erkende vestiging; in Facet worden kandidaten aangemeld per examenlocatie. In sommige gevallen kan zo’n functionele indeling van leerlingen samen vallen met de verzender/ontvanger van het bericht, maar dat hoeft niet.

De examenlocaties in dit voorbeeld zijn specifiek binnen Facet gebruikte examenlocaties. Vanuit Edukoppeling perspectief kan dat zowel specifiek blijven als onderwerp van standaardisatie bijvoorbeeld binnen RIO. Maar dit staat los van de Edukoppeling afspraken.

## 3.2 Externe vs interne bus

Edukoppeling volgt het principe van een servicebus-topologie. Op een servicebus kunnen twee aangesloten partijen zonder tussenkomst van een derde met elkaar uitwisselen. Zoals figuur xxx laat zien richten zij of een leverancier daarvoor een gateway of poort is die de communicatiefuncties uitvoert. De feitelijk aanroep of beantwoording van een service wordt afgehandeld door een applicatie. In de figuur is er één getekend, maar in de praktijk komt het voor dat de serviceverlening niet door één maar door meerdere applicaties wordt afgehandeld. Er is dan een vorm van ketenbesturing nodig en die kan per organisatie anders zijn. De volgende figuur schetst drie mogelijk vormen.



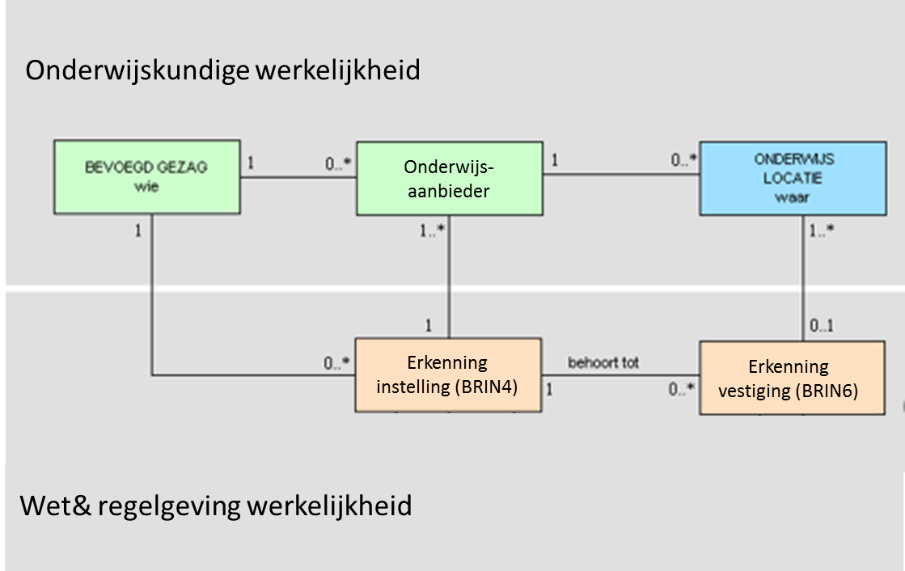
|  |
| --- |
| Principe 2. Edukoppeling volgt het subsidiariteitsbeginsel.  (Anders gezegd: Edukoppeling bemoeit zich niet met interne ketenbesturing) |

Het Traffic Centre (TC) van het Overstap Dossier Onderwijs (OSO) ondersteunt wel (van buiten) de interne ketenbesturing omdat de gevraagde informatie niet op één plek binnen de organisatie ligt. Binnen OSO kunnen verschillende applicaties werkend voor dezelfde BRIN4 een eigen volgnummer krijgen. Deze kunnen apart door het TC worden aangestuurd in de body van het OSO-bericht.

Let op het formaat voor de identiteit van applicatie dat OSO gebruikt lijkt op de structuur die DUO gebruikt voor erkende vestigingen (BRIN6), maar dat is het niet.

