Ontwerp

Overstapservice Onderwijs **'15**

Versie 1.0

Auteur	:	Arjan van Krimpen
Collegiale toetsing	:	Remi Bindadin, Robert Klein
Versie	:	1.0.0
Datum	:	29 januari 2015

Inhoudsopgave

1. INLEIDING

De Overstap Service Onderwijs (OSO) is een dienst die het veilig en betrouwbaar overdragen van digitale overstap dossiers faciliteert. OSO bestaat enerzijds uit een technisch deel, waarbij de centrale component van OSO, het Traffic Center, de toegang regelt van school- en instellings- systemen tot OSO. Het tweede deel is een set afspraken over de inhoud en structuur van de dossiers, de functionaliteit, techniek en beveiliging van de koppelvlakken en de omgang met de gegevens door leveranciers en scholen. Actuele en relevante informatie vindt u op de volgende website:Overstapservice Onderwijs.

De via OSO verstuurde dossiers volgen de afspraken en definities van de EduStandaard OSO gegevensset. De ontwikkeling van de gegevensset is nauw gelinkt met die van OSO, maar staat formeel los van de dienst OSO. De Kennisnet Validatie Service (KVS) maakt formeel geen onderdeel uit van OSO, maar wordt binnen OSO wel toegepast.

In de Overstapservice werken diverse partijen samen om de overdracht van leerlinginformatie tussen [scholen] te optimaliseren. De daadwerkelijke overdracht van dossiers verloopt volgens een viertal use cases die hieronder beschreven worden. Per use case vinden een aantal interacties tussen systemen plaats, die in meer detail in aanroepen en acties worden beschreven. Een belangrijk aandachtspunt van OSO is de beveiliging van de gegevens, de maatregelen die hiervoor voorgeschreven worden, zijn uitgewerkt in beveiliging.

1.1.1. *Use Cases*

- Als doelsysteem wil ik een dossier opvragen (bij een bronsysteem)
- Als bronsysteem wil ik een dossier klaarzetten (voor een doelsysteem)
- Als systeem(bouwer) wil ik op OSO aansluiten
- Als systeem(bouwer) wil ik mijn OSO aansluiting testen

- Ik wil een ouder/verzorger inzage geven en/of toestemming registreren
- Ik wil met de Test School uitwisselen.

- Ik wil voldoen aan het Programma van Eisen

1.1.2. *Hotlinks*

- Architectuur en Proces
- OSO berichtenverkeer en protocol
- Organisatorische Randvoorwaarden en Eisen
- OSO beveiligings - voorschriften en - maatregelen
- EduStandaard OSO (dossier standaard)
- Wijzigingen in OSO'15
- Woordenlijst

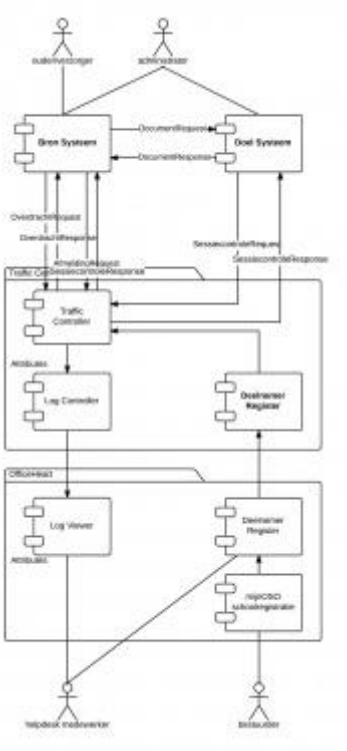
1.1.3. *Communicatie*

Overstap Service Onderwijs site

Atom Feed wijzigingen OSO wiki

2. OSO:ARCHITECTUUR EN PROCES

2.1. Architectuur



De Overstapservice faciliteert het uitwisselen van gegevens (een ?document? of 'dossier' of 'OKR") tussen twee informatiesystemen. De volgende systemen spelen daarbij een rol:

1. Het informatiesysteem van de opvragende partij, het doelsysteem. Dit kan zowel een leerling administratie systeem (LAS) als een regionaal platform (RP) zijn.
2. Het informatiesysteem van de partij die gegevens kan aanleveren, het bronsysteem. Dit kan zowel een LAS als een RP zijn.
3. Het Traffic Center: Dit verzorgt primair de controle op de geldigheid van de uitwisselsessie tussen het doel- en bron- systeem en daarnaast heeft het een rol als register van de adressen van de systemen.
4. De informatiesystemen in de backoffice, OfficeHeart en mijnOSO.
    - De helpdesk medewerkers onderhouden in de backoffice het register van deelnemende partijen, informatiesystemen en aanleverpunten. Tevens kunnen zij de logregels raadplegen die het Traffic Center bijhoudt over uitwisselsessies.
    - Schoolbestuurders hebben toegang tot mijnOSO, een specifieke uitbreiding van OfficeHeart. Hierin kunnen zij gegevens over hun scho(o)len beheren en pki veiligheidscertificaten downloaden.

OSO componenten

Aangesloten systemen kunnen de rol vervullen van bron- of doel - systeem. Eenzelfde LAS of RI-platform kan zowel de rol

'documentbron' als de rol 'documentdoel' vervullen, maar nooit in dezelfde uitwisselsessie. Afhankelijk van het systeem zal het geschikt zijn om als bron of doel te vervullen voor bepaalde typen uitwisseling.

2.1.1. Traffic Center

Het Traffic Center is een belangrijke spil in het OSO web. Het doel van TC is op een veilige en controleerbare wijze communicatie tot stand te brengen tussen de LAS?en. De LAS?en worden gehost voor of op een school en bevatten alle leerling dossiers van een school. Daarnaast biedt TC een koppelvlak voor regionale initiatieven waardoor deze ook in de landelijke keten kunnen uitwisselen. Voor het TC zijn LASsen en RI?s gelijkwaardig.

Binnen het Traffic Center kunnen de volgende componenten worden onderscheiden:

- Traffic controler, deze authenticeert doel- en bron-systemen voor de overdracht van een document. Daartoe geeft de controller eenmalige sessies uit en bewaakt deze.
- Deelnemersregister dit bevat een administratie van deelnemende instellingen met hun aanleverpunten. Ieder aanleverpunt komt overeen met een op een instelling gebruikt LAS of RI-platform. De traffic controller gebruikt het deelnemersregister o.a. om te controleren of een deelnemer via de Overstapservice mag communiceren. Het deelnemersregister in het Traffic Center wordt beheerd vanuit OfficeHeart en is een functionele kopie van de actuele deelnemers in het deelnemersregister binnen OfficeHeart.
- Log controller, dit legt gegevens vast in een logregister over de overdrachten en andere transacties. Het Traffic Center kan alleen maar regels aan het logregister toevoegen; het Traffic Center noch een andere partij kan de log- regels wijzigen of verwijderen.

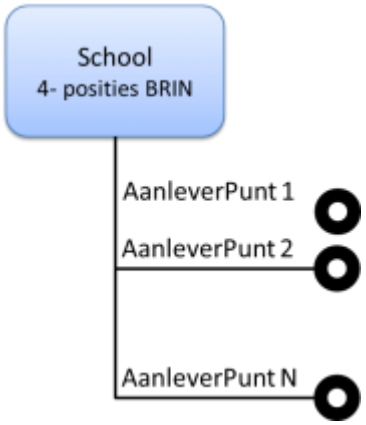
2.1.2. Systemen en aanleverpunten

Een school of instelling kan meerdere systemen gebruiken om gegevens van leerlingen te registreren en te verwerken, soms verspreid over meerdere vestigingen. Al deze systemen kunnen aangesloten worden op OSO. Per school moet voor ieder systeem dat wordt

aangesloten een AanleverPunt (AP) gedefinieerd worden. Via haar AP koppelt een systeem met OSO en kan deschool gegevens uitwisselen met andere OSO deelnemers.

Een AP wordt geregistreerd bij een school op bestuursnivo (ook wel BRIN of BRIN(4) nivo genoemd). Daarnaast heeft een AP een index die samen met de BRIN de unieke sleutel van de AP vormt. Het eerste AP van een school heeft index 0, daarna wordt er door genummerd in volgorde van aanmelding. (De AP index heeft geen relatie met door DUO of de inspectie toegekende nummers aan vestigingen of met het OIN.) Een AP heeft een label dat bij registratie wordt ingevuld en een aanduiding of het een LAS of RP betreft.

School met aanleverpunten



Bij het opvragen van een dossier is bij het doelsysteem (meestal) alleen de BRIN van de leverende school bekend. Omdat de leverende school meerdere AP's kan hebben, geeft het TC een lijst van alle onderliggende AP?s van deze BRIN bij een verzoek tot overdracht. De ontvangende partij moet vervolgens deze ap?s aflopen volgens een set van afspraken. De regels die hierbij moeten worden gehanteerd staan hier beschreven.

2.1.3. PKI infrastructuur

OSO hanteert een private PKI infrastructuur, uitgifte vanuit de backoffice georganiseerd en valt buiten scope Leverancier. Wel belangrijk is dat Leverancier weet hoe een PKI infrastructuur op te zetten, hoe deze werkt, velden uit certificaten uit te kunnen lezen en bewust omgaat met veiligheidsrisico?s in code die kunnen leiden tot het verzwakken van de (PKI) infrastructuur.

2.1.4. TC OTAP Omgevingen

De TC omgeving bestaat uit een:

- Test

- Sandbox
- Qualification
- Productie

De test wordt gebruikt om eerste opleveringen van TC binnen de Kennisnet omgeving te testen. De sandbox wordt gebruikt als testomgeving voor nieuwe LAS?en. Ontwikkelpartijen kunnen hiermee de connectiviteit richting het TC testen. Als de software ontwikkelaar hiermee klaar is komt deze in aanmerking voor kwalificatie. Hiervoor de qualification omgeving. De tester bij Kennisnet loopt de testprocedure af en checkt inhoudelijk of het LAS voldoet aan de eisen die gesteld worden om aan te mogen sluiten in productie. De acceptatie omgeving wordt ingezet om infrastructurele wijzigingen, met name op gebied van loadbalancing te testen. Deze wordt niet ingezet voor LAS?en maar is puur intern gericht.

De productie omgeving wordt ingezet voor gekwalificeerde LAS?en en de daarbij horende scholen. Elke school die gebruik maakt van een gekwalificeerde LAS kan een toegangscertificaat ophalen en hiermee de school ontsluiten binnen het OSO netwerk.

2.2. Proces

In de figuur worden de stappen en berichten weergegeven die bij een succesvolle dossier overdracht worden doorlopen. Een overdracht start bij het systeem van de nieuwe school, het Doelsysteem.

2.2.1. Berichten verkeer

1. Het doelsysteem verzendt een aanvraag (OverdrachtRequest) naar het Traffic Center (TC) voor het opvragen van een dossier.

   De aanvraag bevat het versleutelde BSN van de leerling (het TC kan dit niet lezen). Het TC controleert of het doelsysteem bekend en gekwalificeerd is (zowel de school als de leverancier moeten gekwalificeerd zijn). Als dit het geval is, wordt een sessie id toegekend en teruggestuurd naar het aanvragende systeem (OverdrachtResponse). Sessie intiëren

2. Het doelsysteem verzendt een aanvraag voor een dossier naar het systeem van de huidige school (DocumentRequest), het bronsysteem.

   De aanvraag bevat de BSN van de leerling (één dossier per aanvraag) en het sessie id. Het bronsysteem vraagt vervolgens eerst een controle op de sessie gegevens op bij het TC.Dossier opvragen

3. Het bronsysteem verzendt een sessie controle verzoek (SessiecontroleRequest) naar het TC.

   Dit verzoek bevat het versleutelde BSN en de sessie id uit bericht 2. Het TC controleert deze gegevens; wanneer deze overeenkomen met een uitgegeven nog niet verlopen sessie wordt een ok teruggegeven (SessiecontroleResponse). Controleren sessie

4. Het bronsysteem stuurt het dossier aan het doelsysteem (DocumentResponse).

   Als het gevraagde dossier beschikbaar is wordt een valide dossier geleverd; indien het dossier niet beschikbaar is (onbekend of nog niet gereed voor verzending) wordt de bijbehorende foutmelding verstuurd. De levering van het dossier en de foutmeldingen vormen de response op bericht 2.

5. Het doelsystem meldt de aanvraag af bij het TC.

Bij het afmelden (AfmeldingRequest) geeft het doelsysteem aan of het dossier is ontvangen, of dit valide was of dat het niet beschikbaar was bij het bronsysteem. Het TC antwoordt (AfmeldingResponse) en administreert het resultaat en ruimt de sessie gegevens op. Sessie afmelden

2.2.2. *Soorten overdracht*

Binnen de EduStandaard OSO worden overdrachten beschreven tussen schooltypen. POPO POVO VOVO

2.2.3. *Overdracht type*

Het type overdracht bepaalt regels, structuur en inhoud van een dossier. De mogelijke waarden worden gedefinieerd in de EduStandaard OSO (en dit zouden er meer kunnen zijn dan binnen de infrastructuur worden ondersteund). Binnen de infrastructuur OSO worden twee typen onderscheiden;

- ?overstapdossier?, een 'normale' uitwisseling tussen twee scholen of instellingen.
- 'overdrachtBinnenBRIN?, dan betreft het een overdracht binnen dezelfde instelling (BRIN gelijk).

3. OSO:ROLLEN EN PARTIJEN

Hieronder worden op hoofdlijnen de belangrijkste partijen in de OSO omgeving beschreven. Deze lijst heeft als doel (ontwikkelaars bij) aansluitende partijen de context te schetsen van de omgeving (en is zeker niet volledig). Daarnaast vullen de beschrijving van de OSO architectuur en de randvoorwaarden voor aansluiten dit beeld aan.

In de figuur worden de stappen in het OSO berichtenverkeer weergegeven die worden afgelopen bij het aanvragen, versturen en ontvangen van een overstapdossier. De verzendende school is verantwoordelijk voor het afwegen welke gegevens er al dan niet verstrekt moeten worden aan de aanvragende partij. Het bronsysteem dient deze keuze te kunnen ondersteunen. De overstapservice faciliteert alleen het beveiligd transport van deze gegevens.

1. De verzendende school dient voorafgaand aan verzending te controleren of ouders inzage hebben gehad in of toestemming hebben gegeven voor het verzenden van het dossier. (Uitwisselingen binnen dezelfde instelling zijn toegestaan zonder deze inzage.) Wanneer in het dossier niet is aangegeven dat dit is ingezien door de ouders, mag er niet tot levering worden overgegaan.
2. Een tweede check die OSO vereist, is het instellen door de eindgebruiker van de ontvangende partij door de verzendende school. Alleen wanneer het BRIN van de aanvragende school overeenkomt met deze waarde, mag het bronsysteem het dossier leveren.

3.1. School

Een school kan gebruik maken van OSO om:

- een overstapdossier op te vragen bij de huidige school, als de school de vervolgschool van de leerling is
- een overstapdossier te leveren naar een volgende school, als de aanvragende school de vervolgschool van de leerling is

Voor deze informatie-uitwisseling maakt de school gebruik van een of meerdere leerlingadministratiesystemen en/of regionale platforms, al dan niet verspreid over meerdere vestigingen. Binnen de Overstapservice noemen we het koppelvlak van zo?n systeem met OSO een aanleverpunt. Via het aanleverpunt wisselt een schoolsysteem informatie uit met het TC en andere OSO deelnemers.

