Aanmeldformulier voor in beheer name van “Certificeringsschema Edukoppeling”

Opgesteld door: Frank van Vonderen (Verdonk, Klooster en Associates) en Tonny Plas (Kennisnet) namens SION
Voor: Standaardisatieraad, Edustandaard
Datum: 8 september 2014

1. Toelichting op toepassing van dit aanmeldformulier

Op basis van de antwoorden op de vragen van deze vragenlijst wordt bepaald of de afspraak voldoet aan de gestelde criteria. Het is in eerste instantie de verantwoordelijkheid van de aanmelder om dit aan te tonen. Edustandaard gebruikt de documentatie en gegevens uit de antwoorden om per criterium een oordeel te geven. Bij twijfel over de relevantie, het werkingsgebied of kwaliteit kan het Bureau Edustandaard besluiten een gesprek te voeren met de aanmelder. Voor het schrijven van het oordeel zal Bureau Edustandaard een werkgroep toewijzen dan wel oprichten. Met behulp van het template in bijlage 3 zal deze werkgroep een advies op stellen voor de Standaardisatieraad van Edustandaard.

Doelgroepen van deze vragenlijst:

- ***Bureau Edustandaard (BES):*** beoordeelt op basis van deze vragenlijst of aan alle criteria voor nieuwe standaarden is voldaan (zie bijlage 2). BES adviseert hierin de Standaardisatieraad.
- Op basis van de vragenlijst en het advies van Bureau Edustandaard zal de ***Standaardisatieraad*** besluiten om de standaard al dan niet in beheer te nemen.
- ***Architectuurraad***: bewaakt en beoordeelt de samenhang met de andere afspraken (architectuur) van Edustandaard

2. Vragenlijst

1. Om welke afspraak gaat het?

1.1. Wat is de naam en laatste wijzigingsdatum van de afspraak?

Naam	datum
Certificeringsschema Edukoppeling v1.1	28 juli 2014

1.2. Geef een overzicht van de bijbehorende documentatie, online en offline.

titel en/of URL	auteur(s)	versie
Certificeringsschema Edukoppeling	SION	1.1

2. Beschrijf de afspraak:

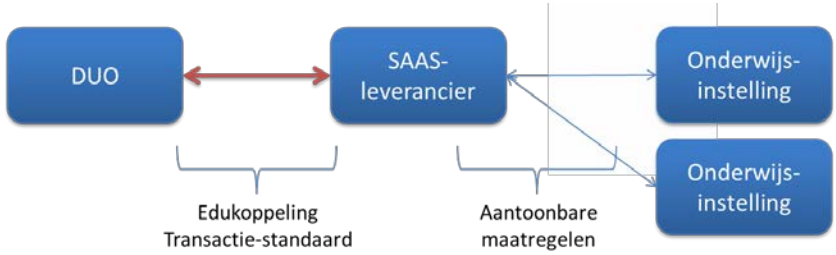
2.1. Waar gaat de afspraak over?

antwoord	verwijzing
Dit betreft een standaard voor audit en assurance op basis waarvan persoonsgegevens end-to-end veilig uitgewisseld kunnen worden, met name bij tussenkomst van een leverancier van clouddiensten.	Zie Bijlage “Certificeringsschema Edukoppeling 1.1”

2.2. Wat is de aanleiding geweest voor de afspraak? (Bijv. wettelijke kaders, een projectdoelstelling of vanuit een bedrijfs- of ketenmissie.)

Antwoord	verwijzing
Vanuit het project Referentie Architectuur Onderwijs (RAO) is in 2013 met ketenpartijen (DUO, leveranciers) gezocht naar een duurzame en standaardoplossing voor gegevensuitwisseling met cloudleveranciers die voldoet aan de benodigde beveiligingsnormen. Daarmee werd ook ingespeeld op een op handen zijnde Europese privacy verordening waarmee een ketenverantwoordelijkheid geïntroduceerd wordt voor alle schakels in een informatieketen.	http://www.sionderwijs.nl/projecten/ref-arch-onderwijs/ http://www.eerstekamer.nl/eu/edossier/e120003_voorstel_voor_een#p1

2.3. Wat is het werkingsgebied en/of functioneel domein van deze afspraak? (Bijv. sectoren, organisaties, administratieve domein, onderzoek, leermiddelendomein.)

