

**Edukoppeling**

Identificatie en authenticatie

(concept)

Edustandaard

Status: Concept

Datum: 12 september 2017

**Inhoudsopgave**

[1. Inleiding 3](#_Toc492618221)

[1.1. Doel en doelgroep van dit document 3](#_Toc492618222)

[1.2. Leeswijzer 3](#_Toc492618223)

[2. Overzicht SAAS-model 4](#_Toc492618224)

[3 Logistieke identiteit (SOLL) 5](#_Toc492618225)

[3.1 Header vs body 5](#_Toc492618226)

[3.2 Onderwijsaanbieder of rechtspersoon 6](#_Toc492618227)

[3.3 Externe vs interne bus 8](#_Toc492618228)

[4 Gebruik Edukoppeling (IST) 9](#_Toc492618229)

[4.1 Van BRIN naar RIO 9](#_Toc492618230)

[4.2 Logistieke identiteiten per toepassing 10](#_Toc492618231)

# Inleiding

In Edukoppeling standaard is afgesproken dat de identificatie van betrokken partijen (scholen, uitgevers, uitvoeringsorganisaties) wordt opgenomen in de header van het bericht. Deze afspraak is geënt op het veelvuldig gebruik van cloudcomputing voor schoolsystemen zoals een leerling administratiesysteem (LAS). We doelen daarom vooral op de SaaS-variant (Software-as-a-Service). De bedoelde identificatie heeft een tweeledig nut:

* Valideren van de mandateringsrelatie

Nagaan aan de hand van een register of er sprake is van een geldige bewerkersrelatie.

* Subrouteren binnen het domein van een SaaS-leverancier

Leveranciers hanteren per klant/tenant een virtuele omgeving. Die moeten niet door elkaar lopen.

Waar Edukoppeling echter nog geen antwoord op geeft is de vraag hoe dan die identificatie kan worden bepaald. In eerste blik op de praktijk wijst uit dat er meerdere oplossingen zijn ontstaan op basis van het zogenaamde BRIN-nummer en die zijn niet te combineren. Het ontstaan van RIO als opvolger van het BRIN is een goede gelegenheid om een klant/tenant onafhankelijk van de toepassing te definiëren. Deze notitie werkt dat nader uit.

## Doel en doelgroep van dit document

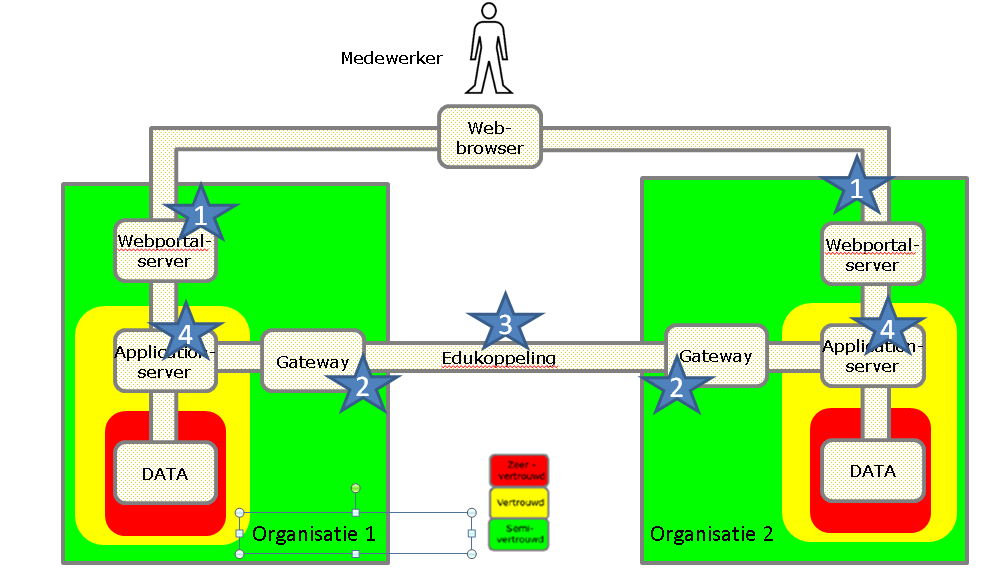
Dit document heeft als doel ondersteuning te bieden bij Edukoppeling implementaties en is bedoeld voor medewerkers die bij de (technische) implementatie van Edukoppeling betrokken zijn. Het gaat hierom werknemers (ontwikkelaars, architecten, projectmanagers, informatiemanagers etc.) werkzaam bij onderwijsgerelateerde 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/>).