3.2. Leerlingen, ouders en verzorgers

Deze partijen interacteren indirect met OSO. Wel zijn zij direct belanghebbende en gelden er wettelijke voorschriften voor hun betrokkenheid.

3.3. Bestuurders, docenten, administratie

Schoolbestuurders zijn betrokken bij de kwalificatie van hun scho(o)l(en) en werken daarbij met de OSO backoffice. De daadwerkelijke uitwisseling wordt doorgaans uitgevoerd door docenten en administratie medewerkers, die daarbij werken met LASsen en/of RP's.

3.4. Back Office

In de backoffice worden de gegevens van de aangesloten scholen en de regionale initiatieven beheerd. Vanuit de backoffice krijgt het Traffic Center informatie over aangesloten partijen en aanleverpunten. De backoffice bestaat uit twee delen:

- mijnOSO een portaal voor deelnemende scholen
- OfficeHeart het pakket dat door de Servicedesk wordt gebruikt.

3.5. Traffic Center

Het Traffic Center is het hart van de Overstapservice. Het Traffic Center verzorgt alle faciliteiten (hardware, software, beheer) die informatie-uitwisseling in de Overstapservice mogelijk maakt. Het Traffic Center is primair de toegangsbewaker van uitwisseling tussen systemen. In het TC bevindt zich een administratie van deelnemende systemen en aanleverpunten (waarvan de gegevens vanuit de back office aangeleverd worden) en een logregister, waarin gegevens over overdrachts- en controle- aanvragen opgeslagen worden.

3.6. LAS/RP leverancier

LASsen en RP's zijn informatiesystemen in de school voor basisadministratie, zorgregistratie en leerlingendossiers. De leveranciers van deze systemen zijn indirect belanghebbenden bij een goed functionerende uitwisseling via OSO voor hun systemen en klanten.

4. OSO:ORGANISATORISCHE RANDVOORWAARDEN

4.1. Kwalificatie van de school

Een school dient gekwalificeerd te zijn om te mogen deelnemen aan de Overstapservice. Het juridische deel van de kwalificatie betreft het ondertekenen van een bewerkerovereenkomst.

4.2. Kwalificatie van de leverancier

4.2.1.1. Bewerkerovereenkomst

Voor de Wet Bescherming Persoonsgegevens is de school de verantwoordelijke voor het verwerken van de persoonsgegevens. Als de school een leverancier inschakelt, bijvoorbeeld een LAS-leverancier, dan wordt deze leverancier een ?bewerker? genoemd. Deze werkt in opdracht van de verantwoordelijke, de school dus. De school blijft altijd eindverantwoordelijk voor de afspraken met de bewerker. Volgens de wet moet de verantwoordelijke er voor zorgen dat de bewerker de juiste beveiligingsmaatregelen neemt. Maar de verantwoordelijke moet ook zorgen voor afspraken over eigendom van de persoonsgegevens (die blijven van de school), het teruggeven/vernietigen van de gegevens of inschakelen van onderaannemers door de leverancier. De afspraken met de bewerker worden vastgelegd in de bewerkersovereenkomst.

4.3. Eisen aan organisatie en proces

Deze wettelijk eisen gelden wanneer er sprake is van ?externe werking?; het overdragen van het dossier van de ene instelling naar een andere.

4.3.1. Inzage en/of Toestemming van ouders/verzorgers

Ouders en/of verzorgers interacteren indirect met de Overstapservice: Via de scholen of via een ouderportaal van een LAS/RIS. In het algemeen geldt dat ouders, verzorgers of de meerderjarige leerling een dossier moeten hebben ingezien alvorens een school het mag overdragen aan de nieuwe school.

Voorafgaand aan het verzenden van een dossier is de huidige school verplicht ouders inzage te geven in het dossier (PO) dan wel

toestemming te vragen voor verzending (VO). Deze wettelijk eis geldt wanneer er sprake is van ?externe werking?; het overdragen van het dossier van de ene instelling naar een andere. Binnen OSO geldt dat het bronsysteem verplicht is te controleren dat de ouderlijke inzage/toestemming heeft plaats gevonden/is gegeven. Een dossier mag niet klaar gezet worden voor verzending wanneer aan deze voorwaarde nog niet voldaan is.

Wanneer er sprake is van een verzoek binnen dezelfde school geldt deze eis niet. Een overdracht blijft binnen dezelfde school, in OSO termen een overdracht tussen AP?s die onder dezelfde BRIN vallen. Het dossier wordt dan bijvoorbeeld overgedragen van een LAS naar het RI-platform of ander LAS van dezelfde school.

Er is wel sprake van ?externe werking? wanneer een RI niet alleen de school faciliteert, maar ook optreedt als bewerker van gegevens (?verrijking? of andere scenario?s). In zo?n geval dient de controle op inzage plaats te vinden voorafgaand aan de overdracht, ook al is er sprake van een ?overdracht binnen een BRIN?.

4.3.1.1. PO versus VO

In het algemeen kan gesteld worden dat in het PO geldt dat ouders inzage moeten hebben gehad in het dossier. Zij kunnen hierbij aangeven dat zij bezwaar aantekenen tegen de inhoud en dit bezwaar dient geregistreerd te worden, maar hun toestemming is niet(!) nodig voor verzending. In het VO geldt dat ouders toestemming dienen te geven voor het verzenden van een dossier.

4.3.1.2. BinnenBRIN

Wanneer er sprake is van een verzoek binnen dezelfde school geldt deze eis niet. Een overdracht blijft binnen dezelfde school, in OSO termen een overdracht tussen AP?s die onder dezelfde BRIN vallen. Het dossier wordt dan bijvoorbeeld overgedragen van een LAS naar het RI-platform of ander LAS van dezelfde school. Er is wel sprake van ?externe werking? wanneer een RI niet alleen de school faciliteert, maar ook optreedt als bewerker van gegevens (?verrijking? of andere scenario?s). In zo?n geval dient de controle op inzage plaats te vinden voorafgaand aan de overdracht, ook al is er sprake van een ?overdracht binnen een BRIN?.

5. OSO:DOSSIER OPVRAGEN

Dit scenario beschrijft hoe een Doelsysteem een dossier opvraagt bij een Bronsysteem. Dit scenario geldt ook voor een binnenbrin overdracht, waarbij een RP of LAS een dossier ophaalt binnen zijn eigen brin bij een andere LAS of RP.

Het proces wordt geïnitieerd door het Doelsysteem en wordt uiteindelijk ook afgemeld door het Doelsysteem.

5.1. Context

Het Doelsysteem haalt een dossier op bij een Bronsysteem. Het Doelsysteem weet welk bsn de leerling heeft en bij welk brinnummer het dossier opgevraagd kan worden.

- Initiator: Doelsysteem (LAS of RP)
- Responder: Bronsysteem (LAS of RP)
- Pre: Veronderstelt wordt dat
    - het Doelsysteem is aangesloten op OSO met een geldig certificaat;
    - het bronsysteem heeft tenminste één aanleverpunt geregistreerd.
- Post: Het Doelsysteem heeft het dossier ontvangen van het Bronsysteem. Sessie is afgemeld.

5.2. Sessie Initiëren

Het Doelsysteem initieert een sessie door een overdrachtsRequest naar het TC te versturen. Dit request bevat o.a. het brinnummer van het Bronsysteem. Het TC geeft een lijst met aanleverpunten en url's terug behorende bij het brinnummer van het Bronsysteem. Daarnaast wordt ook een sessieId teruggegeven, welke uiteindelijk gebruikt zal worden ter verificatie door het Bronsysteem.Lees meer

5.3. Opvragen Document

Het Doelsysteem vraagt het dossier op van de leerling bij het Bronsysteem. De aanleverpunten die verkregen zijn in de stap Sessie Initieren worden afgelopen. De aanleverpunten worden afgelopen

volgens de procedure die beschreven is op de detailpagina van het bericht Opvragen Document. Lees meer.

5.4. Controleren Sessie

Het Bronsysteem controleert bij het Traffic Center of het sessieId geldig is. Het sessieId heeft het Doelsysteem in stap Sessie Initieren verkregen en meegestuurd naar het Bronsysteem bij de stap Opvragen Document. Het Bronsysteem voert een controleren Sessie interactie uit voor elk aanleverpunt dat bevraagd wordt. Het vermeldt hierbij in het SessiecontroleRequest welk aanleverpunt het betreft. Lees meer.

5.5. Afmelden Sessie

Het Doelsysteem meldt een door hem gestarte sessie af bij het Traffic Center. Documentdoel vermeldt hierbij het aanleverpunt dat het gevraagde document verstrekt heeft. Indien geen van de aanleverpunten een document verstrekt heeft, vermeldt Documentdoel ook geen aanleverpunt in het AfmeldingRequest. Lees meer.

6. OSO:DOSSIER KLAARZETTEN

Dit scenario beschrijft hoe een bronSysteem een dossier gereed zet voor een doelSysteem. Dit scenario geldt ook voor een binnenbrin overdracht, waarbij een RP of LAS een dossier ophaalt binnen zijn eigen brin bij een ander LAS of RP.

6.1. Context

Een bronSysteem wordt bevraagd door een doelSysteem (middels het documentRequest bericht); het initiatief voor de uitwisseling ligt bij het doelSysteem ('Pull' mechanisme). Voorafgaand aan een uitwisseling dient een eindgebruiker van het bronsysteem het dossier gereed te zetten voor verzending.

- Initiator: eindgebruiker bronsysteem
- Responder: bronSysteem(LAS of RP)
- Pre: Het bronSysteem is gekoppeld aan een gekwalificeerde instelling en heeft tenminste één aanleverpunt url geregistreerd bij het TC.
- Post: Het bronSysteem heeft het dossier klaargezet voor opvragen door het doelSysteem.

6.2. Controles voorafgaand aan het klaar zetten van een dossier

6.2.1. Dataminimalisatie

Scholen moeten zorgen dat meer gegevens worden over gedragen in het overstapdossier dan noodzakelijk is. De wet schrijft deze eis tot dataminimalisatie voor. Het wordt leveranciers sterk aanbevolen om systemen dusdanig te ontwerpen dat eindgebruikers zich aan deze eis kunnen houden.

De verzendende school is verantwoordelijk voor de inhoud van het verzonden dossier en dient de inhoud per geval te beschouwen.

6.2.2. Toestemming en inzage

- De verzendende school is verantwoordelijk voor het afwegen welke gegevens er al dan niet verstrekt moeten worden aan de aanvragende partij. Het bronsysteem dient

deze keuze te kunnen ondersteunen. OSO faciliteert alleen het beveiligd transport van deze gegevens.

- In het geval van een POVO uitwisseling dient de verzendende school voorafgaand aan verzending te controleren of ouders inzage hebben gehad in het dossiers. (Uitwisselingen binnen dezelfde instelling zijn toegestaan zonder deze inzage.) Wanneer in het dossier niet is aangegeven dat dit is ingezien door de ouders, mag er niet tot levering worden overgegaan.
- In het geval van een VO uitwisseling dient de verzendende school voorafgaand aan de verzending te controleren of de ouders toestemming hebben gegeven voor het verzenden van het dossier. anneer in het dossier niet is aangegeven dat de ouders toestemming hebben gegeven voor de verzending, mag er niet tot levering worden overgegaan.

Wanneer er sprake is van een uitwisseling binnen dezelfde school gelden deze eisen niet. (Er is geen sprake van 'externe werking' door een andere rechtpersoon.)De OSO term voor een overdracht binnen een school, dus tussen aanleverpunten met een zelfde BRIN, is een 'binnenBRIN' overdacht. Een voorbeeld hiervan is het overdragen van een dossier van een LAS naar het RI-platform van dezelfde school. Wanneer de ontvangende partij in de uitwisseling een Regionaal Initiatief is, dat niet alleen de doelschool faciliteert, maar ook optreedt als bewerker van gegevens (?verrijking? of andere scenario?s), ligt de situatie weer anders. In zo?n geval dient de controle op inzage plaats te vinden voorafgaand aan de overdracht, ook al is er sprake van een ?overdracht binnen een BRIN?.

6.2.3. Adressering

Een tweede check die OSO vereist, is het instellen door de eindgebruiker van de ontvangende partij door de verzendende school. Alleen wanneer het BRIN van de aanvragende school overeenkomt met deze waarde, mag het bronsysteem het dossier leveren.

- Opmerking #1: Een dossier moet minimaal één 'doelBRIN' hebben voordat deze verzonden mag worden, er mogen meerdere BRIN's als adres worden opgegeven.
- Opmerking #2: Het wordt aanbevolen om het samenstellen én het addresseren van dossiers te 'ontkoppelen' dusdanig dat het mogelijk is om aan de

inhoud van dossiers te werken zonder dat er een doelBRIN ingevoerd moet worden.

6.3. Gereed zetten dossier

In het bronsysteem wordt geregistreerd naar welk doelsysteem het dossier mag worden geleverd. Alleen wanneer het BRIN van de aanvrager hieraan gelijk is, mag het dossier uitgeleverd worden. Wanneer de BRIN afwijkt wordt geen dossier geleverd, maar de foutmelding ?LeveringGeweigerd? gegeven.

Een LAS of RP mag een voorselectie van doelbrin?s aanbieden aan de eindgebruiker (?meest gebruikte brins?), mits de eindgebruiker deze bevestigt. Er MOET een gebruikershandeling plaats vinden bij het instellen van het doel (het systeem mag niet automatisch kiezen).

Wanneer een bronsysteem een aanvraag krijgt tot leveren van een dossier, dan voert deze een controle uit of de ingevoerde BRIN van de vervolginstelling overeen komt met die van het aanvragende doelsysteem. Als dit het geval is, wordt het dossier verzonden, als dit niet het geval is, wordt een fout gegeven.

Een bronSysteem mag een Overstapdossier pas overdragen als de leerling (indien meerderjarig) of zijn wettelijk vertegenwoordiger(s) het Overstapdossier ingezien hebben. Per type overstap verschillen de regels betreffende het wel of niet mogen overdragen zonder akkoord. De school is verantwoordelijk voor het juist implementeren van deze regels. Hieronder zijn de verschillende type overstappen weergegeven, met de daarbij gestelde eisen:

Type overstap	Eisen	Opmerkingen
PO-PO	Ouder inzage is verplicht	
PO-VO	Ouder inzage is verplicht	
VO-VO	Toestemming ouders is verplicht	
overdrachtbinnenbrin	Ouder inzage niet verplicht.	Hierbij wordt een dossier overgedragen tussen systemen van dezelfde school. Dit type kenmerkt zich doordat de controle op inzage door ouders niet noodzakelijk is, daarnaast wordt een aantal inhoudelijke controles minder strikt toegepast.

Het scenario bestaat uit de volgende stappen:

- De documentbron toont het document ter inzage aan de leerling of zijn wettelijk vertegenwoordiger(s) via de interactie inzienDocument.
- De leerling of wettelijk vertegenwoordiger(s) verklaren zich akkoord.
- De documentbron neemt de inzage en het akkoord op in het document.

6.3.1. *Alternatieve flows*

De leerling of zijn wettelijk vertegenwoordiger(s) tekenen niet voor akkoord. De documentbron neemt de inzage, het niet-akkoord én de reden daarvoor op in het document. Het scenario eindigt.

De melding LeerlingInfoNietOpvraagbaar moet als resultaat in het documentResponse worden teruggestuurd.