Antwoord	verwijzing
Deze afspraak strekt zich uit over systemen die op een veilige en betrouwbare wijze gegevens binnen de administratieve keten van het onderwijsdomein (ongeacht welke sector) moet uitwisselen tussen verschillende organisaties. Deze afspraak omvat tevens de organisaties of onderdelen van organisaties waar deze systemen draaien. Wanneer gegevens worden uitgewisseld met een onderwijsinstelling die gebruik maakt van een multi tenant cloud-oplossing, heb je te maken met de identiteit van het systeem van de cloud-leverancier en de identiteit van de onderwijsinstelling voor wie de gegevens bedoeld zijn of aan wie gegevens worden gevraagd. De afspraak richtte zich daarom in eerste instantie op de kwaliteit van en rechtstreekse uitwisseling met de cloud-leverancier in plaats van met de onderwijsinstelling. Bij deze oplossingsrichting worden gegevens verstuurd 'aan SAAS-leverancier Y, ter attentie van onderwijsinstelling X' (zie onderstaand figuur)  *rode pijl = Edukoppeling Transactiestandaard* De afspraak kan – afhankelijk van de (risico's in) ketenprocessen - ook gebruikt worden voor rechtstreekse uitwisseling tussen ketenpartijen, waarbij een veilige end-to-end beveiliging van gegevens niet alleen technisch geregeld kan worden.	

2.4. Wie is de doelgroep van de afspraak? (Bijv. DUO, onderwijsinstellingen, LAS-systemen, uitgeverijen.)

Antwoord	verwijzing
Eigenaars van systemen die persoonsgegevens uitwisselen binnen de onderwijsketen, het kan hierbij gaan om DUO, onderwijsinstellingen of partijen die namens hen uitwisselen.	

2.4.1. Bestaat de afspraak uit verschillende delen die zich op verschillende doelgroepen richten (en zo ja welke)?

Antwoord	verwijzing
Ja. Het schema bestaat uit een set normen en interpretation notes om inhoudelijk te toetsen of partijen de afspraken (i.c. de normen) nakomen. Daarnaast bevat het schema templates voor de zelfverklaring en de bewerkersovereenkomst.	

2.5. Wat is het doel van de afspraak?

Antwoord	verwijzing
Het beveiligd (end-to-end) digitaal uitwisselen van persoonsgegevens. Met deze afspraak kan verzekerd worden dat ketenpartijen voldoende maatregelen genomen hebben – en dus te vertrouwen zijn - om een veilige uitwisseling te garanderen.	

2.5.1. Wat gaat er fout als de afspraak niet geaccepteerd wordt door het veld?

Antwoord	verwijzing
Leveranciers kunnen niet met DUO uitleveren in het kader van Digitaal aanmelden en Facet. In algemene zin zou je kunnen zeggen dat zonder deze afspraak een technisch protocol zoals Edukoppeling 'alleen maar' een technische beveiliging biedt van systemen.	

2.5.2. Hoe urgent is de afspraak?

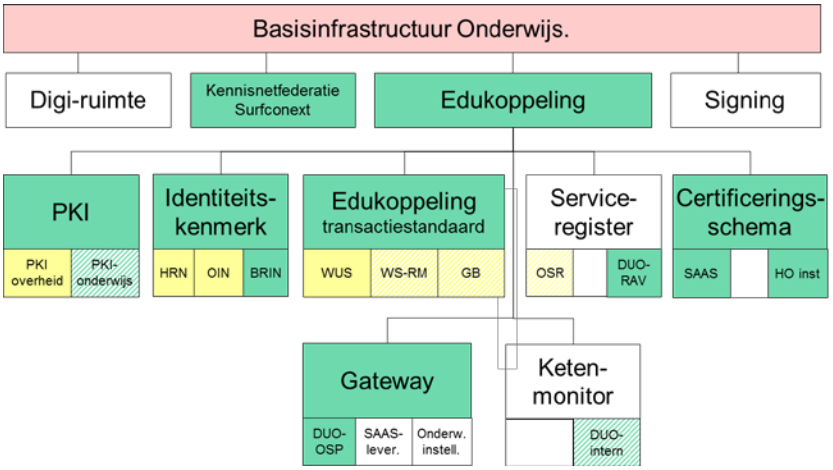
Antwoord	verwijzing
Zonder de standaard kan er niet uitgewisseld worden in het kader van Digitaal aanmelden MBO, waarbij gegevens via DUO hergebruikt kunnen worden. Daarnaast is de standaard een randvoorwaarde voor de uitwisseling met instellingen in het kader van Facet (toetsen) en Doorontwikkelen Bron (bekostigen), dat in najaar 2014 resp. opgeleverd en opgestart zal worden.	