## 3.3 Register Instellingen en Opleidingen (RIO)

In het project Doorontwikkelen BRON wordt gewerkt aan een gemeenschappelijk dataverzameling met een onderwijskundige en een formeel wettelijke werkelijkheid. De BRIN 4 en BRIN6 die DUO gebruikt worden niet vervangen, maar verdwijnen naar de achtergrond. Voor of van wie (groen in de volgende figuur) de data bestemd of afkomstig is wordt in RIO door de instelling zelf gedefinieerd als een onderwijsaanbieder (concept term).



|  |
| --- |
| Principe 3. Edukoppeling gebruikt de onderwijskundige wie-identiteit van RIO.  (Anders gezegd: Zijn er meer administraties/tenants per onderwijsaanbieders gewenst, dan wordt geregeld door een eigen ‘postkamer’. |

Dus op Edukoppeling gebruiken we de op het internet, op straat en in de klas herkenbare eenheid. Onderwijsaanbieder zijn alleen nog niet beschikbaar. Een prognose voor de beschikbaarheid van deze organisatorische eenheden:

MBO: 2017

VO: 2018

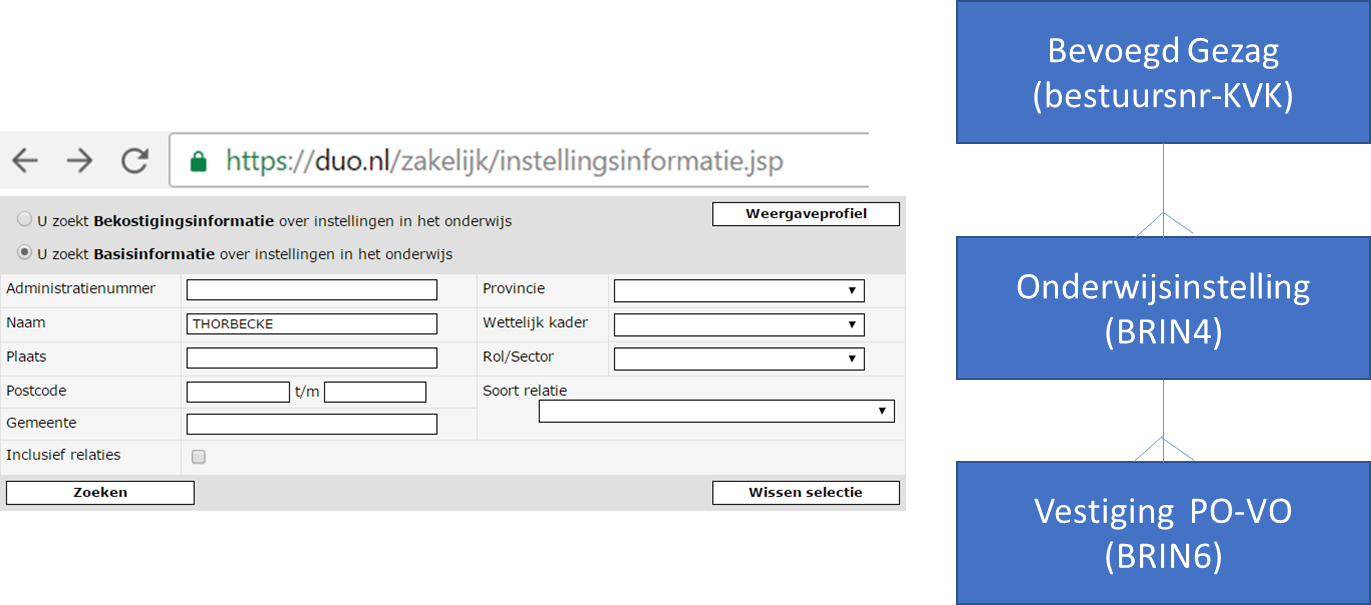
PO: 2019

Dit betekent dat DUO in de uitwisseling met scholen voorlopig blijft werken met de bekende BRIN4 en BRIN6. Zie paragraaf 3.4.

## 3.4 Juridische entiteit

Een rechtspersoon is de formele drager van rechten en plichten. Om een goede werking van het economische verkeer te borgen zijn zulke rechtspersonen geregistreerd in het NHR (voorheen KVK). Aangezien rechten en plichten kunnen worden overgedragen door een gegevensuitwisseling is het gewenst dat de zender en ontvanger van een bericht kunnen worden herleid tot deze juridische entiteit in het NHR

Met een BRIN4 of een BRIN6 is dat mogelijk. Bij de formele erkenning van die entiteiten door DUO is de formele status van het bestuur gecontroleerd aan de hand van een digitale uitwisseling tussen BRIN en NHR.[[1]](#footnote-1). Het bestuur of het bevoegd gezag van een onderwijsinstelling of een vestiging kan worden opgevraagd aan de hand van de volgende webtransactie.[[2]](#footnote-2)