6.3.2. *Bewaartermijn*

Het overstapdossier doet specifiek dienst voor de overstap van een leerling van de huidige naar een nieuwe school. Nadat de overstap is gerealiseerd, en de gegevens van de leerling in het LAS van de nieuwe school zijn ingevoerd en verwerkt, dient het overstapdossier volgens de wet nog twee jaar te worden bewaard. Daarna dient het te worden vernietigd.

	Het verzonden dossier dient twee jaar te worden bewaard (wettelijke eis)
	Na deze twee jaar dient het dossier te worden vernietigd (wettelijke eis)

Voor een leerling die is doorverwezen naar een school voor Speciaal Onderwijs geldt een bewaartermijn van drie jaar voor het overstapdossier.

7. OSO:AANSLUITING TESTEN

Op deze pagina treft u informatie aan over het testen van een aansluiting

7.1.1. Ping verzoek naar het Traffic Center

De operationele status van het Traffic Center kan opgevraagd worden met behulp van het pingRequest. Hiermee is de beschikbaarheid van de service en het versienummer van de software op het Traffic Center te controleren.
Men kan hiermee ook testen of het certificaat correct gebruikt wordt, de juiste berichtstructuur, versie, namespace etc..

7.1.2. Dossier valideren tegen het KVS

Men kan een dossier valideren tegen de Kennisnet Validatie Service. Dit is met name handig voor bronSystemen die dossiers leveren aan doelSystemen.

7.1.3. Randvoorwaarden

Er zijn een aantal randvoorwaarden waar nieuwe partijen aan moeten voldoen voordat ze aangesloten kunnen worden op OSO of het KVS.

7.1.4. Testschool

Er is een testschool beschikbaar gesteld welke fungeert als bronSysteem. Men kan met behulp van de testschool een ketentest uitvoeren. Meer informatie kan hier gevonden worden

7.1.5. Kwalificeren

De kwalificatietest is de uiteindelijke test die elke LAS/RP leverancier moet ondergaan voordat men op productie mag gaan uiwisselen. De testen die doorlopen worden, staan beschreven in het testplan. Het testplan van fase 2b (2014) kan hier gedownload worden.

De individuele scholen moeten ook los van deze kwalificatie test gekwalificeerd worden. Dit is een apart proces, welke in samenwerking met de servicedesk uitgevoerd wordt. Meer informatie kan hier gevonden worden.

7.1.6. Kwalificeren

Om de aansluiting te kunnen testen zijn er 2 testomgevingen en 1 productieomgeving beschikbaar gesteld. Hieronder zijn de endpoints van het Traffic Center per omgeving weergegeven:

Omgeving	Endpoint url	Opmerkingen
Sandbox 2B	https://tc-sandbox2b.oso-od.nl:443/traffic-center/services/overstap/	
Qualification 2B	https://tc-qualification2b.oso-od.nl:443/traffic-center/services/overstap/	Op deze omgeving vinden de kwalificatietesten plaats (zoals hierboven beschreven).
Productie 2B	https://tc.oso-od.nl:443/traffic-center/services/overstap/	Dit is de productie omgeving, waar de feitelijke uitwisselingen op plaatsvinden.

8. OSO:INZAGE OF TOESTEMMING VERLENEN

8.1. Context

- Initiator: Ouder/verzorgende (eindgebruiker bronsysteem)
- Responder: Bronsysteem (LAS of RP)
- Pre: Dossier beheerd door bronsysteem is nog niet ingezien of voorzien van toestemming voor overdracht.
- Post: Toestemming en/of inzage is geregistreerd in dossier beheerd door bronsysteem.

Een bronsysteem mag een dossier pas overdragen als de leerling (indien meerderjarig) of zijn wettelijk vertegenwoordiger(s) het dossier ingezien hebben (PO) of toestemming hebben verleend voor de overdracht (VO). (NB: Dit is een grove samenvatting van de wetten en regels die van toepassing zijn op de overdracht van een dossier. Ook de inhoud, soort leerling en benodigde zorg en de context van de overdracht zijn hierop van invloed. De inhoud van deze wiki ontslaat een verzender van een dossier niet van enige wettelijke verplichtingen!)

Dit is een bijzonder scenario, omdat het zich geheel buiten het zicht en de verantwoordelijkheid van de OSO infrastructuur plaats vindt. Daarom specificeert dit ontwerp niet hoe een LAS/RP dit scenario moet ondersteunen of hoe een school of instelling de processen dient in te richten. De reden om het scenario wel op te nemen is dat het noodzakelijk is om deze stap succesvol te doorlopen alvorens het Overstapdossier over te dragen via OSO.

NB: Er is verschil tussen akkoord voor inhoud en akkoord voor verzending:

- Akkoord voor inhoud is van belang voor verzending in het PO; het dossier dient ingezien te zijn, maar mag met of zonder akkoord op de inhoud worden verstuurd.
- Akkoord voor verzending is van belang in het VO; hier dient akkoord te zijn gegeven voor de verzending voor een dossier mag worden verstuurd.

8.2. Normal flow

1. Het bronsysteem biedt het dossier aan ter inzage aan de leerling of zijn wettelijk vertegenwoordiger(s).
2. De ouders, leerling of wettelijk vertegenwoordiger(s) verklaren zich akkoord.
3. Het bronsysteem legt de inzage en/of het akkoord vast in het dossier.

8.3. Alternatives

- De ouders, leerling of zijn wettelijk vertegenwoordiger(s) tekenen niet voor akkoord. Het bronsysteem legt de inzage, het niet-akkoord én de reden daarvoor vast in het dossier.
    - In het geval van PO mag het dossier na inzage ook wanneer er geen akkoord wordt gegeven toch verzonden worden.
    - In het geval van VO mag een dossier alleen verzonden worden als er akkoord op verzending wordt gegeven.

9. OSO:UITWISSELEN TEST SCHOOL

Er is een testschool beschikbaar gesteld welke door de diverse LAS/RP systemen gebruikt kunnen worden voor een ketentest.
De testschool fungeert als bronSysteem, wat betekent dat een LAS/RP als doelSysteem een dossier kan ophalen bij de testschool.
De testschool werkt volgens de laatste versie van de standaard (xsd, xslt en dossier) en is beschikbaar op de verschillende testomgevingen en productie.

- Initiator: doelSysteem => Het LAS of RP
- Responder: bronSysteem => De testschool
- Pre: Het LAS of RP beschikt over een geldig certificaat en wachtwoord om een testuitwisseling te kunnen doen.
- Post: Indien een bestaand bsn wordt opgevraagd ontvangt het LAS of RP een dossier van de testschool.

9.1. Overzicht beschikbare bsn's

Er zijn een aantal scenario's gedefinieerd die de verschillende alternatieve paden simuleren, zoals beschreven in het kader "Dossier opvragen".

BSN	Type flow (N, A, E*)	Resultaat	Opmerkingen
310008475	N	POPO dossier wordt uitgeleverd	
274957462	N	POVO dossier wordt uitgeleverd	
088584574	N	VOVO dossier wordt uitgeleverd	
238521436	N	binnenbrin dossier wordt uitgeleverd	Dit is een dossier met overdrachtsoort overdrachtbinnenbrin
097902378	A	LeerlinginfoNietBeschikbaar	Het dossier is niet klaargezet
334390205	A	LeerlinginfoNietOpvraagbaar	Er is geen inzage geweest van de ouders
binnenbrin	E	LeveringGeweigerd	Indien men een binnenbrin

			overdracht aanvraagt, maar de brinnrs komen niet overeen dan wordt er een leveringGeweigerd teruggegeven
overig	E	LeerlingNietBekend	Alle overige bsn's zijn niet bekend bij de testschool

* N: Normaal, A: Alternatief, E: Exceptie (fout)

Er zijn testscholen beschikbaar op de sandbox2b, qualification2b en productie omgeving.
Hieronder is per omgeving aangegeven welk brinnummer de testschool heeft.

Omgeving	**Brinnummer**
Sandbox 2B	00YY
Qualification 2B	00YY
Productie	98PO

9.2. Test BRINs

Om op productie testuitwisselingen vanuit diverse systemen uit te kunnen voeren, zonder dat administraties van scholen vervuild raken en/of 'echte' dossiers moeten worden uitgewisseld, zijn er een aantal test BRIN nummers beschikbaar. Aangezien de reeks beperkt is én vanwege de beveiliging worden deze beperkt uitgereikt en geregistreerd. Onderstaande brinnummers kunnen op productie alleen onderling uitwisselen. Vanwege juridische beperkingen is het met deze brinnummers niet mogelijk om met andere "echte" brinnummers uit te wisselen.

Brinnummer	**Schoolnaam**	**AP index**	**Pakket**	**Opmerkingen**
00SS	Testschool Magister	0	Magister Schoolmaster	Uitgereikt aan A. Miedema

10. OSO:PROTOCOL

10.1. Interfaces

De OSO interface specificatie bestaat uit twee webcontracten (wsdl's):

- http://wsdl.kennisnet.nl/oso/20140327/ELDTrafficCenter.wsdl - specificeert de communicatie tussen deelnemers en het TC
- http://wsdl.kennisnet.nl/oso/20140327/ELDDeelnemer.wsdl - specificeert de communicatie tussen deelnemers onderling
- http://xsd.kennisnet.nl/oso/Overstapservice_20140327.xsd - bevat definities die door beide wsdl's worden aangeroepen.

Een aanleverpunt dient een webservice aan te bieden conform de interface specificatie van de geldende ELDDeelnemer_<versie>.wsdl.

10.1.1. Distributie

Voor elke versie van de interface specificatie wordt een package gemaakt van de drie bestanden (ook als er maar één van de drie is aangepast) en in één(1) zip bestand geplaatst.

Binnen een OSO (project)fase is er altijd één versie van de interface specificatie geldig.

10.1.2. KVS webservice contract

Daarnaast is er een interface specificatie voor het KVS:

- Validatieservice.wsdl - specificeert de interface van het KVS
- Validatieservice.xsd - bevat de definities die binnen de KVS interface worden toegepast.

10.2. Interacties tussen systemen

Een overzicht van de ondersteunde interacties tussen systemen en het Traffic Center en achterliggende acties:

- Stap 1: Aanvraag van overdracht aan TC: Sessie Initiëren
- Stap 2: Opvragen dossier bij huidige school: Dossier Opvragen
- Stap 3: Controle aanvraag bij TC: Sessie Controleren
- Stap 4: Aanleveren dossier naar nieuwe schooL: Dossier Verzenden
- Stap 5: Afmelden aanvraag en doorgeven resultaat: Sessie Afmelden

Aanroepen en acties naast de daadwerkelijke uitwisseling:

- Dossier inzien door ouders/verzorgers
- Dossier valideren
- Notificeren van aanvraag
- Aanleverpunt Registreren
- Traffic Center Pingen

10.3. Overige technische randvoorwaarden

10.3.1. Timing

- Initiator van een interactie ontvangt binnen 30 seconden na het versturen van een request een response van het bevraagde systeem. Indien er binnen deze tijd geen response wordt ontvangen, moet de initiator een time-out (fout) afhandelen (en melden aan eindgebruiker en TC).
- Een OSO sessie heeft, indien niet eerder afgemeld, een duur van maximaal 10 minuten.
- Een systeem dat een interactie start, wacht gedurende minimaal de gespecificeerde responstijd op antwoord.

- Een systeem dat een interactie moet beantwoorden, doet dit binnen de gespecificeerde maximale responstijd.

10.3.2. Omvang berichten

Door de invoering van Passend Onderwijs en andere ontwikkelingen is er een behoefte om meer informatie in dossiers en met name bijlagen op te slana. Anderzijds is het loslaten van een bovengrens aan de dossiergrootte onverstandig uit praktische overwegingen. De volgende bestandsgrootte's zijn daarom afgesproken:

- Bijlage: maximaal 10MB (2B: 5MB)
- Compleet dossier: maximaal 30MB (2B: 15MB).

10.3.3. Logging

Een systeem bewaart de verzonden en ontvangen berichten en opgetreden fouten zodat ze in geval van calamiteiten door de leverancier op te zoeken zijn. De gelogde informatie moet redelijkerwijs voldoende zijn om technische problemen op te lossen en in speciale gevallen het verloop van de interacties te reconstrueren.

- De informatie in een logregel voor de gebruiker is voldoende zelfbeschrijvend om zonder contextinformatie uit het bronsysteem de actie te kunnen herleiden tot de verantwoordelijke (rechts)persoon.
- Een systeem registreert logregels voorzien van datum en tijd, met een nauwkeurigheid van ten minste 1 seconde.
- Een systeem garandeert een maximale afwijking van de UTC + 01:00 tijd (de tijdzone waarin Nederland valt) van 5 seconden.
- Log regels bevatten altijd het geldige sessie-id (wanneer dit is toegekend).
- Logregels voor de gebruiker kunnen na creatie niet worden aangepast of verwijderd.
- Logregels voor de gebruiker worden duurzaam bewaard en beschermd tegen verlies en verandering tot 2 jaar nadat de leerling is uitgeschreven.

11. SESSIE INITIËREN

Het Doelsysteem initieert een sessie om een dossier op te vragen bij een Bronsysteem. Het TC geeft een lijst met aanleverpunten terug (met een sessieId) of er wordt een foutmelding teruggegeven.

11.1. Context:

- Initiator: Doelsysteem (LAS of RP)
- Responder: TC
- Pre: Het Doelsysteem beschikt over een geldig certificaat en wachtwoord om dit request te kunnen versturen. Het brinnummer van het te bevragen Bronsysteem is bekend (en actief) in het deelnemersregister.
- Post: Op basis van het brinnummer van het te bevragen Bronsysteem retourneert het TC een lijst met actuele aanleverpunten en url's.
- Request:

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns="http://xml.eld.nl/schemas/Overstapservice/20140327">
   <soapenv:Header/>
   <soapenv:Body>
      <ns:overdrachtRequest>
         <ns:overdracht>
            <ns:bronBrin>98PO</ns:bronBrin>
            <ns:doelBrin>98VO</ns:doelBrin>

<ns:zoeksleutel>534534efgrt34563ery345345eferert34345</ns:zoeksl
eutel>

<ns:overdrachtsoort>overstapdossier</ns:overdrachtsoort>
         </ns:overdracht>
      </ns:overdrachtRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

Element	Uitleg	Opmerkingen
bronBrin	Dit is het brinnummer van het bronSysteem. Het TC controleert of brinnummer bekend en actief is in het deelnemersregister.	
doelBrin	Dit is het brinnummer van het Doelsysteem. Het TC controleert of het certificaat in overeenstemming is met het brinnummer welke hier opgegeven is. Daarnaast wordt ook gecontroleerd of het brinnummer van het Doelsysteem actief is in het deelnemersregister.	
zoeksleutel	Het Doelsysteem vraagt bij het Bronsysteem een dossier van een leerling op.	

	Dit gebeurt middels het bsn van de leerling. Het bsn wordt door het Doelsysteem versleuteld verstuurd naar het TC. Met behulp van het RSA algoritme wordt het bsn versleuteld. De betreffende RSA-Key is: <RSAKeyValue><Modulus>0EVKqqr5JyI4tYnOO1sDbazqyJY78rpBcvrcmbimjRkcw8ekhAiMbdFUivSqfWhkpQ1knwVKURccH5oaSdhaXptg+9QcBqbC0p3SLym7f3hyeLCJvxNEV4JPZ7L5GbnsC8Ux5HxLinW/B6mF8jMYh5du5X7OKytNA2qlGdwe7qM=</Modulus> <Exponent>AQAB</Exponent> </RSAKeyValue>	
overdrachtsoort	Hier wordt onderscheid gemaakt tussen een normale overdracht en een binnenbrin overdracht. Indien het een normale overdracht betreft, dan moet hier de waarde overstapdossier worden gebruikt. Bij een binnenbrin overdracht moet de waarde overdrachtbinnenbrin worden gebruikt.	Het brinnummer van het bronBrin en doelBrin moet hetzelfde zijn voor een binnenbrin overdracht.