2.5.3. Biedt de afspraak een volledige oplossing voor het beoogde doel en de beoogde doelgroep?

Antwoord	verwijzing
Ja, er is in mei 2014 een risico-analyse uitgevoerd met alle stakeholders voor een onderbouwing van het schema. Hieruit kwam naar voren dat de risico's rondom gegevensuitwisseling in het kader van aanmelden, overdragen en inschrijven door de te nemen maatregelen in het schema afgedekt worden. De wijze waarop deze afspraak wordt toegepast is uiteindelijk bepalend voor het vertrouwen dat organisaties onderling kunnen hebben bij het uitwisselen van gegevens.	Zie bijlage "Verslag workshop risiso-analyse digitaal aanmelden, overdragen en inschrijven"

3. Hoe past de afspraak in het grotere geheel.

3.1. Op welke (keten)processen heeft de afspraak betrekking? (Bijv. in- en uitschrijfprocessen tussen instellingen.) (indien mogelijk graag plotten op één van de bij Edustandaard geregistreerde architecturen.

Antwoord	Verwijzing
De afspraak wordt binnen de ROSA geschaard bij andere (nog te ontwikkelen) ICT-infrastructurele afspraken en voorzieningen onder de noemer Edukoppeling.  *Toelichting: Groen = Onderwijs specifieke voorziening. Geel = Voorziening of standaard ook buiten het onderwijsdomein in gebruik. Wit = nog niet gerealiseerd. De witte blokjes moeten in de toekomst nog nader ingevuld worden.*	http://www.wikixl.nl/wiki/rosa/index.php/Doelen_en_principes_referentiearchitectuur

3.2. Welke architectuur principes zijn gerelateerd aan de afspraak (bij voorkeur aangeven hoe die relatie ligt)?

Antwoord	Verwijzing
Principes die van toepassing zijn op het bredere kader waarbinnen deze afspraak een plek inneemt zijn: • Digitaal doen we het zo • Een gezamenlijke basisinfrastructuur De afspraak heeft ook betrekking op de privacy- en beveiligingsprincipes afgeleid van het NORA informatiebeveiligingskatern en de Wet Bescherming Persoonsgegevens. Deze worden opgenomen het privacy en beveiligingskatern van de ROSA dat momenteel ontwikkeld wordt. Tenslotte sluit de afspraak aan bij de Enterprise Architectuur van DUO (2014-2018).	http://www.wikixl.nl/wiki/rosa/index.php/Doelen_en_principes_referentiearchitectuur

3.3. Op welke informatieobjecten heeft de afspraak betrekking? (Bijv. persoonsgegevens, leermateriaal, metadata, leerresultaten.)

Antwoord	Verwijzing
Edukoppeling is bedoeld voor het beveiligd uitwisselen van persoonsgegevens. De afspraak (dit schema) heeft betrekking op onderwijsorganisaties, SAAS-leveranciers, organisatieonderdelen en medewerkers, systemen, auditors, certificaten, assessments etc.	

3.4. Op welke services, bouwblokken en/of infrastructuur heeft de afspraak betrekking? (Bijv. Edukoppeling, Edurep, ENTREE-federatie, Metaplus, BME, Linked Open data-API.)

Antwoord	Verwijzing
De afspraak is onderdeel van de Edukoppeling basis ict-infrastructuur (zie 3.1).	