## 3.5 Organisatie Identificerend Nummer (OIN)

In Edukoppeling (en Digikoppeling) worden organisaties geïdentificeerd met een OIN met een basis in een overheidsregister. Voor een bedrijf, rechtspersoon (ook bevoegd gezag) of uitvoeringsorganisatie geldt de OIN systematiek die door Digikoppeling wordt voorgeschreven voor PKI-overheidscertificaten. In de meeste gevallen zijn deze OIN’s gebaseerd op het NHR. Zie <https://www.logius.nl/fileadmin/logius/product/digikoppeling/algemeen/Digikoppeling_Identificatie_en_Authenticatie_v1.1.pdf>

Voor onderwijsinstellingen wordt doorgaans het BRIN-register van DUO gebruikt. Zoals in paragraaf 3.3 aangegeven ligt het voor de hand om de wie-component van het RIO-register te gebruiken, maar aangezien dat er nog niet is, wordt de BRIN-werkwijze voorlopig gecontinueerd. Met de Digikoppeling gemeenschap zijn afspraken gemaakt hoe BRIN4 en BRIN6 te vertalen naar een OIN. Hieronder is uitgewerkt hoe dat uitpakt voor een paar bekende DUO-uitwisselingen.

*BRON PO/VO*

In PO en VO zijn de verzender en ontvanger van berichten gelijk aan de erkende vestiging (BRIN6) waar ook de leerlingen formeel volgens de WOT zijn ingeschreven in de body van het bericht. De impliciete aanname is dat leerlingen per erkende vestiging in een administratief systeem (of tenant) worden beheerd.



Het is bekend dat leerlingen soms in werkelijkheid op een disclocatie of inspectielocatie les krijgen. Functioneel en logistiek speelt dat geen rol.

*BRON MBO*

Bij BRON-MBO dat nu op het punt staat om gemoderniseerd te zijn de er erkende instellingen (BRIN4) de ontvanger/verzender van gegevens. Leerlingen worden conform de WOT op dit niveau ingeschreven in de body van het bericht. Daarnaast maken enkele instellingen gebruik van een extra aanleverpunt om gegevens te verzenden.



Voor pushberichten vanuit DUO werkt dat niet. DUO weet op leerlingniveau niet het juiste aanleverpunt te bepalen. Om die reden is afgesproken dat DUO de berichten naar alle bekende aanleverpunten stuurt (multicasten). Het juiste aanleverpunt pikt dat op en de foute negeert het bericht.

*FACET*

Facet is ontworpen naar de collectieve afspraak in het MBO gemaakt bij DAMBO (Digitaal aanmelden MBO) dat push-berichten vanuit DUO worden gestuurd naar de MBO-instelling (BRIN4). In de werkgroep Edukoppeling van 14-12-2016 bleek dat de oplossing van multicasten uit BRON-MBO nog niet nodig is. Maar niet uitgesloten kan worden dat dat verandert als een instelling waar dat betrekking op heeft een Facet-module aanschaft.



Facet wordt inmiddels ook voor VO en PO ingezet. Daarbij geldt ook dat berichten worden gepusht naar instellingsniveau (BRIN4). Facet haalt die routeringsinformatie uit de aanlevering van kandidaten per instelling. BRON haalt de routeringsinformatie uit de aanlevering van leerlingen per vestiging. De discrepantie met BRON-PO/VO is besproken in de werkgroep Edukoppeling van 14-12-2016 vanwege het vermoeden dat het in werkelijkheid om dezelfde administratie gaat. In de werkgroep werd dit echter nog niet als een probleem gezien.

1. In de meeste gevallen is dat een vereniging of stichting in het NHR. In een handvol gevallen bestaat het bestuur van openbaar onderwijs uit een gemeentelijk commissie en valt het onderwijs direct onder B&W. Deze situatie was vroeger gebruikelijk maar houdt op te bestaan. [↑](#footnote-ref-1)
2. Via data.duo.nl en api.duo.nl (beta) kan de relatie tussen instelling en bevoegd gezag voor bulk dan wel machinaal gebruik worden opgevraagd. [↑](#footnote-ref-2)