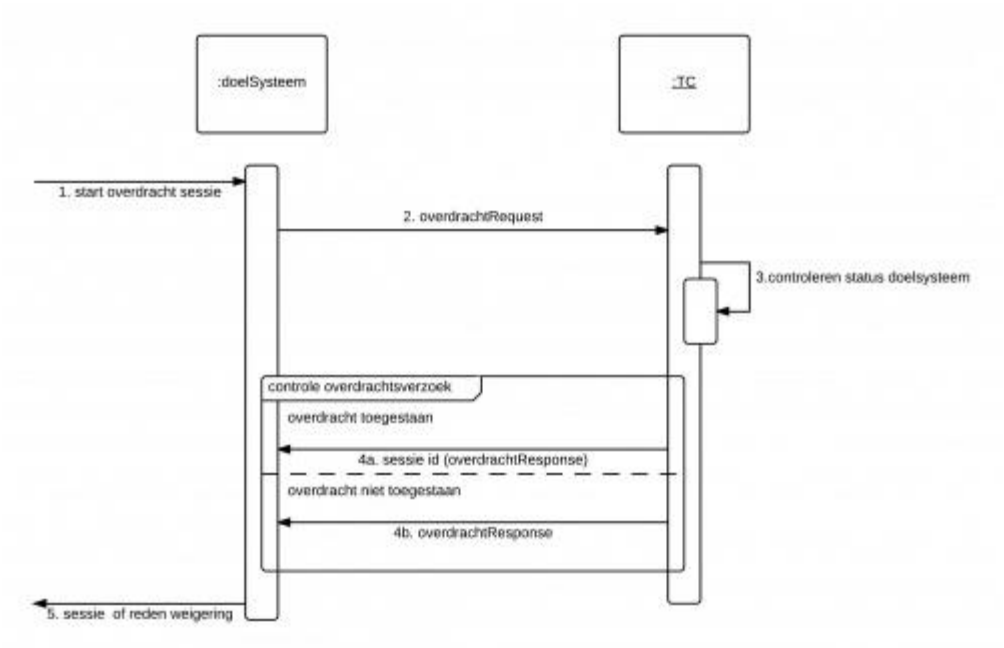
- Response:

```
<SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/">
   <SOAP-ENV:Header/>
   <SOAP-ENV:Body>
      <over:overdrachtResponse
xmlns:over="http://xml.eld.nl/schemas/Overstapservice/20140327">
         <over:overdracht>
            <over:aanleverpunt>
               <over:code>0</over:code>

<over:url>https://start.parnassys.net/bao/services/cxf/elddeelne
mer/20140327</over:url>
               <over:type>LAS</over:type>
               <over:label>98PO0000 LAS OSO-PO school
test</over:label>
            </over:aanleverpunt>
            <over:aanleverpunt>
               <over:code>1</over:code>

<over:url>https://tester.bks.kennisnet.nl/productieDemoSchool.ph
p</over:url>
               <over:type>LAS</over:type>
               <over:label>98PO0001 LAS OSO-PO
school</over:label>
            </over:aanleverpunt>
            <over:sessieId>cf156279-6599-4d23-a0c7-
96977da0a53e</over:sessieId>
         </over:overdracht>
      </over:overdrachtResponse>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Element	Uitleg	Opmerkingen
code	Dit is het aanleverpuntnummer	Alleen de aanleverpunten, waarvoor ook

	van het opgevraagde bronBrin. Er kunnen meerdere aanleverpunten geregistreerd zijn voor een bronBrin.	een url is geregistreerd worden hier teruggegeven.
url	Dit is de url van het aanleverpuntnummer.	De url voldoet wordt door het Bronsysteem geregistreerd middels het bericht registreren aanleverpunt (verwijzing...)
type	Dit beschrijft de type van het aanleverpunt. Het aanleverpunt kan van het type LAS of RIS zijn.	
label	Het formaat van het label veld is: <BRIN> <Vestiging> <AP> <Naam van School> <type> <beschrijving>.... Hier klopt iets nog niet.. Zie Response van bericht..	BRIN : BRIN van school (bestuur). Vestiging: Vestigingscode (of ?00? in geval van hoofd- of vestiging). AP: De aanleverpunt index (twee cijfers). Naam van school, welke geregistreerd is in Officeheart. Type: LAS of RP. Beschrijving: Vrij tekstveld (50 karakters) dat school zelf kan invullen op mijn OSO.
sessieId	Het sessieId welke gegenereerd is door het TC.	

11.2. Sequence diagram Sessie Initiëren



11.3. Normal flow:

(1)De flow start met de behoefte van het doelSysteem om een dossier op te vragen bij een bronSysteem.

(2)Het doelsysteem vraagt bij het Traffic Center een sessie aan (overdrachtRequest).
(3)Het TC controleert of het doel- en bronSysteem beide bekend en actief zijn in het deelnemersregister
(4)Afhankelijk van het resultaat van deze controle wordt door het TC (via een overdrachtResponse>

- ofwel een lijst met aanleverpunten en sessie teruggegeven[4a]
- ofwel een melding teruggegeven met de reden van afwijzing[4b].

11.4. Alternatives:

De volgende alternatives beschrijven waarom een overdracht niet toe wordt gestaan:
.

- AanvragerNietBekend: De BRIN/AP index combinatie van het doelsysteem is niet bekend in de TC database.

Mogelijke oorzaken: Het aanleverpunt is niet aangemaakt in de backoffice of deze informatie is vanuit de backoffice nog niet doorgeleverd aan het Traffic Center.

- AanvragerNietBeschikbaar: Het doelsysteem is bekend bij het TC, maar (nog) niet toegelaten op het OSO netwerk.

Mogelijke oorzaken: Het aanleverpunt is aangemaakt in de back office en doorgegeven aan het TC. De school kan (nog) niet gekwalificeerd zijn of het aanleverpunt is op inactief gesteld.

- VerstrekkerNietBekend: De BRIN/AP index combinatie van het bronsysteem is niet bekend in de TC database.

Mogelijke oorzaken: Het aanleverpunt is niet aangemaakt in de backoffice of deze informatie is vanuit de backoffice nog niet doorgeleverd aan het Traffic Center.

- VerstrekkerNietBeschikbaar: Het bronsysteem is bekend bij het TC, maar (nog) niet toegelaten op het OSO netwerk

of er zijn nog geen urls geregistreerd (er moet minimaal 1 url geregistreerd zijn).

Mogelijke oorzaken: Het aanleverpunt is aangemaakt in de back office en doorgegeven aan het TC. De school kan (nog) niet gekwalificeerd zijn of het aanleverpunt is op inactief gesteld.

- GeenRelatieMetDoel: Als overdrachtsoortis de waarde "overdrachtbinnenbrin" gekozen, echter de bron- en doelBrin verschillen.

11.5. Exceptions:

- OverdrachtReedsActief: Er is al een sessie aangevraagd voor de overdracht van dit specifieke dossier en deze aanleverpunten.

Na 10 minuten verloopt de sessie. De gebruiker kan het na deze tijd opnieuw proberen of de sessie afmelden met behulp van het afmeldRequest (verwijzing)..

11.6. Overzicht meldingen

Resultaat	Type flow (N, A, E*)	Omschrijving
Sessie toegekend	N	Sessie id met lijst actuele ap's van bron verstrekt door TC
AanvragerNietBekend	A	Doelsysteem (aanvragend AP) is niet bekend bij het Traffic Center
AanvragerNietBeschikbaar	A	Doelsysteem (aanvragend AP) is (nog) niet gerechtigd om gebruik te maken van de overstapservice
VerstrekkerNietBekend	A	Bronsysteem is niet bekend bij het Traffic Center
VerstrekkerNietBeschikbaar	A	Bronsysteem is niet gerechtigd om de overstapservice te gebruiken.
GeenRelatieMetDoel	A	overdrachtSoort in overdrachtsRequest is "overdrachtbinnenbrin", echter de bron- en doelBrin verschillen.
OverdrachtReedsActief	E	Er is reeds een sessie actief voor dezelfde parameters.

* N: Normaal, A: Alternatief, E: Exceptie (fout)

12. DOSSIER OPVRAGEN

Dit scenario beschrijft hoe een Doelsysteem een dossier opvraagt bij een Bronsysteem. Dit scenario geldt ook voor een binnenbrin overdracht, waarbij een RP of LAS een dossier ophaalt binnen zijn eigen brin bij een andere LAS of RP.

Het proces wordt geïnitieerd door het Doelsysteem en wordt uiteindelijk ook afgemeld door het Doelsysteem.

12.1. Context:

Het Doelsysteem haalt een dossier op bij een Bronsysteem middels het documentRequest bericht. Het Doelsysteem weet welk bsn de leerling heeft en bij welk brinnummer het dossier opgevraagd kan worden.

- Initiator: Doelsysteem (LAS of RP)
- Responder: Bronsysteem (LAS of RP)
- Pre: Verondersteld wordt dat het Doelsysteem beschikt over een geldig certificaat en actief brinnummer binnen het TC. Het Bronsysteem heeft een actief brinnummer binnen het TC en heeft tenminste één aanleverpunt url geregistreerd.
- Post: Het Doelsysteem heeft het dossier ontvangen van het Bronsysteem.

12.2. Aflopen aanleverpunt:

Een school kan van meerdere gescheiden administratie systemen gebruik maken. Voor elk administratiesysteem hoort een aanleverpunt geregistreerd te worden in het TC. Per aanleverpunt wordt er onderscheid gemaakt tussen een RI en een LAS.

Indien een doelSysteem meerdere aanleverpunten heeft en er wordt ook gebruik gemaakt van één of meerdere RI's, dan is de volgende procedure voorgeschreven:

1. Bevraag een aanleverpunt van type ?RI? <wanneer er geen aanleverpunten van type ?RI? zijn, ga naar stap .5>

2. Wanneer een RI aanleverpunt een geldig dossier uitlevert, dan wordt dit geïmporteerd en worden de verdere aanleverpunten niet bevraagd <ga naar stap .9>
3. Wanneer een RI aanleverpunt de foutmelding ?LeerlinginfoNietOpvraagbaar? of ?LeerlinginfoNietBeschikbaar? teruggeeft, stopt het Doelsysteem met het aflopen van de overige aanleverpunten. <ga naar stap .9>
4. Start bevraging volgend aanleverpunt van type ?RI?<ga naar stap .1>
5. Bevraag een aanleverpunt van type ?LAS? <wanneer er geen aanleverpunten van type ?LAS? zijn, ga naar stap .9>
6. Wanneer een LAS aanleverpunt een geldig dossier uitlevert, dan wordt dit geïmporteerd en worden de verdere LAS aanleverpunten niet bevraagd <ga naar stap .9>
7. Wanneer een LAS aanleverpunt de foutmelding ?LeerlinginfoNietOpvraagbaar? of ?LeerlinginfoNietBeschikbaar? teruggeeft, stopt het Doelsysteem met het aflopen van de overige aanleverpunten. <ga naar stap .9>
8. Start bevraging volgend aanleverpunt van type ?LAS? <ga naar stap .5>
9. Einde van aflopen aanleverpunten

12.3. Meervoudige ontvangst

Doelsystemen moeten om kunnen gaan met meerdere leveringen van hetzelfde dossier (identiek bsn) en deze correct kunnen afhandelen.Uitgangspunten hierbij zijn:

- importeren leidt niet tot gegevensverlies
- balans tussen bruikbaarheid en gebruiksvriendelijkheid.

De verwerking van een volgende versie van een nieuw dossier is een complexe use case die we binnen OSO niet kunnen en ook niet willen uitspecificeren en voorschrijven tot de laatste stap en het kleinste detail veld. Leveranciers en scholen zullen hier zelf hun keuzen en uitwerkingen in moeten vinden.

- Request:

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns="http://xml.eld.nl/schemas/Overstapservice/20140327">
   <soapenv:Header/>
   <soapenv:Body>
      <ns:documentRequest>
         <ns:overdracht>
            <ns:bronBrin>98PO</ns:bronBrin>
            <ns:doelBrin>98VO</ns:doelBrin>

<ns:zoeksleutel>534534efgrt34563ery345345eferert34345</ns:zoeksl
eutel>

<ns:overdrachtsoort>overstapdossier</ns:overdrachtsoort>
         </ns:overdracht>
         <ns:aanleverpuntId>1</ns:aanleverpuntId>
         <ns:sessieId>cf156279-6599-4d23-a0c7-
96977da0a53e</ns:sessieId>
         <ns:pgn>
            <ns:bsn>112233445</ns:bsn>
         </ns:pgn>
      </ns:documentRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

Element	Uitleg	Opmerkingen
bronBrin	Dit is het brinnummer van het bronSysteem.	
doelBrin	Dit is het brinnummer van het Doelsysteem.	
zoeksleutel	Dit is de versleutelde bsn	Dit moet exact overeenkomen met de zoeksleutel, welke ook gebruikt is in het overdrachtsRequest.
overdrachtsoort	Dit bepaalt om wat voor soort overdracht het gaat, een overstapdossier of overdrachtbinnenbrin.	De overdrachtsoort wordt overeenkomen met de overdrachtsoort welke gebruikt is in het overdrachtsRequest. Het brinnummer van het bron- en doelBrin moet hetzelfde zijn voor een binnenbrin overdracht.
aanleverpuntId	Het aanleverpunt van het bronSysteem	Dit aanleverpunt moet teruggegeven zijn in de overdrachtsResponse.
sessieId	De sessieId die verkregen is in de overdrachtsResponse.	
bsn	De bsn van de leerling	Dit wordt onversleuteld verstuurd in het documentRequest.

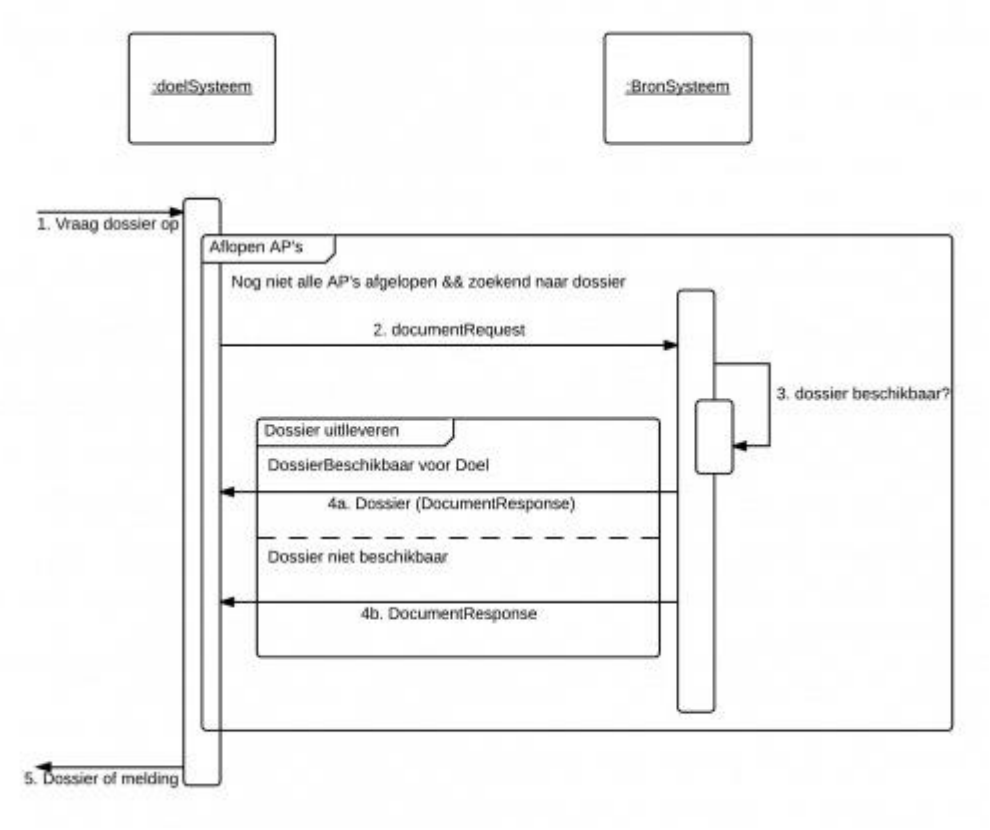
- Response