## Leeswijzer

# 2. Overzicht SAAS-model

In Figuur 1 is schematisch een beeld geschetst van ketensamenwerking. De school[[1]](#footnote-1) is vertegenwoordigd in deze figuur als de organisatie die mensen in dienst heeft (de medewerker). Deze medewerker heeft bijvoorbeeld toegang tot een leerlingadministratiesysteem in de cloud en tot bekostigingsgerelateerde informatie van DUO.



Figuur 1 - Schematische weergave ketensamenwerking

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

1. In de front-office logt de medewerker van de school bij voorkeur in met een federatieve sleutel met een substantieel beveiligingsniveau (zoals een two-factor middel). De authenticatiefederatie is een vertrouwde derde partij die de *delegatierelatie*[[2]](#footnote-2) tussen medewerker en school kan valideren.
2. In de backoffice worden gegevens uitgewisseld conform de Edukoppeling standaard. De SaaS-leverancier is de partij die de uitwisseling feitelijk uitvoert in opdracht van de eindorganisatie (bijv. een school). De school is wisselend de functionele verzender/ontvanger die wordt vermeld in de Edukoppeling-header. De SaaS-leverancier beveiligt het verkeer (tweezijdig TLS) met een PKI-certificaat met eigen identificatie.
3. In een collectief serviceregister wordt bijgehouden (dat doet een medewerker van de school) of een bewerker is *gemandateerd* [[3]](#footnote-3)voor een bepaalde toepassing. Deze mag dan de bijbehorende services namens de school aanroepen en kan het endpoint bepalen voor de bijbehorende services die de school zelf nodig heeft. Dit endpoint ligt ook vast in het serviceregister en is toegankelijk voor ketenpartners met een juiste rol.
4. Voor de beoordeling van de correcte werking van (cloud)systemen zijn normen beschikbaar. Voor scholen is in het kader van Edukoppeling een certificeringsschema opgezet en overheidsorganisaties moeten voldoen aan de BIR.

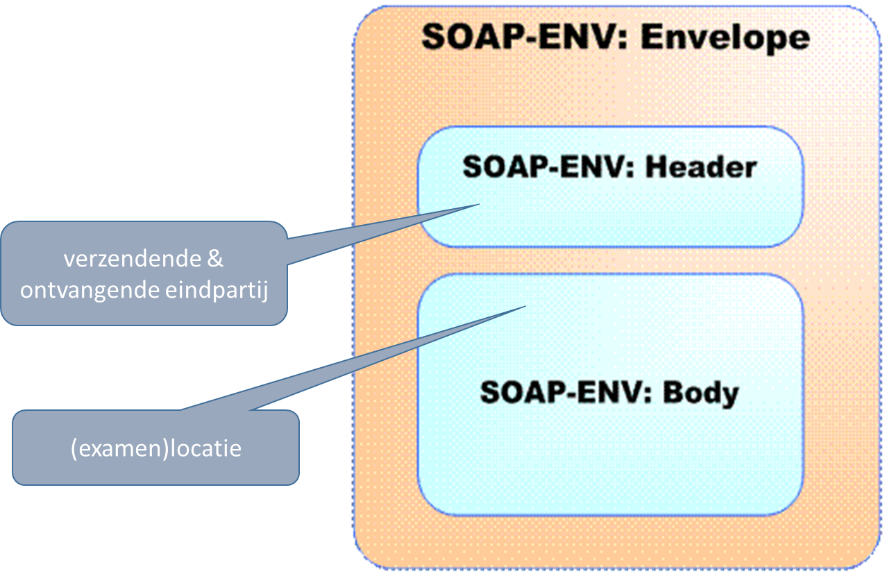
In de volgende paragraaf wordt ingegaan op de identificatie van de eindorganisatie (de functionele verzender/ontvanger). Hierbij wordt voortgeborduurd op de systematiek voor Organisatie Identificerende Nummers (OIN) die is ontwikkeld door Logius voor gebruik bij Digikoppeling.