3.5. Zijn er nog andere relevante zaken waar de afspraak betrekking op heeft en zo ja, welke?

Antwoord	Verwijzing
Onderdeel van de afspraak is het gebruik van de Edukoppeling transactiestandaard. De afspraak maakt ook onderdeel uit van het ROSA katern Privacy en beveiliging.	http://www.edustandaard.nl/afspraken-en-architectuur/beheerde-afspraken/edukoppeling/

3.6. Wat is de samenhang van deze afspraak met andere afspraken en standaarden?

3.6.1. Is de afspraak gebaseerd op (inter)nationale standaarden en zo ja, welke?

naam standaard	versie	datum	Verwijzing
Het schema maakt gebruik van de “Cloud Control Matrix” van de Cloud Security Alliance.	v3.01	11 juli 2014	https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/

3.6.2. Welke afspraken en standaarden zijn gerelateerd met deze afspraak en waar raken ze elkaar? (Bijv. afspraken en standaarden zowel binnen als buiten het onderwijs, zowel binnen als buiten Nederland. Bijv. welke principes komen overeen; zijn er services die ook binnen andere afspraken een rol spelen? Nota bene: Samenhang kan ook worden aangeven door de verschillen te benoemen.)

naam afspraak	raakpunten in overeenkomsten en/of verschillen	verwijzing
SURF normenkader cloudservices hoger onderwijs	Dit normenkader heeft echter een ander vertrekpunt. Er is een verschillen analyse gemaakt. Daarnaast wordt er met SURFnet gewerkt aan meer samenhang tussen het Normenkader en het certificeringsschema. Zie bijlage “Verschillen analyse SURF normenkader”	http://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2013/juridisch-normenkader-cloudservices-hoger-onderwijs.pdf

4. Is de afspraak breed geaccepteerd door de doelgroep?

4.1. Welke partijen en welke personen waren betrokken bij de ontwikkeling? (Geef bij voorkeur ook verwijzingen naar de openbare verslagen en/of besluitenlijsten van bijeenkomsten.)

Antwoord	verwijzing
Ja Betrokken rollen: MT-DUO, CIO DUO CTO Kennisnet, TPM Kennisnet-OSO, CSO Kennisnet, jurist Kennisnet CIO OCW, Systeemarchitect UP learning, CSO Studielink, Functionaris gegevensbescherming OCW/DUO Betrokken gremia: SION (onderwijsraden) Architectuurraad Edustandaard DUO Technisch of SWL overleg PO, VO en MBO OCW/DUO Strategisch I-beraad Informatiekamer	

4.2. Geef een of meer voorbeelden van een *real-life business* situatie waarin de afspraak is gebruikt.

Antwoord	verwijzing
De afspraak wordt momenteel toegepast door UP learning / Educus in de uitwisseling tussen DUO en hun systeem voor kernregistratie in het MBO, genaamd Eduarte. Er zijn nog weinig voorbeelden, omdat we als onderwijs met een dergelijke afspraak momenteel voorop lopen. De Cloud control matrix (CSA) wordt daarentegen veel breder toegepast (zoals banken en internationale organisaties).	

4.3. Wie zijn op welke manieren ingelicht over de afspraak? (denk bijvoorbeeld aan bijeenkomsten, seminars, FAQ's op websites, fora, papers)

Antwoord	verwijzing
December 2013 – Website www.sionderwijs.nl 10 december 2013 – Leveranciers Magister en UP-learning t.b.v. Digitaal aanmelden MBO 9 t/m 16 mei 2014 – Consultatieronde architectuurraad en leveranciersoverleggen DUO t.b.v. Keten Start Architectuur Doorontwikkelen Bron Juni 2014 – SWL en Technisch overleg DUO voor PO, VO en MBO 11 juni 2014 – Leveranciersbijeenkomst MBO t.b.v. Facet	

5. Hoe ziet de implementatie van de afspraak eruit?

5.1. Is er een implementatiehandleiding en/of andere implementatieondersteuning beschikbaar en zo ja, welke?

Antwoord	verwijzing
In hoofdstuk 2 van de afspraak worden aanwijzingen gegeven voor de toepassing van de afspraak. Momenteel moet de leverancier zelf nagaan in hoeverre men voldoet aan de gestelde normen en hierover inzicht verschaffen. De leverancier vult een Management Verklaring waarmee men verklaart aan de gestelde normen te voldoen. De zelfverklaring is een fysiek document en moet worden ondertekend door een bij de KvK geregistreerde tekenbevoegde. Daar waar verbeterpotentieel aanwezig is, worden deze expliciet benoemd in een bijlage bij de verklaring, aangevuld met een planning wanneer leverancier verwacht de verbetering te hebben gerealiseerd. De zelfverklaring heeft een beperkte houdbaarheidsduur (max. 1 jaar) en dient te worden ingediend bij de beheerder (Kennisnet namens SION), die de verklaring controleert en archiveert. Verklaringen of namen van gecertificeerde partijen worden momenteel niet gepubliceerd, maar zijn wel opvraagbaar bij de beheerder.	Zie hoofdstuk 2 van de afspraak

5.2. Is er een tool beschikbaar om implementatie van (delen van) de afspraak op correct gebruik te toetsen zo ja, welke? Zo nee, voor welke delen zou dit wel denkbaar zijn (aanvullen met een korte schets welke technieken daarvoor gebruikt kunnen worden)?