```
<SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns1="http://xml.eld.nl/schemas/Overstapservice/20140327">
   <SOAP-ENV:Body>
```

```
      <ns1:documentResponse
xmlns="http://www.edustandaard.nl/oso_gegevensset/1.1/dossier">
         <ns1:dossier>
            <dossier>
               .........
         </dossier>
         </ns1:dossier>
      </ns1:documentResponse>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Element	Uitleg	Opmerkingen
Dossier	Het dossier van de leerling	Indien het dossier van de leerling niet verstrekt kan worden, wordt er een melding weergegeven

12.4. Sequence diagram Dossier opvragen



(1) De flow start met het opvragen van een dossier binnen een doelsysteem.
(2)Vervolgens stuurt het doelsysteem rechtstreeks een verzoek(DocumentRequest) naar het aanleverpunt van de huidige instelling (indien er meerdere aanleverpunten zijn, dan wordt dit verzoek meerdere malen herhaald.
NB:

- Het TC is niet direct betrokken bij het ophalen van een dossier.
- De lijst met aanleverpunten (door het TC verstrekt) wordt afgelopen, zie informatie onder aflopen aanleverpunten.

(3)Het bronSysteem van het desbetreffende aanleverpunt controleert of het aangevraagde dossier bekend en beschikbaar is.
(4)Het bronSysteem beantwoordt het verzoek (met het DocumentResponse)door

- ofwel het desbetreffende dossier[4a] te versturen
- ofwel een melding[4b] te geven.

Op basis van deze response besluit het doelsysteem om:

- het aflopen te staken omdat het dossier is ontvangen of het bronsysteem een melding geeft die het verder bevragen niet meer nodig maakt
- een volgend aanleverpunt te bevragen.

12.5. Alternatives:

- Geen van de bevraagde aanleverpunten levert een dossier uit. Dit kan de volgende oorzaken hebben:
  - Geen van de aanleverpunten kent het dossier
  - Geen van de aanleverpunten heeft een dossier beschikbaar (nog niet gereed of nog geen toestemming voor overdracht)
  - Geen van de aanleverpunten heeft het dossier beschikbaar gesteld voor dit doelsysteem (BRIN niet ingevuld)

12.6. Exceptions:

12.7. Overzicht meldingen

Resultaat	Type flow (N, A, E*)	Omschrijving
<Document>	N	Het gevraagde document.
LeveringInBehandeling	A	Het bronsysteem kan niet bepalen of het dossier beschikbaar of bij haar bekend is.
LeerlinginfoNietOpvraagbaar	A	Het document mag niet worden verstrekt,

		omdat de ouders/leerling geen toestemming verlenen.
LeerlinginfoNietIngezien	A	Het document mag (nog) niet worden verstrekt, omdat de ouders nog geen inzage hebben gehad.
LeerlinginfoNietBeschikbaar	A	Het document is (nog) niet klaargezet voor overdracht.
LeveringGeweigerd	A	Het dossier van de leerling wordt klaargezet voor een specifiek brinnr. Het document wordt door de bron niet uitgeleverd aan het doelSysteem, omdat het brin van het doelSysteem niet overeenkomt met de in het bronsysteem gespecificeerde brinnr.
LeerlingNietBekend	A	De leerling met de opgegeven bsn is niet bekend bij het bronSysteem.
AuthenticatieVerstrekkerMislukt	E	Het bronSysteem heeft zich niet kunnen authenticeren bij het Traffic Center. doelSysteem hoeft hierop geen actie te ondernemen
SessieOngeldig	E	De sessie is ongeldig; het ID is nooit uitgedeeld. Dit is het resultaat van de sessieControle
SessieAfwijkend	E	De overstapuitvraag wijkt af van die, waarmee de sessie verkregen is. Dit is het resultaat van de sessieControle
SessieReedsAfgemeld	E	De sessie is al afgemeld en dus niet langer geldig. Dit is het resultaat van de sessieControle
SessieVerlopen	E	De sessie is verlopen; de time-out is verstreken. Dit is het resultaat van de sessieControle

* N: Normaal, A: Alternatief, E: Exceptie (fout)

13. DOSSIER VERZENDEN

13.1. Context

Een bronSysteem wordt bevraagd door een doelSysteem (middels het documentRequest bericht); het initiatief voor de uitwisseling ligt bij het doelSysteem ('Pull' mechanisme). Het doelSysteem weet welk bsn de leerling heeft en bij welk brinnummer het dossier opgevraagd kan worden.

- Initiator: doelSysteem
- Responder: bronSysteem(LAS of RP)
- Pre: Het bronSysteem is gekoppeld aan een gekwalificeerde instelling en heeft tenminste één aanleverpunt url geregistreerd bij het TC.
- Post: Het bronSysteem heeft het dossier verzonden naar het aanvragende doelsysteem.

Dossier verzenden is de response op het aanvragen van het dossier door het doelsysteem en de complete transactie en interactie tussen bron- en doel- systeem wordt daar beschreven. Voorafgaand aan het verzenden van een dossier dient het bronsysteem de volgende checks uitgevoerd te hebben:

- registratie inzage/toestemming van ouders/verzorgers.: inzage of toestemming moet geregistreerd zijn en in geval van toestemming op 'ja' zijn ingesteld.
- adressering van dossier naar doelBRIN.: er moet minimaal één 'doelBRIN' gespecificeerd zijn bij het dossier en deze moet overeen komen met de BRIN van het aanvragende doelsysteem.
- validatie van dossier.: het dossier moet voldoen qua vorm en inhoud aan de eisen van de geldende versie van de OSO Standaard OSO.

Pas als voldaan is aan al deze eisen mag het dossier door het bronsysteem worden verzonden naar het doelsysteem.

13.2. Sessiecontrole door Bronsysteem

Elk aanleverpunt van Bronsysteem controleert of de verkregen sessieID valide is door de interactie controleren sessie te starten. Het aanleverpunt stuurt hierbij zijn eigen BRIN, zijn code (van het aanleverpunt dus), het brin van doelSysteem en de sessieID. Het TC antwoordt hierop bevestigend tenzij het een afwijking constateert. Het TC geeft ook de sector terug van Doelsysteem.

13.3. Alternatives:

- Een bronsysteem kan het dossier niet verzenden:
  - Het bronsysteem kan niet (tijdig) vaststellen of het dossier beschikbaar is
  - Het het dossier is niet bekend bij het bronsysteem
  - Het dossier is (nog) niet beschikbaar (nog niet gereed of nog geen toestemming voor overdracht)
  - Het dossier is (nog) niet beschikbaar voor dit doelsysteem (BRIN niet ingevuld)

De correcte response die een bronsysteem in uitzonderingsgevallen naar het bronsysteem dient te versturen, zijn beschreven bij de dossier opvragen interactie.

14. SESSIE CONTROLEREN

Het Bronsysteem controleert bij het TC of het DoelSysteem mag communiceren met het BronSysteem. Indien de communicatie is toegestaan, geeft het TC als positief resultaat de sector terug van het DoelSysteem. Als de communicatie wordt geweigerd dan wordt er een foutmelding teruggegeven.

14.1. Context:

- Initiator: bronSysteem (LAS of RP)
- Responder: TrafficCenter
- Pre: bronSysteem heeft een documentRequest ontvangen van het doelSysteem. In het documentRequest staat de sessieId.
- Post: TC bevestigt geldigheid sessie (sessie id uit DocumentRequest) en geeft aan dat bronSysteem en doelSysteem met elkaar mogen communiceren of geeft een foutmelding.
- Request:

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns="http://xml.eld.nl/schemas/Overstapservice/20140327">
   <soapenv:Header/>
   <soapenv:Body>
      <ns:sessiecontroleRequest>
         <ns:overdracht>
            <ns:bronBrin>98PO</ns:bronBrin>
            <ns:doelBrin>98VO</ns:doelBrin>

<ns:zoeksleutel>534534efgrt34563ery345345eferert34345</ns:zoeksl
eutel>

<ns:overdrachtsoort>overstapdossier</ns:overdrachtsoort>
         </ns:overdracht>
         <ns:aanleverpunt>01</ns:aanleverpunt>
         <ns:sessieId>cf156279-6599-4d23-a0c7-
96977da0a53e</ns:sessieId>
      </ns:sessiecontroleRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

Element	Uitleg	Opmerkingen
bronBrin	Dit is het brinnummer van het	

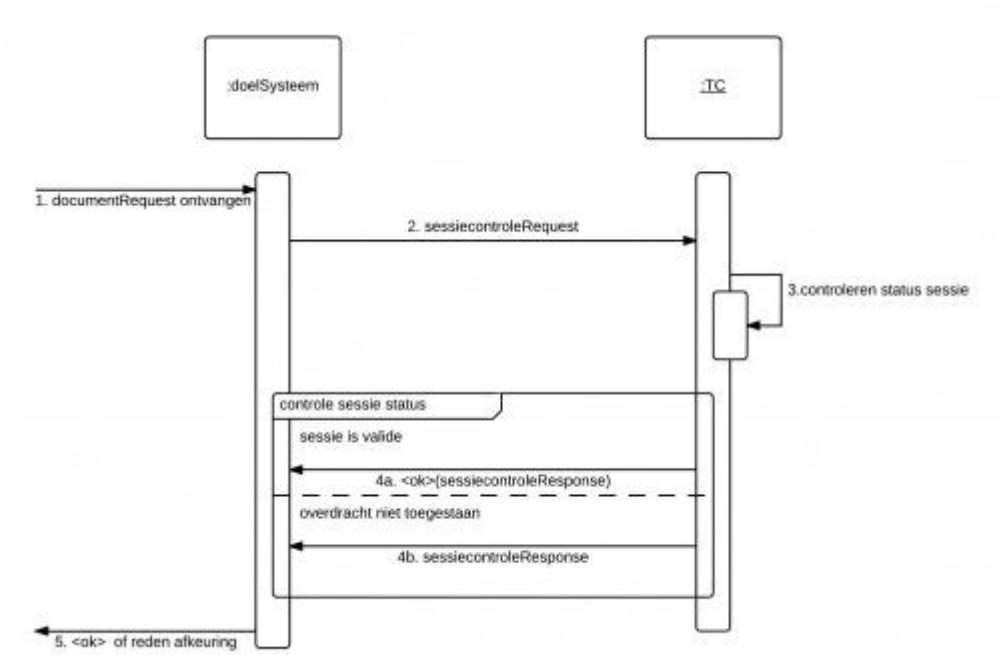
	bronSysteem. Het TC controleert of het certificaat in overeenstemming is met het brinnummer welke hier opgegeven is en of het brinnummer bekend en actief is in het deelnemersregister.	
doelBrin	Dit is het brinnummer van het Doelsysteem. Het TC controleert of brinnummer bekend en actief is in het deelnemersregister.	
zoeksleutel	De zoeksleutel wordt overgenomen vanuit het documentsRequest.	
overdrachtsoort	De overdrachtsoort wordt overgenomen vanuit het documentsRequest.	Het brinnummer van het bron- en doelBrin moet hetzelfde zijn voor een binnenbrin overdracht.
aanleverpunt	Het aanleverpunt van het bronSysteem	Dit aanleverpunt moet teruggegeven zijn in de overdrachtsResponse en via het documentsRequest zijn ontvangen. Daarnaast moet het corresponderen met het certificaat welke het bronSysteem gebruikt.
sessieId	De sessieId die verkregen is in de overdrachtsResponse en via het documentsRequest is ontvangen.	