# Logistieke identiteit (SOLL)

In dit hoofdstuk wordt behandeld hoe logistieke identiteiten binnen Edukoppeling worden bepaald.

## 3.1 Header vs body

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



Figuur 2 - SOAP -onderdelen

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

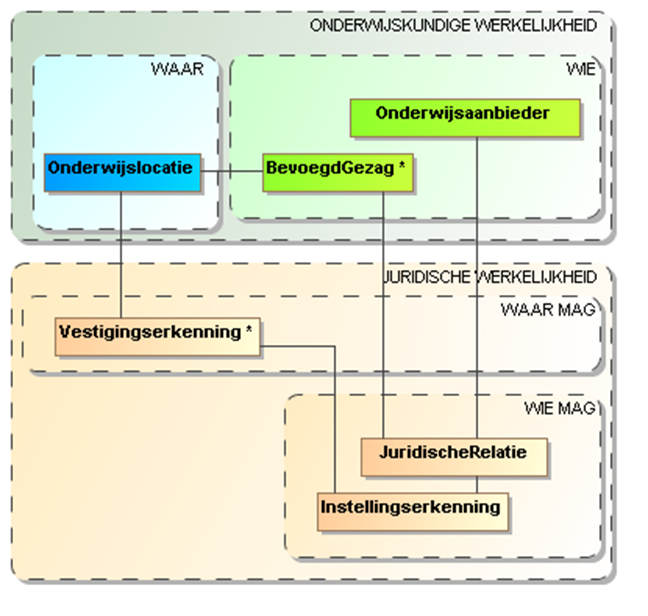
Het zogenaamde Organisatie Identificerende Nummer (OIN) beschrijft binnen de Digikoppeling standaard, waar Edukoppeling op is gebaseerd, de eindpartij. Het is opgenomen in de header van het bericht en heeft een logistieke functie: zorgen dat het bericht (door de postbode) goed wordt afgeleverd en herkenbaar is van wie het afkomstig is.

Functionele aspecten waar de verwerkende applicatie iets mee moet, zitten per definitie in de body van het bericht. Bijvoorbeeld: als je leerlingen wilt kunnen tellen per onderwijsaanbieder (zie RIO), of de onderwijslicentie wilt checken, dan wordt daarover in de body gecommuniceerd

Door deze strikte scheiding kan een ketenpartner “gelaagd” werken: een applicatie werkt met body (payload) en een gateway werkt met de header (adressering). In het geval van DUO bijvoorbeeld wordt het applicatielandschap gelaagd ingericht inclusief beveiligingsmaatregelen per zone.

## 3.2 Onderwijsaanbieder of rechtspersoon

In Doorontwikkelen BRON wordt gewerkt aan RIO. In RIO gaan ”scholen” over hun eigen identiteit en indeling conform de onderwijskundige werkelijkheid. Die is gerelateerd aan de juridische werkelijkheid die we nu al kennen van BRIN. In de SOLL situatie zal de administratieve organisatie zijn gebaseerd op de nieuwe onderwijskundige werkelijkheid.



Figuur 3 - RIO- datamodel (snipper)

Leerlingen schrijven zich in voor een Aangeboden Opleiding en zijn daarmee verbonden aan een Onderwijsaanbieder. Dit vormt de logistieke basis voor uitwisselingen die gaan over individuele leerlingen. Voor de uitwisseling van leerlinggegevens zijn meerdere ketenprocessen via Edukoppeling ingericht en dat zal gaan groeien. Enkele voorbeelden: ECK D&T, OSO, BRON, Verzuim en Facet. Voor alle toepassingen verhouden onderwijsaanbieder en de logistieke identiteit (het OIN) zich tot elkaar, echter voor de aflevering van berichten kunnen er per Onderwijsaanbieder meerdere afleverpunten zijn afhankelijk van het specifieke proces (service).

|  |
| --- |
| Principe 2. Voor elke Onderwijsaanbieder is er exact één OIN en per service kan er per Edukoppeling-toepassing een eigen URL zijn.  (ergo: het OIN is afgeleid van de identiteit van de Onderwijsaanbieder) |

Op basis van dit principe kan voor een bepaalde service een Onderwijsaanbieder niet over Edukoppeling worden opgedeeld. Dit betekent dat een Onderwijsaanbieder per toepassing slechts één tenant/klantomgeving bij een SaaS-leverancier kan afspreken per service. Specifieke oplossingen met een meer fijnmazige routering worden niet ondersteund met Edukoppeling/OIN. Eventueel kunnen deze worden gezocht in serviceregister-functies en de payload in de body.