Antwoord	verwijzing
Het schema bestaat uit een set normen en interpretation notes om inhoudelijk te toetsen of partijen de afspraken (i.c. de normen) nakomen. Daarnaast bevat het schema templates voor de zelfverklaring en de bewerkersovereenkomst.	

5.3. Wat is de globale inschatting voor wat de kosten, benodigde tijdsinvestering en/of expertise voor de betrokken partijen zijn voor de implementatie van de afspraak?

Antwoord	verwijzing
Het toetsen van de controls, het beschrijven van de maatregelen, de invulling van de zelfverklaring en de afhandeling van de bewerkersovereenkomst heeft 2 werkdagen in beslag genomen. De doorlooptijd was een paar weken i.v.m. de afhandeling van de bewerkersovereenkomst.	

6. Hoe zijn het beheer en de doorontwikkeling geregeld? (Indien dit nog niet is vastgesteld kunt u dit nader afstemmen met Bureau Edustandaard.)

6.1. Onder welke Edustandaard werkgroep gaat het beheer vallen? (Bijv. onder een bestaande werkgroep of een nieuw op te richten werkgroep.)

Antwoord	verwijzing
In principe zou de Werkgroep Edukoppeling uitgebreid kunnen worden met experts van DUO, Kennisnet en SURF op het gebied van Informatiebeveiliging. Wellicht dat de werkgroep in verschillende samenstellingen bijeen moet komen, omdat de inhoudelijke agenda van de transactiestandaard en het certificeringsschema nog wel kan verschillen. Het is goed denkbaar dat er 2 subwerkgroepen zullen bestaan die op gezette tijden onderling afstemming hebben. Het beheer door de werkgroep heeft met name betrekking op inhoudelijke wijzigingsvoorstellen op het schema of het normenkader. Bij het beheer worden modellen voor groei en borging van bewustwording en vakbekwaamheid toegepast volgens de PDCA-cyclus of volwassenheids-methodieken, zoals CMM (Maturity Models) of ITOMM of de 5 IT-governance-aspecten van NOREA. Het groeipad van zelfverklaringen naar externe audits wordt nog bepaald binnen SION. Dit geldt ook voor de rol van toezichthouder en uitvoerder, dat momenteel ad-interim door Kennisnet (namens SION) wordt uitgevoerd. Om die reden zal er in de werkgroep ook namens SION een vertegenwoordiger deelnemen. Wijzigingen ten aanzien van deze twee onderdelen (het groeipad en de rolverdeling) kunnen alleen via SION ingebracht worden.	

6.2. Hoe is de doorontwikkeling geregeld? (Bijv. is er een loket voor het beantwoorden van vragen en indienen van wijzigingen?)

Antwoord	verwijzing
Wijzigingen voor de doorontwikkeling van het schema zouden via de werkgroep moeten verlopen. Momenteel verlopen die nog via de SION kerngroep ROSA.	

6.3. Wat is de globale inschatting van wat de kosten, benodigde tijdsinvestering en/of expertise voor de betrokken partijen zijn voor het beheer en doorontwikkeling van de afspraak?

Antwoord	verwijzing
De verwachting is dat de werkgroep zo vaak bijeenkomt als nodig, maar minimaal 1 x per jaar voor het bespreken van de wijzigingsvoorstellen. Voor het voorbereiden en uitwerken van deze voorstellen, dient minimaal nog 1 a 2 dagen gerekend te worden (per voorstel). Daarnaast moet voor het uitvoeren van een risico-analyse om na te gaan of de geselecteerde controls voldoende zijn ook minimaal 1 dag gerekend te worden.	