- Response

```
<SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/">
   <SOAP-ENV:Header/>
   <SOAP-ENV:Body>
      <over:sessiecontroleResponse
xmlns:over="http://xml.eld.nl/schemas/Overstapservice/20140327">
         <over:sectorAanvrager>VO</over:sectorAanvrager>
      </over:sessiecontroleResponse>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Element	Uitleg	Opmerkingen	
sectorAanvrager	De sector van het doelSysteem wordt teruggegeven door het TC.	Voorheen werd er door het bronSysteem een controle uitgevoerd op sector. Dit is niet meer van toepassing. Echter er wordt als positief resultaat nog steeds de sector teruggegeven van het doelSysteem.	Indien het resultaat van de controle negatief is, dan wordt er een fout weergegeven.

14.2. Sequence diagram Sessie Initiëren



14.3. Normal flow:

(1) De flow start na de ontvangst van een DocumentRequest bij het bronsysteem.
(2) Het bronsysteem verstuurt een sessieControleRequest naar het Traffic Center.
(3) Het TC beoordeelt de inhoud van het request en controleert of de opgegeven sessie bekend en geldig is. Daarnaast controleert het TC ook of bron- en doelSysteem beide bekend en actief zijn.
(4) Afhankelijk van het resultaat van deze beoordeling retourneert het TC (via een sessieControleResponse)

- een bevestiging dat de sessie valide is [4a]
- ofwel een melding dat de sessie niet valide is met de reden van afwijzing[4b].

14.4. Alternatives:

- SessieAfwijkend: De aangeleverde overstapinformatie wijkt af van die, waarmee de sessie verkregen is.

- OnbekendAanleverpunt: Er is in de 'SessiecontroleRequest' een aanleverpunt gebruikt, dat niet in de bijbehorende 'OverdrachtResponse' verkregen is
- GeenRelatieMetDoel: Het Traffic Center krijgt een aanvraag van het type "overdrachtbinnenbrin" terwijl de brins verschillen.
- SessieReedsAfgemeld: De sessie is al afgemeld
- VerstrekkerNietBekend: Documentbron is niet aanwezig in het deelnemersregister
- VerstrekkerNietBeschikbaar: Documentbron is (nog) niet gerechtigd om gebruik te maken van de overstapservice.

14.5. Exceptions:

- SessieOngeldig: De sessie is ongeldig; het ID is nooit uitgedeeld of het sessieId klopt niet
- SessieVerlopen: De sessie is verlopen; de time-out is verstreken

14.6. Overzicht meldingen

Resultaat	Type flow (N, A, E*)	Omschrijving
Sessie is valide	N	De sector van het doelSysteem wordt teruggegeven als resultaat.
SessieAfwijkend	A	De combinatie bron/doel brin, overdrachtsoort en zoeksleutel moeten hetzelfde zijn als in het overdrachtsRequest.
OnbekendAanleverpunt	A	Aanleverpunt komt niet overeen met datgene wat in het overdrachtsRequest is gebruikt. Indien het aanleverpunt niet overeenkomt met het certificaat van het bronSysteem, dan wordt er een client certificate foutmelding weergegeven.
GeenRelatieMetDoel	A	Indien overdrachtsoort overdrachtbinnenbrin betreft, maar doel- en bronbrin wijken af
SessieReedsAfgemeld	A	Er is al een afmeldingsbericht richting het TC gestuurd van het doelSysteem.
VerstrekkerNietBekend	A	Bronsysteem is niet bekend bij het Traffic Center
VerstrekkerNietBeschikbaar	A	Bronsysteem is niet gerechtigd om de overstapservice te gebruiken.
SessieOngeldig	E	Het sessieId komt niet overeen met datgene wat verstrekt is in het overdrachtsResponse.
SessieVerlopen	E	Het sessieId is verlopen. Na 10 minuten

verloopt de sessie.

* N: Normaal, A: Alternatief, E: Exceptie (fout)

15. SESSIE AFMELDEN

Het doelSysteem meldt de sessie af na het ontvangen van een antwoord van het bronSysteem.

15.1. Context:

- Initiator: Doelsysteem (LAS of RP)
- Responder: TrafficCenter
- Pre: Sessie-id toegekend door TC aan doelsysteem.
- Post: Sessie afgesloten op TC (inclusief logging)
- Request:

Bericht moet nog aangepast om veld 'status' te faciliteren

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns="http://xml.eld.nl/schemas/Overstapservice/20140327">
   <soapenv:Header/>
   <soapenv:Body>
      <ns:afmeldingRequest>
         <ns:aanleverpunt>0</ns:aanleverpunt>
         <ns:sessieId>cf156279-6599-4d23-a0c7-
96977da0a53e</ns:sessieId>
      </ns:afmeldingRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

Element	Uitleg	Opmerkingen
aanleverpunt	Dit is het aanleverpuntnummer van het bronSysteem, welke als laatste een antwoord terug heeft gestuurd naar het doelSysteem.	Er kunnen meerdere aanleverpunten bevraagd zijn.
sessieId	Dit is de sessieId die ontvangen is in de overdrachtsResponse en gebruikt is in de communicatie met het bronSysteem.	
overdrachtResultaat	Dit is de status die het doelsysteem heeft ontvangen bij het aflopen van de aanleverpunten bij het opvragen van een dossier.	Bij meerdere aanleverpunten wordt het 'beste resultaat' doorgegeven, bepaald door de hoogste plaats in de tabel meldingen bij dossier opvragen.

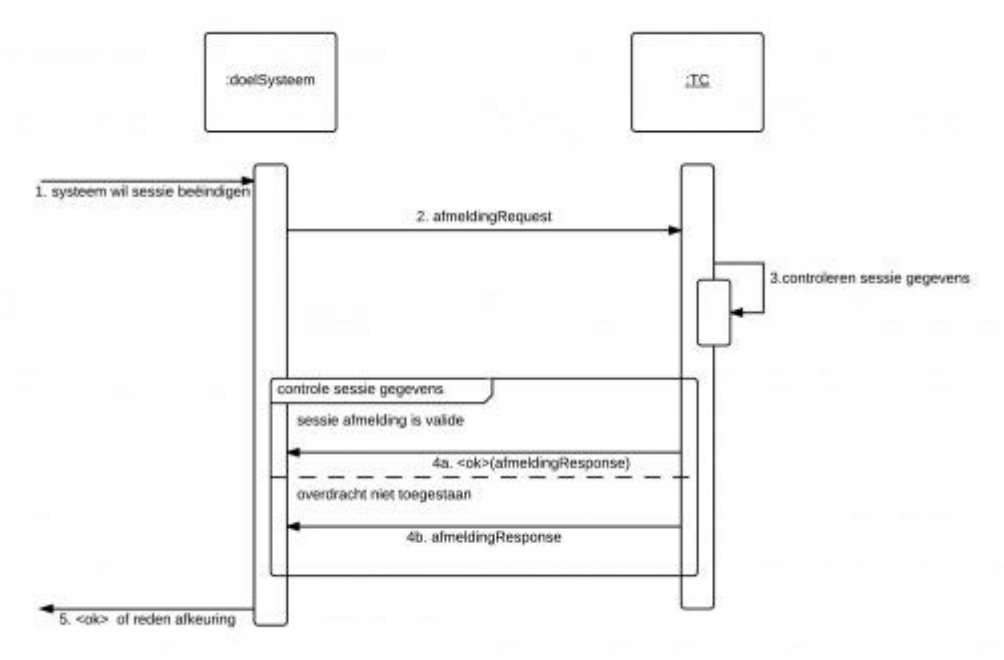
- Response:

```
<SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/">
```

```
   <SOAP-ENV:Header/>
   <SOAP-ENV:Body>
      <over:afmeldingResponse
xmlns:over="http://xml.eld.nl/schemas/Overstapservice/20140327">
         <over:resultaat>OverdrachtGeslaagd</over:resultaat>
      </over:afmeldingResponse>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Element	Uitleg	Opmerkingen
Resultaat	Indien de sessie correct is afgemeld, dan wordt het resultaat "Overdrachtgeslaagd" teruggegeven.	Er wordt een foutmelding teruggegeven indien de sessie niet correct is afgemeld.

15.2. Sequence diagram Sessie Initiëren



(1)De flow start met de behoefte aan het afmelden van een sessie in het doelsysteem.
(2)Het doelSysteem meldt bij het Traffic Center een toegekende sessie af (AfmeldingRequest).
(3)Binnen het TC wordt gecontroleerd of de sessie bekend is, wat de status hiervan is en de relatie met het doelsysteem.
(4)Afhankelijk van het resultaat van deze controle wordt door het TC (via een AfmeldingResponse>

- ofwel een bevestiging van de verwerking van de afmelding[4a]
- ofwel een melding teruggegeven [4b].

15.3. Alternatives:

- OnbekendAanleverpunt: Er is in het 'afmeldRequest' een aanleverpunt gebruikt, welke niet in de overdrachtResponse verkregen is.
- SessieNietGecontroleerd: De aangeleverde overstapinformatie wijkt af van die, waarmee de sessie verkregen is.
- AanvragerNietBekend: Documentdoel is niet aanwezig in het deelnemersregister
- AanvragerNietBeschikbaar: Documentdoel is (nog) niet gerechtigd om gebruik te maken van de overstapservice.

15.4. Exceptions:

- SessieOngeldig: De sessie is ongeldig; het ID is nooit uitgedeeld of het sessieId klopt niet
- SessieVerlopen: De sessie is verlopen; de time-out is verstreken
- SessieReedsAfgemeld: De sessie is al afgemeld.

15.5. Overzicht meldingen

Resultaat	Type flow (N, A, E*)	Omschrijving
OverdrachtGeslaagd	N	Indien de sessie correct is afgemeld, dan wordt deze melding weergegeven.
OnbekendAanleverpunt	A	Het aanleverpunt in het AfmeldingRequest is niet aan documentdoel verstrekt in de bijbehorende 'OverdrachtResponse' (zie scenario ?Overdracht document?).
SessieNietGecontroleerd	A	Bij de sessiecontrole door het opgegeven aanleverpunt is door het TC een sessiefout geconstateerd.
AanvragerNietBekend	A	Doelsysteem is niet bekende bij hetTraffic Center
AanvragerNietBeschikbaar	A	Doelsysteem is (nog) niet gerechtigd om gebruik te maken van de overstapservice
SessieOngeldig	E	De sessie is ongeldig; het sessie id is nooit uitgedeeld
SessieFout	E	De sessie ID bestaat, maar de aanvraag informatie wijkt af van die uit de sessie aanvraag
SessieReedsAfgemeld	E	De sessie is al eerder afgemeld.
SessieVerlopen	E	De sessie is verlopen; de sessie-time-out is verstreken

[*] N: Normaal, A: Alternatief, E: Exceptie (fout)

16. DOSSIER INZIEN

Voorafgaand aan het verzenden van een dossier is de huidige school verplicht ouders inzage te geven in het dossier (PO) dan wel de toestemming van ouders te krijgen/registreren (VO). Zie voor meer informatie: Eisen aan organisatie en proces.

- Context: Dit is een bijzonder scenario, omdat het zich geheel buiten het zicht en de verantwoordelijkheid van de Overstapservice afspeelt. Daarom specificeert dit ontwerp niet hoe een school dit scenario moet implementeren. Dat zou op papier, via een portal of mogelijk nog anderszins kunnen. De reden om het scenario wel op te nemen is dat het noodzakelijk is om ?Inzien document? succesvol te doorlopen alvorens het Overstapdossier over te dragen in het scenario ?Overdracht Overstapdossier?.
- Initiator: De ouder/verzorger van een leerling (of de leerling zelf) (eindgebruiker van bronsysteem).
- Responder: Bronsysteem
- Pre: Het LAS of RP heeft een dossier van de betreffende leerling in beheer.
- Post: Het dossier is ingezien en (in geval van VO) er is toestemming verleend voor verzending
- Request:

In dit scenario:

- vervult het LAS of het RI ?systeem van de huidige school van de leerling de rol documentbron;
- is het document een Overstapdossier.

- Normal flow:

Het scenario bestaat uit de volgende stappen:

(1) De documentbron toont het document ter inzage aan de leerling of zijn wettelijk vertegenwoordiger(s)
(2) De leerling of wettelijk vertegenwoordiger(s) verklaren zich akkoord met de inhoud (PO) of geven toestemming voor verzending (VO).

(3) De documentbron neemt de inzage en het akkoord op in het dossier.

- Alternative #1: Niet akkoord met inhoud (PO)

  (2) De leerling of wettelijk vertegenwoordiger(s) verklaren zich niet akkoord met de inhoud (PO)
  (3) De documentbron noteert de inzage en het bezwaar en de redenen daarvoor op in het dossier.

- Alternative #2: Niet akkoord met verzending (VO)

  (2) De leerling of wettelijk vertegenwoordiger(s) verklaren zich niet akkoord met verzending van het dossier (VO)
  (3) De documentbron noteert de inzage en het bezwaar en de redenen daarvoor op in het dossier. Documentbron blokkeert het dossier voor verzending.

17. DOSSIER VALIDEREN

17.1. Valideren dossier voorafgaand aan verzending

Om de kwaliteit in te keten te borgen moeten dossiers voorafgaand aan verzending gevalideerd worden. De validatie controleert het voldoen aan de EduStandaard OSO en bestaat uit twee delen:

- het dossier dient qua ?vorm? te voldoen aan de specificatie gevalideerd tegen de xsd
- de inhoud van het dossier wordt (beperkt) gevalideerd door de xslt

De xsd en xslt worden beheerd en verstrekt vanuit de [EduStandaard OSO].

In OSO?15 is gekozen om twee varianten van deze controle te ondersteunen:

- centrale controle bij de Kennisnet Validatie Service
- lokale validatie in het eigen systeem.

De lokale validatie variant is nieuwe en houdt in dat leverende systemen voorafgaand aan verzending het dossier binnen hun eigen omgeving valideren. Daarbij dient gebruikt te worden gemaakt van de correcte versie van de xsd en xslt. Kennisnet zorgt voor de beschikbaarheid van deze bestanden.

Een bronsysteem dient één van de twee validatie varianten te implementeren.

18. AANVRAAG NOTIFICEREN

18.1. Notificatie dossier aanvraag

Bronsystemen slaan binnen komende verzoeken tot het leveren van een dossier op. Deze verzoeken moeten door eindgebruikers opvraagbaar zijn, waarbij in ieder geval de overdrachtsverzoeken die voldoen aan:

- valide zijn (Sessievalidatie tegen het TC blijkt correct)
- leerling is bekend (BSN komt voor in het bronsysteem)

getoond moeten worden.

De informatie die getoond wordt van een dergelijk verzoek moet voldoende zijn om een eindgebruiker in staat te stellen het gevraagde dossier (wanneer de eindgebruiker dit besluit) gereed te maken voor overdracht. De minimale informatie die daarvoor getoond moet worden is:

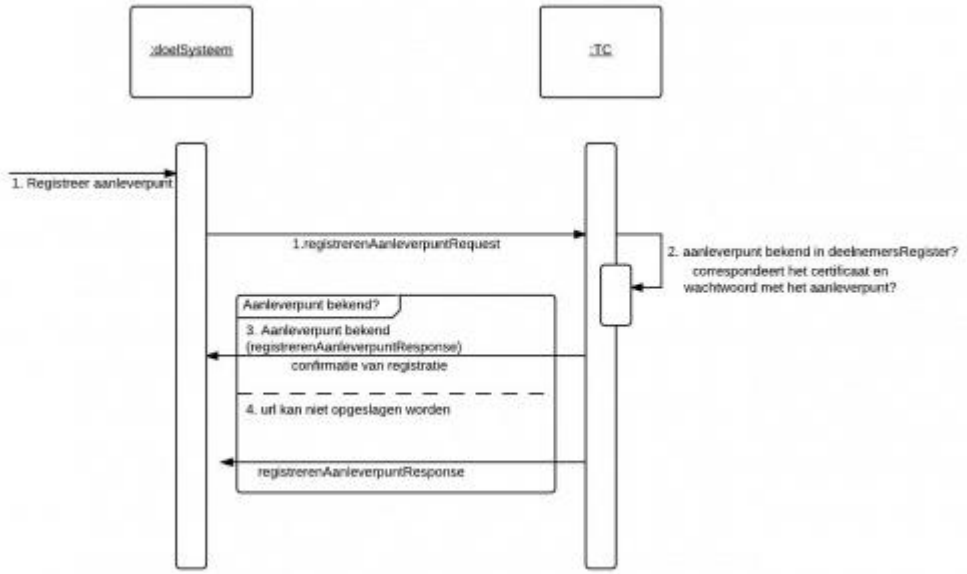
- BSNleerling
- BRIN van aanvragende school
- AP label van aanvragend AP
- datum/tijdstip binnenkomst van aanvraag

19. AANLEVERPUNT REGISTREREN

De Overstapservice biedt deelnemende systemen de gelegenheid om zelf de url's van hun aanleverpunten te onderhouden. Hiertoe moet het bestaan van het aanleverpunt wel al bekend zijn in het deelnemersregister in het Traffic Center.

- Context: In het Traffic Center wordt per brinnummer bijgehouden welke aanleverpunten bekend zijn. Een school/bestuur kan via mijn oso handmatig aanleverpunten aanmaken. Na het aanmaken van het aanleverpunt kan een deelnemende school de url registreren. Uiteindelijk zal deze url gebruikt worden door het doelSysteem om een dossier op te vragen. Het registreren van aanleverpunten is met name van toepassing op bronSystemen.
- Initiator: Het LAS of RP
- Responder: Het Traffic Center
- Pre: Het LAS of RP beschikt over een geldig certificaat en wachtwoord om dit request te kunnen versturen. Het aanleverpunt is bekend in het deelnemersregister.
- Post: Indien het aanleverpunt bekend is en het certificaat correspondeert met het aanleverpunt, dan krijgt het LAS of RP een positief resultaat terug.
- Request:

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns="http://xml.eld.nl/schemas/Overstapservice/20140327">
   <soapenv:Header/>
   <soapenv:Body>
      <ns:registrerenAanleverpuntRequest>
         <ns:aanleverpunt>1</ns:aanleverpunt>
         <ns:schoolId>98PO</ns:schoolId>

<ns:url>https://tester.bks.kennisnet.nl/productieDemoSchool.php<
/ns:url>
      </ns:registrerenAanleverpuntRequest>
   </soapenv:Body>
</soapenv:Envelope>
```



- Response:

```
<SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/">
   <SOAP-ENV:Header/>
   <SOAP-ENV:Body>
      <over:registrerenAanleverpuntResponse
xmlns:over="http://xml.eld.nl/schemas/Overstapservice/20140327">
         <over:resultaat>RegistratieGelukt</over:resultaat>
      </over:registrerenAanleverpuntResponse>
   </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

19.1. Sequence diagram Registreren Aanleverpunt

- Normal flow:

  (1) Een doelSysteem verstuurt een registreer aanleverpunt request naar het Traffic Center.
  (2) Het Traffic Center controleert of het aanleverpunt bekend is en of het doelSysteem gemachtigd is om de url van dit aanleverpunt te registreren.
  (3) Het Traffic Center geeft een positief antwoord indien het registreren van het aanleverpunt gelukt is.