Overigens is de verwachting dat bevoegd gezagen ook gaan communiceren via Edukoppeling.

|  |
| --- |
| Principe 3. Een Bevoegd Gezag is een Rechtspersoon  (ergo: het OIN van een Bevoegd Gezag kan worden afgeleid van het RSIN uit het NHR) |

Met deze systematiek sluit het onderwijs collectief aan bij de werkwijze die is afgesproken binnen de Nederlandse overheid. De OIN’s van onderwijsgerelateerde organisaties zullen toegankelijk worden gemaakt via het Centrale OIN Register (COR). Ze zijn ook bruikbaar voor toepassingen die niet onderwijs-gerelateerd zijn.

Een rechtspersoon is de formele drager van rechten en plichten. Rechten en plichten kunnen worden overgedragen door een gegevensuitwisseling via Edukoppeling. Om een goede werking van het economische verkeer te borgen zijn zulke rechtspersonen geregistreerd in het Handelsregister (NHR, voorheen KVK).

|  |
| --- |
| Principe 4. De logistieke identiteit (OIN) moet herleid kunnen worden tot het NHR  (Anders gezegd: Ketenpartners moeten het RSIN van verzender/ontvanger kunnen opvragen) |

In veel toepassingen zal de ketenpartner van de school per leerling/student bijhouden wat de logistieke identiteit (OIN) is. Dat is nodig om in latere instantie een retourbericht te kunnen sturen over die leerling/student. Bijvoorbeeld: BRON kan “spontaan” een bericht over het woonadres van een leerling aanleveren. Dit is privacygevoelig.

|  |
| --- |
| Principe 5. De logistieke identiteit (OIN) per leerling/student is niet openbaar  (ergo: het kan nodig zijn dat ketenpartners van scholen dat onthouden) |

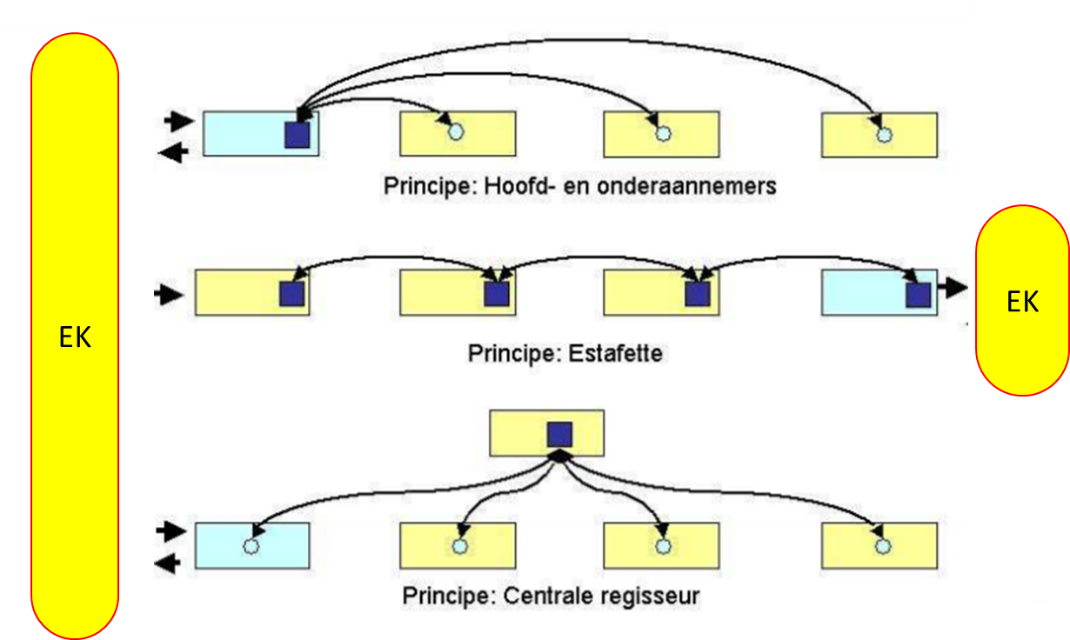
## 3.3 Externe vs interne bus

Edukoppeling volgt het principe van een servicebus-topologie. Op een servicebus kunnen twee aangesloten partijen zonder tussenkomst van een derde met elkaar uitwisselen De feitelijke beantwoording van een service wordt afgehandeld door een applicatie.