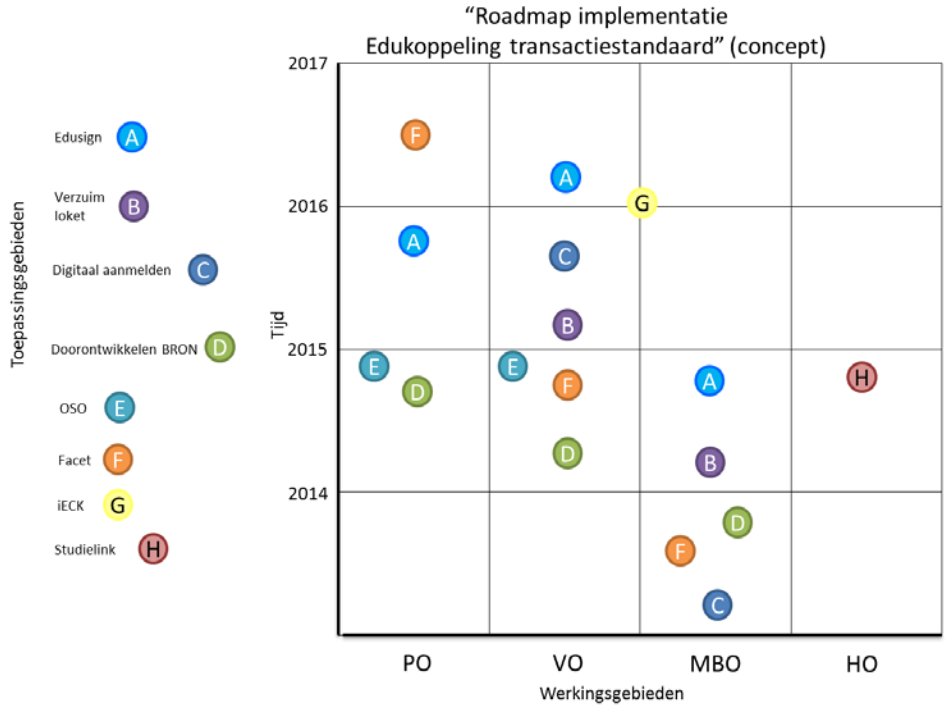
7. Hoe ziet de geschiedenis en toekomst van de afspraak eruit?

7.1. Geef aan wanneer deze en alle voorgaande versies zijn uitgebracht. Geef kort de belangrijkste verschillen aan tussen de versies.

Versie	Wijzigingen	verwijzing
1.0	Eerste versie	http://www.sionderwijs.nl/fileadmin/contentelementen/kennisnet/SI_Onderwijs/Certificatieschema_Edukoppeling_en_SAAS_01.pdf
1.1	Het normenkader is aangepast naar aanleiding van de resultaten uit de risico-analyse. Het normenkader is uitgebreid met nadere vragen voor de normen en de mapping met ISO 27001:2013 (conform het werk van de CSA)	Zie bijlage A van het schema.

7.2. Wat is de roadmap m.b.t. de doorontwikkeling en de toepassing van de afspraak?

Antwoord	verwijzing
De belangrijkste doorontwikkeling van het schema heeft betrekking op de zelfverklaringen. Vroeg of laat zullen hier hogere eisen aan gesteld moeten worden. Hierover worden binnen SION gesprekken met DUO en leveranciers gevoerd. Daarnaast is de verwachting dat de afspraak bij meerdere uitwisselingen toegepast zal gaan worden, bijv. in het kader van Facet (toetsen) en Doorontwikkelen Bron (bekostigen). De roadmap is nauw verbonden met de implementatie van de transactiestandaard. Zie onderstaand figuur voor een indicatie hiervan.	



8. Welke copyrights en andere voorwaarden zijn van toepassing op de afspraak?

8.1. Kan het intellectuele eigendom - m.b.t. mogelijk aanwezige patenten - van de afspraak onherroepelijk op een royalty-free basis aan Edustandaard ter beschikking worden gesteld?

Antwoord	verwijzing
Ja, met naamsvermelding	

8.2. Is het voor een ieder mogelijk om de afspraak (inclusief alle bijbehorende documentatie) te kopiëren, beschikbaar te stellen en te (her)gebruiken om niet?

Antwoord	verwijzing
Ja, met naamsvermelding	