- Alternatives:

  geen

- Exceptions:

  (4) De url kan niet opgeslagen worden bij het aanleverpunt welke in het registrerenAanleverpuntRequest is meegegeven.

19.2. Overzicht meldingen

Resultaat	Type flow (N, A, E)	Omschrijving
RegistratieGelukt	N	De url is geregistreerd voor het aanleverpunt
AanleverpuntOnbekend	E	Het certificaat correspondeert met het aanleverpunt in de registreerAanleverpuntRequest, echter het aanleverpunt is (nog) niet aangemaakt in het Traffic Center. Als men in mijn OSO een aanleverpunt handmatig toevoegt, dan wordt het aanleverpunt middels een synchronisatie proces aangemaakt in het Traffic Center. Het duurt meestal een aantal minuten voordat het aanleverpunt ook daadwerkelijk aangemaakt is in het Traffic Center.
OngeldigeURL	E	De url welke meegegeven wordt in het registreerAanleverpuntRequest is niet valide.
SysteemOnbekend	E	Het certificaat correspondeert met het brinnummer en aanleverpunt in de registreerAanleverpuntRequest, echter het brinnummer is niet bekend in het Traffic Center. Dit scenario kan voorkomen indien een school gedeactiveerd wordt in het Traffic Center.
OngeautoriseerdAanleverpunt	E	De aanleverpuntcode in het certificaat correspondeert niet met het aanleverpunt in het registreerAanleverpuntRequest.

20. TRAFFIC CENTER PINGEN

Het Traffic Center is een essentieel onderdeel in de communicatie tussen Doel- en Bronsysteem. Voor beide partijen is het van belang om te weten of het Traffic Center online is.

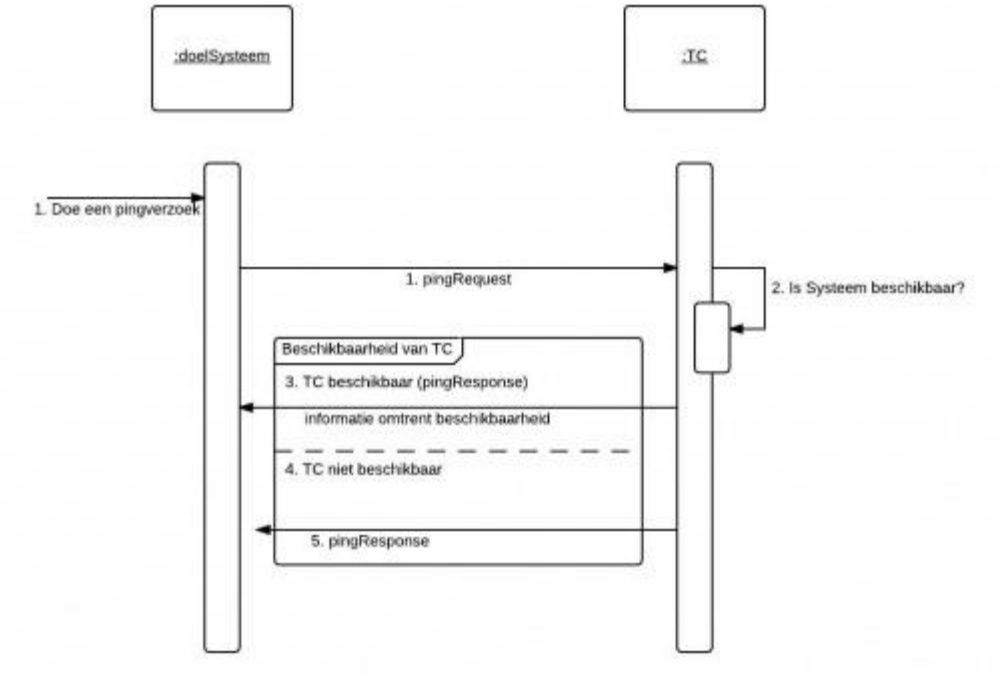
- Context: De operationele status van het Traffic Center kan opgevraagd worden met behulp van de ping service. Dit is een optionele service en kan ten alle tijden worden gebruikt om de status van het Traffic Center op te vragen. Indien het Traffic Center online is, wordt er een positief antwoord teruggegeven omtrent de beschikbaarheid en het versienummer van de software op het Traffic Center.

- Initiator: Het LAS of RP
- Responder: Het Traffic Center
- Pre: Het LAS of RP beschikt over een geldig certificaat en wachtwoord om dit request te kunnen versturen.
- Post: Indien het Traffic Center online is, krijg het LAS of RP een positief antwoord terug met daarin de applicatieversie
- Request:

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns="http://xml.eld.nl/schemas/Overstapservice/20140327">
   <soapenv:Header/>
   <soapenv:Body>
      <ns:pingRequest/>
   </soapenv:Body>
</soapenv:Envelope>
```

- Response:

```
<SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/">
   <SOAP-ENV:Header/>
   <SOAP-ENV:Body>
      <over:pingResponse
xmlns:over="http://xml.eld.nl/schemas/Overstapservice/20140327">
         <over:available>true</over:available>