|  |
| --- |
| Principe 6. Edukoppeling volgt het subsidiariteitsbeginsel.  (Anders gezegd: Edukoppeling bemoeit zich niet met interne ketenbesturing) |

De gateway getekend in figuur 1 is in wezen een “vertaaldoos” van extern naar intern en vice versa. Deze kijkt naar de afzender, de beoogde ontvanger, om wat voor service het gaat en bepaalt waar het bericht afgehandeld met behulp van het ook in figuur 1 getekende serviceregister. Een bericht afkomstig van binnen gaat naar een organisatie en een bericht afkomstig van buiten gaat naar een afhandelend systeem.

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. De volgende figuur (ontleend aan NORA 2) schetst drie mogelijke vormen.



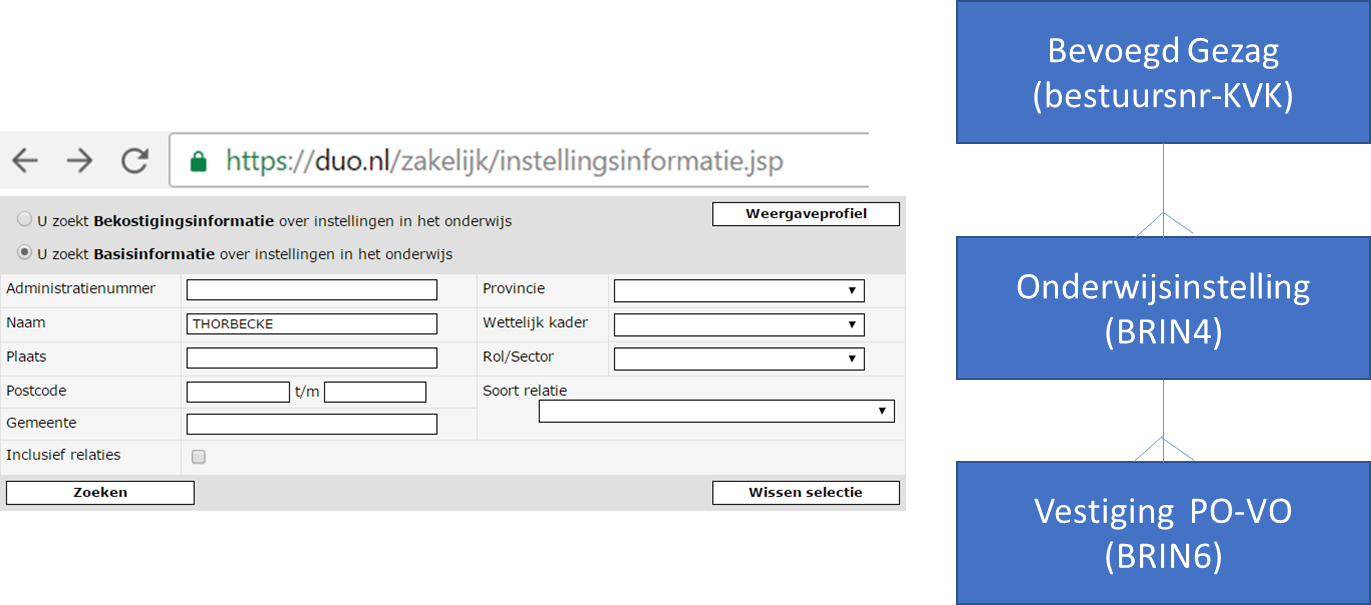
Figuur 4 – Ketenbesturing

Traffic Centre (TC) van het Overstap Dossier Onderwijs (OSO) ondersteunt (als collectieve voorziening van buiten) de interne ketenbesturing. Het OSO Traffic Center is in de basis een register waarin beheerd wordt bij welke loketten bij een onderwijsaanbieder geadresseerd moeten worden om tot een gevuld dossier te komen.