<over:applicationVersion>2.1.9</over:applicationVersion>
```




```
            <over:systemTime>2014-09-29T04:05:37</over:systemTime>
         </over:pingResponse>
      </SOAP-ENV:Body>
   </SOAP-ENV:Envelope>
```

20.1. Sequence Diagram Ping Service

- Normal flow:

  (1) Een doelSysteem verstuurt een ping request naar het Traffic Center.
  (2) Het Traffic Center controleert of er op dit moment geen onderhoudswerkzaamheden plaatsvinden en het systeem beschikbaar is voor uitwisselingen
  (3) Het Traffic Center geeft een positief antwoord terug omtrent de beschikbaarheid, het versienummer van de software welke op het Traffic Center draait en de huidige systeemtijd.

- Alternatives:

(4) Er vinden onderhoudswerkzaamheden op het Traffic Center plaats.

- Exceptions:

  (5) Het Traffic Center geeft een negatief antwoord terug omtrent de beschikbaarheid, het versienummer van de software welke op het Traffic Center draait en de huidige systeemtijd.

Het Traffic Center is niet beschikbaar en/of de omgeving waar het Traffic Center op draait is niet beschikbaar. Er wordt geen antwoord teruggegeven aan het doelSysteem. Afhankelijk van de timeout instellingen bij het doelSysteem wordt er een timeout teruggegeven.

20.2. Overzicht meldingen

Resultaat	Type flow (N, A, E)	Omschrijving
True	N	Het Traffic Center is beschikbaar.
False	A	Het Traffic Center is niet beschikbaar. Er vinden op dit moment onderhoudswerkzaamheden plaats.
Timeout	E	Indien het Traffic Center binnen 30 seconden geen response teruggeeft, moet de initiator een time-out (fout) afhandelen (en melden aan eindgebruiker).

21. OSO:BEVEILIGING

21.1. Uitgangspunten beveiliging OSO

In de Overstapservice wisselen systemen documenten uit die betrekking hebben op leerlingen. De gegevens zijn gekwalificeerd als vallende in risicoklasse II, zoals gedefinieerd in het document AV-23, opgesteld door de Registratiekamer. Deze informatie moet goed afgeschermd zijn tegen inzage en wijzigen door derden. Dit hoofdstuk bevat de eisen en maatregelen voor het beveiligen van informatie voor specifieke interacties en systemen. In essentie bestaat de beveiliging van de communicatie uit twee principes:

1. Alle communicatielijnen zijn versleuteld.
2. De overdracht van een document kan alleen binnen een door het Traffic Center gecontroleerde sessie.

Deze principes zijn vooral gericht op het voorkomen van toegang tot leerlinggebonden informatie door partijen buiten de Overstapservice. OSO is zich ervan bewust dat het Traffic Center op deze manier niet alle mogelijke onbedoelde opvragingen kan ondervangen. Diverse systemen in de Overstapservice moeten een log bijhouden, zodat controle achteraf mogelijk wordt.

21.1.1. Versleuteling BSN

In de Overstapservice is het niet toegestaan om het burgerservicenummer (BSN) te versturen naar het Traffic Center. Daarom bevatten interacties met het Traffic Center nooit het PGN, maar een afgeleide identificatie, de zoeksleutel genaamd. De zoeksleutel wordt afgeleid uit het PGN van de leerling. Om te voorkomen dat onbevoegden deze zoeksleutel weer tot het PGN kunnen herleiden is de zoeksleutel altijd asymmetrisch versleuteld. De cryptografische sleutel voor deze versleuteling is publiek. De bijbehorende privésleutel voor ontsleuteling is echter alleen bekend bij de backoffice.

Een systeem dat beschikt over het PGN van de leerling kan de zoeksleutel met deze stappen afleiden:

TODO: Definitief vaststellen gebruik/opbouw zoeksleutel

21.1.2. PKI certificaten en TLS 1.2

De Overstapservice vereist het gebruik van X.509 certificaten voor het gebruik in TLS ten behoeve van:

- authenticatie van de server;
  - Middels het zogenoemde servercertificaat. Dit bevat metadata waarmee de betreffende server uniek geïdentificeerd kan worden. Bijv. domeinnaam, organisatie van de eigenaar. Het certificaat is ondertekend door een publiek erkende Certificate Authority. Hiermee is de identiteit van de entiteit onweerlegbaar vastgesteld.
- authenticatie van de client;
  - Middels het zogenoemde clientcertificaat. Dit bevat metadata waarmee een unieke (systeem)gebruiker, instelling of natuurlijk persoon zich kan identificeren bij een server. Bijv. BRIN, inschrijfadres. Het certificaat is ondertekend door de OSO CA, waarmee binnen de OSO keten deze identiteit onweerlegbaar is vastgesteld.
- versleuteling van de verbinding tussen client en server.

De certificaten in de overstapservice kunnen uitgegeven zijn door:

- de backoffice, een zogenaamd OSO-certificaat;
- een willekeurige, maar wel publiek erkende Certificate Authority, dit heet in dit ontwerp een Public Trusted Server (PTS-) certificaat.

21.1.2.1. OSO eisen aan verbindingen tussen systemen

- In de OSO keten zal alleen het TLS 1.2 beveiligingsprotocol worden gehandhaafd voor alle verbindingen. Voorgangers als SSL en TLS 1.0 en 1.1 zijn uitgesloten.
- Binnen OSO wordt alleen een RSA key van tenminste 2048 bit toegestaan. Wegens mogelijke

compatibiliteitsproblemen worden ECDSA keys alleen in overleg toegestaan.

Om de beveiligde technische transport laag waarvoor TLS wordt ingezet goed te laten functioneren moeten er een aantal zaken geregeld worden. Deze hebben betrekking op zowel de verzendende kant als de ontvangende kant. Zo zullen de volgende zaken op zijn minst geregeld moeten zijn:

- Zowel de verzendende als ontvangende zijde maakt gebruik van volledig up-to-date gehouden software en onderliggende componenten (webserver software, TLS bibliotheek, etc);
- Er is zowel een geldig OSO- als PTS-certificaat aanwezig;
- De juiste protocollen zijn geconfigureerd;
- De juiste ciphers suites zijn geconfigureerd;
- Een webserver met PTS-certificaat biedt de volledige certificate chain tot de root CA aan;
- Zowel de OSO- als PTS-certificaten worden bij elke nieuwe communicatiesessie gevalideerd tegen het betreffende root CA certificaat;
- PTS-certificaten worden door clients bij elke nieuwe communicatiesessie gevalideerd tegen de bij de root CA horende publieke CRL (Certificate Revocation List) / OCSP (Online Certificate Status Protocol) service. Voor OSO-certificaten geldt deze eis op dit moment nog niet;
- Private keys zijn veilig opgeslagen en niet vanuit de (web)applicatie via het internet of anderszins ongeautoriseerd te benaderen;
- Communicatie is end-to-end versleuteld zonder herversleuteling, packet inspection of wordt onversleuteld verzonden binnen een private netwerk.

Om een basis veiligheidsniveau te kunnen garanderen binnen de OSO keten dient elke webserver die gebruik maakt van een PTS-certificaat, getest te worden middels de Qualys SSL Labs Server Test. Dit is een onafhankelijke test welke de TLS implementatie van een webserver test. Het basis niveau waaraan elke webserver binnen de OSO keten dient te voldoen is A-. Het signature algoritm van het PTS-certificaat moet bij elke nieuwe uitgifte of vernieuwing voorzien worden van minimaal sha256 met RSA encryption. Sha1 wordt medio 2016 uitgefaseerd door grote softwarebouwers wegens inmiddels jaren

bekende zwakheden. Sha256 is hier wel tegen bestand. Voor het OSO-certificaat wordt dit reeds door de backoffice gerealiseerd. Nadat zowel server als client elkaar vertrouwen is het van belang om de juiste versleutelingsprotocollen voor de communicatie sessie te hanteren. Het gebruik van TLS 1.2 maakt het mogelijk gebruik te maken van sterke versleutelingsprotocollen. Om OSO uitwisselingen zo veilig mogelijk te maken worden de volgende voorwaarden gesteld:

- Het is alleen toegestaan cipher suites met een versleutelingssterkte van 128bit of hoger te gebruiken;
- De cipher suite AES GCM wordt als geprefereerde suite gehanteerd;
- Forward Secrecy dient ondersteund en geprefereerd te worden;
- De server bepaalt de cipher suite volgorde;
    - Cipher suites gebruik makend van Anonymous of NULL authenticatie en suites gebaseerd op EXPORT, DES, RC4, 3DES, MD5, PSK, AECDH zijn met name maar niet uitsluitend, niet toegestaan. Mocht er een situatie ontstaan waaruit blijkt dat ook andere ciphers niet veilig genoeg zijn dan zal deze lijst worden uitgebreid.

21.1.3. Verificatie van certificaten

Binnen OSO zijn er drie verschillende interacties waarbij de certificaten tc en/of aangesloten partijen worden toegepast:

Interactie	**Stappen**
LAS/RP maakt verbinding met TC	1. LAS/RP vereist server authentication van het TC met een PTS-certificaat. 2. LAS/RP valideert het servercertificaat van het TC. 3. Het TC vereist nu client authentication van LAS/RP met een OSO-certificaat. 4. Het TC valideert het clientcertificaat van LAS/RP.
LAS/RP maakt verbinding met ander LAS/RP	1. LAS/RP A vereist server authentication van LAS/RP B met een PTS-certificaat. 2. LAS/RP A valideert het servercertificaat van LAS/RP B. 3. LAS/RP B vereist nu client authentication van LAS/RP A met een OSO-certificaat. 4. LAS/RP B valideert het clientcertificaat van

Mocht de situatie zich voordoen dat communicatie tussen twee partijen niet opgezet kan worden omdat niet voldaan kan worden aan de gestelde voorwaarden om te mogen communiceren dan zal het proces moeten worden afgebroken. Aan de gebruiker zal een melding moeten worden teruggegeven dat de overdracht niet gelukt is en dat er contact opgenomen moet worden met de leverancier. Tevens moet dit incident duidelijk gelogd opdat beheerders van het systeem kunnen achterhalen wat er fout is gegaan. De eisen aan certificaten en versleuteling zijn gebaseerd op de stand van de techniek op het moment van schrijven. Het kan gezien de veranderde beveiligingsomstandigheden noodzakelijk zijn om af te wijken van deze ontwerp documentatie. Handige referentiedocumentatie betreffende het correct inrichten van de webserver, met uiteraard in acht name van de OSO eisen, is te vinden op bijvoorbeeld de Qualys sites.

Hoewel Kennisnet geen partij is (en wil zijn) in het LAS/RP - LAS/RP verkeer, zal het beveiligingsniveau van deze verbinding wel periodiek gecontroleerd worden door Kennisnet

21.1.4. Informatiebeveiliging per interactie

Interactie	Maatregelen
Sessie initiëren	• Doelsysteem verifieert servercertificaat van het Traffic Center. • Traffic Center verifieert het clientcertificaat van het Doelsysteem. • Doelsysteem en Traffic Center versleutelen de verbinding. • Traffic Center logt de interactie.
Dossier opvragen	• Doelsysteem verifieert het servercertificaat van Bronsysteem. • Doelsysteem en Bronsysteem versleutelen de verbinding. • Doelsysteem geeft een sessieID door aan het Bronsysteem. • Bronsysteem verifieert sessieID bij TC (zie onder) voorafgaand aan verzenden dossier. • Doelsysteem logt de interactie. • Bronsysteem logt de interactie.
Sessie controleren	• Bronsysteem verifieert het servercertificaat van het Traffic Center. • Traffic Center verifieert het clientcertificaat van de Bronsysteem. • Documentbron en Traffic Center versleutelen de verbinding. • Bronsysteem geeft sessieID door aan Traffic Center. • TrafficCenter verifieert sessieID.

	• Traffic Center logt de interactie. • Bronsysteem logt de interactie.
Sessie afmelden	• Doelsysteem verifieert servercertificaat van het Traffic Center. • Traffic Center verifieert het clientcertificaat van het Doelsysteem. • Doelsysteem en Traffic Center versleutelen de verbinding. • Traffic Center logt de interactie.

22. OSO:RELEASES

Deze pagina geeft een overzicht van de OSO versies.

datum	omschrijving	toegepaste dossier standaard	live datum	opmerkingen
2015-02	OSO'15	[EduStandaard OSO 1.2.1]	Nog te bepalen	Dossier standaard mogelijk 1.2.2
2014-02	Fase 2B	[EduStandaard OSO 1.1.1]	20140701	Huidige versie

23. 2015-02

Hieronder volgen links naar de plaatsen waar de wijzingen in OSO'15 (tov 2b):

- ~~Geen aanpassingen aan distributie pki certificaten~~

1. Uitbreiding afmelden sessie bericht tbv rapportage
2. Notificatie dossier aanvraag
3. Aanpassing bestandsgrootte
4. Meervoudige levering
    1. Meervoudige ontvangst: afhandelen van meerdere leveringen van hetzelfde dossier (identiek bsn)
    2. In OSO?15 is gekozen om de implementatie van selectieve uitlevering niet verplicht te stellen.
5. Toepassen nieuwe versie [EduStandaard (1.2.x)]
6. Lokale controle op correctheid dossier voorafgaand aan verzending
7. Toestemming/inzage ouders/verzorgers aanpassen
8. Aflopen aanleverpunten
    1. Toevoegen status ?LeveringInBehandeling?

24. OSO:PROGRAMMA VAN EISEN

24.1. Programma van Eisen OSO '15

Deze wiki dient als functionele beschrijving van de dienst OSO en aangesloten partijen voor OSO?15 (schooljaar 2015-2016). Deze functionele beschrijving vormt de basis voor het Progamma van Eisen aan deelnemers aan OSO?15. Om te kunnen deelnemen aan OSO?15 en dient een Leerling Administratie Systeem (LAS) of Regionaal Platform (RP) te voldoen aan de functionele en technische eisen die in deze wiki beschreven worden. Deze gelden als minimaal eisenpakket voor het aansluiten van een systeem op de productieomgeving van het OSO Traffic Center. Naast de in de wiki genoemde eisen moet een LAS of RP (en haar leverancier) voldoen aan eisen die voortvloeien uit bestaande wetten en normen, zoals de Wet Bescherming Persoongegevens. Die eisen worden niet gespecificeerd, omdat ze in het algemeen van toepassing zijn op schoolinformatiesystemen en niet specifiek gelden voor het deelnemen aan OSO?15. Het ontwerp doet geen uitspraak over de procedurele/procesmatige aspecten die in deelnemende scholen/organisaties ingericht moeten worden. Deze aspecten worden afgedekt bij de kwalificatie van scholen.

24.1.1. Eisen aan LASsen en RP's

	Bereik	Eis
101a	Algemeen	Ieder systeem ondersteunt ten minste de use cases: OSO:Aansluiting realiseren en OSO:Uitwisselen Test School
101b	Algemeen	Ieder systeem ondersteunt ten minste de scenario's: Aanleverpunt Registreren en Traffic Center Pingen
102a	PO Bronsysteem	Een PO bronsysteem ondersteunt de use cases: OSO:Dossier klaarzetten en OSO:Inzage of toestemming verlene
102b	PO Bronsysteem	Een PO bronsysteem ondersteunt ten minste de scenario's: Sessie Controleren en Dossier inzien door ouders/verzorgers en Dossier valideren enNotificeren van aanvraag en Aanleverpunt F
102c	PO Doelsysteem	Een PO Doelsysteem ondersteunt ten minst de use case: Dossier opvragen
102d	PO Doelsysteem	Een PO doelsysteem ondersteunt ten minste de scenario's: Sessie Initiëren en Dossier Opvragen en Sessie Afmelden.
103a	VO Bronsysteem	Een VO bronsysteem ondersteunt de use cases: OSO:Dossier klaarzetten en OSO:Inzage of toestemming verlene
103b	VO Bronsysteem	Een VO bronsysteem ondersteunt ten minste de scenario's: Sessie Controleren en Dossier inzien door ouders/verzorgers en Dossier valideren enNotificeren van aanvraag en Aanleverpunt F
103c	VO Doelsysteem	Een VO Doelsysteem ondersteunt ten minst de use case: Dossier opvragen
103d	VO Doelsysteem	Een VO doelsysteem ondersteunt ten minste de scenario's:

		Sessie Initiëren en Dossier Opvragen en Sessie Afmelden.
104a	BinnenBRIN Bronsysteem	Een BinnenBRIN bronsysteem ondersteunt de use cases: OSO:Dossier klaarzetten en OSO:Inzage of toestemming verlenen
104b	BinnenBRIN Bronsysteem	Een BinnenBRIN bronsysteem ondersteunt ten minste de scenario's: Sessie Controleren en Notificeren van aanvraag en Aanleverpunt Registreren
104c	BinnenBRIN Doelsysteem	Een BinnenBRIN Doelsysteem ondersteunt ten minste de use case: Dossier opvragen
104d	BinnenBRIN Doelsysteem	Een BinnenBRIN doelsysteem ondersteunt ten minste de scenario's: Sessie Initiëren en Dossier Opvragen en Sessie Afmelden.

24.1.2. Overzicht

	default	POPO	POVO	VOVO	binnenBRIN
bron	• Aanleverpunt Registreren • Traffic Center Pingen	• Inzage of toestemming verlenen • Dossier klaarzetten • Sessie Controleren	• Inzage of toestemming verlenen • Dossier klaarzetten • Sessie Controleren	• Inzage of toestemming verlenen • Dossier klaarzetten • Sessie Controleren	• Dossier klaarzetten • Sessie Controleren
doel	• Aanleverpunt Registreren • Traffic Center Pingen	• Sessie Initiëren • Dossier Opvragen • Sessie Afmelden	• Sessie Initiëren • Dossier Opvragen • Sessie Afmelden	• Sessie Initiëren • Dossier Opvragen • Sessie Afmelden	• Sessie Initiëren • Dossier Opvragen • Sessie Afmelden

24.1.3. Interface eisen

	Bereik	Eis
105	Algemeen	Een aanleverpunt van een bronsysteem dient een webservice aan te bieden conform de interface specificatie van de geldende ELDDeelnemer_<versie>.wsdl. Deze webservice dient via het publieke internet benaderbaar te zijn.
106	Algemeen	Elk aanleverpunt in staat om de webservices van andere deelnemers en van het Traffic Center aan te spreken via het publieke internet.
107a	Algemeen	Een systeem dat een interactie start, wacht gedurende minimaal de gespecificeerde responstijd op antwoord.
107b	Algemeen	Een systeem in een interactie een verzoek moet beantwoorden, doet dit binnen de gespecificeerde maximale responstijd
	Bereik	**Eis**
110	Algemeen	Het verstrekkende LAS verstrekt een opgevraagd document altijd in de actuele versie van de [EduStandaard OSO].
110	Algemeen	Een systeem stuurt geen berichten die de afgesproken maximale

bericht- en bijlage- grootte overschreiden.

24.1.4. Technische beveiligings eisen

	Bereik	Eis
200	Algemeen	Een systeem implementeert en volgt de voorschriften en adviezen op zoals beschreven in het deel OSO beveiliging.
201	Algemeen	Een systeem hanteert alleen TLS 1.2 voor alle verbindingen, zowel naar TC als naar bron- en/of doel- systemen.
201a	Algemeen	Een systeem moet zich bij het Traffic Center kunnen authenticeren met een OSO-certificaat, vallend onder het OSO rootcertificaat;
201b	Algemeen	Een aanleverpunt authenticeert zich aan een client met een certificaat van een vertrouwde Certificate Authority.

24.1.5. Eisen aan logging

	Bereik	Eis
301	Algemeen	Logregels bevatten altijd het sessie-id
302	Algemeen	Een systeem registreert logregels voorzien van datum en tijd, met een nauwkeurigheid van 1 seconde.
303	Algemeen	Een systeem garandeert een maximale afwijking van de UTC + 01:00 tijd (de tijdzone waarin Nederland valt) van 5 seconden.
304	Algemeen	De informatie in een logregel voor de eindgebruiker is voldoende zelfbeschrijvend om zonder contextinformatie uit het systeem de actie te kunnen herleiden tot de verantwoordelijke (rechts)persoon.
305	Algemeen	Logregels worden duurzaam bewaard en beschermd tegen verlies en verandering tot 2 jaar nadat de leerling is uitgeschreven.
306	Algemeen	Logregels kunnen na creatie niet worden aangepast of verwijderd.

25. OSO:WOORDENLIJST

woord	verklaring	toelichting
Aanleverpunt (AP)	Koppelvlak van gekwalificeerd bron- en/of doel-systeem.	Een aanleverpunt bevat het (web)adres van een bron- of doel-systeem van een instelling/school.
Bijlage	Document dat wordt toegevoegd aan een OSO dossier (technisch: een attachment).	De velden in de EduStandaard OSO vormen een basis voor de uitwissel-informatie-behoefte van scholen. Zaken die (nog) niet afbeeldbaar zijn op de velden van de EduStandaard OSO kunnen als bijlage alsnog verzonden worden.
binnenBRIN	Uitwisseling tussen systemen die binnen dezelfde school/instelling gebruikt worden.	Type overstap dat binnen OSO wordt ondersteund.
Bronsysteem	Een LAS, RP of andersoortig systeem aangesloten op OSO dat (een) dossier(s) aanbiedt.	Gekwalificeerd informatiesysteem dat overstapdossiers aanbiedt via een aanleverpunt.
Documentstandaard	Zie EduStandaard OSO	
Doelsysteem	Een LAS, RP of andersoortig systeem aangesloten op OSO dat (een) dossier(s) opvraagt.	Gekwalificeerd informatiesysteem dat overstapdossiers opvraagt bij de aanleverpunt(en) van een school/instelling.
EduStandaard OSO	De open afspraak over en specificatie van de gegevensset en toepassing hiervan binnen OSO.	Zie ook de OSO website.
Gegevensset OSO	De specificatie van het dossier zoals dat overgedragen wordt binnen de OSO infrastructuur. Binnen OSO wordt hier de EduStandaard OSO voor gebruikt.	Zie ook de OSO website.
Kennisnet Validatie Service (KVS)	Zelfstandige voorziening die toegepast wordt binnen OSO om dossiers te controleren op structuur en inhoud (beperkt).	De voorziening is vanwege juridische overwegingen buiten het OSO domein geplaatst. Zie ook KVS Wiki.
Kwalificatie (leverancier)	Proces waarbij wordt vastgesteld dat Leverancier voldoet aan eisen gesteld in het Programma van Eisen van OSO.	De kwalificatie is een voorwaarde voor het toevoegen van door de leverancier geleverde bron- en/of doel-systemen aan OSO.
Kwalificatie (school)	Proces waarbij wordt vastgesteld dat een School voldoet aan de eisen die OSO stelt (????)	De kwalificatie is een voorwaarde voor het toelaten van de school op OSO.

Leerling Administratie Systeem (LAS)	Een informatiesysteem dat door scholen en instellingen wordt gebruikt voor het administreren van leerlingen, studieresultaten en andere zaken.	In OSO een bron- of doel-systeem voor het leveren of ontvangen van dossiers.
Onderwijskundig Rapport (OKR)	Wettelijk voorgeschreven dossier dat door een latende school moet worden opgesteld en verstrekt aan een nieuwe school.	Het OKR wordt wettelijk voorgeschreven, maar de inhoud en de structuur zijn (grotendeel) vrij en wijken regionaal af. De EduStandaard OSO probeert een gemeenschappelijke basis te vormen, waarbij uitbreidingen en afwijkingen via bijlagen aan het dossier kunnen worden toegevoegd.
POPO	Primair Onderwijs naar Primair Onderwijs	Type overstap dat binnen OSO wordt ondersteund.
POVO	Primair Onderwijs naar Voortgezet Onderwijs	Type overstap dat binnen OSO wordt ondersteund.
Regionaal Initiatief (RI)	Een groep samenwerkende scholen die oa gebruik maken van een Regionaal Platform in hun administratieve keten.	Samenwerkingsverbanden zijn een specifieke vorm van RI's.
Regionaal Platform (RP)	Een informatiesysteem gedeeld door scholen van een RI dat naast of in plaats van een LAS wordt gebruikt.	RP's ondersteunen (vaak) een bepaalde type overstap (POVO) in plaats van gebruik te maken van OSO als transportmiddel. RP's koppelen wel met OSO voor andere typen overstap en 'buiten regionale' overstappen.
Traffic Center (TC)	Centraal component binnen OSO die de toegang tot het OSO netwerk bewaakt.	
VOVO	Voortgezet Onderwijs naar Voortgezet Onderwijs	Type overstap dat binnen OSO wordt ondersteund.
Zoeksleutel	Versleuteld burgerservicenummer(BSN) van leerling dat als id voor een dossier wordt toegepast.	De zoeksleutel wordt gegenereerd bij ieder nieuw verzoek.