# Gebruik Edukoppeling (IST)

## 4.1 Van BRIN naar RIO

Vrijwel iedereen in het onderwijs is gewend om bestands- en berichtenverkeer voor wat betreft de adressering te baseren op het register BRIN. Dit is het bekostigingsgerelateerde register van DUO dat als download en als webtransactie openbaar wordt gemaakt.



Figuur 5 - Relaties tussen juridische entiteiten

In het RIO-model (zie figuur 3) zijn de onderwijsinstelling en de vestiging omgebogen naar formele instellings- en vestigingserkenning en zijn onderwijsaanbieders en onderwijslocaties zoals gezien door de school toegevoegd. Anno 2017 moeten we het nog doen met BRIN4 en BRIN6, maar ergens in 2018 komen ook onderwijsaanbieders en onderwijslocaties beschikbaar voor het MBO gevolgd in 2019 door het VO en daarna voor de andere sectoren.

## 4.2 Logistieke identiteiten per toepassing

***BRON-PO***

Logistieke identiteiten zijn gebaseerd op BRIN6. Het is een webservice-toepassing van het eerste uur (geen Edukoppeling). De aanzet in 2016 om het SaaS-model en Edukoppeling te gaan toepassen is niet doorgegaan en daarmee is een grootschalige operatie noodzakelijk geworden om de 7000-8000 PKI-certificaten (uitgegeven per vestiging/school) om de gegevensuitwisseling te beschermen, te vervangen. Het uitgifteproces is overigens wel veranderd en verloopt nu via het bestuur en niet meer rechtstreeks via de school/vestiging. Het aantal certificaten zal er niet minder op worden. Deze operatie loopt tot in 2018 en is maximaal tot 2021 houdbaar.

|  |  |  |  |
| --- | --- | --- | --- |
| **Logistieke entiteit** | **Huidig** | | **Onderhanden** |
| **BRIN(6)** | **Pre\_Edukoppeling** |  |
| Hoofdvestiging | 13XY00 | 13XY00 |  |
| Nevenvestiging | 13XY01 | 13XY01 |  |

Het is bekend dat leerlingen op een zogenaamde dislocatie of inspectielocatie les kunnen krijgen. In het huidige BRON wordt dat genegeerd, waardoor leerlinggegevens van die locatie “op één hoop” kunnen komen van de “hoofdlocatie”. In RIO kunnen Inspectielocaties ofwel als Onderwijsaanbieders ofwel als Onderwijslocaties beschouwd. Vooruitlopend op RIO wordt in 2017-18 voor een aantal scholen waarin dit speelt voor de Inspectielocaties nu ook een veld Onderwijslocaties toegevoegd aan de huidige registratie in de LASsen om de verwerking van Eindtoetsresultaten beter te kunnen splitsen over twee locaties van een “school”. BRON gaat dit al ondersteunen, zodat de Inspectie en de school niet later handmatig de resultaten van de leerlingen moeten verdelen over de Onderwijslocaties (ergo de “hoofdlocatie” en de inspectielocatie dus).

***BRON-VO***

Logistieke identiteiten zijn gebaseerd op BRIN6. Het is op dit moment een batchtoepassing. Per vestiging wordt op het ZP een bestand aangeleverd met leerlingen. In het kader van Doorontwikkelen BRON wordt momenteel gewerkt aan een Edukoppeling 1.2 uitwisseling. Dit impliceert een expliciete toepassing van een logistieke identiteit (OIN) gebaseerd op onderwijsaanbieders in RIO. Dit moet per leerling vastgesteld kunnen worden op basis van de gegevens die worden aangeleverd voor de inschrijvingsperiode. De voorbereidingen lopen in 2017 en 2018.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Logistieke entiteit** | **Huidig** | | **Onderhanden** | |
| **BRIN(6)** | **Batch** | **RIO** | **Edukoppeling (OIN)** |
| Hoofdvestiging | 13XY00 | 13XY00 |  |  |
| Nevenvestiging | 13XY01 | 13XY01 |  |  |
| Onderwijsaanbieder |  |  | 123A321 | 0000000700**123A321**000 |

***BRON-MBO***

Logistieke identiteiten zijn gebaseerd op BRIN4. Het is een Edukoppeling (formeel 1.1 maar praktisch 1.2) uitwisseling inclusief OIN, maar dat kon nog niet worden gebaseerd op onderwijsaanbieders in RIO. In plaats daarvan is gekozen om voorlopig met een OIN te werken dat is gebaseerd op BRIN4. In werkelijkheid blijken er per BRIN4 meerdere aanleverpunten voor te komen. Maar aangezien dat niet per leerling vastgesteld kan worden is door DUO bij uitgaand verkeer voorlopig gekozen voor multi-casten. Het juiste aanleverpunt pikt dat op en de foute negeert het bericht. In de loop van 2018 kunnen scholen in RIO hun Onderwijsaanbieders beheren. Zodra die ook in BRON-MBO zijn opgenomen kan het multi-casten worden uitgefaseerd.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Logistieke entiteit** | **Huidig** | | **Onderhanden** | **Wens** |
| **BRIN(4)** | **Edukoppeling (OIN)** | **RIO** | **Edukoppeling (OIN)** |
| MBO-instelling | 13XY | 00000007000**13XY**000**00** |  |  |
| Extra aanleverpunt |  | 00000007000**13XY**000**01** |  |  |
| Onderwijsaanbieder |  |  | **123A321** | 0000000700**123A321**000 |

Actieve vulling van RIO met Onderwijsaanbieders kan het multi-casten oplossen.

***BRON-HO***

De uitwisseling tussen DUO en Studielink is pre-Edukoppeling. Studielink bepaalt de HO-instelling op basis van BRIN4 in de payload. Daarnaast kennen we rechtstreekse uitwisselingen tussen DUO en de HO-instellingen, ook op basis van BRIN4. Het Studielink systeem wordt 2017/2018 vervangen en uitgevoerd door een andere leverancier.

|  |  |  |  |
| --- | --- | --- | --- |
| **Logistieke entiteit** | **Huidig** | | **Onderhanden** |
| **BRIN(4)** | **Pre-Edukoppeling** |  |
| HO-instelling | 13XY | 13XY |  |
|  |  |  |  |

***DAMBO***

Digitaal aanmelden in het MBO heeft een backoffice push bericht dat is gebaseerd op Edukoppeling. De OIN-nummers, gebaseerd op BRIN4, hebben op applicatieniveau een verkeerde prefix (5 uit een conceptversie in plaats van 7). Dit kan alleen worden rechtgetrokken in een gecoördineerde actie.

|  |  |  |  |
| --- | --- | --- | --- |
| **Logistieke entiteit** | **Huidig** |  | **Onderhanden** |
| **BRIN(4)** | **Edukoppeling (OIN)** |  |
| MBO-instelling | 13XY | 0000000**5**000**13XY**000**00** |  |
|  |  |  |  |

***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 multi-casten 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.

|  |  |  |  |
| --- | --- | --- | --- |
| **Logistieke entiteit** | **Huidig** | | **Onderhanden** |
| **BRIN(4)** | **Edukoppeling (OIN)** |  |
| MBO-instelling | 13XY | 00000007000**13XY**000**00** |  |
| POVO-instelling | 13XY | 00000007000**13XY**000**00** |  |
|  |  |  |  |

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.

Facet kent het begrip Facet Afname Speler (FAO) die per examenlocatie worden ingezet. Er kunnen meerdere locaties zijn per BRIN4 en dat hoeft niks te maken te hebben met de bekende onderwijsaanbieders of vestigingen waarvan hierboven sprake is. De school bepaalt zelf een subnummering per BRIN4 en communiceert dat binnen het systeem Facet. Facet gebruikt dat voor technische adressering bij het distribueren van examensopgaven en -antwoorden. Hierbij speelt Edukoppeling geen rol.

***Verzuim***

Verzuim-uitwisselingen kunnen (naast ZP-bestandsaanleveringen) worden uitgevoerd met webservices gebaseerd op Edukoppeling 1.1 met een OIN gebaseerd op BRIN6.

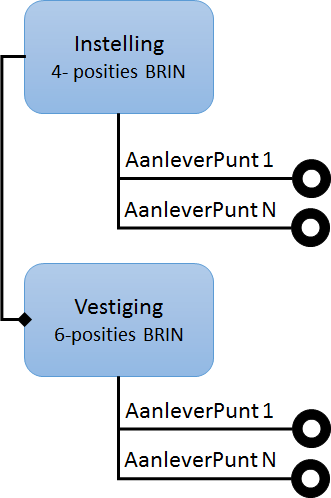
|  |  |  |  |
| --- | --- | --- | --- |
| **Logistieke entiteit** | **Huidig** | | **Onderhanden** |
| **BRIN(6)** | **Edukoppeling (OIN)** |  |
| Hoofdvestiging | 13XY00 | 00000007000**13XY**000**00** |  |
| Nevenvestiging | 13XY01 | 00000007000**13XY**000**01** |  |
|  |  |  |  |

***Het OSO Traffic Center***

Alle systemen/partijen binnen de OSO keten volgen het Edukoppeling SaaS-model:

* De SAAS-leveranciers zijn te identificeren op basis van een OIN op basis van het kvk-nummer. Zij moeten voor de machine-machine uitwisseling een PKI-overheidscertificaat met hierin het OIN gebruiken om voor OSO gegevensuitwisseling geautoriseerd te kunnen worden.
* Een onderwijsinstelling wordt geïdentificeerd met een BRIN(4) en de onderliggende vestigingen met een BRIN(4) gekoppeld aan een OSO volgnummer (‘99’). Onderwijsinstellingen zijn vrij om de OSO volgnummers voor vestigingen te beheren en het kan dus zijn dat deze in aanduiding overeenkomt met het DUO BRIN6. Zowel het formaat als de waarde lijken op het DUO BRIN6 voor erkende vestigingen, maar dat is het dus niet.

Een onderwijsinstelling of vestiging binnen OSO context kan op haar beurt één of meerdere aanleverpunten hebben, deze worden geïdentificeerd met het BRIN(4) van de onderwijsinstelling (niet de vestiging!) aangevuld met een index ‘999’[[4]](#footnote-4). Een aanleverpunt is de combinatie van onderwijsinstelling of vestiging en schoolsysteem (LAS of Regionaal Platform). E.e.a. wordt schematisch weergegeven in Figuur 5.



Figuur 5 – OSO aanleverpunten

De adressering van berichten binnen OSO vindt plaats op Aanleverpunt niveau. Ieder bericht heeft een bron- en doel- Aanleverpunt. Op het moment dat een aangesloten systeem contact maakt met het Traffic Center, wordt er op basis van het OIN gecontroleerd of leveranciers in de keten gegevens mag uitwisselen voor een bepaalde vestiging en welk aanleverpunt hiervoor geregistreerd is. Het Traffic Center levert partijen het webservice endpoint met het aanleverpunt. Het endpoint wordt gebruikt voor communicatie naar de betreffende SaaS-leverancier, het aanleverpunt wordt opgenomen in de payload van het bericht voor verdere routering binnen SaaS.

Bij het toepassen van de Edukoppeling adressering binnen OSO zou de huidige adressering gehandhaafd kunnen worden. Ook zou overwogen kunnen worden om het aanleverpunt op te nemen in de WS-Addressing header. Bij ontvangst van een bericht kijkt het ontvangende systeem naar welk aanleverpunt en daarmee welke onderwijsinstelling/vestiging het bericht intern (binnen het systeem) gerouteerd moet worden.

1. Het begrip school wordt in dit gedeelte ‘slordig’ als een overkoepelend begrip gebruikt. [↑](#footnote-ref-1)
2. Delegatie: relatie op basis van een arbeidsopdracht ; meestal gericht op een natuurlijk persoon. [↑](#footnote-ref-2)
3. Mandatering: Relatie op basis van dienstverlening; meestal gericht op een rechtspersoon. [↑](#footnote-ref-3)
4. Deze indeling is historisch gegroeid en in een eerdere situatie kende een onderwijsinstelling meerdere vestigingen maar waren aanleverpunten altijd gekoppeld aan de onderwijsinstelling en soms aan vestigingen. Dit verklaart de twee ‘onafhankelijke’ identificaties van vestiging en aanleverpunt. [↑](#footnote-ref-4)